GridSAFE: Cyber Simulation of Grid Attacks with AI Anomaly Detection

DESIGN DOCUMENT

sdmay26-08

Client: Nellie Leaverton

Advisors: Julie Rursch

Nellie Leaverton – Hardware & Architectural Design Lead

Jason Di Giovanni – Software and Security Lead

Brant Gicante – Software and Security Assistant

Evan Booze – Hardware & Architectural Design Assistant

Kyle Maloney – Testing Lead & Design Assistant

Anthony Nehring – Software and Security Assistant

TEAM WEBSITE: https://sdmay26-08.sd.ece.iastate.edu/

Executive Summary

Critical infrastructure systems such as electrical grids are increasingly targeted by cyberattacks, yet many students and educators lack accessible tools to visualize how these attacks develop and how they affect physical systems. The GridSAFE project addresses this problem by creating an interactive educational platform that connects simulated network activity to a 3D model of a city. This allows users to see, in real time, how benign and malicious digital events influence critical infrastructure and surrounding areas. The importance of this work lies in its ability to strengthen cybersecurity awareness, improve applied learning, and prepare future professionals for real world cyber defense scenarios, particularly within industrial control system and operational technology contexts.

Our key design requirements include the creation of an educationally focused model that is affordable, safe, and visually intuitive. Hardware requirements specify a stable 3D city layout, secure wiring, reliable LED behavior, and materials that support repeated classroom use. Software requirements include early experimentation with log data, development of a prototype anomaly detection model, and establishing the basic structure that will later allow software output to influence the physical system. Both sides of the design emphasize modularity so that each piece of the system can be improved over time.

Progress this semester has centered on building a functional foundation for both hardware and software. The hardware team produced multiple 3D printed building prototypes, as well as a prototype baseboard to test LED integration. RGB LEDs were tested successfully, controlled through Raspberry PI scripts that change color on command. These accomplishments verify that the hardware can support the visualization goals of the project.

On the software side, the team began with sample HDFS log data and used it to create an initial prototype of an anomaly detection model. While still in early stages, this model demonstrates the feasibility of processing log data and generating output that can later be connected to the physical display. Basic components of the software pipeline have also been outlined or completed, ensuring that future integration work will have a clear structure to follow.

Next steps include completing the communication pathway between the AI model and the Raspberry PI, refining the machine learning model, building a virtual network to generate logs, and continuing to scale the physical city model. Additional emphasis will be placed on accuracy, usability, and preparing the system for future educational demonstrations.

Learning Summary

Development Standards & Practices Used

Circuit & Hardware Practices

- Following component datasheet safety limits (voltage/current ratings).
- Secure wire routing using cable management, zip ties, and insulated connectors.
- Color-coding wiring for consistent debugging and maintenance.
- Easy accessibility to wiring for future maintenance

Software Practices

- Modular program design for future updates and testing efficiency.
- Documentation of software behavior so future users and maintainers can understand indented use.
- Use of configuration files such as JSON to store paths, thresholds, and model settings so behavior can be changed without editing source code.
- Consistent coding style for Python, including clear naming, indentation, and function level documentation to keep the code readable for future teams.

Summary of Requirements

Hardware Requirements

- LEDs update within 1–2 seconds
- LEDs default to blue on reboot or communication loss.
- City model size: approximately 3 ft × 3 ft.
- All wiring are securely enclosed for safety and durability.
- 3D city Model constructed from non-conductive materials (PLA, acrylic, wood, foam).

Software Requirements

- Configurable and modular design
- Cover at least 10 attacks from the MITRE ATT&CK Framework
- 80-90% accuracy for anomaly detection
- 100% accuracy for AI checker program to Raspberry PI signal
- 100% accuracy for Raspberry PI to LED signal

Applicable Courses from Iowa State University Curriculum

EE 230

EE 231

CybE 230

CybE 231

Cybe 331

Cybe 430

New Skills/Knowledge acquired that was not taught in courses

- 3D printing
- Laser cutting
- Wood Working
- AI/ML Training
- Using JSON config files

Table of Contents

List of figures/tables/symbols/definitions (This should be the similar to the project plan)

Intrusion Detection System (IDS) - A security tool that monitors network or system activity for malicious behavior or policy violations, alerting administrators when potential threats or unauthorized access are detected.

1. Introduction

1.1. Problem Statement

The broader context of this project operates within the educational domain and critical infrastructure protection. There is a growing need for awareness and knowledge about how cyber intrusions on power systems have real-world consequences. Our project can raise awareness and promote research into this topic by providing an interactive platform. Stakeholders interested in this research include cybersecurity educators and students, utility operators and infrastructure security professionals, policy makers, and stakeholders in national security critical infrastructure, public, and community stakeholders. Cyberattacks on infrastructure are at the forefront of national security, and many nations across the globe seek low-cost solutions to simulate and train for grid-related cyber incidents. Large-scale attacks on critical infrastructure have cascading effects on the population and the economy. By developing an intuitive and user-friendly simulation, we can illustrate how both regular and malicious activity impact critical infrastructure in a way that is easy for anyone to understand.

1.2. Intended Users

The intended users are students, professors, and industry professionals who need a tool to visualize and understand attacks on critical infrastructure. This tool is a teaching aid for those groups to represent real-time attacks on critical infrastructure visually.

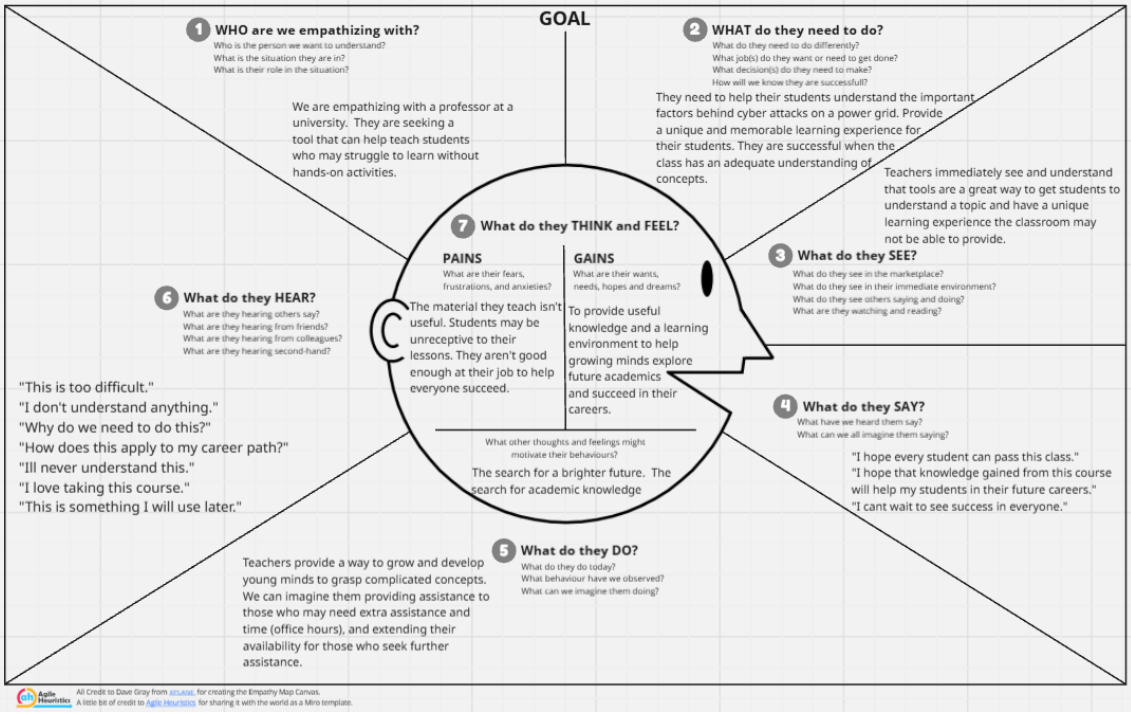
Professors are educators and experts on specific subject matter, and create, implement, and deliver assignments and lessons to guide students' learning. Professors need to engage students with interactive resources and illustrate complex concepts in a way students can understand. Professors can use this tool to visually represent cyberattacks that support lessons and projects on protecting critical infrastructure.

Students seek to understand new ideas, complex problems, and engage in school activities. One way is through visualization and hands-on experience, which bridges the gap between theory and practical applications. Students value interactive and intuitive tools to aid their learning process. This tool provides them with an interactive and intuitive way to aid their learning process.

Industry Professionals practice and apply specialized knowledge in a practical setting. They value practical and efficient tools to streamline processes or provide clear insights into their problems. Industry Professionals can use this tool to simulate cyberattacks on critical infrastructure to analyze potential impacts, essential vulnerabilities of their own system, and gain insight into their own infrastructure.

Empathy Map Canvas

Designed for: Teachers | Designed by: Student | Date: 9-30-25 | Version: 1



2. Requirements, Constraints, And Standards

2.1. Requirements & Constraints

Functional Requirements

- The microcontroller will receive real-time data from the IDS.,
- The microcontroller will parse input data from the IDS and control the corresponding LEDs based on the data.,
- The LEDs will respond dynamically to updates from the IDS within a reasonable time (1–2 seconds).,
- The microcontroller will support a fail-safe mode that defaults all LEDs to blue upon system reboot or loss of communication with the IDS.,
- The microcontroller will allow for a manual reset or override for demonstration and testing purposes.

Physical Requirements

- The city model shall be compact (approx. 3 ft x 3 ft).,
- All wiring and microcontrollers shall be securely enclosed or mounted to prevent short circuits or physical damage.,
- The physical model shall use non-conductive materials such as PLA (3D printed), acrylic, wood, or foam for safety.

Resource Requirements

- Hardware shall utilize components available through the ISU ECpE labs or purchased within the standard senior design hardware budget (~$100–$500).

Aesthetic & User Experience Requirements

- The city model will be visually appealing and intuitive for viewers to understand the relationship between LEDs and IDS.,
- The 3D city model will visually represent a city and simulate what attacks on an electrical grid may look like.

Software Requirements

- The IDS software shall collect, parse, and analyze system logs from all grid components to detect anomalies or attacks.
- Detection shall combine rule-based logic with machine learning for improved accuracy over time.
- The software shall communicate LED status updates to the microcontroller through a defined interface protocol.
- A web-based dashboard shall visualize alerts, system health, and current LED states.
- All configurations (thresholds, model parameters, and file paths) shall be editable without modifying source code.
- The system shall maintain structured logs for system activity, detections, and communication events.

- The software shall include a safe-state condition that triggers if communication or detection fails.
- Source code shall be modular and documented for maintainability and future expansion.

2.2. Engineering Standards

The importance of engineering standards is that they help to ensure consistency, safety, and maintain a common approach towards design. They work like generalized rules towards specific problems and concerns that may occur in development. They provide a shared technical foundation that allows engineers to design systems that communicate and function reliably together. They protect public safety and ensure products meet ethical and environmental expectations. Overall, they are set rulesets made in place for development and frameworks to help work towards success in a project in a way that accounts for potential concerns that could arise without the structuring of these standards.

IEEE 1012-2016 — System and Software Verification and Validation
This standard defines a structured approach for verifying and validating software systems to ensure they meet their intended purpose and user requirements. It outlines procedures for testing, documentation, and traceability throughout the development cycle. For GridSAFE, it helps ensure our IDS software functions reliably, accurately detects anomalies, and meets project specifications.

ISO 9001:2015 — Quality Management Systems
This standard focuses on consistent quality across all development and production processes. It promotes clear documentation, defined workflows, and feedback-driven improvement. Applying it to GridSAFE ensures repeatable testing procedures, organized version control, and reliable system performance during demonstrations.

ISO 14001:2015 — Environmental Management Systems
This standard provides guidelines for minimizing environmental impact during design and development. It emphasizes sustainability, material efficiency, and waste reduction. For GridSAFE, it encourages the use of non-conductive, recyclable materials (like PLA and wood) and promotes efficient use of resources during model construction.

ISO 50001:2018 — Energy Management Systems
This standard establishes best practices for monitoring and improving energy efficiency. It supports designing systems that optimize power usage and reduce energy waste. In GridSAFE, it aligns with simulating realistic grid operations while maintaining efficient power consumption for LEDs and microcontrollers.

ISO/IEC 27001:2022 — Information Security Management Systems (ISMS)
This standard outlines how to protect data confidentiality, integrity, and availability. It includes policies for access control, risk management, and secure data handling. Applying it to GridSAFE ensures that simulated grid logs, IDS configurations, and communication between systems remain secure and protected from unauthorized modification or access.

IEEE 1012-2016 is directly relevant because our project includes a complex software pipeline for intrusion detection. Following this standard helps ensure the IDS software is verified and validated against requirements, minimizing false alerts and logic errors.

ISO/IEC 27001 applies to how we handle simulated grid data and potential attack scenarios. Even though the data is not real-world critical infrastructure data, adopting its principles (like secure storage and access control) reinforces cybersecurity best practices.

ISO 9001 supports documentation, testing, and consistency across hardware and software components, ensuring the system remains reliable during demonstrations.

ISO 14001 and **ISO 50001** have limited but conceptual relevance; our physical model consumes little energy, but the project represents an energy infrastructure system, so these standards encourage awareness of efficiency and sustainability in design choices.

We reviewed our selected standards as a team and noticed some differences in focus. While a few of us concentrated more on the physical components and applications of the project, others focused on the software and digital aspects. Several of the standards we discussed were already familiar to the CybE engineers from previous upper-level coursework. Additionally, we realized that considerations like the choice of PLA and other printing materials weren't something everyone initially thought about until we identified the relevant standards.

Q5) What modifications do you intend to make to your project design to incorporate these standards?

To align with these standards, our team will:

- Implement a **structured verification and validation plan** following IEEE 1012 to document test cases, outcomes, and revisions.
- Apply **secure configuration management** consistent with ISO/IEC 27001 by limiting file access, using hashed credentials, and validating data integrity.
- Maintain **versioned documentation and configuration files** to reflect ISO 9001 practices of continuous improvement.
- Consider **energy-efficient operation** of LEDs and microcontrollers to reflect ISO 50001 awareness.
- Incorporate sustainability considerations into material selection for the city model, loosely aligning with ISO 14001.

3 Project Plan

3.1 Project Management/Tracking Procedures

Project Management Style: Agile Methodolgy
Our team has chosen to adopt the Agile project management style. Agile is well-suited to GridSAFE's research driven and experimental nature, where goals such as training AI models for anomaly detection, integrating hardware and software components, and adding cybersecurity features require frequent iteration and adaptation. Agile provides flexibility to continuously refine

requirements, prototypes, and performance metrics as we move toward our final product. This approach is essential for GridSAFE, where both software and hardware are constantly evolving to coalesce into a unified, functional system.
Each Agile sprint will focus on small, demonstrable deliverables that enable measurable progress while managing technical uncertainty.

Progress Tracking and Communication
To track progress and ensure team alignment throughout both semesters, we will use the following integrated toolset:
Trello with Discord Integration
Automated updates from Trello will be posted to our Discord server via the Trello plugin. This integration allows the team to easily manage To Do, In Progress, Testing, and Completed task lists in real time.
Sprint Meetings and Check-Ins
Weekly meetings will serve as sprint reviews and planning sessions to evaluate progress, identify blockers, and plan upcoming tasks.
Version Control and Code Review
Using Git we will track changes, maintain version history, and review each member's contributions in real time.
Milestone and Deliverable Tracking
Key milestones will represent major integration points or testing phases, ensuring that all subsystems progress cohesively toward the final product.

3.2 Task Decomposition

Software

- Train an AI model on logs/signals sent to it
- Use and test said AI model for accuracy of detection
- Create Simulated Network Logs
    - Normal
    - Anomalous
    - Malicious
        - MITRE ATT&CK
- Create Simulated Host Logs
    - Normal
    - Anomalous
    - Malicious
- Network Map/Topology
    - IT
    - OT
- Build Network
    - Set up/image VMs
- Integrate Network with AI
- Integrate AI with Hardware

Hardware

- Develop a 3D city to model an environment for our simulation.
    - Build City baseboard
        - Research materials (plywood, scrap, etc.)
        - Build/Plan/Implement circuit design
    - Design 3D Models in Autodesk Fusion
        - Design 3D Model types (Skyscrapers, houses, apartments, etc.)
    - Develop lights and connections to a Raspberry Pi/Arduino for communication
        - Buy lighting
        - Test lighting
    - Attach communication between devices to a signal/test output
        - Test signal latency, and accuracy/efficiency
    - Set up Raspberry Pi mini or 3
        - Code python to take in IDS data
        - Set up code to control RGB

3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria

Hardware Milestones

Milestone 1 – First 3D Prototype

- **Task:** Print the first building on mini baseboard.
    - **Metric:** Dimensions within ±15 mm (0.006 in) tolerance.
    - **Progress Measure:** Compare printed dimensions to CAD design; the measurements will be within the tolerance.
- **Task:** Achieve aesthetic quality of prototype.
    - **Metric:** Prototype passes visual inspection checklist (edges smooth, surfaces clean, proper alignment).
    - **Progress Measure:** Checklist completion rate; 80% of criteria met.

Milestone 2 – LED and Raspberry Pi Integration

- **Task:** Integrate LEDs with prototype and map out circuit plan.
    - **Metric:** LEDs are integrated with the first prototype.
    - **Progress Measure:** LEDs are completed and are 100% functional (They can turn on and off).
- **Task:** Program Raspberry Pi to control LEDs.
    - **Metric:** LEDs change RGB color on command.
    - **Progress Measure:** Test sequence of 3 color changes; ≥95% success rate.

Milestone 3 – Build 3D City Layout

- **Task:** Build and Design 3D City Layout
    - **Metric:** Complete 3D city layout with at least 10 distinct buildings.
    - **Progress Measure:** Successfully print and assemble all buildings.
- **Task:** Integrate LEDs and Raspberry Pi with 3D City
    - **Metric:** LEDs change RGB color on command in the entire city.
    - **Progress Measure:** Test sequence of 3 color changes; ≥95% success rate.

Software Milestones

Milestone 1 – Prototype AI

- **Task:** Define and complete 100% of example log criteria.
    - **Metric:** All log criteria documented and completed.
    - **Progress Measure: Checklist of example log sections; completion of at least one example per subsection.**
- **Task: Train Base AI on Example Logs**
    - **Metric: Accurate Detection 90% of the time.**
    - **Progress Measure: Demo of 5 log groups for each log classification.**
- **Task: Connect AI output to RaspberryPi**
    - **Metric: 100% Data transferred from AI to RPI**
    - **Progress Measure: Demo of 5 log groups for each log classification.**

Milestone 2 – IT Network Integration

- **Task:** Create detailed IT network map.
    - **Metric:** Complete network diagram with all nodes, connections, and protocols.

    - **Progress Measure:** Diagram reviewed and approved by team; accuracy rate ≥95%.
- **Task:** Develop full IT network configuration for project.
    - **Metr**ic: 100% of network components identified and configured.
    - Progress Measure: Verification through simulation or test deployment; all devices communicate successfully.
- Task: Feed logs from the network to the AI
    - Metric: 100% of expected network activity/logs received by the AI model.
    - Progress Measure: Verification through simulation

Milestone 3 – OT Network Integration

- Task: Add OT to network map
    - Metric: Complete finalized (IT & OT) network diagram with all nodes, connections, and protocols.
    - Progress Measure: Diagram reviewed and approved by team; accuracy rate ≥95%.
- Task: Add full OT network configuration for project
    - Metric: 100% of IT & OT network components identified and configured.
    - **Progress Measure:** Verification through simulation or test deployment; all devices communicate successfully.

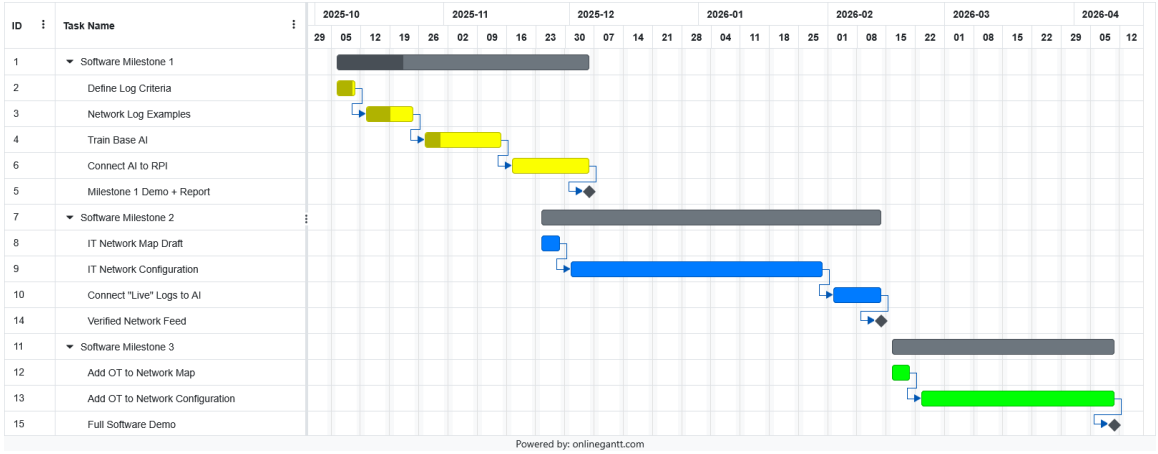
Final Integration

Final Milestone – Hardware and Software Integration

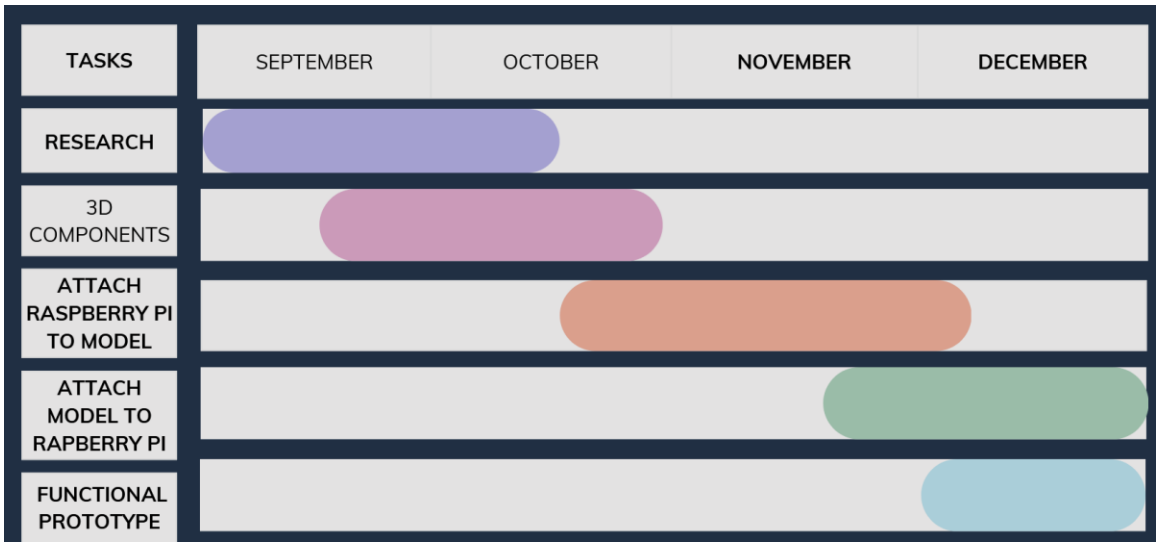
- **Task:** Integrate 3D city with IDS
    - **Metric:** All sensors, LEDs, and Raspberry Pi devices are successful.
    - **Progress Measure:** Verification through simulation and test logs, that all devices communicate successfully.

3.4 PROJECT TIMELINE/SCHEDULE

Software:



Hardware:



3.5 Risks and Risk Management/Mitigation

Software

1. Train an AI model on logs/signals sent to it
    - **Risk factor:** 0.6
    - **Potential risks:**
    - **Risk mitigation plan:** Try out different types of models and evaluate what has the most success. Use and improve training methods until we have acceptable accuracy.

2. Use and test said AI model for accuracy of detection

- **Risk factor:** 0.0
- **Potential risks:**
- **Risk mitigation plan:**

3. Create Network logs

- **Risk factor:** 0.2
- **Potential risks:** Once baseline / preset logs are completed, investigate making our own network for the collection of Realtime logs.
- **Risk mitigation plan:**

Hardware

1. **Develop a 3D city to model an environment for our simulation**
    - **Risk factor:** 0.4
    - **Potential risks:** Models may not fit together correctly; scale or alignment issues; print time could be longer than expected, external environment issues (movement near printers).
    - **Risk mitigation plan:** Start with small test building and incrementally print and test iterations of prototypes.

2. Build city baseboard

- **Risk factor:** 0.3
- **Potential risks:** Baseboard material may warp; measurements may be inaccurate.
- **Risk mitigation plan:** Use commercially available pre-cut boards and verify dimensions with multiple measuring tools before purchasing or assembly.

3. Design 3D Models in Autodesk Fusion

- **Risk factor:** 0.1
- **Potential risks:** Minor modeling errors; complexity may increase print time.
- **Risk mitigation plan:** Use standard libraries and templates to reduce custom modeling errors.

4. Develop lights and connections to a Raspberry Pi/Arduino for communication

- **Risk factor:** 0.6
- **Potential risks:** Wiring may fail; Raspberry Pi/Arduino may not handle timing/voltage requirements; LEDs may not respond correctly.
- **Risk mitigation plan:**
    - Prototype on breadboard first before soldering.
    - Consider using off-the-shelf LED controller boards compatible with Raspberry Pi.
    - Test small sections incrementally.
    - Keep spare LEDs and wiring materials available.

3.6 Personnel Effort Requirements

Include a detailed estimate in the form of a table accompanied by a textual reference and explanation. This estimate shall be done on a task-by-task basis and should be the projected effort in total number of person-hours required to perform the task.

Task Description	Human Effort	Hours Required
Design and build a baseboard for 3D city	Research potential materials to be used for the 3D city baseboard. Build the baseboard for the city model with planned wiring of the LEDs of the city in mind.	6
Design and build a 3D prototype	Use CAD software to design and print the first (and tallest) building on a mini baseboard that is of acceptable quality and aesthetically pleasing	4
LED and Raspberry Pi integration	Integrate miniature LEDs into the prototype building and ensure they are fully functional, being able to be turned on and off. Program the Raspberry Pi to control the switching of the LEDs as well as the RGB functionality.	3

Design and build the 3D city layout	Design and build the 3D city layout with at least 10 unique building designs that make up 3 distinct zones (e.g. a center business district, a surrounding urban district, and an outlying suburban district) Integrate LEDs into every building and program them to the Raspberry Pi to control their switching and RGB functionality so they can change into three different colors on command.	72
Define and complete 100% of example log criteria.	Create our very own logs for both network and host. These logs will have three categories – normal, anomalous, and malicious.	6
Train Base AI on Example Logs	Aggregating and feeding the simulated logs into the AI as its data and training this model such that it can detect and understand in the scope of our project what normal, anomalous, and malicious logs look like.	30
Connect AI output to RaspberryP	Connecting the AI output such that it feeds into the Raspberry Pi.	8
Create detailed IT network map.	Creating and labeling the network map for our project such that every machine and interactions between machines is clear.	4
Develop full IT network configuration for project.	Allocating, imaging VMs, and setting up the machines such that the machines interact as a IT style network needed for our project.	50
Feed logs from the network to the AI	Using python scripts to aggregate and sent the logs from every machine on the network to the AI	10
Add OT to network map	Adding into the IT network, map the OT machines and their new connections.	4
Add full OT network configuration for project	Allocating, imaging VMs, and setting up the machines such that the machines interact as a full IT and OT network needed for our project.	60

3.7 Other Resource Requirements

Software

- Python
- Java
- Wireshark
- XGBoost
    - Computer with at least 16g RAM
- Proxmox

Hardware

- Raspberry Pi / microcontrollers
- RGB LED strips
- MOSFETs for LED control
- Breadboards / jumper wires / connectors
- Power supply (5V/12V depending on LED strips)

Materials / Physical Construction

- Plywood / foam / plexiglass / acrylic sheets for buildings
- Glue, screws, or fasteners for assembly
- Paint, markers, or vinyl for city aesthetics
- Mounting brackets or frames for stability

4 Design

S4.1 Design Context

4.1.1 Broader Context

GridSAFE sits at the intersection of critical infrastructure protection and public safety. It gives students and instructors a hands-on, cyber-physical sandbox to explore how attacks on ICS (industrial control systems)/OT (operational technology) networks manifest and how defenses work, connecting IT (informational technology) monitoring to physical consequences on a simulated grid. This supports situational awareness and workforce readiness aligned with widely used OT/ICS guidance and adversary models.

Public health/safety and welfare raise awareness of grid cyber risk and improve preparedness through experimental learning.
Global/cultural/social: promotes ethical, vendor-neutral education applicable worldwide.
Enviormental: small material footprint; PLA components; heavy use of digital simulation.
Economic: low-cost scalable platform that reduces barriers for under-resourced programs and builds skills demanded by employers.

Area	Description	Examples
Public health, safety, and welfare	The project promotes the general well-being of society by improving cybersecurity awareness and preparedness related to critical	• Increases awareness of cybersecurity risks to power grids and infrastructure that support public safety.

	infrastructure systems. By helping students and educators understand how cyberattacks could disrupt essential services, the project indirectly contributes to public safety.	• Reduces the likelihood of future cyber incidents through education and prevention. • Promotes workforce readiness for cybersecurity roles, enhancing community resilience.
Global, cultural, and social	The project aligns with global and societal values of promoting education, digital literacy, and ethical technology use. It encourages collaboration and responsible innovation across diverse cultural and professional groups.	• Supports the global goal of securing critical infrastructure. • Promotes cybersecurity education without cultural bias—applicable to students and educators worldwide. • Reflects ethical engineering practices and professional codes that prioritize security and transparency.
Environmental	The project has minimal environmental impact, as it uses digital simulations and small-scale hardware.	• Uses minimal resources as well as environmentally friendly, PLA
Economic	The project offers a cost-effective educational tool that makes cybersecurity learning more accessible. It also helps develop skills that are increasingly valuable in the job market, contributing to workforce development.	• Provides a low-cost, scalable platform for schools and training programs. • Reduces barriers to cybersecurity education for underfunded institutions. • Contributes to economic resilience by preparing students for high-demand cybersecurity careers.

4.1.2 Prior Work/Solutions

[1] R. Hanson, "Electric Grid Cyberattack: An AI-Informed Threat Model," *LessWrong*, [Online]. Available: https://www.lesswrong.com/posts/zc5uhndCoxEKZvXoQ/electric-grid-cyberattack-an-ai-informed-threat-model. [Accessed: Oct. 28, 2025].

[2] B. Blakely et al., "Simulating the effect of cyber attacks on a Power Grid — Design Document, SDMAY23-02," Iowa State University Department of Electrical & Computer Engineering, Apr. 2023. [Online]. Available: https://sdmay23-02.sd.ece.iastate.edu/Final%20Design%20Document.pdf. [Accessed: Oct. 28, 2025].

[3] A. Bondok, "Modeling Cyber Attacks on Power Grid Consumers: A Threat-Modeling and Simulation Study," Diploma Thesis, Institute of Telecommunications, Vienna University of Technology, Vienna, Austria, 2025. [Online]. Available: https://repositum.tuwien.at/bitstream/20.500.12708/215733/1/Bondok%20Alhasan%20-%202025%20-%20Modeling%20cyber%20attacks%20on%20power%20grid%20consumers%20a...pdf. [Accessed: Oct. 28, 2025].

Several similar projects exist within the field of critical infrastructure cybersecurity; however, most are developed for private or institutional use and are not accessible to the general pblic. Hese systems are typically designed for internal research, industry-specific simulations, or workforce training with energy or utility organizations. As a result, they are not available for broader educational use or community engagement.

While numerous academic theses and research studies address cyber-physical simulation of power grids, most focus on theoretical modeling or are limited to high-cost laboratory environments. Few provide open, replicable frameworks or low-cost physical demonstrations suitable for classroom settings.

A previous Iowa State University senior design team SDMAY23-02 attempted a related project focusing on cyberattack visualization within a power grid model. However, several aspects remained incomplete – particularly in terms of hardware integration and system scalability. Building upon their groundwork, the GridSAFE team is taking a new approach focused on modularity, affordability, and educational accessibility. Our design diverges from prior efforts by emphasizing open-source tools, real time visualization, and full system integration between the virtual network, machine learning intrusion detection system, and physical 3D printed city model.

Pros	Cons
Public access to research/resources used	Quality may not be professional enough for some scenarios
Affordable options available and used while maintaining professional standards	Effort to produce for groups can be subjective and challenging
Documented effort and progress for replication & reproduction	For our full functionality “extra” materials are required to build our product
Strong educational opportunities for advancing learning	3D printables are a resource for physical appearance.
Great tool for physical understanding & appreciation of critical infrastructure	
Adaptive replication/can be made differently and maintain functionality	

4.1.3 Technical Complexity

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles –AND–
2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

This project is sufficiently complex as it consists of three major technologically challenging components that display many design and implementation challenges. First is our custom network environment and log generation where many virtualization and networking principles are needed. Some of the key principles we need to adhere to are guaranteeing performance by allocating resources properly among our VMs so that everything can function properly without any stalling,

and making sure our network communication is isolated and reliable. We will be processing lots of data with our logs as well as using a fair amount of storage for all the data we collect, so we need to be smart about how we maintain our system and ensure that communication between machines works as intended. We need to ensure realistic log generation that accurately reflects real-world behavior associated with select MITRE ATT&CK techniques. Creating a realistic network topology within Proxmox that allows this will be another key challenge. The second major component that's being developed is the machine learning model that will be used for our IDS. The challenge here is creating an intelligent, accurate, and explainable classifier. To accomplish this, we need to parse the raw data from our captured logs and translate them into data suitable for training. After that, we must experiment with it to see how accurate we can make it and how it responds to different training data. The third major component will be the large physical 3D printed city to give a visual representation of our IDS in real time. This will require multiple electrical and software engineering principles as it requires soldering, use of a microcontroller, 3D modeling and printing, and software development to control the LEDs. Finally, all these components need to communicate with each other so it can all function as one in real time.

4.2 Design Exploration

4.2.1 Design Decisions

1. The team chose to use generic PLA as the filament of choice for printing our structures because it was the most readily available, economical, and easy to work with. Additionally, the decision was made to use generic PLA after consulting the SIC on the optimal filament to be used in their Bambu X1C 3D printers. By choosing this filament, the team will have greater ease procuring the filament needed for our project and will save money while doing so. The team will also be able to use SIC's 3D printers, which will save time when printing our structures.
2. The team decided on the dimensions of our structures to be between 1-7 inches in height so they would be within the plate parameters of SIC's Bambu X1C 3D printers and to save on the amount of filament required when printing our structures. This will enable the team to utilize SIC's 3D printers, increasing the number of structures that can be printed simultaneously while saving time and filament needed for each individual structure.
3. The team also decided to generate authentic network logs within GridSAFE to enhance realism during the project demonstration. Specifically, we saw a piece of the design tradeoffs that we were lacking in cyber – Technical Integration. While this adds complexity, it also provides a more compelling, technically accurate representation of grid-scale cyberattack simulations, aligning with the projects' educational objectives.

4.2.2 Ideation

When the team was deciding what kind of filament we wanted to use to make our structures, we wanted a filament that was cheap, easy to procure, easy to use, and would work well with printers that we were looking to use for our project. The first option that we considered was Polylactic Acid (PLA), which is the most common kind of filament used for 3D printing. It is the most affordable and easy to use. The second filament considered was Acrylonitrile Butadiene Styrene (ABS), this filament is particularly strong and resilient, which was attractive as we wanted our structures to be durable. The third filament was Polyamide (Nylon), which was the strongest filament considered. The fourth filament was Co-polyester (CPE); this filament works best for prints that require

dimensional stability and parts that would snap together. The fifth and final filament considered was Polycarbonate (PC), which is durable and highly heat-resistant.

4.2.3 Decision-Making and Trade-Off

To identify the optional filament for the GridSAFE 3D-printed structures, the team compared several filament types commonly used for prototyping – PLA, PETG, and ABS. The evaluation considered key criteria relevant to our project goals.

1. Cost Efficency
2. Ease of Sourcing
3. Printer Compadability
4. Durability/Strength
5. Print Reliability

Each criterion was weighted according to importance (out of 5), and each material was scored from 1-5 (5 being the best)

Criterion	Weight	PLA	PETG	ABS
Cost Efficiency	5	5	3	2
Ease of Sourcing	4	5	4	3
Printer Compatibility	5	5	4	3
Durability/Strength	3	3	4	5
Print Reliability	3	5	3	2
Weighted Total	—	**71**	60	53

Thus – PLA being at the top = 71.

Based on the weighted analysis, PLA received the highest total score, indicating the most balanced performance across all criteria. While PETG and ABS offered marginally higher strength, they presented challenges in sourcing, cost, and print reliability. After consulting with the SIC makerspace, the PLA was confirmed as the most practical and compatible material for the Bambu X1C printers.

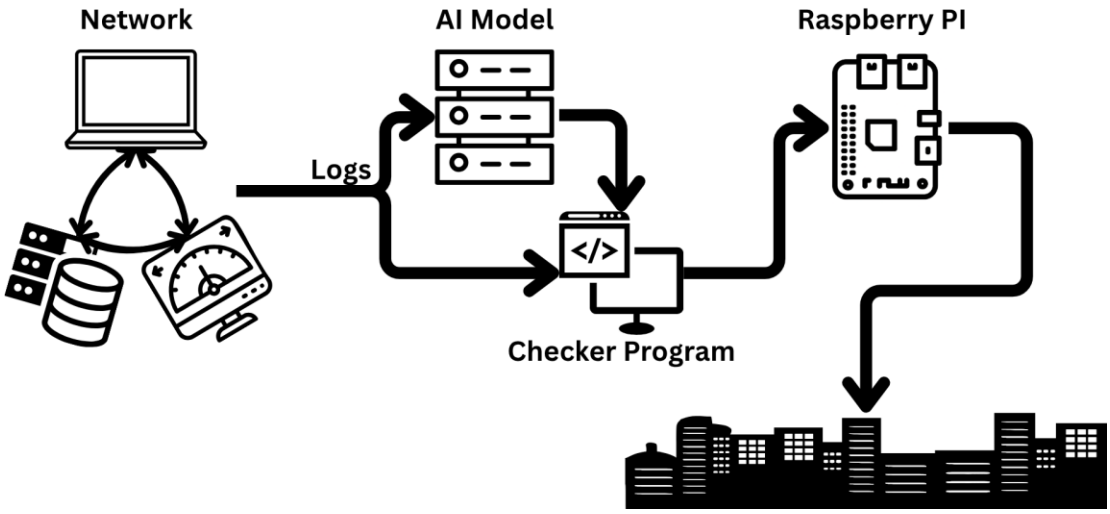
4.3 Proposed Design

4.3.1 Overview

The GridSAFE system is designed to simulate cyberattacks on a model of an electrical grid and display the impact of these attacks through a physical model. The system collects simulated network activity, analyzes the data using an AI model, and sends the results to a physical city model where LEDs represent grid status in real time.

As shown in the figure below, the system consists of three primary components:

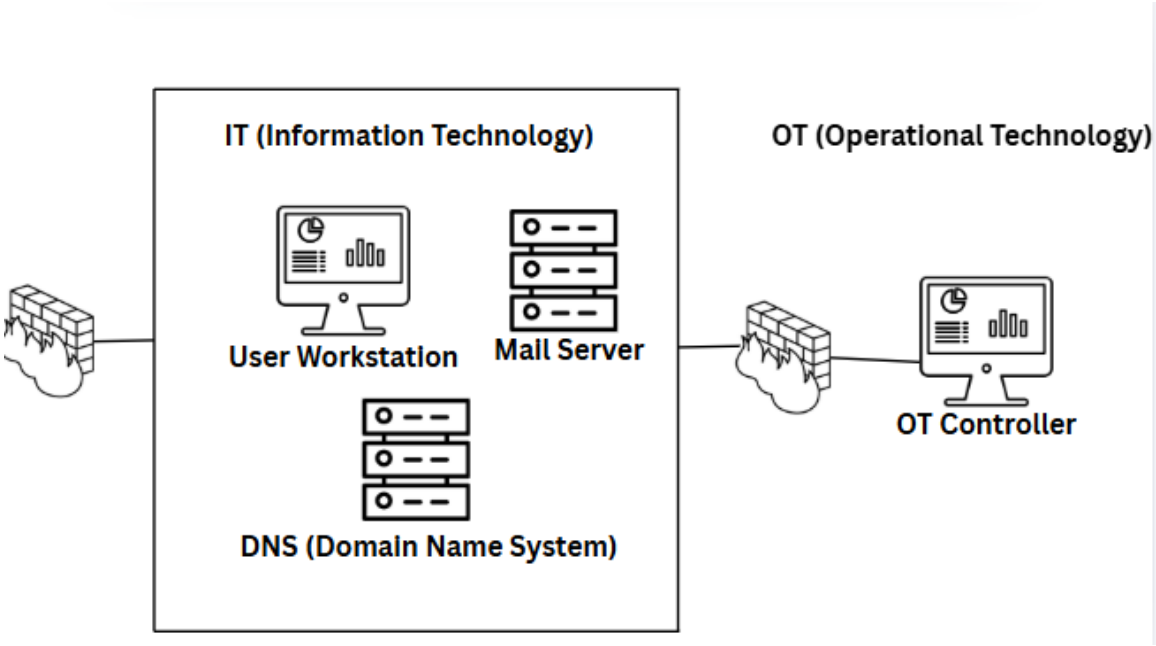
1. **Virtual Network:** Generates network traffic logs that represent both normal and abnormal industrial control system (ICS) and supervisory control and data acquisition (SCADA) activity.
2. **AI Model:** Processes network logs and classifies them as either normal or anomalous using machine learning algorithms, which are then checked by a separate program to verify accuracy.
3. **Physical Model:** Translates classification results into visual LED indicators across a miniature 3D printed city model using a Raspberry Pi to represent affected grid sectors.



4.3.2 Detailed Design and Visual(s)

Network Log Generator

- **Purpose:** Produces network traffic and operational data that mimic both normal and anomalous ICS/SCADA behavior.
- **Implementation:** Network monitoring tools like Security Onion combined with python scripts create log files that include time, device, user, command, and more when applicable.
- **Output:** Structured log data stored in a shared directory accessible to the AI Model subsystem.



AI Model

- **Purpose:** Detects anomalies in the incoming network logs.
- **Implementation:** A machine learning pipeline trained using supervised training with labeled normal and attack logs.
- **Operation:** The model ingests real-time or batch logs, assigns anomaly scores, and outputs predictions (e.g., “normal,” “possible intrusion,” “confirmed anomaly”).
- **Integration:** Output is sent to the Checker Program and validated.

Checker Program

- **Purpose:** Acts as a bridge between the AI Model and the Raspberry Pi.
- **Implementation:** Python script that parses model output, validates data format, and converts classifications into status codes.
- **Communication:** Uses HTTP communication to send the results to the Raspberry Pi.
- **Output:** A JSON message indicating which part of the city model should be which color (green, orange, red).

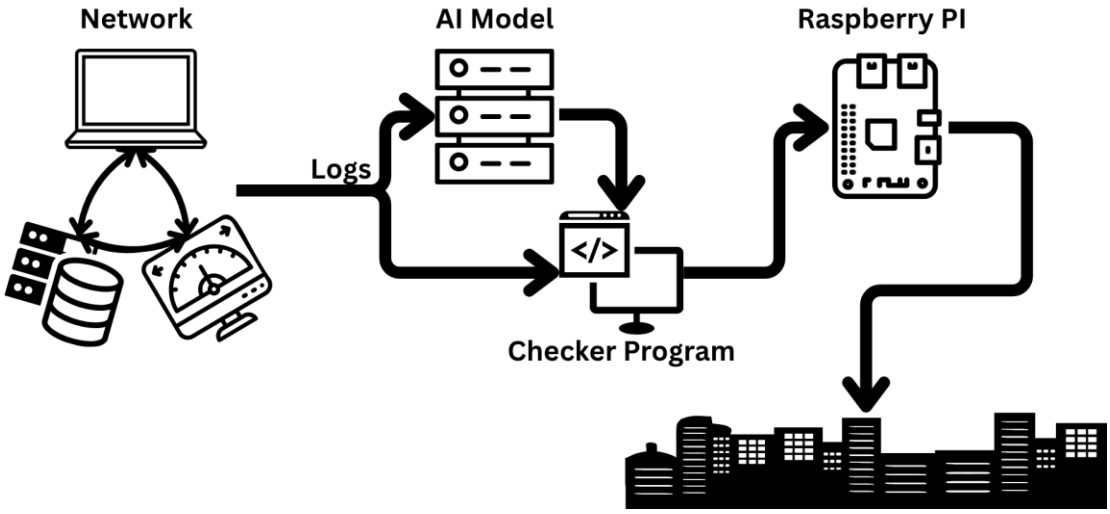
Raspberry Pi Subsystem

- **Purpose:** Controls the LEDs in the physical city model.
- **Implementation:** Raspberry Pi running lightweight Python GPIO driver script. Also, RGB LEDS allow three-color indication per structure.
- **Integration:** Receives commands from the Checker Program and activates LEDs with color coding (green for normal, yellow for suspicious, red for confirmed attack).

- **Output:**

Physical City Model

- **Purpose:** Provides a tangible visualization of grid health and cyberattack impact.
- **Implementation:** 3D-printed buildings placed on a custom baseboard; wiring connects LEDs beneath each sector.
- **Integration:** Powered and controlled by the Raspberry Pi.



4.3.3 Functionality

In real operation, an instructor or student begins the simulation by generating network activity logs or sending pre-generated logs. The AI Model analyzes the logs and classifies activity as normal or anomalous. The Checker Program validates the model's output and sends commands to the Raspberry Pi.

The Raspberry Pi then activates the LED display:

- **Green** indicates normal grid activity.
- **Yellow** signals potential irregular behavior.
- **Red** shows a detected attack.

This process allows users to see how a cyberattack on digital infrastructure can cause visible physical effects in real time.

4.3.4 Areas of Concern and Development

The current GridSAFE design effectively meets many defined functional requirements and aligns well with user needs for an educational and demonstrative cybersecurity system. The prototype demonstrates a complete data flow from simulated network activity to physical visualization,

showcasing how cyber events can affect critical infrastructure in a tangible way. The modular structure allows both software and hardware teams to test and refine components independently, which supports ongoing development and scalability. Additionally, the system's use of AI-driven anomaly detection provides a realistic representation of modern cybersecurity monitoring, fulfilling the project's objective of bridging technical analysis and physical feedback.

The primary concerns center on data realism, system accuracy, and integration reliability. The simulated logs must closely replicate real ICS/SCADA network behavior to ensure the AI model produces meaningful results. Model performance remains a concern, as early prototypes may experience false positives or negatives that could misrepresent system status. Hardware communication between the Checker Program and the Raspberry Pi must also be optimized to maintain synchronization and prevent data delays. Finally, scalability and maintainability will be important to ensure that the system can handle larger datasets, real-time analysis, and potential future expansions such as cloud-based operation or interactive GUI control.

Immediate development efforts will focus on improving data fidelity, model accuracy, and hardware integration. The software team plans to expand the dataset used for machine learning by incorporating a wider range of simulated ICS/SCADA traffic patterns and refining anomaly labels to improve model training and reduce misclassifications.

On the hardware side, integration testing will be prioritized to verify synchronization between the software output and physical LED responses.

Additional plans include beginning development of a web-based GUI or dashboard that will allow users to configure simulation parameters, visualize results in real time, and replay past scenarios. This will improve usability and enhance the system's value as a teaching and demonstration tool.

Questions for clients and advisors:
Are there specific types of cyberattack simulations that should be prioritized for educational use cases?
What level of model explainability (ex: visualization of future importance) would be most valuable for students or instructors?

4.4 Technology Considerations

Network Design: We will be using Proxmox to configure our network. This was chosen as it is open-source and available to run for free locally or on a dedicated server. It allows for low level control, which will be needed when setting up our network to emulate traffic with our generated logs. This does present a weakness as there's a large potential for misconfiguration which could cascade into many other issues. The trade-off with this is that we will have to be more hands on in configuring our network and can't rely on ease of use with an application such as VMware. In the case we need an alternative, VMware is an option, but it would require us to pay for a license and may not have all the networking options needed to set up our network.

IDS Design: To build our IDS, we plan to use XGBoost, a machine learning algorithm. The strength of using a ML model for our detection system is that it may be able to detect different patterns that aren't extremely obvious and recognize an attack early in the process before any hard-coded algorithm could. We chose XGBoost as it allows for supervised training and multi-class

classification so when it triggers an alert for an attack, we'll know what type of attack it detected and can further analyze it to see whether it was incorrect and how to fix it. The weaknesses of these choices are that ML models can be very unpredictable. If most logs in training are normal, it may not be very inclined to detect an attack and can miss something important. If too many malicious logs are included in training, it may have the opposite problem and falsely report a threat. The trade-offs here are that using only our own custom model to detect an attack isn't a great idea, but this project is largely for learning. Using XGBoost will be a more challenging training process compared to a binary classifier, but will end up being more accurate and descriptive, which is necessary for our analysis. If we can't get an accurate enough model, there are other algorithms that we could experiment with to see if we can improve our IDS.

4.5 Design Analysis

So far, our team has developed multiple 3D models which will act as prototypes for our building inside the city. They are all built within 1–7-inch heights and include high value targets such as churches, schools, and the capital. We have also accomplished successfully creating logs for the AI model to train off of.

As many of the physical connections and aspects inside the design of 4-3 are still under development, the physical applications of those designs are still on target for fitting these ideas. What is currently functioning and developed as progress fits the target goals; we have set ourselves in the outlines created.

Plans for our future implementation to be achieved are to get some more physical components created and then connected first. Many implementations of our design revolve around the physical environment that our project will display for users, so our goals are to finish this aspect first. Currently no design elements appear to be problematic for the designs created/implemented this far. More prototypes are required and are a part of the plan for our project to be successful, which we are mid-way through implementation without complications.

5 Testing

Testing is an **extremely** important component of most projects, whether it involves a circuit, a process, power system, or software.

The testing plan should connect the requirements and the design to the adopted test strategy and instruments. In this overarching introduction, give an overview of the testing strategy and your

team's overall testing philosophy. Emphasize any unique challenges to testing for your system/design.

In the sections below, describe specific methods for testing. You may include additional types of testing, if applicable to your design. If a particular type of testing is not applicable to your project, you must justify why you are not including it.

When writing your testing planning consider a few guidelines:

- Is our testing plan unique to our project? (It should be)
- Are you testing related to all requirements? For requirements you're not testing (e.g., cost related requirements) can you justify their exclusion?
- Is your testing plan comprehensive?
- When should you be testing? (In most cases, it's early and often, not at the end of the project)

5.1 Unit Testing

What units are being tested? How? Tools?

(edit this but Im attempting to o my part for missing today –Brant)

We have been testing loads of the hardware for our 3d models that we are using to visualize the city. Going through multiple stages of development, prototyping, analyzing results, and redesigning until we find a satisfactory model. We start with a pre-built design, then we adjust to fit our criteria for the mode (size, holes for lights, bottom hole for electronics). Then we splice the model and see if it prints well, if it does and we like it then we have a working model, otherwise we go back and figure out what happened. (nearby printers shaking too much, not enough supports, extra supports that make it ugly, no holes in a building etc.) We are also testing the LED lights for the hardware, making sure we can connect to a raspberry pi and control the lights so we can then implement a connection to our AI. (someone with better knowledge please finnish)

3D Printed Model Building:

This part of our project will need to be tested for sizing accuracy, structural integrity, and visual quality. To do this we will visually inspect our models by measuring them and ensuring that they look up to standard. We will also need to check compatibility with the LEDs and inspect how they look and if we need to find another method. This will require measuring and testing the LEDs for fitting and displaying correctly. We will use rulers to confirm the measurements and a visual inspection checklist to confirm its functionality.

LED Lights:

For this instance, we need to check power consumption and controllability. We can measure power output with tools like multimeters and check the correctness of the controls with visual inspections. We will need to use dedicated power supplies and simple wiring setups with breadboards to prototype our design and ensure we can be successful.

Virtual Network Log Collection Script & API:

We will need to test the logs we collect by checking correct formatting, timestamping, data integrity, and API call handling. This will be done by mocking network output on our simulated network to check if our collection and API calls are successful. This will be done using Python's testing library "pytest" along with any other testing tools we may find useful.

AI Model Interface:

We will need to check the output of our AI model against the expected output. This will test if we are classifying attacks correctly and can accurately detect an attack. We will parse individual parameters from the log and process them to identify specific parameters which we will use to train our model. This can be done with the "pytest" library to check our outputs against what is expected.

Output Checker:

We will have to check the AIs output against what we expect it to say and see if it is correct. If it is not, we will have to analyze what happened and try to figure out why it classified a log incorrectly. There will be some upper bounds for our model to determine whether or not an attack is occurring, and we need to experiment and find out what a reasonable value is. This will be done with Python's "pytest" library so we can determine the correctness of the results.

Raspberry Pi LED Controller:

We will have to manually check the correctness of this ability by observing the lights while we pass commands through to it. First, we need to run tests to check that the lights are functioning properly, and once we determine that they are, we can test the API requests to make sure the lighting commands trigger as they should. This will be accomplished by sending various commands to the Pi to test the lights and follow with a visual inspection to ensure that they are behaving as intended.

5.2 Interface Testing

What are the interfaces in your design? Discuss how the composition of two or more units (interfaces) are being tested. Tools?

Virtual Network -> AI Interface:

The virtual network generates system logs that are collected through a script or lightweight API call and fed directly into the AI model. We test this by replaying known normal, anomalous, and malicious logs into the AI to ensure the log format, collection method, and model input all work correctly together. This is done using Python log-replay scripts and controlled test datasets.

AI -> Output Checker Interface:

The AI outputs a classification that the Output Checker reads via a script or simple API-style handoff. We test these components together by piping real AI outputs—correct, incorrect, and malformed—into the checker to ensure it parses results reliably and stays aligned with the AI's output format. Automated Python tests validate the combined behavior.

Output Checker -> Raspberry Pi:

When the checker detects an incorrect or malicious event, it sends JSON data to the Raspberry Pi's LED controller. We test this by sending checker-generated JSON to a test endpoint on the RPi and verifying that the expected node status changes are triggered before testing on the physical LEDs. Tools include JSON validation scripts and a mock logging endpoint.

Raspberry Pi -> LEDs:

The Raspberry Pi acts as the control module for the LEDs throughout the model city. The Raspberry Pi runs code to turn the LEDs on or off, or to change the color of the LEDS from green to red.

LEDs -> Model Buildings:

The LEDs reside within each of the model buildings, turned on to the color green in their natural state. When the LEDs receive a command from the Raspberry Pi, the LEDs will turn red, changing the lighting of the model building, signaling an outage.

5.3 Integration Testing

What are the critical integration paths in your design? Justification for criticality may come from your requirements. How will they be tested? Tools?

Log Pipeline -> AI Inference:

This integration path covers the flow of logs from the virtual network's collection script into the AI model. It is critical because accurate anomaly detection depends on logs being gathered, formatted, and delivered correctly; if this path breaks, the AI cannot meet the requirement to classify normal, anomalous, and malicious events. We test this path by replaying labeled log files through the same collection mechanism used in deployment and feeding them into the model, checking that each entry is parsed and classified as expected. Tools include Python log-replay scripts, pytest integration tests, and standard ML metric libraries to compare predictions to ground-truth labels.

AI Inference -> Output Checker:

This path transfers the AI's output into the Output Checker for validation against the original log labels. It is critical because the system must not accept incorrect or malformed AI outputs—our requirements specify that misclassifications must be caught and handled, not silently ignored. We test this by piping real AI outputs, including correct, incorrect, and intentionally malformed examples, directly into the Output Checker. The checker must correctly parse the output, compare it to the ground truth, and return the expected validation result or error handling. Tools include Python-based test harnesses, pytest fixtures containing varied AI outputs, and parsing/assertion checks.

Output Checker -> JSON Alert Generator:

This path produces the structured JSON alerts that represent misclassifications or malicious detections. It is critical because the software must provide a consistent, machine-readable alert format to downstream components; without this, detections never propagate beyond the checker. We test this by triggering the checker with known test cases and verifying that the resulting JSON payloads contain the correct fields, follow the agreed schema, and reflect the correct node/state information. Tools include Python unit tests for JSON construction, schema validation libraries, and a local mock listener to capture and inspect the generated messages.

JSON Alert Generator -> Raspberry Pi -> LEDs

This path sends the produced JSON alert data to the Raspberry Pi which acts as the control module for the hardware interface. This path is critical because the Pi must receive and interpret alerts to correctly drive the LEDs to demonstrate cyber-attacks. If this fails, there is no visual feedback, and no events are detected. This path will be tested by sending different and unique JSON test cases to the Pi, confirming that the Pi can accurately parse the messages and appropriately trigger the corresponding LEDs. Tools include python scripts to parse JSON data from the IDS and to log any errors to verify viability.

5.4 System Testing

Describe system level testing strategy. What set of unit tests, interface tests, and integration tests suffice for system level testing? This should be closely tied to the requirements. Tools?

Preparation:

To prepare for this testing, we will need to ensure that all the components of our system are functioning properly. This will include the unit tests previously discussed about our logger, output checker, and raspberry pi lighting controller.

Execution:

To test the system, we will inject pre-validated, labeled data from the virtual network or other sources into our simulated system and test the output.

Observation and Validation:

Log Validation – We will need to compare the model's classification against the actual expected output to see whether it is predicting attacks accurately or not. This will mean that an alert should be sent whenever an attack is detected, and it should stay idle otherwise.

Log to Output Checker – In the instance of a malicious scenario, we need to verify the JSON that is received by the Raspberry Pi. If the unit tests are passed, this will mean we can process the logs and run a further analysis on the logs to see if the output is correct or if we need to investigate more and improve our model.

3D Model Functionality – The final observational test we will need to run is running through the whole system and checking that malicious logs that are correctly detected will transition states of the city to display a “downed” visualization. The opposite should work the same and if a city block regains functionality, it should properly transition to an online state.

5.5 Regression Testing

How are you ensuring that any new additions do not break the old functionality? What implemented critical features do you need to ensure do not break? Is it driven by requirements? Tools?

The current way we are going about making new additions without breaking old functionality is the research that went into our original designs. Most of our designs have room for leniency (they are built for replacement/reconstruction) so that old designs are not tied down to their limits.

Another example is using GIT for our code. We will push to main for code in our python scripts and log aggregators such that the main is always a working version i.e never pushing bad code to main.

Our 3D models are a great example of the capabilities of our regression testing, starting originally with prebuilt models and then making further progress bit by bit until we achieve the desired result. Our apartment building in particular has been a challenge as the original design has zero holes, was fully hollow, and was meant for a render, not a 3D print. We have since edited the splice and the STL for the model to fix the meshes and its difficulty in correctly printing out the holes so that the building is the right dimension and let's light out, which is a goal of our design so that we can simulate a city with LED's being power going to it.

5.6 Acceptance Testing

How will you demonstrate that the design requirements, both functional and non-functional are being met? How would you involve your client in the acceptance testing?

We will demonstrate that our functional and non functional requirements are being met by running end to end tests that show the full software pipeline working correctly. This includes log collection, AI classification, Output Checker validation, and JSON alert generation using labeled datasets and controlled scenarios. Functional requirements will be confirmed through correct classifications, detection of misclassifications, and consistent alert formatting, while non functional requirements will be shown through reliability testing, graceful handling of errors, and clear modular code structure. Since our client is a member of the team, we will use our presentations to walk through these tests in real time and allow them to verify that the software meets expectations through both our prepared scenarios and any additional cases they want to see.

5.7 Security Testing (if applicable)

Security testing ensures that only the intended components interact with the GridSAFE system and that the Raspberry Pi is safeguarded from unnecessary network exposure. The following tests will be performed:

Network Hardening

- Scan active services and open ports
- Disable or block non essential ports and services
- Verify communication channels function after security testing

Device and Access Control

- Authorized users can access Raspberry Pi
- USB devices cannot interact with the system

5.8 User Testing

To evaluate the usability and overall user experience of GridSAFE, the team will incorporate real users such as college and high school faculty members who will read and review the GridSAFE user setup manual. Surveying different types of users in different types of education ensures diverse feedback for our project, and its purpose as a learning tool. We will give the faculty the GridSAFE setup manual that goes through the process of setting up both the software and hardware, and they will answer multiple questions based on how feasible and usable the tool would be to their class. These insights will allow the team to identify areas for improvement and ensure the product

meets the practical needs of instructors integrating GridSAFE into their classrooms.

Faculty reviewers will be asked to:

- Read the usability guide thoroughly.
- Evaluate the ease of setup for the hardware modules.
- Assess the clarity and completeness of instructions for both hardware and software connections.
- Assess the level of complexity for classroom use (Higher Education, lower education).
- Consider the feasibility of integrating the system into a course or lab session.

Data Collection Methods:

- Survey: After reviewing the guide, faculty will complete a structured survey containing quantitative ratings (on a 1–10 scale) and open-ended questions for additional comments, concerns, or suggestions.
- Optional Follow-Up Discussion: Faculty may be invited to participate in a brief verbal feedback session to clarify responses and provide more nuanced insights.
- Observations: The team will note any recurring points of confusion, questions about setup, or difficulty navigating instructions.

Expected Outcomes:

- Faculty feedback will indicate whether the hardware setup appears feasible and whether the instructions are sufficiently clear and detailed.
- Survey ratings will help determine overall usability, integration potential, and likelihood of adoption in courses.

5.9 Results

What are the results of your testing thus far? Include any numerical, graphical, or qualitative testing results here? How do they demonstrate compliance with the requirements or addressing user needs? Use a summary narrative to discuss what you've learned and what next steps need to be taken.

3D Model Prints:

So far, we have begun printing out or building for the city visualization. There were some errors initially including the hollowness of the buildings, lacking window holes to provide lighting, and mesh errors in the models we were editing. After multiple iterations, we were able to produce various building models that work for our project. This demonstrates the compliance with our physical requirement of having physical models to house our electronics and allow light to pass through.

LED/Hardware interfacing:

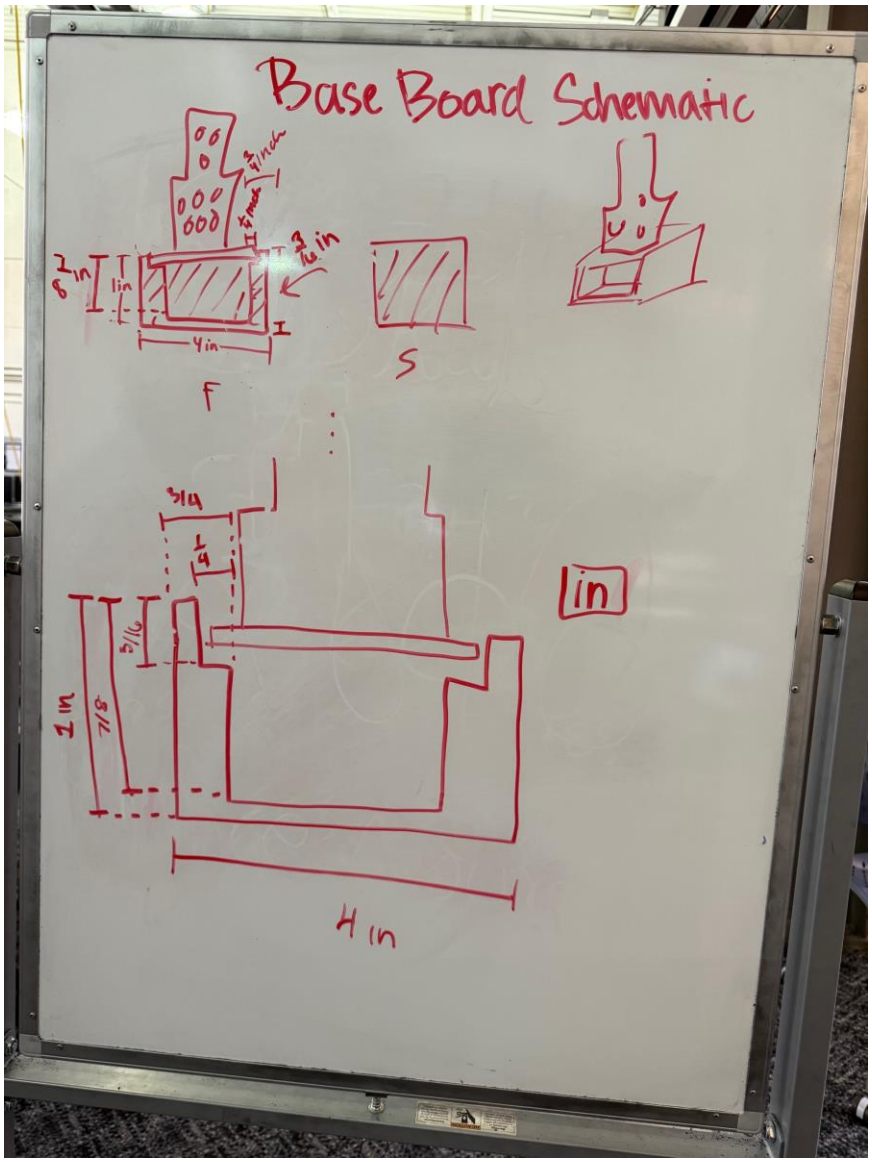
Bench testing of the LED control system connected to the Raspberry Pi has been successful so far. While hosting an API's the Raspberry Pi has shown to be capable of receiving requests and reacting by telling the LEDs to change states. This shows that the Pi can connect to external sources and reliably control the lighting component of the project.

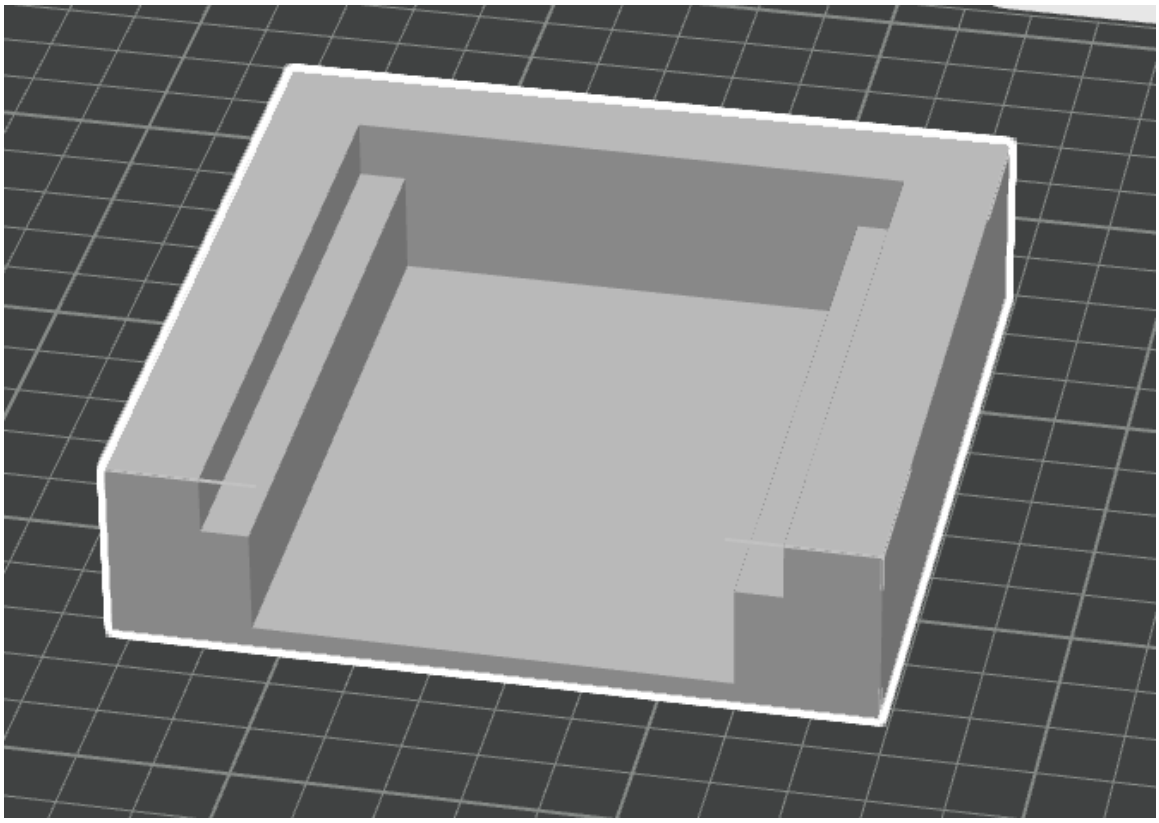
Software Component Testing:

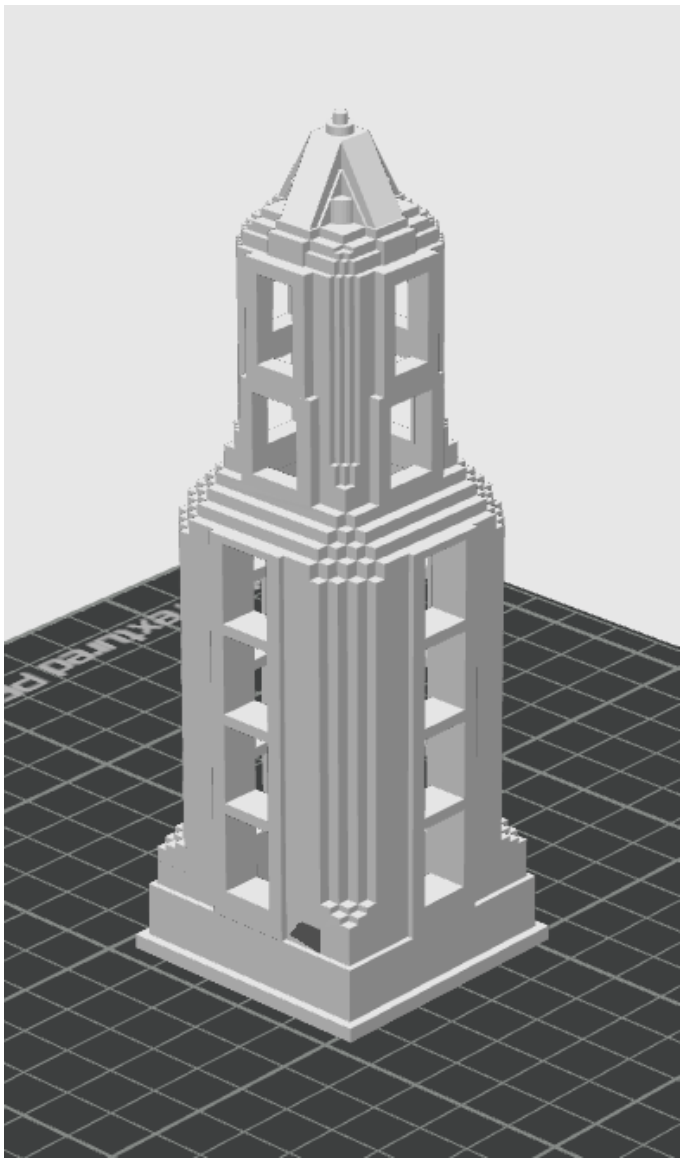
Initial training runs and unit testing of the model's inference show its ability to classify network logs. During the early stages of development, we do not have any impressive results, but we are able to parse our log data into training data for our model and produce estimates on whether a certain attack is taking place.

6 Implementation

GridSAFE has produced a preliminary prototype, a scaled down version of the 3D City Model. The Model consists of a small 3D printed baseboard, a Plexi-glass baseplate, and a 3D printed Skyscraper (Coin Building). We have created a simple schematic for the 3D baseboard shown below, as well as a prototype.


Base Board Schematic
4 in
F
S
in
1 in
4 in

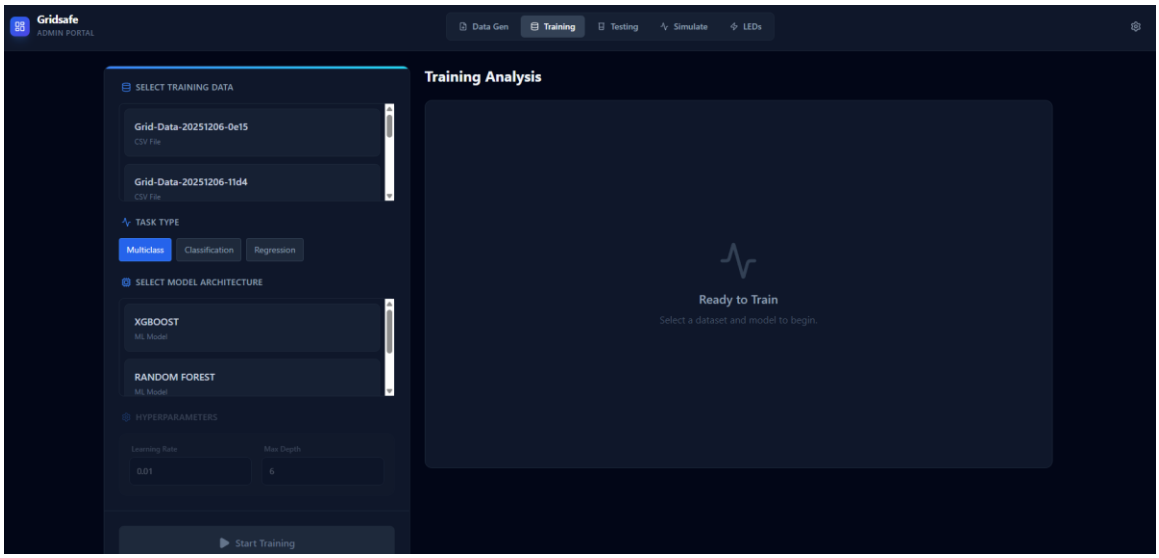




The GridSAFE team has also produced a preliminary implementation of our anomaly detection AI. The model uses HDFS logs, the trained model, and a JSON config file. Below are examples of the HDFS logs and the output.

```
=== Anomaly Distribution ===
is_anomaly
True    201
Name: count, dtype: int64
Saved gridsafe_output.json
(venv)
```

```
=== Anomaly Distribution ===
is_anomaly
True    0
Name: count, dtype: int64
Saved gridsafe_output.json
(venv)
```



7 Ethics and Professional Responsibility

For GridSAFE we have a considerable amount of professional and ethical responsibility dealing with both a network and an AI we are training in. Making sure our resources for training are acquired ethically and appropriately while also maintaining realistic data. Making sure the network can't affect other environments or teach malpractice techniques is another consideration we have for our project. It's important that we follow key concepts for cybersecurity by keeping our design with integrity, safety, and transparency in mind. We want to make sure we follow these principles as accurately as possible, as our goal is to be an example for academic use of our project, so it's imperative that we also follow real world concerns in our design.

7.1 Areas of Professional Responsibility/Codes of Ethics

Area of Responsibility	Definition	Relevant Item from Code of Ethics IEEE	How we addressed this section
Improving understanding of Technology	Helping others realize the importance of cyber-attacks on critical infrastructures.	improve the understanding by individuals and society of the capabilities of conventional and emerging technologies	We address this by having our project simulate a real environment that will work as a visual aid to assist students as a tool.
Maintaining and Improving Technical Competence	Growing our skills and development of network and connected systems. Performing tasks that we can handle competently.	maintain and improve our technical competence and to undertake technological tasks for others	Each team member has knowledge in their respective areas. Other team members teach each other specifics they may not understand when needed.
Honesty and Proper Attribution	Being accurate as possible to our system's capabilities and limitations. Giving credit to data/information provided to us by other sources (logs for training).	be honest and realistic in stating claims or estimates based on available data, and to credit properly the contributions of others	Our design aims to target AI accuracy to a stable point. Citing proper resources used in our system and reporting proper team contributions.
Supporting Colleagues in following the Code	Helping each other to act respectfully, contribute equally, and align our decisions with good engineering practices.	Support colleagues and co-workers in following this code of ethics, to strive to ensure the code is upheld, and to not retaliate against	During our sprint meetings we have open discussions and topic issues being addressed weekly. We also have a way to report

		individuals reporting a violation.	problems we may have with team members. We have code reviews over others' work.

Our team performs well at Improving the understanding of technology with this project. In specific we are all learning a lot while developing further progress on the project. Our project also is to achieve this, so we have been working hard to make sure that this goal gets achieved with our end product. We have developed a prototype already that can display the effects on a singular model but the approach we are taking in our description helps us achieve broadening knowledge to others. The strong performance is indicated by our problem statement's goal, and the progress we have made to develop the product.

We need to improve maintaining and improving technical competence. Our team has different majors with different experience and skills, so our expertise's are separate from one another. This sometimes leads to confusion when we attempt to merge our achievements as not all of us are in full understanding of other sections. Progress has been made on both sides, but the communication between our AI and the raspberry PI has been a problem. To improve, we just need more time to communicate and work together to have a fully integrated system with all its components. Time spent learning other peoples areas, like learning about the circuits for the Cyber's, and learning about the python program talking to the raspberry pi, would solve this very easily.

7.2 Four Principles

Create a table with rows for each broader context area (see Section 4.1.1) and columns for each of the four principles (beneficence, nonmalificence, respect for autonomy, and justice; see Beauchamp, 2007). Within the table, identify at least one way each of the four principles applies to each of the broader context areas. Some principle-broader context connections might be more prominent than others, but you should be able to identify something for each table cell. Note: Your design may end up negative or neutral in some cell. For example, your product might perform poorly in environment-nonmaleficence because it utilizes natural resources without a positive/mitigating effect.

Area	Beneficence	Nonmalificence	Respect for Autonomy	Justice
Public health, safety, and welfare	Our project raises cybersecurity awareness and preparedness related to critical infrastructure systems.	Bad actors in other countries can use our research to find loopholes or create malicious software to get around MITRE attacks on critical infrastructure.	Users and educators maintain full control over how the network simulation and logs are used.	Our design promotes equal access to cybersecurity education by providing a low cost learning tool for all students.

Global, cultural, and social	With the recent prominence of cyber-attacks on critical infrastructure such as in Ukraine, our project promotes awareness of the importance of cybersecurity to the public and students going into relevant fields.	Bad actors in other counties can use our research to find loopholes or create malicious software to get around MITRE attacks on critical infrastructure.	Instructors and students can independently select which attack scenarios, log sets, and system behaviors they want to focus on, giving them control over how the simulation supports their learning objectives.	By offering a tool that is low cost and not platform reliant, we support broad education equity across cultures, communities, and institutions.
Environmental	We're offering digital versions of our project, so new models do not have to be printed. This saves materials and helps the environment while spreading cybersecurity awareness.	Our project slightly harms the environment due to energy consumption; however, the 3D prints for our model buildings are relatively small, and we offer an online version of our simulation.	Users can choose between physical or digital simulations, allowing autonomy in selecting lower impact environmental options.	By minimizing unnecessary material use, we distribute environmental costs more reasonably compared to similar interactive learning tools.
Economic	Our project promotes future growth in cybersecurity in critical infrastructure.	Our project relates to nonmalificence in an economic context in that it is a cost-effective tool that teaches students going into critical infrastructure fields about the importance of cybersecurity, thus protecting	Users and educators decide how extensively they invest in hardware, allowing the project to scale with a wide range of budgets	By keeping the system affordable and modular, we help ensure that institutions with fewer resources still gain access to cybersecurity education tools.

		valuable economic assets.		

A key broader context principle pair that is important to our project is Public health, safety, and welfare x Beneficence. GridSAFE is designed to strengthen awareness of cybersecurity vulnerabilities in critical infrastructure, which directly contributes to protecting essential services such as energy, water, and transportation. By teaching students and future professionals how cyberattacks unfold and how detection systems respond, the project supports a safer and more resilient society. We ensure this benefit by grounding our simulation in real ATT&CK techniques, validating our prototype through iterative testing, and emphasizing accurate, responsible representations of cyber events.

A key broader context principle pair that is currently lacking is Global, cultural, and social x Nonmaleficence. Although the system is intended for education, the same information could theoretically be used to inform malicious activity if taken out of context. While this risk is outweighed by the strong positive impacts in public safety, economic resilience, and equitable access to cybersecurity education, it remains a meaningful concern. To improve in this area, our team must be intentional about what technical details we make publicly accessible and focus project documentation on defensive strategies rather than exploit mechanisms, ensuring the education value remains strong while minimizing unintended harm.

Below the table, note one broader context-principle pair that is important to your project. Briefly describe the benefit in that area you are working towards and how you will ensure it. Also note one broader context-principle pair in which your project/end design is or will be lacking. Describe either (a) how this negative is overcome by other positives in other areas of the project/design or (b) what your team must do to improve in this area.

7.3 VIRTUES

1. Communication

- Communication is the commitment to working together, sharing knowledge, and supporting each other to achieve a unified solution.
- The GridSAFE team reinforces communication through active collaboration on our Discord server, where we provide frequent progress updates, ask questions, share files, and coordinate tasks. This ensures that both software and hardware teams stay aligned as the project evolves.

2. Integrity

- Integrity is the commitment to upholding a strong ethical code in all aspects of our work.
- The GridSAFE team reinforces integrity through a strict adherence to the Iowa State University Academic Code of Conduct and the IEEE Code of Ethics. We prioritize honest reporting, accurate data representation, and transparent decision making throughout the development lifecycle.

3. Accountability

- Responsibility is the commitment to be accountable for work that has been completed or will be completed

- The GridSAFE team reinforces accountability through weekly meetings where we openly discuss progress, challenges, and next steps. We routinely pair software and hardware members to align interfaces, review each other's work, and ensure that both sides of the system integrate smoothly. We also use shared documentation and version-control tools to keep everyone synchronized.

Jason

Leadership is important to me because it ensures that the team stays organized, aligned, and able to move forward even when the project becomes complex. I want to contribute stability and direction, especially when our work spans multiple subsystems and requires coordinated decision making. I have demonstrated leadership by helping guide the software direction of GridSAFE, proposing workflows for anomaly detection, and taking initiative during team meetings to clarify tasks, dependencies, and integration steps. I also support teammates by answering questions, outlining next steps for the AI component, and keeping our progress aligned with project milestones.

Precision is important to me because GridSAFE relies on accurate data processing, correct model behavior, and clean integration between hardware and software. Small errors in logs, parameters, or output mapping can produce incorrect anomaly signals, so careful attention to detail is critical. I hope to demonstrate Precision by improving the structure and clarity of my code, documenting model parameters more thoroughly, and verifying that all inputs and outputs behave consistently across the system. I will also incorporate more rigorous testing and review processes to ensure that my contributions meet the accuracy and reliability the project requires.

Nellie

I have demonstrated the virtues of leadership and accountability throughout our senior design project. I organize our weekly meetings, lead the discussions, and create summaries and "do next" action items, so the team always has structure and direction. I also take responsibility for communicating with our advisor and reaching out to ETG or other external groups whenever we need outside support. This virtue is important to me because every project—especially a student-run one—needs consistent structure to stay on track. I help reinforce that structure by checking in with team members on Discord, making sure everyone has what they need to meet their weekly goals and ensuring that progress stays steady.

A virtue that is important to me but that I may not have fully demonstrated in this project is patience. This virtue matters to me because technical projects rarely go perfectly, and maintaining patience with myself and my teammates helps create a more positive and productive environment. To demonstrate this virtue moving forward, I plan to slow down during problem-solving discussions to make sure every voice is heard, give teammates more room to work through challenges before stepping in, and approach setbacks with a calmer, more constructive mindset.

Evan

One virtue I have demonstrated on the project so far is responsibility throughout our senior design project. I have mostly overseen modeling and modifying the 3D structures for our model city. I have also worked closely with project leaders and other project members to ensure that project milestones are met on time. I have also been responsible for helping other group members who are

willing to help with modeling work to learn how to use the modeling program that we have been using to model our 3D structures. Responsibility is important to me because some parts of a project may be solely the responsibility of a single person or a small number of people. In cases like this, one person may be the deciding factor on whether project deadlines are met or not.

One virtue that is important to me, but I have not demonstrated throughout our senior design project is leadership. Leadership is important to me because good leadership can be what makes a project succeed or fail. Good leadership can motivate a team to work hard to meet expectations. I have not demonstrated leadership on our senior design project because I have not been in a leadership role on the project or had many opportunities to display leadership.

Kyle

A virtue that I have demonstrated during this project is perseverance while designing and implementing different features. This virtue is important to me because I believe it is one of the most important things when it comes to software engineering. Software will rarely work perfectly the first time, and it requires thinking through the problem and working on it until it's done, which can be extremely frustrating at times. During this project I have demonstrated perseverance by pushing through technical challenges while developing our machine learning model and integrating it with the front-end UI. There were various issues that occurred such as not preparing training data properly and not being able to communicate with the backend server. I had to stay patient and troubleshoot each issue until I could figure out what was wrong and fix it.

A virtue that is important to me that I haven't demonstrated as well as I would like to during this project is dependability. This is important to me because being a person that others can count on is essential in many settings. In team projects such as this, everyone relies on the others in their group to follow through on commitments and maintain steady progress. I want to improve in this area by managing my time better and being more consistent with my contributions so that the rest of my group can rely on me throughout the project. I will keep better track of what I need to do each week and try to stick to a schedule to accomplish my goals and contribute reliably.

Brant

One virtue that I have demonstrated throughout the Senior Design coursework is Reliability. It's important to be reliable so that your teammates have someone to turn to if they need assistance. To assist in completing essential deadlines for hardware and software, I was able to assist both sides of our teams to achieve a product that we can display proudly for one semester of work. I also had some knowledge I was able to give to the team that helped us progress even faster for the hardware to end. Knowing how to create, splice, and edit files in fusion 360 and knowing what software to use definitely boosts our efficiency to get physical models.

One virtue that is important, but I don't demonstrate, is creativity. Creativity can be a necessity in many projects and is important to me because it's something I often lack. Many software and hardware diagrams take creativity and imagination to develop something that can be put into practice and use, so it's important for development and progress in the early moments. To demonstrate this, I could be more apart of some of the designs, and we still have parts of the network that need to be made so we can have mocked connections with security onion and other software. I will attempt to take more steps towards development theories and then when I put them into practice over the break, I will have a better idea of what I am do.

8 Closing Material

8.1 Conclusion

Up to this point, our team has progressed through every major stage of the development process in our first semester goals: selecting hardware, creating the initial 3D models, completing multiple 3D printing iterations, researching and choosing appropriate LEDs, researching the Raspberry Pi, writing the necessary Pi scripts, connecting the Pi to the LEDs, designing the prototype baseboard schematic, printing the baseboard, assembling the prototype, and testing the completed system. In parallel with this hardware progress, the software team worked with an existing dataset of HDFS logs and used these logs to build an early prototype of our anomaly detection model. This allowed us to begin forming the initial pieces of the software pipeline even before full system integration. Our first semester goal has been to create a functional, hardware, and software integrated prototype that combines LEDs and Raspberry Pi into one design. The most effective plan for

meeting this goal has been parallel development. Allowing the hardware side to have an iterative approach in researching the 3D models, designing them, testing them and then finally refining before moving on to coding the connection between the software and hardware. This same parallel structure allowed the software team to experiment with the prototype model, test its output, and prepare simple communication steps that help it connect to the Raspberry PI. Along the way, we encountered constraints such as long print times, limited availability of 3D printers, and shipping time for components. In future iterations, these challenges could be reduced through more communication of model requirements.

8.2 References

[1] "3D Printing Materials Guide." LulzBot. Available: https://lulzbot.com/content/3d-printing-materials-guide (accessed Dec. 7, 2025). LulzBot

[2] "Skyscraper Chess Set." Printables. Available: https://www.printables.com/model/20297-skyscraper-chess-set (accessed Dec. 7, 2025).

[3] "Raspberry Pi Tutorial: How to Use a RGB LED." Instructables. Available: https://www.instructables.com/Raspberry-Pi-Tutorial-How-to-Use-a-RGB-LED/ (accessed Dec. 7, 2025). Instructables

[4] "Using a RPi to Control an RGB LED." Instructables. Available: https://www.instructables.com/Using-a-RPi-to-Control-an-RGB-LED/ (accessed Dec. 7, 2025). Instructables

[5] "Raspberry Pi 4 Model B." Raspberry Pi. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/ (accessed Dec. 7, 2025). Raspberry Pi

[6] "Getting Started – Raspberry Pi Documentation." Raspberry Pi. Available: https://www.raspberrypi.com/documentation/computers/getting-started.html (accessed Dec. 7, 2025). Raspberry Pi

[7] "Tutorial: How to Control a LED-Strip With a Raspberry Pi | EN+DE." Dordnung+1. Available: https://dordnung.de/raspberrypi-ledstrip/ (accessed Dec. 7, 2025). Dordnung+1

[8] "Securing the U.S. electricity grid from cyberattacks." GAO. Available: https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks (accessed Dec. 7, 2025). GAO

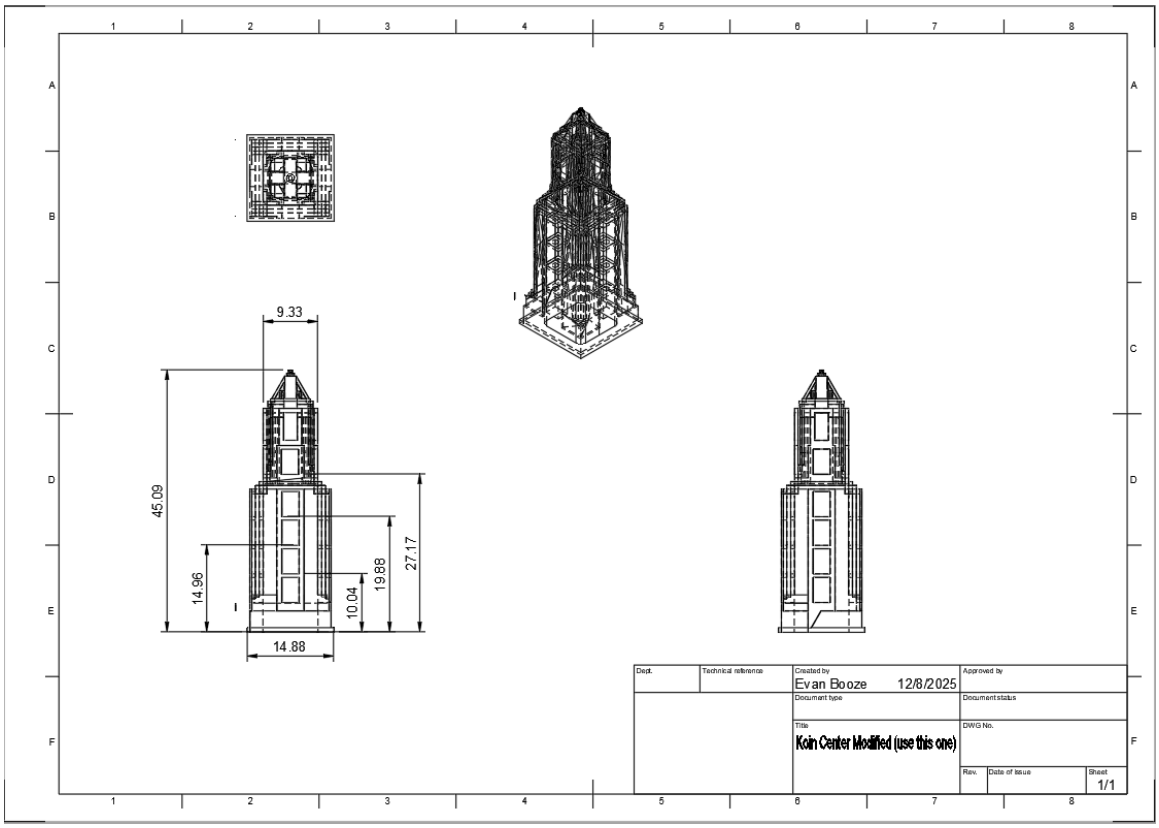
[9] "Reliability Standards." NERC. Available: https://www.nerc.com/pa/Stand/Pages/Default.aspx (accessed Dec. 7, 2025). NERC

[10] "Identify anomalies with Anomaly Detector." Microsoft. Available: https://learn.microsoft.com/en-us/azure/ai-services/anomaly-detector/how-to/identify-anomalies (accessed Dec. 7, 2025). Microsoft

[11] "MITRE ATT&CK Framework." MITRE. Available: https://attack.mitre.org/ (accessed Dec. 7, 2025). MITRE

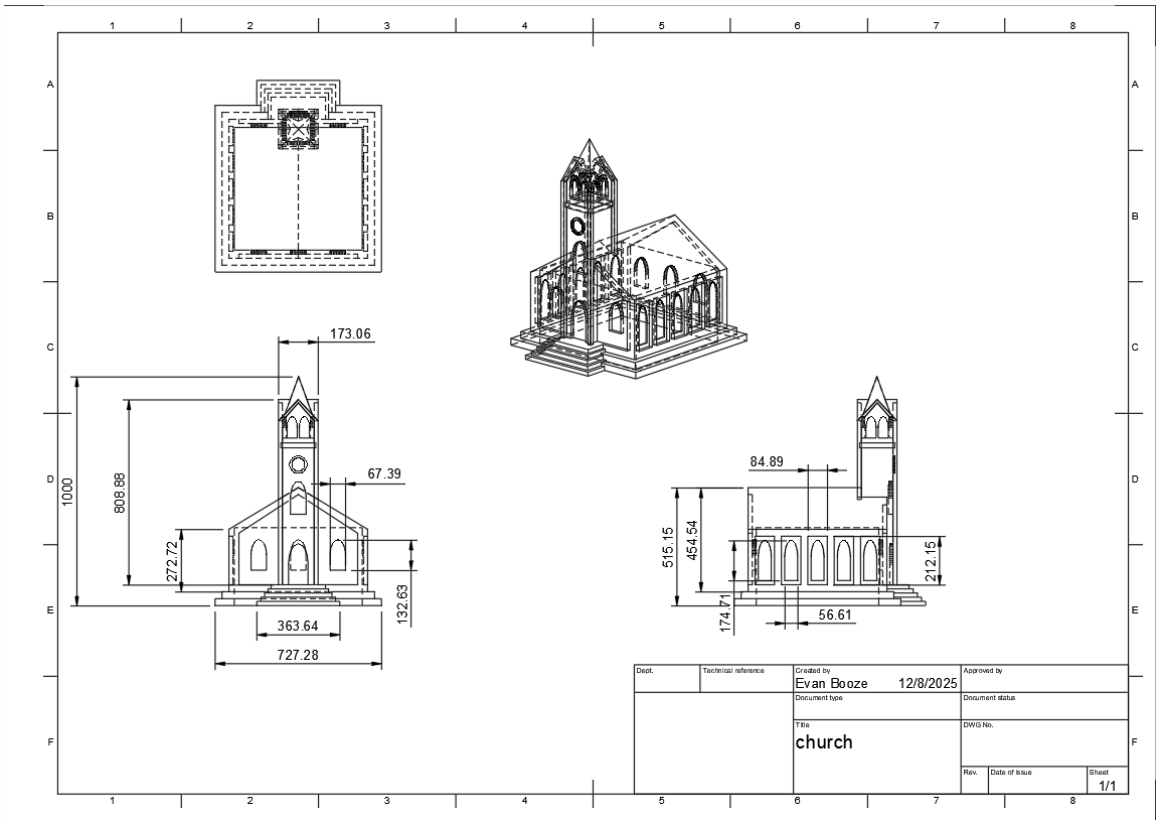
[12] “LogAI example datasets.” Salesforce. Available: https://github.com/salesforce/logai/tree/main/examples/datasets (accessed Dec. 7, 2025). Salesforce

8.3 APPENDICES



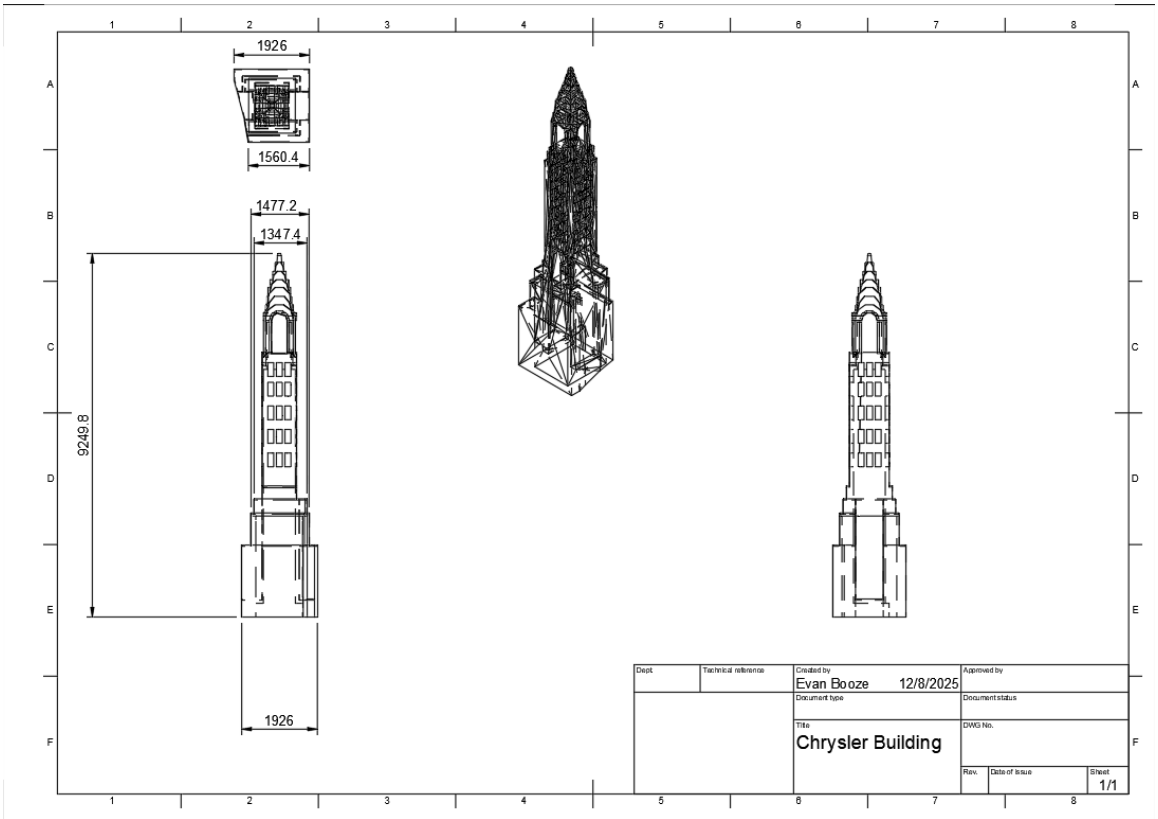
Link to view drawing: https://a360.co/44WjIE3

Note: Dimensions not to scale with final structure



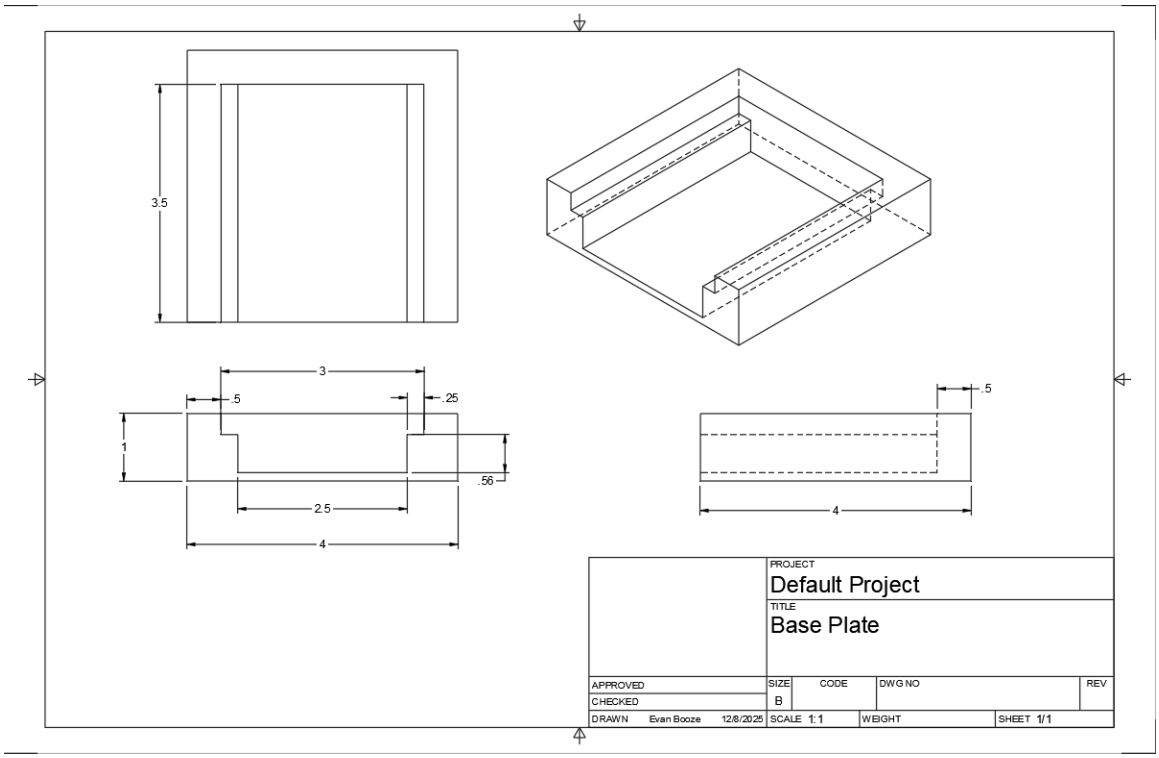
Link to view drawing: https://a360.co/4pssz8S

Note: Dimensions not to scale with final structure



Link to view drawing: https://a360.co/4a2FoSp

Note: Dimensions not to scale with final structure



Link to view drawing: https://a360.co/48XSq2v

9 Team

9.1 Team Members

Nellie Leaverton, Jason Di Giovani, Evan Booze, Brant Gicante, Kyle Maloney, Anthony Nehring

9.2 Required Skill Sets for Your Project

Skills Required
3D Printing
Lazer Cutting
Engineering Schematics
Wood Working
Python Coding
Basic Circuit Design knowledge (201)
JSON Coding
Soldering + PCB Design
EMBEDDED SYSTEMS Knowledge (Hardware integration with software)
CAD SOFTWARE
Networking Fundamentals
API Development/HTTP(S) Communication
Machine Learning Fundamentals
Anomaly Detection Fundamentals
Data Parsing and Log Handling
Technical Writing/Communication

9.3 Skill Sets covered by the Team

Skills Required	Names
3D Printing	Nellie, Evan, Brant
Lazer Cutting	Nellie, Evan, Brant
Engineering Schematics	Jason, Nellie
Wood Working	Nellie, Evan, Brant
Python Coding	Jason, Kyle, Brant, Anthony
Basic Circuit Design knowledge (201)	Nellie, Evan
JSON Coding	Jason, Kyle, Anthony, Brant
Soldering + PCB Design	Nellie, Evan, Brant
EMBEDDED SYSTEMS Knowledge (Hardware integration with software)	Nellie, Kyle, Jason, Kyle, Anthony, Brant
CAD SOFTWARE	Brant, Nellie, Evan
Networking Fundamentals	Jason, Brant, Kyle

API Development/HTTP(S) Communication	Jason, Kyle
Machine Learning Fundamentals	Jason, Kyle
Anomaly Detection Fundamentals	Jason, Kyle
Data Parsing and Log Handling	Jason, Brant, Kyle
Technical Writing/Communication	Jason

9.4 Project Management Style Adopted by the team

The GridSAFE team uses an Agile project management style. Our work is organized into short, iterative development cycles that allow the team to adapt as the project evolves. We hold weekly meetings to review completed tasks, evaluate any issues, and plan upcoming work. These meetings function as regular checkpoints to ensure alignment between the software and hardware teams and to maintain consistent progress toward our milestones.

Agile supports continuous improvement, frequent communication, and flexibility in task assignment, all of which are necessary for a project that integrates multiple components such as the virtual network, anomaly detection AI, and Raspberry PI visualization system. This approach enables the team to refine requirements, adjust priorities, and respond quickly to feedback throughout the development process.

9.5 Initial Project Management Roles

Nellie Leaverton – Hardware & Architectural Design Lead

Jason Di Giovanni – Software and Security Lead

Brant Gicante – Software and Security Assistant

Evan Booze – Hardware & Architectural Design Assistant

Kyle Maloney – Testing Lead & Design Assistant

Anthony Nehring – Software and Security Assistant

9.6 Team Contract

Team Members:

1) Anthony Nehring_____ 2) Jason Di Giovanni_____

3) Brant Gicante_____ 4) Kyle Maloney_____

5) Nellie Leaverton_____ 6) Evan Booze_____

Team Procedures

1. Day, time, and location (face-to-face or virtual) for regular team meetings:

   Regular team meetings will be held on Thursdays from 2:30 – 3:30 PM (with the possibility of adjusting to a later time if needed). Attendance is required for all members, but remote participation will be available if a member cannot attend in person.

   Acceptable reasons for absence include illness, family emergencies, or conflicts with academic obligations such as exams. Unacceptable reasons include lack of motivation or simply "not feeling like it,". Members are expected to notify the group in advance if they will be absent or attending remotely.

   Meetings with the project advisor, Dr. Julie Rursch, will be scheduled every few weeks (date and time TBD). While attendance is not mandatory for all members, it is highly recommended that at least one of the co-proposers be present.

2. Preferred method of communication updates, reminders, issues, and scheduling (e.g., e-mail, phone, app, face-to-face):

   The team's primary method of communication will be Discord, which will be used for updates, reminders, quick messaging, online meetings, and general coordination.

3. Decision-making policy (e.g., consensus, majority vote):

   The team will make decisions based on consensus. If a consensus cannot be reached after thorough discussion, guidance may be sought from the project advisor, Dr. Julie Rursch.

4. Procedures for record keeping (i.e., who will keep meeting minutes, how will minutes be shared/archived):

   A shared **Google Drive** folder will be maintained as the central repository for all meeting notes and project documentation.

   - For **full group meetings**, Nellie will serve as the primary recorder, documenting meetings. If Nellie is unable to attend, the responsibility will be passed along to another group member.
   - For **smaller group meetings**, one member from each subgroup will be designated to record notes and upload them to the shared folder.

Participation Expectations

1. Expected individual attendance, punctuality, and participation at all team meetings:

All team members are expected to attend scheduled meetings and arrive on time to show respect for the group's time and maintain steady progress on the project. Active participation during meetings is required, which includes contributing ideas, providing updates on assigned tasks, and engaging in group discussions.

If a member is unable to attend a meeting due to illness, family obligations, or academic conflicts, they are responsible for catching up on all information discussed. This may involve reviewing the meeting minutes, following up with teammates, or, if necessary, scheduling a brief follow-up meeting to ensure they remain aligned with the group.

2. Expected level of responsibility for fulfilling team assignments, timelines, and deadlines:

All team members are expected to take ownership of their assigned tasks and complete them in a timely manner. To support accountability and progress, the team will establish **weekly milestones** to check in on individual contributions and ensure deadlines are being met.

A **Trello board** will be used to organize tasks, assign responsibilities, track progress, and visualize timelines for the project.

3. Expected level of communication with other team members:

Team members are expected to maintain **consistent and proactive communication** with the group. This includes:

- Notifying the team in advance if you need to miss a meeting or will be unable to complete an assigned task on time.
- Regularly checking **Discord** to stay updated on messages, announcements, deadlines, and project discussions.
- Promptly responding to questions, requests for input, or clarifications from teammates if prompted.

4. Expected level of commitment to team decisions and tasks:

All team members are expected to demonstrate a strong commitment to the team's decisions, goals, and assigned tasks. This includes:

- Staying motivated to work collaboratively toward the **common project goal**.
- Following through on agreed-upon responsibilities and contributing consistently to the team's progress.
- Supporting team decisions even if personal preferences differ, while still providing constructive input during discussions.
- Demonstrating reliability and accountability, ensuring that all tasks are completed with quality and on time.

Leadership

1. Leadership roles for each team member (e.g., team organization, client interaction, individual component design, testing, etc.):

   Client Interaction: Nellie
   Team Organization: Nellie
   Component Design: Nellie (Physical) Jason (Software)
   Testing: Kyle

2. Strategies for supporting and guiding the work of all team members:

   The team will use **weekly meetings and milestone check-ins** to guide progress and ensure that all members stay on track with their assigned tasks. **Discord** will serve as the primary tool for ongoing communication, allowing team members to ask questions, share updates, and coordinate with each other and with Dr. Julie Rursch as needed.

3. Strategies for recognizing the contributions of all team members:

   The team will dedicate time during **weekly meetings** to review work completed by each member and share the progress made.

Collaboration and Inclusion

1. Describe the skills, expertise, and unique perspectives each team member brings to the team.

   Brant brings decent knowledge on 3d printing and filament knowledge such as TPU vs PLU, as well as cad and fusion 360 experience. I also have a great perspective on some cyber knowledge going into my final few semesters within the CybE major, and have enough coding, and AWS bucket experience to assist in the software development adequately.

   Jason brings prior experience with log generation and analysis, as well as base level experience with AWS and locally hosted AI. I'm also confident in my general cyber knowledge as a CybE major.

   Nellie brings decent knowlege of electrical systems, including knowledge of power plants as well as an understanding of how the City of Light should function. She can contribute practical hands-on skills such as 3D CAD design and soldering.

   Anthony: CYBE senior, Cyber intelligence analyst, junior level experience with both network and host analyst positions. I am very interested in red team / cyber threat emulation work. Worked frontend for 309, comfortable with python, java, C, with beginner level capabilities in assembly (CPRE381 and CYBE536 – currently taking). Competent with using Linux and working on the same level with windows.

   Kyle is a software engineer with strong experience in cybersecurity. He has worked with Python for years building tools and applications and has practice training AI models. He also has experience using AWS for development and data management.

Evan understands the basics of circuit design, power plants, and the electrical grid. Evan has moderate experience with circuit design software such as LTspice, and power simulation tools such as PSCAD. Evan also has limited experience using MATLAB.

2. Strategies for encouraging and supporting contributions and ideas from all team members:

Brant's strategy to motivate other team members to support contribution to the work is to remind them how cool applicable the assignment will be for themselves. Everyone needs a project to say they did something, and this is a great opportunity for them to excel and show they have great teamwork in a professional setting.

Jason's strategy to motivate other team members is to always be available if team members are struggling to get work done, so we can resolve issues quickly. I'll also encourage everyone to pause before moving on in our meetings so if anyone has something to say they have a chance to add it instead of getting skipped.

Evan's strategy to encourage work and contributions to the project is to take an active role in working on the project, working closely with other team members and supporting their work on the project to the best of his ability. Evan will actively contribute to the best of his ability during regularly scheduled team meetings and will seek guidance and support from other team members should he face any setbacks or complications with his work on the project. Evan will also try to be as accommodating of other team members as possible to facilitate their work on the project.

Nellie's strategy to encourage contributions is to create an environment where every team member feels heard and valued. She actively invites input during discussions and makes sure to recognize the unique strengths each person brings to the project. By asking thoughtful questions and showing genuine interest in others' perspectives, Nellie helps spark new ideas and ensures collaboration stays inclusive. She also emphasizes clear communication and accountability, so team members feel confident that their efforts directly contribute to the success of the project.

Anthony's strategy to encourage work and contribuation to the project is by always keeping an upbeat attitude and making sure everyone is getting the help they need and maintaining a good pace for completion. Anthony will be open to communicating and be there for other group members when they are stressed. He will also be making sure to keep the group updated and making sure everyone is updating the group on if they are making deadlines / if they need extra help.

Kyle's strategy is to try and encourage those with ideas to build on them if there seems to be any potential. Taking an idea that someone has and trying to incorporate into our design in a meaningful way would be a great way to get everyone in this project to want to be more involved and give more suggestions. This also would mean being openly critical of everyone's ideas so we can have a discussion and really figuring out if an idea will truly work for the design we have in mind or if it's worth changing something.

3. Procedures for identifying and resolving collaboration or inclusion issues (e.g., how will a team member inform the team that the team environment is obstructing their opportunity or ability to contribute?)

   For **minor issues**, members are encouraged to bring them up directly in **Discord** or during a team meeting, allowing the group to address the concern promptly and collaboratively.

   For **more significant issues**, team members should reach out to **Jason or Nellie**, who will help mediate the situation and work with the team to find a resolution.

   If the issue **cannot be addressed within the team**, members may escalate the concern to **Dr. Fila or Dr. Rover** to ensure it is properly handled.

Goal-Setting, Planning, and Execution

1. Team goals for this semester:

   The primary goal for the semester is to develop a small-scale prototype board that can simulate attacks on a power grid.

2. Strategies for planning and assigning individual and team work:

   The team will break the project into **manageable milestones**. As well as work will be assigned to individual team members based on their skills, expertise, and current workload to ensure that responsibilities are balanced and no one is overloaded.

3. Strategies for keeping on task:

   The team will maintain focus and progress through a combination of **regular updates, meetings, and resource management**.

   - **Regular check-ins with Dr. Julie Rursch** will provide guidance, feedback, and accountability.
   - **Nellie will communicate with ISEAGE** to clarify what resources and support are available, including funding or materials.
   - Weekly milestones and Trello task tracking will also help the team monitor progress and stay organized.

Consequences for Not Adhering to Team Contract

1. How will you handle infractions of any of the obligations of this team contract?

   If a team member fails to meet the obligations outlined in this contract, the team will address the issue promptly and constructively.

- For **first-time or minor infractions**, the team will discuss the concern directly with the member to clarify expectations and provide an opportunity to correct the behavior.
- If **infractions occur more than once**, a designated team member (Nellie or Jason) will reach out to the individual to address the issue more formally and work toward a resolution.

2. What will your team do if the infractions continue?

   Persistent or unresolved issues may be escalated to the Senior Design Advisor's, Dr. Rover and Dr. Fila, to ensure the team can maintain a productive and collaborative environment.

****

a) *I participated in formulating the standards, roles, and procedures as stated in this contract.*

b) *I understand that I am obligated to abide by these terms and conditions.*

c) *I understand that if I do not abide by these terms and conditions, I will suffer the consequences as stated in this contract.*

1) Evan Booze_____DATE 9/15/2025 _____

2) Anthony Nehring_____ DATE 9/15/2025 _____

3) Jason Di Giovanni_____ DATE 9/15/2025 _____

4) Brant Gicante_____ DATE 9/15/2025_____

5) Nellie Leaverton_____ DATE 9/15/2025_____

6) Kyle Maloney _____ DATE 9/15/2025_____

7) _____ DATE _____

8) _____ DATE _____