IoT Industrial Battery Surveillance

Filip Jaredson & Ilian Ayoub

Abstract

The purpose of this project was to research solutions for remote logging and surveillance of industrial batteries using Internet of Things (IoT). Using the CANOpen protocol, a CAN bus, 4G communication, a MariaDB database, and Vue.js/Node.js webapp, an was delivered as a proof of concept of the possibilites of remote battery surveillance.

Keywords: IoT, 4G, Logging, CAN, CANOpen

Introduction

The world is getting more and more connected as technology progresses. Information is key in this connected environment since research and productivity are leading factors in development. Thus, the demand for IoT devices is increasing, since they make valuable data more accessible.

When it comes to industrial batteries, their data is essential to both the customer and the producer. The batteries contain information describing their current status, as well as logs of previous states. For the customer, knowing this information is useful for planning logistics, such as knowing how much battery is left in a certain machine or knowing the life expectancy of the battery itself. The producer, on the other hand, uses this information to assess the performance of the batteries by examining how they are used by the customers. Hence, remote logging and surveillance of the batteries is useful for both the customer and producer.

The focus of this project was to develop a prototype machine that provides this funcitonality. This was done using Raspberry Pi 4, with a CAN module and 4G module for communication.

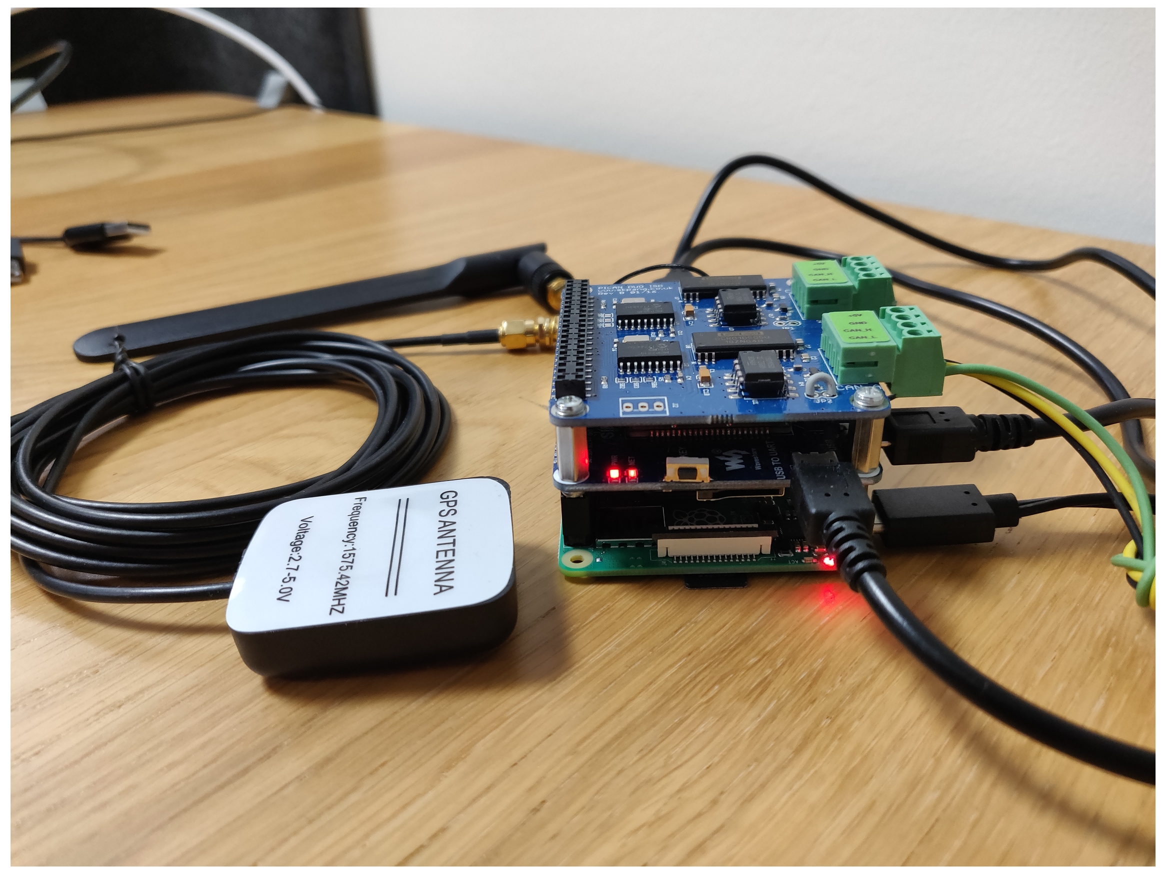

Figure 1: Picture of the finished product.

CAN & CANOpen

CAN is a commonly used hardware communication protocol in the vehicular industry because of its redundance and robustness. In recent years, the status of CAN has driven the development of CANOpen, a high-level communication protocol which extends CAN with a bit more functionality and easier implementation.

In the project, both CAN and CANOpen were used for communication between the battery and IoT device. Using the hardware protocols, the device asked the battery for updates on different kinds of data periodically, and the battery responded with messages that contained the relevant raw data. CANOpen was a particularly good tool for this, since it gave the user knowledge of what kind of data was accessible, and thus allowed the user to ask for specific data.

4G Communication to Server

In order to make the data more accessible to both the users and developers, some form of centralized database was required to keep the most important data updated. In our case, this required some form of communication between the IoT device and the server that hosted this database.

Using a 4G hat for the Raspberry Pi, the IoT device communcated with the server over encrypted telecom internet with the server. This way, the device was able to push the most recent data to the database, and kept the data accessible to authorized users who may or may not be able to access the device physically. This was very useful in both development and after, since the 4G telecom network is wide spread and reliable

Data Processing and Visualization

Finally, after the data was collected and synchronized with the central database, it was processed and visualized. The processing categorized the data depending on the source, and converted the raw data to different data types in order to make them easier to interpret.

This processed data was then viualized on a web page accessible to developers and customers. The web page was implemented using Vue.js as a frontend and Node.js backend, and visually implemented using Material Design, which resulted in a lightweight, responsive user interface.

Conclusions

The ultimate challenge of this project was to collect data and visualize it, which was accomplished in a rudimentary fashion. In this sense, the result of the project is that a device for remote surveillance is entirely possible and can be very beneficial, as has been mentioned. However, along with this important result, we came to some other conclusions during the project.

The most difficult thing that we found was combining automatization with encrypted data traffic. It was difficult to create an automatic push to the database without jeopardizing the data security of the application. This, combined with the lack of reliability of the 4G connection initialization, required a lot of effort in implementation and are important for the system on a larger scale. Thus, more research would have to be done on how to further develop this aspect of the project.

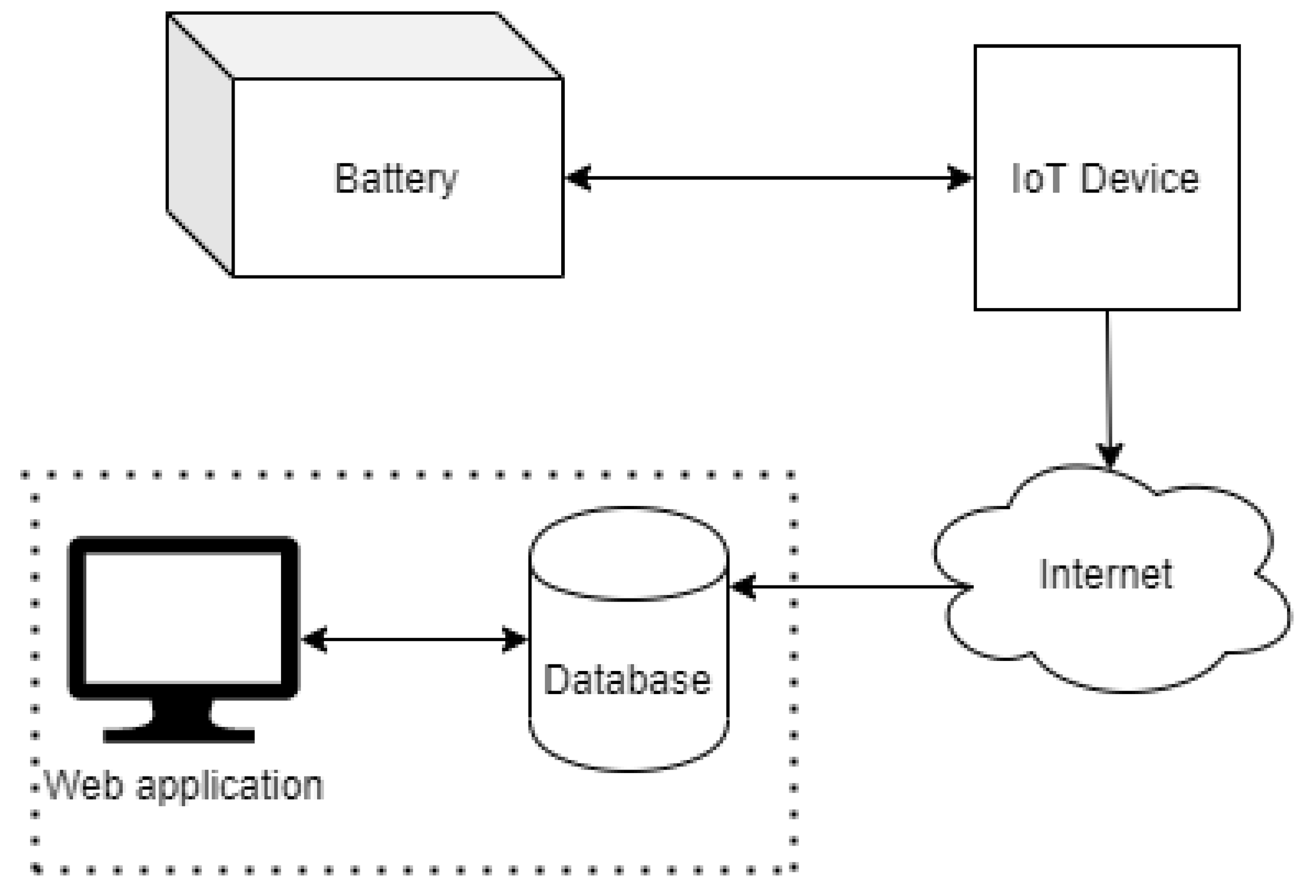

Figure 2: Overview of the system.

Acknowledgements

This project was done in collaboration with Alelion Energy Systems, as well as LINK-SIC. We worked especially close with the Systems Engineering group at Alelion, lead by Peter Tammpere. We would like to thank the parties involved.