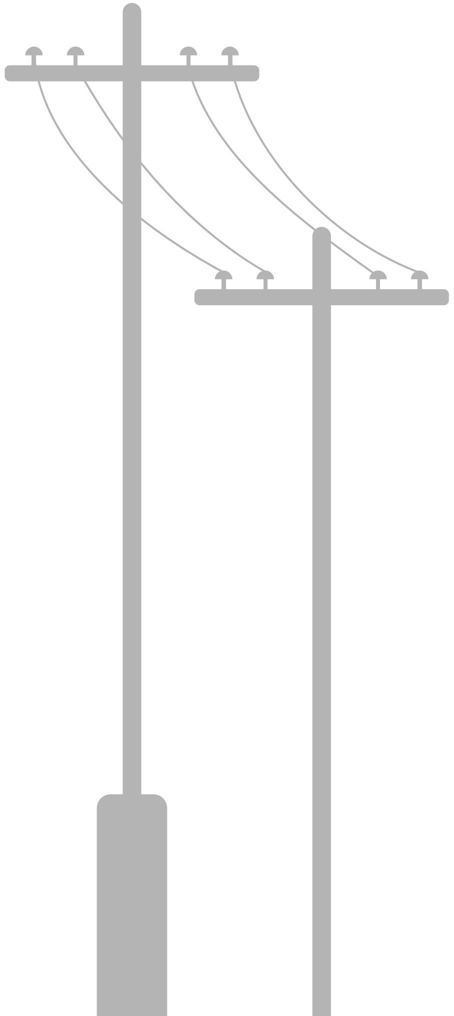


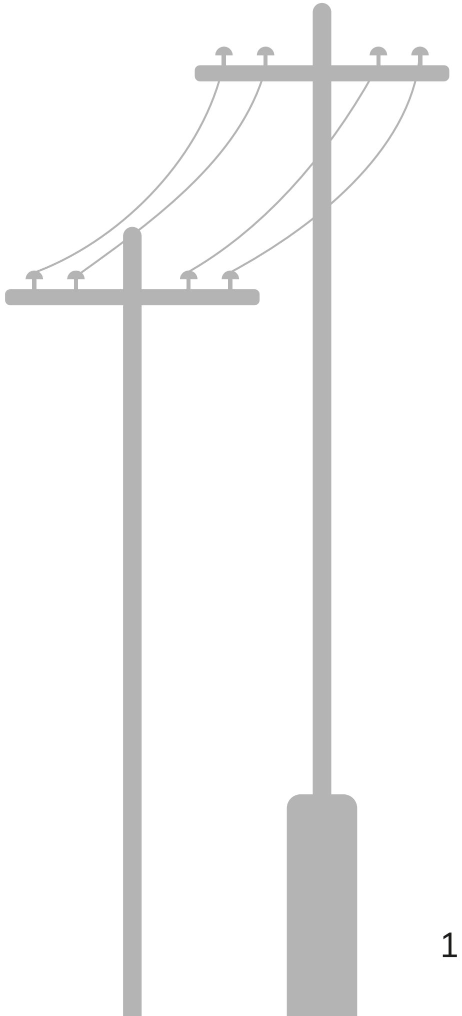
CyHELICS

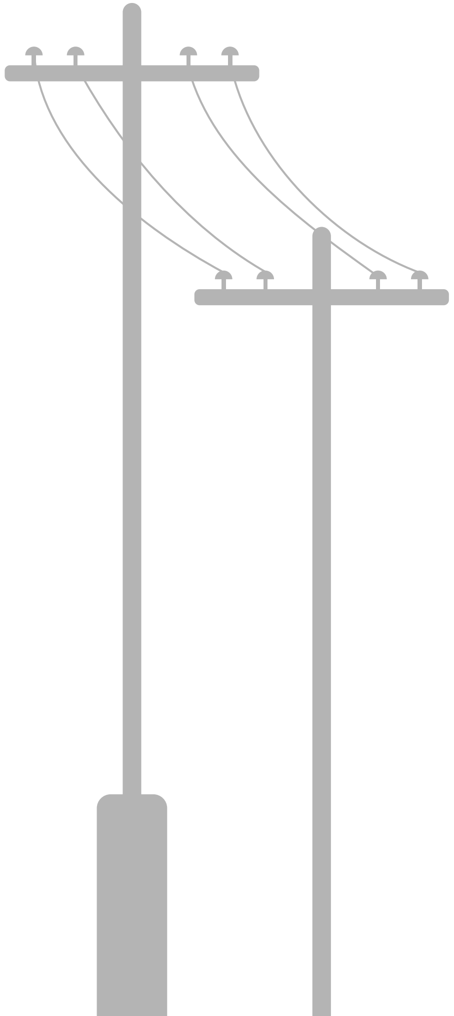
Simulating Large-scale Power Grids and Cyberattacks using HELICS

Senior Design Team 28

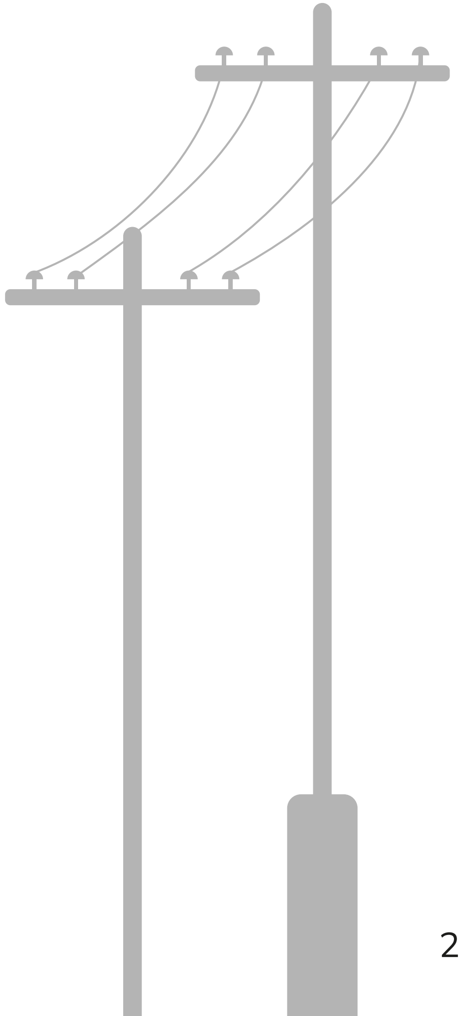
Tyler Atkinson: Attack Design
Zach Hirst: Attack/Frontend Support
Thomas Keeshan: Transmission/Distribution Grid
Matt Nevin: EV Model/Energy Grid Support
Justin Templeton: Frontend/Docker/Network Design Support
Kaya Zdan: Helics Creation/Energy Grid Support

Client and Advisor: Dr. Gelli Ravikumar





Introduction



CyHelics Team

Attack Team

Tyler Atkinson

Zach Hirst

Electric Grid Team

Thomas Keeshan

Matthew Nevin

Frontend and Dev-Ops Expert

Justin Templeton

Helics Infrastructure Expert

Kaya Zdan

Background

Problem: Cyber attacks against the power grid are a growing concern.

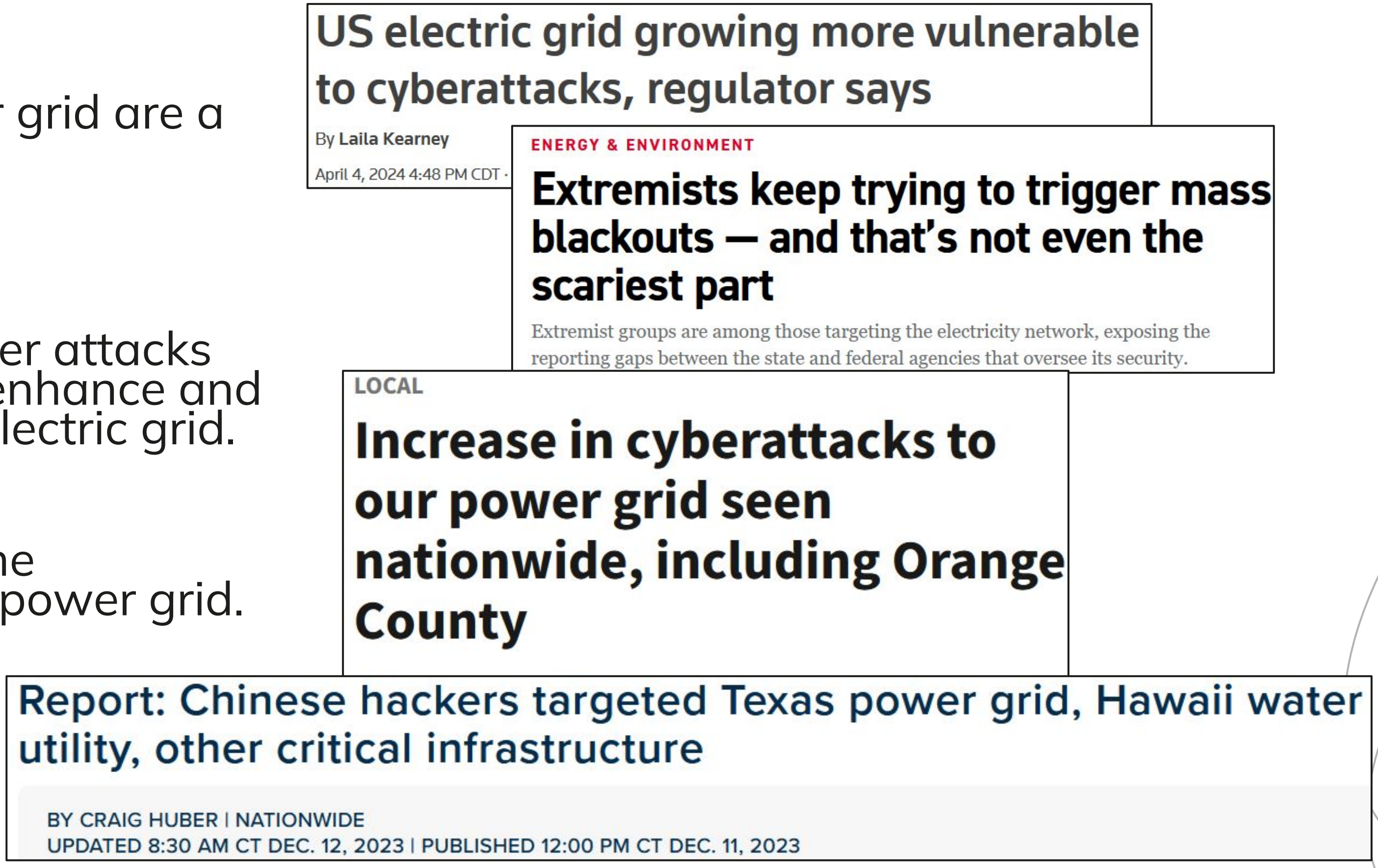
Solution:

CyHelics is a tool to test the impact of cyber attacks against an electrical grid, and help users enhance and validate security measures for their own electric grid.

We will use HELICS to co-simulate both the distribution and transmission sides of the power grid.

Who does it help?

- Utility Companies
- Power Grid Consultant Companies
- City Engineers and Workers
- The General Population



US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney

April 4, 2024 4:48 PM CDT ·

ENERGY & ENVIRONMENT

Extremists keep trying to trigger mass blackouts — and that's not even the scariest part

Extremist groups are among those targeting the electricity network, exposing the reporting gaps between the state and federal agencies that oversee its security.

LOCAL

Increase in cyberattacks to our power grid seen nationwide, including Orange County

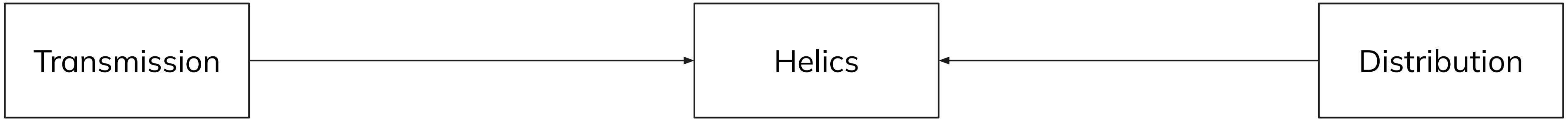
Report: Chinese hackers targeted Texas power grid, Hawaii water utility, other critical infrastructure

BY CRAIG HUBER | NATIONWIDE

UPDATED 8:30 AM CT DEC. 12, 2023 | PUBLISHED 12:00 PM CT DEC. 11, 2023

What is HELICS?

HELICS stands for Hierarchical Engine for Large-scale Infrastructure Co-Simulation (HELICS)



Transmission

Helics

Distribution

Broader Context

Public Health and Safety:

- Can make grids more reliable by finding weak points.
- Can be used to make post fault plans to ensure the least amount of area is affected.
- Optimize design to help reduce power outages.

Economic:

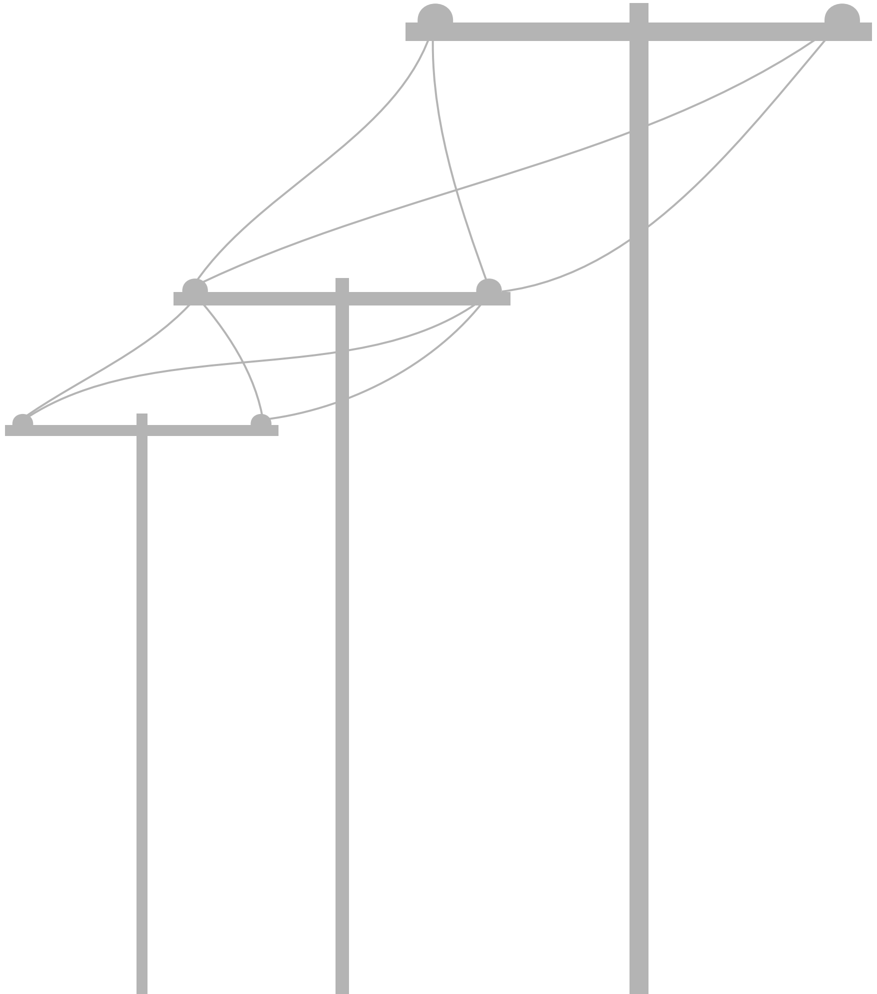
- Saves money by helping optimize grid design.

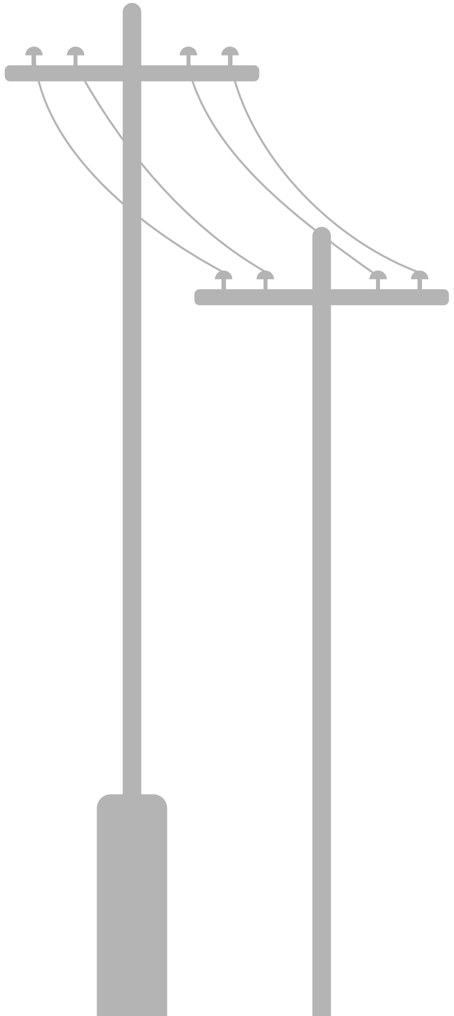
Environmental:

- Other industries depend on the power grid to Continue running.
  - Costs compound based on users.

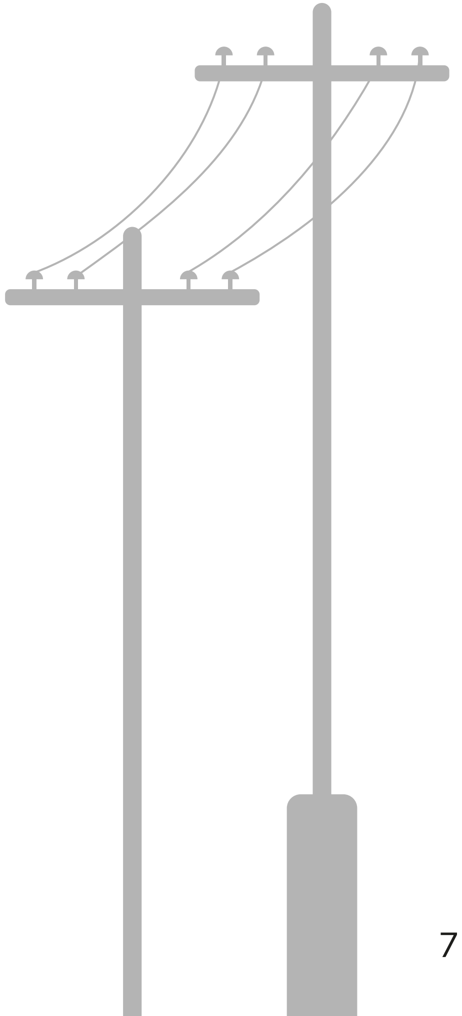
Global, Cultural, and Social:

- Attacks induce fear into Grid users.



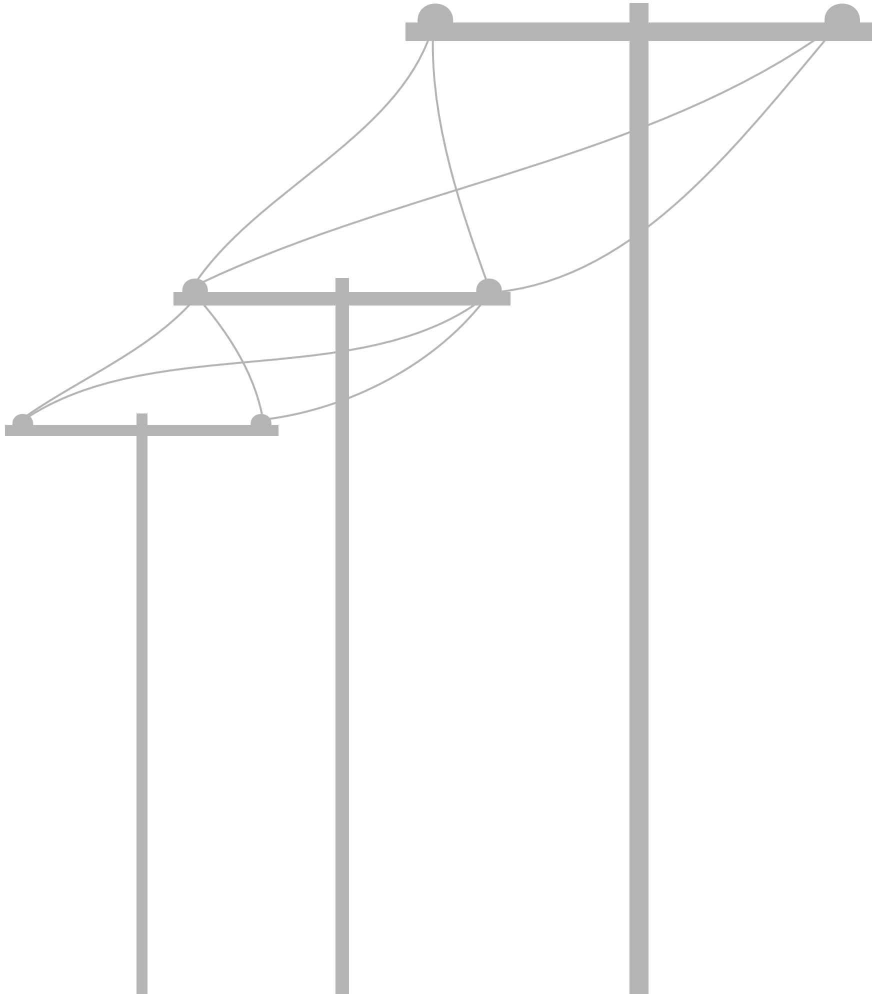


Revised Design



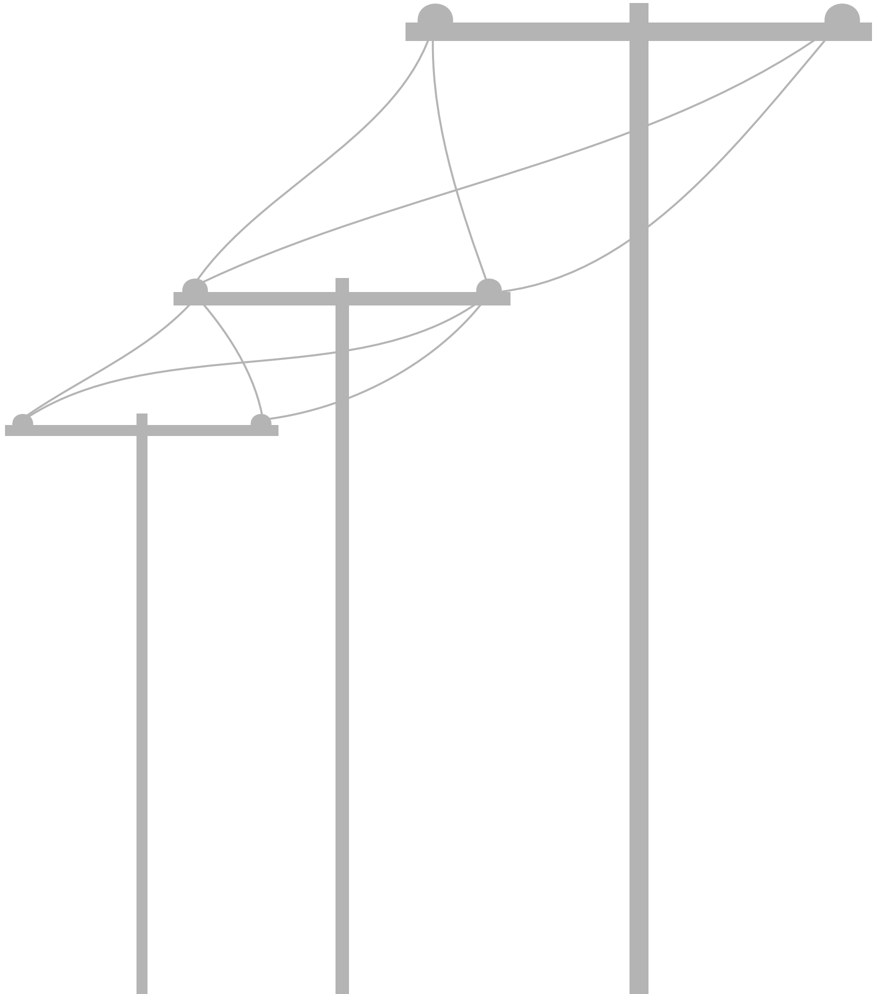
Requirements

- Use CyHELICS to combine multiple substream programs and run concurrently.
- Power Grid will include multiple load types.
- The simulation will be tested in a VM environment.
- The simulation will be set up in a dockerized environment.
- The user must be able to select what attack to use in the flask front end.
- Use HELICS to model electric vehicle load profiles in Sante Fe and inject the model as a load on the Sante Fe model.
- Frontend must have downloadable packages for results
- Frontend must have an archive mode to quickly look at effects of cyber attacks.



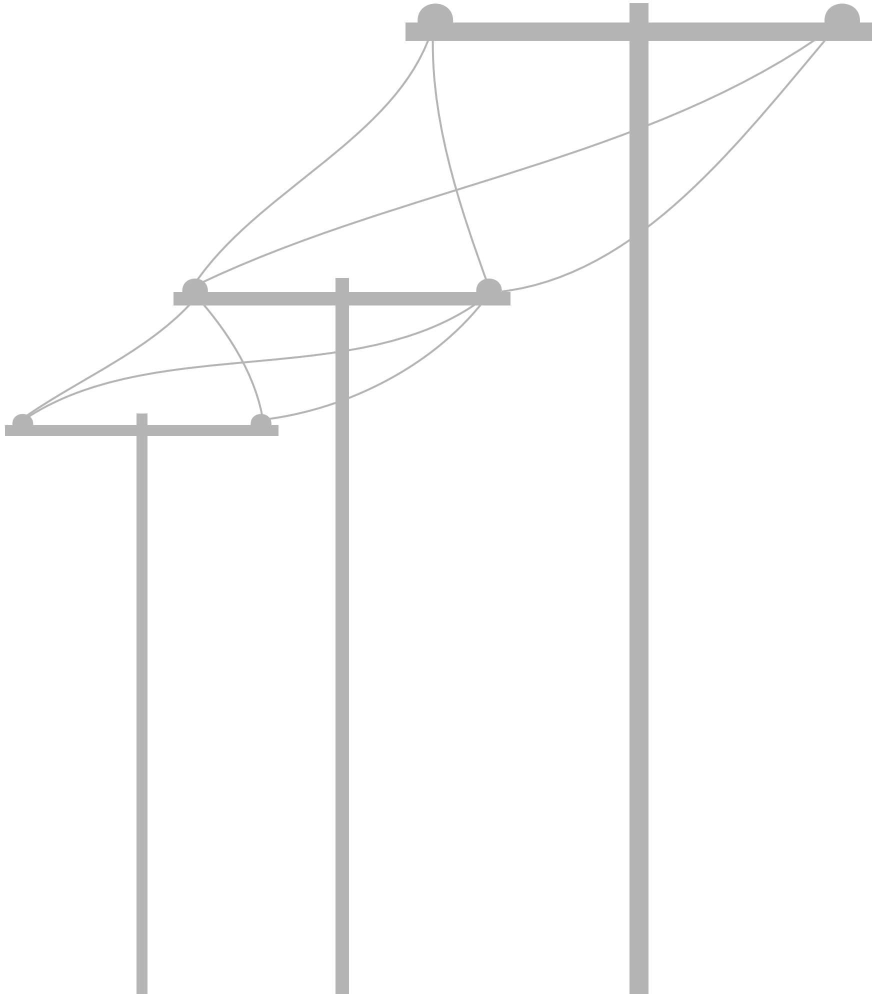
Engineering Standards

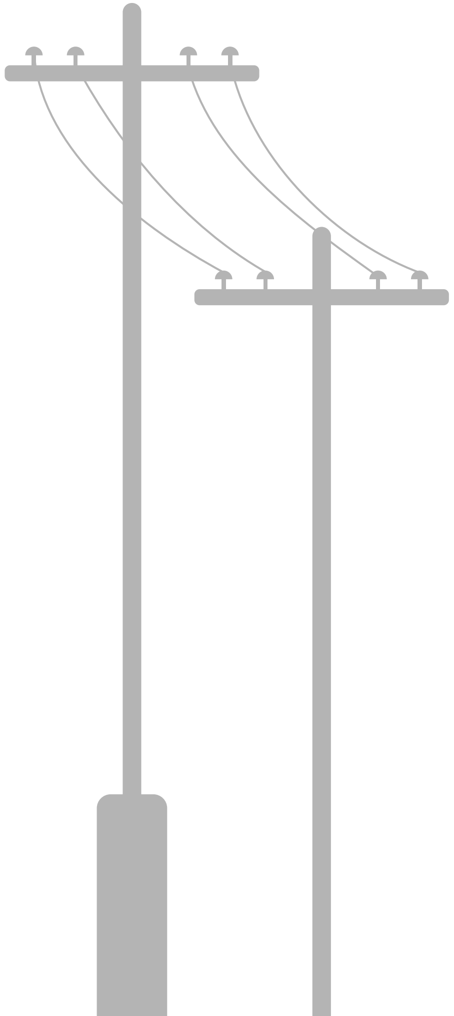
- HELICS and PandaPower use an open-source BSD-3 clause license.
- Python-DSS is open source, with no listed license.
- MITRE ATT&CK Framework is an industry-standard knowledge base for pentesting, gap assessments, threat intelligence/hunting, and more.
- Python is an industry-standard interpreted scripting language.
- Modular Javascript Functions for Frontend



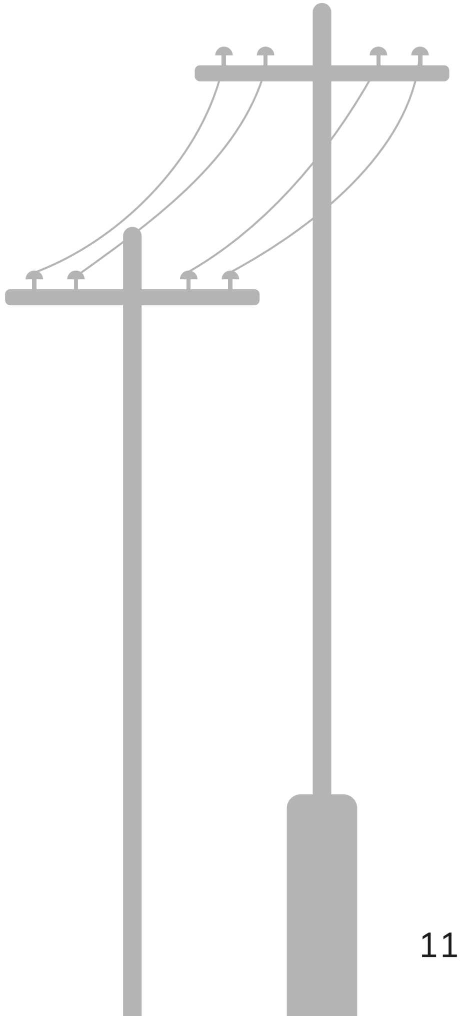
Security Concerns and Countermeasures

- Bad actors can see where faults are in powergrid.
    - Could be used to target specific lines for attack.
- Application is offline, no way to breach it from the internet.
- Application is dockerized - limiting its malicious use on a host computer.





Implementation Details

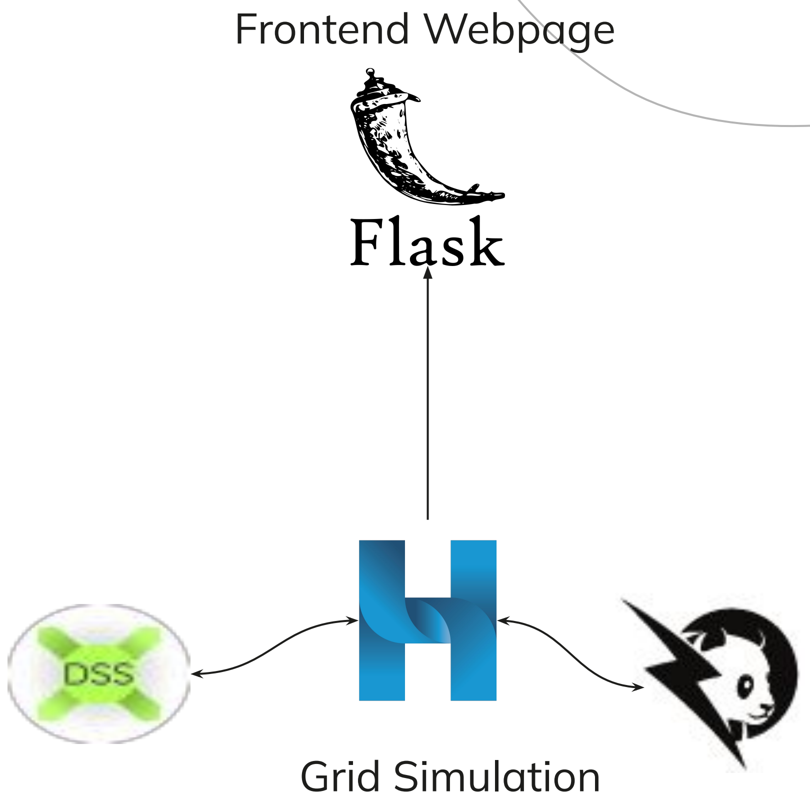


Simplified Design

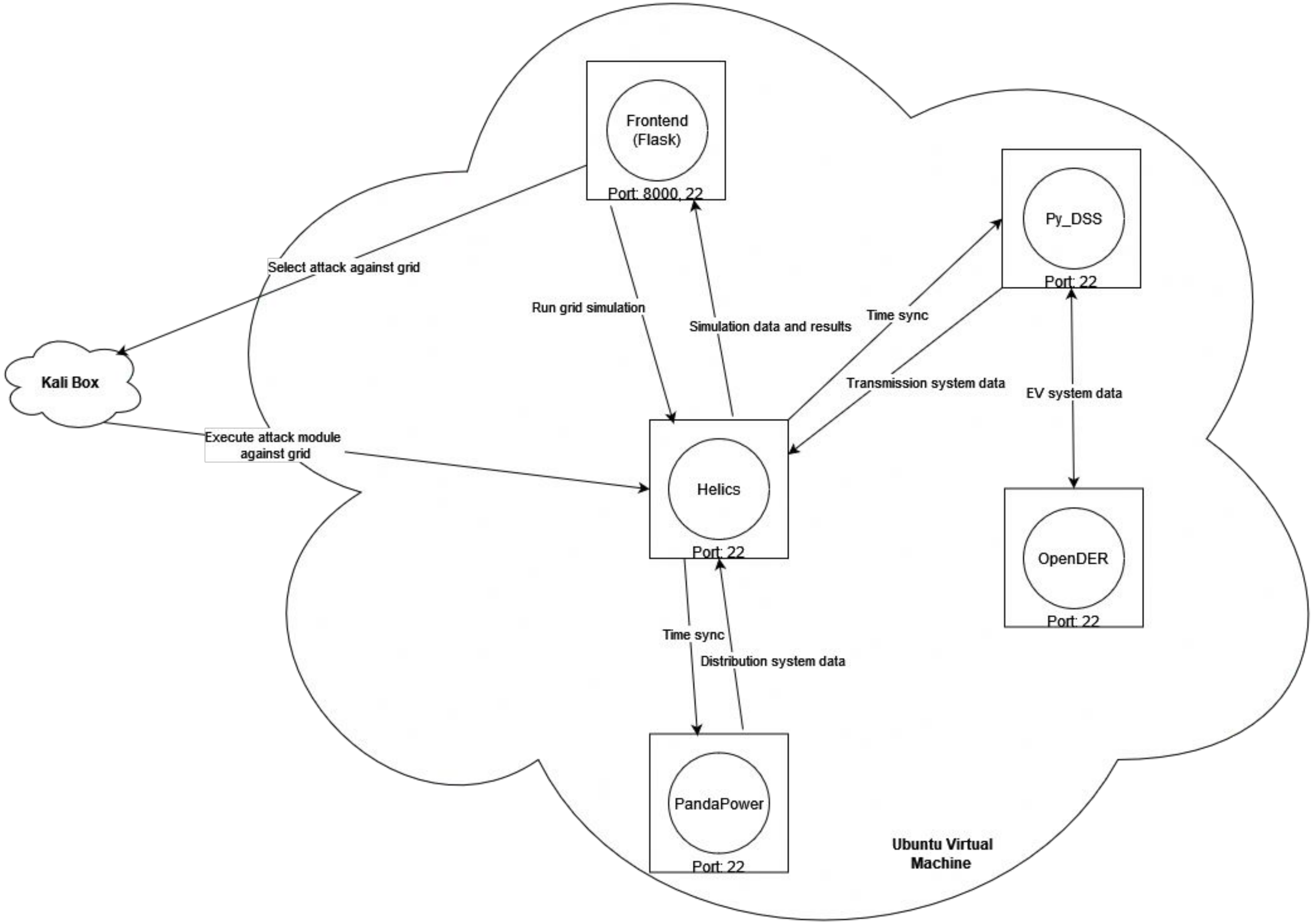
- Our simulation uses Pandapower and DSS-Python simulations running simultaneously, which are communicating with each other via Helics

- The resulting data gets sent to a Flask frontend, and displayed in graphs for the user. The graphs and CSV data can also be downloaded from the webpage.

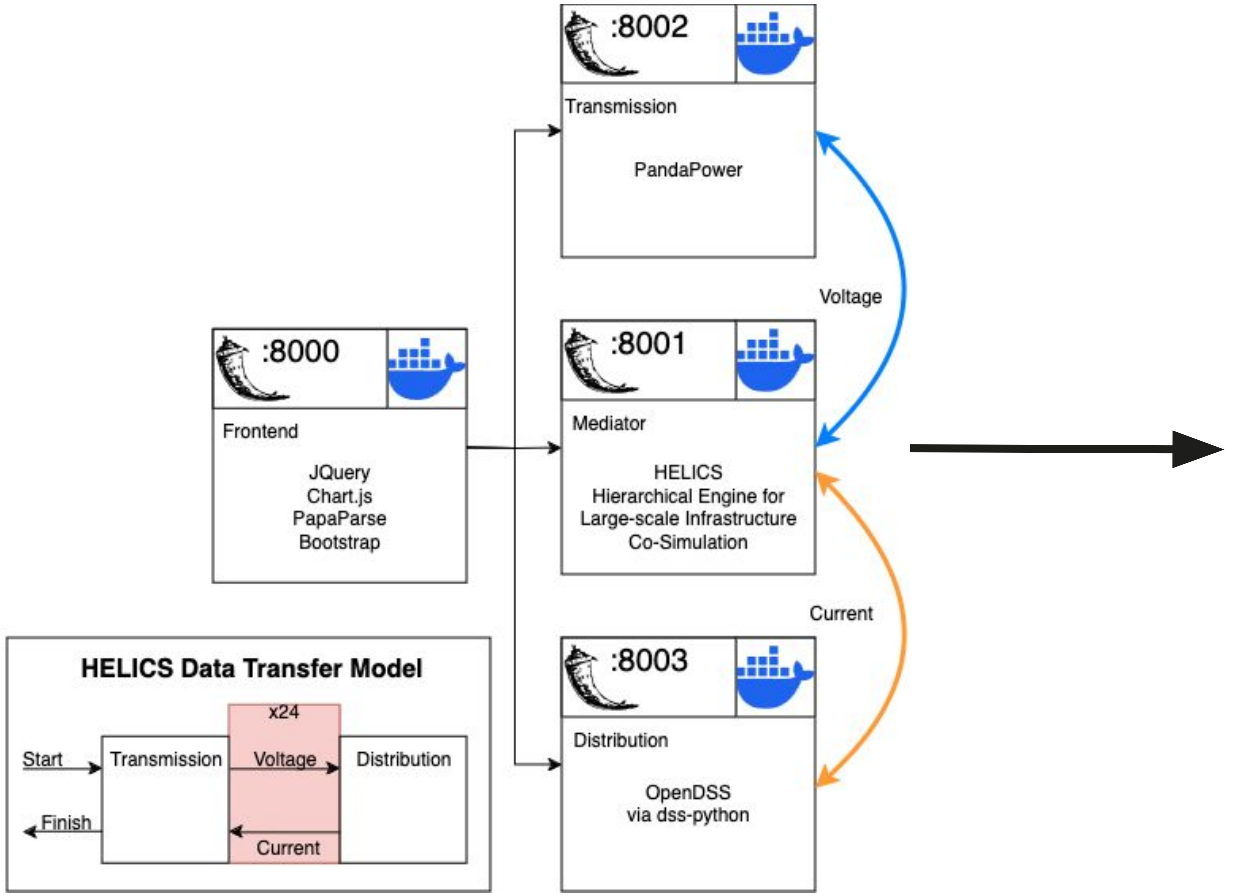
- The simulation system is run within Docker.

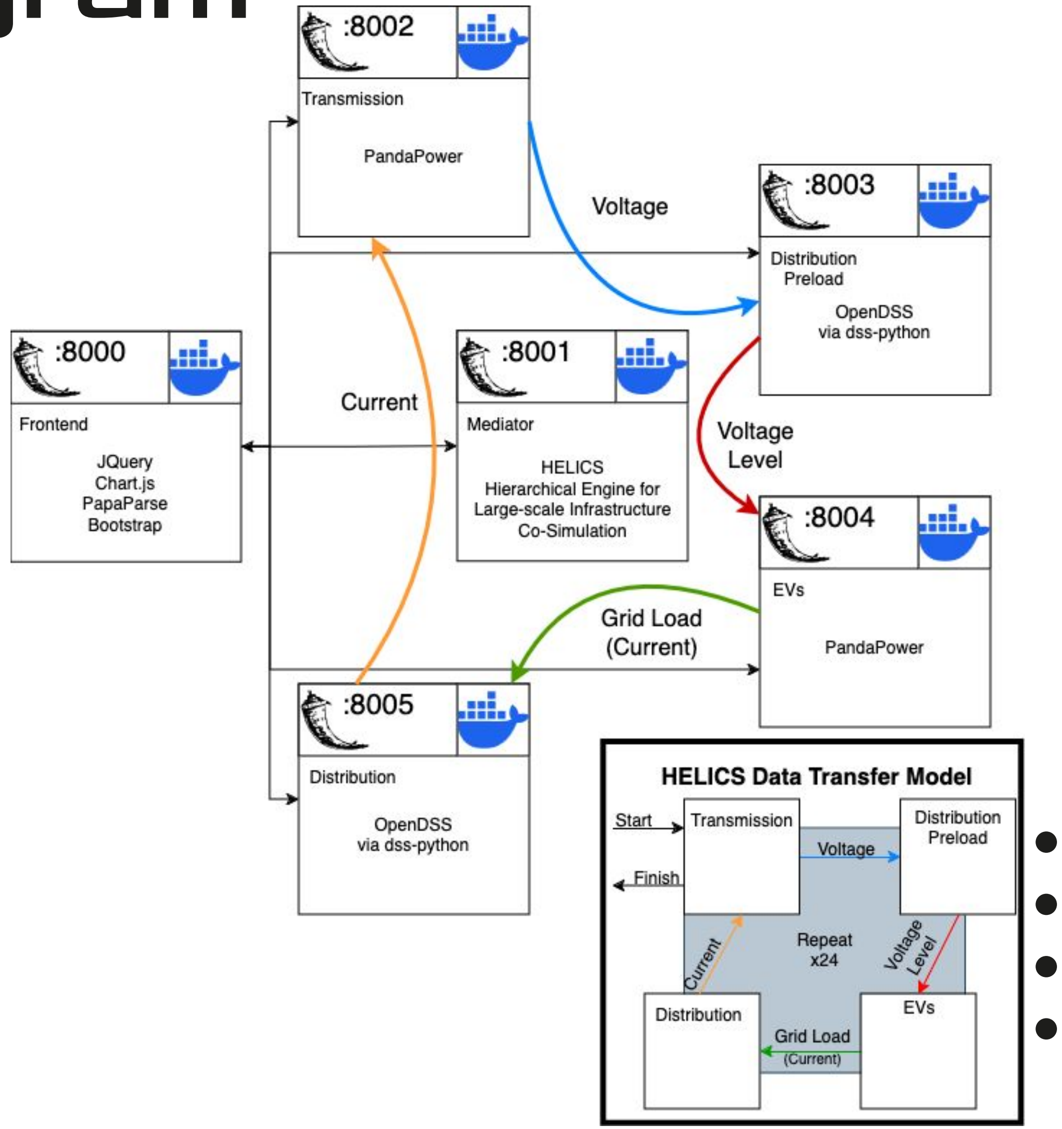


Design Evolution from 491



Docker Design Diagram

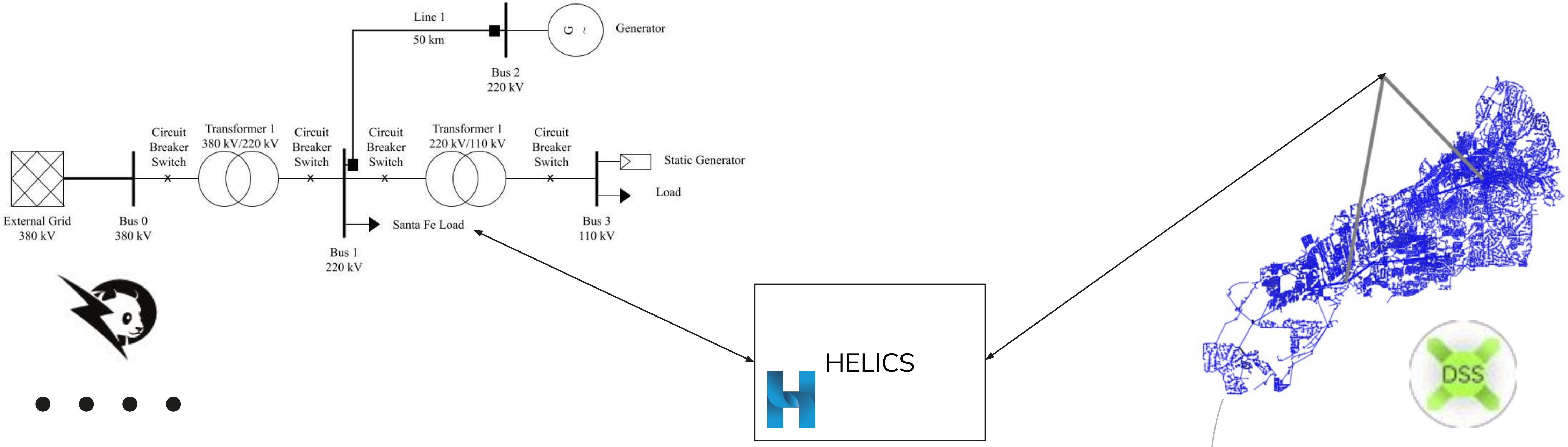




●
●
●
●

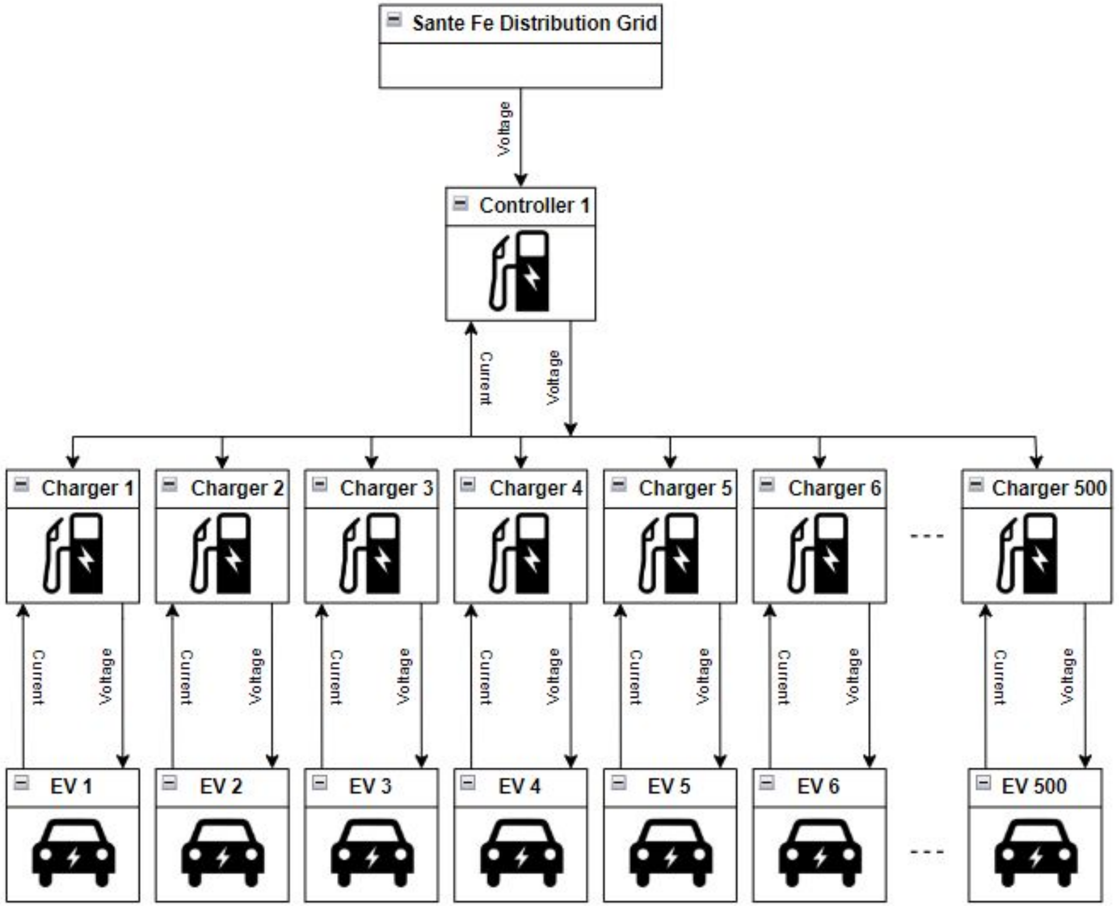
Electric Grid Model

- Transmission simulation = PandaPower
- Distribution simulation = DSS-Python
  - Santa Fe distribution model from BetterGrids.com
- Helics is used to facilitate the communication between the two softwares



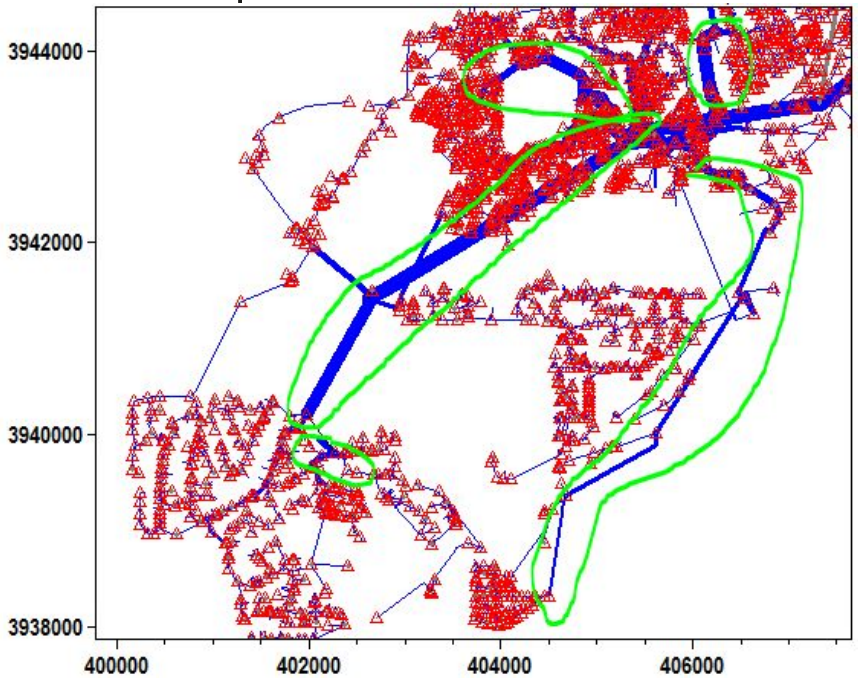
EV Model

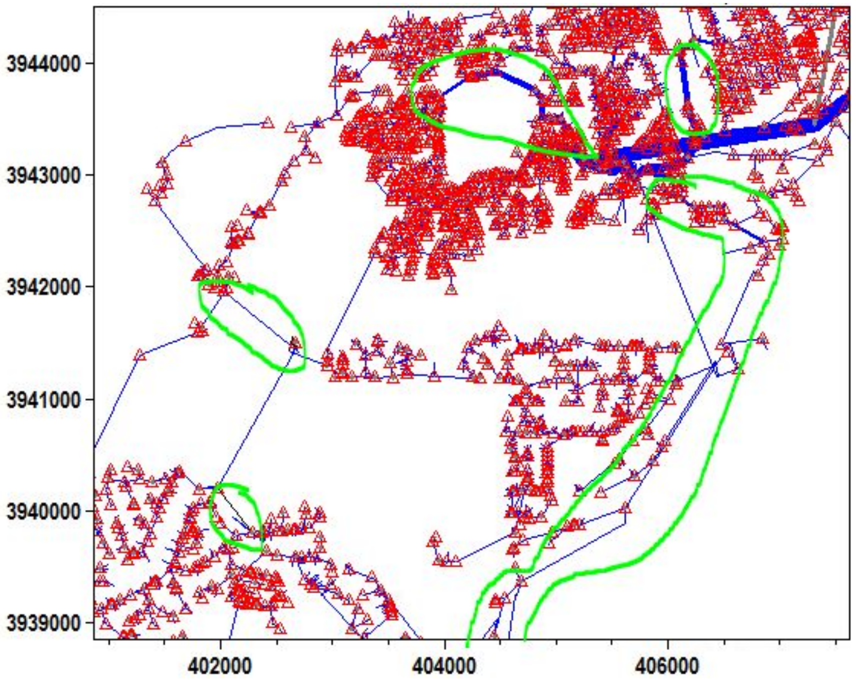
◇ Helic's will also be used to to model electric vehicle load profiles in Sante Fe

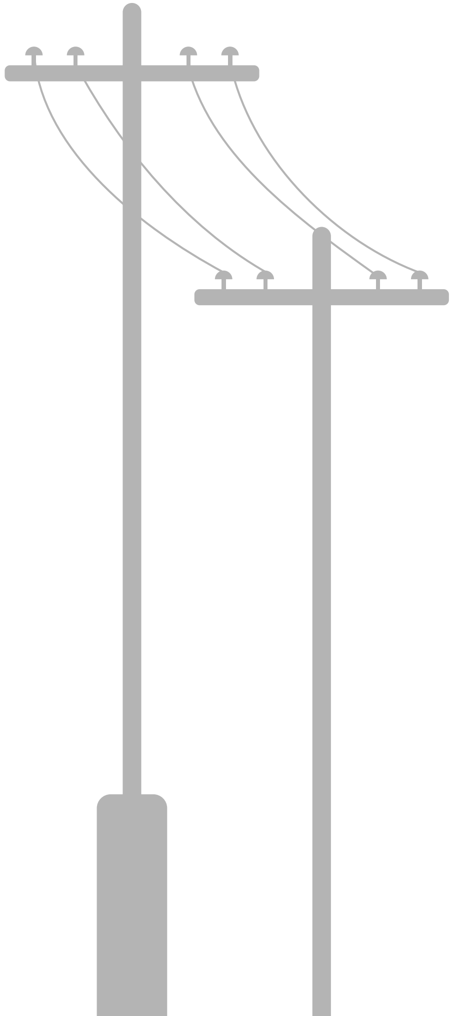


Attacks

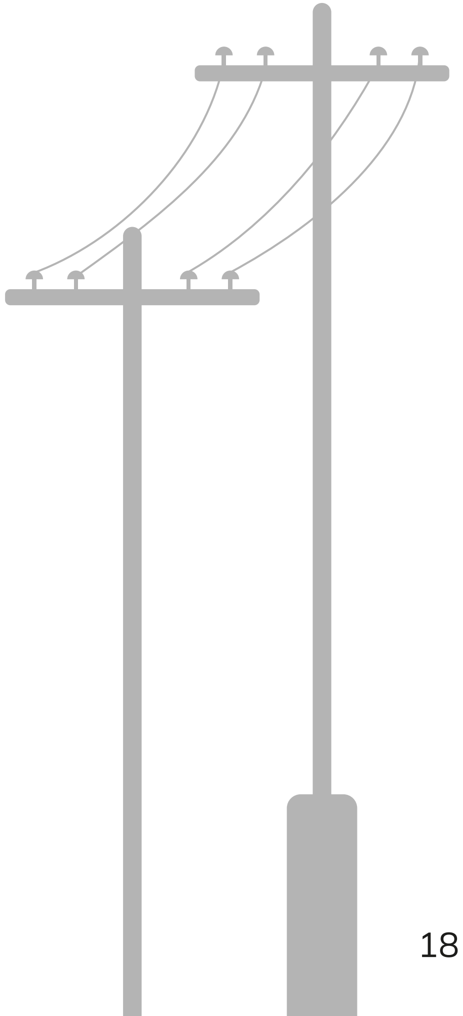
- Came up with 3 different types of attacks focused on the electric grid:
  - Selective line tripping (low, medium, and high severity)
  - Generator short-circuit
  - Load-Shedding due to falsified data
- Due to time constraints, only got one implemented with a partial plan for a second
  - Implemented the line tripping
  - Created a plan for the short-circuit





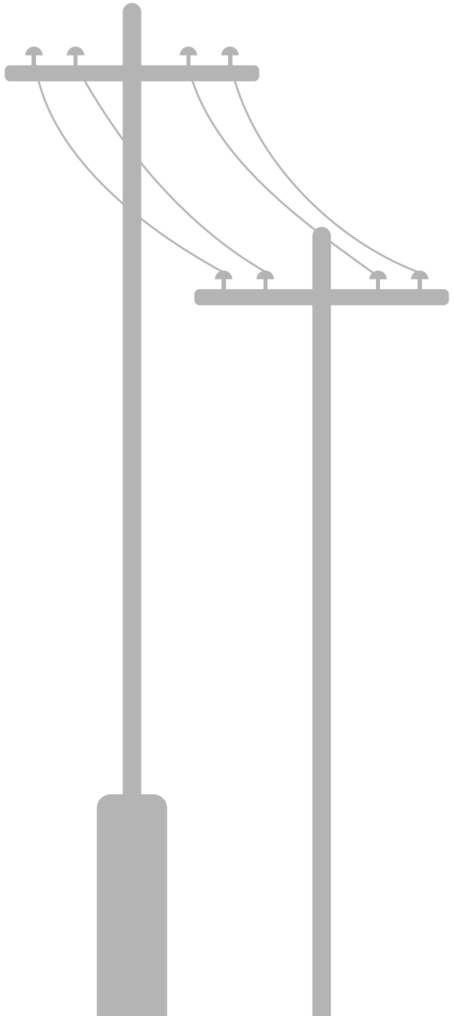


Testing

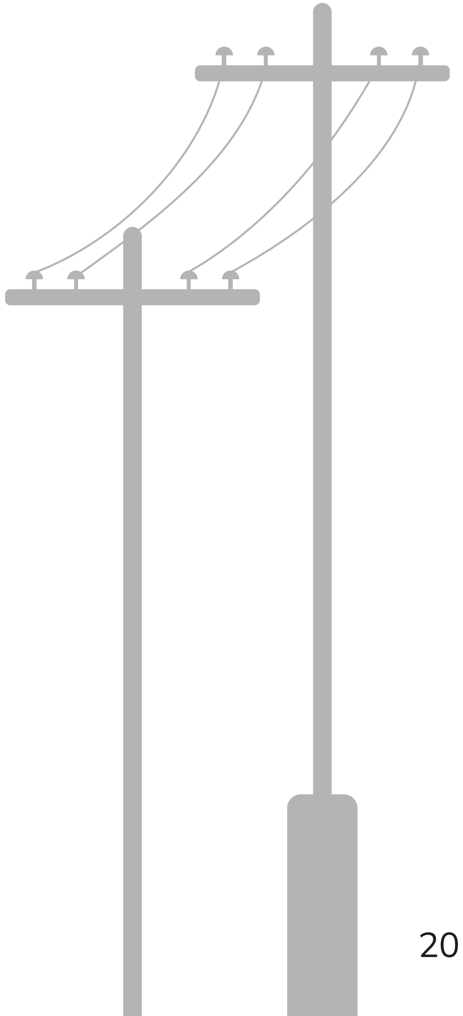


Process

- System and End-to-End Testing
  - Check if Flask Applications are active.
    - If there are conflicts or basic errors, HTTP requests will fail.
- Integration Testing
  - Check for simulations returning error codes
    - If the simulation fails, an error code will be produced to the http request that called it.



Conclusion

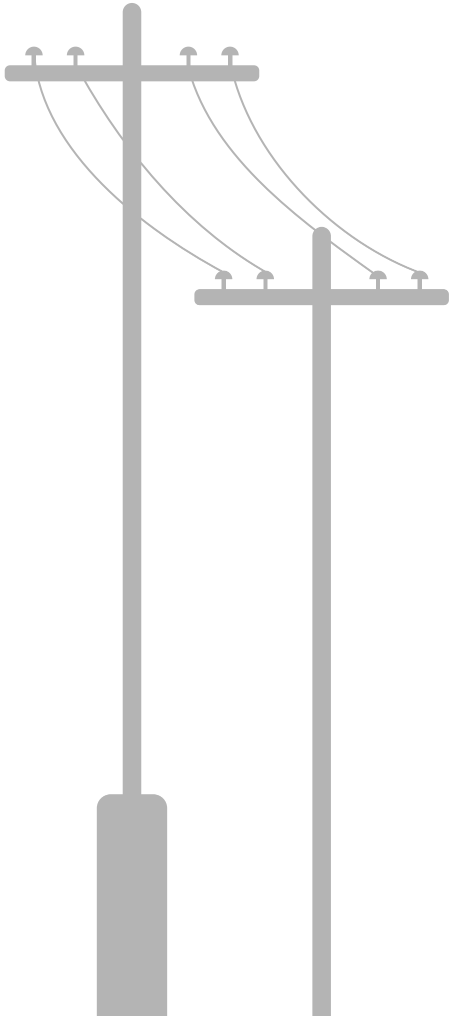


Progress Review

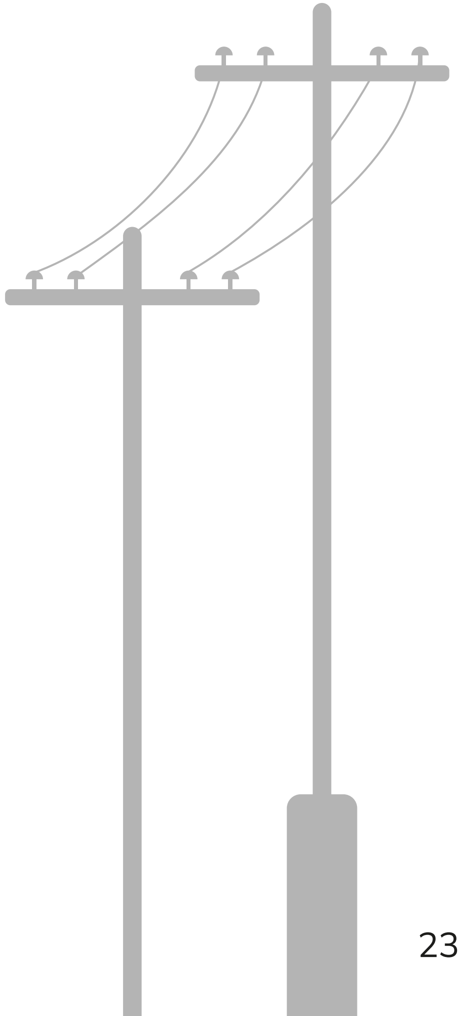
- Created simulated electric grid consisting of a distribution model and transmission model.
- Project is implemented within a containerized Docker solution.
- Results of the electric grid simulation are displayed with procedurally updated graphs on the frontend webpage.
- Frontend includes archive mode, allowing users to view past simulations.
- Frontend allows users to download simulation graphical images and simulation CSV data.
- Implemented line tripping cyber attack with high, medium, and low risk variations.
- Created scalable electric vehicle load model that outputs data in a CSV format.

Future Steps

Challenges
Implementing variable loads over a 24 hour period on the Santa Fe distribution model.
Integrating electric vehicle model load on the Santa Fe distribution model.
Implementing the ability to upload and use a custom distribution model.
Implementing more cyber attacks.
Database for archive mode.



Thank You



News Sources

https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2023/12/11/report--chinese-hackers-targeted-texas-power-grid--hawaii-water-utility--other-critical-infrastructure-

https://www.politico.com/news/2023/09/10/power-grid-attacks-00114563

https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/

https://www.wftv.com/news/local/increase-cyberattacks-our-power-grid-seen-nationwide-including-orange-county/J4AP76IZLZBKHADGYXXOMEIMWM/