Cybersecurity of Onboard Charging Systems for Electric Vehicles

Saif Elsaady, Engineering (Electrical Systems)
Mentor: Ayan Mallik, Assistant Professor
Fulton School of Engineering

How Can We Limit Cybersecurity Attacks On Onboard Charging Systems For Electric Vehicles?

Motivation

To find a way to make the transition from gasoline to electric cars as easy as possible while overcoming any challenges.

Research Methods

1.) Hardware simulation (see Figure 1).
2.) Software simulation (see Figure 2).

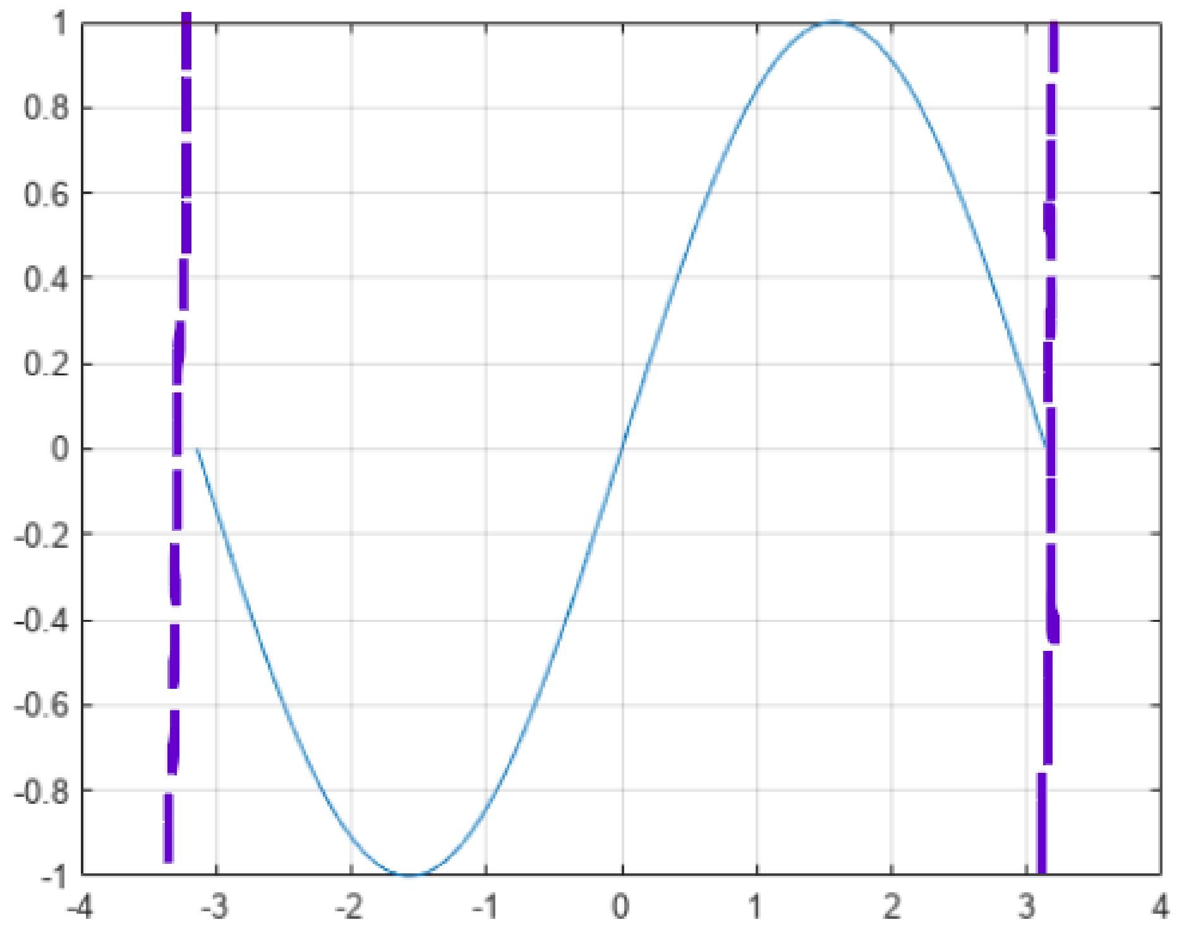


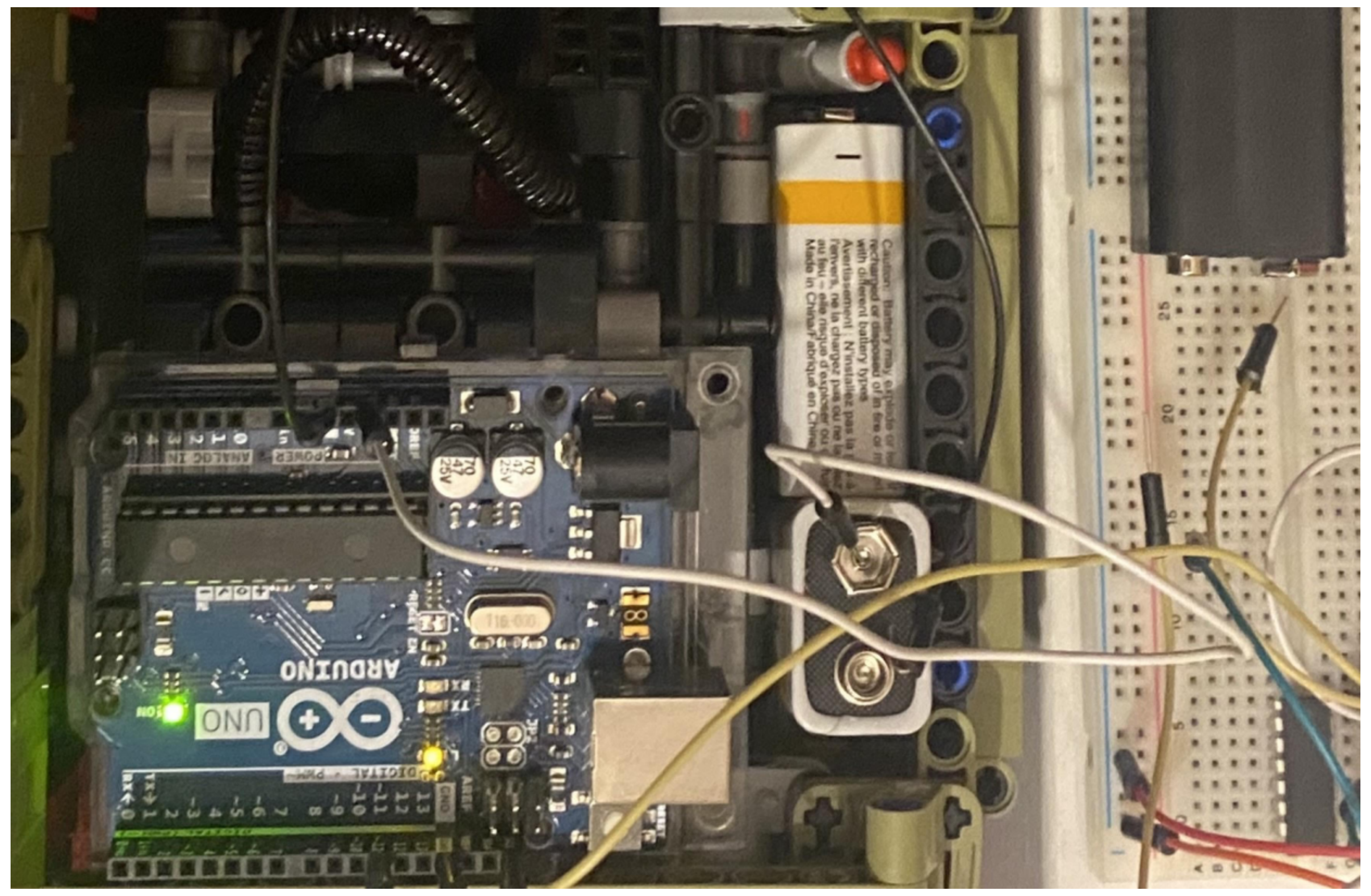
Figure 2. Charge simulation. Vertical asymptotes represents cyber attacks

Obstacles Faced

Obstacle	Overcoming Obstacle
Modeling the EV electronics on a simplistic scale.	The use of prototyping and simplistic hardware.
The modeling of the high levels of software within the EV.	The use of software such as Matlab and Arduino.
The timespan that was given to conduct the research.	The simplifying of the research whilst minimizing errors.

Acknowledgements

I wish to show my appreciation to my mentor and professor Ayan Mallik for his support, and the FURI program for selecting me to conduct this research.



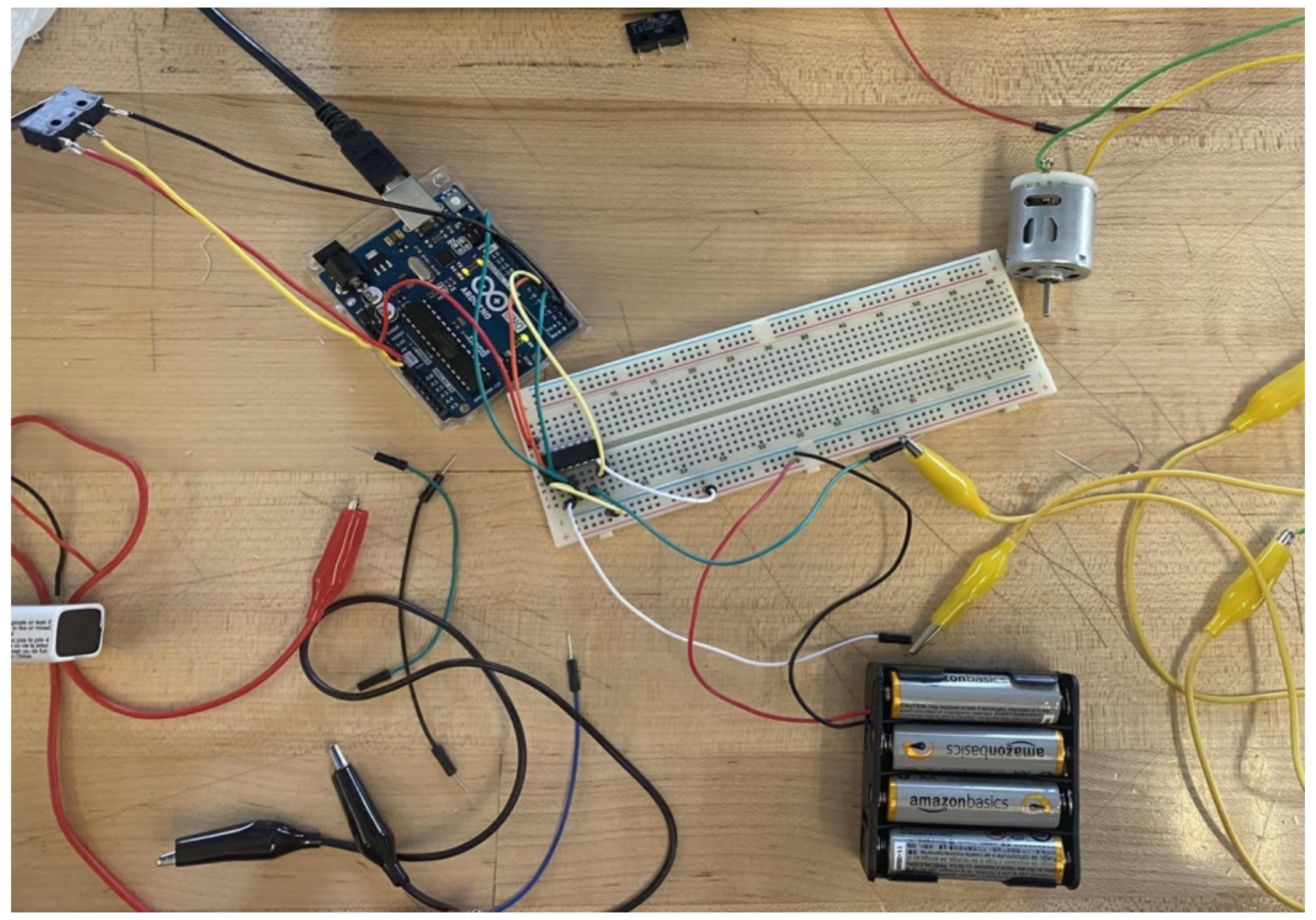
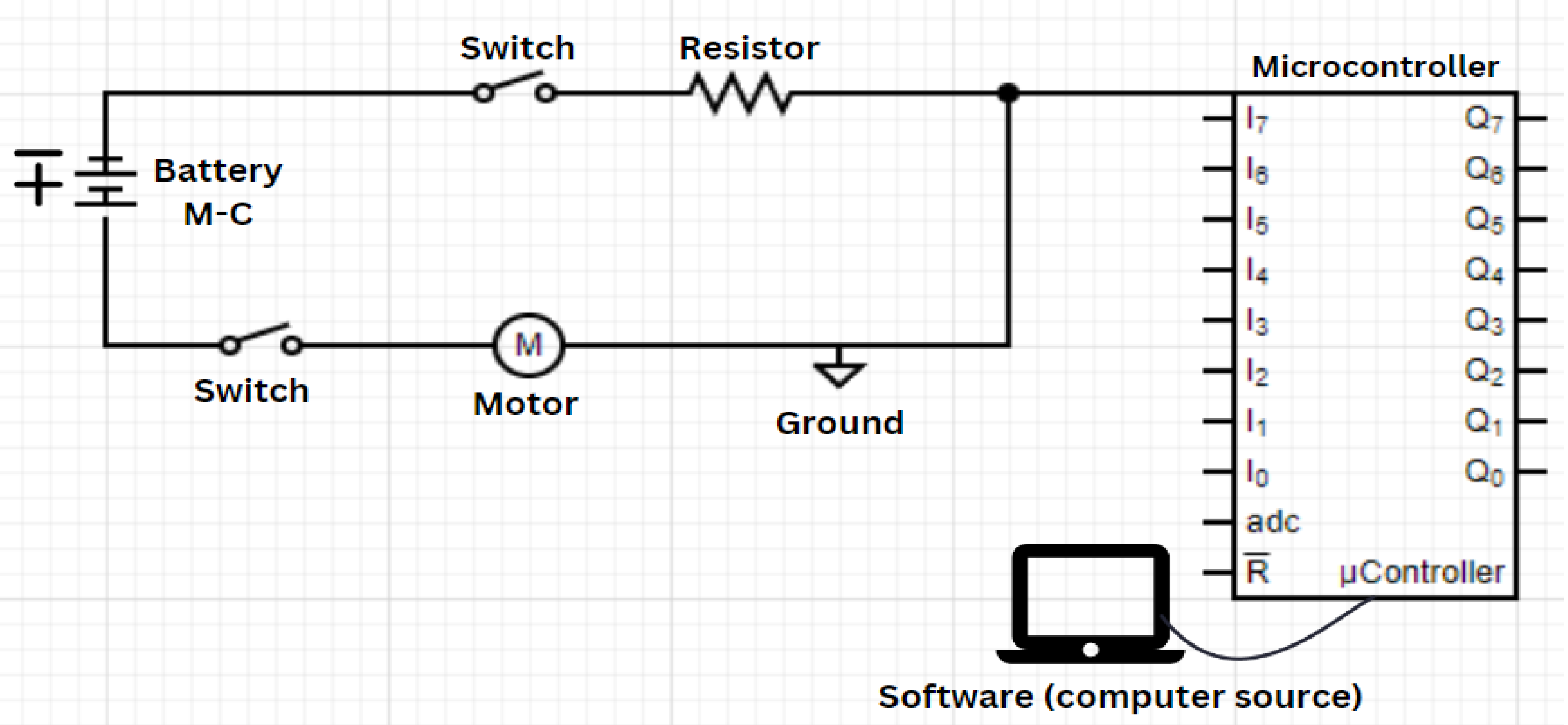


Figure 1. E.V charge attack hardware simulation



Conclusion

To conclude, I think that this research experience has confirmed some of the ongoing assumptions concerning cyberattacks on EVs. With the exception of malfunctions, an attacker needs access to the EVs hardware or the electric charger hardware in order to effectively conduct a cyberattack on an electric vehicle/charger. Otherwise, it is very difficult to conduct a cyberattack without gaining hardware access. Possible other approaches to conduct a cyberattack could involve some sort of electronic malfunction that could disrupt the hardware to make room for software attacks.

Hardware Simulation

Scenario	Interpretence
The attacker attempts to compute wireless attacks, the already existing software within the EV prevents this.	The attacker seems to need physical access of installing a piece of hardware within the car, thus making software attacks difficult without hardware access.
The attacker accesses the charging system and prepares for data transfers that concern charging station consumers. The attacker manages to obtain the information desired concerning consumer information.	The cybersecurity of charging systems can be severely damaged through hardware interaction, which then causes software damage depending on the course of action taken.

Findings & Progress (so far)

It appears that in order to address the research question we have to model attacks and sort of predict what they would be like before they happen. This is difficult at a simplistic scale with limited resources, but we were able to achieve that. Modeling using the attacks using software resources, we were able to simulate programming attacks through a model of input/output in MatLab & Arduino, as shown in *Figure 3.* Modeling attacks through the hardware side we simulated that with two different microcontrollers and power resources acting as the attacker, vehicle, and charging station, and this is shown in *Figure 1.* and under *Hardware*

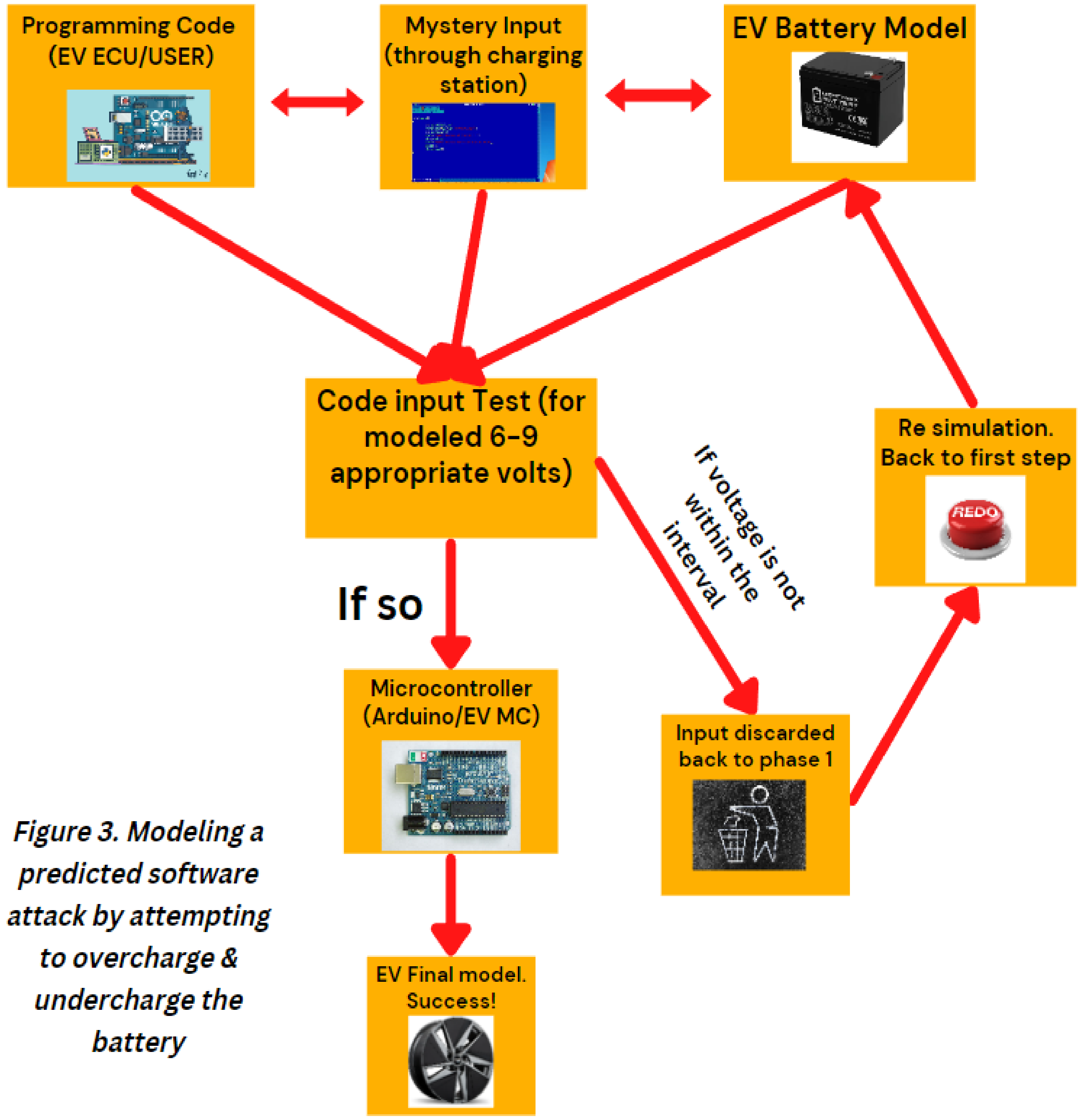

Programming Code (EV ECU/USER)
Mystery Input (through charging station)
EV Battery Model
Code input Test (for modeled 6-9 appropriate volts)
If so
If voltage is not within the interval
Re simulation. Back to first step
REDO
Microcontroller (Arduino/EV MC)
Input discarded back to phase 1
EV Final model. Success!

Figure 3. Modeling a predicted software attack by attempting to overcharge & undercharge the battery