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

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 cause significant damage. This damage includes outages, equipment damage, and standstill in sectors that rely on the power grid.

Solution: Creation of a tool to test the impact of cyber attacks against a simulated electrical grid.

Who does it help?

- Utility companies
- Power grid consultancies
- City engineers and workers
- The general population

LOCAL

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

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

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 | PUB

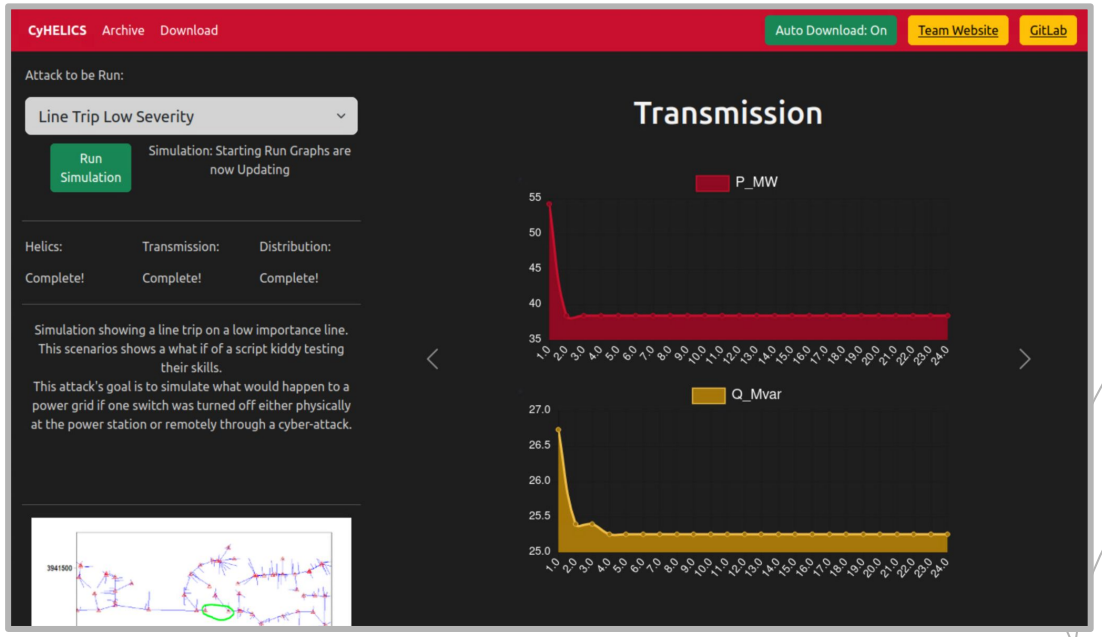
US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney

April 4, 2024 4:48 PM CDT · Updated 18 days ago

What is CyHelics?

- A tool to emulate cyber attacks on a simulated electric grid model.
- CyHelics uses 3 main software tools to run its simulations:
  - Pandapower
  - DSS-Python
  - Helics
- The simulation data is displayed in graphs on the website. The graphs and CSV data can also be downloaded from the webpage.



Requirements

Design

- 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.
- The EV load profile will be connected as a load on the Santa Fe distribution grid.

Attacks

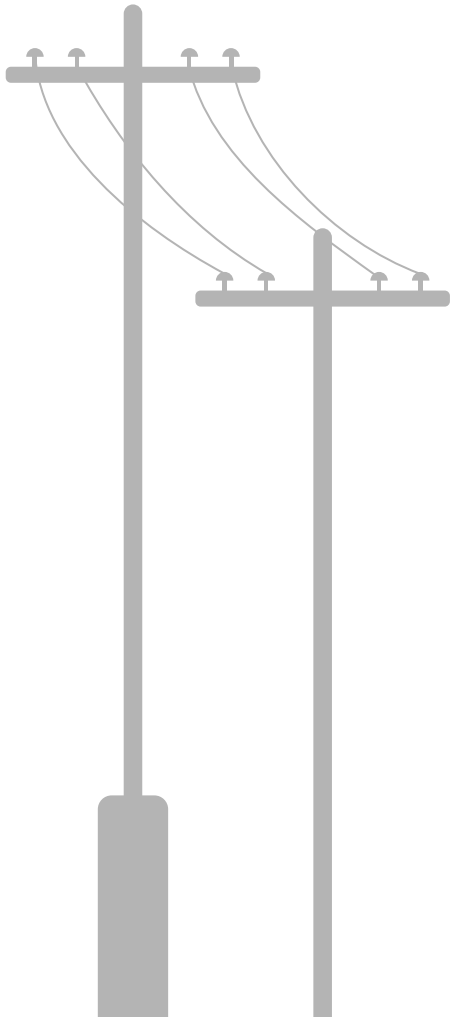
- There must be at least one attack.
- The attacks must have various severity levels.
- The attacks will be focused with an emulation perspective.

Grid

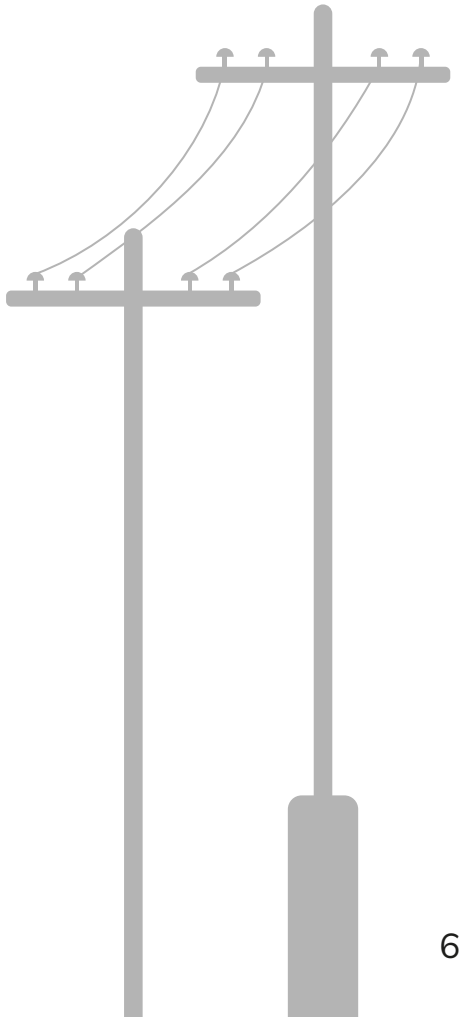
- Power Grid will include multiple load types.
- Distribution Grid must have at least 50,000 nodes.
- Create & simulate a simple transmission grid.
- Use HELICS to combine multiple substream programs and run concurrently.
- Use HELICS to model a 500 electric vehicle load profile within Sante Fe.

Frontend

- Show results of simulation.
- Frontend must have downloadable packages for results.
- Frontend must have an archive mode to quickly look at effects of cyber attacks.
- Frontend must have a continuous graph.

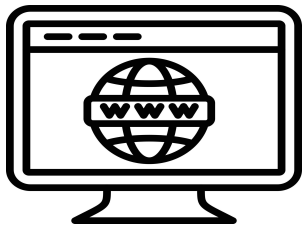


Implementation Details



Electric Grid Design Overview

Frontend Web Page



Web page displays true and reactive power from the simulation.

DSS-python is used to run the Santa Fe distribution model from BetterGrids.org.

Helics is the communication between grid programs, and handles the EV simulation.

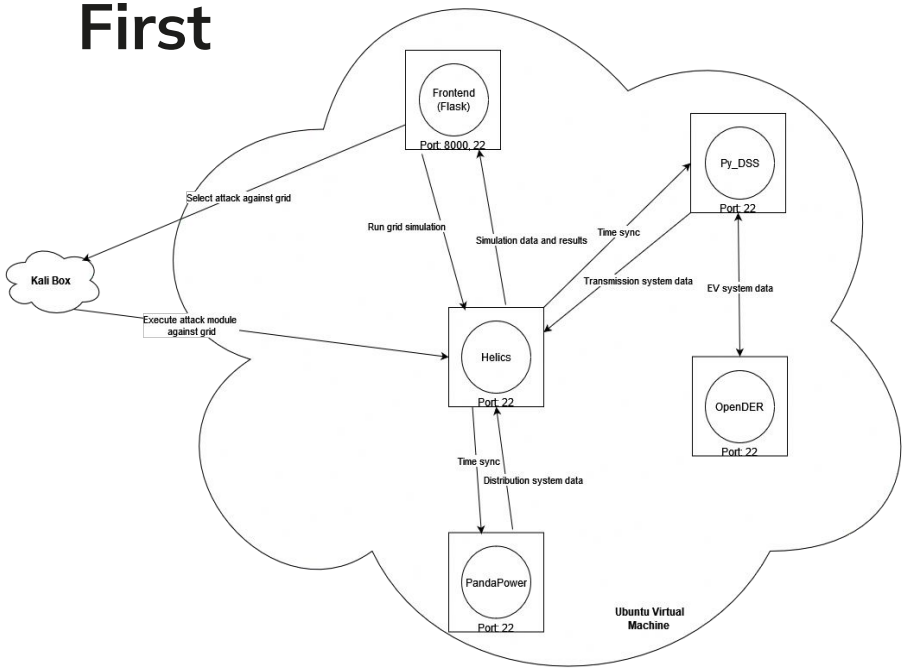
Pandapower simulates a transmission system.

Grid Simulation

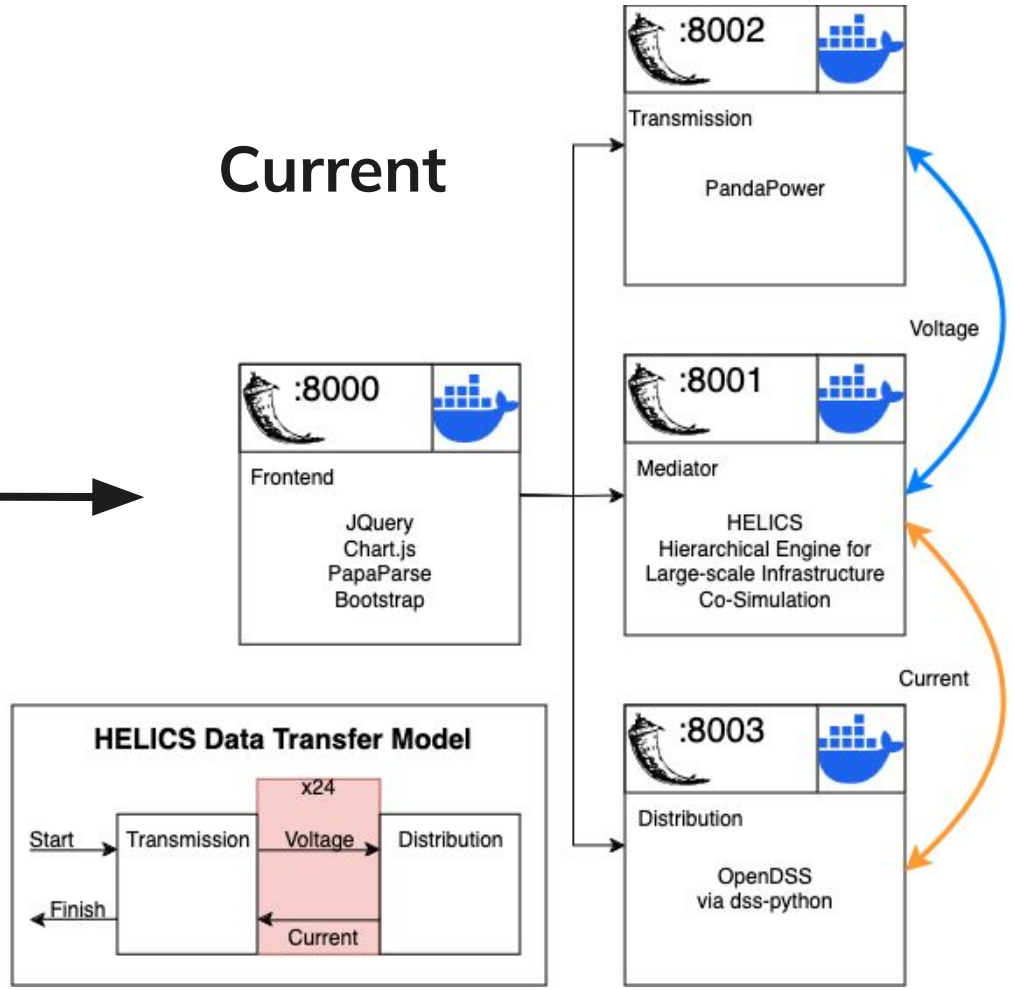
- The simulation systems are run within individual Docker images running Ubuntu.

Docker Design Diagram

First

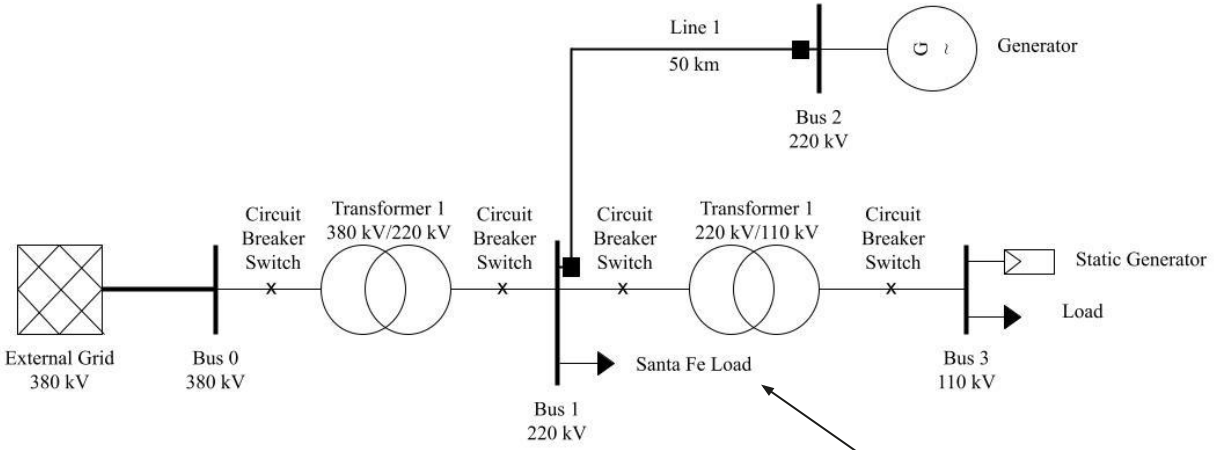


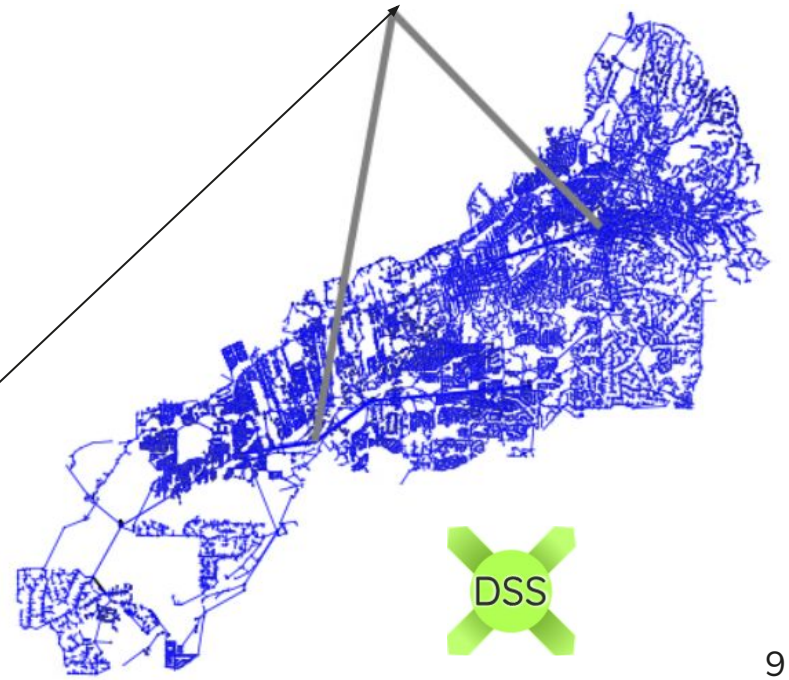
Current



Electric Grid Model

- Transmission simulation - PandaPower
- Distribution simulation - DSS-Python
  - Santa Fe distribution model from BetterGrids.org.
- Helics is used to facilitate the communication between the two softwares and simulate electric vehicle load profiles

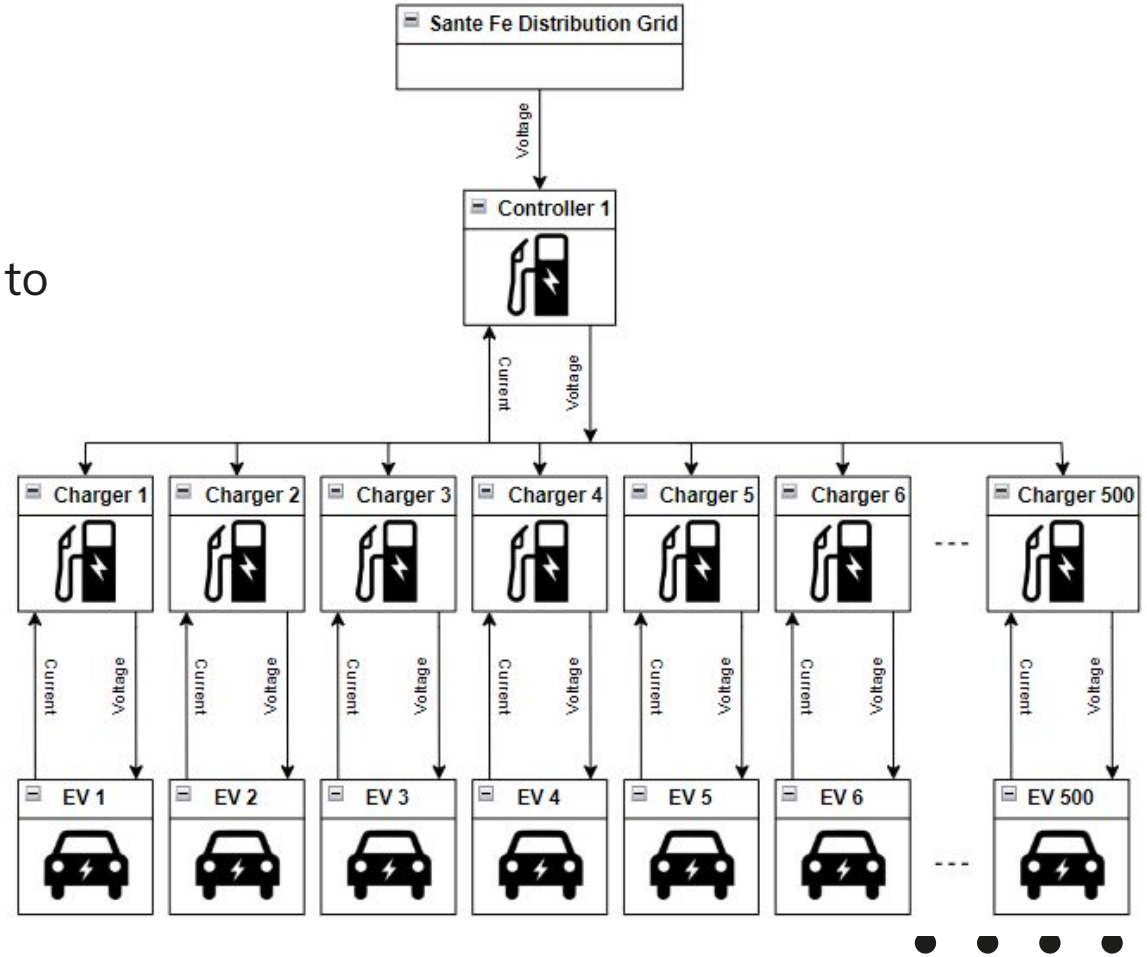




HELICS

EV Model

- The load profile consists of:
  - 500 electric vehicles
  - 500 charging stations
  - A singular controller that is connected to the Santa Fe distribution grid



Attacks

Data Integrity Attacks

- Maliciously manipulates measurements or control signals
- Severity - High

Denial-of-Service Attacks

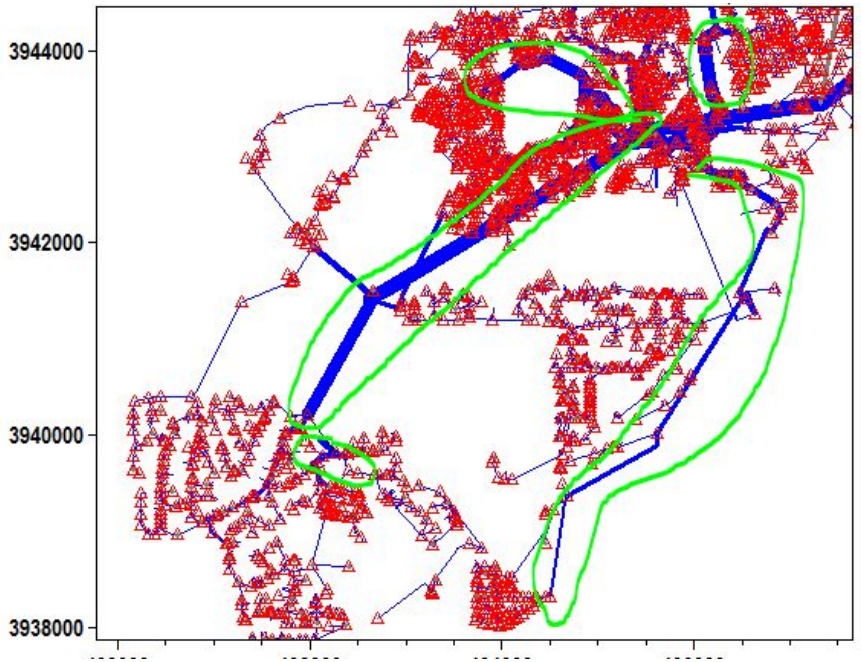
- Maliciously causes a slowdown of grid infrastructure
- Severity - Low

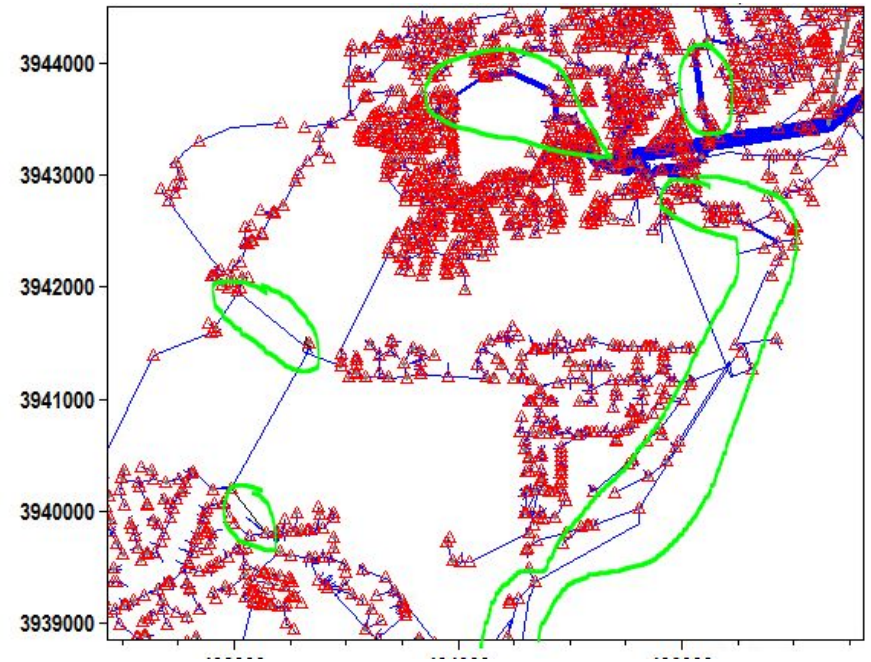
Ramp Attacks

- Maliciously causes a large power imbalance at the generator
- Severity - Moderate

How we attack our grid

- Constraints with the Dockerized environment means emulation instead of simulation.
- Came up with 3 different types of attack outcomes focused on the electric grid:
  - Selective line tripping (low, medium, and high severity)
  - Generator short-circuit
  - Load-Shedding





Security Concerns and Countermeasures

- Malicious actors can see where faults are in the power grid.

- Application is offline, no way to breach it from the internet.

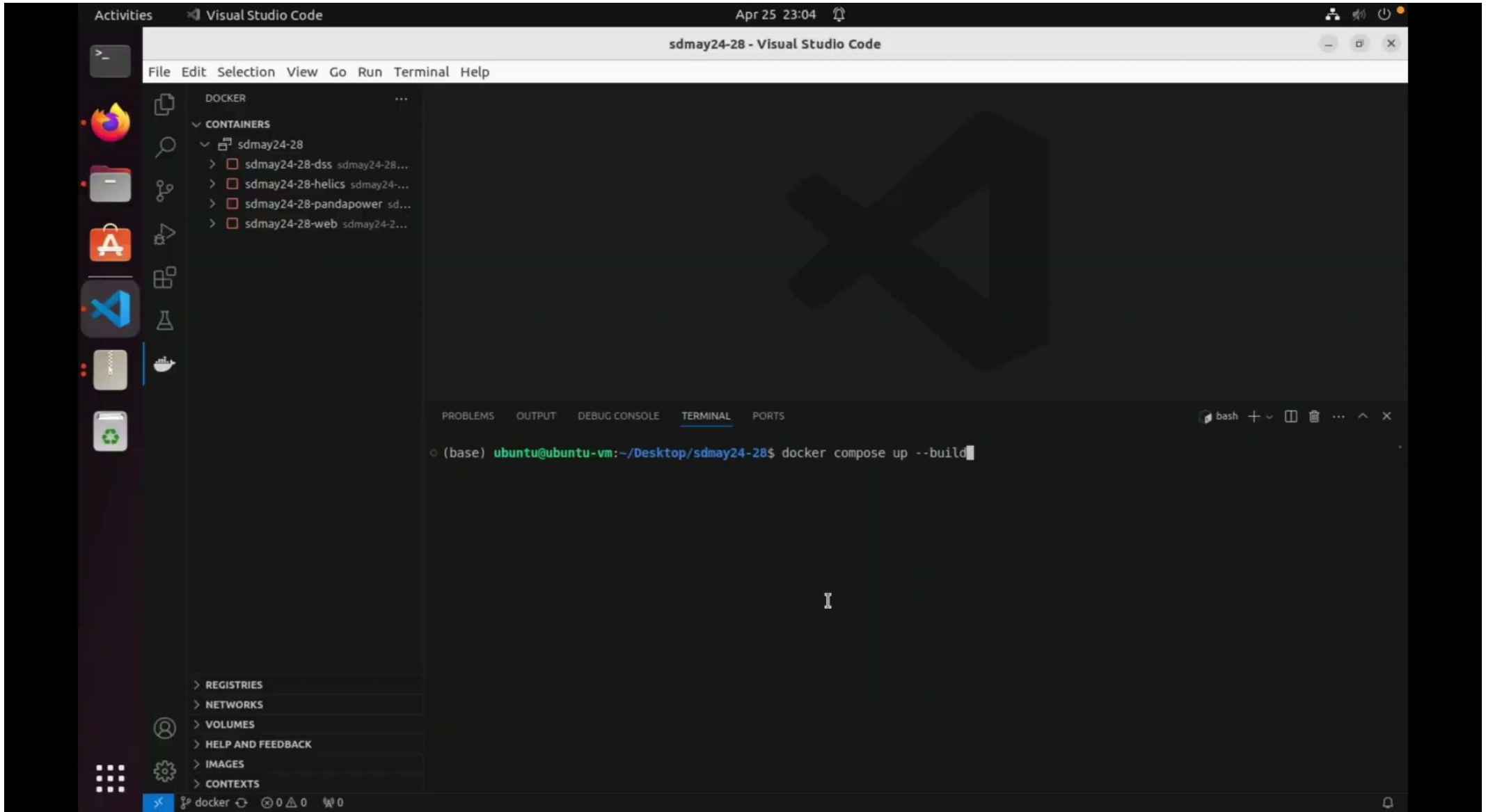
- Application is dockerized - limiting its malicious use on a host computer.

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

Demo


Activities
Visual Studio Code
Apr 25 23:04
sdmay24-28 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
DOCKER
CONTAINERS
sdmay24-28
sdmay24-28-dss sdmay24-28...
sdmay24-28-helics sdmay24-...
sdmay24-28-pandapower sd...
sdmay24-28-web sdmay24-2...
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
bash
(base) ubuntu@ubuntu-vm:~/Desktop/sdmay24-28$ docker compose up --build
REGISTRIES
NETWORKS
VOLUMES
HELP AND FEEDBACK
IMAGES
CONTEXTS
docker

Progress Review

Design

- ✅ 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.
- ❌ The EV load profile will be connected as a load on the Santa Fe distribution grid.

Attacks

- ✅ There must be at least one attack.
- ✅ The attacks must have various severity levels.
- ✅ The attacks will be focused with an emulation perspective.

Grid

- ✅ Power Grid will include multiple load types.
- ✅ Distribution Grid must be have at least 50,000 nodes.
- ✅ Create & simulate a simple transmission grid.
- ✅ Use HELICS to combine multiple substream programs and run concurrently.
- ✅ Use HELICS to model a 500 electric vehicle load profile within Santa Fe.

Frontend

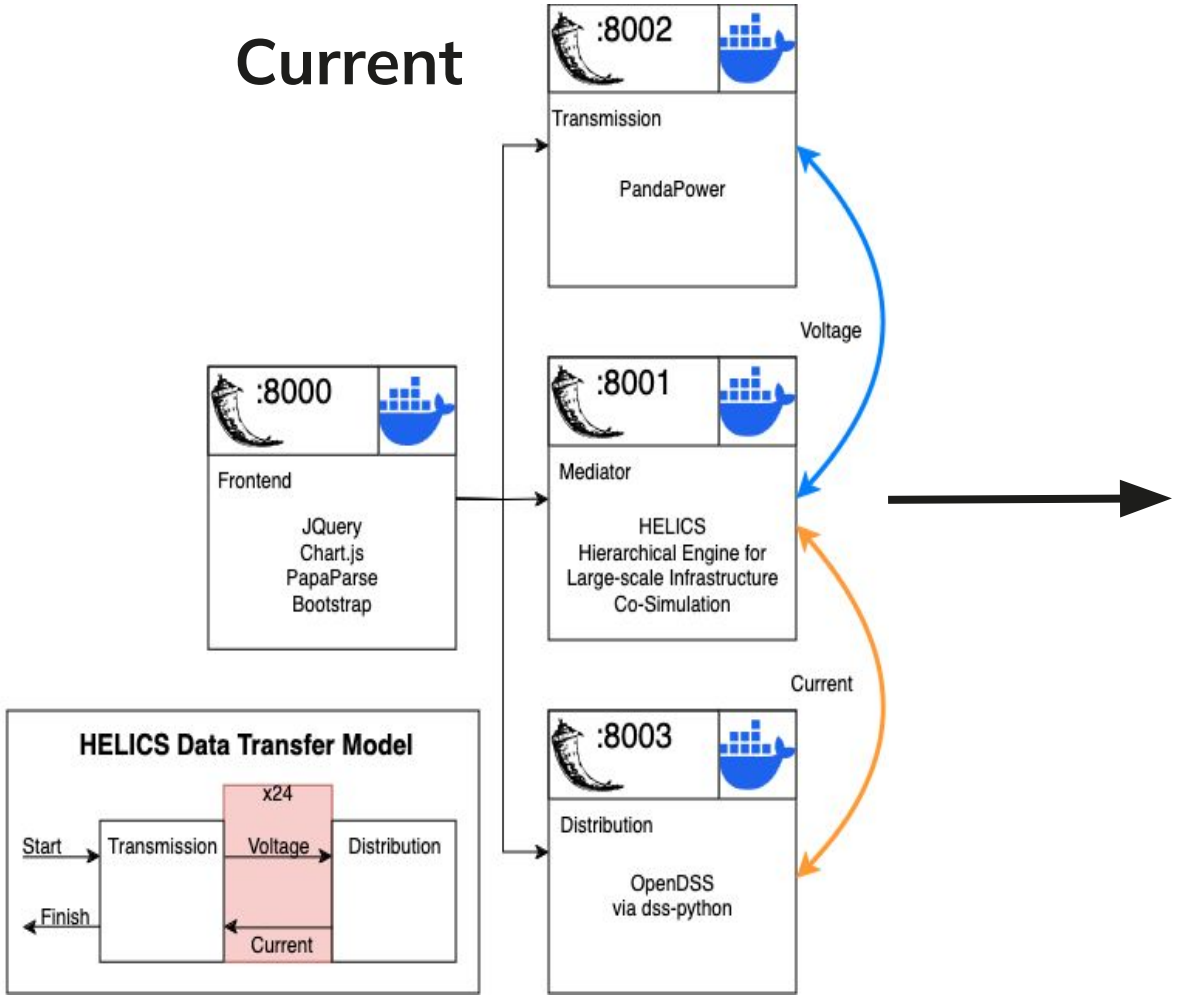
- ✅ Show results of simulation.
- ✅ Frontend must have downloadable packages for results.
- ✅ Frontend must have an archive mode to quickly look at effects of cyber attacks.
- ❌ Frontend must have a continuous graph.

Future Development

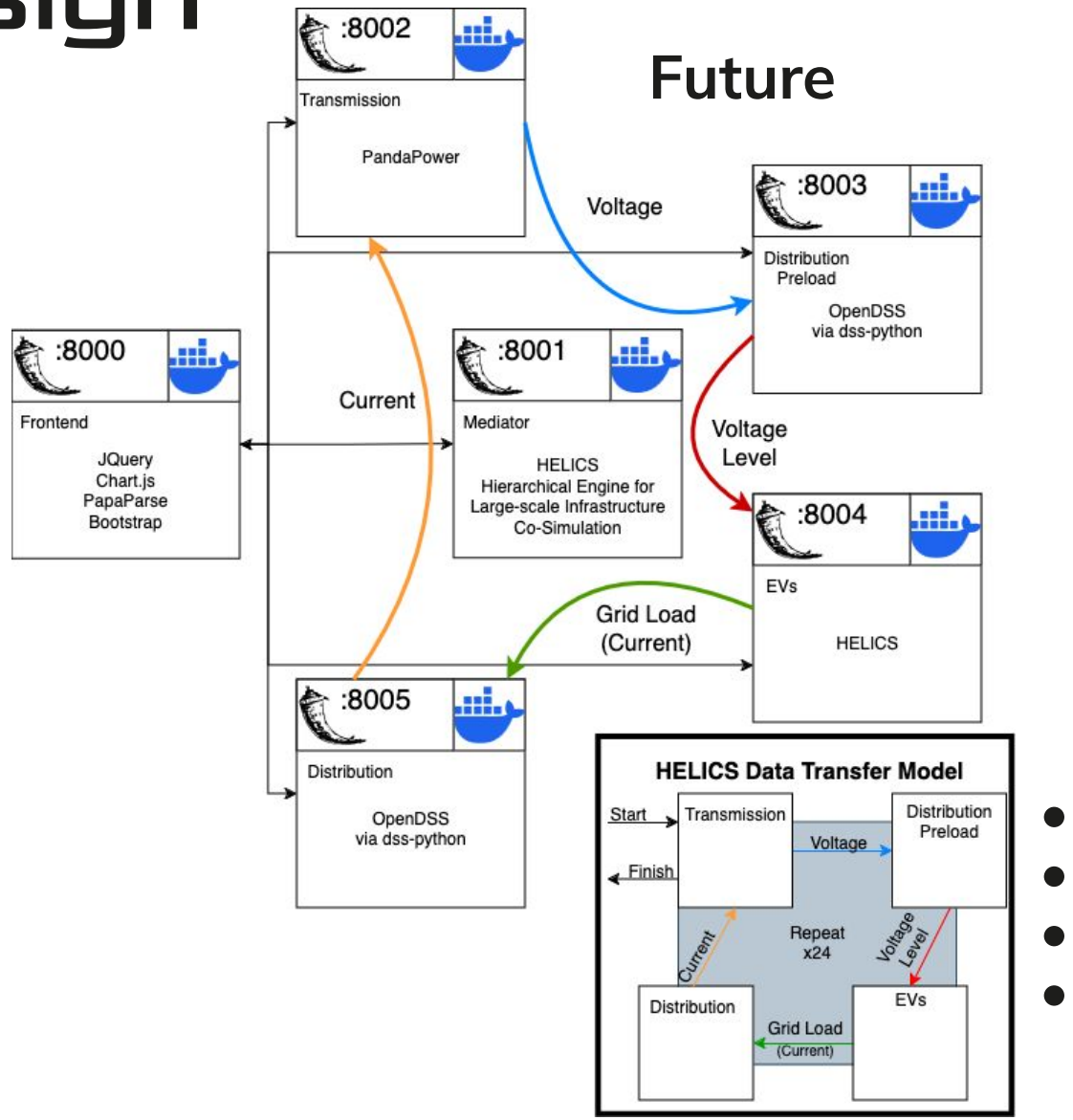
EV	Integration of the electric vehicle load profile into the Santa Fe distribution model.
Power Grid Variable Load	Implementing variable loads over a 24 hour period on the Santa Fe distribution model.
Various Grids	Implementing the ability to upload and use a custom distribution model.
Transmission Grid	Creating a more accurate PandaPower transmission grid
More Attacks	Implementing more cyber attacks - short circuit, botnet DoS, etc.
Frontend database	Implement a database for archive mode data.

Future Docker Design

Current



Future



Thank You

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/

https://clipart-library.com/img/1851344.png

https://www.pinclipart.com/picdir/big/14-147675_hat-clipart-builder-construction-worker-helmet-clipart-png.png

https://static.vecteezy.com/system/resources/previews/005/089/757/original/webpage-icon-style-vector.jpg

https://www.flaticon.com/free-icons/attack

https://afdc.energy.gov/evi-x-toolbox#/evi-pro-ports

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.