LLNL-TR-805864

Lawrence Livermore National Laboratory

Dragonstone Strategy – State of Cybersecurity in the Oil & Natural Gas Sector

February 05, 2020

Disclaimer

Executive Summary

The oil & natural gas (ONG) system touches every corner of the nation and increased communications & control capabilities have not only allowed for greater efficiency of system operation, but have also created a massive target for adversaries to launch cyber-attacks. Like any other heavy industrial process, the ONG system relies on a complex system of information technology (IT) and operational technology (OT) devices.

The current state of cyber-preparedness across the ONG industry varies from organization to organization. Among the most common challenges that ONG companies face are remote locations, long-lived field assets, and lacking capabilities to find and track malware on their systems. ONG companies tend to be concerned with lack of cyber-awareness from employees, risk stemming from remote access for operations & maintenance, and software vulnerabilities within third-party equipment. Various industry and government organizations are performing research and development activities to address some of these challenges, but in many cases industry stakeholders are not aware of solutions that already exist. It is clear that a need exists for a coherent, comprehensive, multi-layered strategy for assuring the security and resilience of the nation's pipeline infrastructure against cyber threats.

For a variety of reasons, the general consensus from stakeholders interviewed by LLNL is that the state of cyber-security within the electric grid is currently outpacing its ONG cousin. Existing strategies for the resilience and cyber-security of the electric grid can and should be leveraged to provide immediate benefits to the ONG system.

In LLNL's view, there are two key factors currently limiting the development of necessary cyber-practices within the ONG industry:

- The sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for ONG cyber-security makes it difficult to create a comprehensive, directed, and coherent strategy that is applicable to all players within the ONG industry
- The ONG industry is unaware of potentially useful technologies that have been developed for ensuring cyber-security of other infrastructure systems, such as the electric grid. Leveraging these technologies—and the science and engineering behind them—can provide some low-hanging fruit that can greatly improve cyber-security in the ONG industry without significant investments in terms of time and money.

In the months following this report, LLNL will continue to perform outreach to key oil & gas industry stakeholders in a continual effort to identify the most pressing cyber-resilience issues in the industry. This outreach will be supplemented with LLNL's threat intelligence capabilities to begin painting a clearer picture of the overall threat landscape faced by this sector. This assessment will be threat-informed and while the strategy itself will not be classified we will leverage intelligence analysis and adversary capabilities to identify gaps in current cybersecurity practices for oil & gas pipeline systems. Recommended efforts will be compiled into a cyber-resilience roadmap for the oil & gas pipeline sector, in which LLNL will highlight priority activities to immediately improve the state of cyber-resilience in the industry.

Table of Contents

Section 1

Introduction

1.1 Report Introduction

This report has been developed by Lawrence Livermore National Laboratory (LLNL) for the Department of Homeland Security (DHS) National Risk Management Center (NRMC) as part of the Dragonstone Strategy project. The goal of this project is to develop a coherent, comprehensive, multi-layered strategy for assuring the security and resilience of the nation's pipeline infrastructure against cyber threats. This involves engagement with stakeholders within the oil & natural gas (ONG) sub-sector to create a framework that highlights the types of capabilities, system characteristics, and R&D efforts that are required to ensure a secure and resilient pipeline system. This analysis will be threat-informed and while the strategy itself will not be classified we will leverage intelligence analysis and adversary capabilities to identify gaps in current cybersecurity practices for oil & gas pipeline systems. The framework developed through this project can help inform a long-term roadmap that can guide prioritization and resource allocation for decision makers.

The security of the nation's critical energy infrastructure is of paramount importance. While significant progress has been made in addressing resilience and security risks on the nation's electric grid infrastructure, the oil & natural gas (ONG) portion of the energy sector has historically not received the same level of attention. Despite this, the risks faced by the ONG sub-sector are greater than ever. Extreme weather such as the Polar Vortex events of 2014 & 2019 highlight the risk of insufficient infrastructure for the delivery of fuel to wide regions and the margin for any additional disruption during these events is minimal. There is an increasing threat of cyber-attacks on the pipeline sector as evidenced by a wave of spear-phishing attempts on personnel in the gas pipeline industry in 2011 & 2012, and a successful breach of Energy Services Group in 2018. In a statement to the Senate Select Committee on Intelligence, Director of National Intelligence Daniel Coats states "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States[1]" .

This report is intended to lay a foundation for the project by surveying the current state of affairs in cyber-security research and development within the ONG industry. Upon the conclusion of the report, LLNL will build upon this foundation to develop its threat-informed strategy for ONG pipeline cyber-resilience.

[1] https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf January 17, 2019

Section 2

Operation of the Oil & Gas Sub-Sector

2.1 Organization of the Oil & Natural Gas System

The ONG system in the United States traces its roots to the early 19th century when natural gas was first produced in Fredonia, New York. By the mid-19th century, oil production had begun in western Pennsylvania. Since then, the ONG industry has undergone a series of massive shifts that have led to the system we have today. Long-haul pipes, originally made of wood or cast iron, have been replaced by steel and plastic; system operations, once an entirely manual process, have been streamlined by wide-area communications and automated control systems; and widespread availability of oil & gas for end-use customers has led to ONG infrastructure permeating every corner of the country.

Processes within the oil and gas industry are generally categorized as belonging to upstream, midstream, or downstream sectors. Portions of this report will refer to these segments of the oil and gas industry. Definitions for each of these sectors is provided below, per International Organization for Standardization (ISO) standard 14224[2]:

> Upstream: business category of the petroleum industry involving exploration and production. Example: offshore oil/gas production facility, drilling rig, intervention vessel.
>
> Midstream: business category involving the processing, storage and transportation sectors of the petroleum industry. Example: transportation pipelines, terminals, gas processing and treatment, LNG, LPG and GTL.
>
> Downstream: business category most commonly used in the petroleum industry to describe post-production processes. Example: refining, transportation and marketing of petroleum products

Figure 1 illustrates the general layout of the upstream, midstream, and downstream delivery systems for the oil and gas networks.

[2] https://www.iso.org/obp/ui/fr/#iso:std:iso:14224:ed-3:v2:en

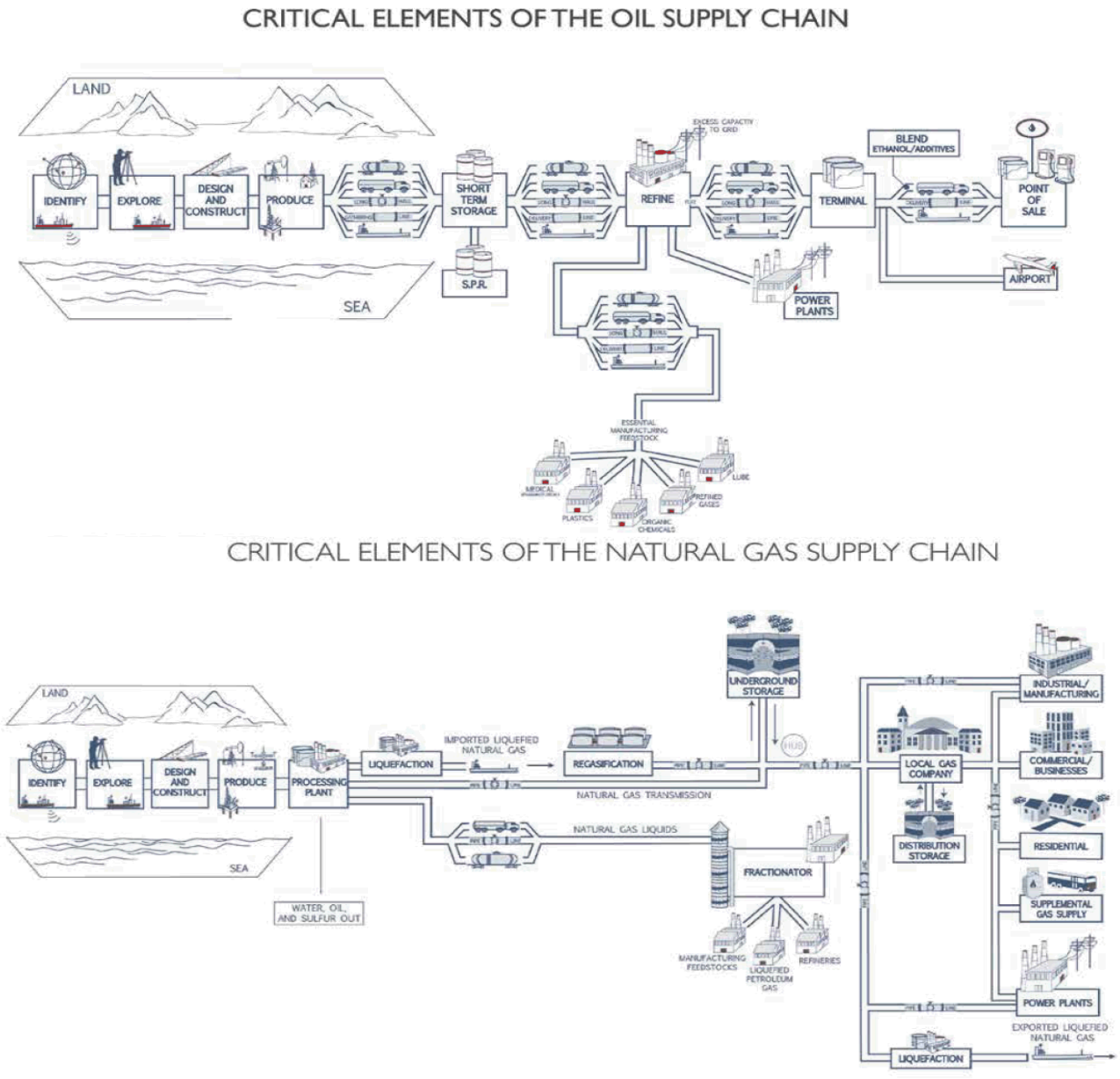


Figure 1: Simplified overview of the supply chain for the oil and natural gas systems. Source: API Oil and Natural Gas Industry Preparedness Handbook, 2016

2.2 Oil & Gas Facilities and Control Equipment

2.2.1 Exploration and Production

Upstream oil and gas processes begin with exploration, wherein petroleum geologists identify areas with large deposits of hydrocarbons. These deposits can be primarily oil-focused, gas-focused, or a mixture of the two. Once identified, these areas can be targeted with complex drilling equipment called “rigs”. While the term rig can be used to describe small, highly mobile drilling units, for the purpose of this report, the

term rig will be used in reference to large, industrial-scale operations. As of January 2020, there are 129 gas-focused drilling rigs in operation and 667 oil-focused rigs[3].

The primary purpose of a drilling rig is to create holes to allow for oil and gas to escape the reservoirs and rise to the surface. Once a hole is created, the well can be "completed". This includes putting into place the necessary equipment to ensure safe, secure, long-term extraction of oil & gas from the well. Drilling and completion activities rely on industrial control systems for machinery operation, but still involve a large amount of human operation and oversight. Compared to processes in the midstream and downstream sectors, the equipment involved in exploration and production has relatively little interconnected control and communications systems.

2.2.2 Processing

After the oil or gas is extracted from the well, it is sent to processing facilities via gathering lines. For oil, processing involves the separation of the raw crude into individual products through distillation. These products include gasoline, diesel fuel, liquefied petroleum gas (LPG) and others. For natural gas, processing involves the removal of water, carbon dioxide, and other impurities. It also includes the separation of natural gas liquids (NGLs) such as butane, ethane, propane, and natural gasoline. These NGLs are used in a wide variety of other industrial processes and are typically sold separately from the pure natural gas.

Being heavy industrial processes, oil & gas processing plants rely heavily on industrial control systems (ICS). Control equipment such as programmable logic controllers (PLCs), distributed control systems (DCS), programmable automation controllers (PACs) are widely used, along with motor controllers, human machine interfaces (HMIs), and remote terminal units (RTUs). Because of the high risk to health and safety from fire and release of toxic products, processing plants require robust emergency shutdown (ESD) controls and safety instrumented systems (SIS). Because the composition of raw crude and raw gas can vary greatly depending on the specific reservoir, processing stations may require unique designs to handle the raw products. The United States currently has approximately 135 petroleum refineries[4] and over 500 natural gas processing plants[5].

2.2.3 Pipeline Transportation

Oil and gas are transported over long distances through large-diameter pipelines, typically referred to as transmission lines. In order to facilitate flow through these lines, pumping stations are required for oil, and compressor stations are required for natural gas. Pumping stations typically rely on an external source of electricity to power the pumps, while natural gas compressor stations tend to burn a small portion of the piped gas in order to spin the compressor turbine. However, as environmental restrictions increase, more and more natural gas compressors are converting to external electricity as a power source.

Control equipment present at these pumping and compressor stations includes motor controllers for the pumps and compressors, along with RTU, PLC, PAC, HMI, and DCS. As with processing plants, the high risk of fire and toxic release drives requirements for robust ESD and SIS designs. These stations can be staffed by on-site personnel but may run without any on-site support. In addition, these stations tend to have communications with operations centers, which may allow for remote control over the facility.

[3] Baker Hughes rig count, https://www.eia.gov/naturalgas/weekly/ accessed January 7, 2020

[4] https://www.eia.gov/dnav/pet/pet_pnp_cap1_dcu_nus_a.htm

[5] As of 2017, https://www.eia.gov/todayinenergy/detail.php?id=38592

Pipeline transport is facilitated by pumping and compressor stations, and pipelines include remote valve stations located along the length of the pipe. These valve stations can control flow either through manually actuation or remote commands, and can be used to isolate pipeline sections if a leak is detected.

At various points along the pipeline, metering stations are placed to ensure pipe flow. These metering stations are commonly placed at transfer points and are used to track the movement of product, which can be used in settlement processes. Meter data is relayed back to operations centers through a variety of communications media, depending on the specific system operator.

2.2.4 Storage

Storage of oil and gas is another controls-heavy process. The storage of oil products can occur at various points along the supply chain, and products are stored in large above-ground or underground tank systems. Storage facilities are typically situated near processing facilities to hold either raw or post-processed products. They are also typically situated closer to end-use customers, at points where products are transferred from pipelines to distribution networks comprised of tanker trucks, barges, or rail cars.

In the natural gas industry, storage can be in the form of either compressed gas or super-cooled liquefied natural gas (LNG). Natural gas storage is typically done in underground storage facilities (such as depleted reservoirs, salt dome formations, or aquifers). These storage facilities require large compressors to pump gas into them during storage seasons, along with equipment to receive the gas as it is withdrawn during the wintertime, when demand for gas is at its highest. There are over 400 major underground natural gas storage facilities in the United States. LNG storage requires the gas to be chilled to temperatures as low as -260F, by which time its volume is reduced by a factor as large as 600. Temperature is kept constant with strong insulation and by allowing gas to boil off and escape from the tank. Escaped gas can be recycled or used for process fuel. There are approximately 100 LNG storage sites in the US, mostly for peak-shaving and local backup, with a large concentration in the Northeast.

The exact design of the ICS that support these storage facilities varies greatly depending on the specific needs of the facility, but the same types of equipment found at other points of the oil & gas supply chain (RTU, PLC, PAC, HMI, DCS) can be found at storage facilities. Similarly, storage facilities have many of the same types of ESD and SIS requirements as other oil & gas facilities.

2.2.5 Natural Gas Distribution Systems

In natural gas pipelines, gas is typically transferred from the large interstate pipelines to local distribution system prior to delivery to end-use customers. At this point, the gas pressure must be reduced to a safe level for the distribution network. Pipeline pressures on interstate transmission systems may reach over 1,000 pounds per square inch-gauge (psig), while most distribution systems operate between a few tenths of a psig to a few hundred psig. Regulating stations serve this purpose by controlling valve equipment which drops the pressure to a pre-set level. It is common at this point to inject an odorizing agent, such as Ethyl Mercaptan, which gives the otherwise-odorless natural gas its distinctive “rotten egg” smell. Injection of an odorant is required as it allows for the detection of natural gas leaks. Very commonly the regulating, odorizing, and metering processes are combined in a single facility called a “citygate” station or a “town border” station. These stations are almost never staffed with on-site personnel but are checked on with varying frequency by utility staff. The control system design of these facilities varies greatly, but they may include PLC, RTU, HMI, and other standard control equipment.

Because of its widespread use in cooking, space heating, and other residential & commercial processes, natural gas is delivered to homes and businesses by these distribution lines. Each facility contains a natural gas meter, which measures the amount of gas being delivered to the customer. A new generation of smart gas meters are becoming increasingly popular, which include capabilities to send meter data directly to the utility for billing purposes.

2.2.6 Pigging

From time to time, pipeline systems must be cleaned and inspected for cracks, leaks, and other issues. To do this, pipeline operators use “pigs”, which are devices that are placed into the pipeline via specially-designed “pig launchers”. Pigs are pushed through the pipeline using the flow of the product and can be used to clean debris and other deposits from the inside of the pipe. “Smart pigs” are used to monitor the conditions of the pipe using a set of sensors and data storage capabilities. “Pig receiver” facilities are placed downstream of the launcher facilities and are used to recover the pig device. These launching and receiving facilities are typically small and may be combined with other facilities such as valve stations, metering stations, or citygate stations. Pigging is mostly a manual process and does not rely on control systems heavily.

2.2.7 Wide-Area Controls

It is common for ONG system operators to have a service territory that spans a large geographic area. As a result, central operations centers may be constructed to control system flow and monitor system conditions. These control centers utilize supervisory control and data acquisition (SCADA) systems to collect data and issue control operations to remote facilities.

2.3 Operations Summary

The ONG system touches every corner of the nation and its operation relies on a complex network of instrumentation, control, communications, and human & business processes. Increased control capabilities have allowed for greater efficiency of system operation, but have also created a massive target for adversaries to launch cyber-attacks. In the end, ONG processes are very similar to any other heavy industrial processes—and as such they utilize many of the same communications and control technologies that are present in other critical infrastructure sectors. The same pieces of equipment that has made life easier for ONG system operators—such as PLCs, HMIs, and SCADA systems—have also greatly increased the attack surface for would-be attackers.

Section 3

Current State of Oil & Gas Cybersecurity

3.1 Risks to the Oil & Gas System

3.1.1 Nature of Risks

The pipeline sector is generally considered to be resilient and versatile. Historically, pipeline operators have been able to quickly respond to the adverse consequences of an incident and quickly restore pipeline service. This has been possible mostly because pipeline infrastructure includes redundancies such as parallel pipelines or interconnections that enable operators to reroute material through the network. However, whether such redundancies alone will be sufficient to avoid disruption in the event of large-scale state-sponsored cyberattacks against pipeline infrastructures is mostly unknown at this time. Figure 2 illustrates a small set of possible attack scenarios against pipeline infrastructure.

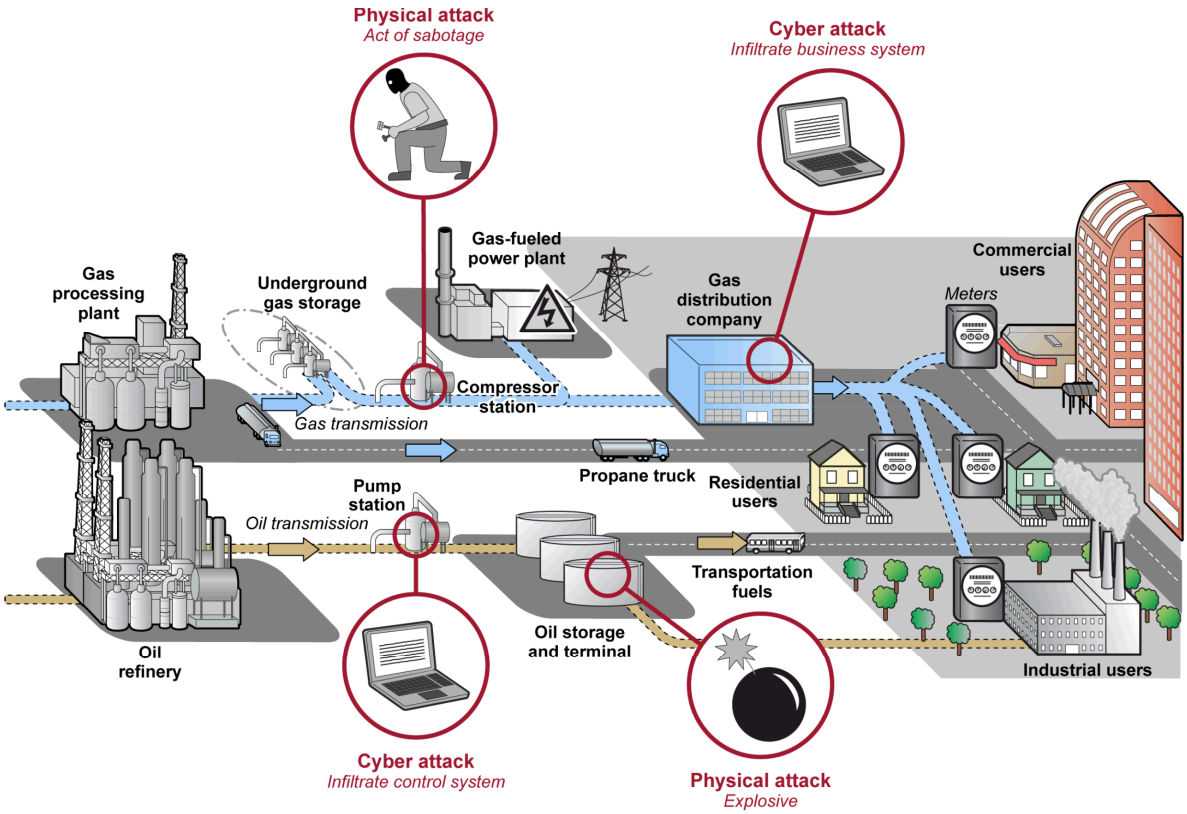


Figure 2: Examples of vulnerabilities in the US pipeline infrastructure. Source: GAO analysis of TSA information (GAO-19-48)

The ONG sector is vital for the prosperity and well-being of our nation. It is these same attributes that make ONG assets prime targets for attacks by our adversaries. Through an outreach effort to the oil & gas industry, LLNL has identified a set of common concerns regarding cyber-security that exist across the ONG industry. What makes it difficult to secure ONG assets against cyberthreats, and practically against all threats, are the following characteristics of this sector:

i. ONG assets are spread over the entire geographical landscape, including significant assets offshore.

ii. Assets are often located in remote and hard-to-access locations.

iii. Assets are interconnected. Disrupting any of the upstream, midstream or downstream business of the ONG sector can potentially disrupt the value chain of the whole industry.

iv. Most ONG production and distribution facilities, including its vast network of interconnected and automated sensors and control equipment, have been designed decades ago and lack modern security features, which make them vulnerable and obvious targets for cyberattacks.

v. ONG companies often deployed and install modern computer technology with a mindset to increase productivity, mitigation of cyberthreats and increasing cybersecurity came only as after-thoughts.

vi. Legacy mindset and reluctance to adopt a proactive cybersecurity strategy. Many U.S. ONG lack the capability to find or track malware that already exists within their systems, including within their operational technology (OT) systems. Adversaries can maintain presence in these systems for months or years to collect data and identify weaknesses.

3.1.2 Cyber Concerns in ONG

In a report[6] prepared for the Lysne Committee, DNV-GL listed the top 10 cybersecurity issues affecting the ONG industry. These include:

- Lack of cybersecurity awareness and training;
- Remote access during operations and maintenance;
- Use of standard information technology (IT) products with known vulnerabilities;
- A limited cybersecurity culture among vendors, suppliers and contractors;
- Insufficient segmentation of data networks;
- Use of mobile devices and storage units;
- Data networks between on- and offshore facilities;
- Poor physical security of data storage facilities;
- Software vulnerabilities; and
- Legacy control systems.

3.1.2.1 Digitization and Automation

Industrial automation, control and safety systems used in ONG sector are more and more becoming digitized and dependent on digital technology. These systems are now to a large extent based on commercially available components, such as a PC with a Microsoft Windows operating system, implying

[6] https://www.dnvgl.com/news/dnv-gl-reveals-top-ten-cyber-security-vulnerabilities-for-the-oil-and-gas-industry-48532

that the control systems of ONG operations are also exposed to the known vulnerabilities of such commercial standard products.

The networks used between process equipment and control systems were previously isolated and proprietary but are now increasingly based on internet technology, including advanced technologies such as the Internet of Things (IoT). Even in recent past, industrial automation and control systems used to be physically separate from traditional information systems and open networks. The need to transfer production data to information systems, which also includes the needs for remote maintenance, implies that such separation is no longer practically possible. There is an increasing use of remote operation from an onshore location or neighboring platform, and this often requires use of shared computer networks, resulting in production equipment being exposed to network-related vulnerabilities.

Malicious codes are usually spread due to human error. Such human errors may include opening an attachment in an email, inserting memory sticks that are previously infected, charging mobile phones, connecting mobile devices to critical and/or secure networks, etc., or users being tricked into revealing passwords, etc. At times, having operations rooms located in remote locations means that less attention may be paid and this increases the likelihood of both unintentional and intentional unwanted incidents. Human error is regarded as the greatest digital vulnerability in the sector.

3.1.2.2 Dependencies

In order to reduce the CO_2 emitted due to power production on ONG installations, newly-built field developments are often based on power supply from existing power plants. Most of these newer remote ONG installations are forced to cease operations if there is a disruption of power that exceeds the capabilities of any backup power sources that exist onsite. There has for a long time been an increasing focus on digital vulnerabilities in electricity distribution systems. Such distribution systems are complex grid structures that are highly dependent on management and control systems.

In regard to ONG production, and off-shore production in particular, large distances and deep waters make it costly to establish a computer network for ONG installations. Fiber-optic cables on the seabed are often used, and such cables are vulnerable to damage from building and fishing activities and erosion. It is challenging to establish redundant and completely independent network solutions. A lack of communication can mean the immediate shutdown of production on platforms that are operated from a shore-based location or neighboring platforms. This is also critical for pipelines where, among other things, it must be possible to regulate and monitor the pressure and volume throughout the system.

3.1.2.3 Fragmentation

The responsibility for preventive ICS security in ONG sector is fragmented. Traditionally, there has not been a contact point for the sector that the authorities can, for example, use to warn about cyberattacks. There are also few formal forums where the sector can exchange experiences, though these situations have been changing rapidly in recent times.

Strict cybersecurity regulations govern power, chemical and nuclear facilities, but no federal laws impose such standards in ONG industry. When ONG companies have been compromised, they aren't required to report the cyber incident. Even when they turn to federal authorities for help, the specifics are typically kept secret because companies disclose information in exchange for anonymity and discretion. The Department of Homeland Security (DHS) publishes aggregated data on cyber-attacks within the ONG sector, but with no mandatory reporting requirements for asset owners, the data may be representative of only a small share of the cyberattacks against the energy industry. Moreover, in the absence of a formal reporting process,

lessons learned from cyberattacks in one company and security procedures implemented in response to such attacks are not always passed on to other companies in the sector, creating a serious knowledge gap.

3.1.2.4 Security vs. Cost

The domestic fracking boom has made the US a major player in global ONG affairs—both as a supplier and as a customer. However, the global nature of the ONG industry at times presents significant uncertainty in oil & gas prices. As a result, ONG companies are frequently in a rush to cut operational costs to maximize profitability. These cost saving measures often pose significant challenge in pursuing and implementing up-to-date security measures, even if the technology is readily available. The increased focus on cost/benefit assessments and new ways of working are important elements going forward. For example, continuous digitization will lead to introduction of more equipment with digital vulnerabilities. At the same time, volume of data to be transported is also growing and more standard IT equipment are likely to be integrated with the specialized control systems in coming years. It is also likely that the risk of key critical functions, essential infrastructure, information that must be protected for security reasons and people being affected by espionage, sabotage, terrorist acts and other serious acts will increase in coming years. It will remain a challenge to address these security challenges in an increasingly tight cost saving regime.

3.1.3 Cyber Threats

In a report release in August 2019[7], Dragos highlighted five tracked adversaries that have been identified as targeting the ONG sector. These actors include

- XENOTIME first detected in The Kingdom of Saudi Arabia in 2017, it expanded to include ONG companies in the US and Europe in 2018. According to Dragos, they compromised several ICS vendors and manufacturers and represented a supply chain threat.
- MANELLIUM according to Dragos, has been targeting petrochemical companies since 2013, but they appear to still lack an ICS-specific capability.
- CHRYSENE was involved with the 2012 Shamoon cyberattack at Saudi Aramco and remains active and evolving in more areas.
- HEXANE was first identified by Dragos in 2019 and not much is known about its capabilities at present.
- DYMALLOY is a highly aggressive and capable activity group that has the ability to achieve long-term and persistent access to IT and OT for intelligence collection and possible future disruption events.

The report highlighted the threat landscape for upstream, midstream, downstream processes. In particular, Dragos assesses that the upstream segment faces relatively few risks compared to the other segments largely thanks to the complexity of processes and technology associated with ONG exploration and production. The greatest concern for the upstream segment is through telecommunications, cellular networks, and satellite connections, because these would be an adversary's most effective likely avenue of gaining access to upstream operations, including wellheads and drilling operations. Economic espionage is of greater concern in this segment than widespread fuel supply interruptions.

The report highlights midstream and downstream operations (particularly pipeline transportation, pumping, and refining) as being particularly high-value targets for adversaries. XENOTIME is highlighted as the adversary most likely to develop capabilities to target the midstream and downstream

[7] Dragos Global Oil and Gas Cyber Threat Perspective report, August 2019

segments. However, other adversaries have conducted cyber operations targeting transport and business operations at ONG entities, for example, the attacks against electronic data interchanges (EDI) at multiple US energy companies in 2018

The report lists five different attack scenarios for global ONG industry. These are:

1. Destructive event causing loss of life
2. Third-party and original equipment manufacturer (OEM) compromises
3. IT malware bridges OT gap, disrupting Operations
4. Electric-targeting operational disruption enablement-
5. Adversary access through cellular or satellite connections

3.2 Regulation in the Oil & Gas Industry

The ONG industry has been in existence for over 150 years, and during its long history of operations, companies in this industry sector have encountered and successfully mitigated many enterprise risks, i.e., risks that could have caused company-wide, and often industry-wide, impacts (changes in market conditions, geopolitical challenges, safety hazards, to name a few). Because of the ever-increasing connectedness of ONG operations over cyberspace and consistent increase in cyberattacks in recent years, ONG companies are beginning to view cyberthreats as a part of their enterprise risks and have started to adopt cybersecurity measures to mitigate such risks. Unsurprisingly, the current state of regulation and standards development for the oil & gas industry is a complex structure, incorporating multiple government agencies as well as private industry trade groups that have issues sets of cyber guidelines. The Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) is responsible for the development and enforcement of safety, reliability, and environmental standards for the oil and gas industry.

With sophisticated and advanced cyberattack technology that has come into play in recent years, it is possible to target the operational technologies (OT) such as ICS in an ONG system. It is also possible for attackers to target the information technology (IT) setup in an ONG company. Taken together, these cyberattacks have the potential of causing adverse impacts on health and safety of personnel, asset destruction and disruption in business continuity, and/or loss of sensitive information and trade secrets. Recognizing the potential for damage from these potential cyberattacks, ONG companies are at present developing comprehensive risk-based "defense-in-depth" approaches to cybersecurity similar to industry's approach to managing other enterprise risks (Oil and Natural Gas Sector Coordinating Council and Natural Gas Council, ONG SCC and NGC, 2018). While the details can be found in ONG SCC and NGC (2018), in the following table we summarize the regulations and standards that the ONG companies are operating under to address cybersecurity challenges.

Document	Description
TSA Pipeline Cybersecurity Guidelines	Document's scope includes all onshore natural gas, LNG, and hazardous liquid pipeline transmission
INGAA Control Systems Cybersecurity Guidelines	Intended to provide guidance to ONG control systems operators on security plans to address TSA's Corporate Security Program guideline
API Pipeline SCADA Security Standards	Intended as supplement to TSA guidelines with road industry consensus and stakeholder engagement

NAESB cybersecurity standards	Largely pertain to protection of market information and secure execution of transactions and electronic inter-organization communications
API Standard 1164	Content unique to pipelines not covered by NIST CSF and IEC 62443
NIST CSF For Improving Critical Infrastructure Cybersecurity	Pre-eminent framework adopted by companies in all industry sectors; ONG companies increasingly orient enterprise-wide programs around NIST CSF.
Department of Energy Cybersecurity Capability Maturity Model	Voluntary process using industry-accepted best practices to measure the maturity of an organization's cybersecurity capabilities and strengthen operations.
International Electromechanical Commission's IEC 62443	Pre-eminent family of standards for ICS security; Widely adopted by production segment of ONG industry; applicable to any type of ONG ICS.
International Organization for Standardization ISO 27000	Leading standard in the family providing requirements for an information security management system (ISMS).

In addition, a number of federal policies have been released in recent years that direct nation-level prioritization of cybersecurity for critical infrastructure systems as a whole. The table below summarizes these policies.

Policy	Description
Cybersecurity Act of 2015	Establishes the legal framework for cyber information sharing. Establishes DHS as a hub for information sharing, providing a conduit for cyber threat indicators to flow back and forth from the private sector to the U.S. Government, including intelligence agencies. Incentivizes the work of ONG-ISAC and DNG-ISAC
Executive Order 13636	Calls for development of a technology-neutral voluntary cybersecurity framework, incentives for the adoption of cybersecurity practices, improved cyber threat information sharing, and explores the use of existing regulation to promote cyber security
Presidential Policy Directive-21	Calls for development of situational awareness capabilities for cyber risk, assessment of cascading consequences, maturation of public-private partnerships, and development of comprehensive R&D plan.
Executive Order 13800	Enhance cybersecurity of federal government networks and critical infrastructure, including to use the NIST Cybersecurity Framework to manage federal agency's cybersecurity risk. Enhance cybersecurity of the nation through deterrence, protection and cooperation; cybersecurity workforce development; and assessment of national-security-related cyber capabilities.

3.3 Cybersecurity Research in Industry

In order to reduce risk, ONG companies have been and are still adopting and implementing different measures, such as implementation of barriers, education of employees, government-industry collaboration,

and peer-to-peer information sharing. In the following, we briefly present some of these cybersecurity measures currently being pursued by ONG companies and their limitations.

3.3.1 Risk Reduction Measures

3.3.1.1 Defense in Depth

Through our outreach to ONG industry contacts, we have identified that one of the most common tools for defending against cyber threats in the ONG industry is multilayered defense. This avenue is being pursued both to prevent unwanted incidents in the first place, as well as to reduce the consequences of an intrusion if it should happen. Internal and external barriers are put in place, but the quality of these barriers varies significantly. Further, there is a lack of equipment and methods for detecting ongoing adversary presence in a network.

Included in any multilayered defense approach is robust employee training to avoid falling victim to social engineering plots. However, despite significant time and energy placed into employee training, recent surveys[8] across all industries have found that over three quarters of survey respondents expect that a careless member of staff would be the most likely source of an attack.

3.3.1.2 Peer-to-Peer Information Sharing

ONG companies participate in an array of intra-industry and industry-government collaborations, including Information Sharing and Analysis Centers (ISACs) focused on the oil & gas industry (specifically the Oil and Natural Gas ISAC [ONG-ISAC] and Downstream Natural Gas ISAC [DNG-ISAC]). This also includes peer-to-peer learning facilitated by trade organizations in an attempt to bolster the limited threat analysis assets available to most individual companies.

The Oil and Natural Gas Sector Coordinating Council and Natural Gas Council (ONG SCC and NGC) provides a broad forum for coordination oil and natural gas security strategies, and trade associations representing the ONG companies are coming under the banner of this forum to formalize the coordination strategies for cybersecurity. The ONG SCC and NGC represents almost all of the major trade associations for the ONG industry sector, including the American Petroleum Institute (API), American Gas Association (AGA), Interstate Natural Gas Association of America (INGAA), Association of Oil Pipelines (AOPL), American Fuel and Petrochemical Manufacturers (AFPM), International Liquid Terminal Association (ILTA), and International Association of Drilling Contractors (IADC).

Finally, conferences and workshops provide a convenient way for stakeholders to share ideas and make worthwhile connections. API hosts an annual Cybersecurity Conference & Expo in the US, as well as the API-IOGP Europe Cybersecurity Conference. The CyberStrike Workshop developed by DOE's Office of Electricity Delivery and Energy Reliability was created in collaboration with the Electricity ISAC and Idaho National Lab (INL). The workshop was developed to enhance the ability of energy sector owners and operators in the US to prepare for a cyber incident impacting ICS. Furthermore, security professionals from AGA's Natural Gas Security Committee, INGAA's Security Committee and the Edison Electric Institute's Security Committee meet multiple times per year to improve coordination across the energy sector and discuss emerging trends.

[8] Ernst & Young Global Information Security Survey 2019

3.3.2 Defense Strategy

ONG companies, at present, are deploying defense mechanisms against potential cyberthreats to varying degrees. These include, as recommended by Dragos[9]:

1. Visibility: Asset owners and security personnel are working together to gather network and host-based logs starting from the most critical infrastructure. The objective is to identify and correlate suspicious network, host, and operational events, which greatly assists in both identifying intrusions as they occur or facilitate root-cause analysis after a disruptive event.
2. Segment: Companies are attempting to segment and isolate networks such that lateral movement by adversaries can be reduced/eliminated. Modern networking hardware are enabling asset owners and operators to virtually segment networks to reduce attack surface and limit adversary mobility.
3. Accessibility: Companies are putting in place mechanisms to identify and categorize ingress and egress routes into control system networks. This includes engineer and administrator remote access portals, but also covers items such as business intelligence and licensing server links that need to access IT resources or the wider internet. To minimize exposed attack surface, companies are restricting these types of connections.
4. Public data: Assess asset owner hosted, publicly posted information and data that, when aggregated, would generate sensitive information that could be utilized by an adversary. Companies are working with vendors, contractors, and other parties to minimize or prevent identification of specific sites, capabilities, or equipment in marketing or related material.
5. Configuration: Identify and store "known good" configuration information for ICS devices in non-network accessible locations to provide baselines for comparison as well as restore points in the event of disruption. Update these items frequently to ensure such storage mirrors production environments.
6. Defense-in-depth: Design and implement defense-in-depth surrounding ICS networks where security controls and enhanced visibility are applied to hosts capable of handling such tasks. Examples include requiring remote access to flow through a jump-host featuring enhanced Windows and network logging to ensure adequate monitoring of remote access to the control system network.
7. Consequence-driven: Identify and prioritize critical assets and connections, and process consequences of cyberattacks. Perform threat assessments to scope the most impactful risk of disruptive or destructive attacks and use such data to shape threat hunting and defensive postures.
8. Third-parties: Ensure that third-party connections and ICS interactions are monitored and logged, from a "Trust, but Verify" mindset. Where possible, isolate or create distinct enclaves for such access to ensure that third-party access does not result in complete, unfettered, or unmonitored access to the entire ICS network.
9. Network infrastructure: Implement router, switch, and firewall configuration review to ensure adversaries do not tamper with configurations and locate security gaps.
10. Threat intelligence: Use and operationalize ICS-specific threat intelligence. Threat intelligence can enable identification of known threat behaviors.
11. Response plan: Develop, review, and practice cyberattack response plans and integrate cyber investigations into root-cause analysis for all events.

3.4 Cybersecurity Activities in Government & Labs

Activities to advance the cybersecurity of the nation's industrial control systems take place within many portions of the US government. DOE's Cybersecurity, Energy Security, and Emergency Response (CESER) office has invested more than $240 million in cybersecurity research, development and

[9] Dragos Global Oil and Gas Cyber Threat Perspective report, August 2019

demonstration projects that are led by industry, universities and National Labs[10]. This investment has helped support the development of a wide array of tools that are in varying stages of deployment to bolster the resilience of critical energy infrastructure.

Within DHS, numerous efforts are underway to support cybersecurity within the ONG sector. Projects such as Cybersecurity for the Oil and Gas Sector (COGS) and the Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) program within the DHS Science and Technology (S&T) Directorate aim to promote cybersecurity across the industry. As part of DHS' Cybersecurity and Infrastructure Security Agency (CISA), the Pipeline Cybersecurity Initiative includes detailed assessments of pipeline assets which enable asset owners to identify and mitigate potential vulnerabilities.

3.5 Research Gaps and Biggest Concerns

Between 2011 and 2015, DHS responded to more than 350 incidents at US energy companies. An equally troubling statistic is that DHS has identified nearly 900 security vulnerabilities within those energy companies, a figure that was higher than any other industry[11]. Although U.S. ONG companies have so far avoided devastating data breaches, cybercriminals are growing bolder. An idea about the magnitude of the challenge can be obtained from the fact that, during an average month, for example, a company like ExxonMobil now blocks more than "64 million emails, 139 million internet access attempts and 133,000 other potentially malicious actions."[12]

The Houston Chronicle recently investigated the state of cybersecurity within oil and gas installations along the Gulf Coast[13], and it found that many facilities have computing systems that still run Windows XP—an operating system that has not been formally supported since 2014. Others were found using Windows predecessors that date back to the 1990s, and "in rare cases, a few still use MS-DOS, the precursor to Windows," the newspaper reported.

Moreover, when the Ponemon Institute surveyed ONG cybersecurity risk managers[14] for their 2017 report, the vast majority said that the cybersecurity practices had failed to keep pace with the increasingly-digital ONG processes and operations. In the survey, 68 percent of respondents said their companies had suffered at least one security compromise involving the loss of confidential information or the disruption of their operations, in the past year. Roughly the same number of respondents expressed concern that digitization had made them more vulnerable to security compromises. Only 35 percent of the survey's respondents scored their organization's cyber readiness as "high".

In 2019, Ernst & Young (EY) performed an investigation ("Global Information Security Survey") of the critical cybersecurity issues facing organizations (Williams et al., 2019). The survey involved 1,200 participants around the glove from 20 industries, including 40 participants from ONG. The survey results, which are summarized below, give an overview of the status of the ONG with respect to their cybersecurity preparedness.

1. 60% have had a recent cybersecurity incident

[10] https://www.energy.gov/ceser/cybersecurity-energy-delivery-systems-ceds-fact-sheets

[11] http://www.houstonchronicle.com/news/houston-texas/houston/article/As-cyberattacks-become-more-sophisticated-energy-10973429.php

[12] http://corporate.exxonmobil.com/en/company/about-us/safety-and-health/workplace-safety

[13] http://www.houstonchronicle.com/news/houston-texas/houston/article/As-cyberattacks-become-more-sophisticated-energy-10973429.php

[14] https://siemensusa.newshq.businesswire.com/sites/siemensusa.newshq.businesswire.com/files/doc_library/file/Cyber_readiness_in_Oil__Gas_Final_4.pdf

2. However, only 15% have a robust incident response program
3. 50% say the lack of skilled resources is challenging information security's contribution and value to the organization.
4. 95% say their cybersecurity function does not fully meet their organization's needs.
5. 17% feel it is very likely that they would detect a sophisticated cyberattack.
6. 48% say it will be challenging to ensure that the implemented security controls are meeting the requirements of today.
7. 78% consider a careless member of staff as the most likely source of an attack.
8. 43% of significant cyber breaches were from a lack of end user awareness, exploited via phishing.
9. 87% have not fully considered the information security implications of their current strategy and plans.
10. 97% of the organizations' information security reports do not evaluate financial impact of every significant breach.
11. 63% would not increase their cybersecurity spending after experiencing a breach that did not appear to do any harm.

While ONG companies generally have become better at securing their information and data systems, the progress is not universal. While major ONG companies have started to install firewalls, anti-virus and anti-malware programs and require stricter security measures from equipment manufacturers, the same cannot be said about smaller entities. Furthermore, while forward-looking ONG companies in recent years have treated potential cyberattacks on critical assets as a major financial risk, others haven't taken the threat as seriously. Overall, the cyber maturity of ONG sector can be termed as low.

Cyber-attacks targeting ONG companies are clearly on the rise, however that trend does not appear to be reflected in the risk strategies of many major ONG companies. Other risks, such as aging workforce and weather disruptions, consistently rank as high or higher in terms of prioritization for ONG organizations. It is clear that significant steps must be taken to safeguard the ONG industry from cyber-threats to protect not only the reliable operation of the energy delivery systems, but also to protect the health and safety of system operators whose lives may be put at risk in the event of a widespread cyber-attack on the ONG system.

3.6 ONG Cybersecurity Summary

The ONG industry has taken a long and winding road to get to where it is today—and the same is true of its regulatory structure. As such, the state of cyber-preparedness across the industry varies from organization to organization. Among the most common challenges that ONG companies face are remote locations, long-lived field assets, and lacking capabilities to find and track malware on their systems. ONG companies tend to be concerned with lack of cyber-awareness from employees, risk stemming from remote access for operations & maintenance, and software vulnerabilities within third-party equipment. Various industry and government organizations are performing research and development activities to address some of these challenges, but in many cases industry stakeholders are not aware of solutions that already exist. It is clear that a need exists for a coherent, comprehensive, multi-layered strategy for assuring the security and resilience of the nation's pipeline infrastructure against cyber threats.

Section 4

Previous Work - Strategy for a Resilient Electric Grid

4.1 Foundational Work on Electric Grid Cyber-Resilience

LLNL's approach to developing a resilient pipeline cybersecurity strategy builds upon work done to develop a resilient electric grid. This work leverages cybersecurity frameworks that were developed by the National Institute of Standards and Technology (NIST) and the Defense Science Board (DSB).

The NIST cybersecurity framework was created with a focus on cybersecurity for critical infrastructure systems—not only the energy sector but other sectors such as communications, defense, and finance. The 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[15] directed all federal agencies to utilize the NIST framework. The framework's core is a set of five concurrent functions: Identify, Protect, Detect, Respond, and Recover. Together, these five functions serve as a set of activities to help manage cybersecurity risk. Definitions for each function is given below:

- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

In addition to these five functions, LLNL has included a sixth function ("Endure") to capture methods for minimizing adverse impacts during a large-scale event.

The DSB has developed a tiered system of cyber threat actors, ranging from very low-capability "script kiddies" to top-tier full capability nation states. Definitions for each cyber actor tier is below[16]:

- Tier I: Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
- Tier II: Practitioners with a greater depth of experience, with the ability to develop their own tools (from publicly known vulnerabilities).
- Tier III: Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing

[15] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

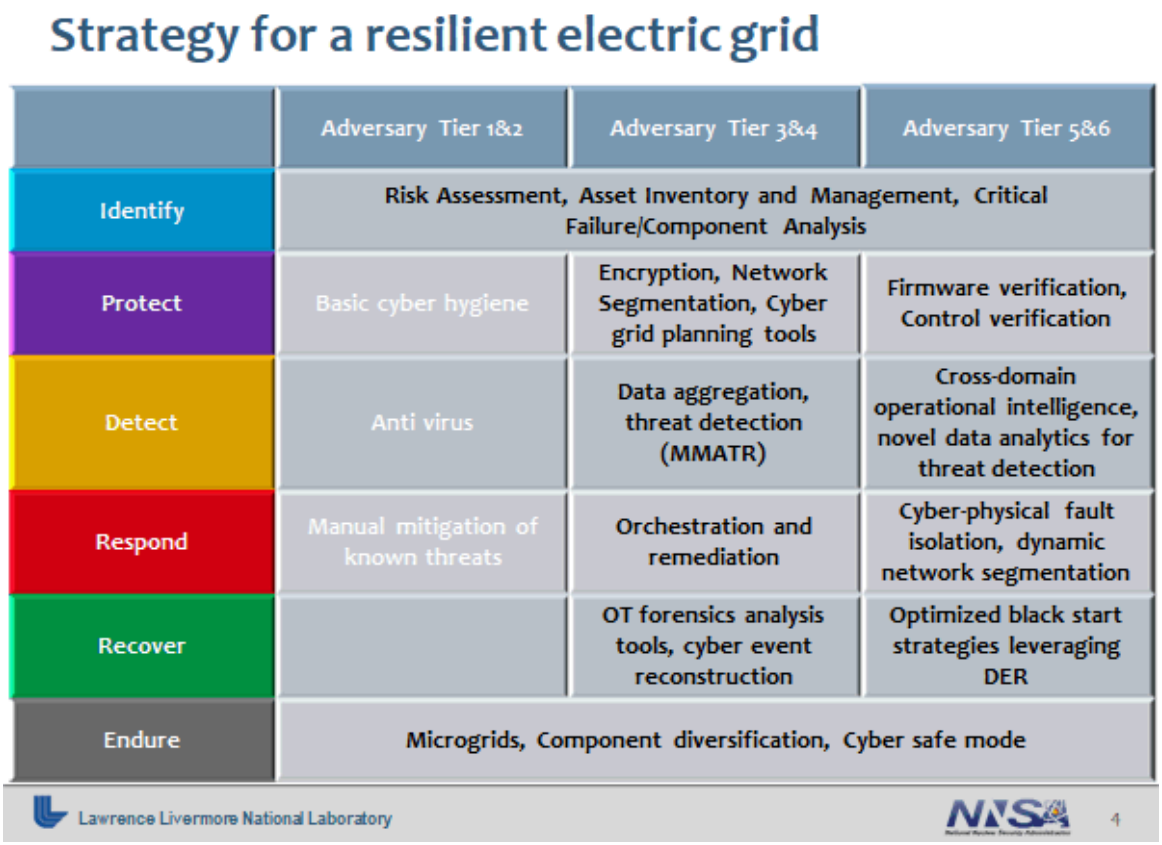
[16] Defense Science Board Task Force Report on Resilient Military Systems and the Advanced Cyber Threat, January 2013

personal and corporate data with the expressed purpose of selling the information to other criminal elements.

- Tier IV: Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
- Tier V: State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
- Tier VI: States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

4.2 Strategy for a Resilient Electric Grid Matrix

In order to develop a robust, risk-informed strategy for an electric grid that is resilient to cyber-attacks, LLNL has combined these two frameworks into a matrix that can be used to identify priority activities for industry, trade groups, national labs, and government agencies. A copy of this matrix is shown below:



In general, asset owners and utility organizations are well-equipped to handle threats from Tier 1 & Tier 2 actors. There is a wide array of commercial cybersecurity products to facilitate protection against these

adversaries, and grid-hardening efforts against these types of threats can generally be combined with efforts to protect against other threats such as natural disasters.

Protection of the electric grid against adversaries in Tiers 3 & 4 involves ongoing collaboration between asset owners, industry trade groups, and governmental organizations including national labs. Protection against these threats may require threat intelligence that is not available to asset owners but requires system information and data that is *only* available to asset owners.

The extent of impacts that are possible from attacks by Tier 5 & 6 actors is such that any single asset owner is unlikely to be equipped to deal with the consequences. Similarly, Tier 5 & 6 adversaries are capable of attacks with levels of sophistication that may allow them to maintain presence on target systems for years—allowing long-term reconnaissance of system operation and attack tuning. An attack by a Tier 5 or 6 actor may have interconnection-wide impacts, wherein dozens of utility organizations are affected. To fully understand the threats posed by these tiers of actors, detailed threat intelligence information is required.

4.3 Resilient Electric Grid Summary

Significant time and effort has gone into the development of a threat-informed cyber-security strategy for a resilient electric grid. Many of the threats faced by the electric grid are also faced by the ONG system, and many of the adversaries that wish to do harm to the grid may also have intentions of disrupting the ONG network. The strategy for a resilient electric grid provides a great foundation to begin the development of an ONG-specific resilience strategy.

Section 5

Strategy for a Resilient Pipeline System

5.1 Commonalities Between Oil & Gas and Electric Systems

Owing to the nature of joint gas & electric operations in many areas, the natural gas industry has a large number of similarities to the electric power industry. In addition, while operation of the oil system is not linked with operation of the electric system, these two industries maintain many similarities as well. This is evidenced by many recent mergers and acquisitions that span both the oil & gas industries—such as the 2018 merger of Spectra (one of North America's largest natural gas operators) and Enbridge (one of North America's largest oil pipeline operators).

Like the electric grid, oil & gas are generally produced in areas that are very remote from demand centers. Natural gas, in particular, must be delivered to downstream customers representing the same sectors as electricity—residential, commercial, industrial, and transportation. On top of all this, natural gas operators require electricity to function, and many electric operators utilize gas-fired power plants to produce electricity. In both the electric grid and natural gas pipeline system, these delivery systems include a complex network of high-voltage or high-pressure transmission systems that move electricity and gas across long distances, which includes transmission across state lines and along some very remote rights of way. The transmission networks then deliver the product to distribution networks, which operate at lower voltages or pressures, and supply electricity and gas to the end-users.

Pipeline transportation of oil and petroleum products differs slightly from the transportation of natural gas, in that oil pipelines tend to be more point-to-point facilities. Petroleum products may be shipped either in their crude or refined state, and pipelines are mainly used for long-distance transmission. Petroleum products aren't typically delivered to residential and commercial end-use customers, and are instead made available via other means. Despite this difference in transmission and distribution network setup, the operation of these facilities shares major commonalities with the operation of natural gas pipelines.

The maps below illustrate the expansive nature of the electric, natural gas, and oil transmission systems.

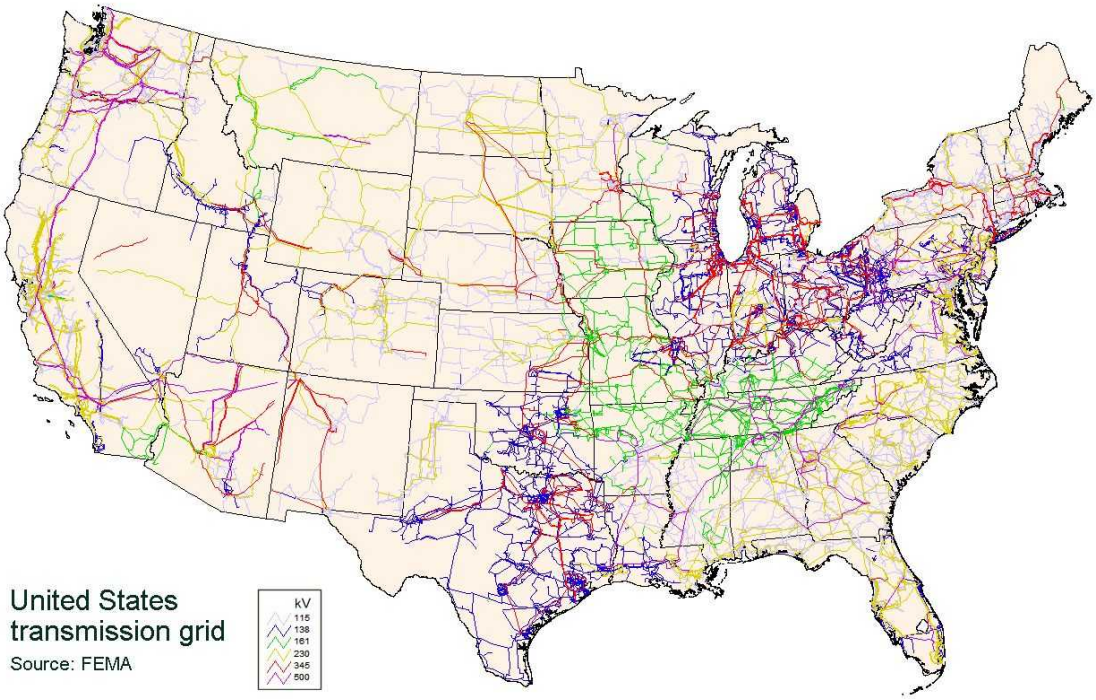


Figure 3: Electric transmission lines in the United States

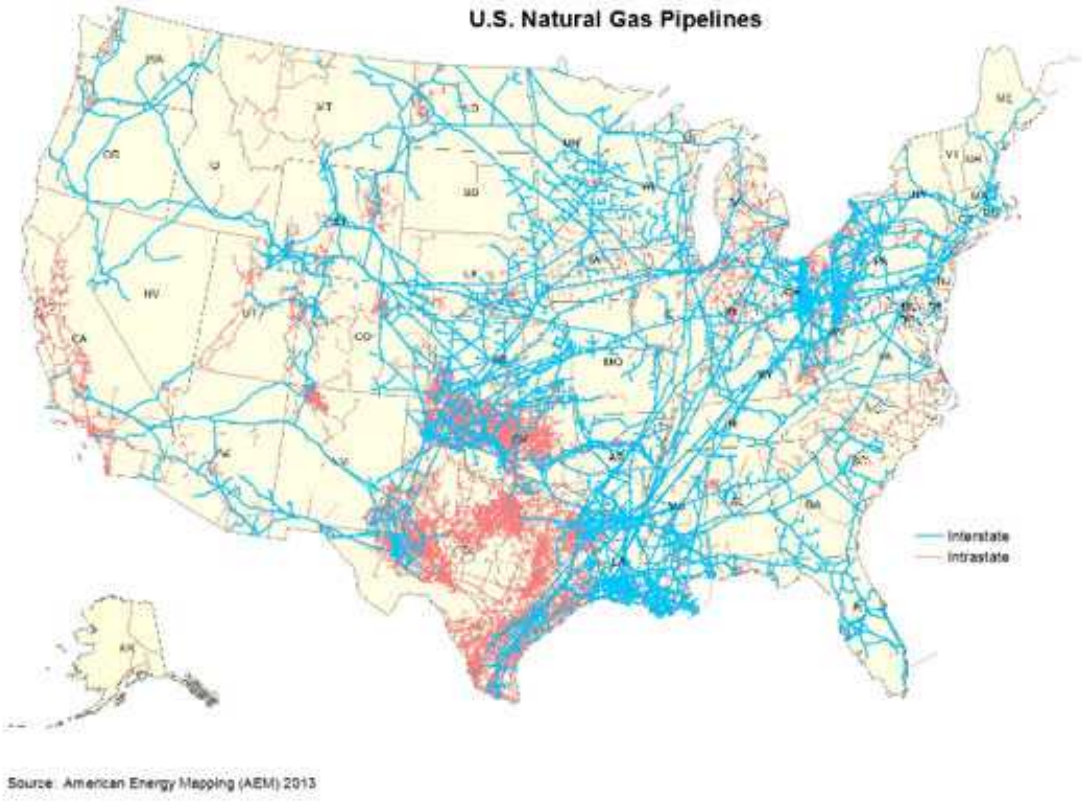


Figure 4: Natural gas pipeline network in the United States

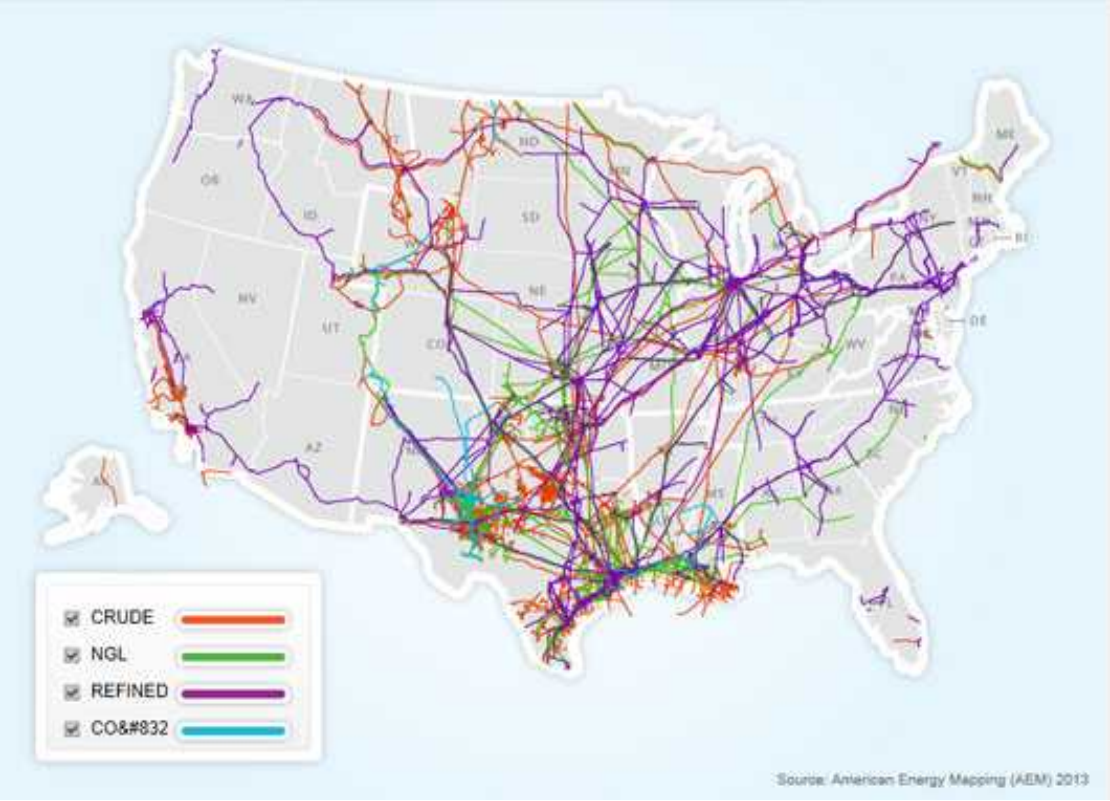


Figure 5: Petroleum pipeline network in the United States

Because of the high degree of hazard related to unsafe operation, each of these energy infrastructure systems requires active control over system performance and close oversight of system operations. This communication and control is performed by SCADA networks which may span an operator's entire footprint. This SCADA network allows for control and monitoring to be performed at a master control center, greatly simplifying day-to-day system operations.

In regard to communications systems and network infrastructure, the oil & gas industry overlaps greatly with the electric power industry. Field assets in the oil & gas industry tend to have long useful lives, and utility decision-makers tend to be hesitant in replacing equipment before the end of its expected life. As a result, continual build-out and sporadic upgrading of communications networks by each organization has created a diverse array of communications systems across the industry. Communications between control centers, from control centers out to field stations, between field stations, and within field stations may occur over fiber, ethernet, satellite, cellular, or any other of a host of different communications networks. On one hand, this heterogeneity provides some resilience to single points of failure. A failure within one communications network may not have widespread consequences in an oil & gas industry that utilizes so many different methods. On the other hand, the complexity of upkeep and coordination for all these different networks presents more latent risks. Many pipeline operators may not know of inherent vulnerabilities in the communications systems that they've been using for decades.

The extent of this commonality between the electric power system and the oil & gas pipeline system provides an opportunity to leverage some existing capabilities that were originally developed to address the cyber-security risks of the electric grid. Section 5.3 lists the electric grid capabilities that may be relevant to similar problems faced by the pipeline network.

5.2 Unique Aspects to Pipelines

Despite the large set of similarities between the electric grid and oil & gas pipeline systems, there are some key differences that may make it challenging to fully leverage existing capabilities for electric grid cyber-resilience into solutions for the pipeline system. A great deal of time and energy has been spent on certain aspects of the electric grid that have no real equivalent in pipeline systems. These topics, such as blackstart, microgrids, and dynamic stability will not be discussed in this document.

5.2.1 Nature of System Failure

Compared to impacts of a failure on the electric grid, failure of processes within the ONG sector can have even broader impacts to downstream processes, the environment, and health & safety in general. This can best be illustrated by a series of recent ONG system failures that were caused by accident or by small mistakes in operation. However, these small mistakes can have dire consequences. The 2010 blowout on the Deepwater Horizon oil rig in the Gulf of Mexico killed 11 crewmen and caused the largest oil spill ever seen in US waters. The San Bruno, California gas pipeline explosion in September 2010 killed 8 and injured 58 more. The explosion was caused by a combination of faulty welds on the pipe itself coupled with PG&E operating that segment of pipe at pressure levels that exceeded PG&E's maximum rated operating pressure. In 2018, a natural gas pipeline exploded in Merrimack Valley, Massachusetts, killing one and injuring at least two dozen more. The explosion occurred as workers were replacing old low-pressure cast iron pipes with new plastic pipe, but they failed to transfer downstream pressure sensors to the new pipes. As a result, regulators upstream received zero-pressure measurements and flooded downstream system with high pressure—causing the accident. With these recent examples of loss of life stemming from simple accidents and organizational failures, it is clear that the risk to health & safety and environmental damage from a directed cyber-attack is a massive unaddressed problem.

5.2.2 System Operations and Impact Propagation

Among the greatest differences between these energy systems is the rate at which impacts propagate. On the electric grid, the failure of a single element—such as a transmission line or transformer—can have near-immediate impacts on surrounding equipment. Electricity travels at the speed of light, and as such there is a high risk of cascading impacts where an equipment failure causes an unbounded string of additional equipment failures. For this reason, electric grid operators are bound by a set of mandatory standards from the North American Electric Reliability Corporation (NERC) to operate the grid in such a way that it can withstand the outage of any single element, regardless of how critical it is to the rest of the system. In cases where there is no feasible way to operate the system with this security guaranteed, grid operators utilize a set of Special Protection Systems (SPS) or Remedial Action Schemes (RAS). These are intended to operate nearly instantly after a pre-defined contingency occurs to protect the rest of the grid.

On the pipeline system, impacts move significantly slower. As a result, pipeline operators generally have sufficient time to diagnose the problem and manually alter the system in such a way as to prevent the impacts from spreading. While this provides some resilience to wide-spread cascading outages, the fact that pipeline operators have a stronger role in day-to-day response to adverse events presents its own risks. In addition, the grid tends to be networked to a much greater degree than oil & gas pipeline systems. In other words, the failure of one or even a few elements within the electric grid may not cause any loss of service to downstream customers since there may be a parallel path to continue the transmission of electricity. With pipeline systems, unless there are looped or dedicated parallel stretches of pipe, the loss of a single corridor of pipe is sufficient to greatly decrease the amount of product that can be delivered to downstream customers. Pipe systems tend to be more point-to-point in comparison to the electric grid.

5.2.3 Processing and Refining

Among the greatest differences, and one that presents major risk for wide-spread disruption, is that oil and gas products must be refined or treated prior to use. Petroleum products can either be refined close to their source and then shipped as refined products, or shipped in its crude state and refined closer to the end use. Natural gas is generally processed near its origin and shipped via pipeline to downstream customers. Byproducts of natural gas processing, such as NGLs may be transported via pipe or other means (road, rail, barge). These processing facilities have no real analog in the electric grid, and are critical pieces of the oil & gas system. The nature of these facilities (massive industrial processes with high levels of communication and controls) makes them a prime target for adversaries planning cyber-attacks.

5.2.4 Product Storage

A key benefit of the oil and gas system is the relative ease of storage of products. Storage facilities provide key supplements when supplies run short, and serve as a sink for surpluses when supply outpaces demand. Storage facilities provide operators of oil and gas networks with a strong tool to wield in the case of operational emergencies. The presence of these facilities does present a risk, however. Industrial control systems at these facilities can serve as targets for directed cyber-attacks, and the loss of even a single storage facility can shine light on potential over-reliance on a single asset, as was the case in the Aliso Canyon natural gas storage facility leak in Southern California during 2015 & 2016.

5.2.5 Design of Remote Facilities

Within the electric power system, substations play a key role in sectionalizing, metering, and routing power. While some substations may contain additional equipment such as reactive support devices (shunt capacitor or inductor banks, static VAR compensators, etc.), there tends to be a significant amount of overlap in the types of equipment found at each substation. Within the oil and gas pipeline systems, that is not necessarily the case. Special-purpose pumping stations (oil) and compressor stations (gas) are placed at points along long-haul transmission pipelines to ensure that there is enough pressure in the lines to facilitate product flow. These facilities are distinct from other pipeline facilities such as metering stations, which tend to be significantly smaller and require fewer control systems and protection equipment. Additional purpose-built facilities on the gas system include citygate stations in which metering, regulation, and odorant injection may occur. The heterogeneous nature of facilities in the oil and gas networks provides some inherent level of resiliency, but also presents challenges in maintenance and upkeep.

5.2.6 Infrastructure Planning and Design

Finally, among the greatest non-technical differences between the electric power system and the oil & gas pipeline system is the way in which infrastructure is planned and built. Within the electric sector, utilities develop long-term transmission plans, and collaborate with neighboring entities to ensure that there are no redundant projects, and that there are no issues at the seams between territories that may be missed. Within the pipeline system, infrastructure build-out only happens when there is a proven demand for flow from point to point. Pipelines are only approved by regulators if enough customers agree to sign up for long-term firm flow service, and infrastructure planning is done *competitively* rather than *collaboratively*.

Because of these differences, certain aspects of the electric grid cyber-resilience strategy may require substantial modifications for relevance in the pipeline sector—and other aspects may not be relevant in any way. Section 5.3 discusses some of these factors and the ways in which they may be modified to be relevant to the pipeline system.

5.3 Resilient Pipeline Strategy Comparison

The table below lists each of the activities in the Strategy for a Resilient Electric Grid from Section 4.2. Associated with each of these activities is a brief description of relevant activities for a resilient pipeline system. Green text suggests that the activities are similar between the electric grid and pipeline system, due to inherent similarities in system operations. Orange text suggest that there is no direct analog for a similar activity on the pipeline system. This table will continue to be revised as the project progresses.

NIST Framework Function	Adversary Tier	Resilient Electric Grid Activity	Resilient Pipeline Activity Analog	Comment on unique features of pipeline system
Identify	1 - 6	Risk assessment	Risk assessment	-
	1 - 6	Asset inventory & management	Asset inventory & management	-
	1 - 6	Critical failure/component analysis	Critical failure/component analysis	-
Protect	1 & 2	Basic cyber hygiene	Basic cyber hygiene	-
	3 & 4	Encryption	Encryption	-
	3 & 4	Network segmentation	Network segmentation	-
	3 & 4	Cyber grid planning tools	Cyber pipeline planning tools	Because of the nature of electric system planning, grid models are currently more mature in their ability to simulate cyber-like disruptions
	5 & 6	Firmware verification	Firmware verification	-
	5 & 6	Control verification	Potentially limited control verification	There is significantly less distributed computing capability on pipeline systems. Difficult to perform control verification on native devices, may need special-purpose equipment
Detect	1 & 2	Antivirus	Antivirus	-
	3 & 4	Data aggregation	Data aggregation	-
	3 & 4	Threat detection (MMATR)	Potentially limited threat detection	There is generally less computing capability at many remote pipeline stations. Difficult to perform MMATR on native devices, may need special-purpose equipment
	3 & 4	None	Cyber-physical intrusion via leak detection	Utilization of existing leak detection methods to detect malicious system operation
	5 & 6	Cross-domain operational intelligence	Cross-domain operational intelligence	-
	5 & 6	Novel data analytics for threat detection	Novel data analytics for threat detection	-
Respond	1 & 2	Manual mitigation of known threats	Manual mitigation of known threats	-

	3 & 4	Orchestration and remediation	Orchestration and remediation	-
	5 & 6	Cyber-physical fault isolation	Cyber-physical fault isolation	Concept is the same, though devices may vary
	5 & 6	Dynamic network segmentation	Limited pipeline network reconfiguration	Due to the point-to-point nature of pipeline system, it is unlikely that widespread network segmentation is feasible while still serving customers
Recover	3 & 4	OT forensic analysis tools	OT forensic analysis tools	-
	3 & 4	Cyber-event reconstruction	Cyber-event reconstruction	-
	5 & 6	Optimized blackstart strategies leveraging DER	None	Blackstart is not a concept for pipelines. Pipes can resume flow operations once pumps are restarted
Endure	1 - 6	Microgrids	None	The closest approximation to microgrids for pipeline systems is small sets of facilities with on-site oil & gas storage
	1 - 6	Component diversification	Component diversification	-
	1 - 6	Cyber safe mode	Cyber safe mode	
	1 - 6	None	Onsite storage and fuel replacements	Somewhat analogous to microgrid, development of scalable onsite storage systems and local fuel-sharing networks

5.4 Resilient Pipeline System Summary

For a variety of reasons, the general consensus from stakeholders interviewed by LLNL is that the state of cyber-security within the electric grid is currently outpacing its ONG cousin. Recent years have seen tremendous development of electric grid-focused cyber-security technologies—leveraging things like collaborative autonomy and system optimization. Although they are currently focused on ensuring the resilience of the electric grid, many of these technologies can be directly applied to the ONG system with minimal modification. Leveraging existing electric grid strategies wherever possible can provide immediate low-hanging fruit for improving the cyber-security of the ONG system.

Section 6

Conclusion

6.1 Report Summary

As can be seen, there currently exists a wealth of surveying and reporting on cyber-preparedness trends within the ONG industry. These surveys provide an excellent glimpse into the high-level direction of cyber-security research and development, but they stop short at identifying specific approaches to mitigating cyber-risk. In LLNL's view, there are two key factors currently limiting the development of necessary cyber-practices within the ONG industry:

- The sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for ONG cyber-security makes it difficult to create a comprehensive, directed, and coherent strategy that is applicable to all players within the ONG industry
- The ONG industry is unaware of potentially useful technologies that have been developed for ensuring cyber-security of other infrastructure systems, such as the electric grid. Leveraging these technologies—and the science and engineering behind them—can provide some low-hanging fruit that can greatly improve cyber-security in the ONG industry without significant investments in terms of time and money.

6.2 Next Steps in Development of Resilient Pipeline Strategy

In the months following this report, LLNL will continue to perform outreach to key oil & gas industry stakeholders in a continual effort to identify the most pressing cyber-resilience issues in the industry. This outreach will be supplemented with LLNL's threat intelligence capabilities to begin painting a clearer picture of the overall threat landscape faced by this sector. The analysis will be threat-informed and while the strategy itself will not be classified we will leverage intelligence analysis and adversary capabilities to identify gaps in current cybersecurity practices for oil & gas pipeline systems.

The combination of the information gained from industry contacts and the intelligence gained on adversarial threats will be used to develop a more detailed pipeline cyber-resilience strategy. These recommended efforts will be compiled into a cyber-resilience roadmap for the oil & gas pipeline sector, in which LLNL will provide its recommendations for priority activities to immediately improve the state of cyber-resilience in the industry.