A Comparative Analysis Approach for Deriving Failure Scenarios in the Natural Gas Distribution Infrastructure

Michael Locasto, David Balenson

Chapter 2

A COMPARATIVE ANALYSIS APPROACH FOR DERIVING FAILURE SCENARIOS IN THE NATURAL GAS DISTRIBUTION INFRASTRUCTURE

Michael Locasto and David Balenson

Abstract An important question facing critical infrastructure owners and operators is how their assets could be made to fail by the various threat actors. Designing, enumerating and analyzing failure scenarios helps explore the assumptions made on the operational side, the value of current mitigations and the need for certain types of protection mechanisms. This chapter describes the formulation of 55 failure scenarios in the natural gas distribution infrastructure. These failure scenarios highlight a range of potential threats across the natural gas infrastructure, from transmission to distribution and home metering. The chapter also describes a multi-pronged approach used to develop failure scenarios for the gas sector and compares them against the scenarios developed for the electric sector. The focus is on the concepts underlying the failure scenarios and their use, the threat model they encompass, and the assumptions, lessons learned and caveats underpinning their creation.

Keywords: Natural gas distribution infrastructure, failure scenarios, cyber security

1. Introduction

Failure scenarios are an important consideration when analyzing the cyber security postures of critical information infrastructure assets. This chapter describes a process for developing cyber security failure scenarios in the natural gas distribution network. The process took shape in a project performed with the Gas Technology Institute/Operations Technology Development (GTI/OTD) Cybersecurity Collaborative. During the project planning and prioritization efforts, it was determined that the specification of failure scenarios would help understand the cyber security implications in the natural gas distribution landscape. The effort was kicked off by exploring the

use and adaptation of the National Electric Sector Cybersecurity Organization Resource (NESCOR) Electric Sector Failure Scenarios and Impact Analysis (Version 3.0) [11] to the natural gas distribution environment.

This chapter reviews the process for designing and generating failure scenarios – a process that necessarily begins with acquiring a thorough understanding of the equipment, protocols and facilities used in the natural gas distribution network. It describes the failure scenarios and their categories, the threat model they encompass and the assumptions, lessons learned and caveats underpinning their creation.

In addition to a significant domain familiarization process, the effort involved adapting existing frameworks for describing failure modes and potential compromises from another critical infrastructure sector (i.e., electric power). The NESCOR failure scenarios developed for the electric sector [11] were employed as a template. However, the translation between the two sectors was not straightforward and certain categories of infrastructure did not map at all. Attempting to translate the electric sector failure scenarios to the natural gas infrastructure provided valuable insights about the assumptions and differences between the two sectors. In large part, the gas sector failure scenarios are not restatements of the NESCOR scenarios. Even the closely related automated meter reading category, has some notable differences. Indeed, it was more natural and productive to develop specialized scenarios that tightly reflect natural gas sector equipment, protocols and facilities.

In addition to specifying a procedure for generating interesting and useful scenarios, this chapter provides a differential comparison between the natural gas and electricity domains with the goal of providing a roadmap for similar efforts in other domains. The advantage of differential conceptualization is the efficient enumeration of failure scenarios in another domain because the comparison highlights the parts of the process that can be generalized and the parts that require time and investment in learning about the target domain. This outcome should reduce the amount of effort required to conduct future analyses because one of the least mechanical and most difficult tasks is to acquire adequate domain expertise to define realistic failure scenarios and identify meaningful impacts. Furthermore, the explicit observations help identify surprising differences and considerations in two closely-related sectors, helping calibrate and temper expectations about how certain concepts, settings, vulnerabilities and impacts translate between sectors.

2. Failure Scenarios

According to the NESCOR document [11]:

> "*A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity and/or availability of sector cyber assets creates a negative impact on the generation, transmission and/or delivery of power.*"

This definition requires one minor edit – replacing power with natural gas – to apply to the natural gas distribution network.

Table 1. Example failure scenarios.

Scenario	**Description**	**Vulnerabilities**	**Impact**
AMR.18	Competitor observes gas consumption at a store or factory	Insecure cleartext protocols permit any party to observe usage data	Competitive advantage and insight into a direct competitor
O.3	Attacker gains access to odorizer controller and modifies setpoints to increase the amount of odorant injected, resulting in over-odorization of the gas	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to manipulate set-points and possibly disable or modify sensor readings or alarms	Increase in service calls as customers report suspected leaks

A scenario is actually not a single event; it is a complex mixture of conditions and events. Scenarios are not limited to direct failures induced by malicious cyber actors. Indeed, scenarios include malicious and non-malicious events [11]:

- Failures due to equipment functionality compromises.
- Failures due to data integrity attacks.
- Communications failures.
- Human error.
- Interference with the equipment lifecycle.
- Natural disasters that impact the cyber security posture.

Failure scenarios are not equivalent to single vulnerabilities or specific software errors that should have been or can be remedied by a simple checklist or adherence to best practices. By considering the mixture of causes listed above, failure scenarios can provide a rich ground for analyses and a variety of other uses that are discussed later. Failure scenarios offer a structured approach for representing the potential impacts of different categories of threat actors and provide an analysis tool for evaluating the utility and sufficiency of existing mitigations.

Table 1 highlights two failure scenarios to provide readers with an idea about the structure of failure scenarios.

As discussed later, the NESCOR report gathers scenarios into similar themes called categories that map to electric power system functions such as demand-response. The natural gas distribution network scenarios are also gathered

into categories, but the categories are more closely mapped to facilities and components of infrastructure rather than functions.

3. Benefits of Failure Scenarios

Failure scenarios can be used in a number of ways, including for risk assessment, planning, procurement, training, tabletop exercises and security testing. While the value proposition for employing failure scenarios as an analytical tool for the natural gas distribution infrastructure encompasses all these uses, the scenario development effort focused on three principal benefits:

- **Assess Sufficiency of Current Safety and Security Measures:** Natural gas distribution companies are aware of critical infrastructure threats. In some cases, companies have electric and gas portions of the business, and cyber security considerations are an active area of planning, protection and analysis. However, a common consideration is whether the current mitigations are sufficient. To help assess whether vendor or internal tools and procedures are adequate, companies need an analytical methodology that directs their attention to relevant threats, vulnerabilities and impacts.

- **Assess Risk/Reward of Incorporating Intelligent Electronic Devices:** The natural gas industry is at an inflection point where automation is set to increase. Companies are making decisions about which portions of their infrastructure have priority during the normal equipment replacement cycle. The industry is also undergoing a generational shift, where experienced engineers are retiring or are on the cusp of retirement. One approach to compensating for this reduction is by introducing automation that is managed by junior engineers.

- **Nurture Ties between IT and OT Personnel:** It is important for information technology (IT) and operational technology (OT) personnel to work together on cyber security implementation and preparedness. The value of such an engagement has been demonstrated by partnerships such as the Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) Consortium [3, 25] and the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) and Cyber Resilient Energy Delivery (CREDC) Consortia [4, 24] that involve academia, government and industry. Trust cannot be built overnight. A key benefit of working with natural gas utilities to specify failure scenarios was that it provided a mechanism for collaboration, interaction and mutual understanding between engineers and cyber security experts. The failure scenarios were also integrated in a tabletop exercise and used to prioritize cyber security planning activities within the GTI/OTD Cybersecurity Collaborative.

3.1 Cyber Security Analysis

Critical infrastructure, industrial control systems and operational technology present unique challenges for cyber security techniques and practice. These specialized domains have legal and regulatory requirements and performance constraints that affect the application of cyber security. Straightforward applications of existing information technology security mechanisms do not always work. Sometimes it requires a minor porting effort; sometimes, although the technology may function out-of-the-box, it does not offer the same benefits as in an information technology environment; at other times, it requires a completely new method or major redesign; and yet other times, it is completely unworkable due to the unique demands of the operational environment. Nevertheless, these complex cyber-physical systems likely contain unintended, latent errors in their software, hardware and procedures, and therefore require monitoring and protection techniques that are suited to the domain. Some of the potential faults, flaws and vulnerabilities exist because of specific combinations of software and equipment, or might only be exercised under very special conditions.

Thus, a critical question for infrastructure owners and operators is how their assets could be made to fail by a variety of threat actors exercising unanalyzed – indeed previously non-existent – system states that result from injecting computerized monitoring and control into physical processes. Asset owners need to comprehend the nature of the threats to the operational technology environment and how and where cyber security protection, detection and control mechanisms should be deployed. Understanding how a system will break or could be made to break are difficult tasks during the hard work of conceiving how the system should properly operate in the first place [8, 9].

Such a conceptualization activity is even harder when applied to systems of systems or where there may be cascading effects due to interdependencies within and across the energy or other critical infrastructures – as there are between natural gas and electric power. To wit, natural gas is used to generate electricity and bulk electric power is used to run some compressor stations that move natural gas. Likewise, if a cyber attack on a communications infrastructure can cause or exacerbate an impact on electricity, gas or both, then because of these interconnections, an event at one location could cascade to multiple events at different locations. The emergent effects that loss of power and storm damage have on the cellular communications infrastructure were evident after Hurricane Sandy: while the cellular infrastructure was mostly undamaged, communications ramped up dramatically due to an increase in calls (because the Internet and other powered infrastructure were out or damaged) and cell tower energy reserves were expended much faster than anticipated. The Liberty Eclipse Exercise [13] has investigated the cyber security concerns surrounding this type of interdependency between natural gas and electric power.

3.2 Understanding Mitigations

Natural gas utilities are looking for procedures that can help avoid significant disruptions of gas flow and destruction of property and infrastructure. Utilities can use product assessments to understand the value of existing mitigations. This process entails iterating through a series of commodity point solutions from a variety of vendors to assess the promised coverage.

A complementary approach for exploring the parameters related to the value of mitigations and utility preparedness is to specify failure modes of concern and work backward to the types of threats that might induce the failures. In short, a framework that categorizes failures is a useful assessment tool for determining the utility and appropriateness of cyber security tools and mechanisms. Designing, enumerating and analyzing failure scenarios can help explore the assumptions made on the operational side, the value of current mitigations and the need for certain types of protection mechanisms. Failure scenarios provide a combination of flexibility, abstraction (e.g., a baseline for further discussion and exploration) and specificity that compare well with analysis techniques that rely on models derived from vulnerability enumeration (e.g., attack trees) and attacker tactics.

4. Caveats and Assumptions

This work has multiple audiences: researchers, practitioners, engineers and regulators. As such, it is important to clearly state the caveats and assumptions that underlie the approach. To the operational technology community, the scenarios are a form of future-gazing and a suspension of disbelief ("our system doesn't work like that" or "our system can't be compromised in that way") might be necessary. It is worth noting that there is a first time for everything and so-called "system failures" arise exactly because a number of seemingly unrelated and unlikely events occur together.

The capabilities and components considered in this work are taken from a representative, notional architecture of the natural gas distribution network. They are not intended to capture or imply existing weaknesses in company infrastructures nor do they directly account for multiple levels of mitigations that may be in place.

The scenarios discussed here do not constitute implied claims or guarantees of successful exploitation nor do they imply that utilities have unmitigated vulnerabilities, are out of compliance with regulations or could be compromised. Some failure scenarios may require significant resources from a potential adversary whereas others may involve an insider taking advantage of an existing crisis or low probability event.

As such, this work does not seek to provide a cookbook for attackers nor is it intended to be a checklist for security defenses. Also, the enumeration of scenarios is not expected to be complete. Furthermore, the goal is not to find holes that utilities have not considered or to claim that specific mitigations in

place would not work, but rather to explore what might happen if some of the mitigations were to fail.

Mitigations include redundant communications, private networks, multiple layers of access control and clear separation of duties (e.g., mostly operate locally, not from the central operations center). Mitigations, however, may fail for any number of reasons: software bugs, expired keys, social engineering, human laziness and complacency, unusable technology or a combination of these shortcomings. Vigilance about the hygiene of operational facilities (e.g., no BYOD policy, vetted upgrades and no removable media) is difficult to maintain at a high level.

Finally, a failure mode need not result in catastrophic damage to an installation, environmental impact or loss of life. It may also relate to compromises of the integrity, confidentiality and availability of information/operational technology assets, as well as the loss of business information and company reputation.

5. NESCOR Failure Scenarios Report

The most relevant starting point in the effort to develop a representative set of failure scenarios in the natural gas distribution network was the NESCOR document [11], which was produced by a broad collaboration between the Electric Power Research Institute, industry experts, asset owners and academia. The NESCOR document has several contributions that make it an attractive template for adaptation. It clearly identifies the major categories of operations across the electric power grid, specifies a comprehensive threat model and lists impacts and potential mitigations.

Version 3 of the NESCOR report from December 2015 contains 129 scenarios across eight categories:

- **Advanced Metering Infrastructure (AMI):** 32 scenarios.
- **Distributed Energy Resources (DER):** 26 scenarios.
- **Wide-Area Monitoring, Protection and Control (WAMPAC):** 12 scenarios.
- **Electric Transportation (ET):** 16 scenarios.
- **Demand-Response (DR):** 7 scenarios.
- **Distribution Grid Management (DGM):** 16 scenarios.
- **Generation:** 16 scenarios.
- **Generic:** 4 scenarios.

The template has four components for each failure scenario: (i) scenario description; (ii) relevant vulnerabilities; (iii) impact; and (iv) potential mitigations. The NESCOR report lists a threat model that covers cyber threats ranging

from intentional and malicious actions to accidental failures. The following threats identified in the report apply equally well to the natural gas distribution infrastructure:

- Adversaries with intent, driven by money, politics, religion, activist causes, recreation, recognition or malevolence.
- Adversary activity may include spying or have direct operational impact.
- Insiders or outsiders, groups or individuals.
- Failures of people, processes and technology, including human error.
- Loss of resources, in particular, key employees and the communications infrastructure.
- Accidents.
- Natural hazards as they impact cyber security (e.g., flooding, foundations, pipelines above and below grade, and wind/blowing gas).

The NESCOR document also lists a number of specific impacts for the failure scenarios that apply to the natural gas distribution infrastructure. These include loss of power, equipment damage, human casualties, revenue loss, customer privacy violations and loss of public confidence.

6. Approach

Significant work is required to derive failure scenarios in different critical infrastructure verticals. During the effort, it was discovered that the adaptation was not necessarily sped up by attempting faithful replication of existing failure scenario specifications. Instead, a comparative analysis was conducted to understand and then deconstruct the essential elements of scenarios. When appropriate, certain scenarios that did not easily translate or provide adequate fidelity were discarded. Ultimately, the set of failure scenarios must be relevant (i.e., speak to the threats that concern gas distribution utilities) and realistic (i.e., not be too generic). The bottom line is that the mapping is neither easy nor straightforward. Effort is needed to identify the real risks with respect to the actual infrastructure – some risks are out of scope, others are irrelevant and some are of concern only in the far future.

The goal was not to dramatically expand the number of scenarios by tweaking minor properties, such as constructing two variants of the same scenario by placing the attacker at different locations, or having an attacker who is a trusted insider in one variant and an external attacker who steals legitimate credentials in another instance. For variety and as realism dictated, only attacker and scenario properties that made sense and were relevant to mitigation were considered.

The following four complementary approaches were employed to generate failure scenarios:

- Directly translate the applicable categories of the NESCOR failure scenarios report (AMI, DER, WAMPAC, DR, ET and DGM).
- Learn from experienced operators about real and hypothetical failure scenarios.
- Review the relevant incident reports produced by the Pipeline and Hazardous Materials Safety Administration (PHMSA) [15] and Transport Canada Pipeline [18], and posit cyber contributions to physical failures.
- Conduct mental walkthroughs of standard network security threats on a notional architecture along with the Transportation Security Administration (TSA) Pipeline Security Guidelines [19–21, 23].

During the first approach, only advanced metering infrastructure (AMI) and wide-area monitoring, protection and control (WAMPAC) translated easily. Distributed energy resources (DER) did not translate well because residential customers do not generate natural gas. Demand-response (DR) was not applicable; although some smart home appliances (furnaces, dryers, ovens, stoves and water heaters) run on natural gas, there is not the same requirement for responsive demand (or load) shedding in the power grid. Although natural gas distribution sometimes has peak demand (i.e., winter) concerns, the scale and degree of control are not as significant as in the smart grid. The concept exists, but largely as a manual process and coordination with large industrial customers, not residential customers. Electric transportation (ET) did not translate well because natural gas refueling does not have the same semantics (in terms of planning optimal recharging or supporting customer chargeback); instead, the cyber risks are very similar to those faced by common gasoline refueling. However, some aspects of distributed grid management (DGM) can be adapted due to custody exchanges and multiple downstream customers supplied by large providers.

With the rough narrative examples provided by the approaches listed above, the procedure for generating failure scenario descriptions (i.e., fleshing out the template) involved:

- Prerequisites:
  - Reasonable notional architecture for each setting (inventory of devices, processes, people).
- End result:
  - Not necessarily catastrophic system-wide total loss; outcomes may vary in scope and severity.
- Key spectrum of setting variations to generate concrete examples:
  - Natural or attacker-induced failure of a single component.
  - Sequence of events targeting multiple components.

– Sequence of events plus interference with protection/remediation efforts.

For this last piece, attacker actions were drawn from two sources. The first included standard network security threats and the second specific types of attacks against the natural gas infrastructure. This helps bridge the gap between general threats and domain-specific threats. Another alternative might be to adapt a model of attacker tactics, techniques and procedures such as MITRE's ATT&CK Matrix [10, 17], which provides a structured menu of attacker actions and tactics for achieving capabilities in a target infrastructure.

Given the focus on remotely-commanded infrastructure, attackers typically engage in the following passive and/or active operations against network communications:

- Eavesdropping (threat to confidentiality).
- Injecting manufactured messages (valid and nonsensical).
- Dropping messages (all, selected and random).
- Network congestion leading to dropped messages (denial of service).
- Redirecting messages to unintended destinations and to self.
- Rewriting messages to legitimate recipients with fabricated data and commands.

While methods such as cryptography and strong authentication can be applied to protect against some of these attacks, they are difficult to deploy and manage in operational technology environments. Specialized threats to the domain include network and software compromises, supply chain attacks and infected maintenance and vendor laptops. Specific risks include attacker actions as well as conditions that facilitate attacker operations:

- Infiltrate the central or backup gas operations center and access on-site programmable logic controllers (PLCs).
- Obtain physical access to the facility, embed malware in the system or in auxiliary systems (e.g., heating, ventilation and air conditioning (HVAC) systems, pumps and monitoring systems).
- Compromise the vendor and supply chain.
- Introduce unauthorized USB, CD and DVD drives in the local control center or gas operations center.
- Scramble GPS receivers.
- Conduct local snooping in the wireless radio frequency (RF) and electromagnetic (EM) domains.

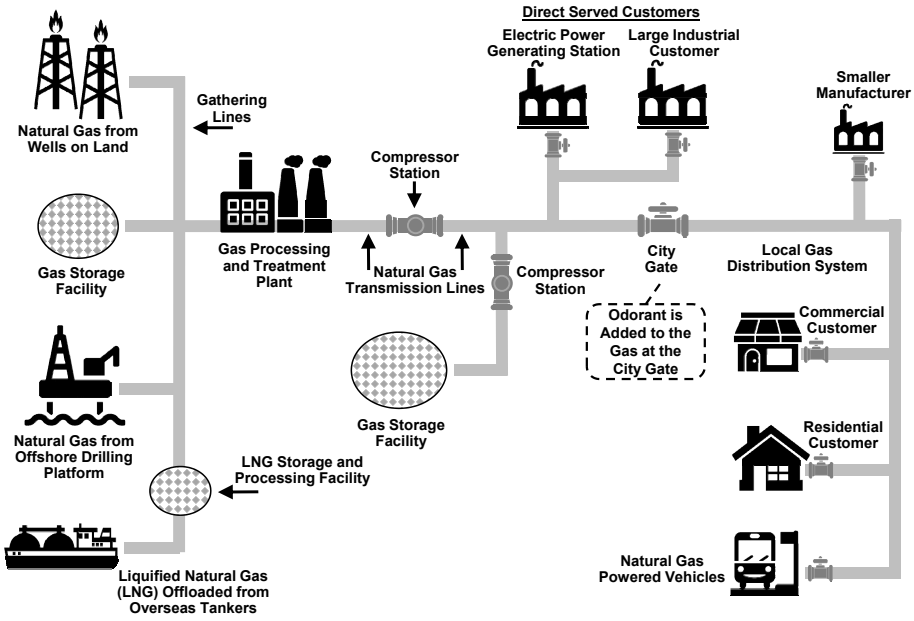

Figure 1. Natural gas distribution network.

- Subvert software upgrade procedures.
- Leverage the lack of operator visibility into supervisory control and data acquisition (SCADA) device internals and operating software.
- Physically link to unattended infrastructure assets and establish remote connections (e.g., modem to programmable logic controller to meter).

7. Analysis of Scenarios by Category

Defining meaningful failure scenarios requires a realistic architecture of the natural gas distribution network. Figure 1 shows the notional architecture [14]. Natural gas extraction and production occur on the left-hand side of the figure and the gas flows toward customers on the right-hand side. Along the way, long-range gas transmission is supported by major compressor stations along the pipeline routes. Compression plays the dual role of moving the product and storing it in the pipeline system (a concept referred to as "linepack"). Separate dedicated storage facilities may be used. High-pressure transmission pipelines transition to lower-pressure distribution lines at major tap points called gate stations (or "city gate" stations) and large industrial customers such as heavy manufacturing and electric power generation facilities. Local distribution lines step down the gas pressure to lower street-level values that depend on the age

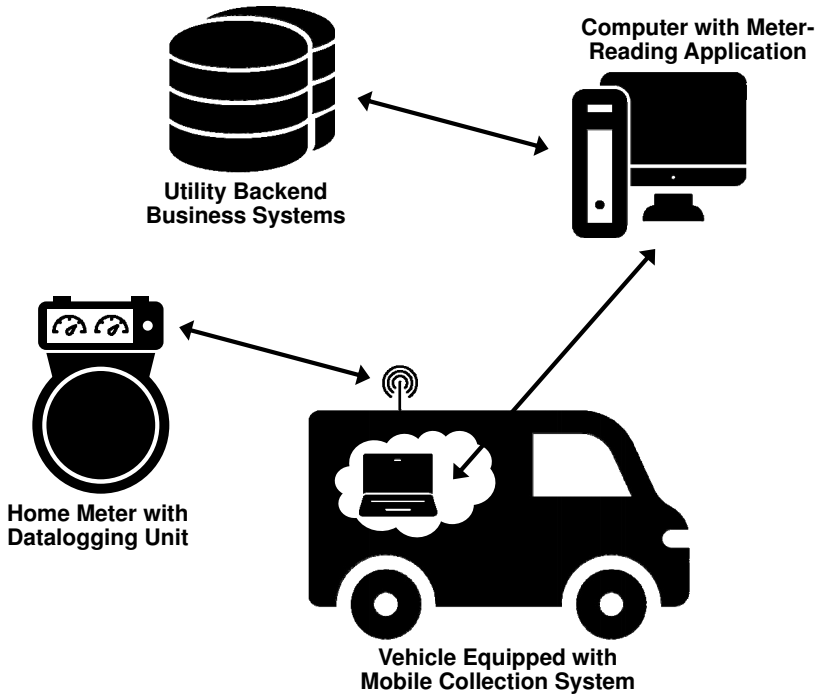

Figure 2. Vehicle-mounted automated meter reading system.

and condition of the local piping and the needs of customers ranging from residential to commercial (e.g., schools, offices and hospitals).

The failure scenarios are organized into categories that are mapped to the major natural gas distribution network components mentioned above. A total of 55 scenarios are specified. The scenarios are categorized as follows:

- **Automated Meter Reading (AMR):** 18 scenarios (AMR.1–AMR.18).
- **City Gate Station**
  - **Facility Information (FI):** 11 scenarios (FI.1–FI.11).
  - **Shutoff Valve (SV):** 7 scenarios (SV.1–SV.7).
  - **Metering (M):** 5 scenarios (M.1–M.5).
  - **Odorizer (O):** 4 scenarios (O.1–O.4).
  - **Heating Plant (HP):** 3 scenarios (HP.1–HP.3).
- **Compressor Station (CS):** 7 scenarios (CS.1–CS.7).

The natural gas distribution network failure scenarios largely follow the structure of the NESCOR failure scenarios developed for the electric sector. Each failure scenario has a description, relevant vulnerabilities and an impact. The specification of potential mitigations is the subject of future work.

7.1 Automated Meter Reading

Automated meter reading, which is conducted for billing purposes at residential, commercial and industrial sites, employs specialized handheld, vehicle mounted or airborne reader devices. Figure 2 shows a vehicle-mounted automated meter reading system. The mobile collection system connects to a home meter with a data logging unit to obtain the meter reading. The data is received by a computer with a meter reading application that sends the data to utility backend business systems.

The meters are usually battery powered; their serial numbers are not secrets and can be discovered via scanning. Communications are transmitted in the clear. The protocols employ non-cryptographic checksums for error correction.

Typical home appliances that rely on natural gas are furnaces, stoves and water heaters. Meters that support automated reading generally have limited power and computational resources. However, future designs will support advanced functionality and demand-response management (as in the smart grid), and would possibly employ Internet of Things (IoT) protocols to communicate directly with home appliances. Future meters are also expected to support dynamic pricing and remote shutoff (e.g., for safety).

Tables 2 through 4 present the eighteen automated meter reading failure scenarios (AMR.1–AMR.18). The scenarios focus on current deployments involving the communications hardware and software in the meter, service vehicle and utility. Automated meter reading failures impact billing and customer relations, and reader device maintenance (e.g., battery life), but not natural gas operations or emergency response.

7.2 City Gate Stations

City gate stations are crucial points in the natural gas distribution network because they are locations where a custody transfer takes place and gas pressure is regulated from the transmission level to the distribution level. As custody transfer points, gate stations require the coordination of the operational practices of organizations, business relationships and physical processes involved in transporting natural gas. Gas may also be odorized and scrubbed depending on the installation and utility.

The infrastructure at a gate station includes shutoff valves, metering devices, odorizers and a heating plant, all of which can be susceptible to cyber-induced failures. Additionally, facility information pertaining to a gate station can lead to failures. The failure scenarios associated with gate stations are structured around these key infrastructure components.

Facility Information. Facility information refers to the physical setting/infrastructure (e.g., security plans, facility designs) and related information technology assets (e.g., access credentials) pertaining to a gate station or other facility. Several failure scenarios involve the unauthorized disclosure of protected critical infrastructure information (PCII) [26], security sensitive information

Table 2. Automated meter reading failure scenarios.

Scenario	Description	Vulnerabilities	Impact
AMR.1	Authorized employee performs unauthorized meter data acquisition system (MDAS) disconnect	Insecure RF channel; limited key management	Reduced consumer confidence; lost revenue for the supplier
AMR.2	Authorized employee manipulates meter data management system (MDMS) data to over/under charge	Unauthorized access to MDMS; no cryptographic integrity; malware	Mischarging; effort to correct billing errors
AMR.3	Invalid access used to install malware enabling remote Internet control	Supply chain; infect readers and/or endpoints	Collection and/or disclosure of customer data
AMR.4	Overused key captured on a meter channel enables usage data manipulation	Applies if crypto is employed; lack of crypto enables manipulation	Untrustworthy data collection; time to remedy errors
AMR.5	Mass meter rekeying when a common key is compromised	Key is extracted from protocol messages or via physical access to units	Effort required to rekey or replace infrastructure; ongoing risk of manipulation
AMR.6	One compromised meter in a network blocks others; interference in the channel	Meters or readers contain malware; local blocking of radio source	Time to rescan customer sites
AMR.7	Deployed meters containing undesirable functionality need repair	Bug and security patching	Time and expense to upgrade meters
AMR.8	False meter data induces unnecessary analytics on the corporate side	Compromised transmitters or homeowner	Data recovery and restoration from backup

Table 3. Automated meter reading failure scenarios (continued).

Scenario	**Description**	**Vulnerabilities**	**Impact**
AMR.9	Invalid messages to meters impact customers and utility	Physical signal or pulse to disable temporarily or permanently	Meter unavailability; battery replacement
AMR.10	Incorrect consumption information impacts utility revenue	Unprotected communications medium enables spoofing or shielding	Effort required to rekey or replace infrastructure; ongoing risk of manipulation
AMR.11	Improper firewall or network access control between reader and corporate network	Readers and/or mobile units are compromised	Significant loss of customer data; access to billing systems
AMR.12	Breach of cellular provider network exposes AMR access	Not under utility control	Loss of customer data
AMR.13	Inadequate security for backend AMR data receivers enables malicious activity	Exposure of networked equipment and data repositories	Replacement costs of equipment and receivers
AMR.14	Malicious creation of duplicate serial numbers or identifiers prevents valid AMR messages	Fake reader; fake tower (for reader-to-office communications)	Effort to reacquire data
AMR.15	Unauthorized devices create denial of service and prevent valid AMR queries and replies	Unprotected communications medium enables spoofing or shielding	Effort to track down or localize problem; law enforcement involvement; reacquire data
AMR.16	Stolen field service tools expose AMR infrastructure	Unattended or unlocked trucks	Loss or exposure of customer data; access to backend
AMR.17	Threat agent performs unauthorized firmware alteration	Update channels for readers and truck communications equipment	Denial of service; battery drain in meters; data disclosure/collection

Table 4. Automated meter reading failure scenarios (continued).

Scenario	Description	Vulnerabilities	Impact
AMR.18	Competitor observes gas consumption at a store or factory	Insecure cleartext protocols permit any party to observe usage data	Competitive advantage and insight into a direct competitor

(SSI) [22] and/or critical energy/electric infrastructure information (CEII) [5] relating to natural gas distribution network facilities.

Tables 5 and 6 present the eleven facility information failure scenarios (FI.1–FI.11).

Shutoff Valves. Gate stations implement a physical process that steps down or regulates the nominal transmission pipeline pressure to distribution pipeline pressure, which is roughly 10% of the transmission pressure. A key safety component in these facilities is an automatic shutoff valve (ASV) or remote control valve (RCV) that permits the gate station to be isolated from the large transmission pipeline in case of a failure or incident in the gate station.

A shutoff valve also provides local, completely manual shutoff in the case of communications or power loss to the motor unit. The operational impact varies on how many valves are compromised. Compromises may have little impact on the system or they could be devastating. Larger impacts may occur if the shutoff valves cannot be operated during an incident, such as system over-pressurization or an explosion.

Table 7 presents the seven shutoff valve failure scenarios (SV.1–SV.7).

Metering. Metering is a critical responsibility of the gate station because it is a handoff point for custody of gas transiting the pipeline.

Several variations in metering setups exist. These include independent meters before and after a tap compared with the distribution company's independent meter on the tap, or jointly-instrumented meters on transmission company pipe. Shared infrastructure assets can present management challenges in coordinating the cyber security practices of the collaborating organizations.

Metering failure scenarios mainly impact other equipment and may require additional operational information or access. Regulators and other equipment have physical safety mechanisms that prevent them from operating outside of safe conditions. Some scenarios require physical access to a station, which may trigger security alarms. In some cases, an attacker may have to corrupt the distribution meter system as well as the transmission meter system, which may be monitored and compared by the utility and the transmission company.

Table 8 presents the five metering failure scenarios (M.1–M.5).

Table 5. Facility information failure scenarios.

Scenario	**Description**	**Vulnerabilities**	**Impact**
FI.1	Risk of disclosure of the relationship between cyber assets and physical infrastructure	Data inference across public sources; observation and surveillance of public facilities	Unauthorized disclosure of PCII and SSI information related to facility location and cyber properties
FI.2	Theft or loss of detailed security plans or facility designs	Inadequate or compromised physical and/or data controls	Unauthorized disclosure of PCII and SSI information related to security plans or facility designs
FI.3	Theft or loss of access credentials	Compromised credentials	Unauthorized access and/or unauthorized disclosure of PCII and SSI information
FI.4	Risk of recording and disclosure of security and safety practices and procedures	Surreptitious observation and surveillance	Unauthorized disclosure of PCII and SSI information related to security and safety practices and procedures
FI.5	Unauthorized, unintentional disclosure by an insider of security and safety system properties, capabilities, configurations and operating procedures	Insider threat – disgruntled or compromised employees	Unauthorized disclosure of PCII and SSI information related to security and safety systems
FI.6	Use of electronic means, tools and online data sources to map physical components of cyber and security systems	Electronic observations and surveillance combined with public information	Unauthorized disclosure of PCII and SSI information related to cyber and security systems

Table 6. Facility information failure scenarios (continued).

Scenario	Description	Vulnerabilities	Impact
FI.7	Extraction of GPS coordinates, settings or other specific location information allows mapping of equipment to physical infrastructure locations	Incorrect configration, software vulnerabilities or weak access control of wireless routable devices	Linking physical locations with specific system identification and vulnerability information leads to leaked CEII and increased attacker capabilities and situational awareness
FI.8	Passive RF monitoring may provide details about communications protocols and infrastructure	RF side channels	Unauthorized disclosure of PCII and SSI information related to communications protocols and infrastructure
FI.9	Corruption and denial of service of security cameras and related systems	Compromised or blinded security cameras or related systems	Hide attack or event requiring attention or hide information needed to respond
FI.10	Attacker pivots through the security camera communications infrastructure	Common physical communications medium used for control and security; compromised third-party communications system	Attacker gains access to both communications streams
FI.11	Unexplained failure of computer communications drops alarms or alerts for a period of time, obscuring the root cause of an incident	Failed communications link	Dropped alarms or alerts obscure the root cause of the incident

Table 7. Shutoff valve failure scenarios.

Scenario	**Description**	**Vulnerabilities**	**Impact**
SV.1	Unauthorized remote user invokes mechanical valve closure	Stolen or lost credentials	Isolated gate station from the transmission system
SV.2	Unauthorized insider invokes unsafe mechanical valve open operation from local human-machine interface (HMI)	Rogue employee accesses unlocked screen or uses an observed password	Unsafe valve operation
SV.3	Damage, disable or remove software functions related to valve control by the PLC	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Modified control logic that ignores open or close commands
SV.4	Issue spurious (i.e., valve closed) status messages to mimic an uncommanded shutoff event	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Depleted trust in the system causes wasted effort
SV.5	Misleading status messages about legitimate commanded valve closure	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Reduced confidence in the equipment or alarm fatigue
SV.6	Unsafe or incomplete assumptions about system state resulting in incorrect attribution of the root cause of alarms	Manipulation of sensor data (selective blocking, partial operation injection or rewriting)	Loss of cyber situational awareness and loss of trust in the system
SV.7	Failure to re-open valve after legitimate event	Corrupt control logic to prevent control messages from reaching the valve motor; spoof or drop legitimate acknowledgement messages to the HMI or gas operations center	Valve appears unresponsive

Table 8. Metering failure scenarios.

Scenario	Description	Vulnerabilities	Impact
M.1	Unauthorized remote user injects false pressure reading in SCADA traffic to the PLC in the local control room	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Potentially dangerous physical operation of a regulator or other critical system
M.2	Unauthorized remote user injects false readings or blocks existing messages from receipt at the local control room or remote gas operations center	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Reporting false good parameter values can lead to a silent pipe or heater breakdown; reporting false bad parameter values can cause delays while sensor readings are checked
M.3	Disable power supply to meter probes	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Disabled data streams to the supplier and distributor
M.4	Unnecessary maintenance caused by spurious unexplained failures of sensor probes	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop	Arbitrary, unpredictable and unexplained errors may cause unnecessary maintenance, repairs or replacement
M.5	Meter readings inconsistent with the linepack models of the transmission operator	Corrupted modeling data or software along with compromised readings from several major gate stations	Could significantly disrupt a major transmission pipeline

Odorizer. In some cases, gas is not odorized during transmission. This is because transporting odorant to remote locations and injecting it in the "middle" of a transmission pipeline may be impractical. Odorant is usually added closer to exit points such as city gates and close-to-terminal compressor stations. Although odorant is often added at a city gate station by a distribution company, in some cases, distribution companies rely on the transmission pipeline operator to inject odorant, but perform an independent verification. The addition of odorant provides an important safety property for consumers.

Table 9. Odorizer failure scenarios.

Scenario	Description	Vulnerabilities	Impact
O.1	Attacker gains access to HMI and reports lower-than-expected or higher-than-expected measurements of odorant in the system	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify displayed sensor readings	Unnecessary increase or decrease in the level of odorant injected into the system
O.2	Attacker gains access to HMI and hides all sensor readings related to odorant levels in the storage tanks and outflowing gas	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to hide displayed sensor readings	Unnecessary maintenance check or possible halt to operations; customers unable to notice gas leaks if enough odorant is not present
O.3	Attacker gains access to odorizer controller and modifies setpoints to increase the amount of odorant injected, resulting in over-odorization of the gas	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to manipulate set-points and possibly disable or modify sensor readings or alarms	Increase in service calls as customers report suspected leaks
O.4	Attacker gains access to odorizer controller and modifies setpoints to decrease the amount of odorant injected, resulting in under-odorization of the gas	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to manipulate set-points and possibly disable or modify sensor readings or alarms	Customers unable to notice existing or induced leaks; escalation of explosive events leading to property damage or loss of life

Table 9 presents the four odorizer failure scenarios (O.1–O.4).

Heating Plant. A critical part of the city gate is the heating plant, which enables safe operations by keeping the gas temperature above the freezing point of water as the gas pressure drops during transmission. The potential for freez-

Table 10. Heating plant failure scenarios.

Scenario	Description	Vulnerabilities	Impact
HP.1	Attacker targets and modifies thermostat readings	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify settings or forge readings	Decreased heating may lead to low gas temperature in regulator piping; overheating may cause inefficient heat exchange or trigger nuisance alarms
HP.2	Remote attacker modifies settings or readings of flow meters for the heat exchange medium	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify settings or forge readings	Increased flow may lead to overheating; reduced flow may lead to decreased heating
HP.3	Remote attacker shuts off pumps or circulation motors that permit the heat exchange medium from entering the boilers or flowing to the regulator piping	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to shut off pumps or motors	Lack of flow may lead to damaged regulator or automatic safety shutdown of regulator

ing exists due to the presence of water in the gas, which is also maintained at the desired level by instrumentation and filtering at the city gate. Should the heating plant fail or be taken out of service, the gate station would have to be isolated from the transmission pipeline, causing loss of revenue and downstream effects on customers large and small, even in the presence of failover or redundant supply to the distribution system from other gate stations.

While heating plants operate relatively simple physical processes, their supporting infrastructure components are targets for attacks. These include thermostats, pumps and flow meters for the heating medium (e.g., glycol).

A heating plant may also be co-located with backup power generation (fed by the gas pipeline) that provides the gate station "hotel" power. Heating plant designs and implementations differ, but the failure scenarios assume there is a programmable logic controller connected in the SCADA network.

Table 10 presents the three heating plant failure scenarios (HP.1–HP.3).

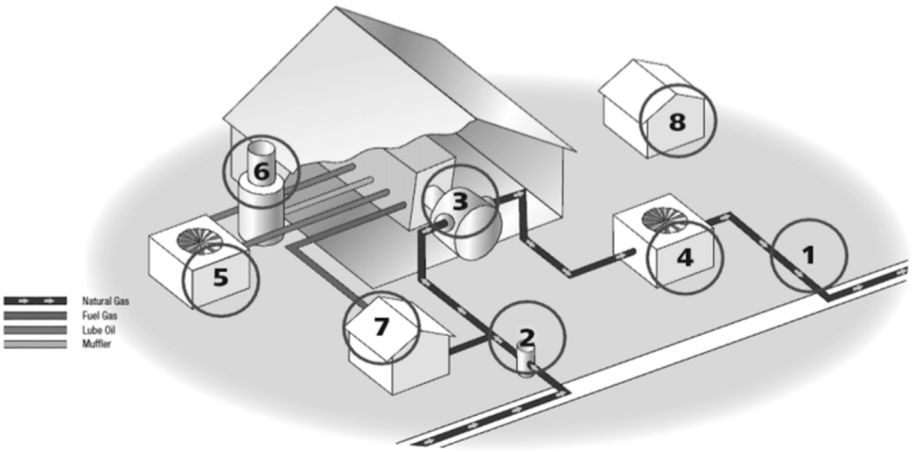

Figure 3. Compressor station yard.

7.3 Compressor Station

Compressor stations have several failure scenarios because they perform a significant physical process and incorporate multiple infrastructure components and smart electronic systems that support, monitor and protect the core process, which may also have a feedback relationship with the electric power grid.

Compressor stations are located at points in the gas system where the gas line pressure must be increased to either increase linepack (i.e., the *de facto* storage of a volume of gas) or push gas downstream through the system. While compressors are present in both transmission and distribution pipelines, they feature prominently in transmission pipelines. As a consequence, compressor station failures in transmission pipelines would have greater impact.

Figure 3 shows a schematic diagram of a compressor station yard (from Spectra Energy). It comprises station yard piping (1), filter separators/scrubbers (2), multiple compressor units (3), gas cooling system (4), lubricating oil system (5), mufflers (exhaust silencers) (6), fuel gas system (7) and backup generators (8).

A compressor station may draw on a larger volume but lower pressure part of the distribution network to concentrate and supply a dense area or several large customers. A compressor station may be paired with a regulator unit to step down pressure if gas needs to be moved from the higher-pressure part of the system back to the lower-pressure portion. The relatively minor difference in pressure places fewer demands on heating; the pressure change may be only about 100 psi, so the temperature change is negligible, roughly 7°F.

Tables 11 and 12 present the seven compressor station failure scenarios (CS.1–CS.7).

Table 11. Compressor station failure scenarios.

Scenario	Description	Vulnerabilities	Impact
CS.1	Suppression of scrubber alarms	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to obscure failure states of scrubbers	Full tanks may go unnoticed; overflow tanks may spill hazardous material
CS.2	Attacker induces anti-surge valve failure	Physical damage to pipe and/or network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify PLC readings	Anti-surge valve is closed or prevented from opening; uncontrolled surge event causes damage or destruction of pipe and/or compressor
CS.3	Remote attacker modifies gas quality readings back to the control center	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify gas quality readings	Hide source of problems with feed to downstream or hide source of condensates in pipe; damage or destruction of pipe and/or compressor
CS.4	Remote attacker modifies firmware or control points of gas quality sensors	Network and software compromise, supply chain attack, or infected maintenance or vendor laptop used to modify firmware or control points	Hide source of problems with feed to downstream or hide source of condensates in pipe; damage or destruction of pipe and/or compressor
CS.5	Failure of compressor process cooling system	Induced or natural failure of process cooling system combined with suppression of high-temperature alarms	Loss of compression; physical damage or destruction

Table 12. Compressor station failure scenarios (continued).

Scenario	Description	Vulnerabilities	Impact
CS.6	Failure of electric power supply to compressor turbines that rely on electric power (as primary source and/or for monitoring and control)	Failure of primary electric power combined with induced or eventual failure of backup generators due to fuel exhaustion	Loss of compression
CS.7	Use of HVAC, auxiliary building control systems or vendor systems as pivot points	Software vulnerabilities, supply chain attacks, poor access control hygiene for vendor/service systems	Establishment of a foothold by the attacker in the environment

8. Lessons Learned

The major lessons of this project relate to performing scenario translations and the cyber security findings.

Lesson 1. During domain translation, it was observed that natural gas distribution incorporates fewer intelligent electronic devices than the electric grid. System properties and business concerns are different because gas and electricity are different physical commodities and their transmission involves significantly different physical processes. Additionally, some parts of the NESCOR report categories simply do not translate because there is no analogous infrastructure component on the gas side or an analogous component exists but has little or no cyber elements.

Lesson 2. Learning about the infrastructure takes time and significant effort. Developing realistic scenarios requires substantial knowledge that must be acquired from domain experts. This requires building trust with utility operators and reviewing authoritative sources such as TSA guidelines, PHMSA reports, device data sheets, vendor case studies about facility installations, and research conducted by academic programs in petroleum engineering and related fields. This engagement facilitated the creation of the notional architecture that provided the setting for failure scenario development.

Lesson 3. When using the failure scenarios, utility personnel should not think in terms of a checklist of mitigations as suggested by current regulatory and TSA guidance, but whether they have an ongoing process for checking security properties that provides easy-to-understand evidence that a monitoring

system is working as intended; in other words, whether or not the cyber security mechanisms in place are operating correctly and observing the cyber-relevant behaviors of the operational technology devices. Because failure scenarios are not meant to be a cookbook for attacks and they rest on the assumption that mitigations could fail, utilities must have a process and not just a checklist that enumerates defenses against specific attacks.

Lesson 4. There is a distinct advantage to being more mechanical. Part of the difficulty in specifying failure scenarios was finding enough details about where computational elements and control processors were located, the equipment to which they were connected and the communications channels that provided access to them. Important pieces of the infrastructure are largely mechanical (e.g., regulators large and small involve physical components and isolated controls).

As the natural gas industry looks toward the future, there will likely be an impetus to embed intelligent electronic devices at a density and rate comparable to the electric power sector. However, before anything is done, the natural gas industry must assess whether this will introduce unjustified risk. Computational elements have latent behaviors that simply do not exist in the case of mechanical equipment.

9. Real-World Application of Failure Scenarios

Significant questions about the utility of the failure scenarios are whether they can be applied in real situations and whether they are tied to real-world concerns. A potential objection to generating and using failure scenarios is that they might be too artificial, and thus lack realism and fail to be beneficial to utilities. The scenario development process compensated for this by engaging with utility personnel and incorporating input from government safety investigation incident reports in the failure scenarios. Indeed, the application of the failure scenarios in the natural gas industry demonstrated that they can model both realistic and real-world scenarios.

One use case is to retroactively study real incidents in terms of combinations of failure scenarios, in essence introducing a synthetic cyber adversary into a real incident. Operators and engineers can model a real incident with a sequence of failure scenarios and re-execute the incident under a what-if analysis while substituting failure scenario elements in the incident timeline.

For example, the San Bruno incident of September 2010 involved the rupture of a 30-inch-diameter intrastate transmission pipeline due to an accidental overpressurization of a "substandard and poorly welded pipe section with a visible seam weld flaw" [12]. This physical material failure was compounded by a number of contributing factors, including side-effects of electrical work that induced false low pressure readings and caused regulator valves to open fully.

Fake pressure readings introduced by an adversary underpin many of the shutoff valve and metering failure scenarios presented in this chapter. During the San Bruno incident, SCADA systems and communications were crucially

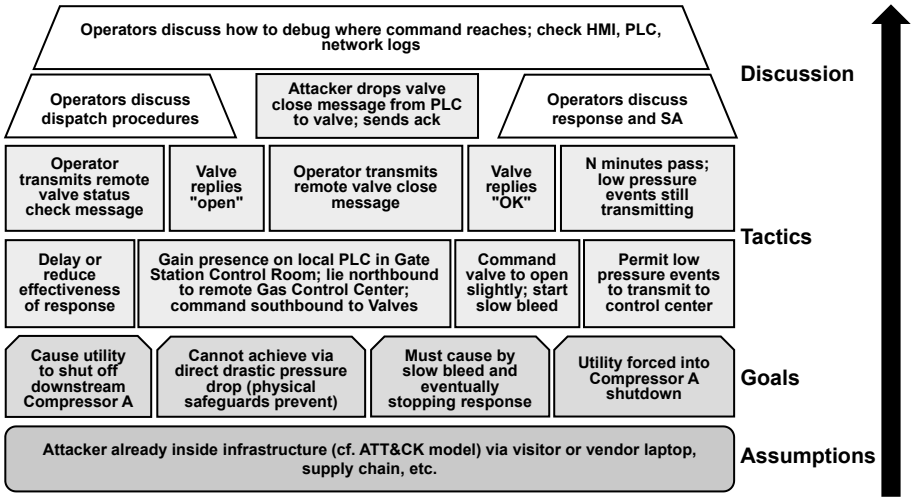

Figure 4. Example tabletop scenario.

important to providing situational awareness. At times during and leading up to the San Bruno pipeline rupture, SCADA system data was not available or reliable due to the side-effects of the repair work; this also affected some control valve positions. Interested readers are directed to the National Transportation Safety Board (NTSB) report on the San Bruno incident [12], especially Sections 1.1.2 and 1.9.1 to note the many opportunities for disrupting SCADA systems that could result in the loss of situational awareness.

Another use case of the failure scenarios is the creation of tabletop exercises. A "low pressure" tabletop exercise scenario was constructed based on real-world events (pipeline incident reports) and some failure scenarios. Figure 4 shows the assumptions, goals and tactics drawn from a small subset of the failure scenarios (FI.10, SV.2, SV.4 and SV.5). These failure scenarios provided the context that supported major discussion topics in the tabletop exercise.

Another way to add realism to a failure scenario is to instantiate it. This can be accomplished in a number of ways, such as in a high-fidelity simulator, by acquiring real equipment or by running it in a test laboratory environment. However, the first step is to provide a concise diagram of the various components.

Figure 5 presents an instantiation of Scenario O.4 of the odorizer, which includes the principal subjects (i.e., actors), objects and an example control and status message exchange. In Scenario O.4, the attacker gains access to the odorizer controller and reduces the amount of odorant that is injected, resulting in under-odorization (see Table 9 for the associated vulnerabilities and impacts). The risk is that real leaks go undetected for a longer period of time than warranted, thus "batching up" and causing a burst of failures over time.

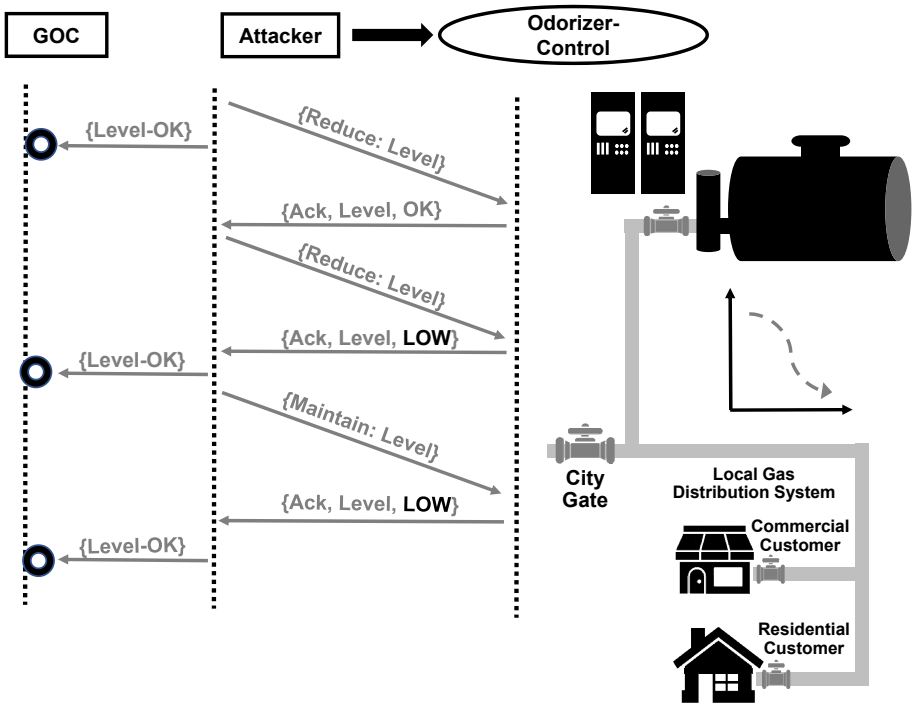

Figure 5. Example odorizer scenario.

A future line of work is to specify a common graphical language to diagram failure scenarios. Ultimately, this would be another structured way to specify failure scenarios that bind abstract objects such as the odorizer controller and the SCADA protocol to specific products and protocols. Diagramming scenarios provides additional details that tie the abstract scenarios to real-world equipment and communications protocols along with adversary actions.

10. Related Work

The failure scenarios for the electric sector discussed in the NESCOR report [11] provided the inspiration and model for this research. Indeed, the focus of this chapter has been a comparative analysis of the failure scenarios for the gas sector and the NESCOR scenarios for the electric sector.

A recent (March 2018) TSA document [21] provides best practices and guidance that extend over the entire gas distribution enterprise. Some of the facility information scenarios described in this work were drawn from the TSA best practices and guidance.

Failure mode modeling is a common practice in reliable systems engineering that is often used to design dependable computing systems. Failure mode and

effects analysis (FMEA) is a systematic approach for collecting and analyzing the conditions under which system components might experience failure. Effective failure mode and effects analyses are informed by experience with statistical evidence pertaining to the prior behavior and failures of similar systems.

A closely-related piece of work is the Waterfall Security Solutions review of 20 prototypical attacks on industrial control networks [28]. The review sketches a number of scenarios in an example water control system. A significant benefit is the consideration of attackers with differing capabilities and placements in a notional architecture and standard defenses against attacks that originate from a number of locations in the topology.

Attack graphs have been an active area of cyber security research for decades. Seminal work [2, 16] introduced the notion of linking vulnerabilities across a network of host computers to provide a structured method for assessing attack impacts. Hawrylak et al. [6] have applied these notions to an industrial control system environment. Recent work by Wang et al. [27] extends the concept to consider probabilistic modeling, which is related to the use of failure scenarios as an analysis and "what if" tool for utilities.

The Lockheed-Martin "cyber kill chain" concept [7] identifies the phases that cyber attackers must complete to achieve their objectives, which enables defenders to map their courses of action to adversary kill chain indicators. Similarly, the MITRE ATT&CK model [10, 17] provides a structured menu of attacker actions and tactics aimed at achieving specific capabilities in a target infrastructure. The model was originally developed as a community resource for enterprise environments, but MITRE is currently working on applying ATT&CK to industrial control systems in the electric power, gas, water and transportation sectors [1]. The failure scenarios described in this chapter do not seek to provide a cookbook for attackers nor are they intended to be a checklist for security defenses. However, future work may leverage ATT&CK to provide more specificity to the failure scenarios, especially for activities such as tabletop exercises.

11. Conclusions

One of the most important questions facing critical infrastructure owners and operators is how their assets could be made to fail by cyber threat actors. The 55 failure scenarios in the natural gas distribution infrastructure presented in this chapter were created to provide a cyber security analysis framework for natural gas utilities. Designing, enumerating and analyzing failure scenarios help explore the assumptions made on the operational side, the value of current cyber defenses and the need for new protection mechanisms.

In addition to describing the multi-pronged approach used to develop the failure scenarios for the gas sector, the chapter compares them against scenarios developed for the electric sector. The focus is on the concepts underlying the failure scenarios and their use, the threat model they encompass and the assumptions, lessons learned and caveats underpinning their creation. The scenario development process and the differential comparison between the natural

gas and electricity domains provide a roadmap for developing failure scenarios in other critical infrastructure sectors.

Future research will extend the scenarios by adding more specificity, expanding them to other areas of the natural gas infrastructure and exploring interdependencies within natural gas systems and between natural gas and other sectors. Attempts will also be made to measure the coverage of the failure scenarios. Additionally, efforts will focus on a more comprehensive mapping of real-world incidents against the failure scenario library as it increases in coverage and specificity.

Any opinions, findings, conclusions or recommendations expressed in this chapter are those of the authors and do not necessarily reflect the views of the U.S. Department of Homeland Security, and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Department of Homeland Security or the U.S. Government.

Acknowledgements

This work was sponsored by the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) under Contract No. HSHQDC-16-C-00034. The authors thank DHS S&T Program Manager, Mr. Gregory Wigton, and the GTI Program Manager, Mr. James Marean, for their guidance and support. Thanks are also due to the member utilities in the GTI/OTD Cybersecurity Collaborative for providing valuable insights into the natural gas distribution infrastructure and potential failure scenarios. Additionally, the authors thank the project participants from the Pacific Northwest National Laboratory (PNNL) and MITRE Corporation.

References

[1] O. Alexander, ICS ATT&CK, presented at the *Thirty-Third Annual Computer Security Applications Conference*, 2017.

[2] P. Ammann, D. Wijesekera and S. Kaushik, Scalable, graph-based network vulnerability analysis, *Proceedings of the Ninth ACM Conference on Computer and Communications Security*, pp. 217–224, 2002.

[3] Automation Federation, LOGIIC: Improving Cybersecurity in the Oil and Natural Gas Sector, Research Triangle Park, North Carolina (`www.automationfederation.org/Logiic/Logiic`), 2019.

[4] Cyber Resilient Energy Delivery Consortium, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana, Illinois (`cred-c.org`), 2019.

[5] Federal Energy Regulatory Commission, Critical Energy/Electric Infrastructure Information (CEII), Washington, DC (`www.ferc.gov/legal/ceii-foia/ceii.asp`), 2019.

[6] P. Hawrylak, M. Haney, M. Papa and J. Hale, Using hybrid attack graphs to model cyber-physical attacks in the smart grid, *Proceedings of the Fifth International Symposium on Resilient Control Systems*, pp. 161–164, 2012.

[7] E. Hutchins, M. Cloppert and R. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, *Proceedings of the Sixth International Conference on Information Warfare and Security*, pp. 113–125, 2011.

[8] M. Locasto, Helping students 0wn their own code, *IEEE Security and Privacy*, vol. 7(3), pp. 53–56, 2009.

[9] M. Locasto and M. Little, A failure-based discipline of trustworthy information systems, *IEEE Security and Privacy*, vol. 9(4), pp. 71–75, 2011.

[10] MITRE Corporation, ATT&CK Matrix for Enterprise, Bedford, Massachusetts (`attack.mitre.org`), 2019.

[11] National Electric Sector Cybersecurity Organization Resource, Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, Washington, DC (`smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf`), 2015.

[12] National Transportation Safety Board, Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California, September 9, 2010, Pipeline Accident Report NTSB/PAR-11/01, Washington, DC, 2011.

[13] Office of Electricity, Liberty Eclipse Exercise Summary Report, U.S. Department of Energy, Washington, DC (`www.energy.gov/oe/articles/liberty-eclipse-exercise-summary-report`), 2017.

[14] Pipeline and Hazardous Materials Safety Administration, Natural Gas Pipeline Systems, U.S. Department of Transportation, Washington, DC (`primis.phmsa.dot.gov/comm/naturalgaspipelinesystems.htm`), 2019.

[15] Pipeline and Hazardous Materials Safety Administration, Pipeline Failure Investigation Reports, U.S. Department of Transportation, Washington, DC (`www.phmsa.dot.gov/safety-reports/pipeline-failure-investigation-reports`), 2019.

[16] O. Sheyner, J. Haines, S. Jha, R. Lippmann and J. Wing, Automated generation and analysis of attack graphs, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 273–284, 2002.

[17] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington and C. Thomas, MITRE ATT&CK: Design and Philosophy, MITRE Product MP 18-0944-11, MITRE Corporation, McLean, Virginia, 2018.

[18] Transportation Safety Board of Canada, Pipeline Transportation Safety Investigations and Reports, Gatineau, Canada (`www.bst-tsb.gc.ca/eng/rapports-reports/pipeline/index.asp`), 2019.

[19] Transportation Security Administration, Pipeline Security and Incident Recovery Protocol Plan, Pentagon City, Virginia, 2010.

[20] Transportation Security Administration, Pipeline Security Smart Practice Observations, Pentagon City, Virginia, 2011.

[21] Transportation Security Administration, Pipeline Security Guidelines, Pentagon City, Virginia, 2018.

[22] Transportation Security Administration, Sensitive Security Information, Pentagon City, Virginia (www.tsa.gov/for-industry/sensitive-security-information), 2019.

[23] Transportation Security Administration, Surface Transportation, Pentagon City, Virginia (www.tsa.gov/for-industry/surface-transportation), 2019.

[24] Trustworthy Cyber Infrastructure for the Power Grid, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana, Illinois (tcipg.org), 2019.

[25] U.S. Department of Homeland Security, LOGIIC: Linking the Oil and Gas Industry to Improve Cybersecurity, Science and Technology Directorate, Washington, DC (www.dhs.gov/science-and-technology/logiic#), 2016.

[26] U.S. Department of Homeland Security, Protected Critical Infrastructure Information (PCII) Program, Washington, DC (www.dhs.gov/pcii-program), 2019.

[27] L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia, An attack graph-based probabilistic security metric, in *Data and Applications Security XXII*, V. Atluri (Ed.), Springer, Berlin Heidelberg, Germany, pp. 283–296, 2008.

[28] Waterfall Security Solutions, The Top 20 Cyber Attacks on Industrial Control Systems, Rosh Ha'ayin, Israel (waterfall-security.com/20-attacks), 2018.