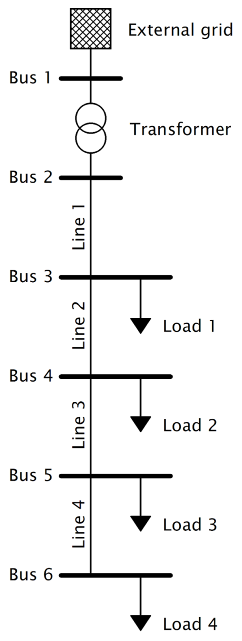
## 4.3 Proposed Design

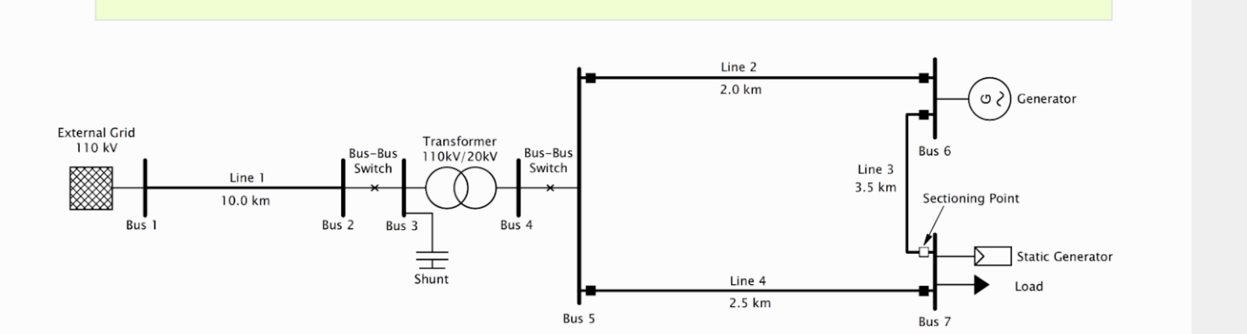
### 4.3.1 Overview

**Provide a high-level description of your current design. This description should be understandable to non-engineers (i.e., the general public). Describe key components or subsystems and how they contribute to the overall design. You may wish to include a basic block diagram, infographic, or other visual to help communicate the overall design.**

For our project and design, we are utilizing a tool that is widely used in the electrical industry. The tool is used to help automate and optimize the distribution of power throughout a power grid. This tool operates and is coded in the language Python. PandaPower has built-in parameters that we will be using to build up our initial power grid. Specifically, we will be working with distributions of power through using buses or simulated electrical lines (transformers). We need to use these parameters to get our initial power grid simulated so that we can begin to automate different series of cyber attacks against the system. We developed an attack taxonomy document to create and plan out which cyber tactics we would be taking. For one of the simulated attacks we will be exploiting false data injections. False data injection attacks (FDIA) have been a rising issue within the power industry and occur when attackers are able to compromise a system or sensor readings in such a way that some or most times they go undetected. We will be using the false data injection attack to run against our simulated power grid and determine the different outcomes it causes to certain sectors of the power grid. We also want to document these results to see and show how users can go about better preventing these types of attacks to an actual city power grid.



### 4.3.2 Detailed Design and Visual(s)



This is a simple single voltage power grid example that we will most likely base our design off. Most of the components used in this diagram such as the buses, switches and other components are also supported by pandapower. This also represents the type of network we want our grid to have, so it is a little bit easier to perform attacks on it as it is not as complicated as a multi-voltage power grid.

- Simulation of cyber attacks on a power grid
    - Utilizing Panda Power on python 3.9
        - Basis for building a power grid, also source of analytics
    - Python scripts in panda power library to simulate cyber attacks on a grid spun up in panda power, master script will execute attack scripts en masse
        - The attack taxonomy includes, but is not limited to, false data injections and mass hacking of IOT devices throughout homes on the grid (increased usage for each consumer)
        - Python scripts will execute random attacks from taxonomy in areas of the grid that have been programmed to be targeted, selected randomly. The script will have weights of some sort to ensure that only areas that are affected by the attack will be attacked (just so distribution sites don't get hit with an attack that can't affect them for example). These attacks will be run numerous times, up to the person who runs the script, and will happen in parallel as best as they can(limited by threads on CPU)
    - Master/Wrapper script will do all of this and output
        - Output will be generated by panda power
        - Will display what attacks happened where, most likely locations for attack, most dangerous locations for attack, most dangerous attack on average, most costly attack & location

### 4.3.3 Functionality

**Describe how your design is intended to operate in its user and/or real-world context. What would a user do? How would the device/system/etc. respond? This description can be supplemented by a visual, such as a timeline, storyboard, or sketch.**

The intended use of our completed project will aim to help end-users get a visual representation of the possible outcomes from a cyber attack. Our primary goal is to be able to successfully simulate and run a "malicious" python script against a simulated power grid and then be able to document its' results. The documentation will help provide these users with outcomes from the attacks, but also suggestions to be able to prevent these intrusions. Ideally our project will also be able to be customized to a users preference where they would be able to get a visualization for outcomes on their power grid. To customize these features, a user would only need to provide a layout of their current grid and it can be simulated based on those diagrams. PandaPower would then take that design and begin to run the attack scripts against that layout and map out that attack pathway. In a timeline; User requests and sends in schematics of grid → The schematics are imputed into PandaPower → Once the grid is simulated, the Python attack scripts can be executed → After the execution, PandaPower will show the distribution and outcomes from each attack → provide results to user and show documentation.

### 4.3.4 Areas of Concern and Development

**How well does/will the current design satisfy requirements and meet user needs?**

Our design and development of this project will meet all the satisfactions for user needs when it is completed. We will have an outlined pathway of an attack and be able to show users how they could be affected from ongoing threats.

**Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?**

There are no major concerns as of now, and this is in part to there being many resource pages available for functionality use of the python tool we are using. Difficulties may occur when attempting to automate the cyber attacks to run against the grid with a makefile.

**What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?**

If more issues seem to arise with automation of the scripts, we can then reach out to our advisor for further assistance, or we can implement the scripts using a different method. Perhaps using different functionalities within our PandaPower tool.

## 4.4 Technology Considerations

**Describe the distinct technologies you are using in your design. Highlight the strengths, weaknesses, and trade-offs made in technology available. Discuss possible solutions and design alternatives.**

For our design we are using python as the programming language. Python is the best language for our design. Since it is primarily a scripting language it fits in well with the requirement of creating attack scripts. Python also has a reputation for being easy to learn and use, this will allow us to focus on the project design right away instead of being stuck for a long  time learning the language. Python also has various packages related to our project, one of which is PandaPower which we will use in our design. We chose to work with PandaPower because it has good documentation, the basic usage of the package seems easy to learn, and it is free. The downside of PandaPower is that it may lack some complex features a pay-to-use package might include. However, based on the scope of our project we decided that issue would have little impact on the final result.

## 4.5 Design Analysis

**Discuss what you have done so far, i.e., what have you built, implemented, or tested? Did your proposed design from 4.3 work? Why or why not? Based on what has worked or not worked (e.g., what you have or haven't been able to build, what functioned as expected or not), what plans do you have for future design and implementation work? For example, are there implications for the overall feasibility of your design or have you just experienced build issues?**

So far our group has discussed strategies on how to attack a power grid, installed the necessary software, and started making some scripts and playing with the implementation software. The plan from 4.3 has been working thus far, and I cannot see a reason yet why we wouldn't be able to meet its requirements. Any work towards finding ways to prevent cyber attacks would greatly benefit those who run cyber grids and potentially save millions of dollars.

We plan to write scripts to attack the devices within a power grid. So far, our biggest issue is learning the software and implementing it into a virtual grid. Once we get this down, we will be able to test our code and see if we can "break" the virtual grid's network.