APPLICATIONS OF SIMULATION IN EVALUATION OF SCADA AND ICS SECURITY

BRANDT REUTIMANN

MOTIVATION

- Industrial control systems are a highly target rich environment
  - Large networks with multiple interacting parts
  - Can span large geographical areas
  - Legacy components, and a “if it’s not broke, don’t fix it” approach
- A large amount support critical infrastructure
  - Gas pipelines, power plants, manufacturing centers
  - Making them desirable attacks for terrorists, nation states and foreign actors

MOTIVATION CONT.

- Testing these systems for safety is a common practice
  - Researched for several decades
  - Refined to prevent harm to workers, and maintain availability
- Many of these safety processes are not yet refined for a world of cyberthreats
- Testing on live versions of these systems can be dangerous, expensive and difficult
  - In one report, the use of ping sweeps caused a robotic arm to swing on a factory floor and in another caused a system failure that resulted in over $50,000 worth of damage to equipment

David P Duggan. Penetration Testing of Industrial Control Systems. Sandia National Laboratories, page 7, 2005.

USING SIMULATION TO ADDRESS TESTING ISSUES

Simulating SCADA systems is not a new practice

Carnegie Melon's SCADASim is commonly used for hands on training, and modeling various sorts of critical infrastructure

Other works have made their own attempts to simulate SCADA Systems

C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim—A Framework for Building SCADA Simulations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011, doi: 10.1109/TSG.2011.2162432.

Thomas H Morris, Zach Thornton, and Ian Turnipseed. Industrial Control System Simulation and Data Logging for Intrusion Detection System Research.7th Annual Southeastern Cyber Security Summit, page 6, 2012.

Physical SCADA Testbeds are also common

Thomas Morris, Anurag Srivastava, Bradley Reaves, Wei Gao, Kalyan Pavurapu, and Ram Reddi. A control system testbed to validate critical infrastructure protection concepts. International Journal of Critical Infrastructure Protection, 4(2):88–103, August 2011.

WHERE DOES SIMULATION FALL SHORT?

- Fidelity and accuracy to real world models
  - Many of these simulation architectures are developed by computer scientists without the proper engineering perspectives
- Simulations may not consider a full scope of attacks
  - Denial of service and network-based attacks are commonly researched
  - Small body of work on control loop and feedback attacks
- Lack of modularity
  - Systems may be designed to simulate several different physical SCADA models
  - However, they don’t integrate existing engineering simulators
  - Or have extensible designs that allow hybrid and real PLCs into the model
- Previous literature has not investigated software for simulating gas systems
  - Gas systems play a large role in electrical power generation
  - Simulating gas systems is a primary focus of our work

WHY BUILD ANOTHER SIMULATOR THEN?

- Where our work fits in
  - Designing and architecting the simulator from the ground up to be modular
    - Being able to integrate different physical simulators, virtual and real PLCs, and different HMI infrastructures
    - Integrating several different SCADA network protocols (Ex: Modbus, and DNP3 in future iterations)
  - Allowing the integration of existing simulation infrastructures
    - MATLAB/SIMULINK
    - In future work: OpenDSS, PowerWorld, etc.
  - Consulting with engineers and cybersecurity experts alike to determine important design considerations
    - Which attacks should be explored?
    - How do these physical systems operate in real world scenarios ?

IMPORTANT CONSIDERATIONS FOR DEVELOPING SCADA SIMULATIONS

INTEGRATING WITH EXISTING PHYSICAL AND ENGINEERING SIMULATORS

- In our preliminary case study we use a MATLAB/SIMULINK/SIMSCAPE stack to model the dynamics of gas pipelines
- Using vetted and existing simulators prevents us from reinventing the wheel, and gives us hyper-realistic mathematical models
- Using a highly extensible simulator like MATLAB/SIMULINK also makes it easy to model other physical systems such as electrical grids, but could even be expanded to simulate manufacturing or heavy vehicle security

IMPORTANT CONSIDERATIONS CONT.

Validation methodologies

How do we validate that our physical models and control schemes are realistic?

Some strategies could be to use different types of modeling, mathematics, and even packet capture comparisons

In our work we consult with gas system experts and engineers to determine whether our physical pipelines and control schemes are representative of real systems

Scaling simulation infrastructures

How can we scale these simulations to represent large scale systems such as the entire Colorado gas distribution pipeline?

Is there a computationally efficient way to do this without losing accuracy?

IMPORTANT CONSIDERATIONS CONT.

Simulating long term system behavior

Being able to simulate the behavior over several, days weeks or months can be valuable

Our gas pipeline model runs a week of pipeline simulation in about 2 – 3 minutes

However, this long-term simulation can lead to a plethora of timing issues in the model

Integrating hardware in the loop

Surveys of SCADA simulation have shown that hybrid models integrating real PLCs and some virtual PLCs can help reach the best of both worlds

This is still a work in progress for our model

Network simulation

Being able to model several different types of network architectures is also critically important and is also a goal of our future work

CYBERSECURITY AND OUR SIMULATION

Currently our model can handle two main types of attacks

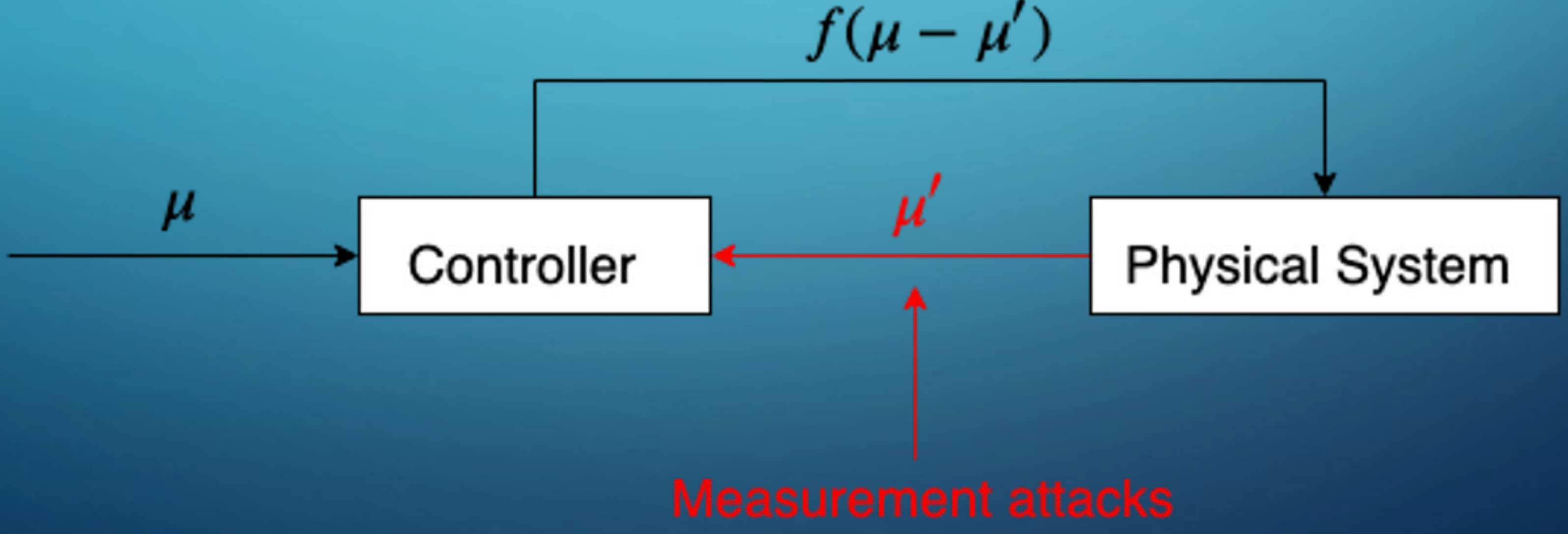
- Measurement attacks
- Command injection attacks
- Other control loop centered attacks

In future work we hope to be able to model:

- Ransomware
- Denial of service
- Network protocol-based attacks
- Malware and worm propagation
- Data Exfiltration

MEASUREMENT ATTACKS AND CONTROL LOOP FEEDBACK

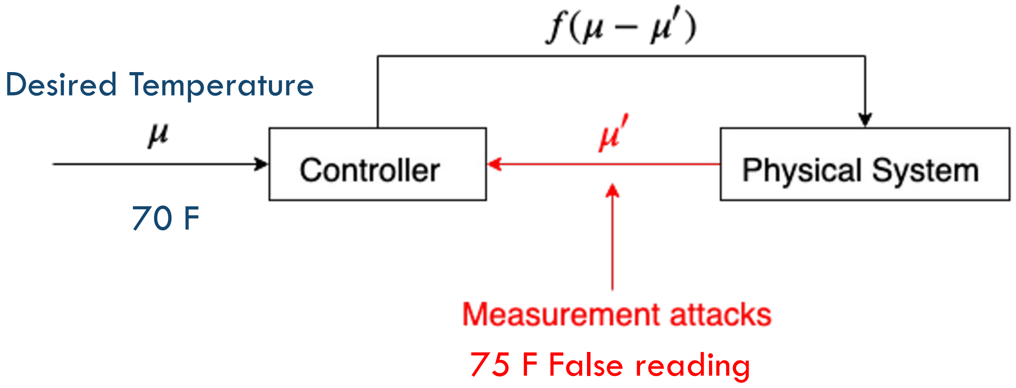
- Measurement attacks work by compromising measurement feedback in the control loop
- This causes the controller to make decisions based on false information



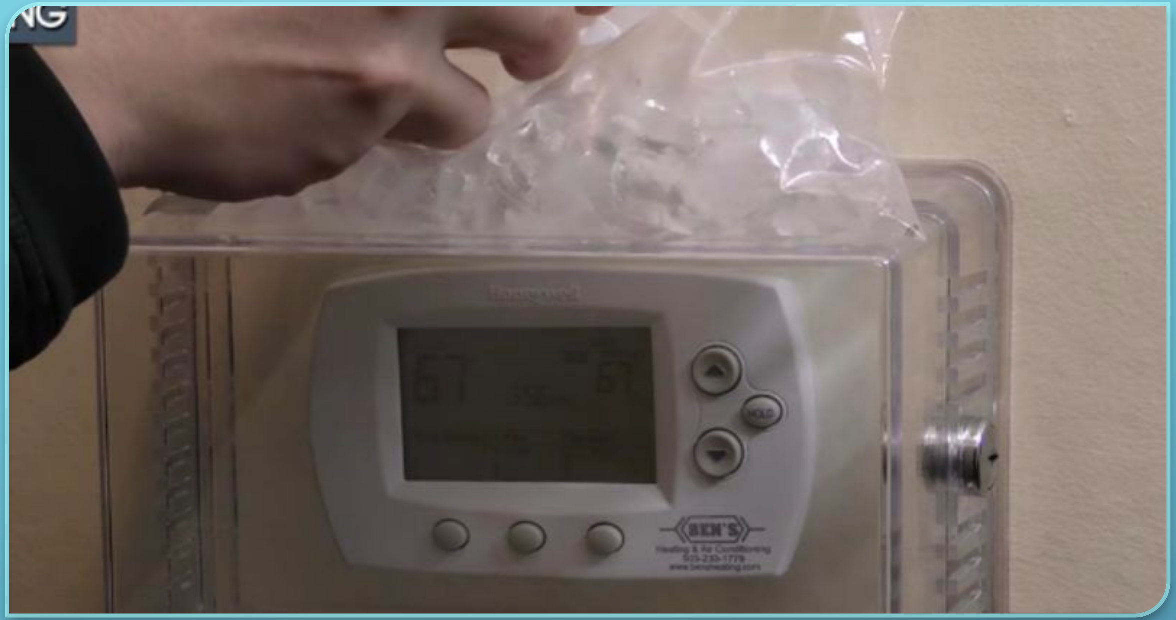
THERMOSTAT EXAMPLE

Example:
It’s a cold day at 40 F and your thermostat doesn’t seem to be turning on the heat… why?

System believes that the temperature is 5 F above desired.
Makes no adjustment.



- Your thermostat likely uses a thermometer
  - When the temperature is too low in your house it turns on the heating using your gas or electric furnace
  - What happens if this thermometer is broken?
    - If it’s falsely reading too low then your heat will always be on even when your house is already heated
    - If it’s falsely reading too high then your heat won’t come on even when it’s freezing cold



IF AN ATTACKER MANIPULATE A SENSOR…

THEY CAN CHANGE THE CONTROL BEHAVIOR

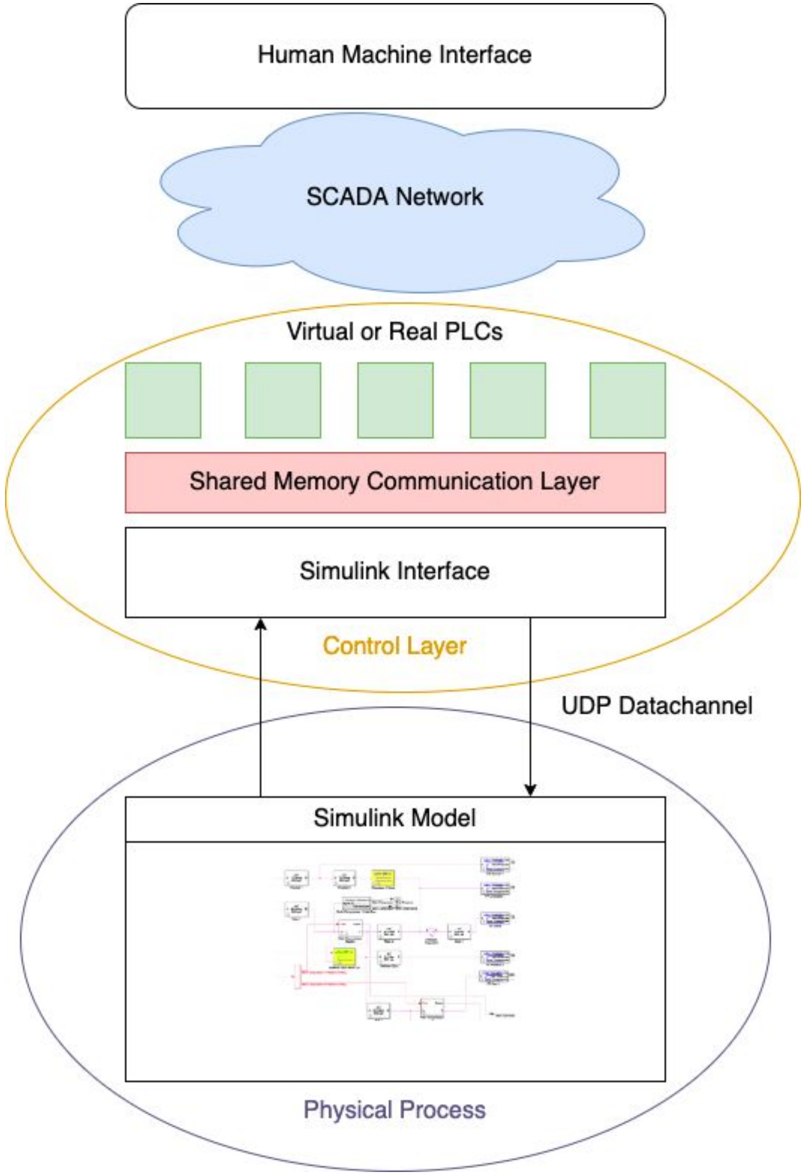
Allan, Patrick. Trick a Guard-Box Protected Thermostat Into Warming Up the Office. *Lifehacker*. Jan 19, 2016. https://lifehacker.com/trick-a-guard-box-protected-thermostat-into-warming-up-1753876434

DESIGN OF OUR SCADA SIMULATOR

- Critical parts of our design:
  - 3-layer architecture: process model, control model, and HMI or system operator
  - Interfacing with Simulink and SimScape
  - Creating realistic gas pipeline models
  - Resolving timing issues in long term simulations
  - Simulating compromises
  - Using an Oracle PLC to validate system data

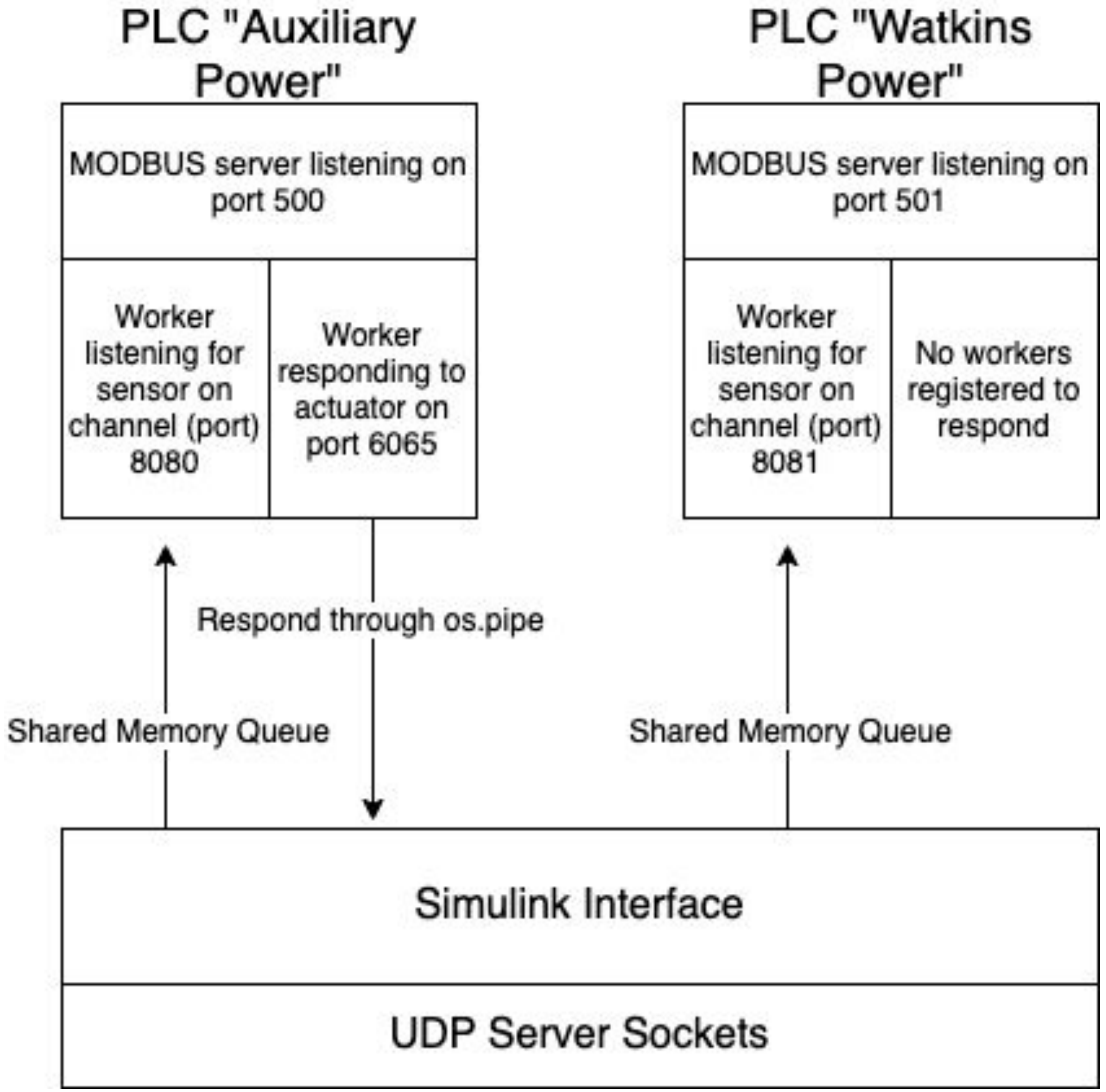
3 LAYER ARCHITECTURE

- This design separates the Simulink system into 3 main parts
  - A physical process that could be an electrical system, gas system, or some other ICS system
  - A control layer that consists of virtual PLCs, hybrid or real PLCs
  - An HMI or system operator model that interacts with the control layer



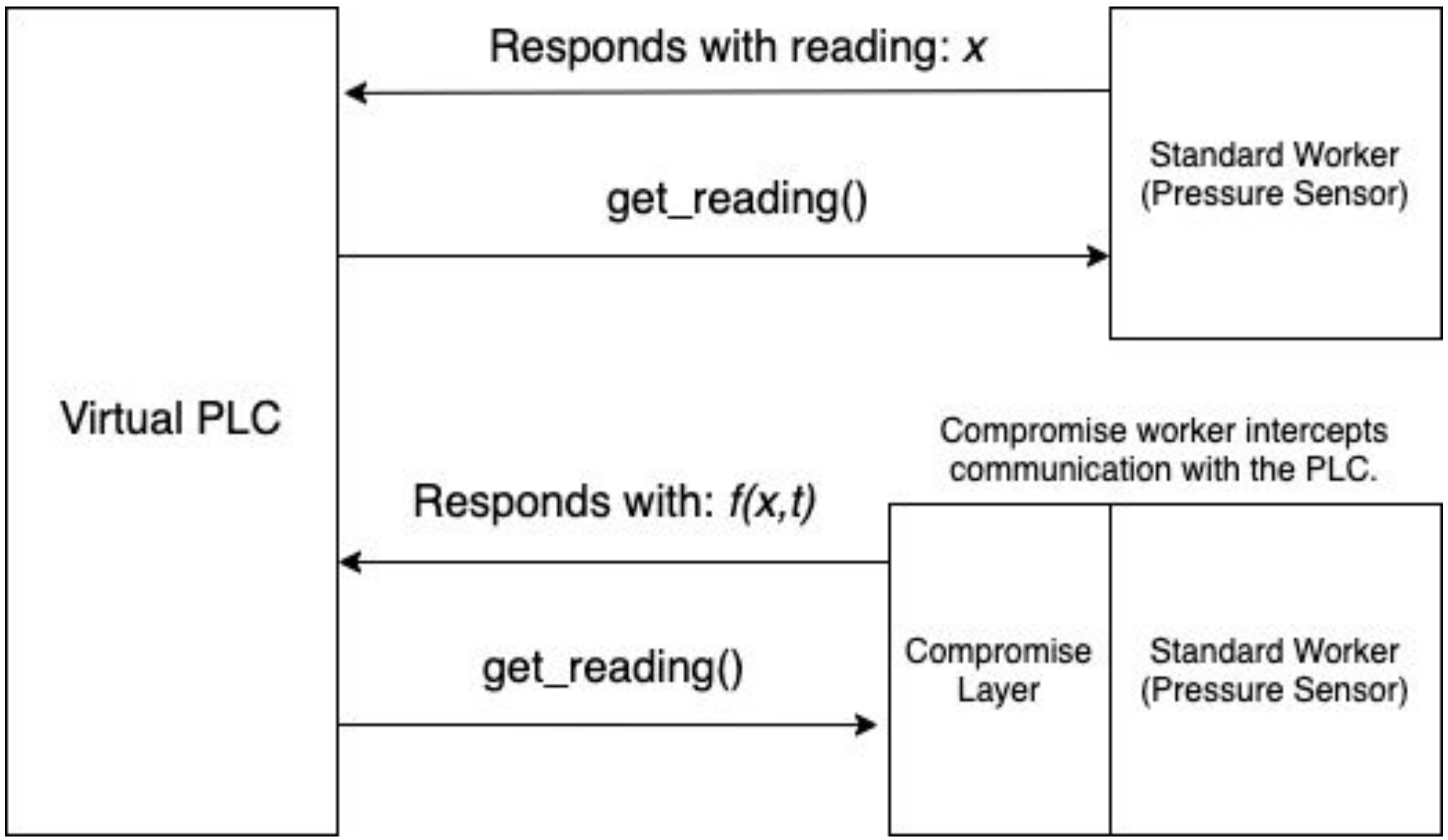
SIMULINK INTERFACE

- Simulink communicates with the interface using UDP network connections
- These connections are associated with sensors and actuators in the simulation


PLC "Auxiliary Power"
MODBUS server listening on port 500
Worker listening for sensor on channel (port) 8080
Worker responding to actuator on port 6065
PLC "Watkins Power"
MODBUS server listening on port 501
Worker listening for sensor on channel (port) 8081
No workers registered to respond
Respond through os.pipe
Shared Memory Queue
Shared Memory Queue
Simulink Interface
UDP Server Sockets

SIMULATING SENSOR COMPROMISES

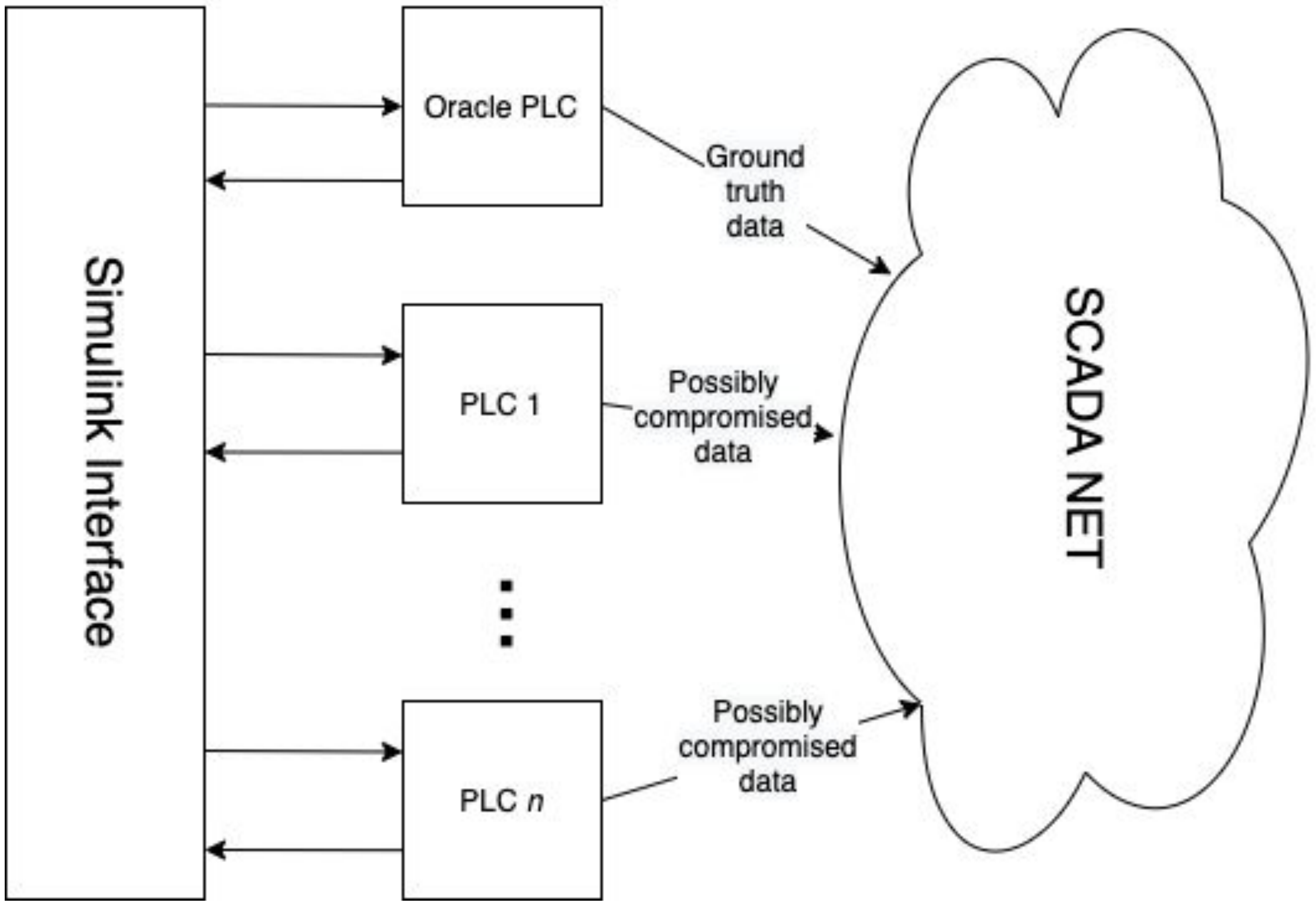
- Any sensor in the model can be marked as compromised in the configurations
- This sensor will return a modified reading as described by the function *f(x,t)* where *x* is the original sensor reading and *t* is the current simulation time



Virtual PLC
Responds with reading: *x*
get_reading()
Standard Worker (Pressure Sensor)
Compromise worker intercepts communication with the PLC.
Responds with: *f(x,t)*
get_reading()
Compromise Layer
Standard Worker (Pressure Sensor)

ORACLE PLC

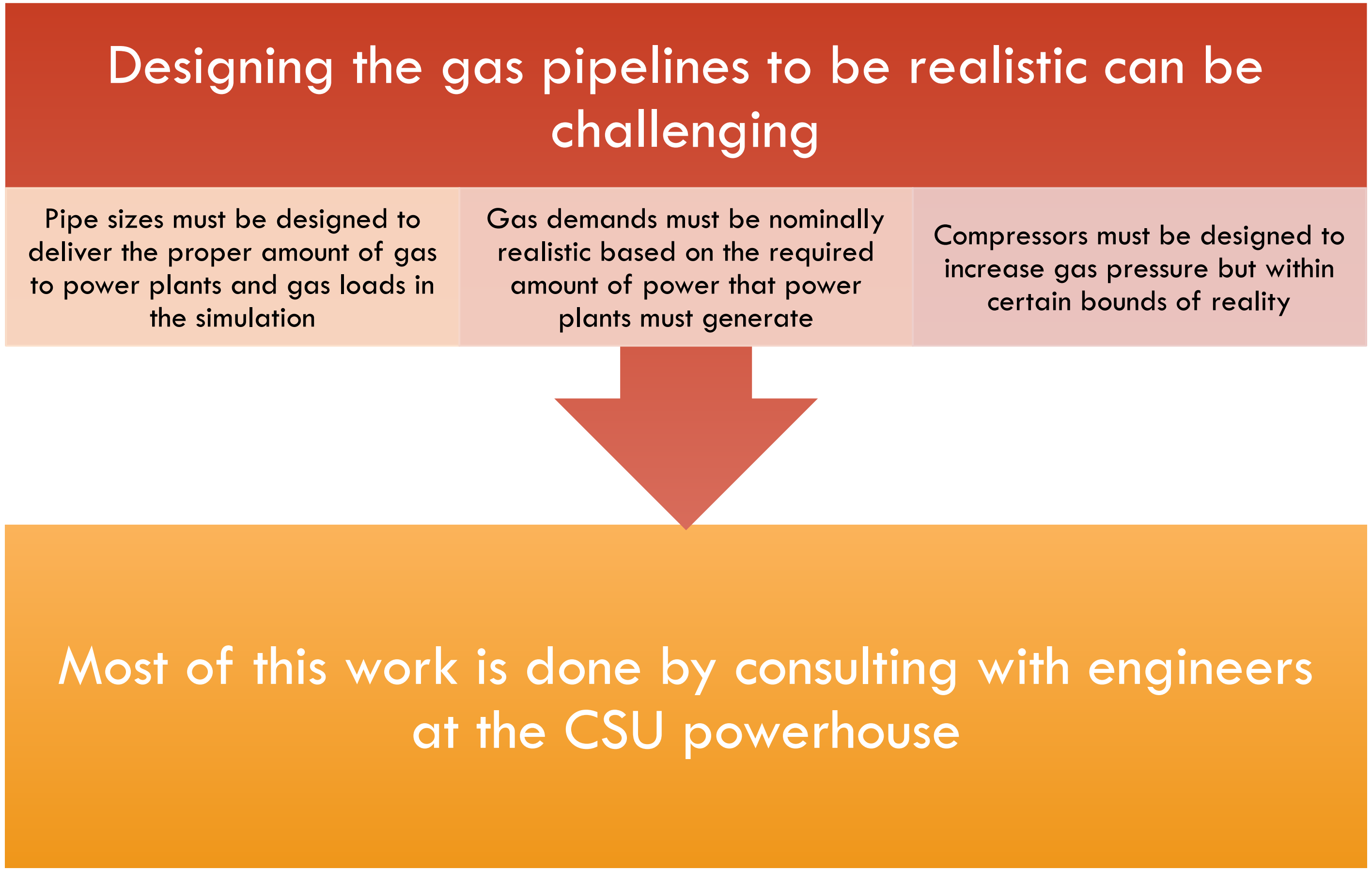
- When recording data on the operator side, we want to be able to observe both compromised and ground truth data
- The oracle PLC records all sensor data in the simulation but is never marked as compromised



PROPAGATING SIMULATION TIME THROUGH THE MODEL

- Simulation time is a concept only native to the SIMULINK/SIMSCAPE
  - As a result we must push this time throughout the model
  - Every sensor reading includes a timestamp
  - Each PLC updates its notion of the current simulation time with each new reading
  - The Oracle PLC reports simulation time to the simulation controller or HMI
- The flaw in this design is that the virtual PLCs and the frontend are always playing catch up
  - Any communication or network delays are magnified by the ratio of simulation to real time

MODELING REALISTIC GAS PIPELINES



Designing the gas pipelines to be realistic can be challenging

Pipe sizes must be designed to deliver the proper amount of gas to power plants and gas loads in the simulation

Gas demands must be nominally realistic based on the required amount of power that power plants must generate

Compressors must be designed to increase gas pressure but within certain bounds of reality

Most of this work is done by consulting with engineers at the CSU powerhouse

MODELING PIPELINE OPERATORS

Our main control model increases upstream gas pressure to meet the gas delivery demands at downstream power plants

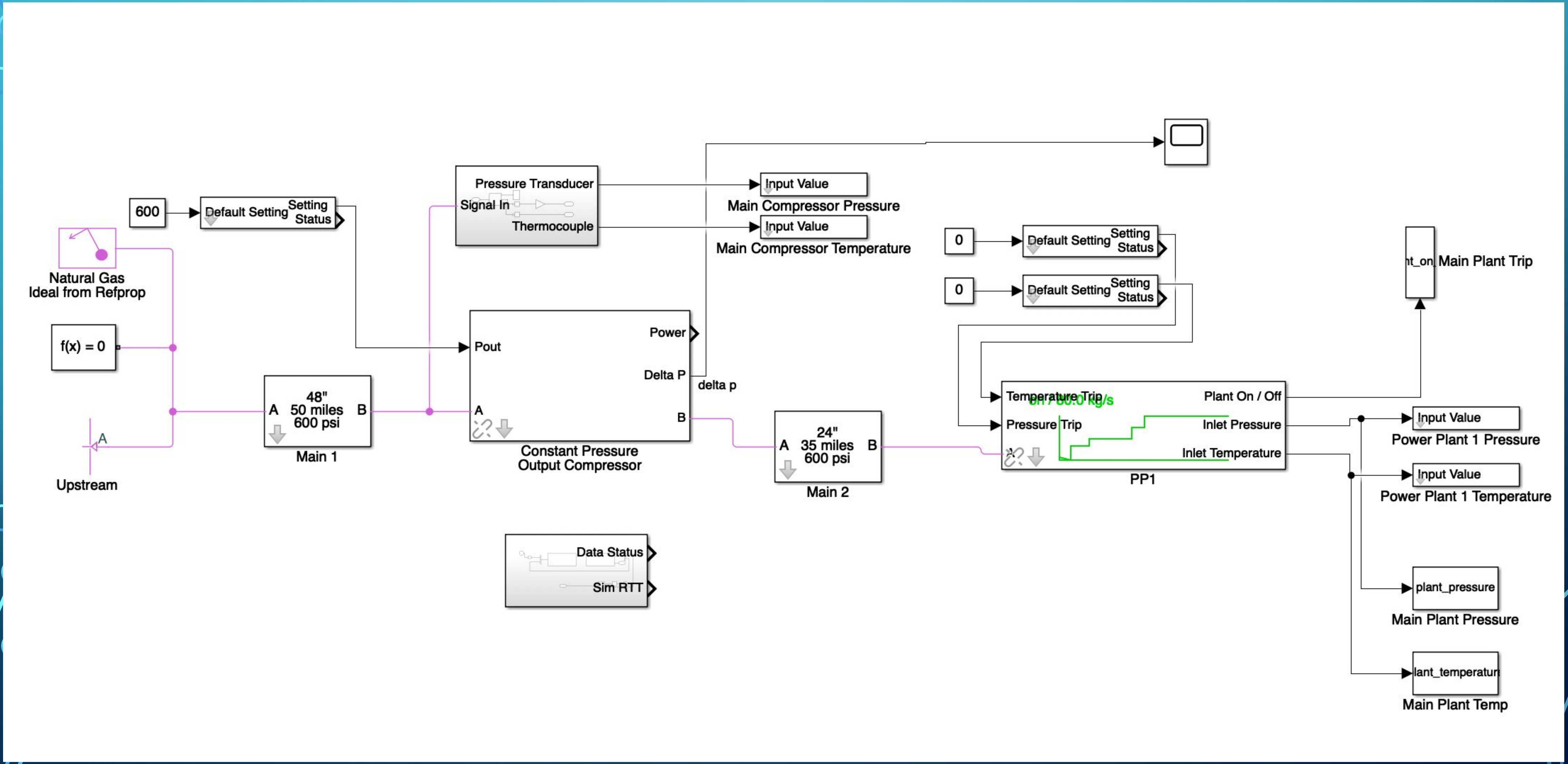
The operator observes pressure sensors and determines their difference from nominal

Looks at immediate upstream compressors and increases their compression ratio

We also need to model safety scenarios like low pressure and temperature shut-offs

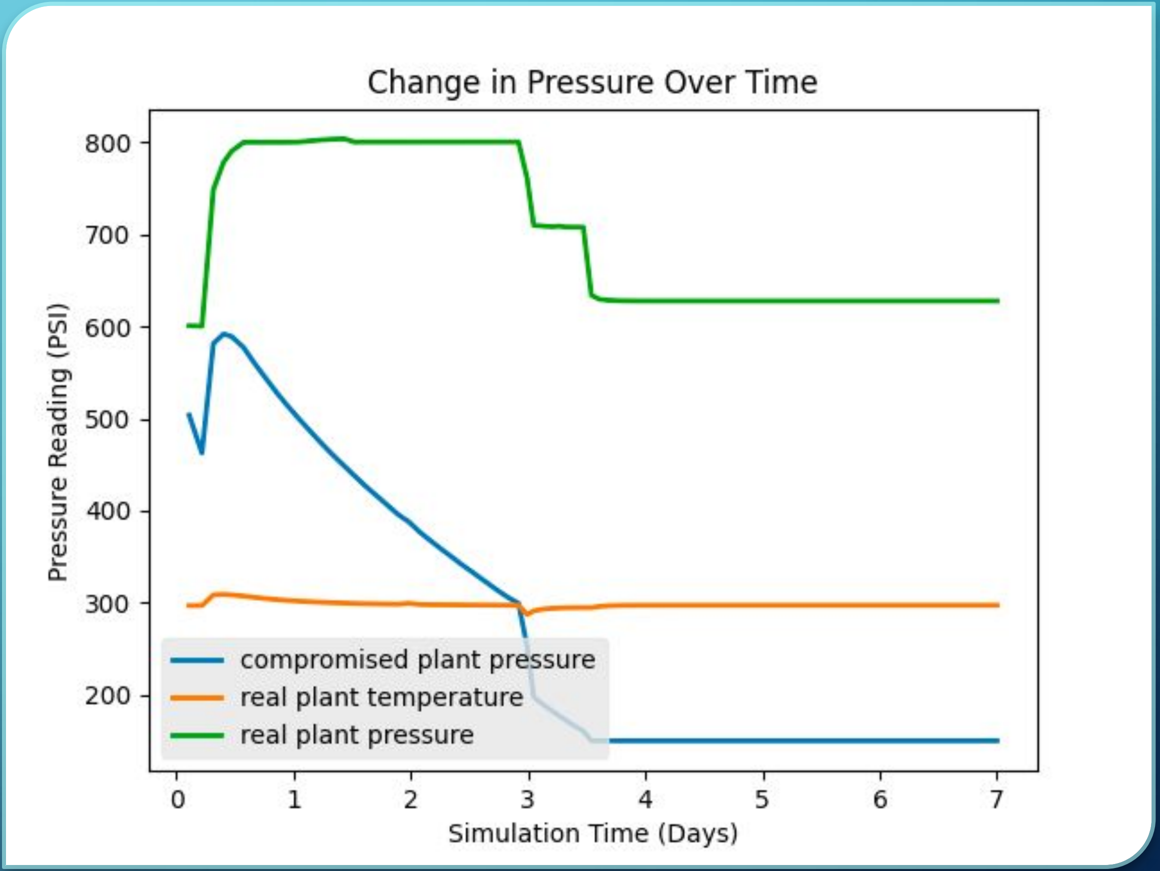
Then apply some reasonable amount of time before plants can come back online

SMALL SCALE EXAMPLE MODEL



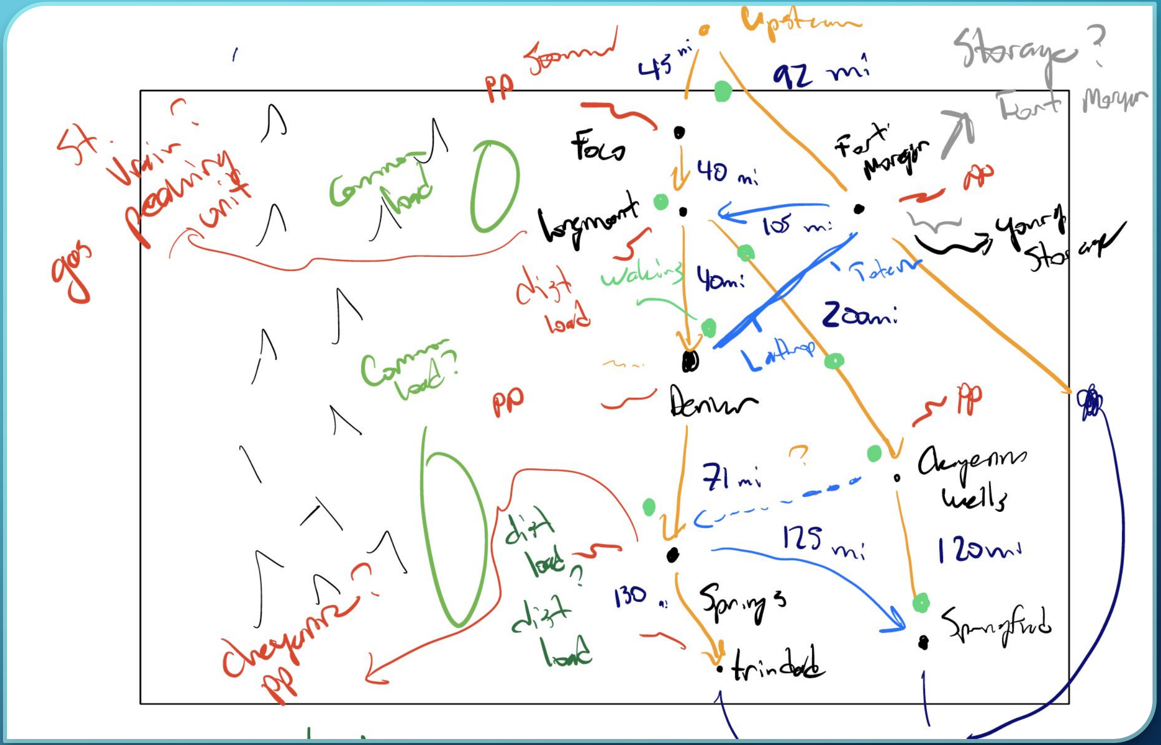
MEASUREMENT ATTACKS ON A SIMPLE MODEL

- As the compromised pressure (the fake reading falls) the operator tries to compensating by increasing the pressure upstream which is reflect by the actual pressure reading
- Note that although the compromised sensor is showing a drop in pressure the temperature remains failure consistent and even rises in some spots



DEMONSTRATING IMPACTS ON A LARGER MODEL

- To truly show the impacts of measurement attacks in a realistic manner we need a more sophisticated model
  - For this reason we designed a large-scale model that is inspired by the Colorado Front Range gas system
  - Using this model we can demonstrate measurement attacks and their affects on interdependent components in the gas system

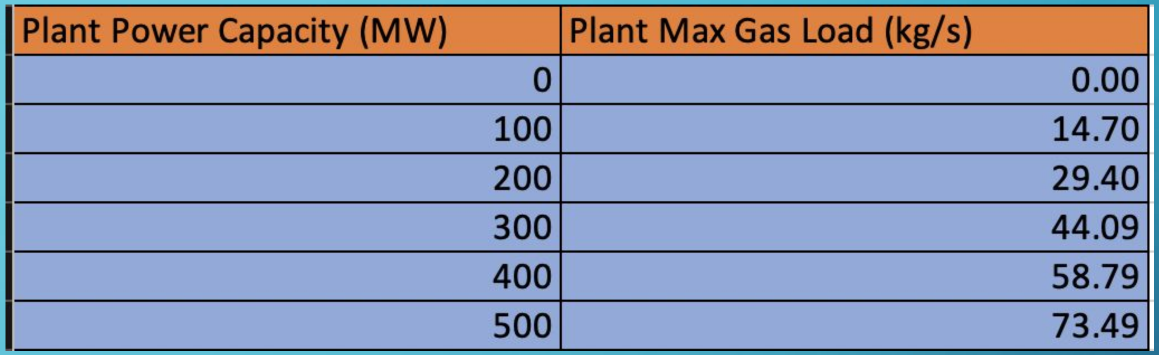


DESIGNING A LARGE-SCALE MODEL

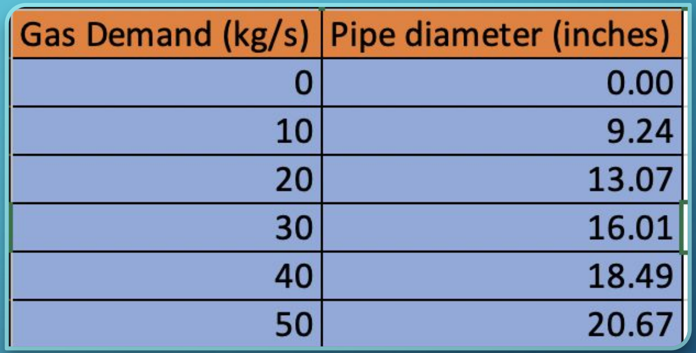
- Primary objective
  - Realistic enough that failure comes from cyberattack and not poor design
  - Does not necessarily need to be a perfect replica system
- Our system consists of
  - 12 pipe segments
    - About 1256 miles in total length
  - 9 loads, 6 of which are simulated power plants
    - Total capacity of about 2900 MW
  - 8 compressor stations

DESIGNING A LARGE-SCALE MODEL

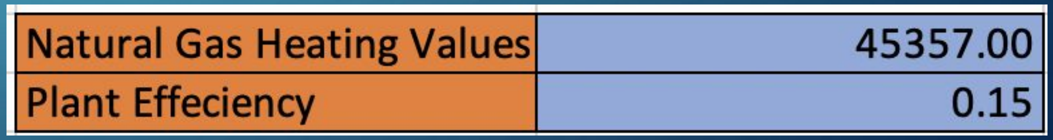
- For the location and the lengths of pipe we used a system map found on Kinder Morgan's website
    - Overlaid on a map of Colorado we extrapolated locations of power plants and gas lines
- For the size of power plants we referenced information on the Xcel energy website
    - Using a chart of gas heating values we can convert the power production in Megawatts to the required amount of gas at a powerplant
- We then design the diameter of gas pipes in the system to meet this gas demand



Plant Power Capacity (MW)	Plant Max Gas Load (kg/s)
0	0.00
100	14.70
200	29.40
300	44.09
400	58.79
500	73.49

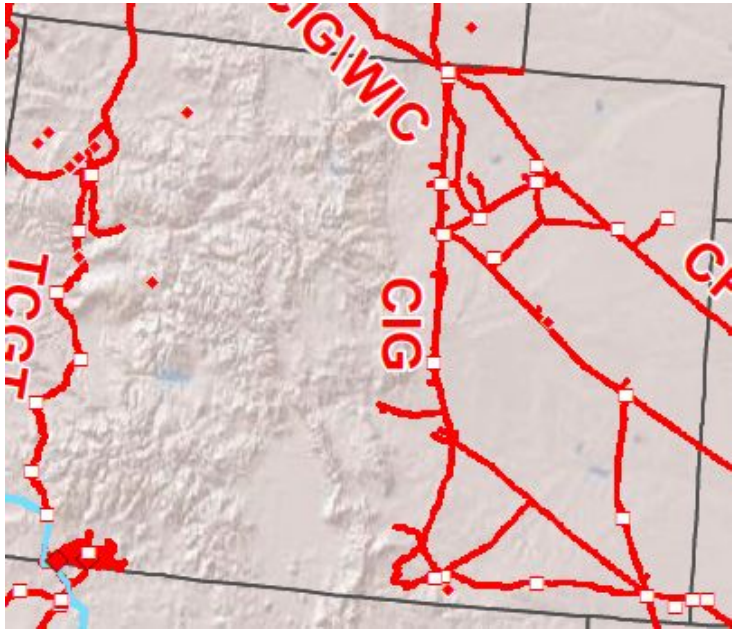


Gas Demand (kg/s)	Pipe diameter (inches)
0	0.00
10	9.24
20	13.07
30	16.01
40	18.49
50	20.67



Natural Gas Heating Values	45357.00
Plant Effeciency	0.15

DESIGNING A LARGE-SCALE MODEL CONT.



Cherokee Generating Station

Key facts:

- **Power Production Capability:** 928 megawatts
  - Unit 4: 352 MW
  - Unit 5: 168 MW
  - Unit 6: 168 MW
  - Unit 7: 240 MW
- **Commercial Operation:** Varies
  - Unit 4: 1968
  - Units 5-7: 2015
- **Generation Type:** Steam turbine and combined cycle

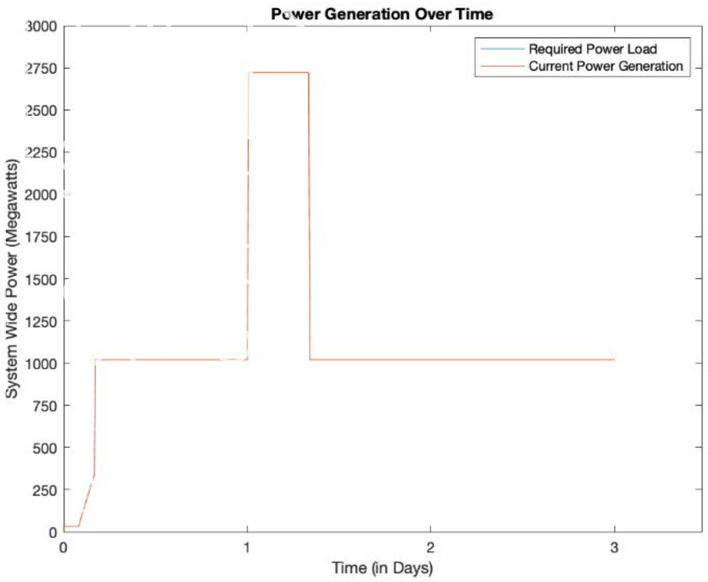


Figure 6.4: Under a period of high stress there is no loss in power if the system corrects properly.

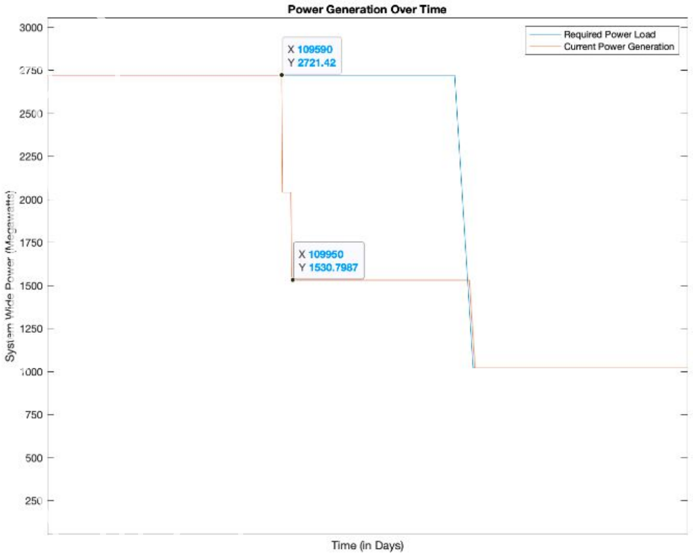


Figure 6.5: Rapid loss of power generation capability can occur without control system intervention.

SYSTEM SCENARIO

- In some places of the world it can be common for wind farms to carry a high amount of the power demand
  - Occasionally wind can die down over an hour or two, shifting load back onto natural gas power plants
  - This causes the natural gas system to ramp up gas loads very rapidly
  - Manual operators must intervene to ensure that compressors are pushing enough gas through the system
- A smart attacker can wait for a moment of high gas ramping and delay the compression
  - This can cause the system to oscillate or causing plants to trip off
  - This can lead to cascading failures through the system as power production must be taken over by other gas power plants
- This is the scenario we've tried to model
  - A successful attack will cause plants to fail within this 12-hour period of high stress

SINGLE POINT OF FAILURE EXPERIMENTS

- The first thing we explored on the system was inserting lies about inlet pressure on each power plant in the system
  - Maintaining the reading at nominal pressure during the simulation
- Out of 6 total trials, we had one ”successful” attack
  - Falsified readings at the Fort Collins plant caused Fort Collins and later Fort Morgan plants to go offline

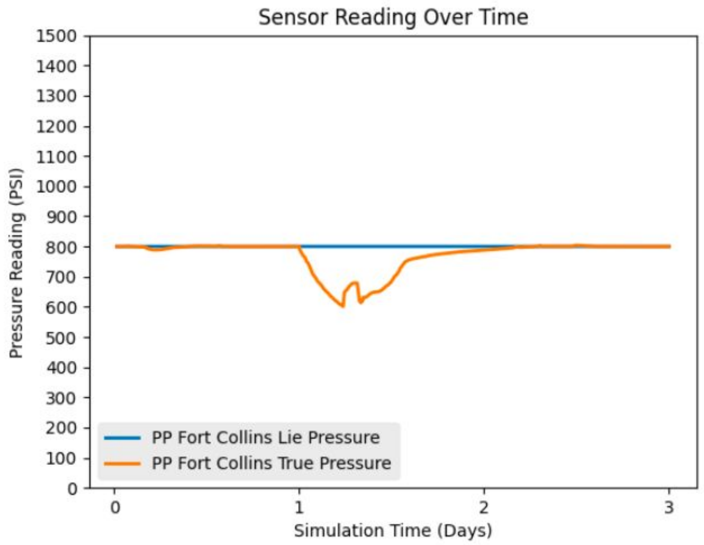


Figure 6.6: Experiment 2: Difference between the actual and falsified readings at the Fort Collins compressor.

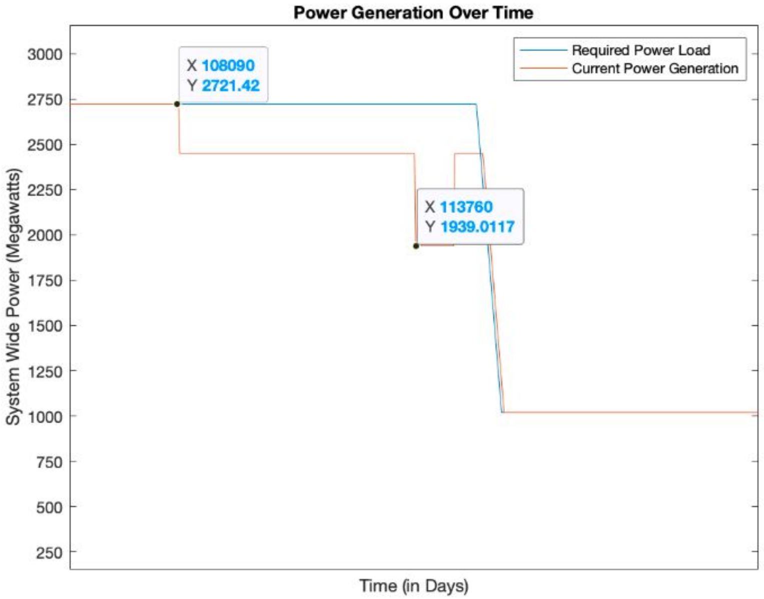
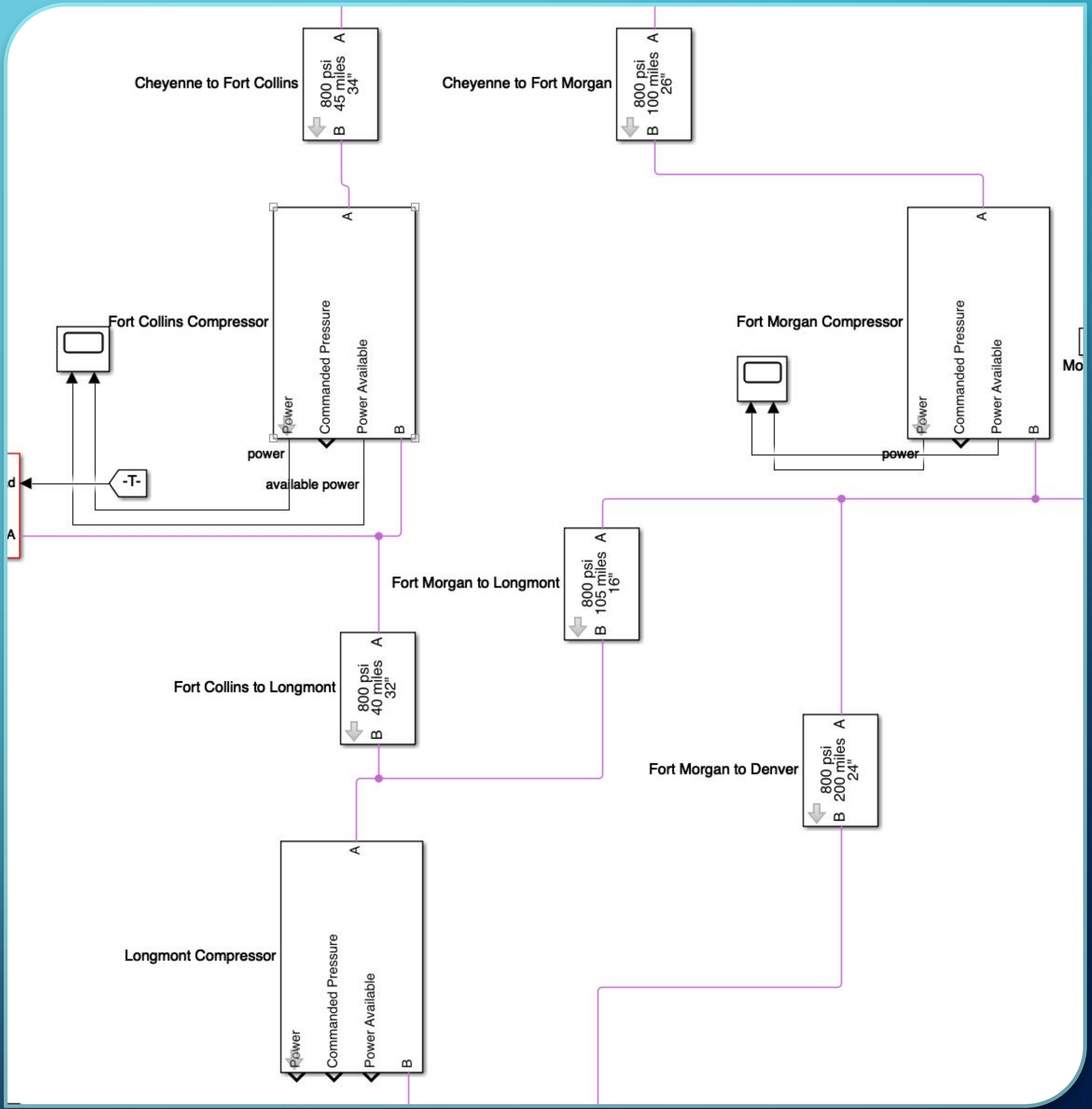


Figure 6.7: Experiment 2: loss in power generation when the Fort Collins and later the Fort Morgan plants go offline.

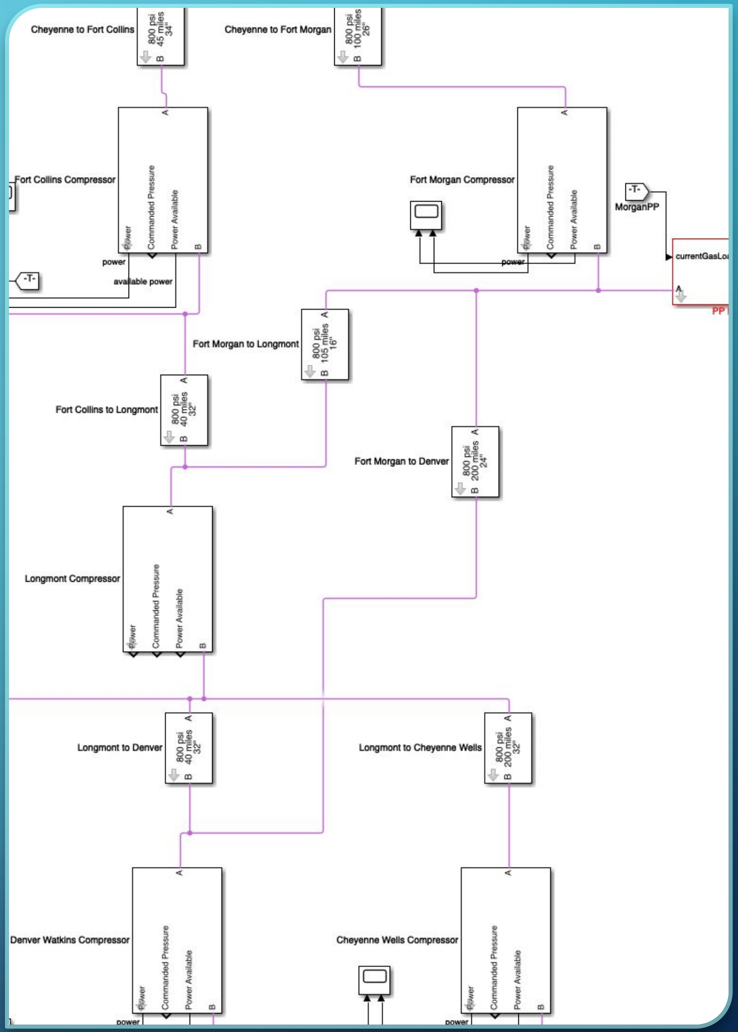
WHY DOES THE FORT MORGAN PLANT GO OFFLINE?

- The Fort Collins compressor acts as a main line to most of the system
  - Power plants downstream rely on the Fort Collins compressor to provide gas at nominal pressure
  - The Fort Morgan plant acts as an auxiliary supporting line if the Fort Collins compressor is lagging behind
- Falsified readings at the Fort Collins plant kept the Fort Collins compressor from ramping up to meet the new gas demand
  - Fort Morgan was left to carry the burden causing its small gas lines to quickly be evacuated



A MORE SOPHISTICATED ATTACK

- Based off our first set of experiments we now know that the Fort Collins compressor is critical to providing gas to the rest of the system
  - Goal: keep the Fort Collins compressor from ramping up, while at the same time try to evacuate the Fort Collins to Longmont line
  - Execution: lie about the pressure at the Fort Collins plant and Longmont compressor to show it remaining at nominal levels, thus preventing Fort Collins compressor from activating. Then lie and show the pressure at the Denver plant as being too low, causing the Denver compressor to ramp up and pull gas out of Longmont, Fort Collins and Fort Morgan



A MORE SOPHISTICATED ATTACK CONT.

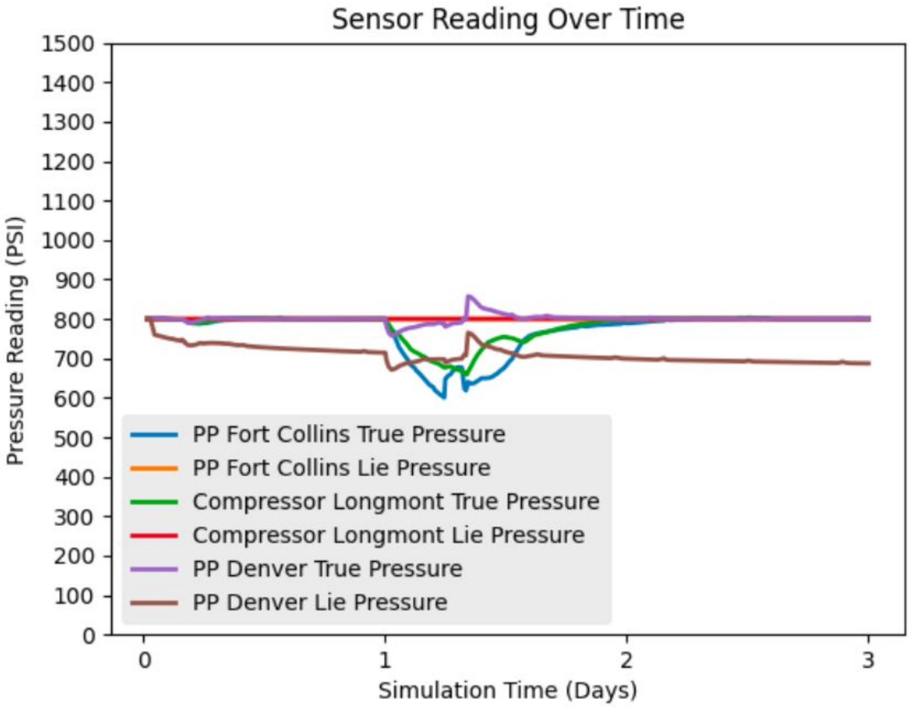


Figure 6.9: Experiment 3: Real and compromised sensor readings.

RESULTS OF THIS ATTACK

- Low pressure at the Fort Collins plant caused it to fall offline, the following increased demand on other plants coupled with the fact the Fort Collins compressor was not pushing along enough gas caused Fort Morgan to rapidly fail as well.
  - Both plants failing in rapid succession was a loss of about 800 MW of generation capacity in ~ 5 minutes

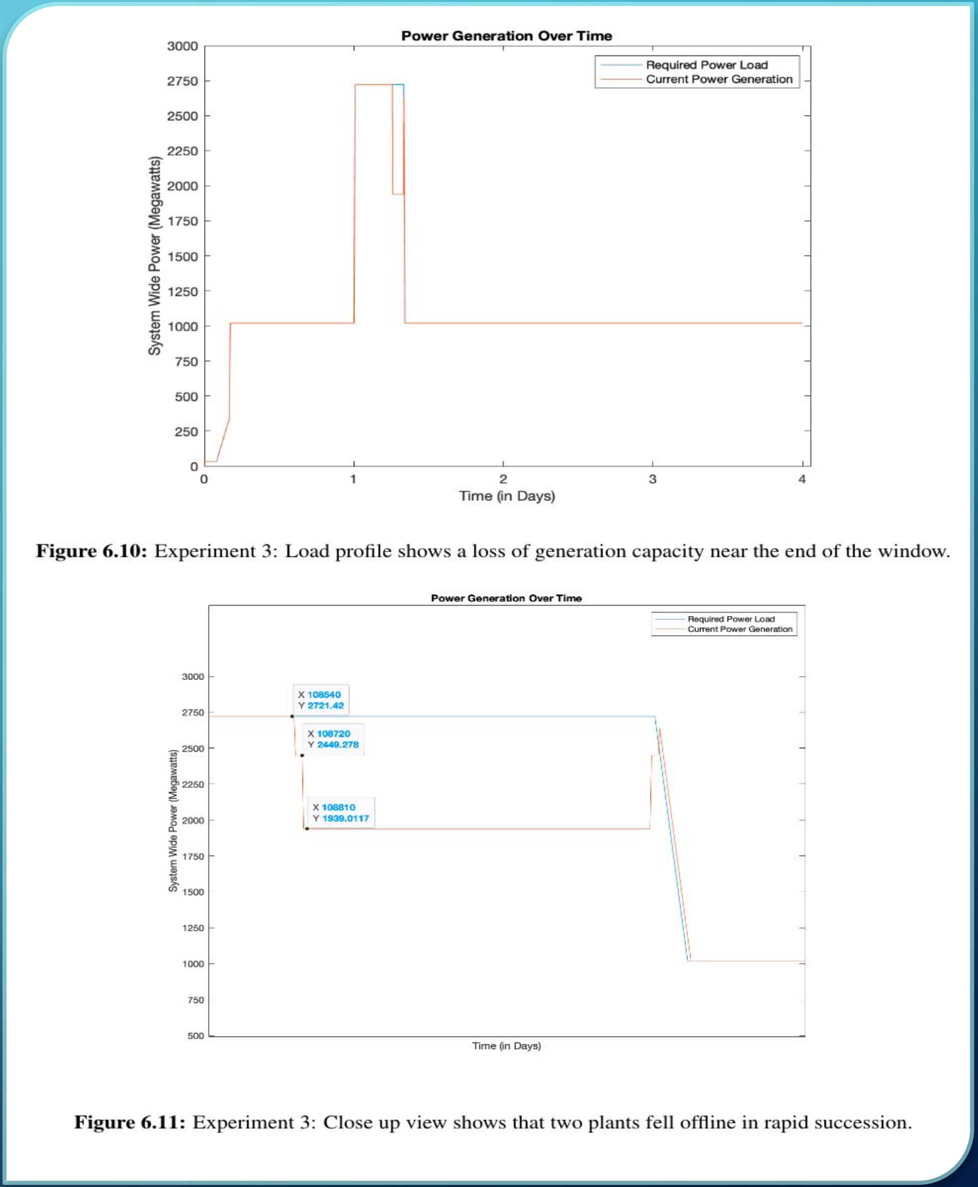


Figure 6.10: Experiment 3: Load profile shows a loss of generation capacity near the end of the window.

Figure 6.11: Experiment 3: Close up view shows that two plants fell offline in rapid succession.

WHAT THESE EXPERIMENTS TELL US

- Single points of failure are typically not as dangerous as multiple sensors lying in coordination
  - With redundant sensors these attacks could be extremely difficult
  - Our simulations also assume that there was no out-of-band cross communication between power plants which is unlikely
- The lies coming from sensors must be sustained for long periods of time
  - Failure for both experiments happened near the back half of the 12-hour period
- Gas pipes contain a certain amount of storage that helps them remain resilient in the face of rapid changes
  - This is very different from electrical grids
- Gas pipelines may have critical points that are more crucial for defense than other points in the system

LIMITATIONS OF THESE SIMULATIONS

- Lack of redundant sensors
- Assumptions about out-of-band communication
- Lack of gas storage
- Large pipe sizes do not match the real-world design of gas pipelines
    - Use of multiple small diameter lines is more common
- Knowledge of the system that most attackers may not have

Google Satellite view of a Kinder Morgan Station

FUTURE WORK

- Modeling network protocols and network behavior
- Integrating a simulation clock in order to control the delays that occur in the model
- Integrating hybrid and real PLCs
- Using machine learning to analyze attacks and discover constraints in SCADA system data
- Designing and implementing encryption schemes in the simulation
- Creating more physical models - such as an electrical system
- Automatic discovery of critical points within the system

Google street view of Kinder Morgan Compressor Station

CONCLUSIONS

- Simulation can lead to interesting and valuable insights we may be able to explore in real systems, or in "thought experiments"
- Simulation is possible for sophisticated systems
  - With some caveats
- Gas systems react very different from electrical systems when it comes to cyber attacks

QUESTIONS?