THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
Department of Electrical and Computer Engineering

# Diamond Vault SCADA Demo


**Jeremy Boyd, Hannah Hanback, William Owen Sanders, Evan Stewart**


**CPE 496-01 Computer Engineering Design I**


**Electrical and Computer Engineering**
**The University of Alabama in Huntsville**

jsb0028@uah.edu

# Technological Vulnerability Awareness

*Cybersecurity* is the practice of defending computers, servers, mobile devices, and networks from malicious attacks.

- Common Cyber Threats
  - Identity Theft
  - Ransomware Attacks
  - Phishing Emails

- Need for Awareness
  - 95% of cybersecurity breaches are due to human error[1]
  - It is estimated that 70% of employees do not understand cybersecurity best practices[2]
  - $12.5 billion in lost from phishing emails alone in 2019[1]

Sources
1 (https://www.cybintsolutions.com/cyber-security-facts-stats/)
2 (https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/ )

# Who is Affected

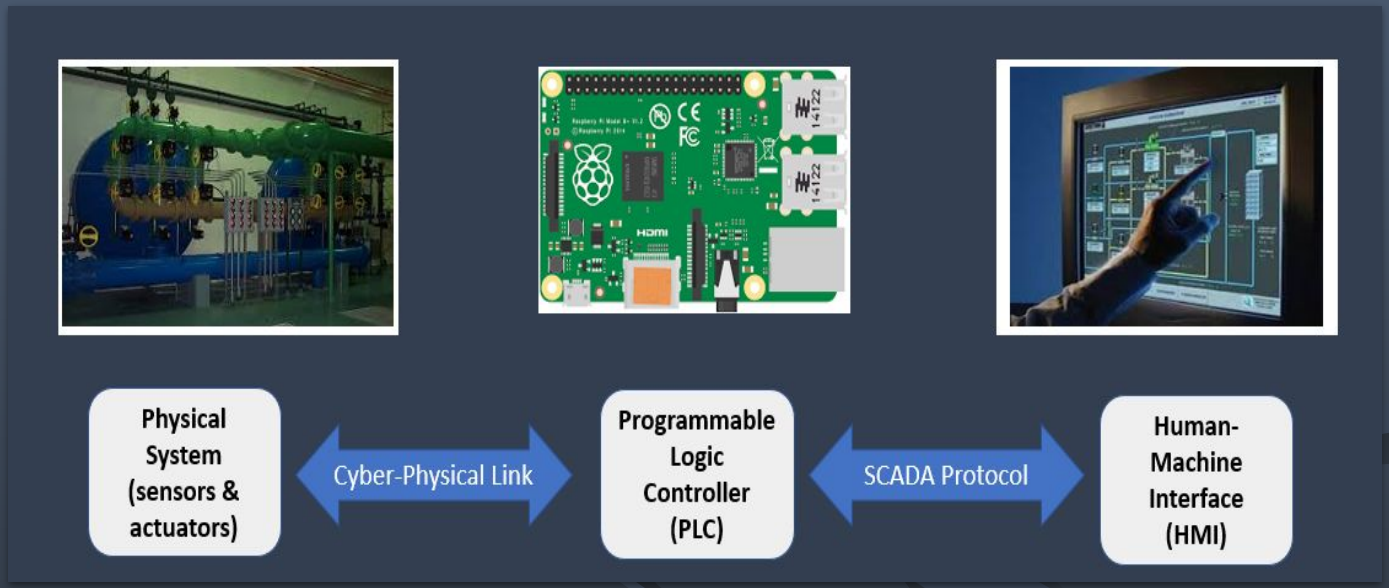
The top industries targeted for cyber attack include:

- Business especially small businesses
- Healthcare/Medical
- Banking/Credit/Financial
- Government/Military
- Education
- Energy/Utilities

# SCADA

SCADA:

- Supervisory
- Control
- And
- Data
- Acquisition




A SCADA system connects a Programmable Logic Controller (PLC), physical sensors, and a Human Machine Interface (HMI) to manage industrial systems.

# Marketing Requirements

- Portable
- Easy and Quick Setup
- Uses OpenPLC Software and Modbus communication protocol
- Able to View Machine State
- Implements 2 togglable cyber attacks and defenses
- Looks professional

# Engineering Requirements p1

| Marketing Requirements | Engineering Requirements | Justification |
|---|---|---|
| Portability | The dimensions should not exceed 27”x21”x14”. | Airline Restriction: Complies with average dimension size limit of 62”. |
| Easy and Quick Setup | There should be no more than 5 minutes of setup time. | Our sponsor would like the project to work out of the box. |
| Portability Easy and Quick Setup | The design does not include water. | Including water in the design causes a risk of damage to the electrical components. |
| Looks professional | No visible wires. All essential parts are recognizable from a distance of 30’. | The project interior should be easily seen across a classroom. |

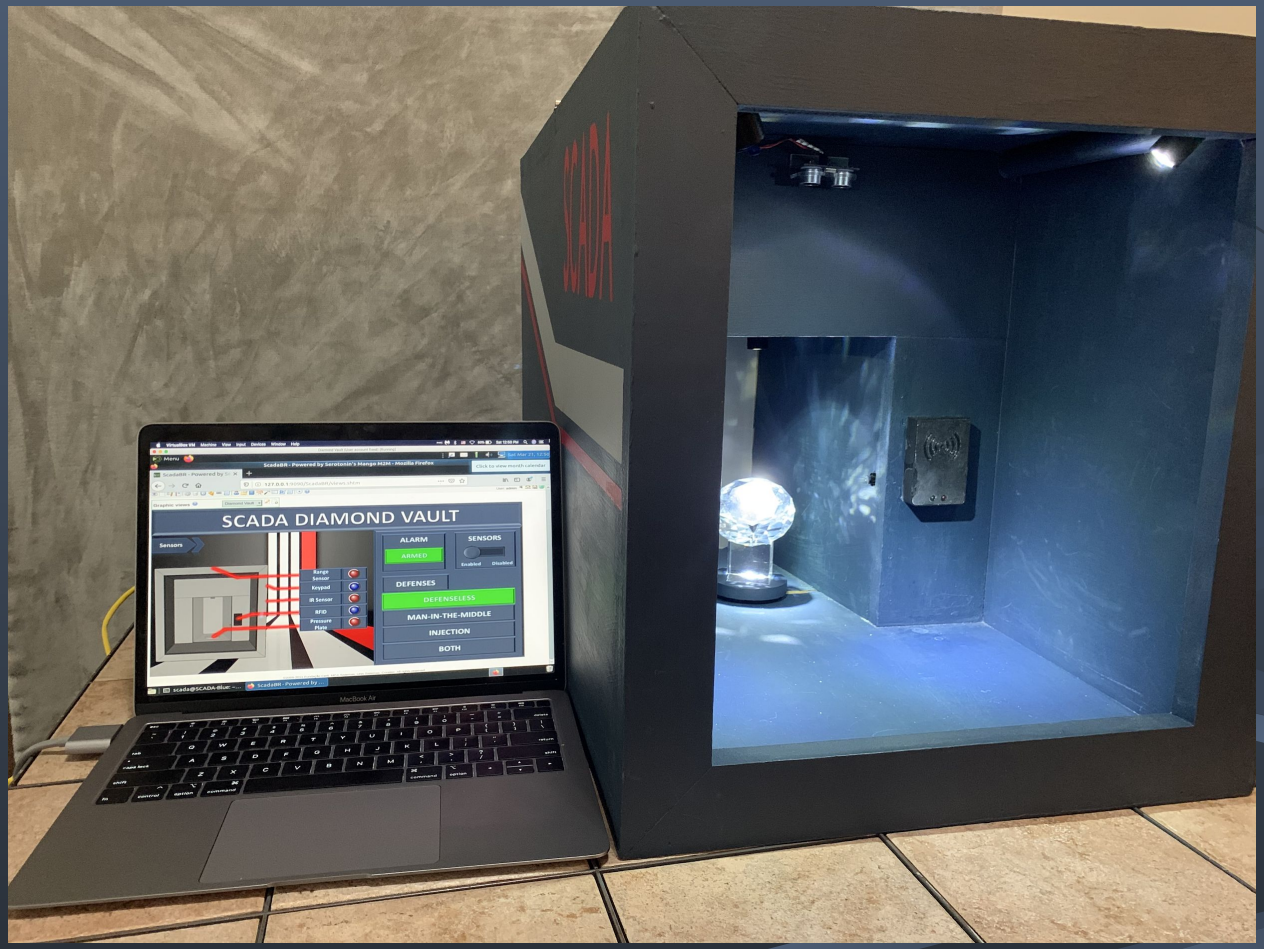
# Engineering Requirements p2

| Marketing Requirements | Engineering Requirements | Justification |
|---|---|---|
| Portability | Able to withstand a drop within the flight case without breaking the project. | The handling at the airport may be rough. |
| Able to View Machine State, Looks Professional, OpenPLC | Includes an intuitive Human Machine Interface connected to the OpenPLC software. | Anyone should be able to interpret the state of the system easily. |
| Implement Attack/Defense, OpenPLC | Have at least one cyber defense per attack. | The implemented attacks need to have defenses that counteract them. |
| Easy to Set Up, Implements Attack/Defense, Open PLC | Must be able to reset to normal (defenseless) state | The project should be able to be put back into startup state whenever needed |

# Design Ideas

- Tesla coil
  - Difficult to transport
  - Risk of electric shock
- Oil Rig Model
  - Potentially illegal to transport
  - Danger of open flame
- Diamond Vault
  - Low risk
  - Easy to transport

# SCADA Demonstration



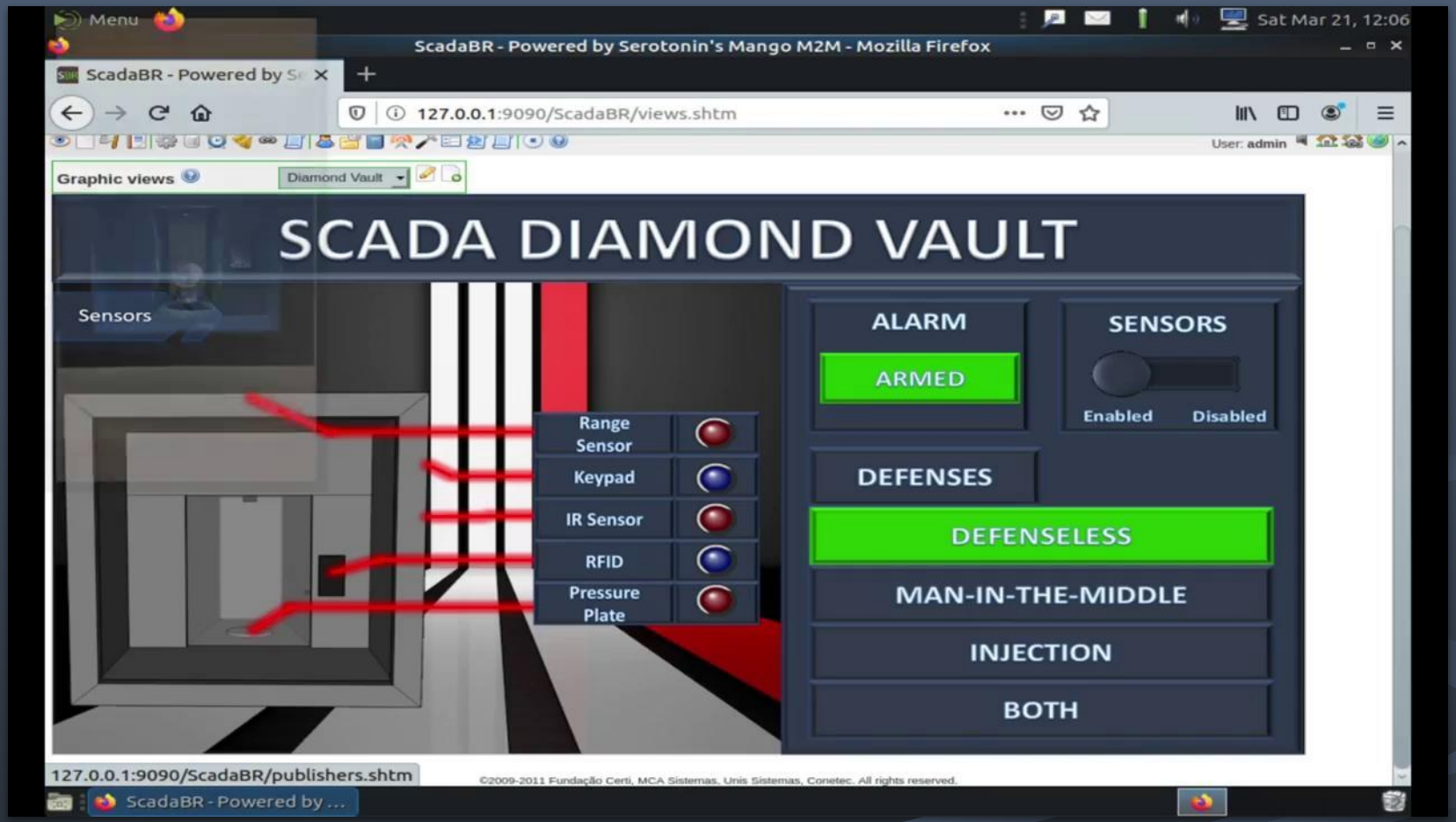
# Project Description

- A SCADA diamond vault used for cyber demos
- Built-in sensors give our project the look and feel of an actual system.
- Uses The OpenPLC Project to turn a RPi into a PLC
- Includes an HMI that shows the status of the vault.
- 2 Attacks created to show vulnerabilities
  - Each attack comes with a defense

# Attacks and Defenses

- Attacks:
  - Modification
    - Man-in-the-Middle attack using ARP poisoning
    - Modifies packets from PLC to HMI
  - Injection
    - Sends a fabricated Modbus packet to the PLC
- Defenses:
  - Modification
    - Sets static entries in the ARP tables
  - Injection
    - Uses IP table rules to restrict outside communication

# Video




Song: Oaklawn Dreams by Wistia

Powerplant image: https://en.wikipedia.org/wiki/File:Bruce_Mansfield_Power_Plant.jpg

# Testing

- Unit Tests
  - Tested each hardware module individually
    - IR sensor
    - Motion Sensor
    - Pressure Plate
    - RFID
    - Keypad
  - Tested OpenPLC Software with a simulation

# Testing

- Integration Tests
  - Plugged all modules into the Pi running OpenPLC
  - Made sure the alarm triggers under normal conditions
  - Tested HMI with the OpenPLC software
  - Tested each attack and defense on the system
- Acceptance Tests
  - Verify that we met all requirements set
    - Portability
    - Easy setup
    - 2 attacks and defenses
  - Have someone who has no involvement test the operation

# Major Issues

- Solenoid
  - Transient voltages
  - Proposed a Zener diode solution
- Denial of Service Attack
  - Insufficient packet flooding
- Many hardware design issues resulted in device failures
  - Unprotected circuits damaged

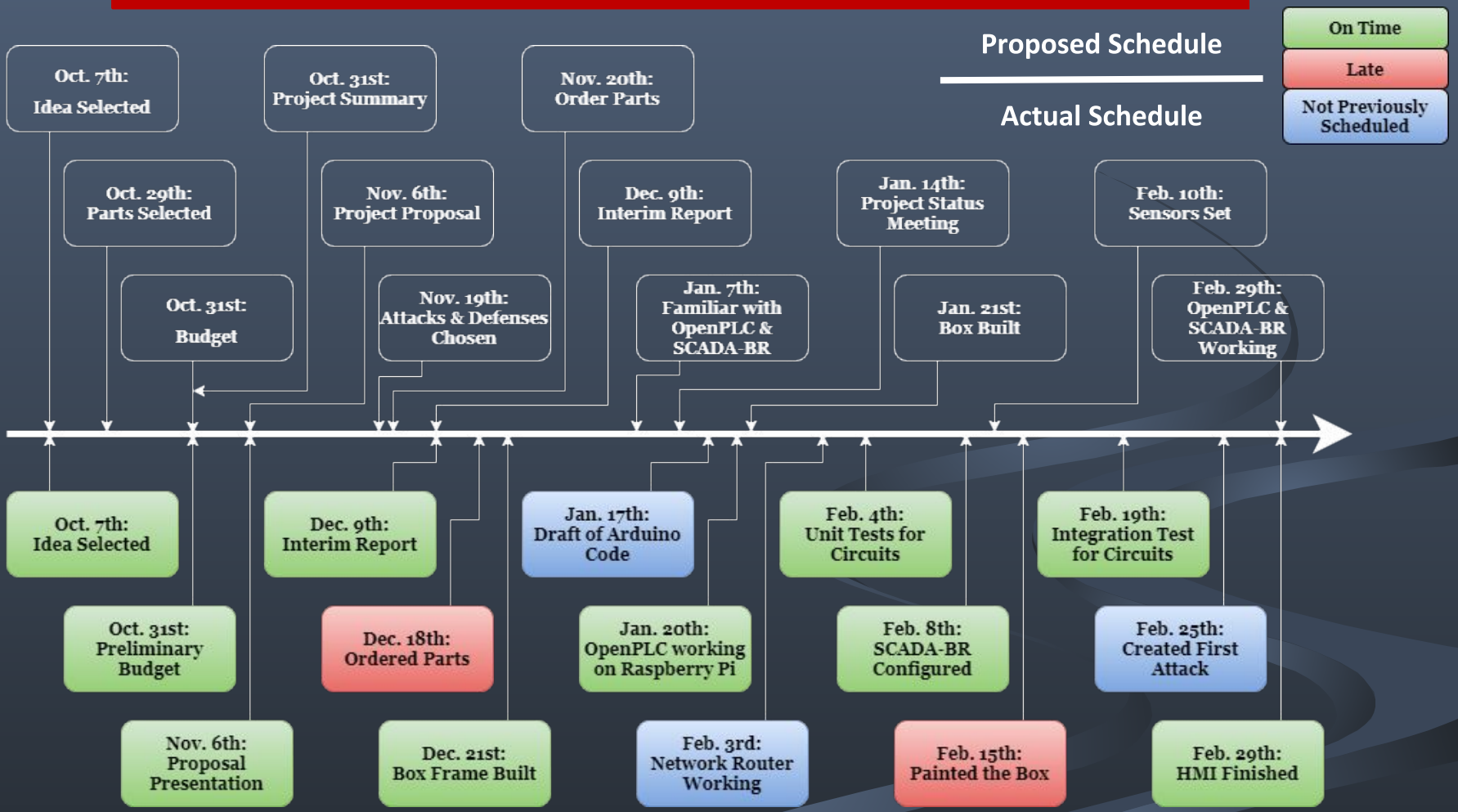
# COVID-19

- **Not much affect on our project**
  - Finished the required physical components
  - Ahead/on Schedule
  - Some Non-Essential items discarded
    - Solenoid/Door

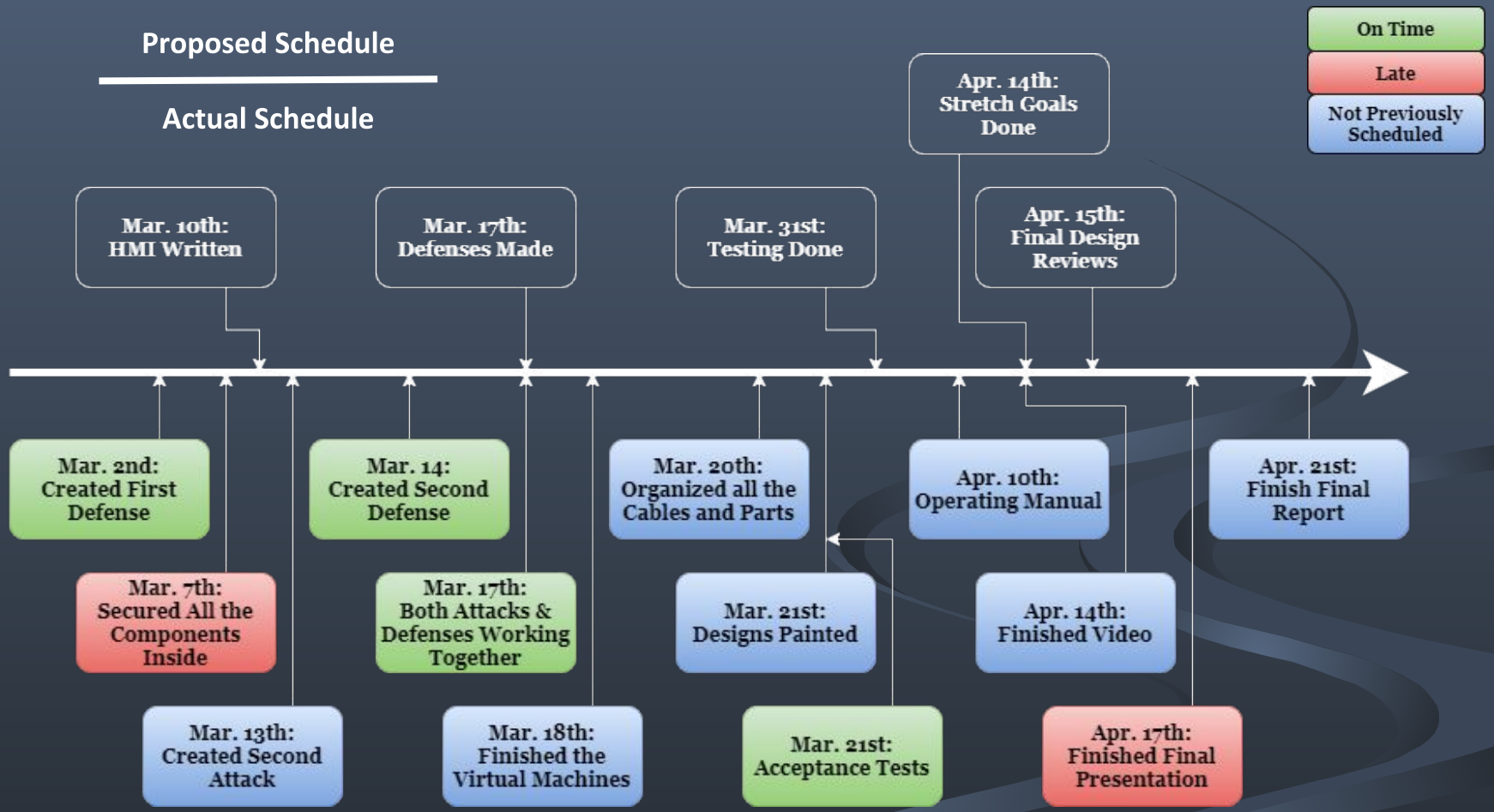
# Modifications

- **Size of the Vault**
  - Changed dimensions to accommodate hardware
- **Did not Include Door**
  - Solenoid locking issues
  - Time issues with Covid-19
- **Used Injection Attack Instead of Denial of Service**
  - DOS attack was unsuccessful in practice
- **Used Wired instead of Wireless Connection**
  - Privacy and security concerns
  - Doesn't need to rely on access to Wifi

# The Project Timeline



# The Project Timeline Cont.



# Cost

| Category | Parts | Price Per Part | Purchased | Price | Module Total |
|---|---|---|---|---|---|
| Laser | Receiver | $1.10 | 10 | $11.00 | $16.77 |
| | Emitter | $0.32 | 10 | $3.20 | |
| | 555 Timer | $0.00 | 0 | $0.00 | |
| | Rubber Washers | $2.57 | 1 | $2.57 | |
| RFID | Reader & Cards | $6.99 | 1 | $6.99 | $6.99 |
| | Arduino | $0.00 | 0 | $0.00 | |
| Pressure Plate | Force Sensitive Resistor | $11.18 | 1 | $11.18 | $11.18 |
| Alarm | Red LED Strip | $7.99 | 1 | $7.99 | $34.88 |
| | 12V Power Supply | $13.99 | 1 | $13.99 | |
| | Alarm Passive | $1.50 | 2 | $3.00 | |
| | Transistor | $0.60 | 5 | $3.00 | |
| | Heat Sink | $3.50 | 1 | $3.50 | |
| | Alarm Active | $1.70 | 2 | $3.40 | |
| Lock Motor | Solenoid | $7.50 | 1 | $7.50 | $16.49 |
| | Power Supply (6v 2A) | $8.99 | 1 | $8.99 | |
| Motion Sensor | Ultrasonic Sensor | $9.59 | 1 | $9.59 | $9.59 |
| KeyPad | Keypad | $5.95 | 1 | $5.95 | $5.95 |
| | Arduino | $0.00 | 0 | $0.00 | |
| Open PLC Controller | Rpi & Heatsinks | $52.99 | 1 | $52.99 | $65.77 |
| | MicroSD Card | $5.79 | 1 | $5.79 | |
| | USB Power Cable | $6.99 | 1 | $6.99 | |

# Cost Cont.

| | | | | | |
|---|---|---|---|---|---|
| Power | Power Strip | $14.96 | 1 | $14.96 | $14.96 |
| Display Light | Two LED Spotlights | $15.99 | 1 | $15.99 | $28.98 |
| | Two More LEDs | $12.99 | 1 | $12.99 | |
| Network | Ethernet Switch | $0.00 | 0 | $0.00 | $0.00 |
| | Ethernet Ports | $0.00 | 0 | $0.00 | |
| | Ethernet Cords | $0.00 | 0 | $0.00 | |
| Box | Plexiglass | $4.98 | 1 | $4.98 | $100.19 |
| | Plexiglass (Door) | $6.68 | 1 | $6.68 | |
| | Piano Hinge | $7.98 | 1 | $7.98 | |
| | MDF | $31.95 | 1 | $31.95 | |
| | Screws | $9.20 | 1 | $9.20 | |
| | PVC Pipe | $1.98 | 1 | $1.98 | |
| | Dark Blue Paint | $3.98 | 2 | $7.96 | |
| | Latch | $0.98 | 1 | $0.98 | |
| | Knob | $1.08 | 1 | $1.08 | |
| | Bolt | $2.98 | 1 | $2.98 | |
| | Gray Paint | $3.98 | 1 | $3.98 | |
| | Red Paint | $3.98 | 1 | $3.98 | |
| | Polyurethane | $7.98 | 1 | $7.98 | |
| | Vinyl | $4.49 | 1 | $4.49 | |
| | Transfer Paper | $3.99 | 1 | $3.99 | |
| Shipping | | $13.17 | 1 | $13.17 | $13.17 |
| Tax | | $24.98 | 1 | $24.98 | $24.98 |
| | | | | **Total Price:** | **$349.90** |

# Labor Hours

| Category | Proposed Estimate | Actual Hours |
|---|---|---|
| Research Parts | 20 | 20 |
| Research Attacks | 10 | 30 |
| Approaches / 3D Model | 5 | 15 |
| Assembling Box | 20 | 55 |
| Making & Testing Sensors With Arduino/RPi | 38 | 100 |
| Securing Sensors & Components in Box | 10 | 30 |
| SCADA Research & Working | 30 | 40 |
| HMI Design & Writing | 20 | 50 |
| OpenPLC Research & Working | 20 | 40 |
| Writing Defenses | 30 | 20 |
| Testing | 30 | 50 |
| Documenting Attacks and Defenses | 30 | 30 |
| Reporting | 30 | 50 |
| | Total Hours: 293 | Total Hours: 530 |

# Deliverables

- The Diamond Vault
- Operating Manual
  - Detailed User Operation
  - Description of Attacks/Defenses
  - Parts and Pieces
- Final Report
- Video

# Modularity

- Built in a way to easily change:
  - Sensors
  - Code
  - Attacks
  - Defenses
- Allows changes to demonstrate current cybersecurity threats

# Social Impact Analysis

- Security
  - Purely Ethernet access
- Privacy
  - Self-contained demonstration
- Health & Safety
  - IR lasers
- Legal
  - Possession of hacking tools
- Ethical
  - Hacking demonstrations

# Lessons Learned

- Communication is Key
- Life Doesn't Always Cooperate
  - Plan ahead for setbacks
- Hardware development can lag behind software
  - No IDE or error checking
  - Common Ground = Happy Circuits
  - Beware of Solenoids!

# Questions?