# Cybersecurity of Recreational Electric Boats Onboard Communication Networks

**Zoltán Farkas[1] and György Györök[2]**

1 Óbuda University, Doctoral School on Safety and Security Sciences, Bécsi Str. 96/b, 1034 Budapest, Hungary, e-mail: farkas.zoltan2@uni-obuda.hu

[2] Óbuda University, Alba Regia Faculty, Budai Str. 45, 8000 Székesfehérvár, Hungary, e-mail: gyorok.gyorgy@amk.uni-obuda.hu

***Abstract:*** *Recreational boating has experienced the emergence of trends that originated in the automotive industry several years ago, including electromobility, telematics systems and cloud-based services. These novel possibilities have given rise to new cybersecurity challenges, which boat builders must address. To ensure the safe operation of a lithium-ion battery, it is essential to implement an effective battery management system. This device processes data from the appropriate sensors and performs complex control tasks. Information is transmitted over a common communication bus, and there is also a need to access the data remotely via a telematics system. Lithium batteries have introduced the possibility of DC fast charging, which brings additional safety risks. To ensure optimal management, it is essential to guarantee data integrity, allowing the BMS to maintain the battery within the optimal operational range. This paper discusses the potential vulnerabilities and risks, and presents some solutions to reduce the cybersecurity risks for electric boats.*

*Keywords: Recreational boating; Cybersecurity; Lithium-ion; Battery*

# 1 Introduction

Recreational electric boats, like most specialized electric vehicles, are built in small numbers. Boatbuilders typically procure and install most components from a specialized company, as these are already available on the market. This makes building a system that meets the rising cybersecurity challenges difficult. The electronic control units (ECUs) usually communicate with each other via CAN bus, which is traditionally unencrypted and easily manipulated if an attacker gains access. Unfortunately, the industry does not emphasize cybersecurity adequately, and has no mandatory requirements. Devices in different functional groups should be physically segmented, with a gateway that allows access to critical systems on the boat only when needed.

In addition to the traditional physical attack surfaces, wireless communications and telematics systems have emerged. Wireless devices must be integrated into the system in a way that prevents them from taking control of critical systems. For example, a telephone connected to the boat's infotainment system does not need to have access to the components of the drivetrain. Telematics systems are becoming increasingly popular in the marine industry. They can be used to remotely control the various onboard devices and monitor the status of the vessel. Features such as remote control of the air conditioner or wine cooler are available for the user. In addition, the service team in the background can receive information on any of the vessel's systems, facilitating the service process. The features offered enhance the user experience and may also decrease the service costs for the manufacturer. Special attention should be given to cybersecurity in the design of these systems. To ensure safety and security, it is crucial to prevent malicious attackers from accessing the telematics system. Despite all efforts, there is always a possibility of unauthorized access, but it should not affect critical vehicle systems. Any unauthorized access should be detected and eliminated.

Current lithium-based battery technologies make it possible to build fast, long-range electric boats. This type of battery chemistry is the preferred choice for boat builders due to its high energy density. However, high energy density also brings higher risks, with faster degradation or, in extreme cases, emergencies caused by overloading lithium batteries. It is worth being prepared for the possibility of malicious attackers targeting the batteries, causing financial losses or personal injuries in the worst case.

# 2 Off-Highway Electric Vehicles

The sales figures for an off-highway electric vehicle are not even close to the sales figures for a standard production car. Electric recreational boats are no different. Some models may sell only a few units per year. To meet these demands, it would be difficult to design and manufacture all the components of a boat individually for a given model. As a result, many of the components built into a boat are not developed for that particular model, but rather, are products of companies that specialize in specific components. A typical example is the multifunction display (MFD) that companies buy off the shelf and install in their boat. They can save on development costs by buying these commercial-off-the-shelf (COTS) products, but they are forced to adapt them to the capabilities of the equipment they are buying. The cybersecurity capabilities of the devices are no different. These devices come from different vendors and use different protocols, firmware, and security solutions. This heterogeneity poses a significant challenge to the coherence of cybersecurity protection [1]. In contrast, the situation is very different for mass-produced cars. In

the automotive industry, cybersecurity has been a serious issue for some time, with existing standards and best practices to help manufacturers design appropriate systems. To get a good picture of the cybersecurity issues of off-highway electric vehicles, it is worth comparing the situation in the automotive industry. Standard automotive models use closed, highly integrated systems where all components and software fit into a comprehensive, centrally designed architecture. This allows them to manage vehicle cybersecurity as a complete system where all devices must comply [2][3].

# 3 Attack Surface Assessment

## 3.1. CAN Bus

The Controller Area Network (CAN bus), a communication protocol that is widely used in the automotive industry, is also employed in this context, with various onboard devices exchanging data using this protocol. The on-board diagnostics (OBD) connector, which is installed on vessels, enables device configuration and monitoring and facilitates the detection of faults by providing access to the CAN bus. However, because communication on the bus is typically unencrypted, direct access also poses a cybersecurity risk. Gary has demonstrated in [4] that communication is vulnerable to exploitation if an attacker is able to attach a rogue device to the bus. If the rogue device is installed, an attacker could reconfigure devices, steal information, or manipulate the vessel's operation. It is good practice to make critical system data and settings accessible only after authentication. Adequate protection can be built into the system with cryptography. After successful authentication, critical functions can be accessed, or devices can be reconfigured. The method allows for the use of multiple access levels. Once authenticated, a timer is triggered that resets the elevated access level to normal and makes the protected functions and settings no longer accessible after a preset time. This authentication method can be supported by all critical onboard devices, making it a more secure solution.

Alternatively, or additionally, the system can include a gateway that handles the authentication process before granting access. If the attacker gains physical access after the gateway, the on-board devices are left unprotected, making this method less secure. It is important to note that the CAN bus can be attacked in several ways. For example, an attacker with access could spoof the values sent by different sensors by sending different values periodically to the same address to which the sensor sends the data. This could interfere with the devices that process the sensor values and make decisions based on them. The transmission rates and amount of data exchanged on the CAN bus limit the feasibility of encrypting all data transmitted

on the bus, although there are existing examples of encrypted CAN bus communication [5].

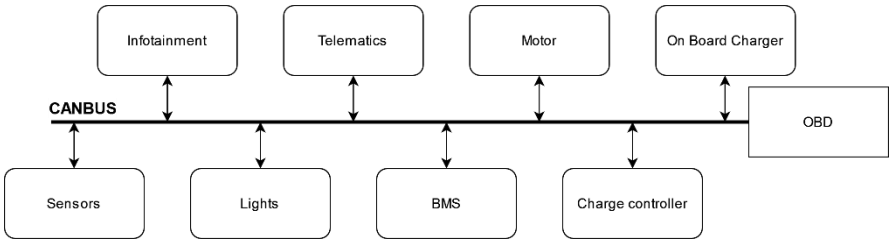


Figure 1
Architecture of the CAN bus

Figure 1 illustrates the interconnection of devices with different functions. Internal communication occurs via the CAN bus, to which the telematics and infotainment devices are connected. As the figure demonstrates, this shared topology presents a dual-use scenario: while it allows for remote control of convenience functions but also poses a security risk as it can provide remote access to attackers. The boat's diagnostic connector provides direct access to devices connected to the bus, making the CAN bus vulnerable to attacks. Better protection is achieved by segmenting the communication bus by function. A gateway can transmit messages between different functional buses if needed. Figure 3 illustrates the schematic of such a system. The devices on the bus can be grouped in an arbitrary manner according to communication requirements. A notable benefit of segmented buses is that their traffic volume is lower than that of a single bus. The diagram also displays the diagnostic connector, which is not mandatory for recreational craft as it is for automotive applications. From a network security perspective, it is recommended to avoid using it altogether. Instead, diagnostics can be implemented much more safely via the telematics module.

The following example illustrates a practical application: the motor status can be displayed on the captain's helm display. The process of doing so is as follows: The motor controller periodically transmits motor data (RPM, torque, temperature) to the drive system's CAN bus with a designated CAN ID. The gateway device receives this message, compares the CAN ID with those that have been predefined, and runs the appropriate routine. In this scenario, the routine retrieves the specific data from the frame and transmits it in the designated format to the NMEA2000 bus. Consequently, in the event of a compromise to a specific device on a given bus, the gateway impedes the ability of malicious devices to disrupt the operation of devices on other buses. It is important to note that devices operating on the same bus as the rogue device would remain unprotected using this method. However, the incident could still be detected.

## 3.2. NMEA 0183

Serial bus communication where devices must be connected to the bus as described in the EIA-422 standard. Interception or disruption of communication is easily achievable through the insertion of a rogue device. The standard is used more in commercial shipping these days. Its use in recreational boating has been entirely replaced by the NMEA 2000 standard [6].

## 3.3. NMEA 2000

The NMEA2000 standard allows onboard instruments, displays, and other devices to communicate with each other. This communication protocol has been developed specifically for the maritime industry. It is a CAN bus communication protocol, electrically identical to the CAN bus. Therefore, the same security requirements apply. The bus cables, connectors and splitters are easy to identify, making it easy to fit a new device on the bus. This significantly increases vulnerability.

## 3.4. OneNet Communication Network

As seen in [7] "The OneNet Standard for IP Networking of Marine Electronic Devices is a marine industry standard, developed by members of NMEA, based on Internet Protocol, Version 6 (IPv6) and the IEEE 802.3 Ethernet Local Area Network." It is crucial to note that the OneNet standard was not created to replace previous standards. Rather, it complements their functionality by linking them to facilitate communication between devices. In developing the standard, the organization also kept cybersecurity in mind. We will not discuss this further because a properly constructed OneNet network is considered secure [8].

## 3.5. Telematics

Telematics can be used to remotely monitor specific parts of the vehicle or the entire system, control equipment, and change its properties. This system enables the transfer of vehicle status data to a remote server and the reception of remote commands. The analysis of shared data can facilitate the streamlining of service processes and the avoidance of costly repairs through the implementation of preventive maintenance measures. The telematics device can access the vessel's communication buses, including the CAN bus, which enables it to monitor the status of other devices and intervene in their operation. In addition to these useful features, the cybersecurity risks associated with the collection and transmission of data cannot be neglected. Therefore, when designing a telematics system, it is crucial to implement state-of-the-art security and encryption technologies. If an unauthorized attacker were to gain access to such a system, they could remotely take control of

the vehicle without having to be near the vessel. Telematics must ensure that communications are fully encrypted and that both sides are only accessible by identification. End-to-end encryption should be used. It is of critical importance that a telematics module be unable to gain access to the data associated with other vehicles through a remote server or, more worryingly, disrupt their operation. Accordingly, each device is required to have its own login ID, which enables it to access only its own data on the remote server. This prevents a compromised device from causing further damage to the network.

## 3.6. Battery Management System

The Battery Management System (BMS) is responsible for ensuring that the battery is loaded under optimal conditions. For the BMS to function effectively, it must have access to the voltages, temperatures, and load currents of the battery cells at all times. The data is typically transmitted via CAN bus. The integrity of the battery data must be protected to ensure that the battery operates within safe limits. The overloading of the battery can result in accelerated degradation, and in extreme cases, may even lead to thermal runaway. To guarantee operational reliability, it is essential to ensure that the communication bus is free from any interruptions or manipulation by malicious actors. These systems are novel in the recreational marine sector, and few manufacturers have relevant experience with their operation. It is therefore recommended that these systems be the subject of special attention during the design phase [9][10].

## 3.7. DC Fast Charging

Lithium batteries can be charged at a much faster rate than previous battery technologies. As a result, fast charging stations have emerged, which can charge the battery pack at high power when directly connected to the battery. The vehicle and charging station negotiate the charging characteristics before and during charging, and this communication can be achieved via PLC or CAN bus. The in-vehicle communication module should be isolated from other devices so that a charging station infected with malicious code cannot attack the boat. The vehicle can share payment information with the charging station to automate payments, but communication between the two endpoints must be encrypted. However, the vehicle has no control over how the charging station shares information with third parties, such as the payment service provider [11-13].

# 4 Threat Assessment

Based on the identity of the attackers, it is possible to distinguish between internal and external threats.

An internal threat refers to unauthorized access by boat users to the boat's systems. An example of such user abuse is when the owner attempts to change the available functions of the vessel or the parameters of the drivetrain in the hope of increasing motor power. In both cases, economic damage could be caused, or unauthorized access could cause a malfunction. Defending against misuse of the vessel's diagnostic port is challenging because the attacker has physical access. The system must prevent users from changing critical system settings.

External threats include unauthorized access, such as hacking, phishing, and malware. To defend against these threats, a variety of security measures should be implemented to prevent unauthorized access and intrusion into the system. Unfortunately, such attacks can also occur remotely. For example, as demonstrated in automotive cybersecurity research [14], a smartphone infected with malware that connects to the boat's unsegmented infotainment system via Bluetooth or Wi-Fi could serve as a bridgehead. From there, if the network lacks a secure gateway, the malware could pivot to the CAN bus and disrupt critical drivetrain communications.

To summarize, the threat model for recreational electric boats encompasses both physical proximity risks (e.g. diagnostic port manipulation by users) and remote, digital vectors (e.g. telematics and wireless exploits). Addressing both of these fronts necessitates a holistic, "defense-in-depth" approach that is tailored to the recreational boating environment.

# 5 Risk Assessment

The challenges of cybersecurity and the actual threats to boat safety demonstrate that digital threats can cause incapacitation or loss of control. Such loss of control over critical systems can lead to disruptions, economic damage, or, in the worst case, endanger the lives of those on board or the environment around the vessel. It is also important to avoid the significant threat of theft of private data from a phone connected to consumer electronics. Theft of sensitive user data can result in a loss of reputation due to inadequate protection. An actual threat is that attackers could modify the settings of a component in the drivetrain, such as the motor control unit. This could result in a reduction in performance, a dangerous increase in performance, malfunction or inoperability of the vessel.

In 2015, two researchers were successful in taking remote control of a Jeep Cherokee without modifying the vehicle beforehand. They were able to remotely control systems such as braking, steering, and engine management. This case shows

just how serious cybersecurity needs to be taken in the connected car concept. The results are frightening [15].

The recreational boating industry must also take serious steps to prevent such attacks. Industry players such as boat builders and software designers have a key role to play in ensuring that vessels are resilient to potential cyber threats.

# 6 Illustrative Attack Scenario, Based on Automotive Incidents

Since publicly documented cyberattacks in the recreational boating sector are currently limited, we rely on well-documented threat models from the automotive industry to illustrate the practical implications of the vulnerabilities discussed in this paper. The following scenarios demonstrate how an attacker could exploit the specific maritime systems presented earlier.

## 6.1. Remote attacks

Based on the mentioned incident [15] in 2015, we can assume that an inadequately protected telematics system or an infected mobile phone connected to the on-board electronics could serve as an entry point to the boat's communication networks.

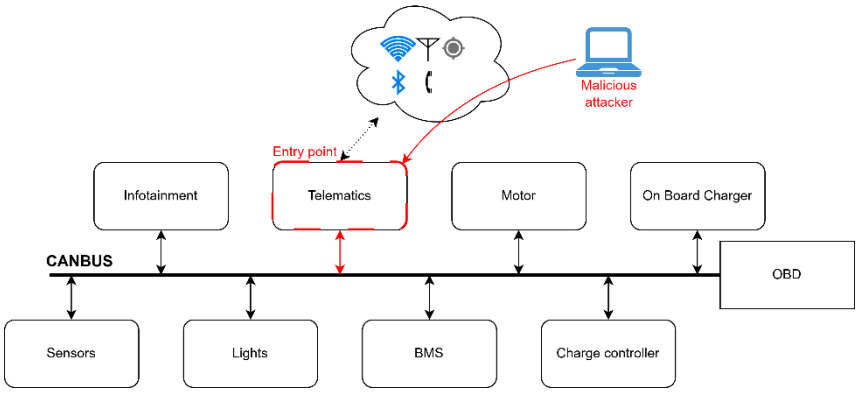


Figure 2
Vulnerability of an unsegmented CAN bus architecture to remote attacks

As demonstrated in Figure 2, a malicious attacker can exploit wireless interfaces (e.g. Wi-Fi, Bluetooth, or cellular networks) to remotely compromise the telematics unit. As illustrated by the diagram, once this designated entry point has been breached, the attacker is granted unrestricted access to the shared CAN bus. If an attacker gains access to such a device and uses it to access other communication

networks, as in the case of a connected car, the attacker can take control of critical systems, such as motor control, steering, autopilot, maneuvering thrusters and BMS.

## 6.2. Physical attacks

Any possible physical access to a communication bus carries serious vulnerability [14][16]. Recreational boats are equipped with easily accessible peripherals such as GPS antennas and environmental sensors that communicate via the NMEA2000 bus. By simply unscrewing or forcibly removing these devices an attacker can gain direct physical access to the entire NMEA 2000 backbone. This process is further facilitated by the fact that the standard's physical connectors and its communication protocol, including the Parameter Group Number (PGN) messages, are well-documented and widely known. Such access makes it easy to identify and manipulate devices connected to the network. By removing a GPS antenna and connecting to the communication bus, the boat's digital switching system becomes accessible, through which additional devices can be controlled.

# 7 Preventive Measures

## 7.1. OTA Software Updates

Regular installation of patches can help maintain secure operation and fix discovered vulnerabilities through remote software updates. However, this useful feature can also be dangerous if the system is not properly protected. To prevent attackers from installing malicious software on one boat or the entire fleet, the boat should always verify the source and integrity of the software package before installing it. The system should be designed to allow the client-side to verify the package received from the server-side using certificates. Additionally, a unique signed software package should be created for each boat to avoid the installation of the same malicious code on the entire fleet. [17][18].

## 7.2. Remote Access Restriction

Marine digital switching is a system that enables the operation of boat devices from the display, other on-board controls, or a mobile device. The control unit is connected to the NMEA2000 bus and can be managed either directly from the bus or via a wireless connection. The control unit is equipped with inputs and outputs, which it switches or processes in accordance with a predetermined program. The present trend in this field is toward the digital control of all functions, either from

the display or remotely via a smartphone. Nevertheless, critical systems, such as the motor starting, may only be enabled via a switch that cannot be activated by the remotely accessible and controllable systems of the vessel alone. This prevents attackers from being able to start the vehicle with only remote access. To enhance security, systems that do not require remote control or do not provide significant convenience, such as anchor winch control, should be switched separately. The use of these switches should be combined with the boat ignition key. It is suggested that on-board equipment be classified at the design stage as to whether it can be remotely controlled. Table 1 shows an example of remote access classification for some devices. As outlined in the table, critical safety and operational functions, such as the side thruster and anchor winch, must have remote access strictly prohibited to prevent unauthorized physical movement of the vessel. Conversely, non-critical convenience features like the audio system, lighting, and air conditioning can remain remotely available without compromising the core safety of the boat.

Table 1
Devices classified by control

| **Function** | **Remote access** |
|---|---|
| Motor start | Combined with the ignition system |
| Side thruster | Remote access prohibited |
| Anchor winch | Remote access prohibited |
| Audio system | Remotely available |
| Lighting | Remotely available |
| Air conditioning | Remotely available |
| … | |

## 7.3. Limit CAN Bus Access

An attack may be indicated by anomalies observed in communication on the bus. These anomalies could include a change in the frequency of periodic messages or the appearance of messages that are not in the device's predefined database. A device connected to the communication bus with sufficient computing capacity can perform detection. The CAN bus gateway module shown in Figure 3 is a suitable choice for this task [19], [20]. In the figure, the communication bus has been divided into several smaller buses, and the gateway device is responsible for the connection between the buses on demand. It has access to the entire communication and can signal to the operator via the telematics module if it detects misuse.

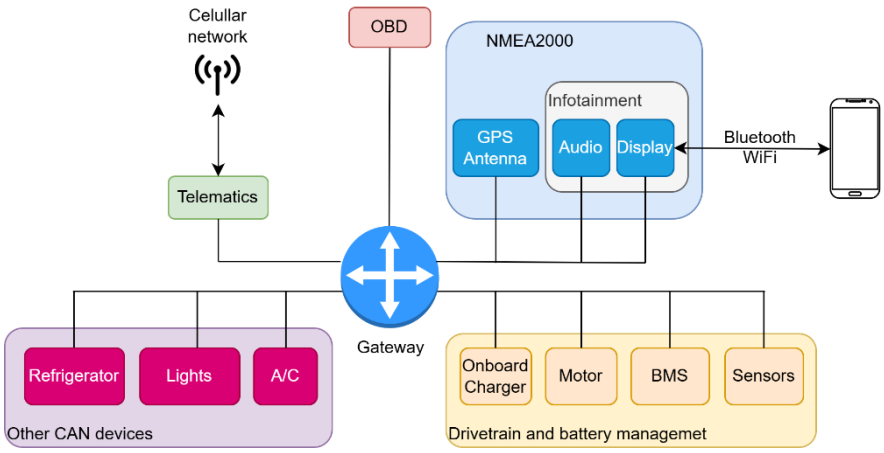


Figure 3

CAN bus protected by a gateway [21]

## 7.4. Restrict Service Accesses of the Onboard Devices

Installed devices often support wired or wireless communication protocols that allow for feature configuration. In boatbuilding, these protocols can simplify manufacturing processes. However, the security of these protocols is often questionable. They are simply not designed to withstand an attack in the end-user application. It is advisable to make these protocols inaccessible after production, if possible. If complete disablement is not feasible, it is imperative to ensure that they are adequately safeguarded against potential attacks by unauthorized personnel.

# 8 Conclusions and Future Work

The recreational boating industry has also been affected by the trend of constantly evolving consumer electronics with the rise of electromobility. Devices are now interconnected with each other and with cloud-based services. However, the use of cybersecurity practices in this industry is not yet widely adopted. Therefore, boat builders must consider the entire system to ensure adequate protection is in place. However, this can be challenging as built-in tools are often not tailored to the specific product and are instead purchased from the market for a specific purpose, leaving little room for customization. Planning and implementing appropriate defenses against attacks is critical to avoiding reputational damage, financial loss, or personal injury.

Research on cybersecurity has been predominantly conducted within the domain of commercial maritime transport [1, 4, 22-24]. The introduction of recommendations

on cybersecurity for recreational boat builders by the organizations that oversee the industry's standards would be a beneficial development. In addition, it is suggested that vehicle cybersecurity be viewed as a large interconnected system, the way it works. Review the need for interconnections between devices and leave only those that are truly necessary.

One suggested approach is the transfer of best practices from other industries to boat design. The automotive industry places great importance on such threats and has conducted extensive research and established numerous standards to help car manufacturers develop robust systems. However, recent studies [3] point out that the regulatory landscape is still evolving and that stringent, mandatory security assessments for all complex vehicular IT components are often lacking, even in modern passenger vehicles. This highlights the fact that the recreational boating industry cannot blindly adopt automotive commercial-off-the-shelf (COTS) systems, but must consciously develop and implement its own rigorous, domain-specific security architecture.

Future work may include the creation of a combined gateway and telematics system that can also serve as an intrusion detection system in a recreational boating environment would represent a valuable continuation of the research. The system would be capable of performing the functions discussed in Chapter 7. The operational efficacy of the system could then be assessed through a rigorous testing process, encompassing both simulated conditions and real-world boating scenarios. Since the current study primarily provides a conceptual framework and risk assessment, this future empirical validation will be crucial. Furthermore, upcoming research should focus on designing and analyzing secure, marine-specific telematics protocols that can withstand advanced remote cyberattacks.

# References

[1] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin, “Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre,” in *2018 2nd Cyber Security in Networking Conference (CSNet)*, 2018, pp. 1–8. doi: 10.1109/CSNET.2018.8602669.

[2] G. Abdelkader, K. Elgazzar, and A. Khamis, “Connected Vehicles: Technology Review, State of the Art, Challenges and Opportunities,” *Sensors*, vol. 21, no. 22, Art. no. 22, Jan. 2021, doi: 10.3390/s21227712.

[3] H. Hegyi and L. Erdődi, “Modern Passenger Vehicles as Cyber Threat Source: Analyses of Surveillance Options through Smart Vehicles,” *ACTA POLYTECH HUNG*, vol. 22, no. 2, pp. 9–28, 2025, doi: 10.12700/APH.22.2.2025.2.2.

[4] G. C. Kessler, “The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities,” *TransNav*, vol. 15, no. 3, pp. 531–540, 2021, doi: 10.12716/1001.15.03.05.

[5] A. Rasheed, M. Baza, Mahmoud. M. Badr, H. Alshahrani, and K.-K. R. Choo, “Efficient Crypto Engine for Authenticated Encryption, Data Traceability, and Replay Attack Detection Over CAN Bus Network,” *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 1, pp. 1008–1025, 2024, doi: 10.1109/TNSE.2023.3312545.

[6] Actisense, “Everything you need to know about NMEA 0183.” Accessed: Nov. 23, 2024. [Online]. Available: https://actisense.com/wp-content/uploads/2021/01/Everything-you-need-to-know-about-NMEA-0183-1.pdf#page=4.05

[7] “NMEA OneNet,” National Marine Electronics Association. Accessed: Nov. 20, 2024. [Online]. Available: https://www.nmea.org/nmea-onenet.html

[8] “NMEA-OneNet-and-Ethernet-Networking-guide-1.pdf.” Accessed: Nov. 19, 2024. [Online]. Available: https://actisense.com/wp-content/uploads/2023/07/NMEA-OneNet-and-Ethernet-Networking-guide-1.pdf

[9] P. V. Chombo and Y. Laoonual, “A review of safety strategies of a Li-ion battery,” *Journal of Power Sources*, vol. 478, p. 228649, Dec. 2020, doi: 10.1016/j.jpowsour.2020.228649.

[10] L. Bravo Diaz *et al.*, “Review—Meta-Review of Fire Safety of Lithium-Ion Batteries: Industry Challenges and Research Contributions,” *J. Electrochem. Soc.*, vol. 167, no. 9, p. 090559, Jan. 2020, doi: 10.1149/1945-7111/aba8b9.

[11] A. Chandwani, S. Dey, and A. Mallik, “Cybersecurity of Onboard Charging Systems for Electric Vehicles—Review, Challenges and Countermeasures,” *IEEE Access*, vol. 8, pp. 226982–226998, 2020, doi: 10.1109/ACCESS.2020.3045367.

[12] J. Johnson *et al.*, “Cybersecurity for Electric Vehicle Charging Infrastructure,” SAND2022-9315, 1877784, 708580, Jul. 2022. doi: 10.2172/1877784.

[13] I. Skarga-Bandurova, I. Kotsiuba, and T. Biloborodova, “Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations,” in *2022 IEEE International Conference on Big Data (Big Data)*, Osaka, Japan: IEEE, Dec. 2022, pp. 3099–3106. doi: 10.1109/BigData55660.2022.10020644.

[14] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN Bus Security Challenges,” *Sensors*, vol. 20, no. 8, p. 2364, Jan. 2020, doi: 10.3390/s20082364.

[15] C. Valasek and C. Miller, “Remote Exploitation of an Unaltered Passenger Vehicle”.

[16] R. Gesteira-Miñarro, G. López, and R. Palacios, “Revisiting Wireless Cyberattacks on Vehicles,” *Sensors*, vol. 25, no. 8, p. 2605, Jan. 2025, doi: 10.3390/s25082605.

[17] H.-Y. Chien and N.-Z. Wang, “A Novel MQTT 5.0-Based Over-the-Air Updating Architecture Facilitating Stronger Security,” *Electronics*, vol. 11, no. 23, p. 3899, Nov. 2022, doi: 10.3390/electronics11233899.

[18] M. Stanojevic, D. Capko, I. Lendak, S. Stoja, and B. Jelacic, “Fighting Insider Threats, with Zero-Trust in Microservice-based, Smart Grid OT Systems,” *ACTA POLYTECH HUNG*, vol. 20, no. 6, pp. 229–248, 2023, doi: 10.12700/APH.20.6.2023.6.13.

[19] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, “Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review,” *J Wireless Com Network*, vol. 2019, no. 1, p. 184, Dec. 2019, doi: 10.1186/s13638-019-1484-3.

[20] A. Taylor, N. Japkowicz, and S. Leblanc, “Frequency-based anomaly detection for the automotive CAN bus,” in *2015 World Congress on Industrial Control Systems Security (WCICSS)*, London, United Kingdom: IEEE, Dec. 2015, pp. 45–49. doi: 10.1109/WCICSS.2015.7420322.

[21] M. Hashem Eiza and Q. Ni, “Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity,” *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017, doi: 10.1109/MVT.2017.2669348.

[22] I. Ashraf *et al.*, “A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2677–2690, 2023, doi: 10.1109/TITS.2022.3164678.

[23] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, “Cybersecurity Challenges in the Maritime Sector,” *Network*, vol. 2, no. 1, Art. no. 1, Mar. 2022, doi: 10.3390/network2010009.

[24] M. A. Ben Farah *et al.*, “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,” *Information*, vol. 13, no. 1, Art. no. 1, Jan. 2022, doi: 10.3390/info13010022.