Analysis of Electrical Manipulation on the ICEBOX Device

12-13-2023
13:28

The Beginning

Since May of 2023, we have been focused on creating an attack for the Icebox power line load sensor. This device is responsible for taking periodic readings of the physical state of power lines in remote regions. These readings are sent to power grid operators using MQTT over LTE. This data helps operators maximize the efficiency of the grids power transmission. This data is used with weather forecasts along with previous readings to make forecasts for power distribution conditions. This sensor provide the opportunity for real time modifications to power distribution to increase efficiency or protect infrastructure. This is because the devices are out in the field and provide real data of the conditions of the power line. The ability to trust these sensors is key to their usefulness. If we are able to find an attack that makes these devices untrustworthy then it would be possible to damage power distribution infrastructure or increase the cost of electricity.

The Components

The Icebox is composed of four main parts.

1. TAL 20000 Load Cell

The TAL 20000 utilizes a Wheatstone Bridge to convert the physical load of the power line into an analog electrical signal.

2. PartnerPlast Amplification Board

The PartnerPlast board is connected to the load cell and is responsible for extending the capabilities of the nRF9160dk through the GPIO pins. It supplies power to the nRF9160dk, amplifies the signal from the Load Cell, and connects the signal from the Load

Cell to the nRF9160dk. The important GPIO connections are:
- P0.14: Amplified Load Cell Signal
- P0.15: Percentage of Battery Voltage (Voltage Divider)
- P0.17: DK Sample Trigger
- P0.31: SCL for 24FC256 EEPROM
- P0.30: SDA for 24FC256 EEPROM
- P0.20: AREF (VDD Reference)

There is a 24FC256 EEPROM on the PartnerPlast board that communicates with the nRF9160dk. We aren't certain of the whole functionality of this EEPROM but we believe that in part it is acts as a hardware key for the nRF9160dk application. This is because if the original nRF9160dk isn't connected to the EEPROM then the application will not start.

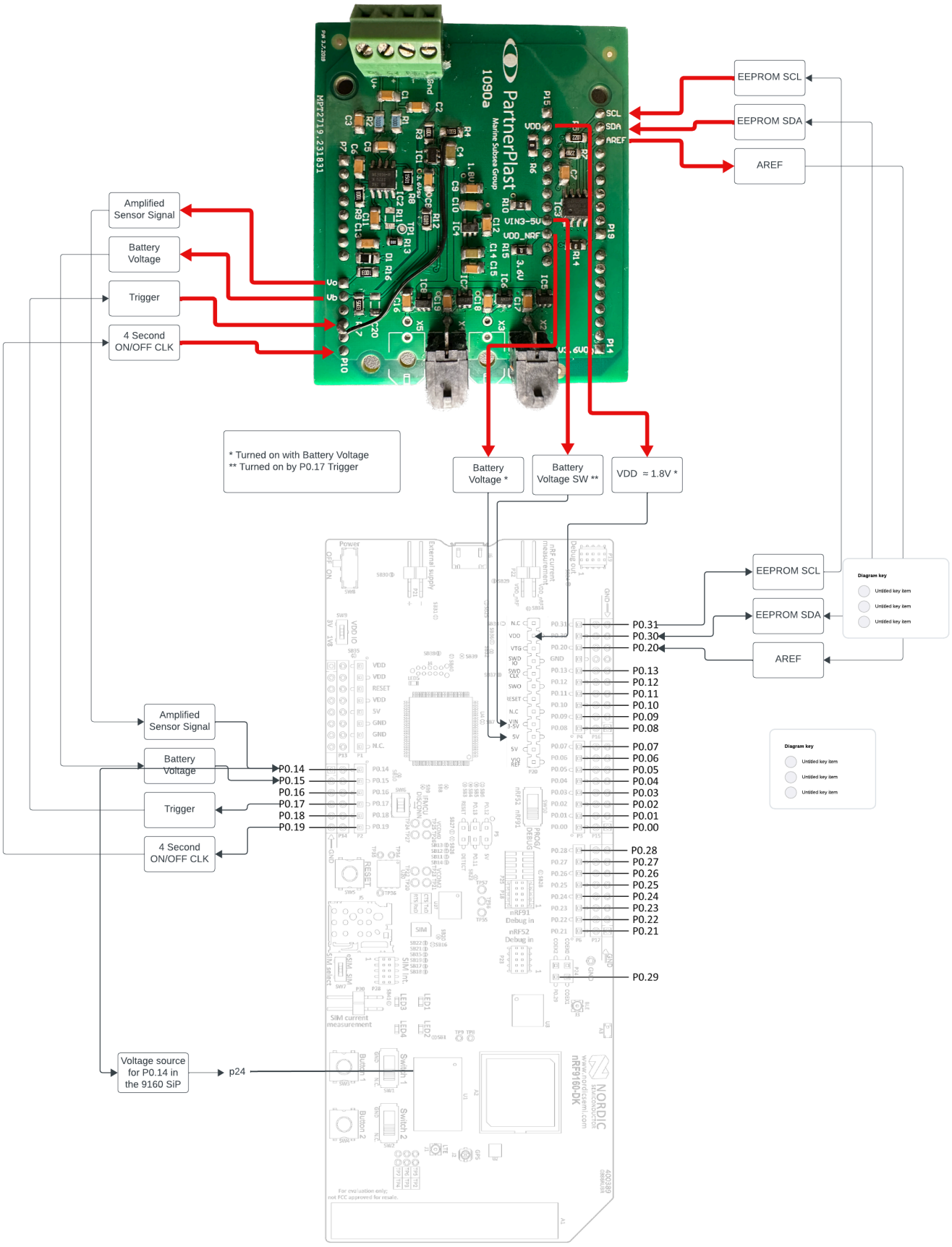
3. Nordic Semi nRF9160dk

The nRF9160dk from Nordic Semiconductor is the main controller of the Icebox device. It is a programmable IOT device with LTE and Bluetooth capabilities along with GPIO (General Purpose Input Output) expansion pins. It has a SAADC (Successive Approximation Analog-to-Digital Converter) along with a Cortex-M33 programmable processor which is used to run the device applications. The nRF9160dk utilizes a Zephyr RTOS (Real Time Operating System) to manage the operations of the application. This is the device that transforms the electrical signals from the batteries and Load Cell into digital numbers.

4. LSH 20 Batteries

The LSH 20 is a Lithium-Thionyl battery which allows for longer operating lifespans, however, these batteries are not rechargeable. They have a wide range for operating temperatures as well as long shelf lives. They have an output voltage of 3.6V and a 13Ah

capacity.



The Attack

The focus of our attack on the Icebox device is the operating Battery Voltage of the device. We chose this as our attack vector for the following reasons:

1. Ease of Attack

Manipulating the operating voltage of the Icebox device is both easy for us in the lab as well as easy for a possible attack vector. All it would require is changing out the batteries. There is no complicated PCB modification or anything that would require extended time with the device.

2. Functionality of Wheatstone Bridge

When studying the Load Cell we found that the Wheatstone Bridge was the electrical mechanism for the sensor and the output of the Wheatstone Bridge was dependent on what Excitation Voltage was applied to the bridge. This made us want to discover what exactly would happen if we manipulated the Excitation Voltage for the Load Cell/Wheatstone Bridge. We measured that the Excitation Voltage was equal to the operating Battery Voltage so we theorized that we could manipulate the Excitation Voltage by manipulating Battery Voltage.

3. Power Supply Range of the nRF9160dk

The nRF9160dk has a Supply Voltage range of 3.0V-5.5V which means that we have a wide range for manipulation while keeping the nRF9160dk operational. It also means that we could explore under powering the device as well as increasing the operation Battery Voltage.

Experimentation

After deciding our attack vector we needed to begin taking measurements so we would have data on the effect our attack had at different parts of the Icebox device. We have two nRF 9160 Development Kits that we could use to program with our own custom applications so we started by creating our ADC Terminal application. The first tests we ran were not representative of the state of the Icebox device so we could not rely on the data from the first experiments. However, we were able to see a change in the output voltage from the Load Cell.
After those first experiments we kept developing the ADC Terminal

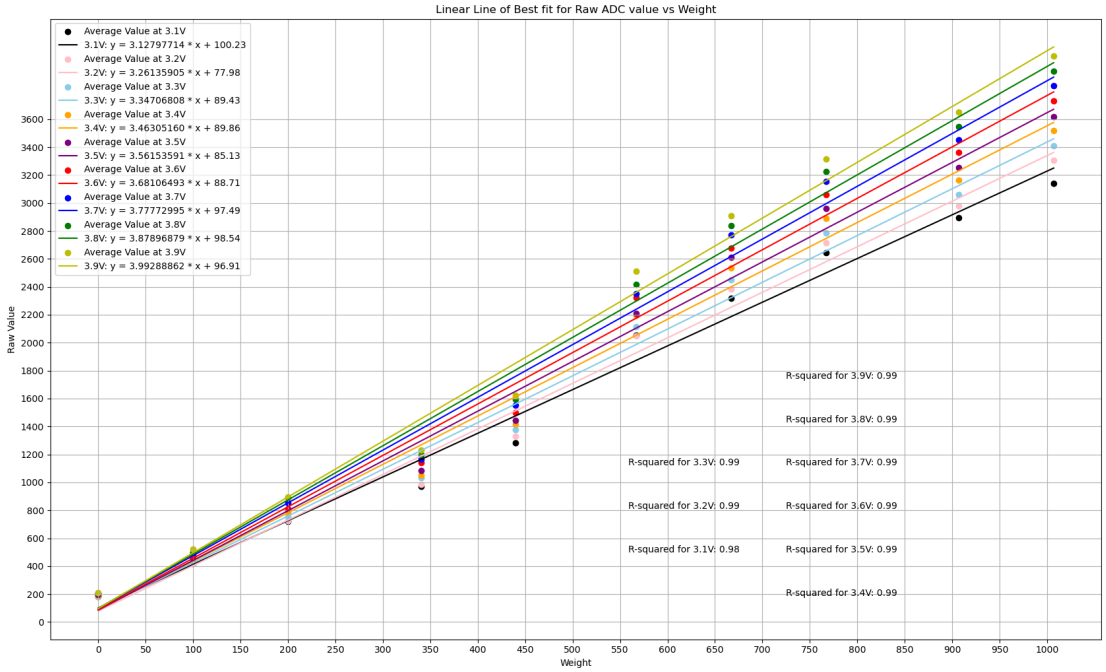
application along with creating a new AWS Terminal application. The ADC Terminal application would print the SAADC measurements to the serial terminal of the nRF9160dk while the AWS Terminal application would connect to AWS and send the SAADC measurements to AWS through MQTT.
This new AWS Terminal application would allow us to replicate the connection between the nRF9160dk and PartnerPlast boards. We were also able to read the Memory Registers on the nRF9160dk which gave us the actual configuration for the SAADC. Now that we had the correct SAADC configuration along with replicating the correct connection state of the two boards we could begin collecting data on the effects of out attack.
For this new experiment we ran tests with different weights on the Load Cell at different battery supply voltages.

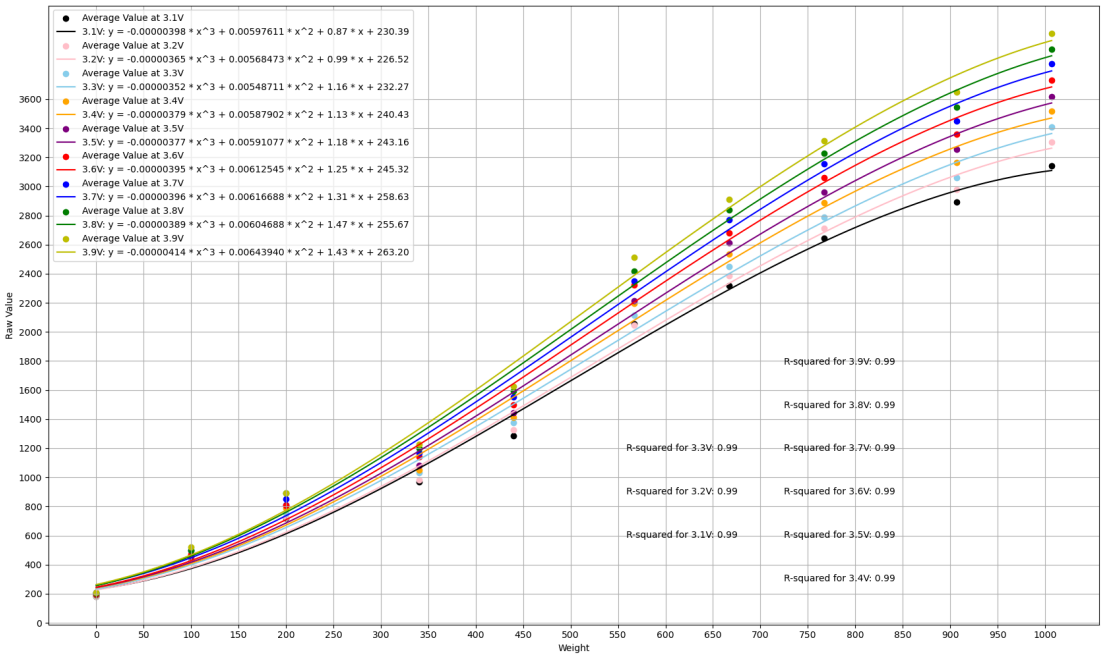
- Weights: 0g, 100g, 200g, 340g, 440g, 567g, 667g, 767g, 907g, 1007g
- Voltages: 3.1V, 3.2V, 3.3V, 3.4V, 3.5V, 3.6V, 3.7V, 3.8V, 3.9V
  This would give us a wide data set that we could use to analyze the effectiveness of the attack. We had the PartnerPlast board on top of the nRF9160dk and used a variable power supply to power the device. We measured many different points on the PartnerPlast board so we could understand what was happening with the voltage as it traveled from the Load Cell to the SAADC. The nRF9160dk sent messages to AWS containing the SAADC raw results that were saved into a DynamoDB database.

Results of the Attack

We started examining the effects of the attack by looking at the SAADC raw values in the AWS database. If we were able to see a change in this value then it was likely that the change would be reflected in the actual Icebox device. I used Python with the Matplotlib library to create a graph comparing the SAADC raw values at different weights. I plotted all of the raw values at different voltages and created lines of best fit so we could visualize the

effect that the attack had.





If there was no effect from the attack then we would expect there to be no difference in the raw values for different battery supply voltages. We clearly see that there was a difference and we calculated that there was around a 3% change in SAADC raw value for each 0.1V change of battery supply voltage at the same weight. Since

3.6V was our normal operating voltage, when we changed the Battery Voltage to 3.9V, we saw a 9% increase in the raw value. When we went down to 3.3V we say a 9% decrease in the raw SAADC value.

What are we Attacking?

Since we were able to see a repeatable change in the SAADC raw value when manipulating the battery supply voltage, it was likely that the attack was effective. We wanted to understand why could attack and what parts of the device were affected by manipulating the battery supply voltage. We wanted to prove that the change we created was not because of a random factor but caused by a defect in the design of the Icebox device. This is where the voltage measurements of the PartnerPlast board became useful. It allowed us to follow the voltage path of the device to see where the signal voltage changed.
We defined the path of the Load Cell signal as:

$$ExcitationVoltage \rightarrow Signal \rightarrow Amplified \rightarrow P0.14 \rightarrow ADC(Processing) \rightarrow Result(RawValue$$

We start with the Load Cell which creates a voltage signal from applied weight. That signal is then amplified by the INA122. The amplified signal is then transferred to the nRF9160dk using P0.14. That signal travels to the SAADC where it is converted from an electrical signal into a digital number which is out result that is sent out to AWS over MQTT.
We decided to follow this chain, isolating part each so that we could measure any effect that Battery Voltage had at each point in the chain.

1. Load Cell

Load Cell Effect Theory

To test this we powered the Load Cell using the power supply and measured the signal with a multimeter. We changed the weights so we could see what the effect was at different Excitation Voltages as well as weights. From our testing of the effect that Excitation Voltage had on the signal of the Load Cell was change of around 3% for each 0.1V variation in Excitation Voltage. This was consistent with the total effect that we saw in the SAADC raw values.

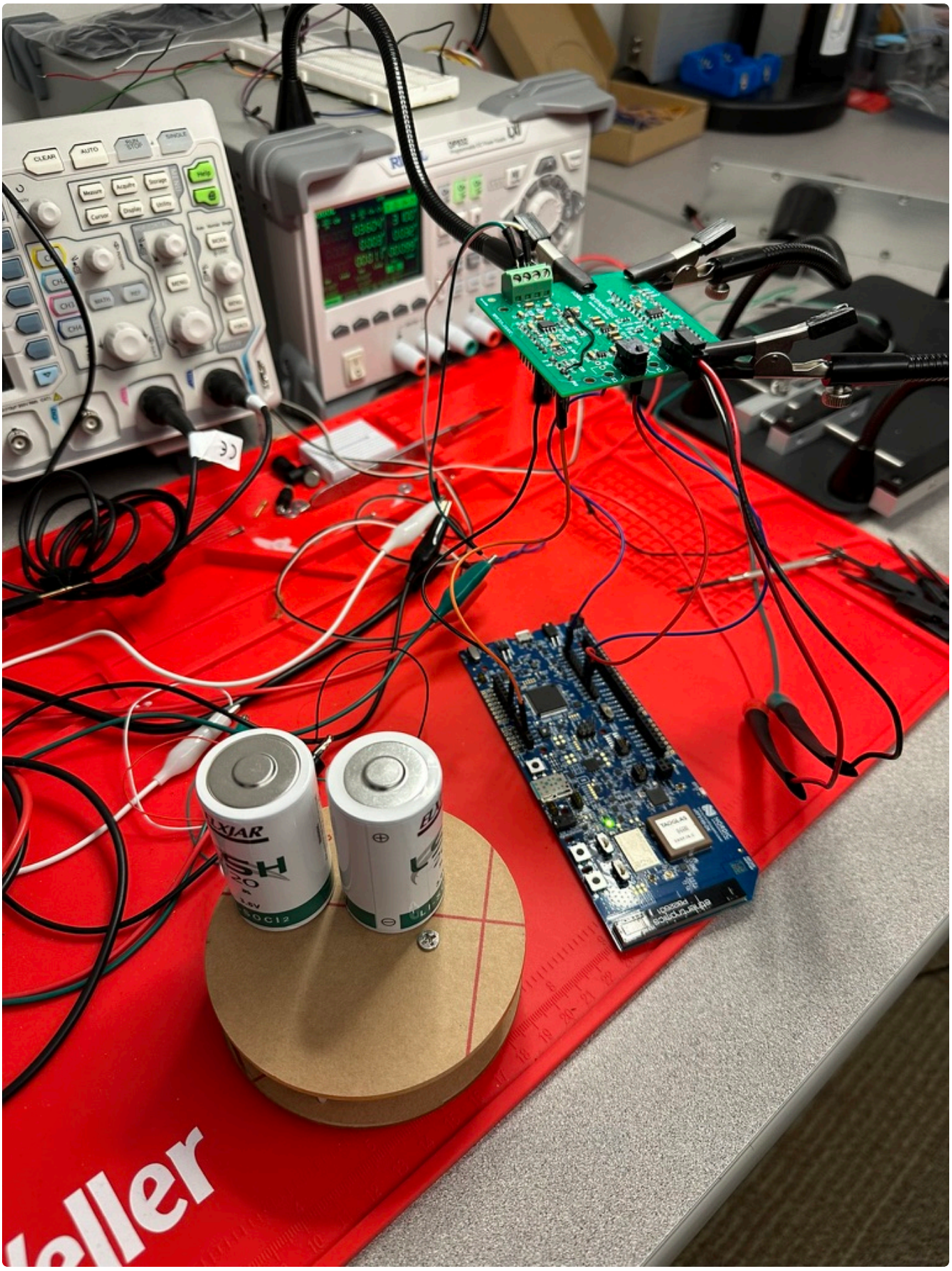
2. INA122

IC2 Deep Dive

IC2 Amplification Test

IC2 Amplification Test V2

The first test we ran on the INA122 gave us inconstant results that confused our understanding of the IC. It turned out that our test configuration caused these inconstancies. We connected the Amplification Board's signal terminal's to a power supply so that we could keep the signal constant while changing the Battery Voltage of the Amplification Board. This ended up causing issues for unknown reasons, but for the second test we changed the setup.



We used the Load Cell with a constant Excitation Voltage and weight to generate our constant signal. We then used the power supply to change the Battery Voltage. This gave us results with a constant

amplification which matched the documentation of the INA122. This meant that there was no effect of Battery Voltage on the INA122 amplification chip.

3. P0.14

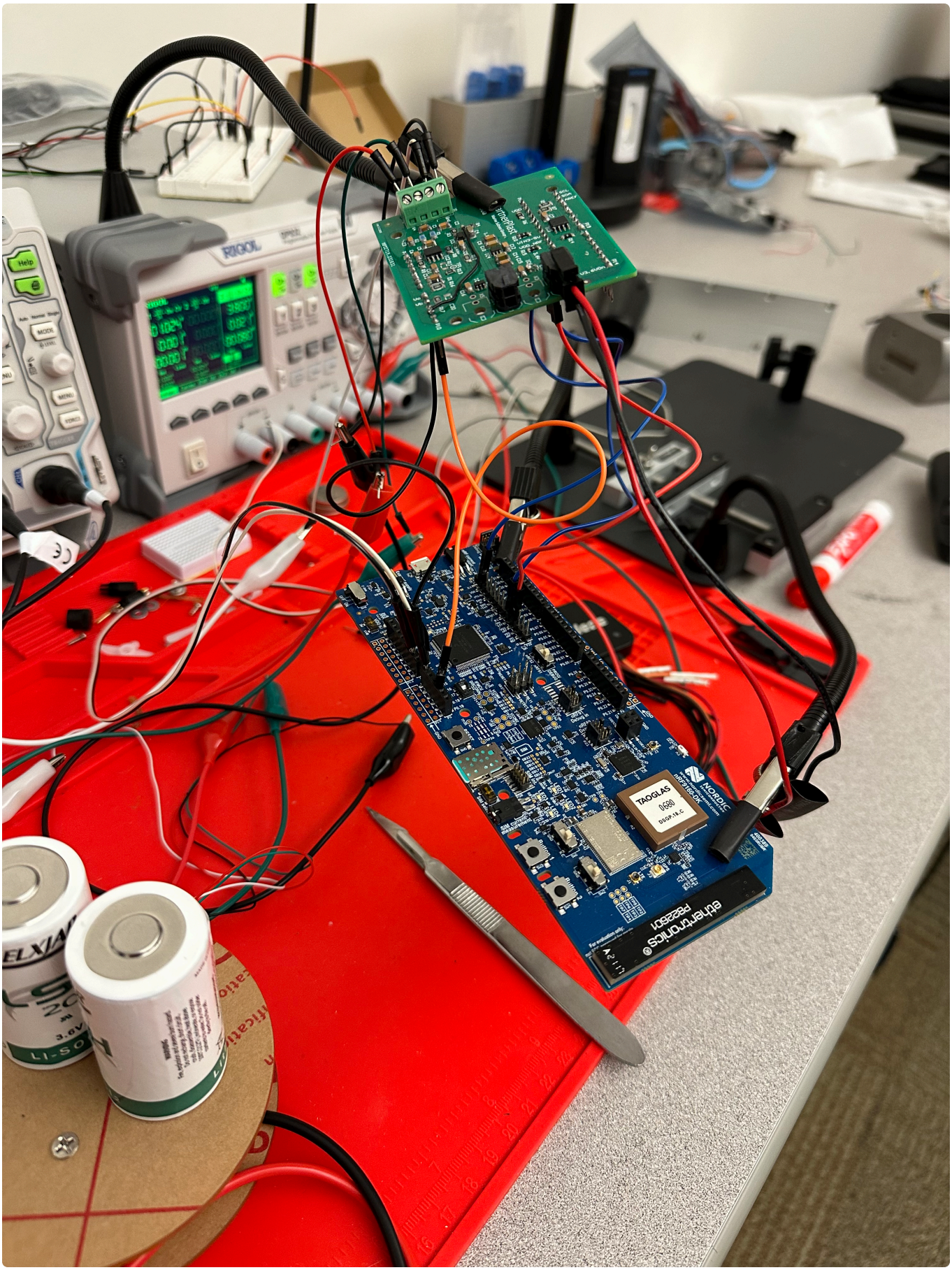
P0.14 to 9160 SiP Test

We wanted to test the path between P0.14 and the SAADC. To do this we measured the voltage at P0.14 and then again at P24 on the 9160 SiP. P24 is the connection point for P0.14 on the processing unit where the SAADC is located. This test showed that there was no difference of voltage at these two points.

4. SAADC

ADC 1V Test

For this test we wanted to focus on the effect that Battery Voltage would have on the readings from the SAADC. To accomplish this we separated the nRF9160dk from the Amplification Board so that the Battery Voltage was supplied from the Amplification Board but the Load Cell signal was not transferred. Instead we used a power supply to provide a constant 1V to P0.14 as out signal.



This way we could manipulate the operating voltage of the nRF9160dk while keeping the signal voltage for the SAADC constant. We collected the SAADC raw values from AWS and used an Single Factor

ANOVA test to prove that there was no statistical difference between the SAADC raw readings at different Battery Voltages. The ANOVA was required because the readings out of the SAADC jump around so an objective test comparing the readings was needed.

5. AWS

AWS Data Comparison

We finally wanted to confirm that AWS was not modifying the data that we sent it from the nRF9160dk. To do this we needed a second way to collect the SAADC raw readings. We used Serial Wire Debug (SWD) pins on the nRF9160dk to get access to the console output of the device. In this log the message that was being sent to AWS was printed. We collected all of these messages and then formatted them to match the AWS data. I used a custom algorithm to compare the two data tables, marking matches or missing data. From this we found that there was no modification of the data in AWS.

Conclusion of the Attack

From our analysis of our collected data along with the tests of each individual part of the electrical chain, we can say that our attack of manipulating the Battery Voltage had an effect on the SAADC raw result. This means that changing the operating Battery Voltage of the Icebox device would have a meaningful effect on the output of the device. For each 0.1V change in Battery Voltage we would be able to affect the perceived load on the device by 9%.