



Development Standards & Practices Used

List all standard circuit, hardware, software practices used in this project. List all the Engineering standards that apply to this project that were considered.

Summary of Requirements

List all requirements as bullet points in brief.

Applicable Courses from Iowa State University Curriculum

List all Iowa State University courses whose contents were applicable to your project.

New Skills/Knowledge acquired that was not taught in courses

List all new skills/knowledge that your team acquired which was not part of your Iowa State curriculum in order to complete this project.

Table of Contents

[1](#_heading=h.1v1yuxt) Team 5

[1.1](#_heading=h.4f1mdlm) Team Members 5

[1.2](#_heading=h.2u6wntf) Required Skill Sets for Your Project 5

[(if feasible – tie them to the requirements) 5](#_heading=h.19c6y18)

[1.3](#_heading=h.3tbugp1) Skill Sets covered by the Team 5

[(for each skill, state which team member(s) cover it) 5](#_heading=h.28h4qwu)

[1.4](#_heading=h.nmf14n) Project Management Style Adopted by the team 5

[1.5](#_heading=h.37m2jsg) Initial Project Management Roles 5

[2](#_heading=h.1mrcu09) Introduction 5

[2.1](#_heading=h.46r0co2) Problem Statement 5

[2.2 Requirements & Constraints 5](#_heading=h.2lwamvv)

[2.3](#_heading=h.111kx3o) Engineering Standards 5

[2.4 Intended Users and Uses 6](#_heading=h.3l18frh)

[3 Project Plan 6](#_heading=h.206ipza)

[3.1 Project Management/Tracking Procedures 6](#_heading=h.4k668n3)

[3.2 Task Decomposition 6](#_heading=h.2zbgiuw)

[3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria 6](#_heading=h.1egqt2p)

[3.4 Project Timeline/Schedule 6](#_heading=h.3ygebqi)

[3.5 Risks And Risk Management/Mitigation 7](#_heading=h.2dlolyb)

[3.6 Personnel Effort Requirements 7](#_heading=h.sqyw64)

[3.7 Other Resource Requirements 7](#_heading=h.3cqmetx)

[4 Design 8](#_heading=h.1rvwp1q)

[4.1 Design Context 8](#_heading=h.4bvk7pj)

[4.1.1 Broader Context 8](#_heading=h.2r0uhxc)

[4.1.2 User Needs 8](#_heading=h.1664s55)

[4.1.3 Prior Work/Solutions 8](#_heading=h.3q5sasy)

[4.1.4 Technical Complexity 9](#_heading=h.25b2l0r)

[4.2 Design Exploration 9](#_heading=h.kgcv8k)

[4.2.1 Design Decisions 9](#_heading=h.34g0dwd)

[4.2.2 Ideation 9](#_heading=h.1jlao46)

[4.2.3 Decision-Making and Trade-Off 9](#_heading=h.43ky6rz)

[4.3](#_heading=h.2iq8gzs) Proposed Design 9

[4.3.1 Design Visual and Description 10](#_heading=h.xvir7l)

[4.3.2 Functionality 10](#_heading=h.3hv69ve)

[4.3.3 Areas of Concern and Development 10](#_heading=h.1x0gk37)

[4.4 Technology Considerations 10](#_heading=h.4h042r0)

[4.5 Design Analysis 10](#_heading=h.2w5ecyt)

[4.6](#_heading=h.1baon6m) Design Plan 10

[5 Testing 11](#_heading=h.3vac5uf)

[5.1 Unit Testing 11](#_heading=h.2afmg28)

[5.2 Interface Testing 11](#_heading=h.pkwqa1)

[5.3](#_heading=h.39kk8xu) Integration Testing 11

[5.4](#_heading=h.1opuj5n) System Testing 11

[5.5](#_heading=h.48pi1tg) Regression Testing 11

[5.6](#_heading=h.2nusc19) Acceptance Testing 11

[5.7](#_heading=h.1302m92) Security Testing (if applicable) 11

[5.8](#_heading=h.3mzq4wv) Results 11

[6 Implementation 12](#_heading=h.2250f4o)

[7 Professionalism 12](#_heading=h.haapch)

[7.1](#_heading=h.319y80a) Areas of Responsibility 12

[7.2 Project Specific Professional Responsibility Areas 12](#_heading=h.1gf8i83)

[7.3 Most Applicable Professional Responsibility Area 12](#_heading=h.40ew0vw)

[8 Closing Material 12](#_heading=h.2fk6b3p)

[8.1 Discussion 12](#_heading=h.upglbi)

[8.2 Conclusion 12](#_heading=h.3ep43zb)

[8.3 References 13](#_heading=h.1tuee74)

[8.4 Appendices 13](#_heading=h.4du1wux)

[8.4.1 Team Contract 13](#_heading=h.2szc72q)

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

# Team

* 1. Team Members
	Zach Hirst

Justin Templeton

Thomas Keeshan

Tyler Atkinson

Kaya Zdan

Matthew Nevin

* 1. Required Skill Sets for Your Project

Coding proficiency

Power grid analysis

Power grid creation

Analysis of cyber attacks

Generation of cyber attacks

Web Development (frontend and backend)

Communication

* 1. Skill Sets Covered by the Team

Coding proficiency (All)

Power grid analysis (Matthew, Thomas)

Powergrid creation (Matthew, Thomas)

Analysis of cyber attacks (Kaya, Tyler, Zachary, Justin)

Generation of cyber attacks (Kaya, Tyler, Zachary, Justin)

Web Development (frontend and backend) (Kaya, Tyler, Zachary, Justin)

Communication (All)

* 1. Project Management Style Adopted by the team

Agile - Scrum (sprint based)

* 1. Initial Project Management Roles

Tyler - Scrum Master

Kaya - Webdev Manager

Zachary - Cyber Attack Simulation Manager

Justin - Cyber Attack Generation Manager

Matthew - Powergrid Analysis Manager

Thomas - Powergrid Creation Manager

# Introduction

* 1. Problem Statement

Cyber attacks against the power grid are a growing concern.

* 1. Requirments & Constraints

Use CyHelics to combine multiple substream programs and run concurrently (functional)

Include both power grid model analysis and cyber security-focused programs

The simulation will be capable of handling multiple attack simulations, based on the OWASP top 10. (functional)

Create a power grid with several transmission models that connect with several distribution models and demonstrate proper power flow. (functional)

Power Grid will include multiple load types. (functional)

The power grid interface will be able to simulate different grid set ups (functional)

The interface must be easy to use for non technical users. (non-functional)

The simulation will be tested in a VM environment. (functional, maintenance)

The user must be able to select how much of the grid they want to simulate an outage for, with specialized attacks for each one. (non-functional)

The simulation will be integrated with cyber defense products such as Security Onion. (functional)

The simulation will be set up in a dockerized environment. (functional)

* 1. Engineering Standards

Helics and pandapower uses an open source BSD-3 clause license.

OpenDSS is open source, no listed license.

MITRE ATT&CK Framework is an industry standard knowledge base for use in pentesting, gap assessments, threat intelligence/hunting, and more.

OWASP Top 10 as a security guidance standard.

Python is an industry standard interpreted scripting language.

* 1. Intended Users and Uses

**Who benefits from the results of your project?**

The general population benefits from the project. It ensures that the companies running their power grid have substantial protection against attacks.

**Who cares that it exists?**

Power grid companies, city planners, maintenance companies, city politicians, city citizens, researchers.

**How will they use it?**

Find weaknesses, improve their grid, and Test future expansion

# Project Plan

* 1. Task Decomposition

Set up the VMs as a Dockerized environment

Set up and connect Helics with pandapower and OpenDSS

Create electric grid diagram

Analyze the power flow and design of models

Create smaller sections of the transmission and distribution grid

Co-Simulation between transmission and distribution models

Create a working simulation

Create a Kali/red team box that can perform attacks against the power grid

Set up security onion to defend against the attacks against the power grid

Frontend for attack modules



* 1. Project Management/Tracking Procedures

Agile Management Style

Allows for multiple adjustment periods to become acclimated with our software

Using the agile project management style allows for small parts of the project to be developed and tested continuously throughout the design process

Goals and tasks may become more advanced and in depth as we discover more in our project

Breaks our main tasks into smaller & more obtainable goals

We will use Gitlab to list tasks and track current progress

* 1. Project Proposed Milestones, Metrics, and Evaluation Criteria

**Preliminary Grid**

Simulate pre-existing transmission models

Simulate pre-existing distribution models

Simulate pre-existing load models

Both models co-simulate through the Helics software

**Grid Design**

Design several different transmission models

Transmission model demonstrates proper power flow

Several aspects can be analyzed such as power flow, faults, harmonics, and unbalanced power flow

Design several different distribution models

Distribution model supports a dynamic load

Can use linear and nonlinear models

Design a dynamic load profile

Load will simulate real world loads such as EV and neighborhoods

Load will increase and decrease based on data collected from real-world loads

**Simulation Set Up**

Dockerize each simulation in their own environment

**Attack Modules**

Set up Kali box to perform the attacks against the simulated grid

Create a frontend interface to easily perform attacks against the grid

**Defense**

Set up security onion to detect the attacks against the grid

Create automated defenses

Send logs to centralized database and write rules to detect problems

* 1. Project Timeline/Schedule

|  | **1/22-29** | **2/5-12** | **2/19-26** | **3/4-11** | **3/18-25** | **4/1-8** | **4/15-22** | **4/29-5/6** | **5/13-20** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Analyze pre existing transmission and distribution models** | Deliver by 1/29 |  |  |  |  |  |  |  |  |
| **Analyze the power flow and design of models** |  | Deliver by 2/12 |  |  |  |  |  |  |  |
| **Co-Simulation between transmission and distribution models** |  | Deliver by 2/12 |  |  |  |  |  |  |  |
| **Working simulation** |  |  |  | Deliver by 3/11 |  |  |  |  |  |
| **Set up VM and Dockerized Environments** | Deliver by 1/29 |  |  |  |  |  |  |  |  |
| **Create and run attacks** |  |  |  |  |  |  | Deliver by 4/22 |  |  |
| **Frontend for attack modules** |  |  |  |  |  |  |  |  | Deliver by 5/20 |
| **Integrating security onion** |  |  |  |  |  | Deliver by 4/8 |  |  |  |
| **Using security onion to detect the attacks** |  |  |  |  |  |  |  |  | Deliver by 5/20 |

* 1. Risks and Risk Management/Mitigation

**Losing our VMs and our progress** - 0.5 (moderate)

Mitigation: Create regular backups and VM snapshots

**Using too many resources** - 0.3 (low)

Mitigation: Being aware of our resources and making sure nothing runs out of hand

* 1. Personnel Effort Requirements

| Task | Justin Hrs | Kaya Hrs | Matt Hrs | Tommy Hrs | Tyler Hrs | Zach Hrs | Total Hrs |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Set up and connect Helics with pandapower and OpenDSS | 5 | 5 | 2 | 2 | 5 | 5 | 24 |
| Analyze the power flow and design of models | 0 | 0 | 5 | 5 | 0 | 0 | 10 |
| Create smaller sections of the transmission and distribution grid | 5 | 5 | 30 | 30 | 5 | 5 | 80 |
| Co-Simulation between transmission and distribution models | 2 | 2 | 2 | 2 | 2 | 2 | 12 |
| Create a working simulation | 20 | 20 | 10 | 10 | 20 | 20 | 100 |
| Create a Kali/red team box that can perform attacks against the power grid | 2 | 2 | 0 | 0 | 2 | 2 | 8 |
| Set up security onion to defend against the attacks against the power grid | 0 | 0 | 0 | 0 | 20 | 0 | 20 |
| Frontend for attack modules | 5 | 5 | 0 | 0 | 5 | 5 | 20 |

* 1. Other Resource Requirements

**High Performance Compute Cluster**

Used to perform analysis & testing on power grid designs

**Virtual Machines**

Kali Purple Box (Pen Testing)

Ubuntu & Windows HELICS/PandaPower/OpenDSS Hosts

Higher resource VM’s for Security Onion