Simulating the effect of cyber attacks on a Power Grid

Design Document

Sdmay23-02

Benjamin Blakely

Team Members

Jake Stanerson

Noah Peake

Cole Medgaarden

Conner Spainhower

Michael Gierek

Hrijul Balayar

https://sdmay23-02.sd.ece.iastate.edu

Executive Summary

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.

MITRE Framework:

The MITRE framework gives us a good overview of how industrial control systems can be vulnerable to specific types of attacks. These are specific standards from this framework that are related to our project:

Command & Control- by mimicking normal or expected traffic, it is possible for hackers to obtain access to your system within a network. Once they achieve administration privileges, they are then able to take control of the system, or in our case the power grid.

Privilege Escalation- after already achieving access to the system, attackers will then follow up by trying to obtain the highest level of privileges. By escalating their privileges to an administration level they could then have the ability to make permanent changes (i.e. delete user accounts, delete/transfer files, or upload malware to the servers) to a system.

Discovery- this tactic is used to gather information about a network or system, and is used as a means of reconnaissance. Attackers use this technique to obtain specific information about a network or system to find out if there are any potential vulnerabilities that could be exploited.

Credential Access- this is typically gathered through phishing attempts and is used to obtain user credentials and access at any means. Once a hacker is able to achieve access to some credentials and user access, they could then begin their mission to achieving higher privileges.

IEEE Standards:

IEEE 1547 & 2030 - Distributed energy resources interconnection & interoperability with electrical grid.

Summary of Requirements

Functional requirements:

- Program needs to output results of attacks: increased power consumption, blackout, etc.

- Shell environment to replicate real grid in code
- Run attacks individually or in large quantities on grid
- Initialize a functioning power grid to be tested on

Resource requirements:
- Github connection is reliable for submitting code
- Connectivity to PyCharm is reliable
- Panda Power implementation (modeling tool)
- Python scripts for Cyber Attacks (attack anomaly)
- Utilize make files to automate cyber attack process
- Other associated python libraries needing to be installed
- Being able to pull, push, & commit code from other team members
- Can be ran on basic laptops without need for expensive hardware / computers

Aesthetic requirements:
- The output should be able to be formed into different visual representations including: tables, charts and diagrams.
- Accessibility to be able to find and read the results provided from the project

Applicable Courses from Iowa State University Curriculum

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

- CybE - 230
- CybE - 234
- CybE - 331

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.

- Usage of PandaPower and its functions
- Usage of Pandas functions
- Basic knowledge of using Python
- Basic knowledge of power grids and power distribution strategies

Table of Contents

1 Team

1.1 TEAM MEMBERS

- Jake Stanerson
- Noah Peake
- Cole Medgaarden
- Michael Gierek
- Hrijul Balayar
- Conner Spainhower

1.2 REQUIRED SKILL SETS FOR YOUR PROJECT

- Knowledge of Cyber threats/risks
- Python Experience
- Power Grid Knowledge

1.3 SKILL SETS COVERED BY THE TEAM

- Python Experience: Jake Stanerson, Michael Gierek, Noah Peake, Cole Medgaarden, Hrijul Balayar, Conner Spainhower
- Knowledge of Cyber threats/risks: Cole Medgaarden, Noah Peake, Hrijul Balayar, Conner Spainhower
- Power Grid Knowledge: Jake Stanerson, Michael Gierek

1.4 PROJECT MANAGEMENT STYLE ADOPTED BY THE TEAM

- Linear progression of project tasks

1.5 INITIAL PROJECT MANAGEMENT ROLES

- Jake Stanerson: Developer/scripter
- Noah Peake: Developer/scripter
- Michael Gierek: Developer/Grid knowledge
- Conner Spainhower: Scripter/Threat analyzer
- Hrijul Balayar: Scripter/researcher
- Cole Megaarden: Scripter/recorder of progress

2 Introduction

2.1 Problem Statement

What problem is your project trying to solve? Use non-technical jargon as much as possible. You may find the Problem Statement Worksheet helpful.

Our project is aiming to show and simulate the potential risks and outcomes of different cyber attacks being exploited on an electrical power grid. Places like the City of Ames could use this information to help make their power grids more secure. These attacks can lead to an attacker to gain access to a workstation and then proceed to manipulate movement of power throughout the power grid. These threats are ongoing and can occur at any time if a hacker is able to infiltrate the system. It is important to prepare for these potential threats because serious damages could occur to a city's distribution of power and leave lasting results. Our project is to help show how power grid companies can see results of specific attacks and the outcome that results from these attacks.

2.2 Intended Users & Uses

Who will use the product you create? Who benefits from or will be affected by the results of your project? Who cares that it exists? List as many users or user groups as are relevant to your project. For each user or user group, describe (1) key characteristics (e.g., a persona), (2) need(s) related to the project (e.g., a POV/needs statement), and (3) how they might use or benefit from the product you create. Please include any user research documentation, empathy maps, or other artifacts as appendices.

Ideally the results of this project can be used by any electrical power grid company to simulate and help show and inform these companies how cyber attacks could threaten their networks. The engineers that work at these electrical power plants will benefit from the results of this project in support to help them become aware of these active threats. From the companies that run the power plants to every day consumers are the ones who should care about this, since nearly everyone requires electricity in day to day activities. The users relevant to this project are the power grid companies, average consumers of electricity, and the employees that work with the power grid.

-Power grid companies: These are the companies that supply the electricity to their designated consumers and contain distribution centers. Our project will supply this user with the need to be aware of the potential impacts that a cyber attack will incur on the system. They will benefit from this product by being able to better prepare for ongoing threats and how to prevent them from occurring.

-Everyday Consumers: These are the consumers of the distributed electricity from the power companies. Our project will supply these consumers with visual charts and statistics that will be viewable via the company's website. The consumers will benefit from this information and be able to feel more confident that their IOTs (Internet of Technologies) are more secure and protected from intrusion.

-Company Employees: Employees of a company with the ability to use the tool would be able to use it for vain purposes. Employees may need to check the current condition of the power grid, analyze how the results of the test change based on proposed changes to the power grid. This would allow for more detailed reports, letting those in the company make more educated decisions based on the risk and result of possible cyber attacks if they are successful.

2.3 REQUIREMENTS & CONSTRAINTS

List all requirements for your project. Separate your requirements by type, which may include functional requirements (specification), resource requirements, physical requirements, aesthetic requirements, user experiential requirements, economic/market requirements, environmental requirements, UI requirements, and any others relevant to your project. When a requirement is also a quantitative constraint, either separate it into a list of constraints, or annotate at the end of the requirement as “(constraint).” Ensure your requirements are realistic, specific, reflective or in support of user needs, and comprehensive.

This project’s intended use is for a power company that does not have access to any super computers and wants to observe potential results of attacks that could occur on their grid. These are the requirements that we have associated with the project.

Functional requirements:

- Program needs to output results of attacks
- Shell environment to replicate real grid in code
- Run attacks individually or in large quantities on grid
- Initialize a functioning power grid to be tested on

Resource requirements:

- Github connection is reliable for submitting code
- Connectivity to PyCharm is reliable
- Panda Power implementation (modeling tool)
- Python scripts for Cyber Attacks (attack anomaly)
- Utilize make files to automate cyber attack process

- Other associated python libraries needing to be installed
- Being able to pull, push, & commit code from other team members
- Can be ran on basic laptops without need for expensive hardware / computers

Aesthetic requirements:

- The output should be able to be formed into different visual representations including: tables, charts and diagrams.
- Accessibility to be able to find and read the results provided from the project

2.4 ENGINEERING STANDARDS

What Engineering standards are likely to apply to your project? Some standards might be built into your requirements (Use 802.11 ac wifi standard) and many others might fall out of design. For each standard listed, also provide a brief justification.

MITRE Framework:

The MITRE framework gives us a good overview of how industrial control systems can be vulnerable to specific types of attacks. These are specific standards from this framework that are related to our project:

Command & Control- by mimicking normal or expected traffic, it is possible for hackers to obtain access to your system within a network. Once they achieve administration privileges, they are then able to take control of the system, or in our case the power grid.

Privilege Escalation- after already achieving access to the system, attackers will then follow up by trying to obtain the highest level of privileges. By escalating their privileges to an administration level they could then have the ability to make permanent changes (i.e. delete user accounts, delete/transfer files, or upload malware to the servers) to a system.

Discovery- this tactic is used to gather information about a network or system, and is used as a means of reconnaissance. Attackers use this technique to obtain specific information about a network or system to find out if there are any potential vulnerabilities that could be exploited.

Credential Access- this is typically gathered through phishing attempts and is used to obtain user credentials and access at any means. Once a hacker is able to achieve access to some credentials and user access, they could then begin their mission to achieving higher privileges.

IEEE Standards:
IEEE 1547 & 2030 - Distributed energy resources interconnection & interoperability with electrical grid.

3 Project Plan

3.1 PROJECT MANAGEMENT/TRACKING PROCEDURES

Which of agile, waterfall or waterfall+agile project management style are you adopting? Justify it with respect to the project goals.

We are taking an agile approach for this project by continuously updating our project and uploading code to GitHub for continuous integration. We plan to continuously work towards simulating a power grid and then exploiting cyber attacks against it. In terms of the agile method, we want to consistently be working towards our goals towards completion.

What will your group use to track progress throughout the course of this and the next semester. This could include Git, Github, Trello, Slack or any other tools helpful in project management.

We are tracking our progress in GitHub for seamless ability to upload to one location. Additionally we are also keeping track of meeting notes as another method to track progress and tasks that need to be completed.

3.2 TASK DECOMPOSITION

In order to solve the problem at hand, it helps to decompose it into multiple tasks and subtasks and to understand interdependence among tasks. This step might be useful even if you adopt agile methodology. If you are agile, you can also provide a linear progression of completed requirements aligned with your sprints for the entire project.

We will be utilizing tickets on GitHub to keep track of who is in charge of which tasks and what tasks need to be completed by a specific time. GitHub has a feature that allows users/teams to create these tickets and assign them to team members in a cooperation to help members know the tasks at hand.

3.3 PROJECT PROPOSED MILESTONES, METRICS, AND EVALUATION CRITERIA

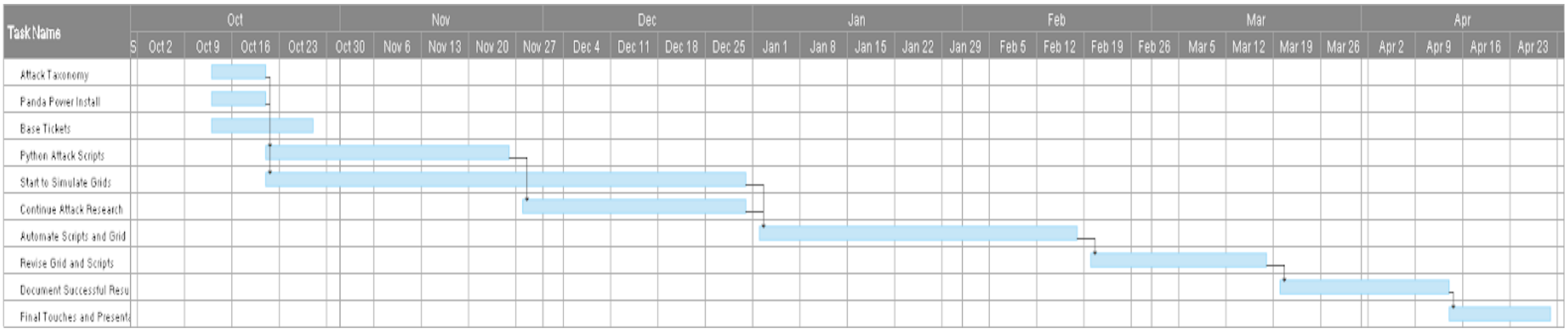
What are some key milestones in your proposed project? It may be helpful to develop these milestones for each task and subtask from 2.2. How do you measure progress on a given task? These metrics, preferably quantifiable, should be developed for each task. The milestones should be stated in terms of these metrics: Machine learning algorithm XYZ will classify with 80% accuracy; the pattern recognition logic on FPGA will recognize a pattern every 1 ms (at 1K patterns/sec throughput). ML accuracy target might go up to 90% from 80%. In an agile development process, these milestones can be refined with successive iterations/sprints (perhaps a subset of your requirements applicable to those sprints).

Some of our key milestones towards completing this project include: Simulating any version of a power grid via Panda Power tool in Python, Running python attack scripts against this simulated grid to determine outcomes, & Creating documented results of the outcomes presented from executing different attacks.

3.4 PROJECT TIMELINE/SCHEDULE

- Map out an attack taxonomy for cyber scripts to run (10/20/22)
  - Specific attacks we want to exploit
  - What attacks have been proven to be vulnerable to Power Grid systems in the past
- Users have Panda Power installed on their hosts (10/20/22)
  - Using IDE of preferred choice
  - Added to GitHub Repositories
- Starting to create base tickets for upcoming tasks (10/27/22)
- Start to create python attack scripts based off of taxonomy (11/25/22)
  - Create the required scripts in python and upload to the GitHub repository
  - Then start to determine how to run against in combination with Panda Power
- Begin to simulate grids through the panda power tool (12/30/22)
  - Determine which path we want to continue with
  - Which grid/s are the most feasible/realistic

- Continue to research how to utilize the created attacks scripts to use against the simulated power grid (12/30/22)
    - Make files
    - Automated another way possibly
- Begin to automate and run the cyber scripts against the Panda Power grid (2/18/23)
    - Possibly run multiple scripts against the same grid
    - Observe feedback and output
- Make an revisions to grid and scripts as needed (3/17/23)
    - Fix any issues with grid simulation or issues with running scripts
    - Double check to make sure issues are correctly triaged and work properly
- Begin documentation of successful attack results (4/13/23)
    - Correctly document the results from these exploited attacks
    - Map out specific attack points on the grid for a visual representation
- Finish our project and present (4/30/23)
    - Present to peers or senior design board members



3.5 RISKS AND RISK MANAGEMENT/MITIGATION

Consider for each task what risks exist (certain performance target may not be met; certain tools may not work as expected) and assign an educated guess of probability for that risk. For any risk factor with a probability exceeding 0.5, develop a risk mitigation plan. Can you eliminate that task and add another task or set of tasks that might cost more? Can you buy something off-the-shelf from the market to achieve that functionality? Can you try an alternative tool, technology, algorithm, or board? Agile projects can associate risks and risk mitigation with each sprint.

- Map out an attack taxonomy for cyber scripts to run- risk: 0.05
    - Resources might not be easily available to find
- Users have Panda Power installed on their hosts- risk: 0
    - No risks associated with this task
- Starting to create base tickets for upcoming tasks- risk: 0.05
    - GitHub resources may be down due to network connectivity issues or server issues

- Start to create python attack scripts based off of taxonomy- risk: 0.1
  - Scripts may not compile as expected and revisions may need to be made
- Begin to simulate grids through the panda power tool- risk: 0.1
  - This tool is open-source and very reliable for simulating grids
  - They're are good reviews for simulating powers grids and testing vulnerabilities against it
- Continue to research how to utilize the created attacks scripts to use against the simulated power grid- risk: 0
  - Researching how to use the scripts against the grid does not provide any risk
- Begin to automate and run the cyber scripts against the Panda Power grid- risk: 0.35
  - False data injections may arise to become an issue
  - The make file may not properly simulate attacks on the grid as needed
  - According to reviews, Panda Power can help to visualize interactions between these attack scripts on the outcomes on the grid
- Make an revisions to grid and scripts as needed- risk: 0.2
  - More issues may incur when revising the scripts or grid
  - These issues don't present a high risk because the tool will provide adequate explanations to why errors may occur
- Begin documentation of successful attack results- risk: 0
  - There will be no risk associated with the documentation of the results

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.

Map out an attack taxonomy for cyber scripts to run	Estimated time : 4 hours	We plan to have 3 of our cyber security students do research on what kind of attacks have been successful against power grids in the past and start mapping out in a document what attacks we might want to pursue. With the three of them working on this it shouldn't take more than 4 hours, might be even less.

Users have Panda Power installed on their hosts	Estimated time: 1 hour and 30 minutes	Since Panda Power is a library none of our group members have used before it might be a little difficult to get it set up quickly, so just for being safe an hour and thirty minutes should be about the time that takes.
Starting to create base tickets for upcoming tasks	Estimated time: 4 to 5 hours	This isn’t something that will be done in one sitting, but a process that will be done throughout the project, it will involve people in the group creating tickets for upcoming tasks and what needs to get done. This is an estimate for the whole project as creating tickets does not take very long at all.
Start to create python attack scripts based off of taxonomy	Estimated time: 10 to 15 hours	This will be one of the more difficult parts as it is a lot more technical and will require more time in figuring out certain attacks and how they work. Then obviously testing and implementing, which will also come with debugging.
Begin to simulate grids through the panda power tool	Estimated time: 10 to 20 hours	As neither of us have any experience with power grids or Panda power it will take some time to get used to it. However, since we all have programming experience we should be able to pick it up fast. As mentioned making a grid then simulating it will require a lot of electrical engineering aspects also

		which we aren't all particularly familiar with. The amount of research we have to do will take a lot of time, but then also implementing it. This might be our biggest time consumer.
Continue to research how to utilize the created attacks scripts to use against the simulated power grid	Estimated time: 5 to 6 hours	After we have a general power grid designed and also have made some attack scripts based on the taxonomy above. We should be able to figure out how to test and use them to see if it actually works. However, if we do run into problems or we are running the scripts wrong we will have to do additional research on it. This shouldn't take much time though unless we really do something wrong.
Begin to automate and run the cyber scripts against the Panda Power grid	Estimated time: 2 to 3 hours	If everything has gone right to this point then running the scripts shouldn't take much time at all since they are automated and don't have to be done manually.
Make an revisions to grid and scripts as needed	Estimated time: 4 to 5 hours	As mentioned above if we do end up running into problems then we will have to revise the designs along the way and we expect it to happen a decent amount of times depending on how the project goes. Therefore, this time will have to be reconsidered in the future.
Begin documentation of successful attack results	Estimated time: 2 to 4 hours	If everyone in the group works on documenting the

		results and what we found throughout the project it shouldn't take much time at all since we already have the results, but writing the findings might take time.

3.7 OTHER RESOURCE REQUIREMENTS

Identify the other resources aside from financial (such as parts and materials) required to complete the project.

Github, Panda Power, Pycharm, Kali linux tools, other IDEs if needed, Power grid designs to base our design off, different automation tools like Calderal

4 Design

4.1 Design Context

4.1.1 Broader Context

Describe the broader context in which your design problem is situated. What communities are you designing for? What communities are affected by your design? What societal needs does your project address?

List relevant considerations related to your project in each of the following areas:

Area	**Description**	**Examples**
Public health, safety, and welfare	**How does your project affect the general well-being of various stakeholder groups? These groups may be direct users or may be indirectly affected (e.g., solution is implemented in their communities).** Our project is related to public health through the different IOT devices that are connected through the grid. Items like a smart refrigerator can be affected by outcomes of the project. The users affected by this will primarily be the consumers of the power.	**Increasing/reducing exposure to pollutants and other harmful substances, increasing/reducing safety risks, increasing/reducing job opportunities** If the smart refrigerator is compromised by an attacker and they choose to exploit vulnerabilities, they could control the distribution of power throughout the IOT. By doing this, they could completely destroy the device's capabilities and possibly harm a user if they are in proximity to the device.

Global, cultural, and social	**How well does your project reflect the values, practices, and aims of the cultural groups it affects? Groups may include but are not limited to specific communities, nations, professions, workplaces, and ethnic cultures.** This project affects everyone that uses any type of electricity. This means almost everybody in the United States and most people in developed countries as well. The project is ultimately trying to defend against cyber attacks in the long-run, so this affects workers at power grids and consumers that use the power for their homes.	**Development or operation of the solution would violate a profession's code of ethics, implementation of the solution would require an undesired change in community practices** The results of our project can provide multiple utility providers with information regarding their systems or something related to it. Looking at the potential outcomes of these different cyber attacks can help prepare these distributors to better protect their services.
Environmental	**What environmental impact might your project have? This can include indirect effects, such as deforestation or unsustainable practices related to materials manufacture or procurement.** We could have multiple different effects on the environment through the attacks on the power grid. Through doing simulated attacks, we will know how to prevent them which can save a lot of money and resources depending on the attack prevented. In extreme cases, it could even save from loss of life, if an overloaded electrical component attack is prevented.	**Increasing/decreasing energy usage from nonrenewable sources, increasing/decreasing usage/production of non-recyclable materials** By being able to better maintain a power and keeping it secure will allow for the power to flow with less chance of an incursion. By helping increase the security, power grid companies will incur less intrusions and in the end it would be beneficial for the environment as well.
Economic	**What economic impact might your project have? This can include the financial viability of your product within your team or company, cost to consumers, or broader economic effects on communities, markets, nations, and other groups.** Large economic impacts could result from potential attacks exploited on a power grid. These attacks could end up causing these power distributors lots of funding if they are compromised.	**Product needs to remain affordable for target users, product creates or diminishes opportunities for economic advancement, high development cost creates risk for organization** The outcomes from our project can be utilized to help these utility companies save money from potential attacks. The results could be used to show how

	Foreign attacks could leave certain sectors of the power grid vulnerable and damaged, which will end up costing the distributors much more after being attacked.	companies can better prepare for potential attacks. This will save them money and show how they could lose money if these actions are taken.

4.1.2 Prior Work/Solutions

Include relevant background/literature review for the project

– If similar products exist in the market, describe what has already been done

– If you are following previous work, cite that and discuss the **advantages/shortcomings**

– Note that while you are not expected to "compete" with other existing products / research groups, you should be able to differentiate your project from what is available. Thus, provide a list of pros and cons of your target solution compared to all other related products/systems.

Detail any similar products or research done on this topic previously. Please cite your sources and include them in your references. All figures must be captioned and referenced in your text.

There are no similar products compared to the project that we are working on. Cyber threats are still a fairly new attack vector that companies are starting to prepare for. This project will provide a great resource for electrical companies to use when trying to figure out how best to secure their network and power distribution. We will be utilizing a product that is generally just used to simulate a power grid and its distribution of power, but we will also be implementing intrusions on this grid to simulate outcomes from different attack methods. Resource pages will be the majority of the work that we will follow just to become familiar with the software.

4.1.3 Technical Complexity

Provide evidence that your project is of sufficient technical complexity. Use the following metric or argue for one of your own. Justify your statements (e.g., list the components/subsystems and describe the applicable scientific, mathematical, or engineering principles)

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles –AND–

   Our design consists of three components: Power grids & making sure they converge (not blacked out immediately), Cyber attacks on said grids, and the delivery of information in a comprehensible format (accessibility). The last listed may seem easy, but the information we are going to be delivering will be analyzing thousands and thousands of simulated attacks, each unique in their own way. To get a power grid up and running, we will need to code it in Python using the Panda Power library. We will be using lots of math and physics to get these power grids to actually function properly. The cyber attacks on these grids will also be coded in Python scripts and the authors will need to have extensive knowledge on these types of attacks and knowledge of the grid itself, as knowing where to automate these attacks is crucial. The delivery of the data will need to be accessible to a wide audience, as the target for this product is not only power companies and experts, but also consumers and potential customers/investors.

2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

   We have several challenging milestones in our project. One of them is to get a certain cyber attack called a false data injection working in our environment inside Panda Power, as it does not directly support these. Another milestone is getting cyber attacks to work on the grid, make sure the grid itself doesn't bug out and break, and then also create an analysis we can view after the run is successful. After this is all working, we need to turn this up to 100. We will eventually be running hundreds if not thousands of these attacks in parallel, each needs to have a working grid with no bugs, and each needs to be analyzed and put into a report of some sort along with all the other attacks. When we have all this data being spit out, we need to figure out a good way to display it. Having one page for each attack seems a little silly, as nobody wants to go through a 1000 page document. We will have to find ways to create graphs that aren't too noisy that display most if not all of these attacks and the statistics from each of them so that people can read them and aren't overwhelmed by the massive amounts of information and jargon on the report.

4.2 Design Exploration

4.2.1 Design Decisions

List key design decisions (at least three) that you have made or will need to make in relation to your proposed solution. These can include, but are not limited to, materials, subsystems, physical components, sensors/chips/devices, physical layout, features, etc. Describe why these decisions are important to project success.

Key design decisions:

- Attack Taxonomy
- How to design the simulated power grid or which existing power grid to replicate in the simulation
- Which simulation software to use
- How end-user interaction will work, e.g. shell vs GUI

4.2.2 Ideation

For at least one design decision, describe how you ideated or identified potential options (e.g., lotus blossom technique). Describe at least five options that you considered.

Power Grid:

We knew we could either create our own power grid design to simulate or replicate an existing power grid. We used a compare and contrast methodology to decide between the two options. The biggest difference between the two was having more freedom with design with creating our own and having more directly applicable results with replicating an existing power grid.

End-User Interaction:

In order to find our options for end-user interaction we used a lotus blossom. Through this we found our best options would be to let the user interact directly with a shell, have a GUI for the user to interact with with the same functionality underneath, or a combination of both where the user could use the GUI and have the option for a type of "advanced" mode with direct shell interaction.

4.2.3 Decision-Making and Trade-Off

Demonstrate the process you used to identify the pros and cons or trade-offs between each of your ideated options. You may wish to include a weighted decision matrix or other relevant tool. Describe the option you chose and why you chose it.

Things that have no trade-offs

- Attack Taxonomy
- Panda power

Trade-offs

- Gui VS shell
- Existing grid vs generated grid

The process we used to identify the pros and cons of each idea was to compare them and figure out what would be best suited for what we are doing, and also to make sure to mitigate any cons that our decisions had. These cons might not even apply to the scope of the senior design project, which in that case they are not considered in the decision. We also made sure to list ideas that didn't have any trade-offs at all, like deciding on our attack taxonomy and choosing Panda Power as our supporting Python library. These are just what we are going to be doing in our project, and while Panda Power technically does have its drawbacks, it is outside the scope of the senior design project. Although we can add more attacks to our taxonomy, we decided to go with false data injections and mass hacking of Internet of Things devices because these are some of the more common and feasible attacks that could happen in the near future or have already happened, like in Houston a while back. We decided to use the Panda Power library in Python because our client suggested it and it has a massive library that supports everything that we want to do in this project.

5 Testing

5.1 Unit Testing

What units are being tested? How? Tools?

We have several different units of our project that are being tested as they are implemented. The interface used for our grid is one of the units that is tested to ensure that the parameters used are working properly and working functionally as expected. We also unit test the simulated grid by checking to make sure that the grid converges and is simulated and complies correctly. For these testing purposes we will be utilizing PandaPowers built-in compiler and any additional Python library we may need to make a functionally simulated power grid. Using Python 3.9 we will also be creating the scripts used for the attack vectors of the project. This leads into another unit of the project that will be tested; by executing the scripts alongside the simulation of the grid we will need to verify that the expected results match those of the results received.

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?

The only interfaces that we use are the PandaPower electricity grid that we generate through Python and then PyCharm as a compiler. We could also use online GitHub, but it won’t be necessary for testing. As we test PyCharm, we also test PandaPower as both are synonymously tested. This can be done with a simple script and as long as we have a valid interpreter, it should work if nothing was corrupted in the install process.

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?

The critical integration paths in our design are verifying if instances of attacks work, and their correctness. Verifying these tests will include running an attack script on our grid and then simulating it in PandaPower. Following this if the grid does not converge we will need to verify a blackout occurred. Otherwise we will need to verify the attack was successful and the outputs are reasonable. The tools used for this will be our attack scripts, PandaPower, and our grid.py.

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?

The essential parts for testing the system as a whole is ultimately making sure that the fundamental components are working properly. Since the only components we use are Python, PandaPower, and GitHub, this makes things easy. For Python, we just need a simple test program that uses the libraries we will need to verify they work. PandaPower is a library in Python, so this can be tested in conjunction with Python. GitHub is also quite easy to test as we can do simple push and pull requests to see if our code uploads and downloads respectively.

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 they do not break? Is it driven by requirements? Tools?

We will confirm that new features don't break old ones by continuously testing as soon as a new feature is implemented. We will utilize Panda Power's simulation environment and different wPython compilers to verify any warnings that come up, and also create use-case tests to ensure that using a new feature doesn't brick an old one, and vice versa, just to make clear that the features are preserved in new updates. We can set up these tests in GitHub by using a pipeline, or by making a build-deploy script that will be run before a commit/pull request.

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?

In order to show that the requirements have been met for both functional and non-functional requirements users will test the project at several stages. The users will consist of employees who would work with the program. We want to ensure that the interface functions as intended, the interface has a comprehensible use-case statement (--help, -h), the interface easy to understand and use, and grid.py was generated. The users will complete testing by; running the interface, running any commands to create their specific grid, and test if the user has questions, use-case statements will help.

5.7 Security Testing

Not applicable

5.8 Results

What are the results of your testing? How do they ensure compliance with the requirements? Include figures and tables to explain your testing process better. A summary narrative concluding that your design is as intended is useful.

The results of these conducted tests will help to further improve and enhance our procedure for completing the project and design. The results ensure compliance through proving and providing visualizations of the outcomes so individuals are able to physically see the different outcomes from the attack vectors. Once the results are created for the designated user, they will then be able to implement any countermeasures as desired. Our intended use for the final product is for companies to be able to take the information that is simulated from our project and use that to become more aware of ongoing threats.

6 Implementation

Describe any (preliminary) implementation plan for the next semester for your proposed design in 3.3. If your project has inseparable activities

between design and implementation, you can list them either in the Design section or this section.

Once we are able to configure a functional power grid, our next step is to begin adapting our layout to one similar to that of Iowa State's power grid. After successfully simulating a power grid using PandaPower, we will then begin incorporating cyber threats to be exploited against the grid. PandaPower will allow us to manually configure the distributions of power through the grid, and this will help us be able to exploit False Data Injections. The first exploit will change and edit the distributions of power throughout each of the transistors used by the grid. Finally, we will document the changes that are observed from exploiting the cyber script and use these results to help educate others of the effects from these attacks.

7 Professional Responsibility

7.1 AREAS OF RESPONSIBILITY

Pick one of IEEE, ACM, or SE code of ethics. Add a column to Table 1 from the paper corresponding to the society-specific code of ethics selected above. State how it addresses each of the areas of seven professional responsibilities in the table. Briefly describe each entry added to the table in your own words. How does the IEEE, ACM, or SE code of ethics differ from the NSPE version for each area?

#	Area of responsibility	Definition	NSPE Canon	IEEE
1	Work Competence	Perform work of high quality, integrity, timeliness,and professional competence.	Perform services only in areas of their competence; Avoid deceptive acts.	To maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

				This code revolves around qualified individuals being needed to maintain technical competence.
2	Financial Responsibility	Deliver products and services of realizable value and at reasonable costs.	Act for each employer or client as faithful agents or trustees.	To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, to be honest and realistic in stating claims or estimates based on available data, and to credit properly the contributions of others; This code reflects on criticisms and being able to be held accountable for them.
3	Communication Honesty	Report work truthfully, without deception, and are understandable to stakeholders.	Issue public statements only in an objective and truthful manner; Avoid deceptive acts.	To improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems; This aims to help educate society about our technologies and being able to maintain their understanding of the products.

4	Health, Safety, Well-Being	Minimize risks to safety, health, and well-being of stakeholders.	Hold paramount the safety, health, and welfare of the public.	To hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment; This code also strives to comply with ethical designs and being consistent with their sustainable development.
5	Property Ownership	Respect property, ideas, and information of clients and others.	Act for each employer or client as faithful agents or trustees.	To avoid injuring others, their property, reputation, or employment by false or malicious actions, rumors or any other verbal or physical abuses; This code is for the protection of not only other individuals, but also property or other intellectual things.
6	Sustainability	Protect the environment and natural resources locally and globally.		To hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and

				sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment; This code is for the protection of disclosing factors of endangerment to the public or the environment.
7	Social Responsibility	Produce products and services that benefit society and communities.	Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession.	To treat all persons fairly and with respect, and to not engage in discrimination based on characteristics such as race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression; This one is to ensure that there is no offensive demeanor occurring between parties or co-workers.

7.2 PROJECT SPECIFIC PROFESSIONAL RESPONSIBILITY AREAS

Work Competence- Our group is applicable for good work competence by following our set goals/milestones towards the completion of our project. We have consistently met each goal so far this semester and are performing at a High rate currently.

Financial Responsibility- The product we use for our project is open source software and free to use, so we do not meet any financial obligations.

Communication Honesty- Our group has done a good job with communicating so far this semester in terms of being able to communicate between each other and the professor. We are performing at a High rate for our communication.

Health, Safety, Well-Being- We do not have any health or safety risks associated with our project, but do ensure group members are feeling comfortable.

Property Ownership- We hold this in high standards because we need our laptops to be able to not only complete our tasks, but also for easier communication between peers.

Sustainability- One goal of our project is to help maintain and secure our power grids, and this would then ensure that our environment is better protected.

Social Responsibility- Our group has done a good job being able to communicate aspects of our project in a social manner through presentations. This is rated as High because of our ability to demonstrate descriptive features of our project and outcomes that could arise.

7.3 MOST APPLICABLE PROFESSIONAL RESPONSIBILITY AREA

Our most applicable professional responsibility is our communication honesty. This is because through each of our bi-weekly meetings we have been able to demonstrate effective communication between each other and the professor. Specifically, we have demonstrated this ability through asking the professor questions and being able to gather materials from him as well.

8 Closing Material

8.1 DISCUSSION

Discuss the main results of your project – for a product, discuss if the requirements are met, for experiments oriented project – what are the results of the experiment, if you were validating a hypothesis – did it work?

The main results of our project will consist of a functionally simulated power grid that will have scripts executed on it, so that intrusions will occur and inflict disbursements on the grid. From this we wish to show the possibility of different attacks occurring and how they could be better prevented. Our project is still in earlier stages of simulation for our grid. We have consistently met our goals so far.

8.2 CONCLUSION

Summarize the work you have done so far. Briefly reiterate your goals. Then, reiterate the best plan of action (or solution) to achieving your goals. What constrained you from achieving these goals (if something did)? What could be done differently in a future design/implementation iteration to achieve these goals?
We have taken time to map and figure out our best path for being able to complete this project. We just recently received some schematics that will be very useful for the implementation of the grid we wish to compose. Having this schematic will help us to better display and visualize the impacts from these attacks. So far we have not faced any major constraints, but have also started to create some test cases for being able to use the UI portion of our project.

8.3 REFERENCES

List technical references and related work / market survey references. Do professional citation style (ex. IEEE).
We have utilized several different references for finding documentation and resource pages for the software we are using and others, including:

Muhammad, Roomi M. “False Data Injection Cyber Range of Modernized Substation System.” *False Data Injection Cyber Range of Modernized Substation System*, Nov. 2020, https://www.researchgate.net/publication/348090545_False_Data_Injection_Cyber_Range_of_Modernized_Substation_System.

“Pandapower.” *Pandapower*, https://pandapower.readthedocs.io/en/v2.9.0/index.html.

Mohsenian-Rad, Hame. *Topic 1: Basics of Power Systems - Department of Electrical and ...* 2021, https://intra.ece.ucr.edu/~hamed/Smart_Grid_Topic_1_Power_Systems.pdf.

8.4 APPENDICES

Any additional information that would be helpful to the evaluation of your design document. If you have any large graphs, tables, or similar data that does not directly pertain to the problem but helps support it, include it here. This would also be a good area to include hardware/software manuals used. May include CAD files, circuit schematics, layout etc,. PCB testing issues etc.Software bugs etc.
We can not reveal the schematics that we were given because they are sensitive to the actual grid that is used today and could lead to issues if released.

8.4.1 Team Contract

Team Name ________Blakely's Ballers__________________________

Team Members:
1) ____Cole Medgaarden__________________ 2) ______Noah Peake_______________
3) ____Michael Gierek____________________ 4) _____Conner Spainhower_______________
5) _____Hrijul Balayar____________________ 6) ______Jake Stanerson__________________

Team Procedures

1. **Day, time, and location (face-to-face or virtual) for regular team meetings:**
    a. Face-to-Face meetings on every other Thursday @ 2:30 PM
2. **Preferred method of communication updates, reminders, issues, and scheduling (e.g., e-mail, phone, app, face-to-face):**
    a. We have a group chat on snapchat and will create a discord group?
3. **Decision-making policy (e.g., consensus, majority vote):**
    a. We will make decisions as a group and listen to other possible opinions until a decision is made.
4. **Procedures for record keeping (i.e., who will keep meeting minutes, how will minutes be shared/archived):**
    a. We can create a shared google doc folder to keep track of minutes, meeting notes, and other potential collaborations.

Participation Expectations

1. **Expected individual attendance, punctuality, and participation at all team meetings:**
    a. Attendance is expected for all face-to-face meetings.
2. **Expected level of responsibility for fulfilling team assignments, timelines, and deadlines:**
    a. We will have "soft" deadlines which are when work is expected to be completed by
    b. and "hard" deadlines where work must be completed by, in terms of advancing the project.
3. **Expected level of communication with other team members:**
    a. Communication is expected by all members and are encouraged to state opinions about the project and its steps towards completion.
4. **Expected level of commitment to team decisions and tasks:**
    a. We should focus on sticking to our decisions, but as the project advances these commitments may change based on the outcomes that we are receiving.

Leadership

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

   a. Cole- I would like to be in charge of creating and implementing the python scripts we will use to test impacts of cyber attacks, additionally keeping track of meeting notes, and assisting with others tasks as needed.
   b. Conner - I will also help with any Python scripting and security aspects of the project that need to be looked at.
   c. Noah- I would like to focus on finding different kinds of attacks that could be simulated. Which might work better to see the impact.
   d. Hrijul - I would like to work with Noah Peake on different cybersecurity threats and how we can help things be more effective and secure. I also would like to contribute with python scripting.
   e. Jake - I will be assisting in the scripting and automation side of the project. I will also be working with a python library called Panda Power to set up and test environments.

2. **Strategies for supporting and guiding the work of all team members:**
   a. We will complete our work as timely as possible and will help others complete their tasks if issues are to arise.
3. **Strategies for recognizing the contributions of all team members:**
   a. We will be utilizing GitHub as one of our resources and this will help to see individual contributions, but also we will be keeping track of individual updates as a part of the meeting notes.

Collaboration and Inclusion

1. **Describe the skills, expertise, and unique perspectives each team member brings to the team.**
   a. Cole- I work as a Cyber Security Analyst at Kingland Systems and have had some experience with real world settings for Cyber Security and will use this knowledge to help when thinking about how to infiltrate the power grid. I have had some coding experience throughout my experience at Iowa State and should be able to create the python scripts for attacks and try to help assist in the formation of the power grid itself.
   b. Conner - I had an internship at Hy-Vee this past summer that could be useful when we need to deal with server attacks or network issues. I am specifically trying to get into network security, so any issues we have with this aspect I will take a look into personally. I also have experience with Java, C, Python, and other miscellaneous programming languages to hopefully advance the scripting process.
   c. Noah- In my internship I focused on pentesting. I have a good background of understanding cyber attacks. I have experience with coding in Java, C, and Python. For this project my skills would best suit finding how to test the system we build.
   d. Hrijul- I work as an analyst for the College of Veterinary medicine where we used python scripting to automate different tasks used for normal IT departments. This included active directory, powershell scripting, and developing tools for better management for new student computers. I also worked with Professor Manimaran

in the engineering department where we did automation for cyber attacks using Caldera.

   e. Jake - I work at Collins Aerospace as an ASIC/FPGA engineer where I develop radio parts and test them via waveforms and lab inspection. I also work on the security of these radio parts, making sure they cannot be physically compromised. In addition to writing VHDL, I also work with a group in my department that writes scripts that automate any of these given processes, and also automatically bring any outdated tools up to date with standard use.
   f. Michael - I worked at The Grieve Corporation this past summer and dealt with a lot of coding and EE work. I helped develop software and GUIs for the company and had a role in technical support which had me looking at electrical schematics. I think I can bring some EE insight to the team as well as some software development experience.

2. **Strategies for encouraging and supporting contributions and ideas from all team members:**
   a. We will give opportunities for people to state their opinions during our meetings as the meeting is going on, additionally we can discuss options in our group chats as well.
   b. We will be open to any constructive criticism as we advance our project and see how the attacks play out. Along with this, any new ideas are welcome as sometimes ingenuity is simple and can be overlooked.
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?)**
   a. We can talk about ongoing issues during our meetings as well, and then be able to discuss potential solutions to this problem on the spot.

Goal-Setting, Planning, and Execution

1. **Team goals for this semester:**
   a. To complete this project and go above and beyond the expectations.
2. **Strategies for planning and assigning individual and team work:**
   a. We can assign tasks within the shared doc, and also keep track of the status of these tasks.
3. **Strategies for keeping on task:**
   a. Hopefully the deadlines will help team members keep track of their current tasks.

Consequences for Not Adhering to Team Contract

1. **How will you handle infractions of any of the obligations of this team contract?**
   a. Team members will be given multiple chances to complete their obligations, and if the problem continues we will seek higher authority for advice.
2. **What will your team do if the infractions continue?**
   a. potential removal of the team if the problems persist and prevent project completion.

****

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) _____Cole Medgaarden_____________________________ DATE ___09/19/2022______
2) ______Noah Peake_________________________________ DATE ___09/19/2022_______
3) ______Conner Spainhower___________________________ DATE __ 09/20/2022_______
4) _______Hrijul Balayar______________________________ DATE __09/22/2022_______
5) _________Jake Stanerson____________________________ DATE __09/22/2022_______
6) _______Michael_Gierek_____________________________ DATE ___09/22/2022______