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.**	**Increasing/decreasing energy usage from nonrenewable sources, increasing/decreasing usage/production of non-recyclable materials**

	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.	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. Foriegn attacks could leave certain sectors of the power grid vulnerable and damaged, which will end up costing the distributors much more after being attacked.	**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 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 you 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.