Chapter 7

SIMULATING MEASUREMENT ATTACKS IN A SCADA SYSTEM TESTBED

Brandt Reutimann and Indrakshi Ray

Abstract Industrial control systems are target-rich environments for cyber criminals, terrorists and advanced persistent threats. Researchers have investigated various types of industrial control systems in smart grids, gas pipelines and manufacturing facilities to understand how they can be compromised by cyber threats. However, the manner in which industrial control systems are attacked is domain-dependent. Testbeds are a necessary tool to model specific domains and understand potential attacks. This chapter discusses the development of a virtual supervisory control and data acquisition system testbed for gas systems and how it is used to simulate the impacts of measurement attacks. The testbed provides opportunities for researchers and domain experts to model, simulate and understand the behavior of a real-world gas system and respond to cyber attacks.

Keywords: Natural gas system, SCADA system, testbed, measurement attacks

1. Introduction

Industrial control systems are target-rich environments for cyber criminals, terrorists and advanced persistent threats. Control technologies have become more connected to internal corporate networks as well as the Internet. As a result, industrial control systems have become more accessible to malicious actors. Securing industrial control systems and, by extension, the critical infrastructure assets they manage, are a priority.

Most work in industrial control system security has focused on supervisory control and data acquisition (SCADA) systems. SCADA systems are sophisticated from the engineering and information technology perspectives. They comprise large networks of interconnected sensors, actuators and controllers, along with human-machine interfaces, engineering

Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XV, IFIP AICT 636, pp. 135–153, 2022.
https://doi.org/10.1007/978-3-030-93511-5_7

workstations and historians. Often SCADA systems are connected to corporate networks where typical information technology security can become just as much of a concern as SCADA system security.

The architecture, interconnectivity and scale of SCADA systems lead to large attack surfaces. Controllers in SCADA systems tend to be heterogeneous because it is infeasible to replace or update large numbers of devices at the same time. The modification and replacement costs are high because availability is a priority and industrial processes cannot simply be shut down. Isolating SCADA networks from the outside world is a good security strategy, but it is not impervious. Attackers can find ways to tunnel into air-gapped SCADA networks from corporate networks, the Internet or merely by using a thumb drive as in the case of Stuxnet [9]. An Idaho National Laboratory report describes 22 high significance attacks on SCADA systems between 2000 and 2018 [7].

Experimenting with SCADA systems to enhance their security is difficult and potentially dangerous. Information about most SCADA systems and the assets they control is proprietary. Studying live systems can cause safety hazards and place physical assets at risk. The solution is to develop and engage a high-fidelity simulation of a SCADA system that enables accurate experimentation without the downsides of interacting with a real system.

This chapter describes experiments with a testbed comprising a simulated SCADA system that operates a modeled gas system. The main problem is to understand what happens when the control layer sends incorrect information to a SCADA system about the state of a physical system, a scenario referred to as a measurement attack [2]. Two experiments involving measurement attacks are considered. The first is a single point of failure experiment that explores the impact of compromising a single controller in a large gas system. The second experiment explores the impact of manipulating several controllers using advanced knowledge of the gas system.

2. Related Work

In order to enhance the security of SCADA systems, it is important to anticipate and defend against possible attacks. The best approach is to probe the systems for flaws and vulnerabilities. Unfortunately, this is a complex and possibly dangerous task. In one instance, ping sweeps caused a robotic arm to swing wildly on a factory floor and in another instance they caused a system failure that resulted in significant equipment damage [5].

A promising approach is to conduct security testing of simulated SCADA systems and environments. Researchers from Mississippi State University have created a testbed comprising several physical systems, including a water tank, water tower, small gas pipeline, factory conveyor belt and smart grid [14]. They also created virtual models of their water tank and gas pipeline systems, which were validated against the physical implementations of the systems [15]. Although the simulation models have actual physical implementations, the physical testbeds are extremely simple. The models have single feedback loops and simple control sequences that do not accurately reflect the real-world systems. As a result, the models support security testing involving attacks on the network and physical components of the testbed, not attacks on the control algorithms.

Researchers have demonstrated various network-based attacks on virtual SCADA system testbeds [2]. Other researchers have conducted attacks on virtual systems that model the large-scale behavior of SCADA systems from the testbed or network-based perspectives [6, 11]. However, these research efforts are limited because they only model the network behavior of SCADA systems or employ small-scale physical testbeds.

Many testbeds that employ physical implementations do not incorporate many of the components in real systems due to resource constraints. Some researchers attempt to address this problem using hybrid models with hardware-in-the-loop simulations [18]. However, these solutions are not as cost effective as software models and virtualized systems. Previous work on SCADA system simulation has focused mainly on single facilities or models of electrical systems [12]. Scalability, accuracy and fidelity are key requirements for designing system simulations from an engineering standpoint. Simulations of full-scale SCADA systems should also be considered when designing and evaluating the security of large-scale assets such as gas pipelines and electrical grids.

In addition to studying SCADA system simulation in general, the interactions between gas and electrical systems is a popular area of study. Gas systems can induce failures in electrical systems and vice versa. Researchers have modeled and analyzed the interdependencies between the systems [4, 10]. Other researchers have created and worked with models that simulate system interactions. The simulated systems have shown that failures of a few gas lines can lead to cascading failures in an interconnected electrical system [3]. However, the models only consider limited sets of variables as opposed to the high-fidelity model described in this chapter.

Despite the body of research in the area of SCADA system simulation, the work described in this chapter addresses some novel issues. Little, if

any, work on SCADA system simulation focuses on gas systems or their effects on electrical systems, especially with regard to cyber vulnerabilities and attacks. Although this work does not cover the interactions between electrical and gas systems in detail, it explores vulnerabilities in a simulated gas system that has the potential to harm a hypothetical electrical system. The work also explores measurement attacks on a large-scale gas pipeline model. Additionally, it presents a simple SCADA system simulation architecture that can be used to create modular simulations of a variety of cyber-physical systems. Indeed, previous research has mostly created simulations of specific types of (mainly electrical) systems instead of presenting methods for creating more expansive simulation models.

3. Gas System Model and Experimental Setup

This section describes the design and simulation of the gas system model used in the experiments, along with the experimental setup, including the experimental gas system scenario and data collection.

3.1 Gas System Model

The gas system model used in the experiments was designed to capture gas pipeline assets in the state of Colorado. The main objective was to make the model realistic enough that the system would fail due to cyber attacks and not because the engineering concepts underlying the model are weak. To accomplish the task, the model development team consulted with engineers at the Colorado Powerhouse and other gas system experts to define appropriate model constraints. The principal concern was to obtain data that would provide scale to the model. However, the process of acquiring accurate data on control systems was very challenging.

Data from several sources was collected and gas dynamics principles were employed to determine appropriate measurements. A Kinder Morgan system map provided the general locations of gas pipelines, compressors and power plants in the state of Colorado [19]. The map was augmented with large cities at their rough distances from gas pipelines and other assets. Moderate-sized power plants near medium-sized cities in Colorado and a large power plant in Denver were also included in the map. Distribution loads were sprinkled on the map to add complexity to the gas pipeline system. Having determined the placement of power plants, compressors and distribution loads, Xcel Energy resources were used to discover the peak load capacities (in MW) for power plants

around the state [17]. The peak capacities (in MW) were converted to the required gas mass flow rates (in kg/s) using gas heating values.

The peak mass flow gas loads for each power plant (in kg/s) were used to determine the gas pipe diameters that would meet the demand at a nominal pressure of 800 psi using Bernoulli's equation (ignoring gravity and height differences). As the gas loads in the designed system and in the real world are very high, the gas pipelines had to be large enough to distribute the required gas. Gas pipe typically comes in nominal sizes that do not exceed 36 inches in diameter and, when more gas has to be distributed, additional pipes are laid in parallel. However, the system does not consider this situation and uses a single large pipe. This leads to adverse effects on some of the gas properties. For example, there is more friction when using several small pipes than when using a single large pipe. Additionally, gas flow rates are higher in smaller pipes, which means that temperature changes can be more dramatic.

Having determined the gas model structure and worked out the basic numerical constraints, the gas model was simulated using a SCADA system simulation tool. The SCADA system simulation tool developed by the research team comprises a controller and software simulator that interfaces with MATLAB Simulink to integrate virtual programmable logic controllers and hardware-in-the-loop devices. These virtual and real devices communicate using Modbus, their native SCADA protocol. This provides a window into the Simulink simulations using traditional controllers and control system software. The design considerations and development of the SCADA system simulation tool are outside the scope of this research and are not described in this chapter.

3.2 Experimental Setup

Gas systems can become extremely hazardous when pressure or temperature drop rapidly. Rapid drops in pressure can prevent gas delivery while temperature drops can lead to dew pointing and solids traveling with the gas. Previous simulation experiments employed an external control system to trip (switch off) a power plant when its pressure or temperature reached the set values. However, in the experiments, it was desired to keep switch-off control inside the process model to model a power plant engineer tripping the plant when the gas pressure or temperature reaches the set values. In the gas system model, a MATLAB function block was incorporated to set a power plant load to zero and switch it off for a number of seconds specified by a parameter at the beginning of the simulation. The shutoff duration of a power plant was set to 3,600 seconds (one hour). This time represents how long after a

shutoff it takes power plant engineers to run through their safety procedures and ramp the plant back up to meet the current load. The goal of the experiments was to get power plants to trip their automatic shutoffs by dropping the gas pressure in the system.

The gas system model uses a dynamic load distribution algorithm that enables it to simulate a systemwide load that different power plants in the system have to cooperate to meet. Every load was specified individually in previous experiments. However, in this case, a single load could be specified to model a realistic scenario. The advantage of this approach is that when one power plant in the system trips, the load switches to other power plants in the system. This effectively models scenarios where the loss of a power plant can possibly cause a cascading failure because gas demands increase very rapidly in other parts of the system.

Each power plant in the system is specified with a gas load capacity (kg/s), which helps determine its current load. If the gas load capacity of a plant is p_c, total system gas load capacity is s_c and the current total gas load at time t is l_t, then the current gas load of the plant at time t is $p_c/s_c \cdot l_t$.

Also, a scenario must be considered where the total gas system load exceeds the capacity of the available power plants. In this case, each plant outputs at its maximum load, but the systemwide demand will not be met. This scenario corresponds to a situation where the gas system is not generating enough electrical power to meet demand.

The control system used in the experiments has considerable complexity. The compressors in the system are designed so that the power capacity of a power plant can be modified. When compressing gas, a compressor examines the value δ_p corresponding to the difference in pressure between the desired set point (800 psi in the model) and the current pressure reading. As δ_p increases, more power is required to compress gas to meet the pressure differential. In order to render the system realistic, there must be a limit on the amount of power that a compressor can use to achieve its goal. The limit has a base value of 5 MW. When the system requires more power than is available, δ_p is modified to the maximum compression available for the current maximum amount of power. This plays into the control system as the system operators desire to minimize the amount of power being used by compressors whenever possible.

The control algorithm for the gas model increases the power available to upstream compressors based on the current pressure readings at downstream power plants and compressors. The controller iteratively checks the state of the system and updates the power available to each immediate upstream compressor. Power is updated in 5 MW increments. If the

pressure is less than 750 psi then power is increased by 5 MW whereas if the pressure is at 800 psi the available power is decreased by 5 MW to conserve energy. Upstream compressors are identified by consulting the directed graph that represents gas flow in the system. Each node in the graph is either a power plant or a compressor. Every power plant is always a leaf node because gas does not flow through a power plant to other nodes in the system.

Gas System Scenario. The gas model was set up in a scenario to conduct two experiments. The scenario covers a period of time when the gas system is placed under a high level of stress. This is important because cyber attacks are especially serious when systems are under high stress.

The scenario, which covered three days, was intended to demonstrate the potential impacts of data manipulation in a SCADA system. During the first day, the system operates under a moderate load. Such a situation occurs when a renewable energy source like wind provides a large portion of the electricity demand [1]. Although this may be slightly contrived, it is a good starting point for demonstrating the value of SCADA system simulation.

On the second day, there is a sudden loss of wind power coupled with an increase in electric power demand. As a result, the natural gas power plants ramp up to generate enough electricity to meet the demand. After a 12-hour period, things return to normal because wind power comes back up and electricity demand drops.

Figure 1 shows that the power generation matches the required power load over the three days of the scenario. This is because, during the high-stress period, when natural gas power plants ramp up to generate electricity, control systems in the gas system adjust the compressors to deliver gas to the power plants. When wind power comes back up and electricity demand drops, the control systems enable the gas system to ramp down to match the required power load.

When natural gas power plants ramp up to generate electricity, the demand for natural gas in the gas system increases dramatically, which reduces the pressure in the gas system. If the compressors in the gas system are not adjusted by the control systems to meet the demand, power plants begin to trip because gas is not delivered at a high enough pressure. Figure 2 shows the rapid loss in power generation when the control systems do not intervene.

The goal of measurement attacks in the scenario is to prevent control systems from adjusting gas pressure at the beginning of the high-stress

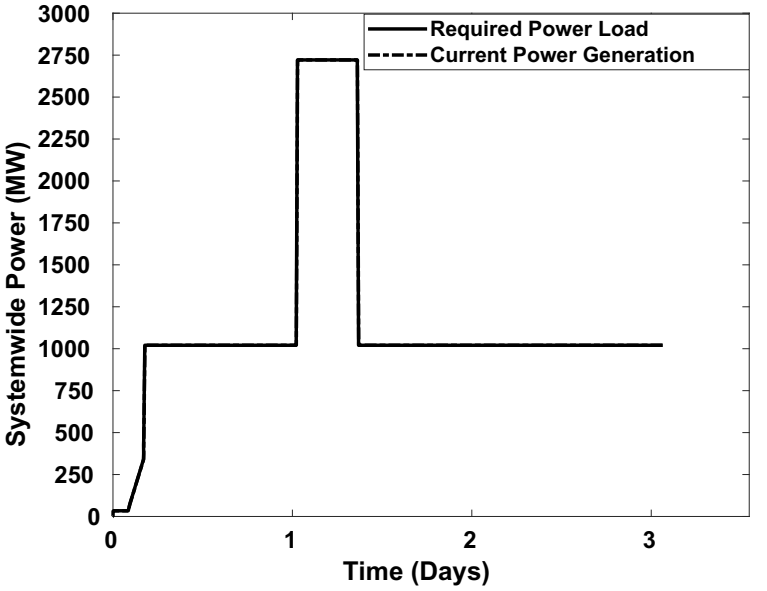

Figure 1. Electric power generation and power load over the three-day scenario.

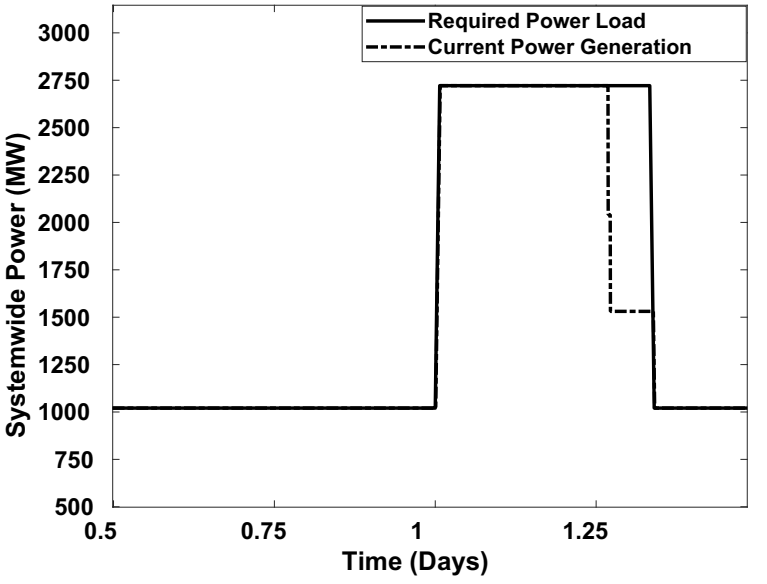

Figure 2. Rapid power generation loss without control system intervention.

period. An attack is successful if it causes a power plant to trip during the high-stress period.

Data Collection. Data was collected in several places in the simulated system to demonstrate consistency and the effects of control system compromises. The Simulink model logged all the data during the simulation and data coming from the programmable logic controllers to the simulated operator was tracked. This data was marked on the operator side. Thus, there is a copy of the authentic data as well as a copy of the compromised data. The two sets of data can be compared to show how the real state of the system is affected by the control actions made using the compromised data.

4. Single Point of Failure

The first experiment explored the impacts of a single point of failure on the gas system during the 12-hour high-stress window. When gas loads on the system increase, gas pressure drops at the natural gas power plants as they start evacuating their upstream gas lines. It is vital that the power plant controllers recognize the pressure drops and make more power available to the upstream compressors. Therefore, the attacks in the first experiment provide false pressure readings to the power plant controllers. The false pressure readings at the power plants would prevent upstream compressors from ramping up, dropping the gas pressure at the power plants to levels at which they cannot operate.

The compromise used in the experiment was very simple – no matter the system state, a compromised power plant would always report 800 psi. The experiment comprised five trials, each trial involving the application of the compromise to each power plant and running the simulation. An attack was deemed successful if a power plant failure occurred within the 12-hour window of high stress. The goal of the experiment was to determine if a single compromise could induce catastrophic effects on the gas system.

Interesting results were obtained in the experiment. In four of the five trials, although a measurement attack was taking place, the compressor immediately upstream of the attack was not affected. This is because multiple downstream entities showed low pressure values and a single false pressure value did not prevent the control system from updating the pressure value at the compressor. In the case of power plants that were isolated, the measurement attacks could have disabled their compressors, but as the compressors on the main lines in the simulation were still running, there would be enough gas being pushed through the system to prevent failures.

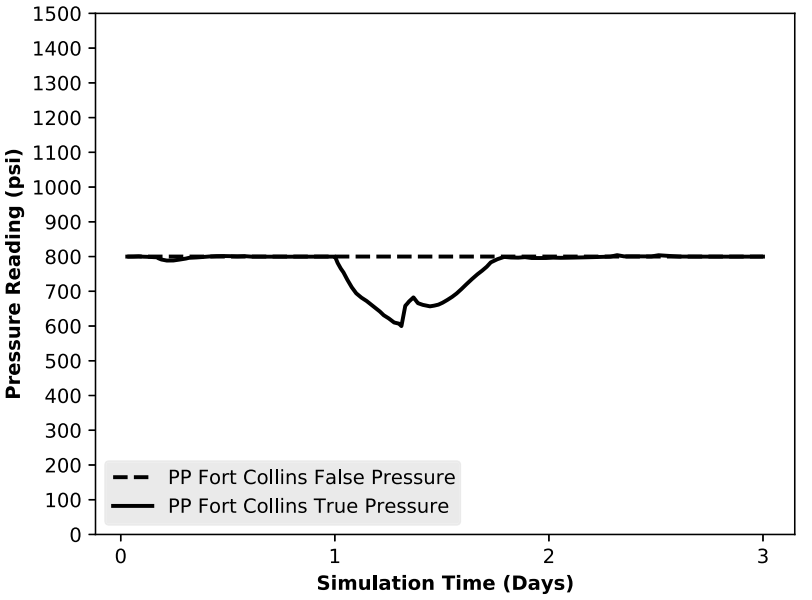

Figure 3. True and false pressure readings at the Fort Collins plant.

The one trial that resulted in failure provided interesting insights. Compromising the pressure reading at the Fort Collins power plant led to its compressor being temporarily disabled, which caused the Fort Collins plant to go offline. Figure 3 shows the true and false pressure reading differentials at the Fort Collins plant over the simulation.

The increased gas demand imposed on the auxiliary line from Fort Morgan caused the Fort Morgan plant to trip. Figure 4 shows the failure of the Fort Collins plant followed by the failure of the Fort Morgan plant near the end of the 12-hour window.

The interesting takeaway is that the Fort Collins compressor is a critical point in the system because it feeds gas to a number of downstream power plants. When the Fort Collins compressor does not meet the demand of the downstream plants, increased loads are induced on the auxiliary lines, leading to the failure of the Fort Morgan plant.

5. Sophisticated Measurement Attack

The second experiment explored compromises of multiple sensors in the system to induce a rapid failure. The objective was to prevent a compressor from ramping up when it should while encouraging other compressors to ramp up when they need not. The attack is similar to

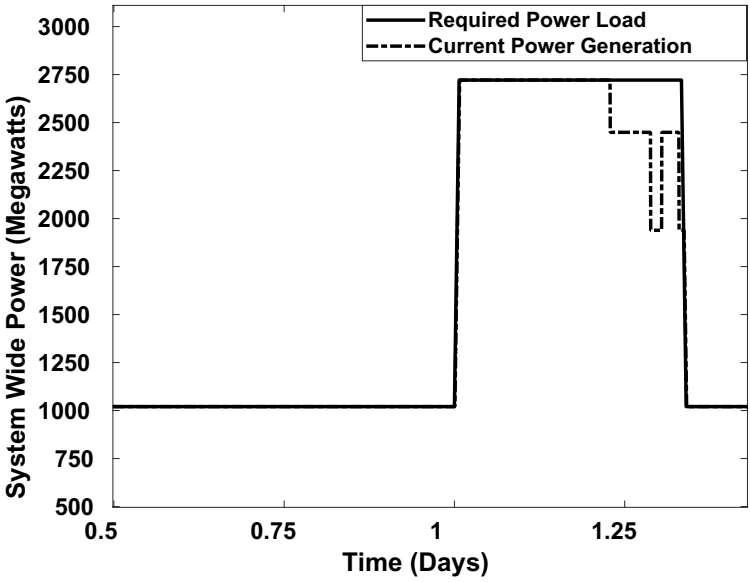

Figure 4. Failures of the Fort Collins and Fort Morgan plants.

the one in the first experiment because it falsifies data, but it is more sophisticated in that the false data manipulates the actions of multiple upstream compressors.

The first experiment revealed that the Fort Collins compressor is a critical asset in the gas system. Therefore, the second experiment sought to target the immediate downstream neighbors of the Fort Collins compressor – the Fort Collins power plant and the Longmont compressor. The attack caused the Fort Collins power plant and Longmont compressor to always read 800 psi regardless of the actual pressure. Additionally, the attack set the Denver power plant pressure reading low to ramp up the Denver compressor, pulling gas through the line from Fort Collins to Denver. The objective was to pull gas down the line while preventing the Fort Collins compressor from ramping up to meet the new demand. This would empty the gas lines and induce failures in the system. Figure 5 shows the discrepancies between the true and false pressure readings.

The second experiment yielded interesting results related to measurement attacks. The compromised high readings at the Fort Collins power plant and Longmont compressor prevented the Fort Collins compressor from ramping up during the period of high stress. Additionally, the control system increased the power to the Denver compressor to compensate for the false low pressure reading. This caused the pressure in the Fort

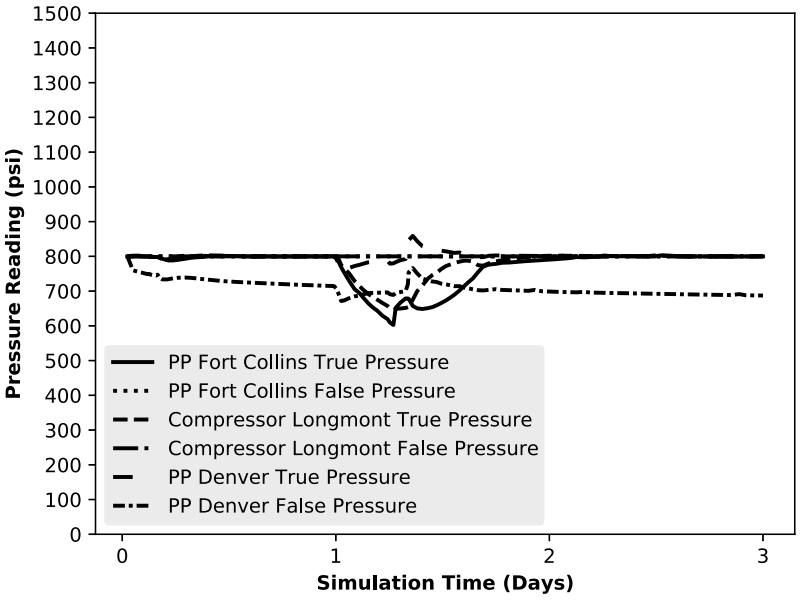

Figure 5. Discrepancies between the true and false pressure readings.

Collins to Longmont line to drop (Figure 6) as well as increase the demand on the auxiliary line from Fort Morgan. As gas was evacuated from the two lines coming into Longmont, the pressure dropped rapidly in both lines. As a result, the Fort Collins and Fort Morgan plants tripped in rapid succession (Figure 7). This resulted in the gas and power generation systems not being able to meet their total demands. The total loss of capacity of gas load (in kg/s) translates roughly to a loss of about 800 MW in just five minutes (Figure 8).

6. Discussion

The experimental results provide insights into the hazards posed by measurement attacks. The first experiment explored how a single point of failure can affect a complex system. The results show that, although there could be catastrophic effects at critical points in the system, isolated portions of the system tend to incur minimal impacts. Therefore, the isolated portions do not require comprehensive defenses. It may be adequate to secure the overall system from catastrophic failures by identifying and applying maximal defenses at the critical points.

The second experiment is interesting, albeit troubling, because it demonstrates that an attacker with intimate knowledge of system dy-

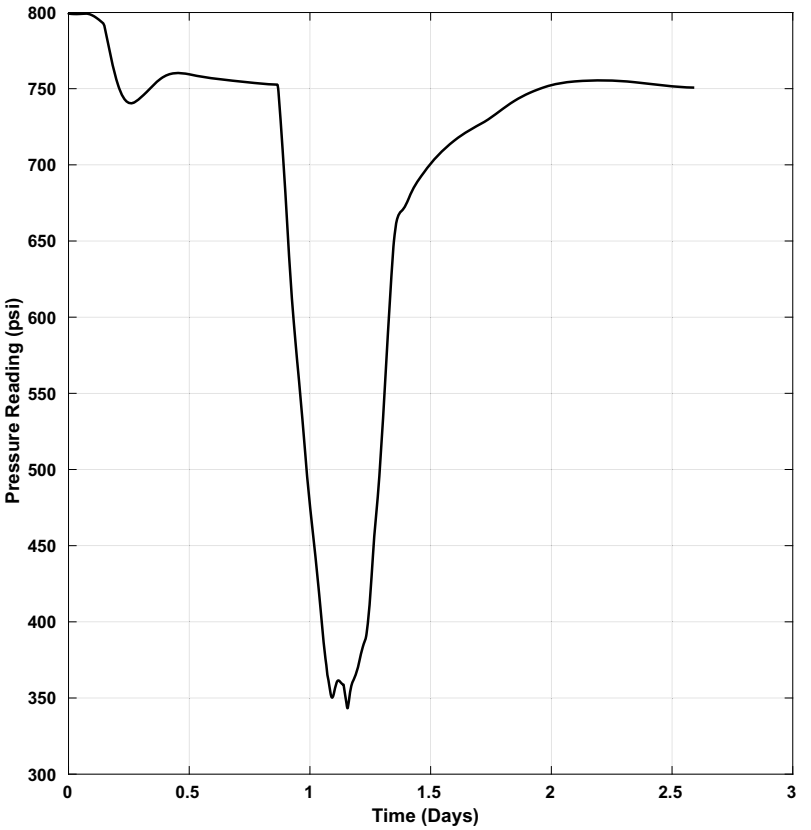

Figure 6. Pressure drop in the Longmont gas line during the high-stress period.

namics could use measurement attacks to manipulate the control response. Measurement attacks can put the system into a state that induces failures that would not occur with normal control behavior. As more sensors are compromised, measurement attacks become increasingly complex and likely more difficult to detect. However, they require the attacker to have knowledge of how the control system operates, the gas system topology and when the system is in a period of high stress.

The experiments also show that the responses of gas systems to cyber attacks are very different from the responses of electrical systems. Failures in electrical systems occur very rapidly. For example, in the case of the August 14, 2003 blackout in the United States and Canada, system operators noticed anomalies around 4:06 pm, just four minutes before a power surge took out a large power line that induced cascading failures leading to the blackout [16]. In the case of the San Diego

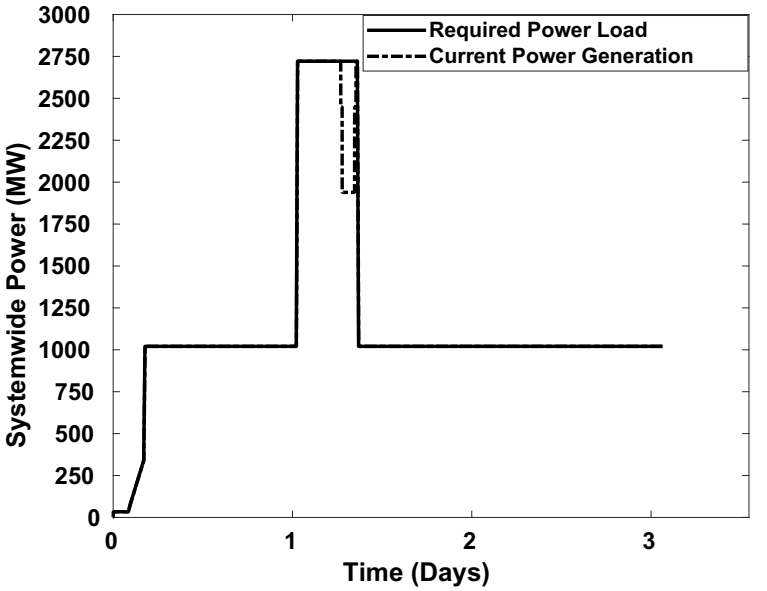

Figure 7. Load profiles show that power plants trip and fail to meet the demand.

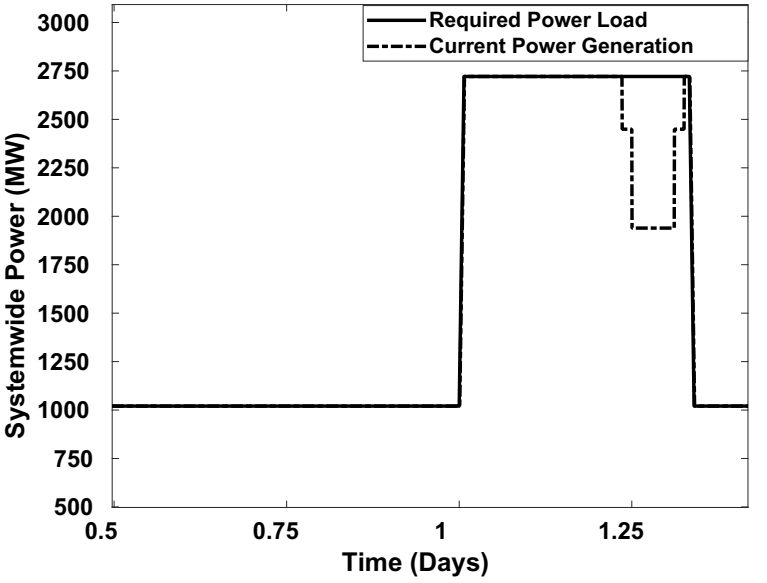

Figure 8. Load profiles show that power plants trip and fail to meet the demand.

blackout of 2011, a system supported primarily by a 500 kV line went down in roughly 10 minutes following a maintenance problem at a remote substation [13].

Unlike in electrical systems, physical effects in gas systems have high latency. This is seen in the experimental results – even under a sustained measurement attack, several hours passed before a drop off in electricity production occurred. This is partly due to how the scenario was set up. But this could also be because it takes a long time (relative to electricity) to physically move gas through pipes. This could also explain why isolated attacks have less impact on the system.

Additionally, large pipes hold substantial amounts of gas. The stored gas can prevent failures during rapid increases in gas load because there is not an immediate reaction to the change in system state. This was seen in the scenario, where even with no control response, the system did not fail until the near the end of the 12-hour window. This suggests that there is ample time to react when the system is not operating normally. The positioning of gas storage tanks at strategic locations on gas lines is another way to avoid failures during periods of high stress. This does not bode well for attackers intending to damage a gas system, but it also does not mean that the system is safe from strategic and coordinated attacks.

The principal takeaway from the experiments is that cyber attacks have to be sustained for hours or even days to have impacts on gas systems. For example, in the single point of failure scenario, where the system was sustained by a primary source of gas (like the 500 kV line in the San Diego blackout example), a measurement attack had to be sustained for nearly 12 hours before any impact was observed. A variety of scenarios would have to be investigated to advance this hypothesis. The single point of failure scenario was designed to be challenging for a gas system in order to demonstrate the value of simulation and the impacts of measurement attacks. Regardless, the length of time a measurement attack would have to be sustained to produce a negative impact is encouraging because it would be very difficult to trick system operators for hours on end. Redundant sensors and frequent communication between operators could enable them to identify false data before failures occur. However, because cyber attacks on gas pipelines are rare, a gas system operator would likely attribute anomalous phenomena to faulty sensors or devices instead of attacks. Of course, the important point is that a sustained measurement attack on a gas system that goes undetected long enough could cause rapid cascading failures as seen in the second experiment.

7. Future Work

An important area of future research is to detect measurement attacks using machine learning techniques. One approach is to employ statistical methods for outlier identification; these methods could enable control systems to identify sensor readings as outliers in time series data. Another approach is to apply deep learning and classification algorithms to identify anomalies in time series data.

SCADA system data could also be analyzed to identify constraints within and between sensor data streams. An example constraint within a data stream is that a pressure sensor reading should be in a certain range during normal operations. A constraint between data streams is the mathematical relationship between the temperature and pressure of a gas. Another such constraint is that pressure readings at power plants downstream of a large compressor vary together in response to changes in the compressor output. An intelligent SCADA system could be trained to identify and report constraint violations to system operators for analysis and mitigation.

A primary issue with identifying constraints in SCADA systems is that as the systems scale, the constraints become increasingly complex and interconnected. Identifying constraints between multiple components requires considerable expertise, and is time-consuming and error-prone. Researchers have developed an automated methodology for identifying and verifying constraints in large data sets using a feedback loop with subject matter experts [8]; this methodology is certainly applicable to automated constraint discovery in SCADA system time series data.

Another area of future research is the automated discovery of critical points to prioritize the application of security controls. This research has shown that compromises of certain controllers can be much more devastating than compromises of others. For example, in the first experiment, compromising the Fort Collins power plant controller prevented the Fort Collins compressor from feeding gas to several downstream power plants, resulting in a partial failure of the gas system. Automated discovery would require the simulation of a real-world gas system and iteratively applying measurement or command injection attacks to each controller. Analysis of compromises and the failures they induce would help determine the critical points and their relative importance.

8. Conclusions

Realistic SCADA system simulations are vital to understanding the behavior of real-world systems and the impacts of cyber attacks. The principal contributions of this research are the development of a high-

fidelity gas system simulation and the application of measurement attacks to understand their local and overall gas system impacts. The simulation experiments show that an intelligent attacker can cause considerable harm to a gas system via measurement attacks. The experiments also provide useful insights about critical points in gas systems and the propagation of the negative impacts of attacks. The simulation environment supports high-level reasoning about SCADA system security without having to work on a real system. Additionally, it enables the exploration of diverse scenarios that would simply not be possible on real gas system.

Acknowledgements

This research was supported by the National Science Foundation under Grant no. CNS 1822118 and by the National Institute of Standards and Technology, American Megatrends Inc., CyberRiskResearch, Statnett and the Colorado State Cyber Security Center and Energy Institute at Colorado State University. The authors wish to acknowledge the Colorado State University Powerhouse and METEC Gas Testing Site for their assistance in modeling high-fidelity gas systems. The authors also wish to thank Aeric Walls for his assistance with the experiments and presenting the results.

References

[1] V. Akhmatov, Analysis of Dynamic Behavior of Electric Power Systems with Large Amount of Wind Power, Ph.D. Thesis, Department of Electric Power Engineering, Technical University of Denmark, Lyngby, Denmark, 2003.

[2] A. Ashok, P. Wang, M. Brown and M. Govindarasu, Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed, *Proceedings of the IEEE Power and Energy Society General Meeting*, 2015.

[3] B. Cakir Erdener, K. Pambour, R. Bolado Lavin and B. Dengiz, An integrated simulation model for analyzing electricity and gas systems, *International Journal of Electrical Power and Energy Systems*, vol. 61, pp. 410–420, 2014.

[4] C. Correa-Posada, P. Sanchez-Martin and S. Lumbreras, Security-constrained model for an integrated power and natural gas system, *Journal of Modern Power Systems and Clean Energy*, vol. 5(3), pp. 326–336, 2017.

[5] D. Duggan, Penetration Testing of Industrial Control Systems, Sandia Report SAND2005-2846P, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[6] S. Duque Anton, M. Gundall, D. Fraunholz and H. Schotten, Implementing SCADA Scenarios and Introducing Attacks to Obtain Training Data for Intrusion Detection Methods, arXiv: 1905.12443 (`arxiv.org/abs/1905.12443`), 2019.

[7] K. Hemsley and R. Fisher, History of Industrial Control System Cyber Incidents, INL/CON-18-44411-Revision-2, Idaho National Laboratory, Idaho Falls, Idaho, 2018.

[8] H. Homayouni, S. Ghosh and I. Ray, ADQuaTe: An automated data quality test approach for constraint discovery and fault detection, *Proceedings of the Twentieth IEEE International Conference on Information Reuse and Integration for Data Science*, pp. 61–68, 2019.

[9] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE Security and Privacy*, vol. 9(3), pp. 49–51, 2011.

[10] T. Li, M. Eremia and M. Shahidehpour, Interdependency of natural gas network and power system security, *IEEE Transactions on Power Systems*, vol. 23(4), pp. 1817–1824, 2008.

[11] B. Masset and O. Taburiaux, Simulating Industrial Control Systems Using Mininet, M.S. Dissertation, Department of Computer Science, Catholic University of Louvain, Louvain-la-Neuve, Belgium, 2018.

[12] K. Mathioudakis, N. Frangiadakis, A. Merentitis and V. Gazis, Towards generic SCADA simulators: A survey of existing multipurpose co-simulation platforms, best practices and use cases, *Proceedings of the Scientific Cooperations International Conference on Electrical and Electronics Engineering*, pp. 33–40, 2013.

[13] J. McDonald and M. Lee, Blackout sparks multiple investigations, *San Diego-Union Tribune*, September 9, 2011.

[14] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu and R. Reddi, A control system testbed to validate critical infrastructure protection concepts, *International Journal of Critical Infrastructure Protection*, vol. 4(2), pp. 88–103, 2011.

[15] T. Morris, Z. Thornton and I. Turnipseed, Industrial control system simulation and data logging for intrusion detection system research, *Proceedings of the Seventh Annual Southeastern Cyber Security Summit*, 2015.

[16] North American Electric Reliability Council, Technical Analysis of the August 14, 2003 Blackout: What Happened, Why and What Did We Learn? Report to the NERC Board of Trustees by the NERC Steering Group, Princeton, New Jersey, 2004.

[17] Public Service Company of Colorado, Colorado Generating Stations, Denver, Colorado, 2017.

[18] Q. Qassim, N. Jamil, I. Abidin, M. Rusli, S. Yussof, R. Ismail, F. Abdullah, N. Ja'afar, H. Che Hasan and M. Daud, A survey of SCADA testbed implementation approaches, *Indian Journal of Science and Technology*, vol. 10(26), 2017.

[19] N. Schubert, KMI System Map, Kinder Morgan, Houston, Texas, 2014.