DYNAMIC DELIVERY

America's Evolving Oil and Natural Gas Transportation Infrastructure

CHAPTER FOUR – TECHNOLOGY ADVANCEMENT AND DEPLOYMENT

A Report of the National Petroleum Council

December 2019

This chapter was last updated on

January 5, 2021

Chapter Four

TECHNOLOGY ADVANCEMENT AND DEPLOYMENT

I. TECHNOLOGY ADVANCEMENT AND DEPLOYMENT OVERVIEW

A. Introduction

Technology advancements in the oil and natural gas[1] transportation sector have contributed significantly to the improvement in safety and environmental performance over the past several decades and helped to drive improvements in reliability, efficiency, and cost effectiveness. The oil and natural gas transportation sector and American energy consumers have benefited from these technology advancements as industry continues to harness technology to further improve performance in the safe and environmentally responsible delivery of energy using multiple modes of transportation.

This chapter investigates advances in technology that could further improve safety, reliability, efficiency, environmental performance, and other public interest concerns in the transportation of oil and natural gas. It identifies process improvements and technology applications that warrant additional focus.

Also discussed are cybersecurity issues—identifying risks that threaten operational technology systems and network environments impacting industrial control systems (ICSs) across the midstream and downstream oil and natural gas industries.

1 References to "oil and natural gas" generally indicate crude oil, refined petroleum products, natural gas, natural gas liquids, and liquified natural gas.

B. Scope of the Study

The study's scope covers modes of transportation that come under the jurisdiction of the Pipeline and Hazardous Materials Safety Administration (PHMSA), including natural gas and oil pipelines and storage facilities. Also included in the scope are transportation of oil and natural gas by marine vessels (under U.S. Coast Guard jurisdiction), by railroads (under Federal Railroad Administration jurisdiction), and trucks (under Federal Motor Carrier Safety Administration and Department of Transportation jurisdiction).

The following technology areas are in the scope for this study:

- Technologies that address public interest concerns surrounding infrastructure requirements to address changing supply and demand scenarios
- Identification of any regulatory impediments to deploying and adopting emerging technologies that could strengthen operational safety
- Technologies related to improving environmental integrity and reducing direct methane emissions from pipelines, storage facilities, and compressor stations
- The cost effectiveness of new technology applications that support enhancing safety, reliability, and environmental performance
- Cybersecurity risks related to the midstream and downstream oil and natural gas industries.

Excluded from this study are natural gas and oil production and gathering systems and local natural gas distribution systems for retail use. Also

excluded are emissions from mobile transportation sources. In addition, cybersecurity issues associated with information technology (IT) systems and business networks are excluded from the scope.

C. Industry Safety and Environmental Performance Trends

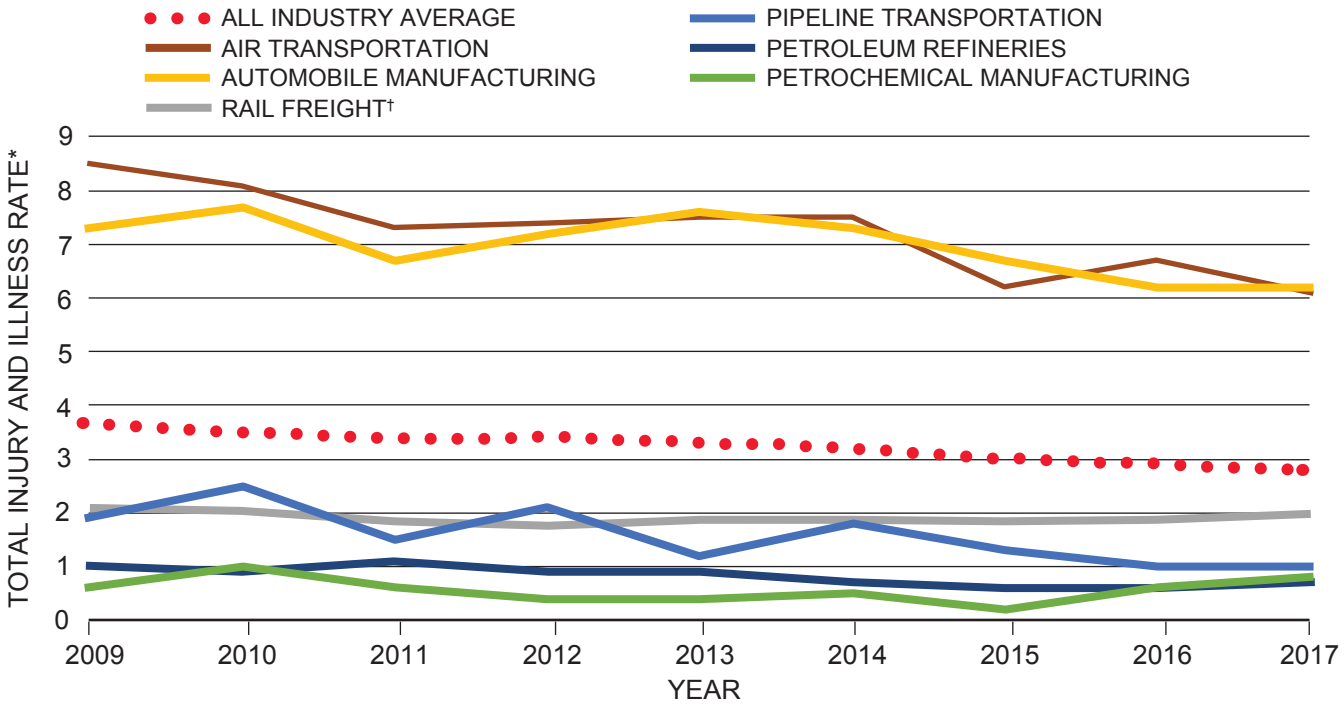
The oil and natural gas transportation industry has improved its safety and environmental performance over time across all primary modes of transportation; pipeline, rail, marine, and trucking. The following sections of this chapter describe safety and environmental performance trends for each transportation mode, including pipeline and storage, liquefied natural gas (LNG), marine, rail, and trucking. In the analysis, the leading causes of incidents are identified and the most important technology development and deployment opportunities to mitigate incidents and advance safety and environmental stewardship are highlighted.

1. Oil and Natural Gas Transportation Workplace Safety

The oil and natural gas transportation companies in the United States focus on workplace safety and achieve results significantly better than most other industries. According to the Bureau of Labor Statistics, petroleum refining, petrochemical manufacturing, pipeline, and rail transportation continue to provide some of the safest workplaces compared to all other private industries listed and much safer than the private industry average (Figure 4-1).

2. Crude Oil Transportation Spill Performance by Rail, Truck, Marine, and Pipeline

The Department of Transportation (DOT) issued a report to Congress on the delivery performance of shipping crude oil transported by truck, rail,

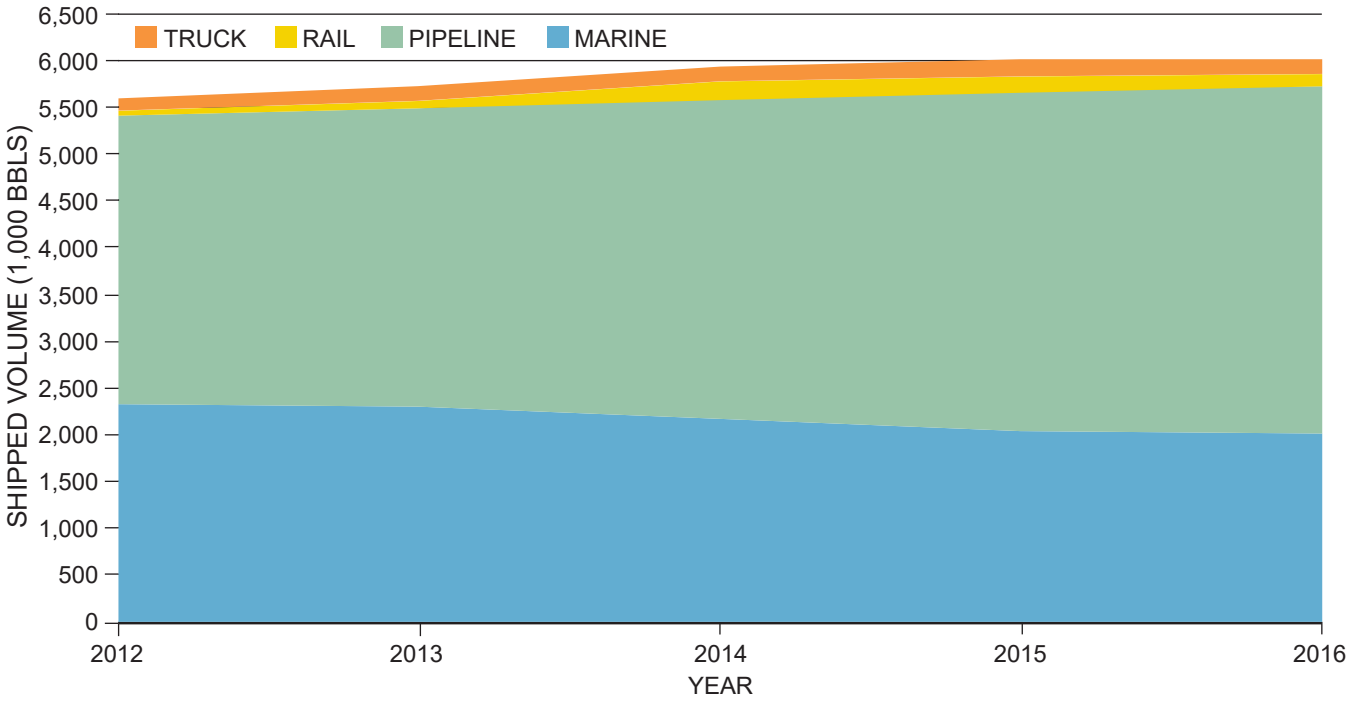


* Incidence rates represent the number of injuries and illnesses per 100 full-time workers and were calculated as (N/EH) x 200,000 where N = number of injuries and illnesses, EH = total hours worked by all employees during the calendar year, 200,000 = base for 100 full-time equivalent workers (working 40 hours per week, 50 weeks per year).

† Source for 2011-2018 rail freight data: http://safetydata.fra.dot.gov/officeofsafety/publicsite/summary.aspx. FRA, *Railroad Safety Statistics Annual Report*, 2010. Tables 1-2, 4-1. Note: Casualties include fatalities as well as injuries and occupational illnesses. Data for 2018 are preliminary as of March 2019.

Source: Bureau of Labor Statistics, U.S. Department of Labor, July 11, 2019.

Figure 4-1. *Total Injury and Illnesses Rate per Industry, 2009 to 2017*



Source: Pipeline and Hazardous Materials Safety Administration, Office of Hazardous Materials Safety, *Report on Shipping Crude Oil by Truck, Rail, Pipeline*, 2018.

Figure 4-2. *Crude Oil Shipments by Transportation Mode, 2012 to 2016*

marine, and pipeline on March 19, 2019. From 2012 to 2016, volumes of crude oil shipped increased to approximately 6 billion barrels per year (Figure 4-2). This report showed that over a 10-year period through 2016, crude oil transported by pipeline, marine, and trucking safely reached its destination more than 99.999% of the time. Over the 5-year period ending in 2016, crude oil volumes by rail increased significantly from prior years. During 3 of those 5 years, crude oil by rail safely reached its destination 99.999% of the time. Unfortunately, during 2 of the years the performance declined due to the occurrence of low probability but significant events. Further analysis and mitigating actions taken by the rail industry as a result of those events will be discussed in the rail transportation section (section III.C) of this chapter. Oil and natural gas transportation companies' focus is now on addressing the remaining 0.001% to eliminate incidents.

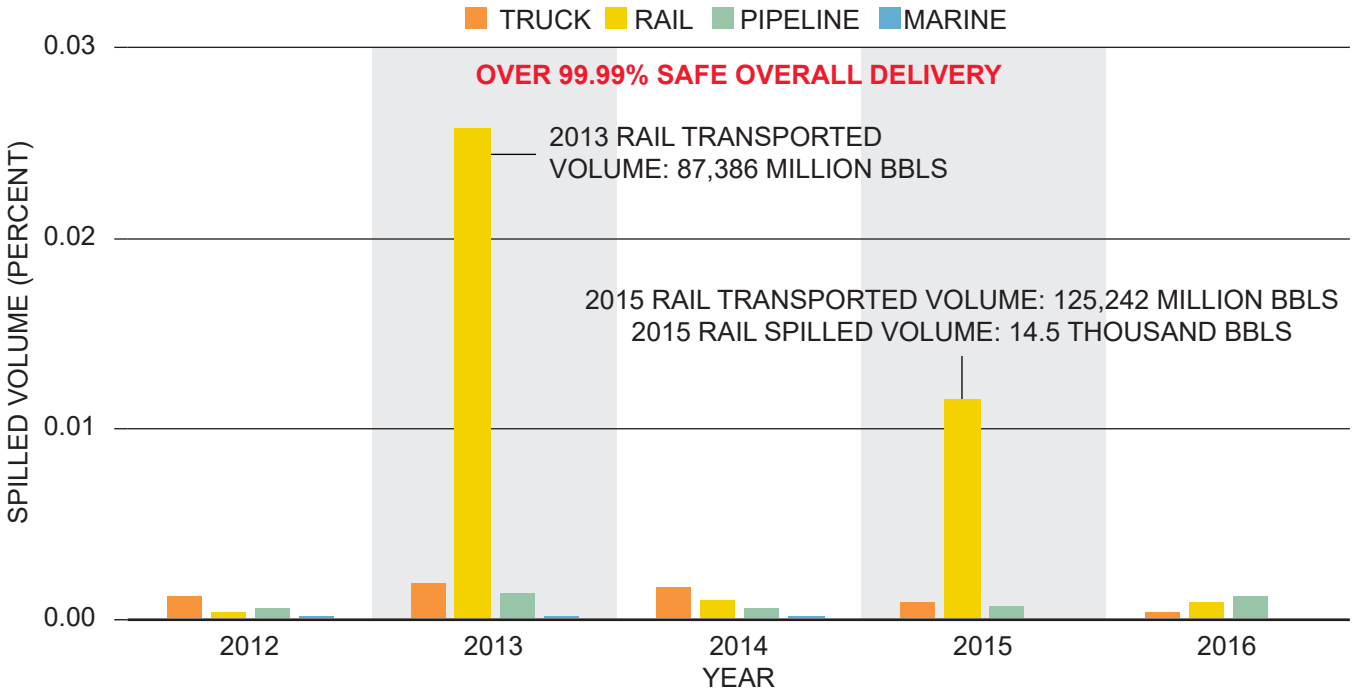
Since crude oil by rail volumes began to increase in 2012, as Figure 4-3 illustrates, there has been a positive level of safety and environmental performance for all transportation modes over the 5 years from 2012 to 2016. To put what it means to deliver safely 99.999% of the time into an everyday context, 99.999% is the equivalent to an error rate of 1 in 100,000 or an availability with only 5.26 minutes or less of downtime in an entire year.

The oil and natural gas transportation industry and regulators are constantly striving to eliminate incidents through continual learning, stronger management systems, and new technology research and development.

D. Industry and Government Research, Development, and Deployment

1. Research and Development Overview

Research and development (R&D) has and will continue to be a key part of the oil and natural gas transportation story. The industry is continuously in search for ways to enhance the safety and integrity of oil and natural gas operations and, in the process, reduce its environmental impact. Specifically, advancing new state-of-the-art technology development and the deployment



Source: Pipeline and Hazardous Materials Safety Administration, Office of Hazardous Materials Safety, *Report on Shipping Crude Oil by Truck, Rail, Pipeline*, 2018.

Figure 4-3. *Crude Oil Spill Performance by Transportation Mode, 2012 to 2016*

of leading engineering practices is critical to further improving an already strong energy transportation safety and environmental performance record. Safety improvements through innovation will help instill confidence in the general public, federal and state regulators, and other key stakeholders in the industry's ability to safely maintain and build new infrastructure in support of growing energy demand, global prosperity, and economic growth here in the United States. The energy and raw materials supplied by oil and natural gas are critical elements of our national economy, heating our homes, enabling our manufacturing, powering our vehicles, and providing the chemical building blocks that support modern life.

The importance of energy transportation to the economy and standard of living, globally and here in the United States, dictates that all stakeholders, including the government and private industry, place a priority on funding safety technology research. The industry and government must continue to invest in innovative technologies that can put critical capabilities and necessary knowledge in the hands of decision-makers to enable the continuous reliability and safe delivery of oil and natural gas energy on which so many depend. For additional information regarding research programs of government agencies and industry research associations, see Table 4-1.

2. Pipeline Industry's Role in R&D

In 1952, the various companies making up the natural gas pipeline industry came together in a collaborative venture to address the need for technological solutions to common pipeline operations problems. The success of this effort led to the creation of the Pipeline Research Committee (PRC) of the American Gas Association (AGA). Since its inception, PRC, now the Pipeline Research Council International (PRCI), an independent research association, has invested hundreds of millions of dollars in energy pipeline systems research. PRCI now includes the transportation of natural gas, crude oil, petroleum products, emerging fuels, and the associated facilities in its research programs.

Today, PRCI's members include companies in oil and natural gas pipeline operations, solution providers, and academic researchers from across the globe. It also partners with key governmental agencies in North America—DOT's PHMSA, the Environmental Protection Agency (EPA), U.S. Department of Energy Office of Fossil Energy (DOE-FE), Bureau of Safety and Environmental Enforcement (Department of the Interior), and the Canadian National Energy Board. PRCI is actively working to reduce the impact of corrosion, mechanical damage, and geohazards. PRCI is also researching ways to enhance construction and welding practices, material selection, and new construction. Other PRCI research areas include the next generation of tools for inspection, integrity, monitoring and surveilling rights-of-way to reduce the impact of third-party damage, and enhancing the use of satellites and unmanned aerial vehicles—remote sensing devices used to better understand the safety and integrity of the global pipeline systems.

These research programs are working to enhance public safety, pipeline integrity, and reduce the environmental impact of these assets. PRCI continuously works to enhance the needed technologies, processes, and people associated with safety and integrity. (For additional information, see https://www.prci.org/Research/ResearchObjectives.aspx.)

The American Petroleum Institute and Interstate Natural Gas Association of America work with other industry trade associations and member companies to carry out research programs that have benefited the safety and environmental performance of the oil and natural gas industry.

Another research group is the Gas Technology Institute (GTI). It conducts research focused on improving the integrity of natural gas pipeline systems, and new tools, methodologies, and technologies that can improve the accuracy of integrity inspections or reduce the costs associated with implementing an integrity management program. GTI works with state and federal agencies, national laboratories, natural gas utilities and pipeline companies, technology developers, and equipment manufacturers. (For additional information, see https://www.gti.energy/focus-areas/pipeline-integrity/.)

While industry technology development has focused on the pipeline network, as the demand for oil and natural gas has increased and as supply centers have shifted, there has been a need to add additional modes of transportation for these products: rail, marine and waterway shipping, and trucking. With the recent increase in production of natural gas and natural gas liquids from shale plays and oil from tight oil plays, it is

Government Research Programs	
DOT Pipeline & Hazardous Materials Safety Administration – Research Program	https://www.phmsa.dot.gov/research-and-development/pipeline/about-pipeline-research-development
DOE Office of Fossil Energy	https://www.energy.gov/fe/office-fossil-energy
Department of Energy Advanced Research Projects Agency-Energy	https://arpa-e.energy.gov/
Federal Railroad Administration – Research, Development, and Technology Program	https://www.fra.dot.gov/Page/P0019
Industry Research Associations	
Pipeline Research Council International	https://www.prci.org/Research/ResearchObjectives.aspx
Gas Technology Institute	https://www.gti.energy/focus-areas/pipeline-integrity/
Transportation Technology Center, Inc.	https://aar.com/

Table 4-1. *Research Programs*

even more important that the industry examine transportation alternatives. Historically, industry has primarily focused on research that addresses immediate- to short-term challenges (0 to 3 years).

3. Government's Role in R&D

The safe transportation of energy products is a shared responsibility that requires the support of the government. Based on the multimodal nature of energy transportation, DOT has several agencies focused on oil and natural gas transportation issues: the Federal Railroad Administration (FRA), the Federal Motor Carrier Safety Administration (FMCSA), the Maritime Administration (MARAD), and PHMSA. Each of these agencies generally focuses on research that targets short- to mid-term needs (3 to 5 years) or longer. They work in coordination with industry to identify and address strategic issues facing each mode of transportation.

DOE-FE oversees fossil energy research at the nation's National Laboratories, including the National Energy Technology Laboratory (NETL). NETL is responsible for implementing DOE-FE's R&D programs. Federally funded energy research tends to focus on the development of technologies that are longer term with higher uncertainties, hence, less likely to be led by industry; typically, the research is in fundamental science, high risk–high reward technologies, or longer-term challenges.

Improving collaboration on safety and environmental protection is an industry priority. One successful example of this is the iPIPE (intelligent Pipeline Integrity Program) consortium. iPIPE is a consortium of pipeline companies operating in several major production areas and the state of North Dakota. The consortium funds research for technology development in leak detection and prevention. The Energy and Environmental Research Center at the University of North Dakota issues requests for proposals for emerging technologies. The iPIPE consortium then commits funding to projects. Approximately $4 million in R&D has been funded by the consortium, with some of the underlying technology now entering the market with iPIPE consortium members.

a. Oil and Natural Gas Pipelines

i. Pipeline and Hazardous Materials Safety Administration

The mission of PHMSA's Pipeline Safety R&D Program is to sponsor R&D projects focused on providing near-term solutions that will improve the safety, reduce the environmental impact, and enhance the reliability of the nation's pipeline transportation system. The current Pipeline Safety R&D Program has a 5-year plan that employs a coordinated and collaborative approach to address recognized pipeline operational challenges and remove technical and regulatory barriers. The agency works to measure research results, outputs, and impacts, and publicize program processes, actions, and products.

As part of this effort, PHMSA co-funded with PRCI the development of a state-of-the-art pull test facility with the goal of developing, testing, and improving in-line inspection tools for pipelines. This led to the creation of the Technology Development Center (TDC), located in Houston, Texas. The TDC houses more than 1,700 pipeline samples, four pull test systems, and two pipeline flow loops for tool development and enhancement, as well as for personnel training and procedure testing and verification. The site enables the industry to test tools in a controlled environment and allows the validation of the tools, personnel, and processes needed to enhance pipeline safety and integrity, and reduce the environmental impact of the pipeline operation. (For additional information, see https://www.phmsa.dot.gov/research-and-development/pipeline/about-pipeline-research-development.)

ii. Department of Energy, Office of Fossil Energy

DOE-FE has maintained a robust combination of basic and applied research, conducted both in-house and externally, that accelerate the development of technologies supporting the oil and natural gas pipeline industry. Traditionally, DOE research has looked at long-term research needs with applications beyond 5 years, but the department has also invested in high-potential, high-impact research with closer commercialization horizons, particularly combining National Laboratory expertise with industry-academia

collaborative efforts. Current programs are developing technologies to cost-effectively detect, mitigate, and prevent the release of methane from natural gas pipelines and associated equipment.

DOE-FE is also conducting early-stage, foundational research on advanced pipeline technologies to support the mitigation of methane emissions. The ongoing DOE-FE Natural Gas Infrastructure Program is focused on developing specific technologies including: designing next-generation pipeline materials and coatings; improving the reliability of gathering, compression, and storage system components; creating multiparameter sensor platforms; advancing technologies for repairing pipeline damage without disruption of service; and developing data analysis systems to enhance pipeline infrastructure integrity management. All of these technological improvements could enhance the operational efficiency, reliability, safety and stewardship of natural gas midstream infrastructure.

In addition to natural gas pipelines, DOE-FE has funded basic National Laboratory research into the safety of transporting volatile crude oils by rail from the Bakken Shale of the Williston Basin. (For additional information, see https://www.energy.gov/fe/office-fossil-energy.)

iii. Department of Energy Advanced Research Projects Agency-Energy

The Advanced Research Projects Agency-Energy (ARPA-E) invests in high-potential, high-impact energy technologies to create new options for the nation's energy future, economic security, national security, and environmental well-being. ARPA-E awardees create entirely new ways to generate, store, and use energy, as the agency selects innovative projects that can make a significant impact over a finite period of time. Program directors and technology-to-market advisors provide projects with hands-on support to help them meet specific technical and market milestones. ARPA-E's goal is to develop a funded project to the point where private or public partners commit to advancing it.

The Methane Observation Networks with Innovative Technology to Obtain Reductions (MONITOR) program, for example, is developing innovative technologies to accurately and cost-effectively locate and measure methane emissions associated with natural gas production. Such low-cost sensing systems are needed to reduce methane leaks throughout the natural gas value chain, minimize safety hazards, promote more efficient use of domestic natural gas resources, and reduce the overall greenhouse gas impact from natural gas development. (For additional information, see https://arpa-e.energy.gov/.)

b. Surface Transportation

i. Federal Railroad Administration

Another mode of transportation for oil and natural gas regulated by the DOT is the railroad industry, which is supported by the FRA.

FRA's Research, Development & Technology (RD&T) mission is to ensure the safe, efficient, and reliable movement of people and goods by rail through basic and applied research and development of innovations and solutions. Safety is DOT's primary strategic goal and thus, the principal driver of FRA's RD&T program. The RD&T program also has an important role to play in workforce development. (For additional information, see https://www.fra.dot.gov/Page/P0019.)

The Transportation Technology Center (TTC) in Pueblo, Colorado, has a strategic role in the rail transportation R&D program. Since its dedication as the High-Speed Ground Test Center in 1971, it has played an important part in research, development, and testing of rail infrastructure and equipment. For example, Amtrak's Acela train was tested at the TTC prior to commencement of revenue service in 2000. The facility will continue to be used to ensure the safe implementation of new rolling stock and infrastructure technology.

The TTC is a partnership between the state of Colorado (which owns the land), FRA (which owns the structures), and the Association of American Railroads (AAR) (which currently manages the site). The TTC is managed under a unique care, custody, and control contract. The contractor, AAR, can use the facility for its own purposes, but in return it must maintain the facility and invest in site improvements. Annual maintenance and improvement plans will continue to be agreed with

the FRA and reconciled with the site master plan. Environmental sustainability improvements will continue to be made toward the DOT's targets for high-performance buildings and renewable energy. (For additional information see https://aar.com/.)

4. Academic Collaboration—Competitive Academic Agreement Program

PHMSA launched the Competitive Academic Agreement Program (CAAP) in 2013 to provide funding for academic research and provide tomorrow's pipeline safety workforce with an early opportunity to contribute safety solutions. PHMSA is working to drive innovation by funding projects that can deliver cutting-edge research and/or technology for the safety of the nation's 2.6-million-mile pipeline transportation network.

In its first 2 years alone, CAAP has provided more than $1.5 million to student researchers at the undergraduate, graduate, and PhD levels. PHMSA typically opens applications every spring and awards five or more research proposals every fall. Thanks to additional appropriated funding from Congress, PHMSA tripled the available award amounts to $300,000 from $100,000 in 2015, plus a 20% cost sharing by university partners on each project. Awards cover research projects up to 3 years in duration.

The cooperative agreements are competitively selected, and the number of awards depends on the quality of submissions and budget limitations. PHMSA prioritizes projects based in part on their potential to deliver preliminary pipeline safety findings (e.g., validating a thesis or theory's proof of concept) that can be further investigated through PHMSA's core research program or later CAAP project.

5. Technology Advancement and Deployment Challenges

Despite the significant improvements in safety, environmental, reliability, and operational performance that technology has contributed to the oil and natural gas transportation industry, there are challenges that companies face with respect to research, development, commercialization, and adoption of new technologies. The inherent challenges to deploying new technologies in this industry include required time and cost to develop and deploy, adequate acceptance testing, and regulatory impediments, among others. Most of these challenges translate into higher risks, costs, and uncertainty in the benefit-cost evaluation of new technology investments. The following represents several of the more prevalent challenges to advancing technology development and deployment in this sector.

- *Transformational effects of new technologies on organizations.* The implementation of new technologies can bring about transformational change to both processes and people within an organization, especially for a mature industry. For example, the increased penetration of digital technologies requires organizations to adapt to process automation and the accompanying systems and tools. They must also learn to collect, analyze, and use vast amounts of data at a rapid pace to make effective business decisions. This paradigm shift demands additional skills and expertise from the workforce and that transition takes time and investment. These technologies also introduce new risks such as those associated with the cybersecurity of operating system technologies and information. The costs and risks associated with such transformational change can be a significant barrier to new technology adoption.

- *Limited regulatory pathway for the testing, evaluation, and acceptance of new technology.* Existing regulations can challenge the advancement and deployment of new technology because they can hamper an operator's ability to address potential problems through the application of the most innovative technology, critical engineering assessment processes, and fit-for-purpose repair criteria based on data and sound engineering principles. The existing special circumstance permitting processes for incorporating new technologies are cumbersome and time-consuming, and there is lack of clarity around the requirements for approval. Also, these permits do not exempt operators from complying with existing requirements to address potential issues identified during a trial assessment, even if the technology and its accuracy are still under evaluation.

Regulations contain both prescriptive requirements and performance-based requirements. Both types of rules are important to establish clear expectations and to achieve high levels of operating safety. The key is to find the right balance of driving compliance and promoting continuous improvement through technology innovation. Prescriptive regulations that specify which methods and techniques to apply hinder the use of new alternative technologies that have the potential to achieve improved outcomes. Over time, regulations should adapt to accommodate to changes in the market such as new technologies and improved standards and practices, but the rulemaking process is lengthy and takes years before a regulation change is adopted.

- *Integration of new technologies with legacy infrastructure.* The oil and natural gas transportation system in the United States comprises many legacy assets, some of which have been in operation since the middle of the last century or earlier. This extensive physical asset base is also characterized by mechanical operating processes, although automation has become more prevalent. Retrofitting legacy infrastructure with new high-end technologies can be technically complex and costly and can slow the technology adoption process.

- *Ineffective sharing of technology evaluation results among peers.* The insufficient sharing of technology evaluation results among peers can lead to duplicative efforts. Valuable resources and time can be spent on repeating new technology initiatives that do not build upon already established know-how. Closer cooperation and cost sharing among operators, as well as with government, can alleviate some of the cost burdens associated with testing and validation of safety technologies.

- *Proving the effectiveness of new technologies can be difficult to establish.* Trials can take longer than expected and delay scale-up adoption. The impact of these tendencies has historically led to a slower rate of new technology adoption in the oil and natural gas extraction industries compared to some other industries (e.g., information technology).

- *An insufficient end-to-end level of technology readiness can impede adoption.* Cutting-edge innovations are often developed by small start-up companies that are focused only on a specific aspect of a problem and must rely on operators for end-to-end technology integration. Early technology adopters face the risk of technology functionality challenges and high early-adopter costs. When the cost of early technology adoption does not provide an adequate return on investment, additional incentive mechanisms and collaboration among operating companies and technology providers may help encourage wide-scale deployment of advanced technologies.

- *Demonstrating a favorable benefit-cost analysis of new technology.* Innovation will not gain traction without a demonstrated favorable benefit-cost ratio. Evaluating the benefits and costs of new technology can be difficult because of their inherent uncertainty. On the benefits side, there are both economic and noneconomic benefits to consider, but the latter are difficult to quantify. For example, risk reduction benefits resulting from the implementation of safety technologies can be difficult to measure. From the cost perspective, initial costs of new technology tend to be very high. Costs can be driven down as technologies mature and as industry adoption increases. Achieving wide-scale industry adoption often requires additional investment in technology development and field validation and the amount and timeliness of cost reduction is uncertain. Some new technologies can have far-reaching impacts across the oil and natural gas supply chain, which can translate into very high implementation costs and should be factored into the decision-making process.

Findings:

- Industry, in cooperation with federal agencies, is advancing promising new technologies to prevent high-impact events. Adoption of new technology can be impeded by high early-adopter costs.

- Existing regulations, prescriptive and performance based, are designed to promote safety. However, some prescriptive aspects of existing regulations slow the adoption of

new technologies. The sometimes-lengthy regulatory review and approval process for introducing new technology increases the cycle time for wide-scale adoption.

The NPC recommends that Congress should authorize DOT to lead a collaborative effort, with support from industry, to develop and prioritize pilot programs that can accelerate pipeline, storage, and LNG technology adoption based on performance-based rules with a goal of enhancing public safety. Upon successful completion of pilot programs, regulators should promptly update their regulations to allow use of new technology.

Pilot programs should be established to include multiple industry operators to facilitate widespread adoption of new technologies. This collaborative effort between PHMSA and industry should include defining the process for program management, prioritizing which opportunities to accept into the pilot programs, and identifying field validation requirements. The pilot program should be a two-step process:

- Lab testing for 6 to 12 months at sites (e.g., PRCI's Technology Development Center, FRA's Transportation Technology Center, or DOE's Methane Emission Test and Evaluation Center site) to validate performance against set criteria/performance metrics.

- Field testing for 1 to 3 years to develop a database of performance on state-of-the-art technology that can help inform regulatory changes and leading industry practices. This step would include test runs in actual field operating environments that should not be burdened by prescriptive regulation during testing, provided operators maintain compliance and ensure public safety.

The pipeline industry, associations, and standards bodies, in collaboration with DOE and DOT, should develop criteria and performance metrics for technology adoption to enhance in-line inspection, nondestructive evaluation, leak detection, and technologies to reduce methane emissions and to increase safety, integrity, and reduce the environmental impact of our nation's pipeline systems. This coordination will enable a greater focus on the key challenges facing the industry and encourage more efficient use of limited resources and drive the adoption of new technology.

The NPC recommends that:

- Oil and natural gas transportation companies should establish a collaborative effort with participation from DOT, DOE, EPA, and industry research consortiums to prioritize promising, risk-based research opportunities, to establish consistent technical readiness processes, and to prioritize field validation testing needs.

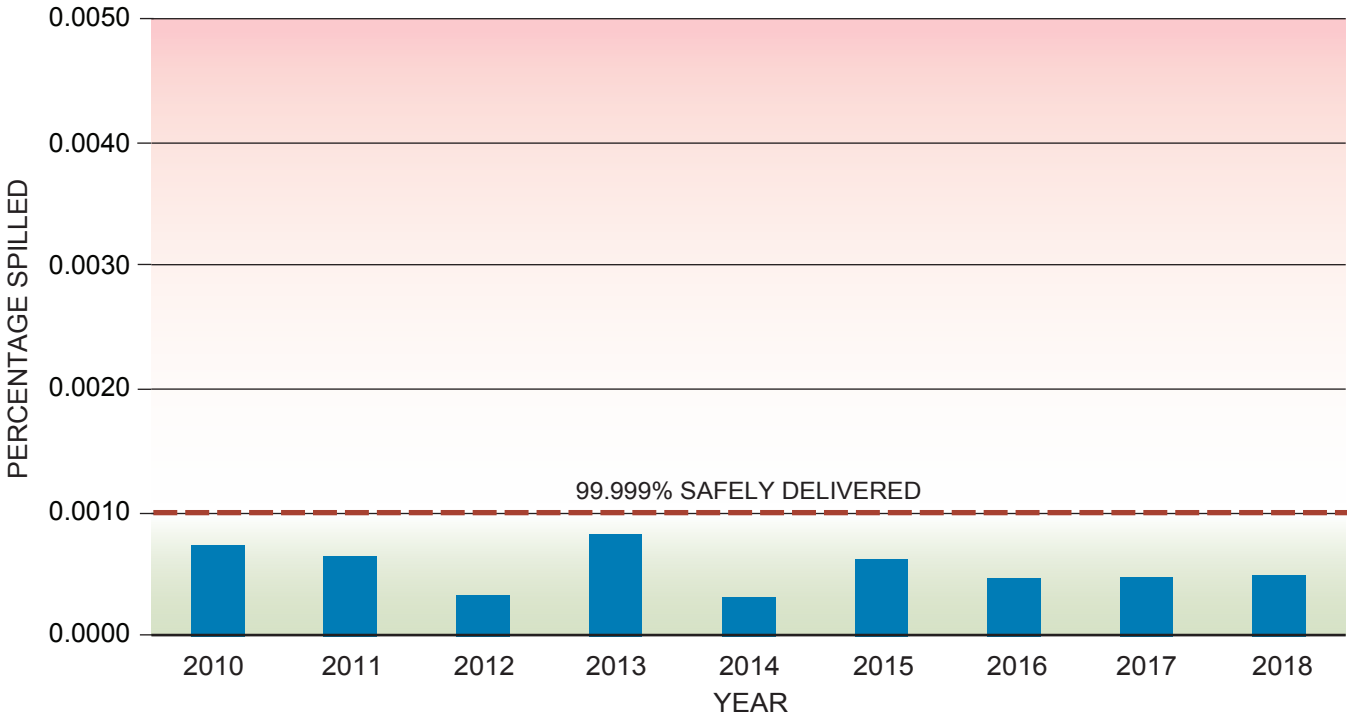
- DOT should lead, while working with DOE, EPA, and U.S. Coast Guard, creation of an agile pathway for evaluation and regulatory acceptance of new technologies that can improve transportation safety and shorten the research, deployment, and adoption cycle time.

- The Federal Energy Regulatory Commission and state regulatory agencies should work with DOT, DOE, and others to promote laws, regulations, and public-private partnerships that support funding protocols and/or cost recovery for natural gas and oil pipeline safety research.

II. PIPELINE AND STORAGE INDUSTRY TECHNOLOGIES

A. Pipeline Industry Overview

There are more than 210,000 miles of regulated crude oil and other liquid petroleum products and more than 300,000 miles of regulated natural gas transmission pipelines in the United States—and these products arrive safely at their destinations more than 99.999% of the time (Figure 4-4). This strong safety and environmental record is due to the dynamic nature of the pipeline industry, which is constantly developing safer and more efficient technologies, as well as enhancing its safety management systems.



Source: Pipeline and Hazardous Materials Safety Administration, Program Management, Data, and Statistics Division, *Incident Statistics*.

Figure 4-4. *Spilled Percentage of Total Liquid Pipeline Volumes Transported by Year, 2010 to 2018*

Over the years, much of the existing pipeline infrastructure has been expanded or repurposed to accommodate demand growth. Some pipelines have reversed directional flow or changed service to meet business needs. Technology plays an important role in these changes to ensure fitness-for-duty design and testing. The pipeline industry has consistently raised the bar for responsible operation, thanks to the wealth of trend data built up over many decades. These data have been put to great use by individual operators as well as industry coalitions to drive specific initiatives for advancement. Together with a well-known regulatory framework, this ongoing collaboration and focus on continuous improvement has fostered the development of a wide range of commercial technologies and helped make them broadly available for use in the field. The technologies have targeted improvement across a range of areas, all focused on the leading causes of incidents.

As shown by government data publicly available from PHMSA in Figure 4-5, Figure 4-6, and Figure 4-7, corrosion failures represent the number one cause of all liquid and natural gas pipeline incidents,[2] averaging 25% to 30% of the incidents. While equipment failures drive the next highest number of incidents for liquid pipelines, they account for only 4% of the volume. Four categories of causes (i.e., corrosion, excavation damage, natural force damage [e.g., geohazards], and pipe/weld failures) contribute to approximately 75% of all volume released from pipelines. This section will explore key pipeline technologies associated with each of these major incident drivers.

2 Liquid pipeline incident definition:

Tier 1 (independent of location): Fatality, injury requiring in-patient hospitalization, ignition, explosion, evacuation, wildlife impact, water contamination, or private property damage.

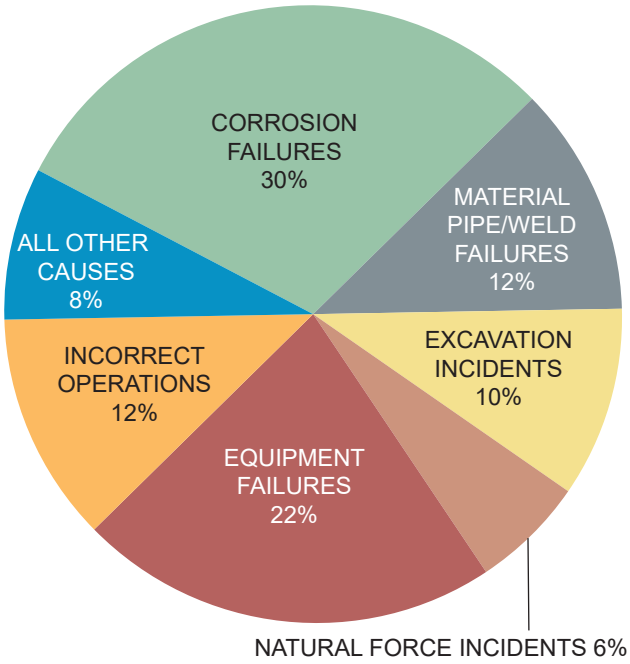
Tier 2 (location not contained on operator-controlled property): Unintentional release volume greater than or equal to 5 gallons and in a high consequence area (HCA); or unintentional release volume greater than or equal to 5 barrels and outside of an HCA; or water contamination; or soil contamination.

Natural gas pipeline incident definition:

I. A death, or personal injury necessitating in-patient hospitalization

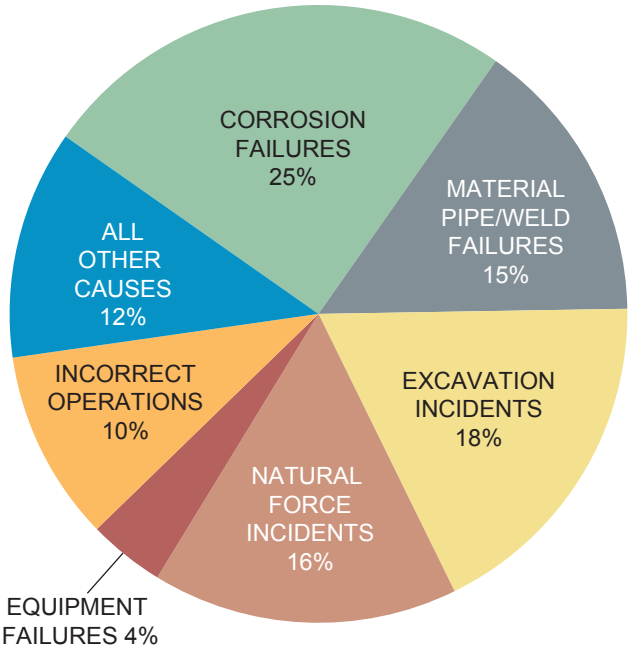
II. Estimated property damage of $50,000 or more, including loss to the operator and others, or both, but excluding cost of gas lost

III. Unintentional estimated gas loss of 3 million cubic feet or more.



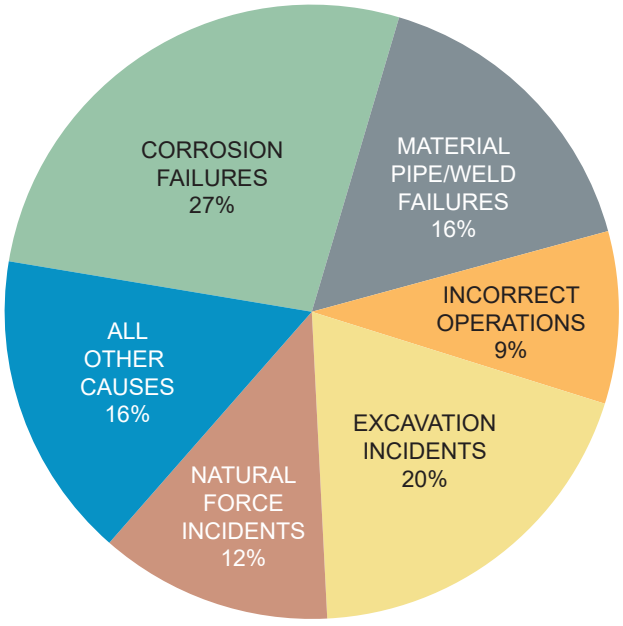
Source: Pipeline and Hazardous Materials Safety Administration, "Annual Report Mileage for Hazardous Liquid or Carbon Dioxide Systems," July 1, 2019.

Figure 4-5. *Percentage of Liquid Pipeline Incidents Impacting People or the Environment by Cause, 2014 to 2018*



Source: Pipeline and Hazardous Materials Safety Administration, *Annual Report Mileage for Hazardous Liquid or Carbon Dioxide Systems*, July 1, 2019.

Figure 4-6. *Percentage of Pipeline Barrels Released Impacting People or the Environment by Cause, 2014 to 2018*

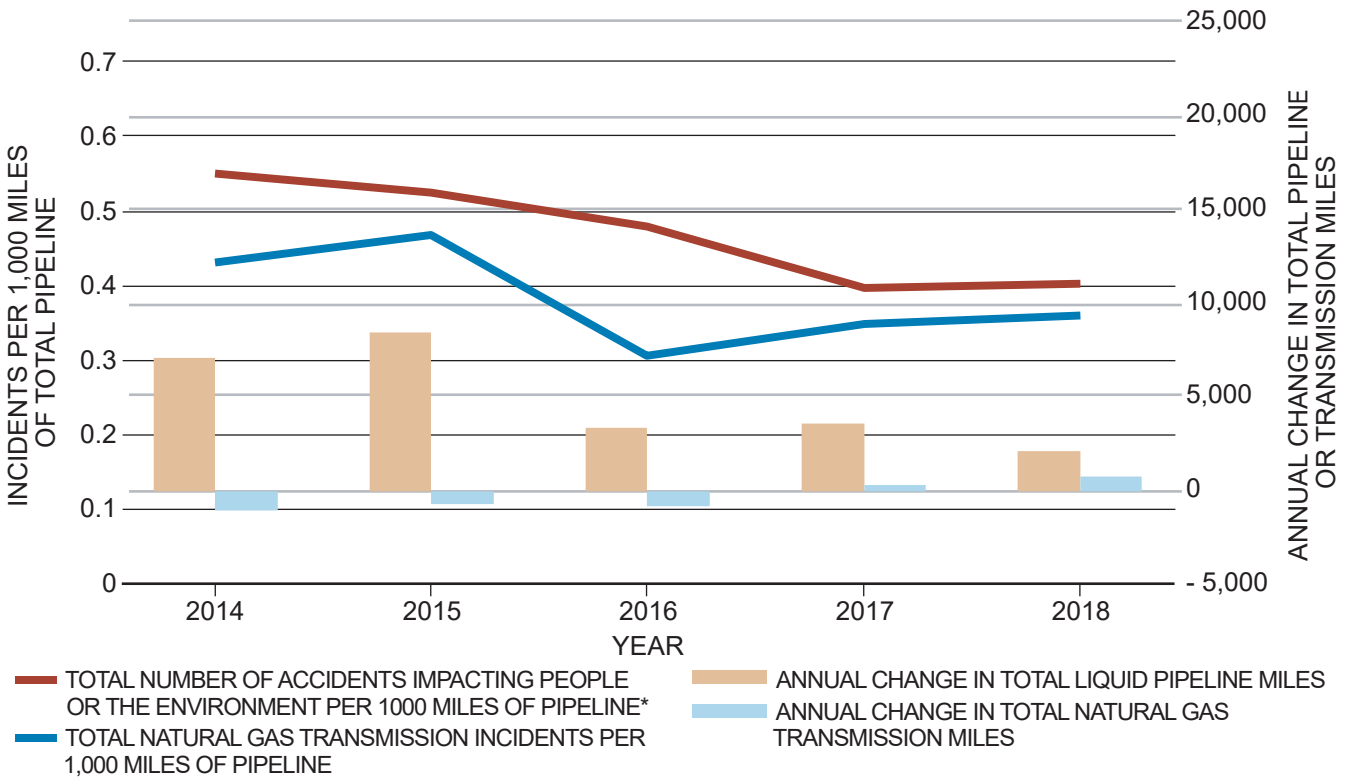


Source: Pipeline and Hazardous Materials Safety Administration, Program Management, Data, and Statistics Division, *Incident Statistics*.

Figure 4-7. *Onshore Natural Gas Transmission—Percentage of Significant Incidents by Cause, 2014 to 2018*

Pipelines are getting safer. The number of incidents in the natural gas transmission and hazardous liquid pipeline industry has declined in the past 5 years while industry infrastructure mileage and volumes shipped have increased. As seen in Figure 4-8, liquid pipeline incidents impacting people or the environment have declined by 20% while infrastructure has grown. The number of natural gas transmission incidents has also declined in the most recent 5 years while pipeline capacities have increased from the existing infrastructure.

As shown in Figure 4-9, the primary causes of pipeline accidents involving fatalities since 2010 are related to material/weld incidents, excavation incidents, incorrect operations, and outside forces. This further supports the priorities for pursuing technology innovations in those areas. Improving incorrect operations is one of the pillars for industry's ongoing commitment to safety excellence and is addressed primarily through training and management systems. To the extent that



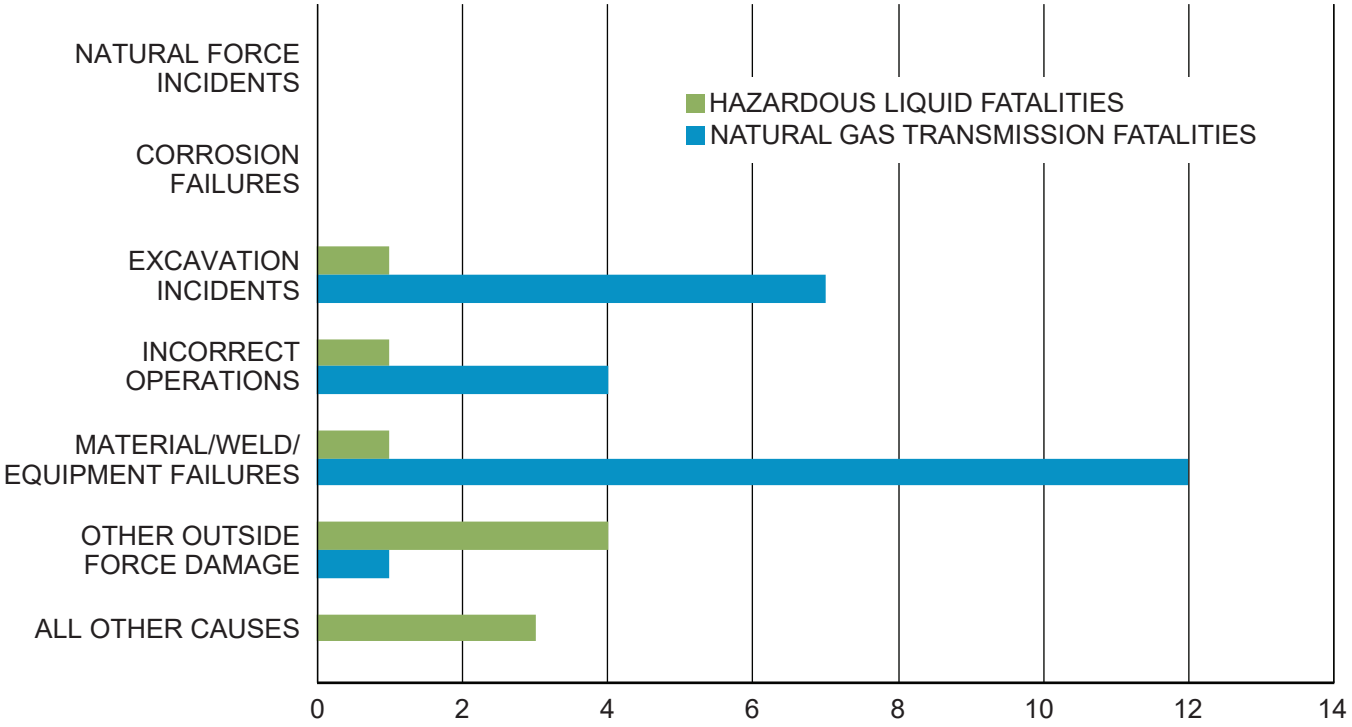
Source: Pipeline and Hazardous Materials Safety Administration, Program Management, Data, and Statistics Division, *Incident Statistics*.

Figure 4-8. *Total Liquid Pipeline Incidents Impacting People or the Environment and Natural Gas Transmission Incidents per 1,000 Miles of Pipeline with Annual Change in Total Pipeline and Transmission Miles, 2014 to 2018*

technology innovations can assist with reducing human error, those are also opportunities to support performance improvement.

The safety improvement trend is supported by a layered integrity management program approach used across the industry. As shown in Figure 4-10, this covers both preventative and mitigating measures. Technology advances are foundational to some of these, and this chapter investigates those related to construction and maintenance, as well as both asset and operations integrity. The construction and maintenance category involves employing appropriate materials, fabrication, and installation practices for long-term integrity of new assets, and on ensuring maintenance and repair practices lead to long-term integrity of existing assets. Asset integrity focuses on inspection tools and assessment protocol of pipeline assets. Operations integrity covers leak detection as well as surveillance of external threats, particularly geohazards and encroachment of right-of-way. Technology improvements in each of these areas support key safeguards for managing overall pipeline integrity, thereby reducing loss of containment incidents that could otherwise impact people or the environment.

Pipeline safety improvements are also supported through robust, collaborative industry associations. Through organizations including the American Petroleum Institute (API), American Society of Mechanical Engineers, American National Standards Institute, NACE International, and National Fire Protection Association (NFPA), among others, the pipeline industry creates and maintains a comprehensive set of industry standards and recommended practices. These standards and practices address management systems, safety, asset integrity, manufacturing and materials, emergency response, operations, etc. Pipeline companies devote staff and



Source: Pipeline and Hazardous Materials Safety Administration, Program Management, Data, and Statistics Division, *Incident Statistics*.

Figure 4-9. *Total Liquid Pipeline and Natural Gas Transmission Fatalities by Cause, 2010 to 2018*

resources to develop and update these standards and practices. Government agencies and third-party stakeholders are frequently represented on committees that draft the standards and practices. This system helps establish expectations for responsible operations, provides technical resources for pipeline companies, and contributes to safety and performance improvements across the industry.

There are numerous industry standards (including those of API, ASME, NACE, NFPA, etc.) referenced by government agencies, including the U.S. Coast Guard, the EPA, the Federal Trade

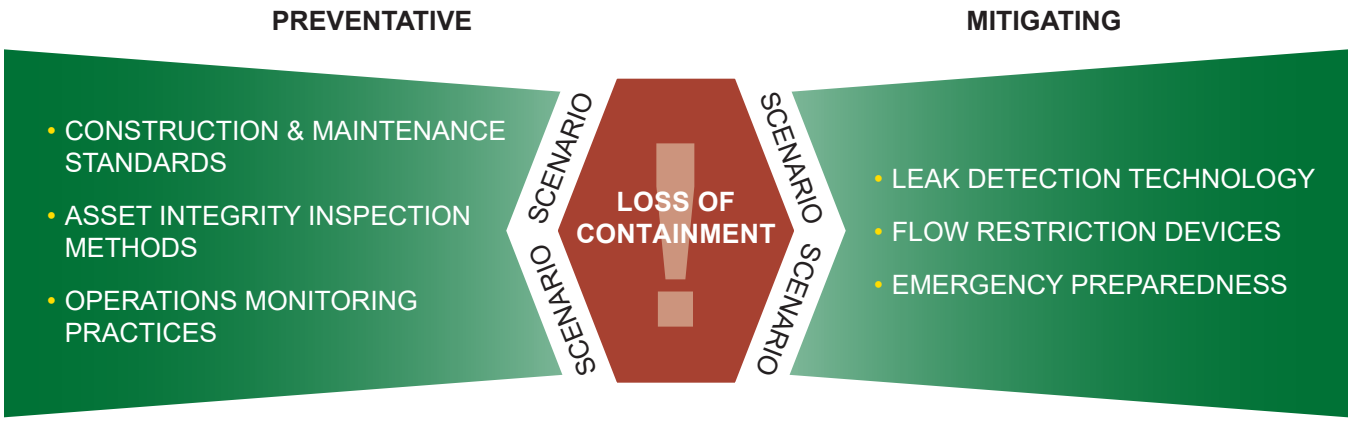


Figure 4-10. *Key Safeguards for Managing Pipeline Integrity*

Commission, the DOT's PHMSA, and the Occupational Safety and Health Administration, in addition to the Bureau of Safety and Environmental Enforcement. It is beneficial to have PHMSA's participation in the review of key new industry standards being developed. This provides more awareness for PHMSA to understand industry practice as well as to share their insights into new standards and recommended practices being developed.

B. Pipeline Asset Integrity

1. Asset Integrity Overview

Asset integrity entails the inspection and assessment of the condition of pipelines, as well as the areas in which pipelines operate. Asset integrity programs identify and address specific operating conditions and threats encountered by pipelines. Pipeline companies have extensive programs and procedures, often referred to as integrity management programs, that meet DOT PHMSA regulatory requirements as well as the requirements of state regulators and industry standards bodies (e.g., API, American Society of Mechanical Engineers, etc.) and these programs are subject to audit and inspection by regulators. Programs specify the methods and intervals for pipeline inspections and assessments, risk analysis methodologies, methods for incorporating new data and information, acceptable repair methods, and the roles and responsibilities for administering the program. A critical component of all integrity management programs is program evaluation and continuous improvement. The goals of integrity management programs are to prevent product releases to the environment and ensure the continued safe operation of pipelines.

The industry is committed to improving safety performance through the effective and reliable management of asset integrity related threats.[3] While deploying technological advancements has helped improve overall safety and performance records in the industry, opportunities remain for achieving pipeline operations free of incidents. Figure 4-11 demonstrates this, showing the decline in the number of liquids pipeline incidents impacting people or the environment between 2014 and 2018. The decrease in incident rates, while the miles of pipeline operating and throughput of product are increasing, indicates that the industry is advancing its capabilities, although continued technology advancement and deployment are necessary to maintain the trend and realize further improvements.

Improved management systems have also been essential to asset integrity performance improvements. The industry, federal and state regulators, and representatives of the public collaborated to draft and implement API Recommended Practice (RP) 1173, Pipeline Safety Management Systems, the first edition of which was released in 2015. RP 1173 advances the industry's capabilities and provides a comprehensive framework for managing pipelines, including asset integrity. Pipeline operators develop the specific programs, plans, and procedures necessary to safely manage their systems and enable continuous improvement (through Plan-Do-Check-Act feedback loops) in accordance with the RP 1173 framework. Safety management systems are essential to reinforcing a safety culture and deploying the processes and programs within a company to effectively deploy advanced technologies. The industry is advancing with the adoption of RP 1173; a recent study[4] polled a sample of industry operators who indicated that approximately 74% of the industry has adopted RP1173 while the remainder has implemented similar programs.

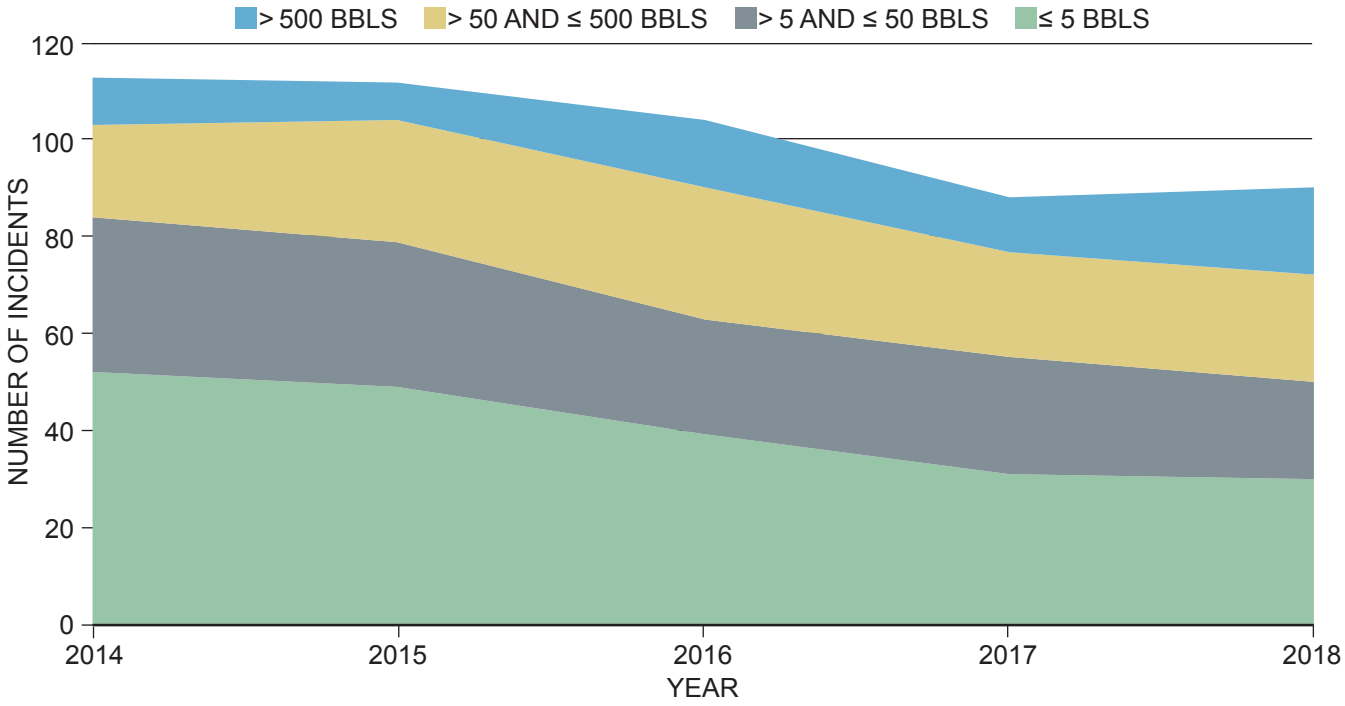
Finding: API RP 1173 has been vital to improving pipeline industry safety performance through standardization of key elements and expectations of management systems.

The NPC recommends that pipeline companies should continue to seek opportunities to proactively implement safety management systems and strengthen industry-wide safety culture to continuously improve performance.

Successful management of asset integrity encompasses a wide range of technological

3 Fang, S. (2016). *Industry Reinforces Core Value of Safety and Goal of Zero Pipeline Incidents*, American Petroleum Institute, https://www.api.org/news-policy-and-issues/news/2016/03/17/industry-reinforces-core-value-of-safety.

4 Collier, R., "Pipeline Safety Management Benchmark Study: Adoption of API RP 1173," *Western Energy*, Spring 2019.



Source: American Petroleum Institute (API) and Association of Oil Pipelines (AOPL), *Pipeline Safety Excellence Performance: 2019 Annual Liquids Report*.

Figure 4-11. *Liquid Pipeline Incidents Impacting People or the Environment by Size, 2014 to 2018*

expertise relying on effective detection, measurement, and assessment of a range of pipeline threats. The industry has developed a large suite of technologies to address asset integrity threats, including corrosion, cracking, and dents. Research is underway to advance these technologies in a variety of areas. Detection and measurement technologies are critical to preventing product releases. With more reliable and higher quality technology, the industry can improve safety performance by proactively addressing any damage to the pipeline.

Recent industry incident data (Figure 4-6) indicates that pipeline releases are caused by a variety of factors. Of these primary industry failure causes, asset integrity programs are primarily focused on managing corrosion. Material pipe/weld failures are another important focus of asset integrity programs.[5] Adequately addressing these pipeline failure causes requires multiple technologies. Continued development of a combination of in-line and field (or, in-the-ditch) inspection tools, assessment techniques, integrity management frameworks, and regulatory processes will be required to ensure that the industry continues to advance. This will require investment in technology development through established frameworks, enhancement to regulations that allow use of the best available technologies, and support for increased collaboration among regulators, operators, vendors, and researchers. Damages to pipelines can occur over the lifetime of operation, even after rigorous engineering design standards and effective protection strategies are applied. The purpose of asset integrity programs is to reduce operating risk, to identify any damaged areas of the pipe (typically referred to as features) and repair them before they create an opportunity to leak, thus protecting public safety and the environment. The vast majority of asset integrity concerns within pipelines fall under three primary threat types—metal loss, cracking, and deformation (Table 4-2)—which can occur separately or in combination with each other (commonly referred

5 The Pipeline Operations Integrity and Pipeline Construction and Maintenance sections (II.C and II.D) address excavation incidents and natural force incidents, among other areas.

Threat	Description	Detection and Management
Metal Loss (Corrosion)*	• Thinning of the pipe wall typically caused by general internal or external corrosion. • Can reduce the pressure containing capacity of the pipeline or lead to the formation of small leaks if not identified and effectively managed over time. • In most cases, occurs over long periods of time.	• Prevented through coating the external surfaces of the pipe, using cathodic protection, and managing the products being transported by the pipeline (e.g., using corrosion inhibitors). • Effective integrity management techniques can be used to identify and track growth of corrosion and ensure that repair is prioritized and occurs expeditiously. • Typically seen as one of the best understood threats to transmission pipeline safety.
Cracking†	• Defects where the pipe material splits apart due to the application of stress within the material. • Often grow at preexisting manufacturing flaws, areas where corrosion can form, in and around welds used to form the pipeline, or in the base metal of the pipe itself. • Can be caused by changes in loading condition (i.e., fatigue) or as a result of loading and environment (e.g., stress corrosion cracking). • Can grow over time or remain stagnant unless certain operating thresholds (operating pressures or pressure cycling intensities) are reached. • Many crack types, or morphologies, that may be difficult to identify depending on inspection technology and behave differently over time. • Crack-related failures may result in small leaks or have historically been shown to have the potential for significant releases if not properly managed.	• Considered to be more difficult to manage and inspect than other threats due to the complex nature of crack morphology and fracture mechanics. • Current methods have been effective for managing the crack threat; additional technological advancements will be beneficial.
Deformation‡	• Conditions that cause unintended permanent deformations to the pipeline and are typically caused by accidental contact of construction equipment with the pipe, settlement of the pipe onto rocks, or ground movement. • Equipment impacts, and settlement damage typically form dents or gouges. • Pipeline dents represent a change in the pipe's cross-sectional area, which can pose a threat to the pipe's integrity. • Gouges occur when the pipe is scraped causing material removal and often coincide with dents. • Dent formation can lead to instantaneous failures (like popping a balloon) or the damage can remain dormant for long periods of time (delayed failure mechanisms), which are the focus of asset integrity programs.	• Dent features are easily identified but can be challenging to analyze due to the variability in possible dent shapes. • The severity of mechanical damage is typically assessed based on the depth of the dent, the shape of the dent, and the presence of any metal loss, gouging, or cracking within the dented pipe area. • Current assessment methods for dents are not as detailed or quantitative as those used for cracking and corrosion and are thus a current focus of industry development.

* Abdolrazaghi, M., Hassanien, S., Li, Y., Garcia, A., Krissa, L., and Place, T. (2019). *Corrosion Management Technologies and Methodologies*. Topic Paper 4-3. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

† Refer to Potts, S., MacKenzie, B., Lamborn, L., Abdolrazaghi, M., and Bubenik, T. (2019). *Crack Detection and Management*. Topic Paper 4-4. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

‡ Refer to Langer, D., and Kainat, M. (2019). *Dent Inspection and Assessment*. Topic Paper 4-5. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

Table 4-2. *Pipeline Asset Integrity Threat Types*

to as interacting threats). Pipeline operators make significant investments to maintain the demonstrated high levels of safety performance of their assets.

Three primary asset integrity management strategies—direct assessment, hydrostatic testing, and in-line inspection—are typically used in combination by pipeline operators as they seek to evaluate pipelines, identify potentially at-risk pipeline conditions, and direct necessary repair efforts. Direct assessment typically occurs when a pipeline (or portion of a pipeline) is excavated and inspected with hands-on approaches yielding detailed information about the excavated area. These inspections are typically nondestructive examinations where multiple inspection tools are used to identify any defects in the pipe material. In some cases, pipe sections or materials will be removed for destructive testing. The primary challenges with direct assessments are that they are costly, they only investigate a small portion of the pipeline, and they have inherent risks due to the excavation process. Large diameter piping systems are typically designed to be piggable and therefore, in most of those integrity programs, pipeline operators use direct assessments to investigate areas of pipe already identified as requiring further investigation or repair by other integrity management strategies, to validate in-line inspection tool performance, and to ensure that all features of interest have been appropriately identified.

Pipeline operators use hydrostatic testing to prove the safety of a pipeline at a given operating pressure through filling the line with water and holding it at a specified pressure for a defined period of time. Any weak features on the pipeline (i.e., those which are incapable of holding this pressure) will fail and hydro testing water will be released, after which the release location is identified, repaired, and the testing process is restarted. As the pipeline is cleaned prior to this test and filled with clean water, each test is designed to minimize environmental consequences. Following successful completion of a hydrostatic test, the line is proven to be safe up to the test pressure and usually operated at some percentage of this maximum value to ensure a sufficient safety margin. Through analysis, the growth of any nonhazardous features remaining on the line after hydrostatic testing can be estimated and the line retested before any of these features has any potential for failure. Hydrostatic testing is effective and commonly used in the industry; however, it can be very costly to perform, has the potential to cause incremental damage to the pipeline, and provides limited detail about the distribution of undetected features remaining on the pipeline after the test is performed.[6]

In-line inspections (ILIs) have become the preferred method for many operators for inspecting the pipe integrity of pipelines. ILI provides substantial amounts of data about the pipeline in comparison to the historical method of hydro testing to determine pipeline integrity. These inspections use a variety of in-line inspection tools, also known as "smart pigs," which can travel through the pipeline and, through the application of multiple sensing technologies, provide detailed information about the pipe condition including threats such as metal loss, cracking, or deformation.

ILI results are analyzed on a feature-by-feature basis to identify any potential areas of concern. Features with an insufficient safety margin are repaired. Growth prediction models can be utilized to estimate how the features may change or grow over time. Pipeline operators use the results to schedule reinspection intervals (i.e., acceptable time periods until the next inspection) to ensure that the line remains effectively monitored and analyzed. ILI requires the effective application of a variety of inspection tool technologies, data handling technologies, and assessment engineering methods. This section documents findings and recommendations for ILI technology improvement opportunities.

Pipeline operators typically maintain asset integrity through a combination of methods. In general, hydrostatic testing is typically performed when a pipeline is brought into operation and repeated if major operating changes are expected or if there are integrity concerns that cannot be managed through other means. Following the

6 Further, in natural gas pipelines, it requires blowdown (i.e., venting gas to the atmosphere) of the segment being tested. Refer to the Pipeline Methane Emissions section (II.F) for more details.

hydrostatic tests, ILI are performed at regular intervals to monitor the condition of the pipeline and to identify and assess any threats that might be present on the line. Databases store ILI data to allow for comparison between inspections and monitor features of interest. Any features deemed to be potentially injurious, based on assessment of the inspection data, are mitigated through pressure reductions or pipeline repair. When a pipe section is selected for repair, the pipeline operator will excavate a portion of the line and perform a direct assessment before repairing any defects using a variety of proven methods. The pipeline operator will use the results of the direct assessment to validate the in-line inspection tool performance and provide additional information about line condition. If any concerns are identified during the validation, the pipeline operator may order the in-line inspection to be repeated or that the line be reassessed to account for any deficiencies. This process is repeated at regular intervals throughout the life of the pipeline to ensure that safe operations are maintained.

2. Inspections and Feature Detection

The oil and natural gas pipeline industry has decades of experience inspecting pipelines and detecting features. Inspections are regular parts of pipeline integrity management programs. The purpose of inspections is to identify features on the pipeline system and create mitigation or repair programs based on the findings. Inspections help pipeline operators gather the data necessary for understanding the condition of the pipeline system and to responsibly operate and maintain the system. The industry deploys highly specialized technologies to conduct pipeline inspections and data analysis. Mature management systems, supported by industry standards (e.g., API 1173), steer integrity and promote robust safety cultures.

Technology that supports the pipeline business is developing at a rapid pace and many improvements to standards/recommended practices that incorporate these technology advances are available for regulatory adoption today. Many industry committees are actively developing and enhancing standards and best practices for all critical asset integrity threats to support industry-wide adoption of the best available techniques. For example, the current version of the API Standard 653 (5th edition) recognizes risk-based tank inspection methodologies while current pipeline regulations still reference an older edition that does not consider risk-based inspection. Other examples such as the API's Recommended Practice 1160 (Managing System Integrity for Hazardous Liquid Pipelines), Standard 1163 (In-line Inspection Systems Qualification), and Recommended Practice 1176 (Assessment and Management of Cracking in Pipelines), and ASME's B31.8S (Managing System Integrity of Gas Pipelines) offer industry best practices that could be adopted into pipeline regulations.

Operators typically lead the advancement of consensus standards through organizations such as API. Regulators are key stakeholders and participate in the development of these standards, where applicable. Several DOT PHMSA regulatory references to industry standards continue to reference earlier editions than the latest edition. Accelerating assessment and acceptance of the latest industry standards that are incorporated into regulations by reference would help to accelerate cost-effective implementation of new technologies across the industry. As API and other industry standards bodies update and develop new standards, PHMSA should continue to actively participate in the standards development process.

Finding: Industry-led standards and recommended practices continue to be updated with the latest methods and a more streamlined regulatory acceptance process could promote accelerated risk reduction.

The NPC recommends that PHMSA should accelerate its process for validating and incorporating safety and environmental performance aspects of the latest editions of industry standards and recommended practices that are referenced in the regulations, to the extent practicable.

Pipeline inspections are typically performed using either in-line or nondestructive field examination technologies. In-line tools typically consist of mechanical or electrical devices that detect

features as the tool travels through the pipeline. Skilled technicians perform field inspections outside of an exposed pipe using handheld tools of varying complexities. When combined, these technologies allow the pipeline operator to identify locations that require repairs to maintain safety and provide data that support planning of proactive maintenance programs.

There are many different technologies available for in-line inspection that can each identify and measure different types of pipeline threats. Magnetic flux leakage tools generate magnetic fields within the pipe wall to identify its thickness and are commonly used for corrosion measurements. Ultrasonic tools use sound waves in the pipe wall and can identify areas of potential cracking or determine pipe wall thickness depending on the orientation of the sound waves. Caliper tools use a series of mechanical arms to identify changes in the internal diameter of the pipe to identify areas of deformation. Inertial measurement tools can track the pipe centerline using accelerometers to identify areas where the pipe has moved or may be experiencing strain.

The latest technologies supporting in-line inspection are phased array ultrasonic and electromagnetic acoustic sensors. Industry deploys these tools primarily for crack measurement. Through different combinations of these in-line inspection tools, operators can identify the presence of potential integrity threats and leverage the tool data to perform assessments on each reported feature to identify areas of potential integrity concern. Industry constantly enhances these and other technologies to improve their resolution, accuracy, repeatability, and overall performance to help ensure the best accuracy possible for integrity assessments.

Inspections performed in the field look at the pipeline from the outside, as cutting out portions of the pipe for inspection is costly and only performed for special cases. These inspections are referred to as nondestructive examinations and are frequently used to validate the results of ILI. Field inspections use a variety of technologies ranging from mechanical measurements using depth gauges, rulers, and levels (measuring corrosion or deformation) to advanced measurement technologies using ultrasonic tools (measuring potential cracking) or laser measurements (measuring corrosion or deformation). Other techniques such as magnetic particle, liquid penetrant, and radiographic tools are used to identify cracking or material inhomogeneities and are very similar to those technologies used for pressure vessel inspection in other industries. As most of these measurements are performed manually, the technicians and technologists performing the inspections are highly trained to ensure accuracy and repeatability of the results.[7]

A summary of commonly used inspection technologies and their primary use cases is provided in Table 4-3, including emerging technologies that are currently being adopted into many operator's integrity programs. It should be noted that many of these technologies are being adapted for various use cases (such as characterization of material properties[8]), inspection locations, and product type (media). These technologies are offered by multiple vendors with variations in how the technologies are implemented within the tools, tool performance specifications, and available use cases.

Industry has decades of experience conducting integrity inspections, and as technologies continue to advance, there are opportunities for additional improvements in the inspection tools. Until recently, inspections were limited to pipeline segments that had favorable characteristics for in-line inspection tools. Lines that could not accommodate these tools were referred to as unpiggable. In-line inspection tool vendors are developing many new technologies to help alleviate difficult and costly pipe modifications that would facilitate pipeline inspections.[9] These enhancements will help to ensure efficient project execution is coupled with high-quality data to guarantee effective tool performance and to ensure accurate data that supports integrity decision-making.

7 Refer to the Pipeline Construction and Maintenance section (II.D) for additional information on nondestructive examination.

8 MacKenzie, R., Sen, M., MacKenzie, B., and Moran, S. (2019). *Use of Inspection Technology to Characterize Material Properties.* Topic Paper 4-6. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

9 Paonessa, S., and MacKenzie, B. (2019). *Challenges for In-Line Inspection.* Topic Paper 4-2. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

Technology	Inspection Location	Medium	Primary Use
Electromagnetic acoustic	In-line (emerging)	Gas & Liquid	Cracking
Phased array ultrasonic	In-line (emerging) & Field	Gas & Liquid	Cracking
Compression wave ultrasonic	In-line & Field	Liquid	Metal loss
Shear wave ultrasonic	In-line & Field	Liquid	Cracking
Caliper	In-line	Gas & Liquid	Deformation
Inertial	In-line	Gas & Liquid	Strain, pipe locations
Magnetic flux leakage	In-line	Gas & Liquid	Metal loss
Eddy current	Field	Gas & Liquid	Cracking
Laser mapping	Field	Gas & Liquid	External corrosion, deformation
Liquid penetrant	Field	Gas & Liquid	Cracking
Magnetic particle	Field	Gas & Liquid	Cracking
Mechanical measurements	Field	Gas & Liquid	External corrosion, deformation
Radiographic	Field	Gas & Liquid	Internal corrosion, weld inspections

Table 4-3. *Summary of Inspection Technologies*

The accurate detection of features by in-line inspection tools can be particularly challenging. Crack detection and sizing poses technical challenges that are exacerbated by varying specifications across inspection tool vendors and by pipeline characteristics. Characteristics of the pipe and the identified features affect the tool's probability of correctly identifying and sizing the feature. These challenges can be addressed through a combination of technology enhancements, use of multiple technologies for inspection and verification, and incorporation of uncertainties in the analysis, either deterministically or through use of a risk-based or probabilistic approach. Crack tool technology for in-line inspection is rapidly improving and operators are embracing these technologies for crack management, either exclusively or in combination with hydrostatic test and direct assessment. The industry continues to make improvements in the detection and sizing of defects that threaten integrity. Additional developments would benefit from more sharing of learnings between the inspection technology service companies (ILI and data interpretation vendors) and the pipeline operating industry.

Gas pipeline operators also continue to innovate and deploy new technology to manage cracks. Typically, gas pipelines have used hydrostatic testing and direct assessment to inspect for cracks. Ultrasonic tools are designed for crack detection, but they require a couplant (liquid interface between the sensor and the internal pipe wall) that is not present in gas pipelines and therefore this technology is not currently utilized. Industry innovation has led to the development of electromagnetic acoustic transducer (EMAT) technology that can detect cracking without the use of a couplant. While EMAT has been deployed in other industries, a few gas pipeline industry operators have begun using this technology, and the liquid pipeline industry has conducted a few isolated tests of this technology. Continued development of effective crack inspections may allow for a decreased reliance on hydrostatic tests to prove the safety of gas pipelines.

As shown in Figure 4-6, approximately 25% of barrels released result from corrosion failures. While corrosion management has well-established technologies, assessment protocols, and regulations, enhancement opportunities exist and there is significant ongoing research to further improve measurement and assessment accuracy. Some of the topics of interest include improving in-line inspection capabilities for detecting very small

diameter pinhole corrosion, assessment techniques for threat integration involving corrosion (such as corrosion under high strain conditions), quantification of tool performance especially related to internal corrosion and manufacturing defects, and understanding of temperature severity when evaluating corrosion growth rates. Many additional areas of technological enhancement in the corrosion management area relate to improvements in preventive measures such as coatings, cathodic protection, and corrosion inhibitors. The continuous improvement of corrosion integrity technologies will help to bolster preventive and predictive methods to increase safety while maximizing the effectiveness and efficiency of integrity programs.

In some cases, tool performance specifications can be misleading, and caution should be taken when trying to understand tool accuracy, especially in unique or nonconventional inspection situations. Poor tool performance will produce poor data, which can have a significant impact on the accuracy of engineering assessment and associated asset integrity decision-making. There are many specialized in-line inspection tools available that have been specifically designed for use in nonconventional inspections, but not all of them are able to meet the detection and sizing accuracy expectations. For these nonconventional applications, there has been limited deployment that makes it difficult to fully validate and optimize detection and sizing algorithms, which could lead to tools performance falling below specifications normally obtained. Many operators find it difficult to validate tool performance and deciding if a new tool will provide sufficient accuracy to be included in their inspection arsenal. These concerns could likely be mitigated through collaboration among operators, sharing performance and validation information from new tools to quicken the optimization of the tool algorithms, and the eventual adoption of the tools into the market. This collaboration could help support technological advancement, which would provide benefit to operators, tool vendors, and ultimately the public.

EMAT, phased array ultrasonic sensors, and pitch-catch ultrasonic sensors are examples of emerging technologies where such collaboration could be helpful.

Many of the in-line inspection technologies available to the pipeline industry collect large amounts of data that are processed and interpreted to allow for engineering assessment to occur. As inspection technologies advance and have become more prevalent in the industry, the amount of data collected has increased dramatically. The results of each in-line inspection are analyzed using complex anomaly detection and sizing software and results are verified and further enhanced by skilled analysts. The processing time for complex ILI can be months long and industry is working to further enhance algorithms and increase automation of the processes. Once processed and validated, data from multiple inspections can be integrated to help provide a better understanding of the pipeline and identify areas where multiple threats may be combining their effects on pipeline integrity.[10]

Finding: Many of the in-line inspection technologies available to the pipeline industry collect large amounts of data that must be processed and interpreted. Currently, operating companies, working with their ILI supplier, do this validation and interpretation individually. With better collaboration between and among industry operators and ILI tool suppliers, the accuracy and validation cycle time could be accelerated.

Some of the data challenges could be simplified through data standardization efforts in the industry, which would simplify analysis and allow for improved data sharing. Future enhancements through leveraging advanced software technologies (such as machine learning and big data techniques) could further help to improve the speed and costs associated with handling inspection data and developing new approaches, which may bring in a new understanding of the data to support assessment.

3. Enhancing Regulator and Industry Collaboration

The development of technology is not the only required area of innovation for industry

10 Heaney, D., MacKenzie, B., and Bubenik, T. (2019). *Use of Data Integration to Support Integrity Assessment*. Topic Paper 4-7. Washington, DC: National Petroleum Council. See list of topic papers in Appendix C.

advancement, as regulatory and societal challenges can pose difficulties for pipeline operations as challenging as technological ones. Regulators protect public interest by ensuring that standards are met but structurally can struggle with incorporating technological advancements into their established frameworks. Societal pressures hold the industry to their commitments to maintaining public safety and protecting the environment but concerned individuals do not always possess the means required to understand the full asset integrity framework used within the industry (due either to the technical complexity or the sheer quantity of technological advancements), and this can be a barrier to trusting that their interests are protected. These barriers can delay the implementation of technological advancements designed to yield benefits to both the industry and society in general. Different groups within the industry also have different priorities and focus areas. However, collaboration among the groups can help to speed the overall enhancement of technology and safety through new technology.

a. Regulatory Pathways

While pathways for utilizing new technology are generally neither defined nor prescribed, there are opportunities for pipeline operators to implement new technologies. Regulators have been accepting of trial implementation of new inspection methods (for example, when operators have clearly identified these in advance and have met all requirements from the regulating agency). Some of the regulatory acceptance processes for new technology deployment could be enhanced including technological implementation, special permits, and intellectual technology.

Technologies for inspecting liquids pipelines are rapidly improving. Since the early 2000s when PHMSA issued its pipeline integrity management regulations, several generations of in-line inspection smart pigs have harnessed multiple ways to use magnetic resonance, ultrasonic waves, and electromagnetic acoustics to find ever smaller defects in pipes. Research and development projects have confirmed in-line inspection capabilities with field-observed conditions. Analytical modeling improvements allow engineers to predict the maintenance needs of pipelines with increasing certainty. However, existing regulations have not kept up with rapid technology advancements, and the core pipeline repair criteria have not been thoroughly updated in more than 15 years. A collaborative effort is underway between industry and PHMSA to propose regulatory updates. Timing of those changes is still uncertain.

For example, ILI repair criteria for dents are fully prescriptive, not allowing operators to consider factors such as pressure cycling, age of the dent, and other uncertainties associated with in-line inspections that would allow operators to more effectively prioritize mitigation to maximize risk reduction.

Finding: A subset of prescriptive requirements within PHMSA regulations have limited industry's ability to accommodate risk-based assessments which, if incorporated, would allow companies to improve resource allocation and speed adoption of technology.

PHMSA regulations provide an avenue to implement alternate technology and this has been used by some operators. Through these regulations, an operator is able to leverage another technology that the operator can demonstrate will provide an equivalent understanding of pipeline condition, provided sufficient notice is provided to PHMSA prior to execution of the assessment. However, this program has limited ability to enable ongoing technology development as the clauses are limited to alternate technologies, which are required to achieve an equivalent level of performance as the approved technologies with the same prescriptive response requirements that an operator must undertake. The use of the alternative technologies approach is also administratively intensive for the operators and PHMSA as it requires each use case to be individually approved, even if a group of operators is intending to trial test the same technology.

PHMSA provides a special permit process through which operators may apply technology advancements and best practices. This process can be complicated, and operators may have difficulty preparing successful applications to use new technologies due to the uncertainties of

the expected results from the technologies and in the associated regulatory expectations. For the special permit approach to be a viable tool for improving the speed of regulatory adoption of new technologies, the process needs to have a core uniformity of structure with defined expectations. A new guideline that clearly addresses the industry requirements for special permit applications would help these permits be a more effective tool for the industry and could accelerate adoption of recent technology advancements.

PHMSA and other regulators should clarify regulatory expectations for field testing of new technologies that could help to reduce an operator's risks associated with implementation. A regulatory guideline that could outline how an operator may conduct trials of new technologies between required reinspection intervals, in advance of regulatory deadlines, would be valuable. Without this clarification, operating companies may be reluctant to perform trial tests of new technologies that augment their existing programs out of concern that it could result in a significant amount of unnecessary field work from unreliable data or compliance exposure. This overall hinderance can slow industry-wide testing and implementation of new technologies.

Finding: Certain prescriptive requirements within existing PHMSA regulations discourage field testing of new inspection technologies where the performance, accuracy, and repeatability of a technology is not yet proven. This issue can add significant costs to address regulatory requirements associated with conducting trial runs and thereby can slow the adoption of new technology.

b. Industry Collaboration on Safety

Technology development is typically focused on connecting what needs to be solved with the community of vendors, entrepreneurs, and academics who can drive toward solutions. This process can vary significantly in the time required to develop ideas and, in the costs required to pursue them, but coordinated efforts help to maximize the speed and efficiency of developing the most critical technologies. Collaborative programs allow their results to be easily shared among different industry stakeholder groups to raise the capabilities of the industry, thus lowering overall incident rates and enhancing social acceptance. These benefits have been shown to deliver industry-changing technologies and assessment techniques.

The industry is committed to continuous improvements that reduce risks to public safety and the environment. As current technologies still have limitations under certain conditions, additional focused investment and commitment from industry on advancing new technologies is important. Similarly, new processes that enhance the analysis and interpretation of data from technologies support improved decision-making and overall risk reduction. Developing improved industry frameworks to share data could help to drive the capability to develop and test these critical technologies and assessment methods. Implementing programs to help foster collaboration among various industry groups would help to ensure that the most critical industry-wide problems and associated technology development are being pursued, while focused efforts and pooling of resources will help to expedite the research and development process.

Finding: Additional participation and investment in joint industry projects could improve prioritization and speed development and deployment of new and promising technologies that address industry-wide challenges, such as those related to corrosion, cracking, and material pipe/weld failures.

The NPC recommends that industry, working with PHMSA and ILI technology providers, should develop a collaborative pathway to support the testing and validation of new inspection technologies that can lead to acceptance into approved integrity management requirements.

C. Pipeline Operations Integrity

1. Operations Integrity Overview

Operations integrity is the combination of people, processes, and tools that enable effective

threat management to ensure pipeline reliability. Technology is critical to proactively identify threats and either prevent or mitigate impacts. For pipeline assets, key operations integrity issues are associated with geohazards (i.e., natural force damage) and encroachment of right-of-way (i.e., line strike during excavation). These two areas are of focus since they contribute to one-third of the volume of liquid pipeline releases (Figure 4-5), as well as roughly one-third of all natural gas pipeline incidents (Figure 4-7). Overall pipeline incident rates are on a gradual decline (Figure 4-11), although they still occur, and rapid leak detection is imperative to mitigate impact to public safety and the environment.

Mature technologies exist that support surveillance activities for geohazard and encroachment threats, as well as effective leak detection programs. Currently these are specific to individual use cases, although more versatile technologies are evolving that offer the potential to support a range of operations integrity issues. This section addresses key technologies, outlining the advantages and disadvantages of each with recommendations for further research and development.

a. Technology Focus Areas

The past decade has been marked by a significant acceleration of new technologies into the research and development landscape to support operations integrity. Two key areas of technology development that have the potential for versatile application across multiple use cases are remote sensing and linear monitoring systems. The hardware associated with these technologies is in large part proven. More of the challenge is with validating sophisticated algorithms required to analyze the significant volumes of data produced and with translating this data into an operations context. The algorithms are used to facilitate rapid data-to-knowledge capability with a high degree of confidence to identify threats in real-time that would trigger response by an operator. While the two emerging areas of remote sensing and linear monitoring systems are both equally meaningful for development, a key differentiator between the two that may drive priority is the ability to retrofit existing assets. Remote sensing does not have the retrofit challenge, unlike linear monitoring systems. Retrofit capability is a major consideration given the large base of installed infrastructure that exists.

Beyond hardware-based technology (e.g., sensors), an area of development that is often not of focus but equally valuable is information technology that enables common sharing of data. This collaboration would have the potential to evenly raise the effectiveness level of operations integrity programs across industry, as well as aid in emergency response. Pipeline infrastructure is in larger energy corridors where a wealth of data exists that is associated with individual operator surveillance activities of pipeline rights-of-way. In addition, agencies at the local, state, and federal level generate data of value for operations integrity management of energy infrastructure, such as geohazard monitoring. Considering that this type of data is safety and environmental related, it is not an arena for competition; collaboration should be encouraged, particularly in high-consequence areas.

The following three technology sections will provide specific recommendations for additional high priority research and development. Two key themes cut across that merit highlighting, specifically data analytics and technology validation. The magnitude of data tied to operations integrity technologies is significant (i.e., terabyte levels). Access to tools that manage and expedite analysis of this information is key to innovation. Alignment on validation is an equal area of focus to ensure expedient technology deployment. Validation opportunities include standardizing test protocols, aligning on performance criterion, and providing real-world testing infrastructure. Data analytics and technology validation are opportunities for government and industry collaboration.

b. Deployment Challenges

Penetration of new technologies into the commercial market in support of operations integrity has occurred at a slower rate than the flow of concepts to the research space. This is in part due to the long fuse required to mature such critical technologies into reliable and robust solutions. Technology challenges stem from the requirement to handle changes in physical properties ranging

from contact with hydrocarbons, to the detection of unique acoustic signatures in a noisy environment, to actual ground movement resulting from geological changes. The validation of monitoring technologies is not straightforward. Validation can be done in a laboratory or other controlled setting, but those conditions will always differ from an actual field environment that is challenged by varying operational and environmental conditions. Finally, many monitoring modalities require retrofitting a pipeline with sensors, and such complicated installation on or in the vicinity of a pressurized pipe does not always have an obvious technical solution. These technology challenges can be overcome, in part, through the build-out of significant testing infrastructure to support a wide variety of technology form factors. The designs of these test sites should consider how to map results from such field-like surrogates to actual operating pipeline cases. This approach directly ties into the pilot program recommendation in the Industry and Government Research section (I.D).

Market challenges also arise from the fact that many innovations in this space are from relatively small technology development firms that do not have the resources to quickly drive their concepts through the range of technology readiness levels. These companies may not have portfolio diversity to subsidize one product through the sale of others and instead must quickly move new technologies to market. This poses a challenge because the pipeline industry is cautious to avoid rapidly deploying technologies without first proving out the technology in a variety of scenarios. This development and testing can be quite expensive for small companies and is often done without any commitment of purchases upon completion of a validation program. This difficulty is compounded by a lack of standardization of novel sensing technologies, so the validation performed to meet the requirements of one operator might not be applicable to another. These market challenges can be overcome by significant investments in promising technologies that are in earlier stages of readiness to drive them to late stage development including field testing and validation. This shortens the remaining challenges for full commercial adoption. An example model would be to create a program similar to the ARPA-E, but with a focus on technologies that improve pipeline infrastructure safety.

2. Leak Detection Technologies

Pipeline integrity inspection programs (refer to the Pipeline Asset Integrity section, II.B) are the primary method across industry for ensuring safe operations. For liquid pipelines in particular, rapid leak detection capability is important as a second layer of protection to mitigate public domain impacts should an incident occur. Leak detection can be achieved by technologies that operate inside or outside the pipe on either a continuous or intermittent basis. The most common approach is the combined use of computational pipeline monitoring (CPM) to supplement supervisory control and data acquisition. This technology provides continuous monitoring to certain levels of sensitivity. Detection of leaks with a very slow rate of release below the limits of CPM is an area of opportunity for additional research and development. Newer continuous leak detection systems are evolving that offer benefits versus the current conventional approaches. These are referred to as external linear monitoring systems and involve sensors placed outside the pipe along the installed length. Examples include fiber-optic strands, hydrocarbon detection cables, and hybrid discrete sensor systems. The four dimensions of leak detection performance are listed in the text box below.

LEAK DETECTION PERFORMANCE DIMENSIONS

Sensitivity: Size of leak detectable and time required for alert.

Accuracy: Validity of leak parameter estimates, such as leak location, volume, etc.

Reliability: Probability of correctly or incorrectly declaring a leak, i.e., false call rate.

Robustness: Ability to function under changing operating conditions.

No single method today provides a comprehensive solution to leak detection, with an increase in one performance dimension often made at

	Continuous Leak Detection			Intermittent Leak Detection			
Release Rate	Supervisory Control Monitoring (SCADA)	Computational Pipeline Monitoring	External Linear Monitoring Systems	Acoustic Monitoring	Visual Surveillance	Remote Sensing	Public Notification
Rupture				Not a Primary Method for Rupture Detection			
Leak							
Pinhole	Not a Primary Method for Pinhole Detection						

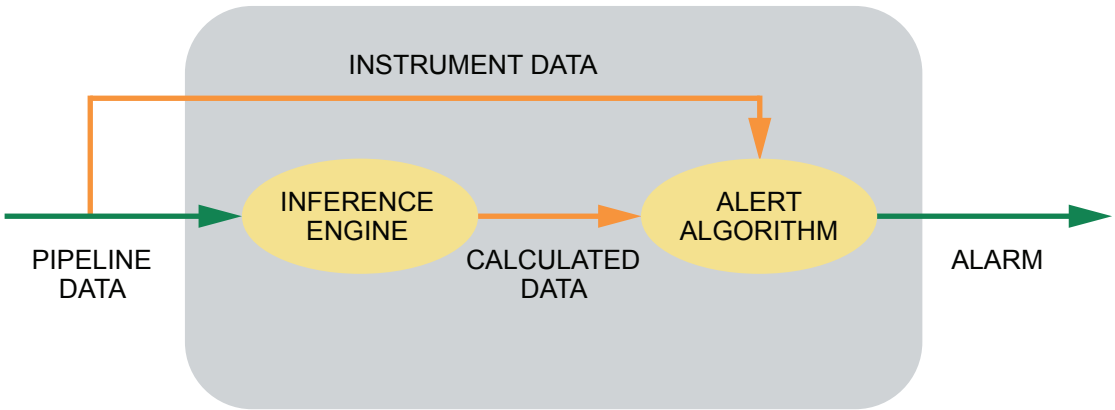
Leak detectability: Probable Possible

Figure 4-12. *Technology Comparison for Key Performance Dimension.*

the expense of another (i.e., higher sensitivity decreases reliability or increases false call rate). As a result, effective systems benefit from integration of multiple approaches, such as the targeted use of more sensitive technologies in high-consequence areas. Technologies are often complementary and can be used in combination to improve overall performance, as illustrated in Figure 4-12.

Finding: Robust and effective leak detection capabilities exist today. Additional detection of the smallest release rates may be improved by validating newer linear monitoring systems and integrating them with other mature technologies.

Computational pipeline monitoring is a continuous internal leak detection system that is deployed with supporting field instrumentation and communications infrastructure to capture flowrates, pressures, and/or temperatures (Figure 4-13). It leverages computing algorithms to infer the potential for a leak and integrates the real-time assessment into operating alarm systems. CPM methods include statistical analysis, volumetric and mass line balancing, pressure and flow monitoring, real-time transient modeling (RTTM), and negative pressure wave detection. Of these, RTTM is the most sophisticated, involving a detailed mathematical model that solves fluid mechanical equations of mass, motion, and energy in real time.



Source: American Petroleum Institute, API Recommended Practice 1130, Appendix B, 1st Edition, September 2007, Reaffirmed April 2012.

Figure 4-13. *Example of a Computational Pipeline Monitoring System*

CPM technology deployment across industry is mixed, influenced by operating restrictions and requirements for technical expertise. Operating limitations stem from technical complexity associated with handling multiphase flow, transient operations, shut-in conditions, and unreliability of data input from field instrumentation or network communications systems. These can lead to false alarms, which result in a general practice of troubleshooting most CPM notifications by an operator before initiating a response in the field. Ongoing tuning of CPM algorithms is required, and given intricacies of the systems, especially RTTM-based algorithms, this maintenance requires highly qualified individuals. Development and sustainment of these skillsets is a challenge. CPM technologies are the most mature leak detection systems now used, although advancement opportunities would be beneficial. Potential opportunities recommended for further advancement include use of machine learning and artificial intelligence.

Acoustic inspection is an intermittent internal leak detection technology designed to detect very small leaks that are outside of the detectability of traditional CPM systems. It involves acoustic sensors housed in a device that is launched periodically via the same access points used for pig inspections. The device directly measures acoustics as it traverses through a pipeline and records measurements on a data acquisition system for postprocessing analysis.

It is possible to identify a leak location with a high degree of confidence using acoustic inspection, although it cannot estimate leak size. The most significant limitation on performance is timeliness of detection. Time delay depends on how frequently the technology is used, with a single run requiring from days to several weeks depending upon pipeline length. Acoustic inspection-based leak detection technology is offered by a limited number of technology providers. Acoustic inspection continues to be developed with an emphasis on expanded sensor capabilities, advancement of data analytics, and optimization of power requirements to extend pipeline run length.

Fiber-optic sensing is a continuous external linear monitoring system that utilizes a fiber strand. While a variety of physical measuring principles can be used, in general, laser light is sent into the strand and the scattered illumination is measured. This process is known as "interrogation" and effectively converts the fiber into an array of distributed sensors. The technology is highly sensitive to changes in temperature, vibration, and strain. Depending on the application, a fiber-optic system can be optimized for distributed temperature sensing (DTS), distributed acoustic sensing (DAS), distributed strain sensing (DSS), or a hybrid system that incorporates a mix of technologies.

Benefits of fiber-optic sensing include excellent event location determination and immunity to pipeline transients. DAS and DSS offer the added capabilities of detecting ground shifts (refer to section II.C.3, Geological Hazard Monitoring Technologies) and third-party interference. The most significant technical drawback is susceptibility to false alarms that are caused by events with similar signatures as a pipeline release, even when those events are unrelated to operations (i.e., vibrations from vehicular traffic). The probability of false leak alarms increases if the cable is placed away from the pipeline. This introduces challenges for use on existing underground pipelines since retrofit in crowded right-of-way corridors is difficult. These are more cost effective to install during new pipeline construction while the pipeline ditch is open. Installing cables on existing pipelines is much more challenging because of the difficulty of excavation near active pipelines and higher cost of installation.

Fiber-optic systems typically generate large volumes of data. As a result, installation is difficult in remote areas without broadband communications. Although running the systems remotely in autonomous or semi-autonomous mode is possible, a trained operations analyst is typically required to interpret the anomalous results in real time; the effectiveness of analytical interpretation algorithms needs improvement and is still under evaluation.

Hydrocarbon sensing cables (HSCs) are under development as an external linear monitoring system alternative to the more established fiber optics. HSCs detect changes in electrical parameters when contact is made with liquid hydrocarbons. The

sensing element is typically constructed by mixing inert conducting particles into a polymer substrate, which preferentially absorbs hydrocarbons and swells. The polymer sensor element is often protected by an outer jacket, which increases the robustness of the cable but can impede hydrocarbon absorption and lead to slower responses.

This technology has not achieved widespread adoption primarily due to slow response times and long-term maintenance issues. Detection is dependent on direct contact with escaping hydrocarbons and a leak can be missed altogether if it does not follow a favorable path relative to installation of the cable. Although some manufacturers claim abilities to locate the leak along the cable, HSCs are not yet optimized for accurately pinpointing leak location along the cable.

Hybrid discrete sensor cables (HDSCs) are external continuous leak detection systems also under development. These have the potential to provide power and communications to a network of electronic sensor nodes positioned along a cable. The sensor nodes have onboard microprocessors and can be outfitted with advanced sensing capabilities such as hydrocarbon sensing, vibration sensors, temperature sensors, or other sensors as needed. This flexibility allows HDSCs to offer a mix of capabilities currently only available as individual systems.

Advances in chemistry have enabled the development of a new generation of polymer absorption sensors that are able to reliably detect hydrocarbon gas migration underground. This permits HDSC placement at greater distance from the pipeline with only a potentially minor loss of sensitivity. In addition, HDSCs are relatively low power systems and do not require large data bandwidths. As such, HDSCs can be deployed in remote locations with limited power and communications. These characteristics make HDSCs a promising technology for rapid retrofit deployment in areas of elevated risk.

Table 4-4 compares key aspects of leak detection technologies.

The NPC recommends that industry, working through research consortiums, should pursue a pilot program as recommended to be established by PHMSA to advance linear monitoring systems (e.g., fiber optics, hydrocarbon detection cables, hybrid discrete sensor cables) that could provide additional leak detection capabilities.

	Continuous Real-Time Technologies				Intermittent Technology	
	CPM	Fiber Optic	HSC	HDSC	Acoustic	Remote Sensing*
Stage of Development	Mature	Emerging	Nascent	Nascent	Mature	Emerging
Typical Performance Parameters						
Sensitivity (lower limit of leak size detection)	Small	Pinhole	Pinhole	Pinhole	Pinhole	TBD
Location Accuracy (miles/yards)	Miles	Yards	Yards	Yards	Yards	TBD
Reliability (ability to minimize false calls)	Low	Low	Low	TBD	High	TBD
Robustness (tolerance to transient operations)	Low	High	High	High	High	High
Retrofit Capability of Existing Assets	Feasible	Difficult	Difficult	Difficult	Feasible	Feasible

* Covered in section II.C.4, Remote Sensing Technologies and Geospatial Analytics. Note: CPM = computational pipeline monitoring; HSC = hydrocarbon sensing cable; HDSC = hybrid discrete sensor cable; TBD = to be determined.

Table 4-4. *Comparison of Liquid Leak Detection Technologies*

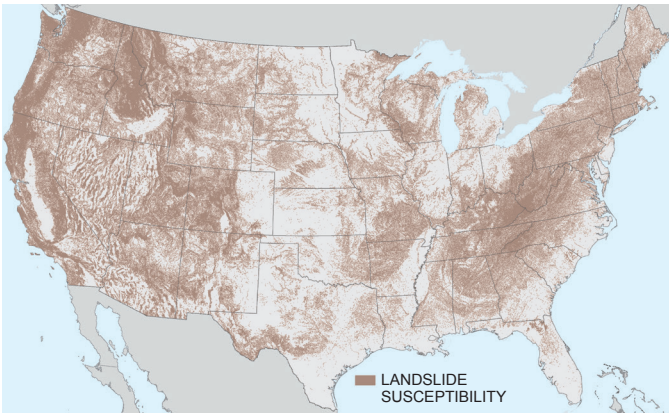
3. Geological Hazard Monitoring Technologies

The substantial U.S. energy infrastructure system covers a vast and diverse geologic landscape involving significant river crossings, fault crossings and seismic zones, landslides, and other natural subsidence hazards (i.e., karstic terrain, permafrost, sensitive soils). As noted in Figure 4-5 and Figure 4-6 of the Pipeline Industry Overview section, II.A, natural force damage accounts for 6% of the liquid pipeline incidents but a higher 12% of the total volume released. These statistics underscore the more impactful nature of geohazard events. An analysis of industry incidents over an extended timeframe indicate that geohazard pipeline failures are equally divided between those caused by earth movement and those resulting from hydrotechnical issues, such as river flooding (Figure 4-14). Releases at river crossings tend to be of higher consequence due to the potential to impact larger areas as material is carried downstream, in addition to the impact to drinking water, wildlife, and sensitive environmental assets. Geologic activity can be exacerbated by natural causes as well as human activities. Identifying and monitoring direct and indirect factors is critical to mitigating damage to energy infrastructure.

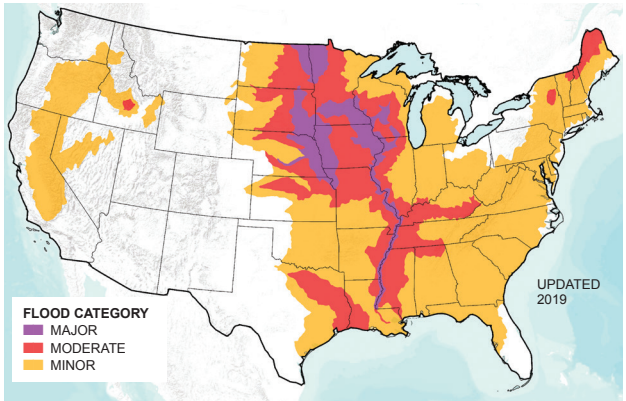
Geohazards are managed through an integrated, multiple technology approach, combined with desktop research. Key information leveraged as part of foundational research includes large-scale and local topographic information, geographic maps and reports, digital elevation model data, aerial photography, and precipitation and flow data reports. This type of data is in part proprietary, generated by individual operators. Some data is publicly available from government entities, although they are challenged for efficient consumption due to lack of centralization and uniform format. A common data set in higher consequence areas, together with the following technologies, would help to formulate engineering controls for monitoring and mitigation of geohazards. The technologies covered are not exhaustive but rather focused on those recommended for further development and deployment.

Finding: Desktop research continues as the foundational approach for geohazard management. A portion of the applicable data that is needed is publicly available but is not readily accessible from central repositories for consistent use across industry.

Light Detection and Ranging (LiDAR) is a high-resolution laser surveying technique that allows the ground surface to be approximated as it would appear with the overlying vegetation removed. It is a primary tool for identifying surficial expressions that have the potential to result in geologic hazards. Repeated surveys generate change data that can highlight movement of existing hazards as well as the formation of new ones.



Source: United States Geological Survey.



Source: Proceedings of the 2016 11th International Pipeline Conference, IPC2016-64085; National Oceanic and Atmospheric Administration.

Figure 4-14. *Maps showing Examples of Primary Types of Geohazards, Earth Movement, and Hydrotechnical Issues*

The widespread integration of LiDAR has been transformative for geologists, enabling identification of geohazard evidence that often is subtle or may be obscured by tree canopy. There are key challenges with the technology. For example, while LiDAR is mature with multiple service providers, the industry lacks uniform standards for use in the geohazard context. In addition, it is data intensive, which poses challenges with both timeliness of results as well as storage of data for run comparison.

Predictive models for geohazard management are built by using various inputs such as meteorological and geologic conditions, soil and flow parameters, peak ground acceleration, slope steepness, and vegetation. Models can be helpful for providing guidance on where to focus monitoring and mitigation efforts, particularly since geohazard areas are broad. Many hazards can be triggered by events occurring significant distances from infrastructure rights-of-way and over a variety of timeframes (e.g., sudden or across years). Support for the development of more accurate local/regional maps and predictive models would allow the industry to scale the level of risk and appropriately apply technologies. For example, a hydrotechnical predictive model could help determine river crossings that are likely to experience scour or channel migration. The use of predictive models in the pipeline industry has been limited due to data challenges. The models are only as valuable as their inputs, with accuracy requiring large volumes of data that can be difficult to manage. Development and public dissemination of reliable models would aid the industry in managing these types of issues.

Scour sensor technologies include those that enable tracking of adverse conditions of scour or erosion during flood events. The technology can take a variety of forms but is divided into two major categories: sensors mounted on the pipeline versus those placed in river channels or banks. Scour sensor technology is still under development for real-time monitoring of loss of cover that would enable timely operator intervention either with remediation or emergency response. Examples include the use of fiber-optic cables (refer to the Leak Detection section, II.C.2), hydrophones, and temperature sensors. Further research is required to prove these technologies and overcome the challenges of installation and maintenance. For example, hydrophones that leverage pipeline acoustic signatures are high-power devices that require sophisticated digital signal processing for data analysis.

Strain gauges are a series of point sensors that measure the internal stresses acting on a body, typically involving use of wire. Vibrating gauges use sensors to excite the wires and measure changes in frequency, whereas resistance gauges measure changes in electrical resistance as the wire deforms. Calibration factors are then used to convert either the frequency or resistance reads to strain levels. Strain gauge technology is relatively inexpensive and can be installed on existing pipeline infrastructure. Strain measurement is produced at single points, which requires gauge sets to be installed across an area of concern. The technology is durable and accurate, although accuracy is best when installed in a relatively stress-free state (i.e., at time of original construction). The technology can be set up for either automated or manual readings, which makes it useful for implementation in areas of slower moving geologic hazards that require long-term monitoring. Those with automated monitoring systems require significant maintenance for power source and communications equipment.

In-line inspection strain sensing is the analysis of inertial measurement unit (IMU) positioning data to identify bending that extends across one or more girth welds. It can be used to inform decisions on potential geohazard activity, but it is not a stand-alone technology. It does not provide tension or compression measurements, and the bending strain data it does provide could be driven by factors other than geohazard activity. In addition, ultimate strain capacity of pipelines is not well understood, making use of the data for mitigative action difficult. While IMU positioning can be expensive if run stand-alone, it is a relatively low-cost addition to planned in-line inspection runs and provides useful supplemental information.

The NPC recommends that DOE and DOT should work with FEMA, NOAA, USGS, or other relevant agencies to organize an

information sharing effort to increase collaboration on geohazard management among federal, state, and local agencies, and pipeline operators. This should drive use of consensus-based standards for storing data (e.g., Pipeline Open Data Standard or other similar standards) now used within the pipeline industry.

4. Remote Sensing Technologies and Geospatial Analytics

A smaller but emerging field of leak detection and geohazard monitoring techniques employs the use of remote sensing technologies (RSTs) and geospatial analytics (GAs). RSTs are in widespread use across private, public, academic, and government sectors. More recently, the application of RSTs and GAs within oil and natural gas has gained interest (see "Geospatial Analytics" text box). RSTs and GAs have two primary utilities for oil and natural gas monitoring. First, they detect surface changes, which are used to identify potential geohazards, and natural and anthropogenic encroachment risks. Secondly, they conduct analyses on electromagnetic radiation reflected from targeted surfaces. Targeted surface analyses may be used to detect chemical, physical, and biological characteristics that provide the information used to detect gas as well as liquid leaks.

Within these fields, the rapid growth of novel sensing platforms, such as unmanned aerial vehicles and nanosatellites, enable monitors to cover larger areas more cost effectively. RST and analytics sensitivity could be expanded using short-wave infrared radiometry deployed on high-altitude aircraft and satellites. The ability of short-wave infrared radiometry to accurately detect methane emissions via space-borne platforms would help industry develop steps to address and mitigate methane leaks on a broad scale.

RST-GA technologies enhance the ability to monitor geohazard and encroachment risks, detect leaks at earlier stages, and improve both the response time and response quality of mitigation. As an added advantage, the methods and scope of the data gathered through GA and RST integrates with the larger artificial intelligence, machine learning, and big data space to improve and expand predictive analysis in the future.

a. Overview

RST and GA are commercially available technologies that identify, alert, and quantify specific measurements, using noncontact sensors in conjunction with advanced analytics. RST-GA offers capabilities to detect liquid and gas (methane) leaks, to identify encroachment, and to monitor geohazards. The technology employs a passive approach that minimizes field activity, personnel, and resources. Comprehensive RST-GA applications can utilize one set of data to evaluate numerous operational areas and integrity threats. RST-GA tools can be used to support mapping and analysis, permitting and siting, emissions reductions, asset integrity, and emergency response.

RST sensors collect data obtained from electromagnetic energy reflected or emitted from a targeted surface. GA applies complex algorithms and analyses to sensor data to enrich the understanding of the surface's characteristics. Sensors may be located on ground-based (mobile or fixed), airborne, or space-borne platforms. Platform selection is application-specific and varies according to pipeline location and geographic distribution. RST-GA offers unique but complimentary monitoring and detection alternatives to in situ leak detection technologies. Figure 4-15 illustrates steps involved in RST-GA technologies.

Deployment and adoption of RST-GA is contingent primarily upon data cost, the operator's familiarity with the technology's applications, and validation of technologies. Data costs are contingent upon data age, data capture (tasked capture versus precapture), and data resolution (spatial, temporal, spectral). Data logistics and standardization—including computing platforms, continuity, delivery, sharing, display, and storage—are essential to the advancement and long-term adoption of RST-GA.

b. Remote Sensing

Remote sensors are well developed and widely deployed across scientific communities. Table 4-5 provides a list of key sensors currently available for encroachment, geohazards, and leak detection applications. Applications of sensors listed in Table 4-5 are discussed below.

GEOSPATIAL ANALYTICS

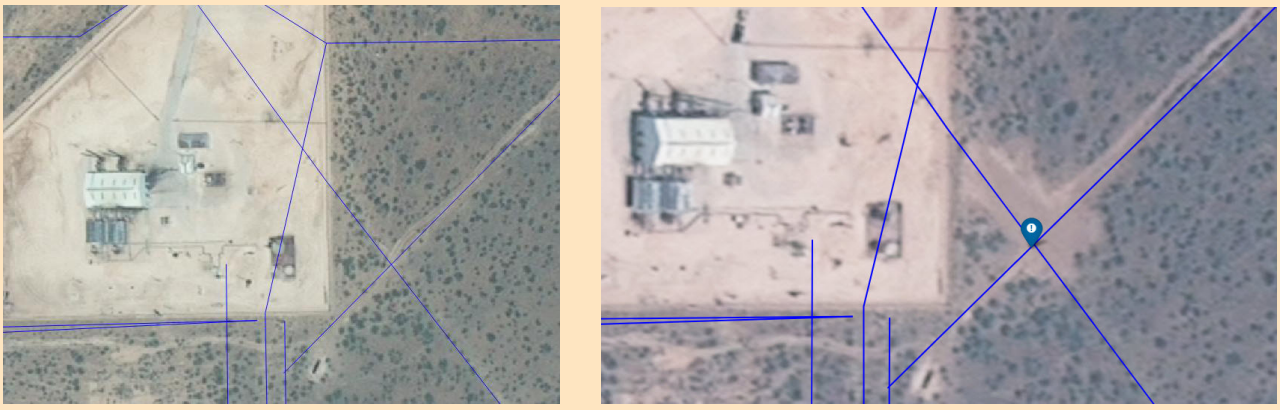
Geospatial analytics has helped advance satellite detection and short-term quantification of liquid and gas leaks where pervious ground surfaces exist. Determination of flux, however, still requires ground-level measurements and operational data although vendor-operator field experiments have reported success in determining short-term release rates.

Costs are directly proportional to resolution, bandwidth, and frequency of measurement and significantly increase if satellites are tasked to perform nonroutine data collection. Limited availability of commercial short-wave infrared radiometry data—currently one vendor and one satellite—makes methane monitoring essentially cost prohibitive.

Methane and Liquid Pipeline Leak Detection

Opportunities exist to help drive cost reductions. Several large commercial data vendors (Planet, Airbus, Digital Globe, etc.) who provide data imagery on request or through user interface platforms are seeking to expand their services. The oil and natural gas industry is a new market for commercial imagery providers who need to be informed on the enormous market potential for providing data solutions both within the oil and natural gas supply chain and across the energy and transportation sectors at large. Over the next few years, technology titans are planning to launch many low-cost nano- or cube-satellites, with a view to forming constellations across the globe. This new generation of satellites lowers the capital cost of the data platforms and delivers the opportunity for higher frequency measurements (daily to hourly), predictably driving the cost of data downwards. Leveraging the expansion of short-wave infrared radiometry sensors within these constellations offers tremendous opportunity for monitoring and mitigating methane leaks at higher frequency than current regulatory prescribed intervals.

Collaboration to acquire and share data solutions across common energy transmission corridors and within on-land industry transportation modes provides both knowledge-sharing and data cost reduction opportunities. The iPIPE consortium—one example of this type of collaboration—has been successful in bringing multiple operators together to fund research and deploy leak detection technologies. As iPIPE enters its third year of R&D, remote sensing technologies, primarily from satellites, have consistently demonstrated success.



Before (July 21, 2019) ***After (July 29, 2019)***

Source: Satelytics.

Example of Vegetation Change Indicating a Possible Leak

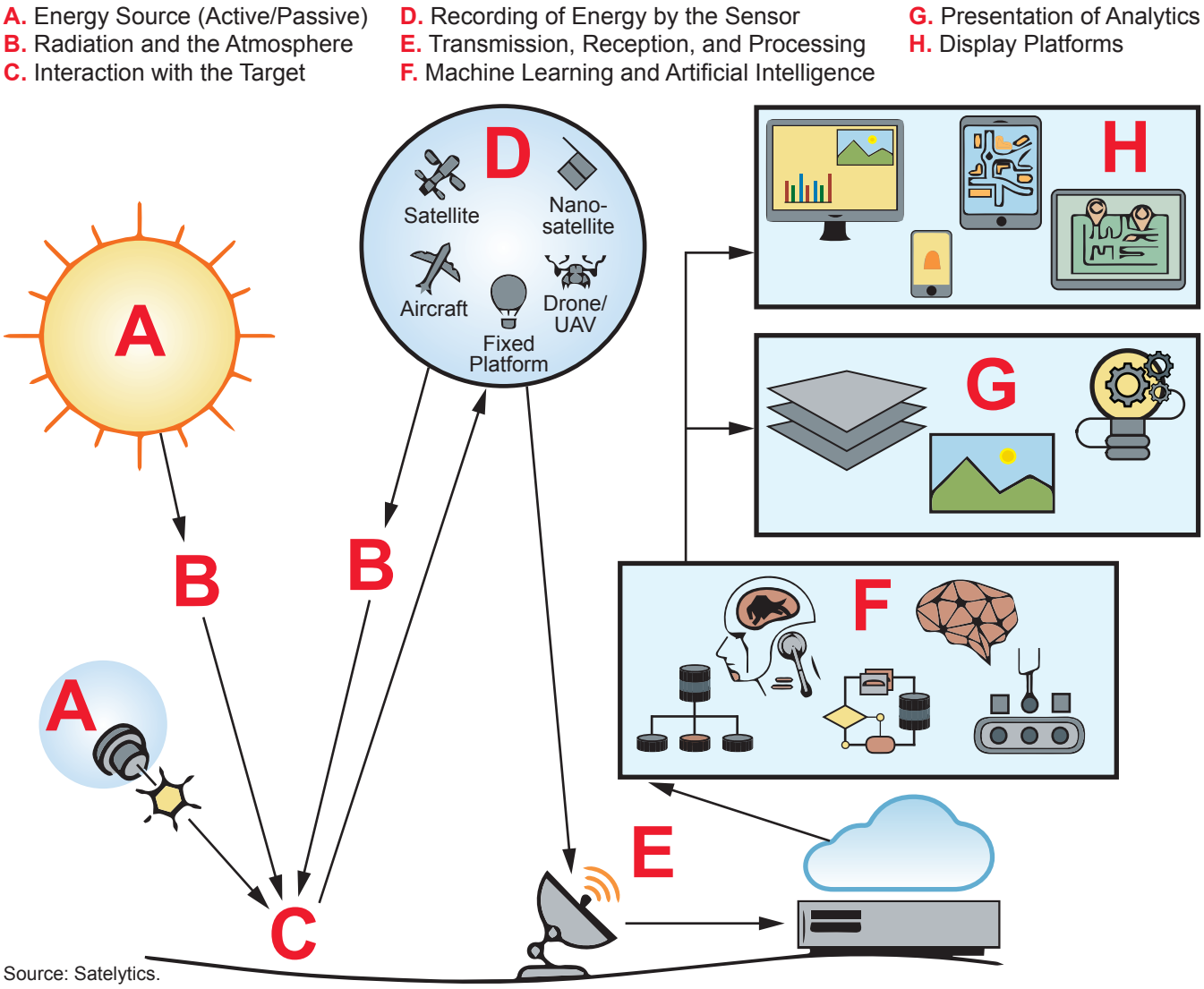


Figure 4-15. *Process Flow for Remote Sensing Technologies and Geospatial Analytics (RST-GA)*

ACTIVE SENSORS	PASSIVE SENSORS
• Light detection and ranging • Radio detection and ranging – Synthetic aperture radar – Interferometric synthetic aperture radar	• Radiometers and Spectrometers – Hyperspectral radiometer – Multispectral radiometer – Imaging radiometer

Table 4-5. *Key Sensors*

The electromagnetic radiation characteristics of active sensors allow them to penetrate atmospheric disturbance, whereas passive sensors are more susceptible to weather, cloud coverage, and other climatic interferences.

Encroachment. Active and passive sensing technologies utilize change detection analyses that can readily address encroachment risks. Their use has been widely adopted by utility companies for monitoring vegetation growth along utility corridors. Pipelines, although less exposed to vegetation risks, face other natural and anthropogenic risks (i.e., construction and maintenance activities,

urban development, agriculture, etc.). Currently, encroachment monitoring is handled primarily by field operations personnel as part of their daily routines. If broadly adopted and deployed, basic change detection RST applications could support, if not supplant, these activities by monitoring encroachment risks remotely.

Geohazards. Specific active sensors (i.e., LiDAR) and high-resolution passive sensors can detect subtle changes in the earth's surface. Over time, RST can monitor and detect natural (and anthropogenic) changes in water and land features and alert operations to potential geohazards for supplemental risk assessment. RST-GA can be targeted at critically sensitive areas and locations geohazards are known to exist (i.e., fault crossings, seismic zones, landslides, subsidence areas, etc.) to provide both early detection and analytical data in support of other geohazard monitoring techniques such as scour and strain sensing.

Liquid Leak Detection. RST-GA use both radiometry (measurement of the intensity of electromagnetic radiation) and spectrometry (analysis of the spectral content of electromagnetic radiation) for the detection of liquid leaks. Liquid leak detection employs a cross section of techniques that corroborate visible imagery changes with detailed analyses. RST-GA provide the ability for early detection of small leaks not likely detectable through conventional visual surveillance inspections. RST-GA may be tasked to target critically sensitive and high-consequence areas, particularly in remote areas where other technologies are difficult to deploy.

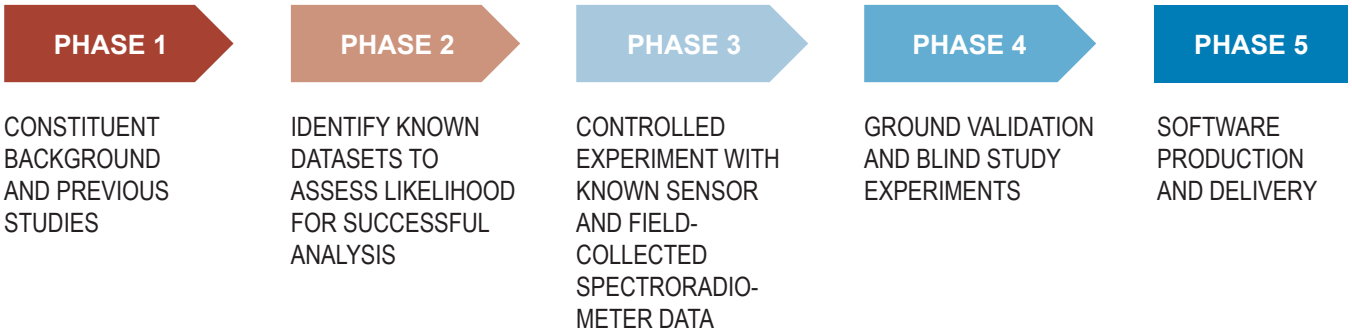
Methane and Natural Gas Leak Detection. A significant emerging area of application for RST-GA is its use in the detection of methane and natural gas leaks. Complex algorithms applied to hyper- and multispectral short-wave infrared radiometry and medium-wave infrared radiometry data can detect methane and natural gas, respectively. Medium-wave infrared radiometry data also provides the ability to perform basic constituent analyses of natural gas. RST-GA can detect gas leaks from both aboveground and buried pipelines.

c. Geospatial Analytics

RST data sets generate thousands of raw data points for evaluation. GA uses a series of techniques and algorithms developed specifically to evaluate these data sets. GA algorithm development proceeds through an iterative process of ground-truthing, updating, and operator collaboration (Figure 4-16).

The entire RST-GA cycle—acquisition of sensor data, application of analytics, and product delivery—requires massive data storage, computation, and operator interface solutions.

Finding: Currently no industry-wide standards exist to support consistency in design of data analytics software or data management solutions for reliable and cost-effective remote sensing applications.



Source: Satelytics.

Figure 4-16. *Phases of Geospatial Analytics Algorithm Development*

The NPC recommends that DOE, in cooperation with DOT and other relevant agencies, should organize an information sharing effort to assist with efficient acquisition and management of industry-specific geospatial data.

d. Applications by Platform

Ground-based platforms. RST may be deployed on fixed or mobile ground-based platforms. Mobile handheld optical gas imaging cameras are common and are prescribed by well-developed regulations (i.e., 40 CFR 60, Subparts OOOO & OOOOa, BLM Venting and Flaring Rule, and Colorado Regulation 7). Fixed sensors are more suitable for asset-level monitoring and less suitable along extended pipeline runs. Certain high-consequence or high-risk sections of pipelines lend themselves to fixed RST-GA, particularly where linear detection technologies previously discussed are not feasible or as cost effective.

Airborne platforms. RST airborne platforms are widespread and offer versatility for numerous monitoring and surveillance applications. Use of unmanned aerial vehicles (UAVs) deploying advanced sensors is also becoming more common in the industry. Operators are collaborating independently with vendors to advance pipeline mechanical integrity and leak programs by deploying UAVs equipped with sensor and video technologies. Currently, UAV platforms are restricted to a line-of-sight geographical area, limiting their deployment.

Space-borne platforms. Fixed-wing and satellite RST platforms currently support hundreds of applications for military, environmental and natural resources, insurance, tax assessments, infrastructure mapping, human activities, etc. Smaller, more cost-effective space-borne platforms (i.e., nano- and cube-satellites) and industry-specific applications are rapidly emerging.

Finding: The pipeline industry has not widely adopted space-borne remote sensing technologies because of the limited availability and selection of appropriate sensors, delayed frequency of data collection, and high costs of data acquisition. Field-level validation of sensors and analytical methods are necessary to advance their acceptance and use in integrity management programs.

Table 4-6 shows advantages and disadvantages of the various platforms.

The NPC recommends that DOE should work with industry to sponsor R&D programs to promote collaboration among data vendors (existing and emerging), operators, and government that can bolster regulatory and industry confidence and acceptance of RST-GA solutions to expedite the adoption and deployment of the technologies, and leverage improvements in data accessibility and costs.

D. Pipeline Construction and Maintenance

1. Construction and Maintenance Overview

Pipeline construction and maintenance focuses on technology advancements related to the materials, fabrication, installation, and maintenance and repair practices for long-term integrity of new and existing assets. Oil and natural gas pipeline design, construction, and maintenance methods have benefited from numerous generations of technology improvements related to pipeline materials, coatings, fabrication, construction methods, and protection methods. These technological developments have improved the integrity of the assets, improved cost efficiency, and allowed the industry to extend the life of the existing asset base. This is achieved through a cycle of continuous improvement over the life of the asset. For instance, when pipeline operators adopt new manufacturing and maintenance practices, they often discover new opportunities for further technological development based on actual field performance.

Incident statistics from 2014 to 2018, as noted earlier in this report, indicate that the leading causes of both liquids and natural gas pipeline incidents are related to construction and maintenance

Platforms	Advantages	Disadvantages
• Ground-Based • Mobile • Fixed	• Detection of small leaks in real time or on as-needed basis • Optical gas imaging cameras are ubiquitous • Methane emission monitoring • Improved maintenance, inspection, and safety programs	• Require resources and personnel in proximity to the targeted area • Require maintenance, repair and calibration of multiple sensors, as well as power supply management for remote and expansive pipeline segments
• Airborne • Manned fixed-wing and rotary • Unmanned aerial vehicles (UAVs)	• Versatility of deployment • Improved maintenance, inspection, and safety programs	• UAVs are currently limited to line of sight • May create concerns for nearby public stakeholders
• Space-Borne • High-Altitude Planes • Satellite	• Comprehensive monitoring - Analytics applied to one set of data across various integrity threats • Passive solution, allowing monitoring of assets while reducing on-the-ground impacts to the public and operators (minimizes field activities, personnel risks, and resources) • Platforms offer remote surveillance capabilities over vast coverage areas	• Rely on the availability of an appropriate sensor for the application • Somewhat limited by cloud cover and other climatic challenges • Short-wave infrared and mid-wave infrared data is currently cost prohibitive due to a limited number of platforms and current sole-source provider • Cost of high-resolution multi/hyperspectral data

Table 4-6. *Platform Advantages and Disadvantages*

and involve corrosion, excavation incidents, and pipe material and weld failures. These are priority areas of focus for industry technology advancement and deployment. The industry deploys pipeline construction and maintenance technologies to address incident causal factors, with the industry striving toward a goal of eliminating incidents (Table 4-7).

2. Prevention of Pipeline Corrosion Failures

Most pipelines are made of steel, which is subject to various types of corrosion based on environmental factors in and around the pipe. Corrosion is a natural process that is difficult to completely stop but can be controlled to a very low level to extend the asset life of the nation's oil and gas infrastructure.[11]

Internal corrosion can be minimized by controlling the corrosiveness of the gases or fluids transported in the pipeline. This is accomplished by either removing the corrosive constituents from the transported products (such as dehydration of natural gas) or by injecting into the pipeline specialized chemicals (called inhibitors) to prevent the corrosive constituents from causing corrosion. In addition, specialized corrosion monitoring practices, such as corrosion coupons or corrosion probes, can be used to monitor the corrosiveness of the environment inside the pipeline and help assure that treatments and preventive measures are effective. Pipeline operators continuously support research into more effective methods of removing corrosive components from transported products and into more effective treatment chemicals to minimize corrosion.

External corrosion can be minimized through a combination of effective coatings (essentially removing the ability of the corrosive environment to contact the pipe) and cathodic protection. No

11 The Pipeline Asset Integrity section (II.B) details how in-line inspection is used to combat corrosion leaks.

Corrosion Failures	Pipe Material/Weld Failures	Excavation Incidents
• Application of high-performance coatings (protective, damage resistant, highly durable) • Installation practices to minimize coating damage • Early detection of potential corrosion issues • Early detection and monitoring of corrosion to allow repairs before significant damage occurs (asset integrity focus)	• Improved control and application of high-strength pipeline steel • Improved welding practices • Improved field inspection technologies • Rigorous training and qualification programs for inspection, construction, and maintenance personnel on new technology applications • Improved assurance of long-term pipeline repair integrity	• 811 Program enhancement (Call Before You Dig programs) • Improved location/ mapping of aboveground and underground utilities • Advanced sensors and early warning systems for excavators and horizontal directional drilling equipment

Table 4-7. *Technology Improvements to Address Primary Causes of Significant Pipeline Incidents*

coating is ever 100% perfect, and coatings may also degrade over time and with exposure to the environment. To provide added protection against corrosion, cathodic protection[12] is employed as a complementary approach to minimizing pipeline external corrosion. Because coatings can be damaged and will degrade over time, the importance of cathodic protection to minimize the corrosion increases over time.

Various coatings have been tried throughout the history of pipelines, with differing results as to protectiveness against corrosion and effective life of the coating. The pipeline industry and coating manufacturers continuously conduct research to develop more effective, damage-resistant, longer-life coatings.

The NPC recommends that the DOE, working with PHMSA, industry research organizations, and coating manufacturers, should support research and development on new pipeline and repair coating systems that are highly durable and damage resistant during construction and remain so throughout the expected life of a pipeline with minimal need for other protective measures.

12 Reduction or elimination of corrosion by making the metal a cathode by means of an impressed DC current or attachment to a sacrificial anode (usually magnesium, aluminum, or zinc) (L.S. Van Delinder, ed. [1984]. Corrosion Basics, An Introduction, Houston, TX: NACE, p. 14).

3. Improvements to High-Strength Steels and Welding to Reduce Material Pipe/ Weld Failures

Conventionally manufactured pipelines get stronger as the carbon content increases. Increased carbon can also result in increased susceptibility to cracking. To address this, the industry worked with pipe mills and manufacturers to develop new, higher-strength steel pipe using a process called thermo-mechanically controlled processing (TMCP). TMCP involves very high heats (approximately 1,200°C) for the initial phase of the work, which is similar to conventional, higher carbon steel. Then, during the final hot work portion, temperatures are reduced to 775°C. During this phase, heavy equipment is used to roll the pipe at temperatures lower than conventional pipe manufacturing processes. TMCP results in finer grain size in the steel and higher-strength material than conventional steel of the same alloy content.

Conventionally manufactured steel pipe achieves the needed strength mainly through carbon content, but higher carbon content leads to more brittle steel properties with lower resistance to cracking. TMCP allows the pipes to achieve the strength via manufacturing process with a lower carbon content and better resistance to cracking. Thus, TMCP enables production of higher-strength pipes than conventional manufacturing techniques. This means that pipelines can contain more pressure and allow higher throughput

without increasing the wall thickness as would be necessary with lower-strength steels. The thinner pipe means less total tonnage of steel, and less cost per foot, than would be needed to build the same pipeline with lower-strength steel pipe.

Finding: The development of a new generation of high-strength pipeline steels has allowed companies to build new pipeline infrastructure more cost efficiently.

Though the steel is stronger, TMCP steel pipe also behaves differently compared to conventional lower-strength pipe. The optimized microstructure may be changed at high temperature. For example, when welding TMCP pipe joints, the heat from the welding can decrease the strength of the adjacent areas, which are referred to as the heat-affected zone (HAZ). On the contrary, research also found increased strength when the TMCP pipe is heated up at a lower temperature, such as 500°F during pipe coating application. These changes can lead to uncertainties related to final in-service mechanical properties.

Additional research would be beneficial to more fully understand the steel microstructure transformation in TMCP steel at elevated temperature, which results in the strength decreasing in the HAZ. This could lead to changes to steel and pipe manufacturing techniques to stabilize the steel microstructure during reheating. A combination of thermo-mechanical manufacturing control and addition of chemical elements may be considered.

The NPC recommends that the DOE, working with the pipeline industry, should sponsor research and development to improve stability of TMCP steel's physical properties that are exposed to high heat conditions above 500°F.

In addition to research on steel pipe manufacturing, the pipeline industry has updated welding procedures and methods for installing the new TMCP steel pipes. API and industry are continuing to make updates to welding standards where needed. To keep pace with updates to industry standards, regulations should incorporate, as appropriate, updated industry standards more quickly. For example, the 22nd edition of the welding standard for new construction, API 1104, is to be published soon but the current CFR still refers to the 20th edition. Recently PHMSA published a document *Notice of Exercise of Enforcement Discretion with Respect to API Specification 5L, 45th edition*. Instead of the traditional method of incorporating by reference the (new) 46th edition into the U.S. CFR, PHMSA issued this notice that appears to notify the industry that they have concluded that the 46th edition of API 5L does provide a higher level of safety than the 45th edition, and PHMSA will not enforce any actions against use of pipe produced according to the 46th edition. This appears to be a departure from normal practice by PHMSA and perhaps supports the need for a better process for incorporating updated industry standards.

4. Improved Field Inspection Technologies to Reduce Material Pipe/Weld Failures

The industry has been challenged to improve its capabilities for inspecting new and existing assets to ensure proper integrity during their life cycle. Traditional radiographic and ultrasonic nondestructive examination (NDE) techniques, including film radiographic testing, manual ultrasonic testing, and magnetic particle inspection, have worked reasonably well but have limitations. The challenge is reliably detecting, characterizing, sizing, and locating imperfections in the base material and weldment. When results from NDE are not reliable, fitness-for-service determinations of in-service assets become challenging and potentially inaccurate.

The advancement of digital technology has provided the opportunity to inspect welds and base material with new media at a higher resolution than previously available with typical film radiography. New technologies such as digital radiographic testing, real-time radiographic testing, and computed tomography have the potential to enhance reliability over traditional NDE technologies.

One such new technology, computed tomography (CT), helps solve the problems of imaging defects in in-service lines, which require high energy to render an image. CT can penetrate steel and liquid using a linear accelerator or X-ray tube

to focus the energy into a controlled column that points at the digital detector panel that received the energy and generates the image. The process captures the images from the top (similar to traditional radiographic testing) and then tangentially from the side. A computer then processes and combines the collected images, using tomographic reconstruction, into a single three-dimensional image of the scan. CT allows interpretation of the size and depth of the defect, which is challenging for two-dimensional images.

The most challenging priority is inspection of long seam pipe welds in the field.[13] Once the long seam is exposed, traditional NDE methods are quite capable of detecting medium-to-large sized defects in the weld and base material but less reliably report the defect's shape and position. Advances in computer processing speed have made full matrix capture-total focusing method (FMC-TFM) and other similar ultrasonic testing methods practical for oil and natural gas application. The algorithms used by the FMC-TFM approach to predict the location of the reflector have not been fully qualified to validate accuracy for all conditions. FMC-TFM is capable of being configured to work longitudinally or circumferentially on pipe, but it must be used on material with internal and external surfaces that are parallel. It typically needs between 2 and 6 inches of parallel material to introduce the sound energy.

Three-dimensional image presentation using FMC-TFM makes interpretation of the size and depth of the defect less challenging compared to traditional UT presentations. The process records each defect and calculates the likely location for the indication and then plots that location in a three-dimensional image. FMC-TFM reduces the risk of missing defects due to geometry, misorientation, or obstruction from other defects.

The NPC recommends that industry and research consortiums should collaborate with PHMSA to complete technical development and validation of advanced field inspection technologies to accurately size features.

These data will validate the various technologies' ability to deliver known and quantified results, which will provide confidence to move from the traditional inspection methods to a more robust solution.

5. Assurance of Long-Term Pipeline Repair Integrity to Protect Against Corrosion and Material/Weld Failures

In-line inspection assessments of in-service pipelines allow pipeline operators to discover conditions or anomalies on pipeline systems requiring maintenance or repair. Steel sleeve repair is the industry's preferred repair option, with engineering and installation guidance for applying these repairs published by the American Society of Mechanical Engineers. Newer composite sleeves have also been researched and tested as an option for pipeline repair. Steel and composite sleeves are proven for specific applications and additional technology research and deployment would be helpful to expand applications for these products.

Steel sleeves come in two tight-fitting halves and are joined and welded together over an anomaly on the steel carrier pipe (Figure 4-17). Type A sleeves are used for nonleaking defects. The ends of Type A sleeves are not welded to the carrier pipe and are used most commonly to restrain deformations (e.g., dents). The ends of Type B sleeves are welded to the carrier pipe, meaning they can be used to repair more injurious defects or leaking defects.

With modern materials, qualified low-hydrogen welding procedures and personnel, and modern coating technologies, steel sleeves are a reliable repair option for pipeline operators and can last for the life of the asset. Current in-line inspection technology has limited ability to assess the condition of external sleeves attached to pipe. Future research and development of in-line inspection methods could provide additional integrity benefits.

13 Nondestructive examinations in field (rather than laboratory) settings are often referred to as "in-the-ditch NDE." In-the-ditch indicates that the pipeline often must be exposed and that the NDE technician must conduct the inspection in the excavated area around the pipe.

Source: Marathon Petroleum.

Figure 4-17. *Type A and Type B Sleeves*

Finding: The pipeline industry uses both steel and composite pipe sleeves as suitable, reliable repair methods for restoring integrity to damaged pipeline systems. When inspection of these sleeves may be needed, a visual inspection is the primary method, which can be challenging to access.

To develop a viable alternative to steel sleeves, PRCI, GTI, pipeline operators, and composite repair companies have performed research to validate long-term performance of composite repair options. Composite repairs (Figure 4-18) typically involve different types and layers of fiber and a hardening filler. American Society of Mechanical Engineers has defined composites as an acceptable repair alternative and has published some guidance for the use of nonmetallic repairs. Composite repairs do not require welding to the pipeline.

The NPC recommends that DOE should sponsor research and development on inspection technologies that would allow pipeline operators to inspect the condition of installed steel and composite sleeves throughout their life cycle without need for excavation and field inspection.

When appropriately applied, composite repairs offer advantages over steel sleeves, such as conforming to pipe ovality or irregular geometries (i.e., girth welds, elbows, tees, etc.) and ease of installation. Each type of composite has different specialized installation techniques, making standardized quality assurance more difficult. Typically, application personnel are trained and certified by the composite vendor in proper installation practices.

A reliable NDE or other inspection technique for composite installations would assure long-term safe performance of these repairs. Research would also focus on refining installation methods to help ensure consistent high-quality installations across the industry and development of in-line or remote inspection technologies to allow long-term integrity monitoring of the repair.

Composites have proven to be an effective repair for external corrosion and deformation defects. While composite materials have been used to reinforce a wide array of pipeline anomalies and features, they are still not an accepted repair for crack-like defects, planar flaws, or leaking defects. Research is underway in evaluating composite repair of these defects in high-pressure pipeline systems. Continued research is required prior to broad adoption and acceptance of composites in these applications.

The NPC recommends that industry and research consortiums, working with PHMSA and DOE, should conduct research to establish the viability of using composite repairs for crack-like defects, planar flaws, and leaking defects. This research would entail

Source: NRI/ClockSpring.

Figure 4-18. *Composite Repair on Carrier Pipe*

full-scale destructive testing and qualification of repair methods appropriate to each of these flaw types.

6. Locating Underground Utilities to Prevent Excavation-Caused Incidents

Oil and natural gas pipelines, high-voltage power transmission lines, and other types of utility infrastructure often share utility corridors, tracts of land set aside by planning authorities (Figure 4-19). Utility corridors also often cross roadways and city streets. As corridors become more crowded, excavation risks from construction and maintenance activities in the corridors increase. Risks to the pipeline infrastructure from colocated infrastructure assets (e.g., high-voltage power lines) can also increase.

Sharing common corridors for oil and natural gas pipelines along with other utilities provides benefits that include safe routing through communities and visibility awareness to neighbors. As common ground corridors become more crowded from infrastructure growth, safe construction activities in these areas become more challenging. Accurately locating pipelines and other infrastructure in underground utility corridors, which are often shared with aboveground utilities and infrastructure, is one of the keys to reducing line strikes during both construction and maintenance activities, which can result in threats to public safety and environmental damage. Maps and GIS systems are not always as accurate as needed to efficiently locate lines and to help reduce risk of excavation-related line strikes.

The NPC recommends that PHMSA, working with DOE and industry research organizations, should sponsor additional research and development to accelerate improvements in precise mapping of underground asset location (improved handling of GIS data).

Trenchless excavation (e.g., boring, horizontal directional drilling, etc.) allows pipe or other utilities to be installed under obstructions such as roadways or waterways using drilling technology, eliminating the need for difficult and intrusive open trench excavations in these areas. Trenchless excavation is also used to safely install pipelines below areas subject to surface ground movements that would otherwise be a threat to pipeline integrity. In the case of crowded utility corridors, it may be used to navigate replacement sections of pipe within the corridor between or below other pipelines, or to safely cross below other pipelines when crossing a corridor.

Although trenchless excavation can help prevent excavation damage by navigating around existing infrastructure, trenchless excavation can also cause excavation damage. For example, this can be due to actual locations of horizontal directional drilling and bore pipe that is difficult to map accurately or due to unexpected changes in soil conditions that cause the boring or drill to divert from its planned path.

The Common Ground Alliance,[14] which is funded in part by the oil and natural gas pipeline industry, supports a national call number created by Congress as a simple way for excavators (commercial and homeowners) to call one number, 811 (Figure 4-20), from anywhere in the United States, that will enable underground utilities, including pipelines, to locate their lines in advance of digging. This has greatly helped reduce the number of excavation-caused pipeline strikes. Even with robust public awareness programs being implemented by state programs and industry operators and the 811 Call Before You Dig number, excavator damage to pipelines still occurs.

14 Common Ground Alliance, http://www.commongroundalliance.com and http://www.call811.com.

Source: Marathon Pipe Line Company.

Figure 4-19. *Typical Crowded Utility Corridor Containing High-Voltage Power Transmission Lines and Buried Pipelines*

Finding: The leading causes of line strikes during excavation activities are from excavators not properly following procedures and from excavators failing to contact 811 Call Before You Dig to have underground utilities properly marked.

These excavation incidents can occur anywhere there are buried utilities and often do occur in remote areas.

The NPC recommends that oil and natural gas pipeline companies, working with DOE, PHMSA, industry research organizations, and technology providers, should expand research and development of excavator-based warning systems and proximity-based warning systems to use during drilling and digging operations to prevent pipeline strikes. These systems need to be reliable and cost effective for excavator owners and drill owners to install and use.

E. Pipeline Storage Facilities

1. Underground Storage of Gas

a. Underground Storage Overview

The underground storage of natural gas is a critical component of the natural gas supply system in the United States. Gas storage facilities store the natural gas when demand is low and supply the natural gas when demand increases. On the highest demand days underground storage delivers about half of the natural gas consumed. Natural gas storage also reduces overall energy costs as it is stored when demand and prices are low and is delivered when needed.

Approximately 400 natural gas storage facilities, comprising almost 18,000 storage wells, provide service today. Eighty percent of storage facilities employ geologic formations, or reservoirs, that originally contained natural gas or oil reserves, were depleted, and then converted to reservoir gas storage. The rest of the underground facilities are engineered for gas storage using either deep, water-filled geologic formations, aquifers, or

811®

Know what's below.
Call before you dig.

Source: Common Ground Alliance.

Figure 4-20. *811 Call Before You Dig Logo*

caverns that have been created in salt formations using a solution mining process.

Salt caverns are created from underground salt formations by solution mining. Solution mining a cavern is accomplished by drilling a wellbore into a suitable salt formation, dissolving the salt by circulating fresh or low-salinity water into the wellbore, and withdrawing or returning the brine to the surface. As the salt is dissolved, the wellbore grows to form a cavern, or cavity, in the salt formation. By carefully controlling the pressure and direction of the solution mining process, salt caverns of relatively precise dimensions can be created. When the cavern has reached its planned size, natural gas or natural gas liquids are injected into the cavern displacing and emptying the brine out of the cavern, making it ready for product withdrawal. Properly located, designed, operated, and monitored, solution-mined salt caverns are safe and efficient storage containers for very large volumes of natural gas and natural gas liquids.

Depleted reservoir storage involves developing a reservoir from which all economically recoverable oil and natural gas has been produced. Testing is conducted to ensure the reservoir can store natural gas safely and reliably. Additional infrastructure—such as injection and withdrawal wells, pressure observation wells, and compression and

pipeline facilities—is required to connect the reservoir into the gas storage and delivery system. Properly located, designed, and operated, depleted reservoirs make safe and efficient storage containers for natural gas. Key factors that influence the developments include available gas inventory, location, size, and injection and withdrawal rates.

The industry has adopted frameworks for managing underground storage wells and reservoirs, including API RP 1171 (Functional Integrity of Natural Gas Storage in Depleted Hydrocarbon Reservoirs and Aquifer Reservoirs, September 2015) and API RP 1170 (Design and Operation of Solution-Mined Salt Caverns Use for Natural Gas Storage). API RP 1171 focuses on storage well, reservoir, and fluid management for functional integrity in design, construction, operation, monitoring, maintenance, and documentation practices, and recommends that operators manage integrity through monitoring, maintenance, and remediation practices and apply specific integrity assessments on a case-by-case basis. API RP 1171 includes detailed tables that identify common threats or hazards, as well as preventive and mitigation measures. API RP 1170 provides functional recommendations for salt cavern facilities used for natural gas storage service and covers facility geomechanical assessments, cavern well design and drilling, and solution mining techniques and operations, including monitoring, and maintenance practices.

b. Underground Storage Reservoir Well and Reservoir Design and Integrity Management

Well design and integrity are a critical aspect of managing underground storage reservoirs. Industry deploys a variety of technologies to manage wells, including well logging to verify cement bonds at different sections of the well and to determine integrity of well casings (Figure 4-21). Gamma ray/neutron density logs can determine the presence of gas behind the casing. Industry also performs regular well testing to evaluate reservoir properties and well mechanical integrity. Supervisory control and data acquisition systems and or operators control and monitor the operation of the well and reservoir, and companies perform material balance analyses to evaluate

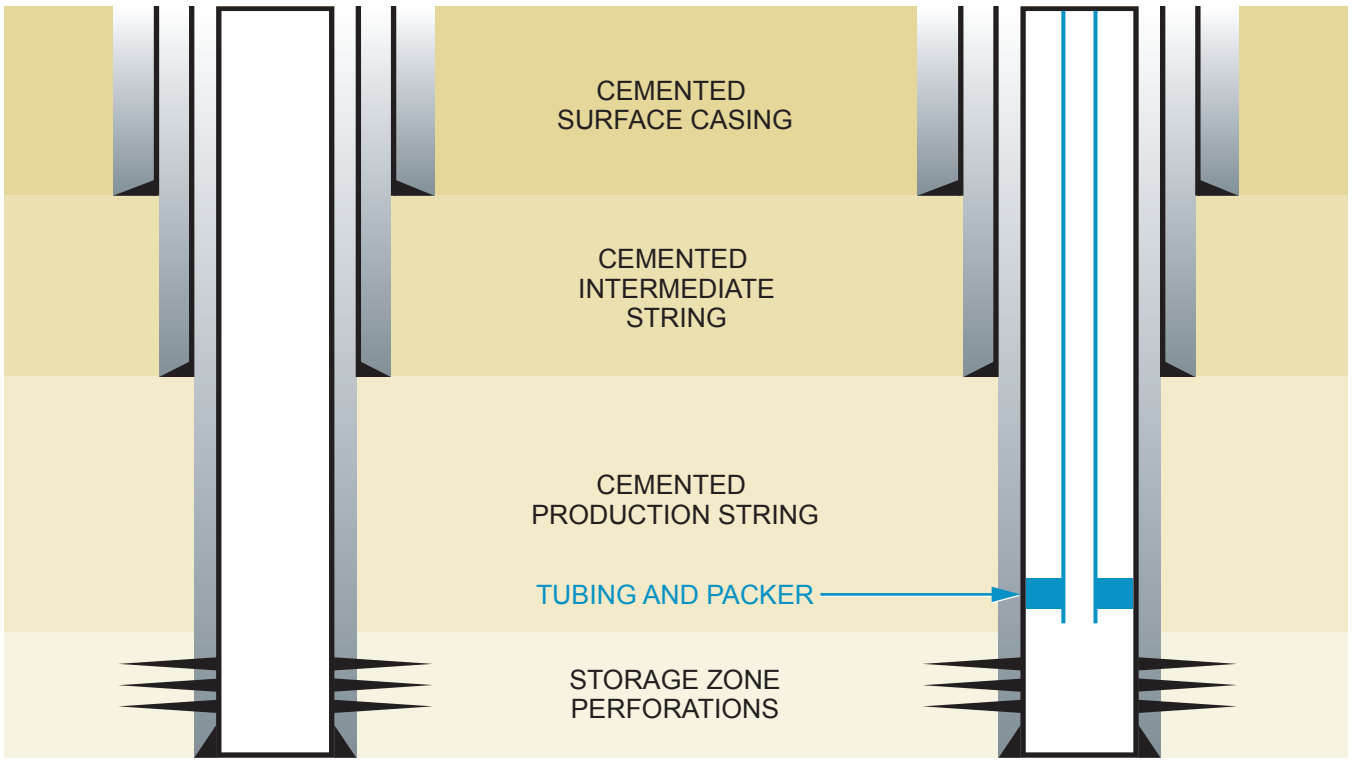


Figure 4-21. *Examples of Concentric Storage Well Casing and Well with Tubing and Packer*

containment. Other technologies include storage reservoir simulation and modeling, seismic technologies, advanced drilling technologies, and innovative software technologies to analyze rock mechanics. The current suite of metal loss inspection tools cannot detect point-specific metal loss in concentric casings or through tubing.

While industry has had an excellent safety record overall with underground gas storage, incidents have occurred. One notable incident was the Aliso Canyon SS-25 well gas leak, which lasted from October 2015 until February 2016. During the incident approximately 6 billion cubic feet of natural gas escaped to the atmosphere. The leak was a result of external microbial corrosion (MIC) of the 7" casing. The MIC caused approximately 80% wall loss which resulted in bulging, thinning, and ultimately a failure of the well casing, 892 feet below grade. The well was eventually controlled months later via a relief well and permanently plugged. The facility resumed limited operations in July 2017, and resumed full and routine operations, albeit with fewer wells, in November 2017 through an agreement with the state regulators. (See text box titled "Regulatory Response to Aliso Canyon Event.")

The Public Utility Commission of California commissioned an investigation report that was conducted by Blade Energy Partners. This May 2019 report, *Root Cause Analysis of the Uncontrolled Hydrocarbon Release from Aliso Canyon SS-25*, included several recommendations that can be found at this website, https://www.cpuc.ca.gov/aliso/.

Finding: High-resolution casing inspection logging tools have size and availability limitations relating to the diameter of the casing. High-resolution logging tools for smaller diameter wells are still in development. In addition, it is important to continue to improve the accuracy and calibration of these tools, including the ability to assess the integrity of multiple concentric casings.

The NPC recommends that DOE should lead a collaborative effort with PHMSA and industry trade associations to determine the most effective measures of casing and cement integrity and explore opportunities for casing and cement logging improvements, including additional research and development opportunities.

Identifying deterioration in well casing and cement is a critical component of maintaining well integrity. DOE's Interagency Task Force[15] recommended that a systematic assessment of casing wall thickness assessment tools be carried out by the DOE and DOT, subject to appropriations, with multiple tool types used to test manufactured articles and one or more reference wells with well-characterized corrosion issues. The goal should be to rigorously test and compare the ability of these techniques to identify, locate, and characterize corroded casings. Such a study could also inform better log interpretation practices and explore mitigative technologies, such as cement/epoxy squeezes and liners, to restore well integrity in existing wells. The advantage of DOE/DOT support is all industry participants benefit from new tool developments and improved analytical algorithms.

Finding: Technology developments are underway on casing inspection log tools and analysis that may allow the inspection of the production casing without the removal of tubing. More work needs to be done to pinpoint specific metal loss in the outer string of concentric casings.

The NPC recommends that DOE should pursue additional research and development on well inspection technologies that can improve integrity logging, and reduce the frequency of tubing removals, which would reduce risk to personnel and the environment, as recommended by DOE's Interagency Task Force.

15 Freifeld, B., Oldenburg, C., Jordan, P., Pan, L., Perfect, S., Morris, J., White, J., Bauer, S., Blankenship, D., Roberts, B., Bromhal, G., Glosser, D., Wyatt, D., and Rose, K. (2016). Well Integrity for Natural Gas Storage in Depleted Reservoirs and Aquifers. NETL-TRS-15-2016. NETL Technical Report Series. Morgantown, WV:U.S. Department of Energy, National Energy Technology Laboratory, https://www.energy.gov/sites/prod/files/2016/12/f34/Appendix%20I%20-%20Well%20Integrity%20Working%20Group%20Report.pdf.

REGULATORY RESPONSE TO ALISO CANYON EVENT

Section 12 of the PIPES Act of 2016 required minimum safety standards for underground natural gas storage facilities, and Section 31 required the establishment of an Interagency Task Force on underground natural gas storage. The Task Force, cochaired by PHMSA and Department of Energy, issued their final report in October 2016. PHMSA published an Interim Final Rule in December 2016 with an effective date of January 2017, principally based on the referenced industry standards API RP 1170 and 1171. PHMSA began inspections in March 2018 and has already conducted inspections at 92 facilities. A Final Rule is estimated to be issued in November 2019. Ten states have already joined PHMSA as regulatory partners for underground natural gas facility inspections, and two more states are expected to join for inspections in 2020.

c. Solution-Mined Cavern Design and Integrity Management

The cavern storage well integrity process starts with a comprehensive risk assessment. The risk assessment includes data collection, hazard and threat identification, likelihood of occurrence estimation, and consequence severity determination. Preventive, mitigative, and monitoring practices can reduce the potential for a loss of well and/or cavern integrity. Current technological topics concerning the development, operation, and maintenance of solution-mined natural gas storage caverns include the following:

- Dissolution theory and cavern development
- Mechanical integrity testing of wells and caverns
- Pressure monitoring, trending, and the establishment of alert limits
- Casing strength and salt creep (very slow creep tests to verify cavern creep rate)
- Safe distance of caverns to a domal boundary and distance between caverns
- Extents of bedded salt
- High-frequency cycling of salt storage caverns cyclic thermal loading creep tests
- Hanging strings dynamics/deformation of cemented casings
- Cavern sealing and abandonment
- Sonars of the cavern interior
- Subsidence and sinkholes
- Satellite subsidence monitoring.

Technologies such as synthetic aperture radar (SAR) satellites acquire images of the Earth's surface by emitting electromagnetic waves and analyzing the reflected signals. Technologies such as SAR allows different techniques to extract surface displacement measurements and to detect information about surface characteristics and variations making it possible to monitor ground uplift and subsidence in response to injection and extraction cycles. Precise displacement measurements enable operators to:

- Optimize working gas, when coupled with injection and extraction rates
- Fulfill regulatory cap rock integrity monitoring obligations
- Estimate cavern volume and pressure changes
- Monitor possible impact on surface facilities
- Calibrate cavern model and salt cavern creep calculations.

2. Aboveground Storage of Oil and Liquids

a. Aboveground Storage Overview

For nearly a century, the floating roof has maintained its status as the preferred method for controlling product evaporation loss from aboveground hydrocarbon storage tanks and preventing tank fires. While industry has a strong safety record for operating aboveground tanks, tank incidents have occurred. Recent technology advancements with floating roof integrity monitoring offers promising opportunities to reduce risk of mechanical roof failures. Large diameter tanks designed and constructed to API Standard 650 are integral to the midstream petroleum industry. The minimum requirements for long-term integrity management are defined by

API Standard 653, Tank Inspection, Repair, Alteration, and Reconstruction.

Aboveground floating roof storage tanks are used both as break out tanks for pipeline operation and long-term storage. The U.S. EIA reports that over the past decade the fast growth in domestic crude oil production has strained storage capacity and demand for new infrastructure has been acute with the U.S. crude oil storage capacity increasing by 60% since March 2011 to 590 million barrels in 2019. Although petroleum storage tanks have an excellent safety record, significant incidents can occur. The development and adoption of technologies for early detection of conditions leading to storage tank failure provides an opportunity for reducing the risks of future accidents.

While aboveground storage tanks are both reliable and safe, serious accidents can occur if the roof sinks or containment is breached. For example, boilover accidents on floating roof tanks can occur if an attempt is made to extinguish an oil or petrochemical fueled tank fire with water. Under certain conditions, the water on the bottom rapidly vaporizes into steam, causing it to expand more than 1,600 times in volume. The rapidly expanding steam may violently expel the oil or fuel out of the tank, resulting in the uncontrolled discharging of burning oil onto a large area outside of the storage tank. This can also put adjacent tanks at risk of damage.

Finding: Industry research and incident investigations have concluded that a sizable portion of floating roof incidents could have been prevented through earlier recognition of specific roof behavior patterns. Technologies have been developed to detect threats in real time, the threat that a floating roof may sink, but widespread field adoption is limited.

The Large Atmospheric Storage Tank Fire (LASTFIRE) work group concluded that in the event of a full surface fire in crude oil storage tanks, boilover should be considered as the probable outcome unless the fire is extinguished prior to build-up of a hot zone in the product.

b. Sensors

Using multiple (wireless) sensors, a floating roof monitoring system provides early warning for potential problems associated with floating tank roofs and can track roof temperature, vibration, inclination, liquid levels on deck, and potential hydrocarbon vapors. This remote monitoring can mitigate risks associated with:

- Excessive rainwater or snow accumulation
- Roof misalignment or inclination
- Mechanical damage due to misalignment of seals or ladders
- Overfilling and the effects of settling
- Potential aftereffects of a seismic event.

The NPC recommends that industry and PHMSA should consider additional research and validation on tank integrity monitoring technologies, including camera technologies and associated pattern recognition software, wireless sensors, and unmanned aerial systems (drones) to measure floating roof stability and integrity.

c. Firefighting Foams

In the event that a floating roof sinks from mechanical failure, it is critical to prevent hydrocarbon vapor emission, minimize the probability of ignition, and, if ignition does occur, rapidly extinguish fire. New and environmentally friendly foams are entering service. Application of fluorosurfactants-based firefighting foams remains the most effective tool in the arsenal of first responders. These foams face growing concerns regarding their environmental impact. After a major atmospheric storage tank fire, subterranean chemical accumulation and migration into aquifers is a serious concern. International pressure is mounting to minimize the use of fluorosurfactants-based chemicals and outright bans have been called for in some areas, including several U.S. states.

Unless an equally capable firefighting foam solution enters service over the next several years, such bans could leave the oil industry unprepared to respond effectively to large industrial accidents. A new generation of foams has been developed

that does not act as persistent environmental pollutants. The effectiveness of these foams is still under investigation. The LASTFIRE group leads this effort on behalf of the petroleum industry. Based on this work, opportunities have been identified to develop improved deployment equipment and protocols, as well as novel post-incident processing techniques.

Finding: The effectiveness of the new and environmentally friendly foams that are entering service warrants additional study and field testing. The ability to dispense foam rapidly when needed can mean the difference between a manageable incident and a crisis situation. Opportunities to transition to more environmentally friendly firefighting foams are under review.

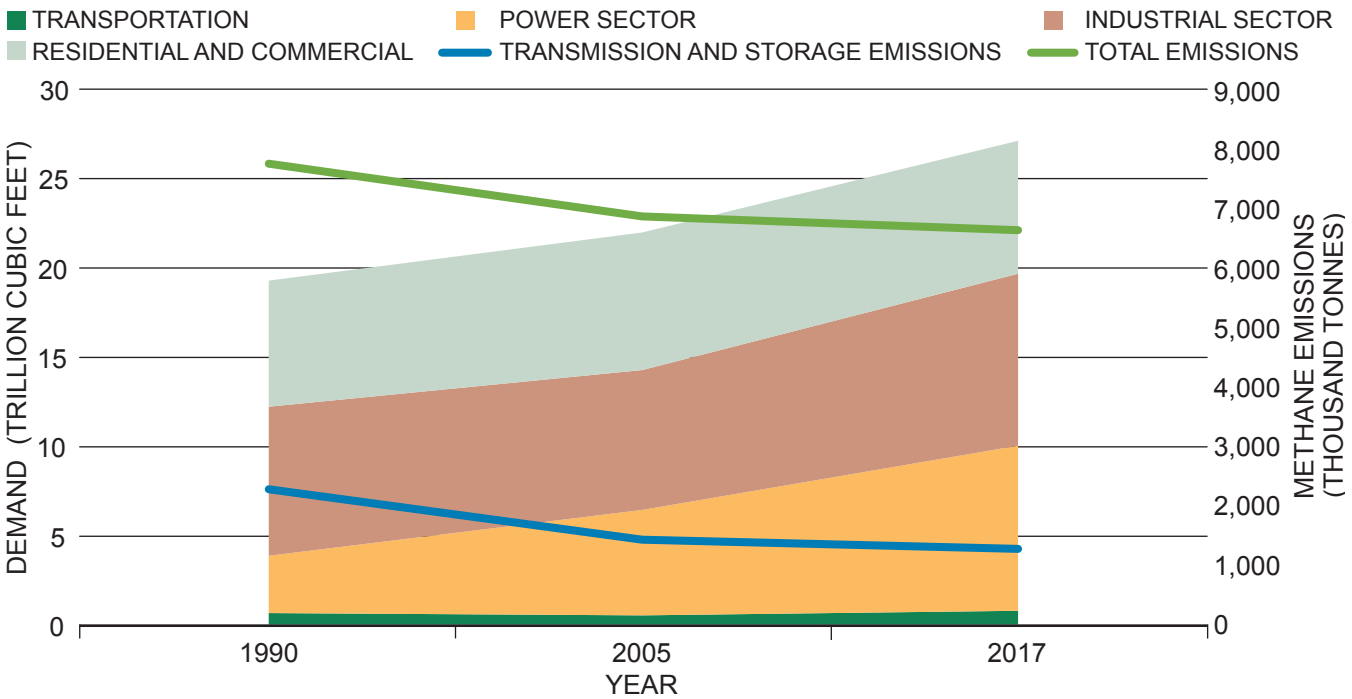
F. Pipeline Methane Emissions

1. Pipeline Methane Emissions Overview

Natural gas consumption volumes since 1990 have increased more than 40%. In the same timeframe, transmission pipeline and storage sectors have reduced methane emissions by 43% (Figure 4-22). Most of the consumption increase has occurred in the power sector. Methane is the primary component of natural gas, typically making up about 95% by weight. Growth in natural gas production, transport, and use is expected to continue increasing in the future.[16] At the same time, the oil and natural gas transportation industry shares with the public and environmental agencies the desire to continue reducing emissions of methane along with criteria pollutants. Leveraging technology, implementing best practices, and updating regulations will further reduce methane emissions while continuing progress in reducing criteria pollutant emissions. Because industry and vendors continue to develop ways to reduce criteria pollutant emissions, there is not a current need for additional DOE funding to support criteria pollutant reduction efforts.

Total methane emissions in the transmission pipeline and storage sector represent 20% of

16 See Chapter One of this report, "Supply and Demand."



Sources: EIA, Monthly Energy Review, May 2019, and U.S. Environmental Protection Agency, *Inventory of U.S. Greenhouse Gas Emissions and Sinks, 1990–2017*, April 2019.

Figure 4-22. *Natural Gas Demand versus Methane Emissions*

total methane emissions in the complete natural gas value chain (Figure 4-23), and represents less than 1% of the U.S. total greenhouse gas footprint.[17] While the transmission pipeline and storage sector has made significant reductions in methane emissions, further reductions to its 20% share of total methane emissions are possible. Methane emissions in the transmission pipeline and storage sector have been reduced primarily through voluntary initiatives while transportation volumes have grown significantly. Data from 2013 through 2017 indicate that reductions have plateaued. The development and deployment of new technologies, consistent implementation of best practices, and regulatory changes that encourage adoption of new technology will help achieve additional reductions in methane emissions.

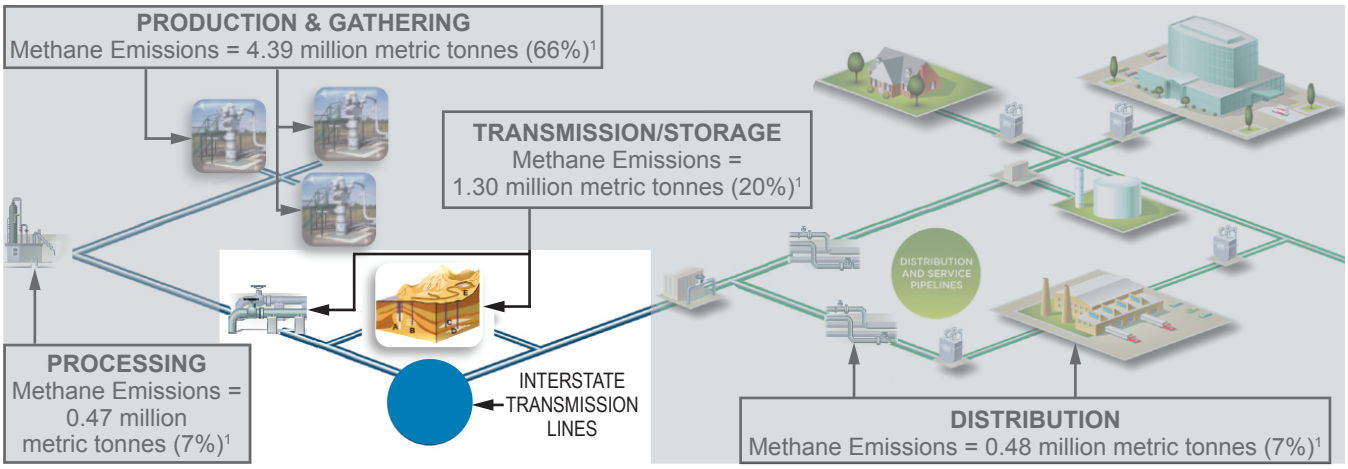
Finding: Pipeline companies are committed to extending the progress made in reducing methane emissions through voluntary programs such as the Environmental Partnership, EPA's Methane Challenge, Natural Gas STAR, and ONE Future.

17 Environmental Protection Agency, Inventory of U.S. Greenhouse Gas Emissions and Sinks, https://www.epa.gov/ghgemissions/inventory-us-greenhouse-gas-emissions-and-sinks.

Figure 4-24 shows the relative contribution of methane emissions by source from the transmission pipeline and storage sector for 2017. The primary addressable sources of emissions in the transmission pipeline and storage sector are compressor station leaks, uncombusted methane in the exhaust stream of reciprocating compressors (referred to as methane slip), and planned pipeline blowdown events (the controlled release of natural gas from a section or sections of the pipeline). These sources account for approximately 88% of the methane emissions in the transmission pipeline and storage sector.

2. Reducing Compressor Station Leaks

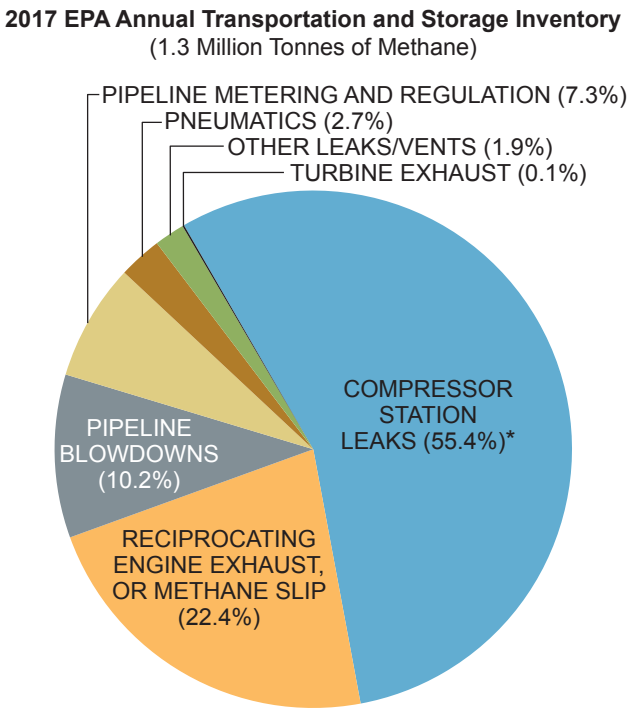
Compressor stations account for approximately 55% of the methane emissions from the transmission pipeline and storage sector. Fugitive emissions—leaks to the atmosphere from process equipment—are the primary source of compressor station leaks. Fugitive emissions are a result of leaks from sealed surfaces, which typically occur as a result of wear of mechanical joints, seals, gaskets, and rotating surfaces. Fugitive emission sources include components such as compressor seal rod packing, flanges, connectors, valves, open-ended lines, and pressure relief valves. Federal regulations in 40 CFR 60 Subpart OOOOa, as well as some state regulations, are currently in



[1] EPA, 2019a. Inventory of U.S. Greenhouse Gas Emissions and Sinks. Table 2-1 and Table 3-65 (https://www.epa.gov/ghgemissions/inventory-usgreenhouse-gas-emissions-and-sinks.

Source: United States Department of Energy, Office of Oil and Natural Gas.

Figure 4-23. *Natural Gas Value Chain and Sources of Methane Emissions*



* Includes reciprocating engine leaks from seals, centrifugal leaks/seals, station leaks, and station.

Source: Environmental Protection Agency. (2017). Inventory of Greenhouse Gas Emissions and Sinks.

Figure 4-24. *EPA Annual Inventory—Contribution by Source to Methane Emissions Inventory*

place to reduce fugitive methane emissions from compressor stations.

The primary technology and operational practices for reducing emissions from reciprocating compressor seal rod packing leakage are periodically monitoring leak rates and repairing or replacing seals either when leak rates exceed a threshold or when the seals exceed the operating hours or calendar requirements in Subpart OOOOa.

The primary technologies or operational practices for reducing gas leakage emissions from unit isolation valves, blowdown valves, and other station components are through (1) preventive maintenance (particularly for large isolation valves and blowdown valves) and (2) directed inspection and maintenance surveys.

The technologies and operational practices discussed above continue to be implemented to reduce compressor station emissions. There is a limit to methane emissions reductions with current technologies and practices. Furthermore, low levels of compressor station and pipeline emissions occur from normal operations, maintenance, and integrity of the facility. Pipeline system reliability requirements and safety/emergency issues are two critical factors that must be considered when evaluating methane emissions mitigation options.

There is an opportunity to improve the regulations to better encourage, not discourage, the development and deployment of technology. Resources could be used to develop and demonstrate new technology or more effective practices to further enhance the management and mitigation of the methane emissions. For example, OOOOa, which applies to new and modified transmission and storage compressor stations, requires the replacement of engine rod packing on a defined schedule of operating hours or a defined timeframe, regardless of its condition. The requirements may lead to replacements when the rod packing is still in good condition. A condition-based maintenance approach requiring replacement of rod packing based on leak rates exceeding a defined threshold would avoid replacing rod packing in good condition and incentivize operators and manufacturers to develop and install longer-lasting, more efficient rod packing that reduces emissions. Subpart W rod packing leak rate measurement data could be used as a resource to determine the appropriate thresholds for maintenance.

The OOOOa regulation also requires periodic fugitive leak surveys to be performed using optical gas image (OGI) technology to identify and locate leaks at compressor stations. OGI technology is not currently able to quantify the leak rate, and Subpart OOOOa requires that all detected leaks be repaired regardless of the leak rate. Resources are required to address all the detected leaks, most of which are small. Regulation should instead be performance based to encourage the development and adoption of real-time detection equipment that can quantify leak rates and identify the most critical leaks and prioritize leak repairs.

Initial discussions between industry and EPA have signaled a willingness by the agency to

develop a real-time measurement approach which applies a leak rate threshold for repairs (similar to the Method 21 concept, which establishes a threshold for making required repairs). Further, this technology will give industry a more effective tool to prioritize and reduce its methane emissions.

Finding: Prescriptive elements of existing regulations (e.g., rod packing changeout requirements) create barriers to the advancement and deployment of new technology that could be used to more effectively reduce methane emissions.

The NPC recommends that the EPA, in collaboration with industry, should develop performance-based regulations that will encourage the advancement and deployment of new rod packing and real-time emissions detection technology to better manage and minimize methane emissions.

The opportunities to improve methane emissions mitigation strategies from compressor stations are related to tools to rapidly detect, locate, and quantify leaks, and cost-effective technologies and work practices to mitigate the emissions. Smart leak detection and repair programs using enhanced OGI or other similar technologies to identify leaks and prioritize the leaks for repair based on the leak rate are needed. The enhancements would include:

- Leak classification by OGI. Current OGI does not quantify leak rates, there is ongoing research and product development to integrate leak rate quantification algorithms into OGI functionality. Before such leak rate quantification algorithms are developed, the ability to bin, or classify leaks (e.g., as large/repairable or small/insignificant), using OGI could be developed.

- Next generation fixed or aerial sensors that will identify, locate, and quantify leaks. The sensors can be linked with communication equipment that will notify local management if the leak exceeds a defined leak rate.

The above technology advances and regulatory changes could cost-effectively reduce compressor station methane emissions. The technology advancements, in conjunction with regulations that are performance based would provide additional opportunities for cost-effective methane emissions reductions.

Findings:

- Compressor station fugitive methane emissions could potentially be further reduced through the use of new, innovative technologies for identifying, locating, and quantifying methane emissions.

- The development of a protocol to demonstrate regulatory equivalency is needed as well as test sites such as Colorado State University's Methane Emission Test and Evaluation Center (METEC) to verify the equivalency of the technology.

The NPC recommends that:

- DOE should work with industry and technology developers to fund the development of technologies to better identify, locate, and quantify methane emissions.

- EPA should work with industry to develop a protocol to validate when new technology is equivalent to or better than existing regulatory requirements. DOE should work with industry to continue funding the Colorado State University METEC site or other similar sites to test and prove the equivalency of technologies to support timely deployment of new proven technologies. The METEC site simulates real-world equipment, operations, and leaks.

3. Reducing Uncombusted Methane Fuel Gas from Reciprocating Engines (Methane Slip)

The U.S. natural gas pipeline industry operates about 5,600 spark-ignited natural gas fueled engine-compressors generating around 9,150,000

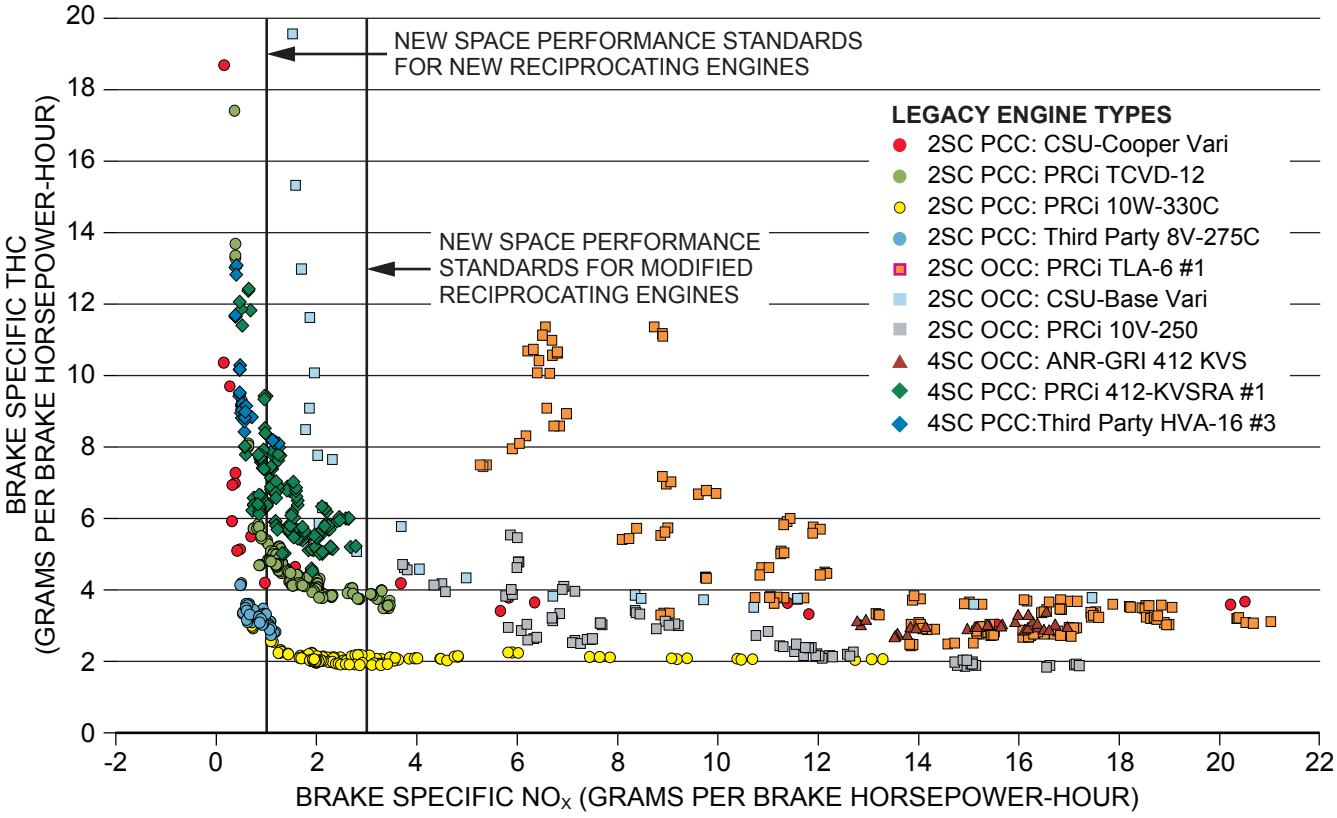
brake horsepower (more than 6,800 MW). Most of these engines operate on a lean burn cycle to maximize efficiency and minimize emissions of NOx. These engines typically emit 2 to 10 grams per brake horsepower-hour (1,000 to 5,000 parts per million) total hydrocarbons, primarily methane, in the exhaust. Moreover, as the engines run very lean to reduce NOx emissions, the total hydrocarbons in the exhaust increases (Figure 4-25).

The focus of technology advancement and deployment is to reduce natural gas transmission pipeline and storage methane emissions without increasing NOx or other EPA criteria pollutants.[18] Industry has reduced NOx from 1970 to 2017 by 60%.[19] Technological changes have been one of the major drivers in reducing criterial pollutant emissions. System modernization projects, and the continued implementation of more efficient and effective technology, will further reduce criteria pollutant emissions.

This total hydrocarbon (or methane) slip (i.e., uncombusted fuel gas from reciprocating engines) comes from fuel gas that is trapped in the cylinder during the combustion process but does not actually combust. This unburned fuel comes from crevices, quench zones, and extremely lean pockets in the combustion system. During the expansion stroke, the unburned fuel gas expands into the exhaust.

18 EPA criteria pollutants include carbon monoxide, lead, nitrogen dioxide, ozone, particulate matter, and sulfur dioxide. Criteria pollutant emissions from the transmission pipeline and storage sector are primarily nitrogen oxide, volatile organic compounds, carbon monoxide, and particulate matter.

19 Environmental Protection Agency, Air Pollutant Emissions Trends Data, https://www.epa.gov/air-emissions-inventories/air-pollutant-emissions-trends-data.



Source: "Final Report: Carbon Pollutant Emissions and Engine Performance Trade-Offs vs NOx Emissions for Reciprocating Internal Combustion Engines Utilized in Gas Transmission Service," PRCI Report PR-260-9726, December 1998.

Figure 4-25. *Typical Total Hydrocarbon versus NOx Emissions from a Variety of Legacy Engines*

Consequently, the challenge exists to develop new technologies to improve in-cylinder combustion, which will reduce methane in the exhaust without causing an increase in NOx and other criteria pollutant emissions. Additionally, cost-effective measurement methods are needed to better assess concentrations of methane in reciprocating engine exhaust. While combustion mechanisms have been studied by PRCI and others, the scope of the associated fundamental research exceeds the capabilities of equipment suppliers, engine operators, and the PRCI.

Two areas of opportunity for research and reduction of unburned fuel in the exhaust are combustion improvements and the development of cost-effective methods for quantifying the methane component of that unburned fuel in the exhaust. Extensive testing has demonstrated that improved mixing via technologies such as high-pressure fuel injection will significantly reduce unburned fuel.[20] This result suggests that much of the unburned fuel in the exhaust arises from localized, excessively lean pockets in the main combustion chamber due to nonuniform mixing. Further improvements in mixing are possible via changes to port design, piston crown design, and fuel injector nozzle geometry. Moreover, the general degree of mixing can be quantified via modern computational fluid dynamics (CFD) tools.

Additional research would be helpful to identify ways to quantify the amount of mixing required and the required associated compression ratio. Research is needed to determine the minimum equivalence ratio that will still burn to completion at typical in-cylinder pressures and temperatures for ultra-lean engines operating at less than 1.5 grams per brake horsepower-hour NOx. The results of this research would allow designers to use modern CFD tools to optimize in-cylinder mixing. Other factors such as local temperature, pressure, and fuel quality may be other factors adding to the uncertainty in emissions and may warrant studying. The industry lacks the tools to make such spatially localized equivalence ratio measurements and to measure and assess the contributions of radical formation to the precombustion chamber combustion process.

Finding: Additional research on enhanced combustion processes and technologies could provide new opportunities to further reduce methane slip while also continuing industry's progress in reductions of criteria pollutant emissions from reciprocating engines.

The NPC recommends that DOE should fund research and development with research consortiums for combustion engines that will enhance combustion efficiency and reduce methane slip while not increasing criteria pollutant emissions.

The other research opportunity is in the measurement of methane in exhaust. Most field measurement devices such as electrochemical cell portable emissions analyzers measure total hydrocarbons in the exhaust. While such analyzers have proven reliable for measuring criteria pollutants (NO, NO_2, and CO), the accuracy for total hydrocarbon is sufficient only for screening or relative measurements. Flame ionization detector reference method analyzers measure bulk or unspeciated total hydrocarbons. More laboratory grade devices such as Fourier infrared spectrometers or gas chromatographs can speciate the various hydrocarbon components; however, they are not cost effective for source screening in field use.

Finding: An efficient and cost-effective method for measuring methane slip is not yet available to support the development of enhanced combustion systems that could reduce methane slip.

The NPC recommends that DOE should fund research and development to develop efficient and cost-effective methods for directly measuring methane in the exhaust.

20 Ladd, J., Stevens, M., and Olsen, D. B. (August 2016). "Methane Reduction Data Analysis for 2-Stroke Lean Burn Natural Gas Engines," PR-179-15212 prepared for the Compressor and Pump Station Technical Committee of Pipeline Research Council International, Inc.

4. Reducing Methane Emissions from Planned Pipeline Blowdowns

Natural gas pipeline transmission system operators routinely reduce line pressure and discharge gas from pipeline sections to ensure safe working conditions during planned activities. Operators isolate a pipeline segment from upstream and downstream sections of the pipeline, typically by closing valves. Natural gas within the isolated pipeline segment is blown down in a controlled release. Methane emissions levels associated with such planned pipeline blowdowns are determined by the natural gas composition, the pipe diameter, the operating pressure, and the length of the pipeline segment.

Pipeline blowdowns are a part of normal and safe operations and account for approximately 10% of all transmission pipeline and storage methane emissions. Planned blowdowns are primarily conducted when (1) connecting new facilities to existing pipelines, (2) performing operations and maintenance activities, and (3) engaging in pipeline integrity activities such as hydrostatic testing to verify the safety of pipelines. Methane emissions from these activities could be significantly reduced by applying best practices, advancing in-line inspection technology, and enhancing DOT/PHMSA pipeline safety rules.

EPA includes pipeline blowdown emissions as a source to consider under "Best Management Practices" (BMPs) in its Methane Challenge program, which is the next generation of the Natural Gas STAR program.[21] The Natural Gas STAR voluntary methane emissions reduction program is an industry and EPA initiative to reduce methane emissions by voluntarily implementing the BMPs. EPA identified the following approaches to reduce pipeline blowdown emissions in the Methane Challenge BMP technical document:

- Routing the natural gas to a low-pressure system by taking advantage of existing piping connections between high- and low-pressure systems
- Temporarily resetting or bypassing pressure regulators to reduce system pressure prior to maintenance
- Installing temporary connections between high- and low-pressure systems.

Pipeline pump down and/or routing the natural gas to lower pressure lines is an effective method to achieve reductions. In some cases, this involves the use of a portable compressor to move the natural gas from one line to another. Some jurisdictions require the emissions to be flared using portable flares. Flares are not practical options for most blowdowns because of their limited ability to handle the high pressures and volumes of methane to be blown down from transmission pipelines. Access constraints and physical space limitations pose additional restrictions. EPA acknowledges limitations in the ability to use a flare and agrees a case-specific review is needed.

Pump down or rerouting requires significant pre-job planning and may extend the duration of the pipeline capacity reduction. A feasibility assessment is necessary when considering pipeline pump down. Factors to consider include potential system reliability issues or service disruptions from the pipeline being out of service for an extended period of time.

The best opportunity to lower emissions from pipeline blowdowns is to reduce the need for planned blowdowns. One source of planned blowdowns is from the application of hydrostatic pressure testing utilized for the purpose of assessing the integrity of pipelines. Hydrostatic testing of pipelines requires blowing down and depressurizing the pipeline. Another driver of additional pipeline emissions is the current regulatory requirements to replace pipe when population density increases, even when the pipeline in place is in good condition. Replacing pipeline segments also requires blowing down and depressurizing the pipeline.

There are several industry and regulatory accepted methods for assessing the integrity of pipelines. Two of the most common methods are hydrostatic pressure testing and the use of in-line inspection tools. Among the advantages of in-line inspection technologies is that their use results in substantially reduced emissions compared to hydrostatic pressure tests. While hydrostatic tests require blowing down the pipeline, in-line inspection tools utilize the pipeline segment gas flow and

21 U.S. Environmental Protection Agency, "Methane Challenge Program," https://www.epa.gov/natural-gas-star-program/methane-challenge-program.

pressure to move the tool down the pipeline and therefore do not require blowing down the pipeline segment.

While in-line inspection is generally preferred for assessing the integrity of pipelines, there are some limitations with their use. For example, in-line inspection tools are not able to collect all necessary information about the pipeline. One of the limitations is the ability to measure certain material properties of the pipe, such as toughness and yield strength, to validate pipeline maximum allowable operating pressure. Another challenge with in-line inspection technology is the limitations with identifying and sizing girth weld defects.

Finding: Continued technology development advancements of in-line inspection technologies to better assess threats should enable a reduction of hydrostatic testing.

The NPC recommends that industry, in coordination with PHMSA, DOE, and other agencies, should conduct research and development to improve in-line inspection tool capabilities for natural gas pipelines to address technology gaps, thus enabling the application of integrity management principles and technologies to replace hydrostatic testing and pipe replacement requirements of in-service pipelines where possible.

The regulations should reflect the options proposed by the Gas Pipeline Advisory Committee, which was supported by PHMSA. These technology improvements and regulatory support could help to reduce pipeline blowdowns and associated emissions.

III. SURFACE MODES OF TRANSPORTATION

A. Liquefied Natural Gas Transportation

1. LNG Industry Overview

The LNG industry has advanced significantly since inception in both safety and technology, resulting in global liquefaction facilities that are designed and constructed for safe, reliable and efficient operations. The industry has an exemplary safety record that has been built up over its first half century: as reported by the International Group of Liquefied Natural Gas Importers, some 97,000 LNG cargoes have been delivered without any major accident attributable to the cargo.[22]

Numerous infrastructure projects are positioning the United States to significantly expand exports of LNG to the world market (see Chapter 1, Supply and Demand, for more information). According to a May 30, 2019, report from the U.S. EIA, the nameplate capacity of the LNG plants either in operation or in construction amounts to approximately 98 million tonnes per annum (Mtpa) (98 Mtpa of LNG is equivalent to 12.89 billion cubic feet per day of natural gas).[23] The IGU World LNG Report for 2019 notes that in addition to those export projects which are either in operation or under construction, there are nearly 20 other LNG export facilities that have been proposed in the United States with a total proposed LNG export capacity of approximately 190 Mtpa. This significant growth in U.S. LNG export is depicted in Figure 4-26, which would make the United States one of the top producers and exporters of LNG in the world within the next decade.

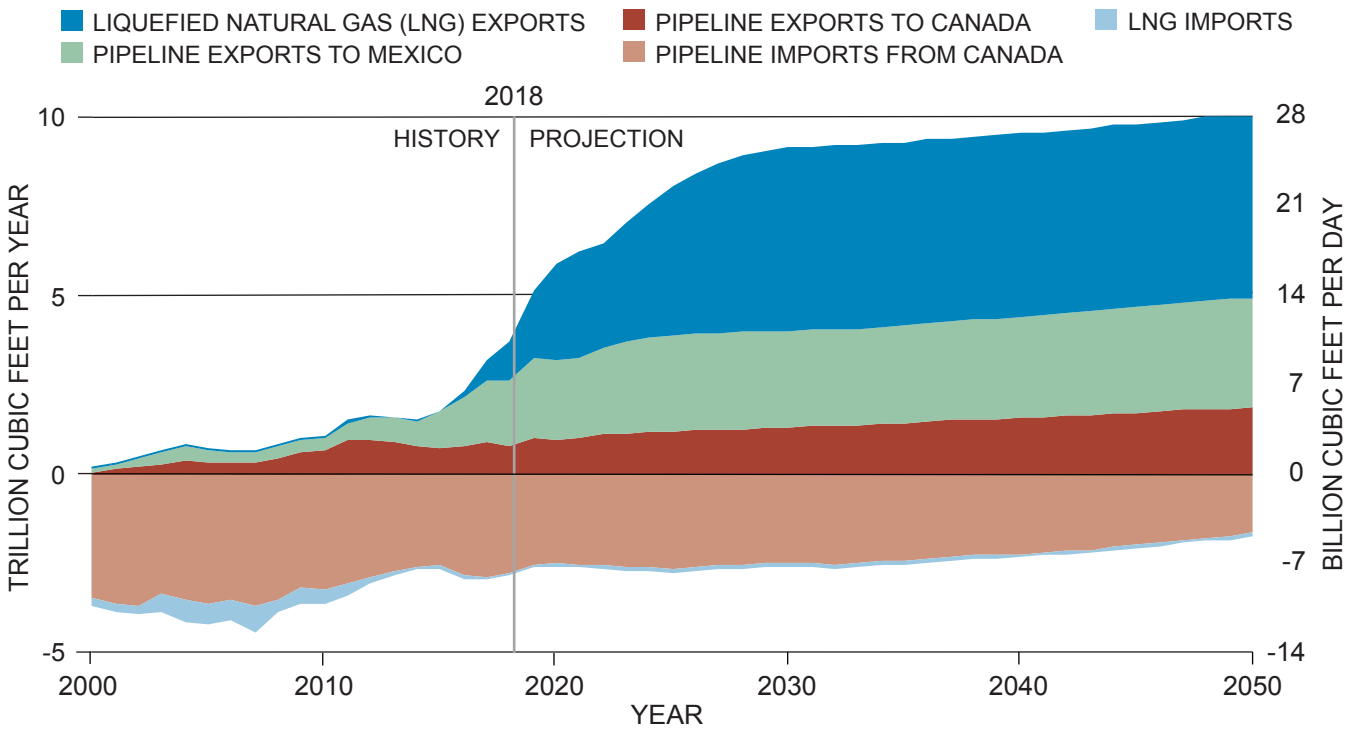
According to PHMSA (November 1, 2019)[24] there are 157 LNG facilities operating in the United States. These facilities perform a variety of services as follows:

- The largest and most complex of the LNG production facilities have been built to export LNG to other countries.
- The smaller but more numerous facilities provide natural gas supply to interstate pipeline systems, or local distribution companies.

22 International Group of Liquefied Natural Gas Importers. (2019). The LNG Industry: GIIGNL Annual Report 2019, https://giignl.org/publications/giignl-2019-annual-report.

23 U.S. Energy Information Administration, https://www.eia.gov/naturalgas/U.S.liquefactioncapacity.xlsx.

24 Pipeline and Hazardous Materials Safety Administration. (November 1, 2019). https://www.phmsa.dot.gov/data-and-statistics/pipeline/liquefied-natural-gas-lng-facilities-and-total-storage-capacities.



Source: EIA, *Annual Energy Outlook 2019.*

Figure 4-26. *U.S. Net Export of Natural Gas, 2000 to 2050*

- The local utility owned and operated facilities are used to store natural gas for periods of peak domestic demands.
- There are also natural gas liquefaction facilities that produce LNG used as a fuel for vehicles or for industrial purposes.

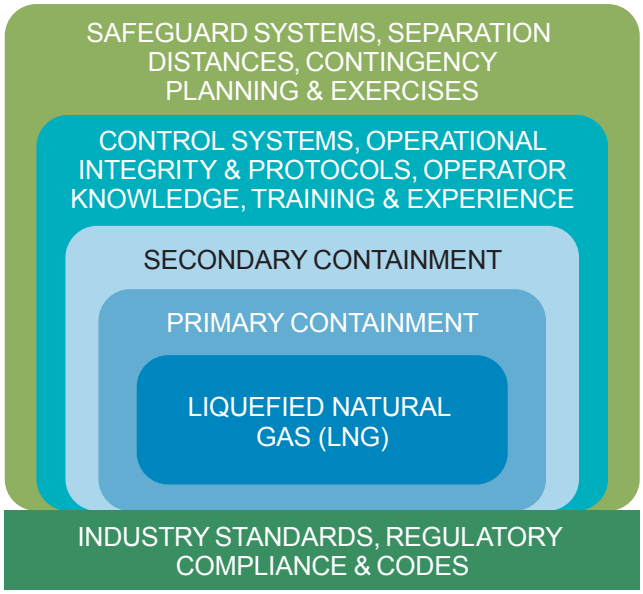
Finding: There is a healthy and broad range of LNG operating experience in the United States spanning from the first U.S. export facility in Kenai, Alaska, peak shaving plants located in the Northeast and Midwest, to the new, large purpose-built LNG export facilities located on the Gulf and East coasts of the United States.

2. Onshore LNG Storage and Containment Integrity

Overall, from an industry perspective, LNG storage tanks and related safety systems have been based on proven technology and sound engineering. Design and operational practices are governed by several layers of protection supported by industry standards, regulatory requirements, and design codes (Figure 4-27).

Containment integrity starts with design, employing sound engineering principles and applying design codes to satisfy an array of safety and regulatory requirements. This is coupled with robust quality assurance/quality control and testing programs during fabrication and construction with strong emphasis on material selection to meet the cryogenic condition that equipment, vessels, and structures might be exposed to.

LNG is stored at nearly atmospheric pressure in aboveground tanks, with safety systems to deal with any vacuum or increase in pressure due to upset conditions. Typically, the inner or primary containment is constructed of 9% nickel steel, which will not crack under cryogenic temperatures. Outer or secondary containment may be constructed of either steel or concrete. LNG storage tanks for large export facilities are usually designed without bottom or side wall penetrations, thus eliminating these as potential leak points.



Source: International Group of Liquefied Natural Gas Importers, LNG Information Paper #5, "Managing LNG Risks – Containment." 2019 Update.

Figure 4-27. *Illustration of Layers of Protection for LNG Containment Systems*

There are three predominant types of onshore storage designs for LNG that have evolved over the years; single containment, double containment, and full containment. All three storage concepts are based on having secondary containment of the LNG in case of complete failure of the main or primary container. The secondary containment is sized for 110% of the volume of the primary container volume. In the case of single containment, there is an outer tank of mild steel to hold the insulation material, but the secondary containment is a bunded area around the tank. Double and full containment tanks employ concrete outer tanks surrounding the inner tank to contain any liquid spills and hold the insulating materials.

Membrane tank technology is being considered for onshore LNG storage and has been recognized by the applicable design standards NFPA 59A and API 625. Membrane technology is based on the containment design system for LNG carriers. The membrane tank is constructed of a composite structure consisting of a thin metallic liquid barrier and a self-standing outer wall, with a load bearing thermal insulation in between the two. The outer wall may be constructed of either concrete or steel.

LNG storage tanks are designed with fire and gas monitoring and alarm systems, which include optical flame detection as well as spot flammable gas detection and open path gas detection. Low temperature sensors are provided in the bottom of the annulus (between the primary and secondary container) to detect cryogenic liquid release. LNG storage tanks have a leak detection system to produce an alarm when low temperature is detected in the annular space located between the primary and secondary container.

In the United States FERC is responsible for authorizing the siting and construction of onshore and near-shore LNG import or export facilities under Section 3 of the Natural Gas Act. The environmental permitting of waterfront LNG facilities is regulated under 18 CFR 380, Regulations Implementing the National Environmental Policy Act. The federal safety standards for siting, design, construction, operation, and maintenance of the LNG terminals and its storage components are codified in Title 49 CFR Part 193, Federal Safety Standards for Liquefied Natural Gas Facilities. The DOT Part 193 Regulations that govern the design, siting, and operation of LNG terminals was historically developed from Part 192 pipeline regulations and was mainly to serve the growth in peak shaving plants around the United States at the time. Part 193 prescribes the minimum federal safety standards for LNG facilities and incorporates by reference several industry consensus standards, including the National Fire Protection Association (NFPA) 59A-2001 and -2006 editions, Standard for the Production, Storage and Handling of LNG for the siting, design, construction, equipment, and fire protection of LNG facilities. The need for an updated regulatory framework suitable for large-scale LNG production and export terminals has been recognized in Executive Order 13868, "Promoting Energy Infrastructure and Economic Growth."[25]

There are more current design codes that are applied specifically to LNG facilities. The design and construction of the steel inner tanks are covered under API 620, Design and Construction of

25 E.O. 13868 of April 10, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-promoting-energy-infrastructure-economic-growth/.

Large, Welded, Low-Pressure Storage Tanks (less than 15 psi) and the design of concrete tanks is covered under ACI 376, Code Requirements for Design and Construction of Concrete Structures for the Containment of Refrigerated Liquefied Gases.

NFPA 59A in its 2019 edition includes a risk-based approach to the design of LNG facilities. This initiative brings the United States standards more in line with the European standards (for example EN 1473) and the international LNG industry that has had a long history of applying risk-based design. The 2019 edition of NFPA 59A also includes a new chapter on performance-based LNG Plant Siting Using Quantitative Risk Assessment.

Finding: Current DOT Part 193 regulations do not recognize updated design codes and standards used today for LNG production and export facilities. These requirements do not recognize relevant risk-based standards that are used internationally for LNG export projects, which can impair the cost competitiveness for U.S. LNG operators.

The NPC recommends that, pursuant to Executive Order 13868, PHMSA, working with the LNG industry, should jointly review and update 49 CFR Part 193 for design, construction, and operation of LNG facilities to ensure they align with world-wide best practices, advances in design codes and reflect risk-based standards.

Modern day LNG export facilities may have several storage tanks each ranging from 160,000 m^3 to 220,000 m^3 of LNG (equivalent to 1 million to 1.4 million barrels of LNG). As a result, LNG storage plays a significant role in plant siting due to these large volumes of inventory.

Computer modeling is used to determine the consequences of vapor dispersion and thermal radiation in case of a breach of primary containment. LNG is nontoxic and noncorrosive and, if spilled, will not pollute waterways or penetrate groundwater. LNG vaporizes on contact with warmer ground and rises because methane is lighter than air. For plant siting and layout requirements, there are several applicable thermal flux and vapor cloud dispersion limits, which are designed to protect the public outside the facility boundaries. For example, the location of the secondary containment should be such that the thermal radiation flux limits in case of ignition of a design spill from an LNG storage tank should not be greater than 5kW/m^2 at the facility property boundary.

The secondary containment must also be sited to ensure that the resulting methane concentration in the air does not exceed 50% of lower flammability limit outside the LNG plant property. These limits set exclusion zones to protect the public by containing the LNG hazard within the facility property boundary, or that which the operator has control over. The modeling of such releases is also used to determine equipment location and spacing within the plant boundary as well as the demarcation of safe zones for plant personnel.

Modeling and the siting requirement are addressed in the Federal Energy Regulatory Commission (FERC) permitting process for FERC-jurisdictional facilities. PHMSA ensures that the LNG operator complies with the requirements prescribed in Part 193, including requirements for modeling and the facility's site location with respect to land use adjacent to an LNG facility. Additionally, Part 193 requires that LNG transfer areas, like the rundown line from the liquefaction plant to the LNG tanks be provided with spill collection sumps to contain the volume released from a flow of 10 minutes in case of leak from the transfer line. Similar LNG spill collection systems are provided at the marine transfer area.

The NPC recommends that industry, through its trade associations, should work with PHMSA to develop an inspection regime/protocol specifically for LNG tanks that are built to API 625 and ACI 376, and based on the failure mechanisms unique to LNG storage. This initiative could take the form of a standard similar to API 653 that is applicable to API 650 tanks.

3. LNG Maritime Shipping

a. Overview

The LNG maritime shipping industry since its inception has operated without a marine incident causing a release of LNG from an LNG carrier's cargo tank. The excellent safety record is a result of robust vessel design, proven industry standards, strong regulations, and the LNG industry commitment to risk management.

Many of the standards and regulations that have been adopted for LNG shipping originate with the International Maritime Organization (IMO), an arm of the United Nations. The IMO promulgates rules and regulations through conventions and codes, which are adopted and enforced by the member states. In the United States, the U.S. Coast Guard is responsible for enforcement of IMO regulations and codes. For LNG tankers, IMO codes cover safety (SOLAS), construction (IGC Code), Watchkeeping (STCW convention), pollution control (MARPOL), safety (ISM) and security (ISPS code).

In addition to the IMO and the classification societies there are three international industry groups that play a critical role in LNG shipping and terminal operation: Oil Companies International Marine Forum (OCIMF); Society of International Gas Tanker and Terminal Operators (SIGTTO); and the International Group of Liquefied Natural Gas Importers (GIIGNL).

Sharing best practices and standards through nonprofit trade organizations has served to strengthen the safety environment of the entire industry. Strict adherence to a combination of applicable regulations, codes, and standards has led to the LNG industry's exemplary safety record.

For LNG shipping, just as with onshore LNG facilities, multiple layers of protection are implemented to minimize the likelihood of an LNG release and, if a release occurs, to mitigate the consequences. Industry standards and regulatory compliance (see text box titled "Key U.S. Maritime Regulations Pertaining to LNG Shipping") create a comprehensive safety framework within which each protective layer functions to create a safe operational environment for LNG vessels. The layers of protection are employed by LNG carrier and terminal operators to ensure the safe liquefaction, storage, transportation, and regasification of LNG.

KEY U.S. MARITIME REGULATIONS PERTAINING TO LNG SHIPPING

- 33 CFR Part 127 – Waterfront Facilities Handling Liquefied Natural Gas and Liquefied Hazardous Gas[26]
- 33 CFR Part 104 and 105 – Maritime Security: Vessels and Facilities
- 33 CFR Part 160 – 96-hour advanced notice of arrival to the National Vessel Movement Center
- 33 CFR Part 165 – "Regulated Navigation Areas," as established by the U.S. Coast Guard (USCG)
- 46 CFR Part 154.22 – Certificates of Compliance Inspections
- USCG National Ballast Informational Clearinghouse reports on the LNG carrier's ballast management plan

Containment systems on LNG carriers were traditionally designed so that the rate of laden boil off gas was 0.15% per day. Improvements in containment technology and insulation has reduced the boil off rate to about 0.08% per day thus increasing transportation efficiency. For further efficiency, the LNG carriers are now fitted with reliquefaction systems such that any excess boil off is reliquefied back into the cargo tanks.

b. LNG Shipping in the United States

With the U.S. EIA projected estimate of 98 Mtpa of LNG production in the near term for export, and assuming a nominal ship capacity of

26 Navigation and Vessel Inspection Circular, no.01-2011, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2011/NVIC%2001-2011%20Final.pdf.

approximately 70,000 tonnes, the United States is likely to see more than 1,400 LNG cargo loadings per year. As a result, an increasing number of LNG carriers, of larger sizes, will be calling at U.S. ports and transiting coastal waterways. Most of these LNG ships will be sailing through deepwater navigation channels to LNG terminals in the U.S. Gulf Coast.

- Most if not all of these channels for ocean-going vessels have limited width and depths to accommodate the increasing size and capacities of LNG carriers as well as other ships, crude oil carriers, and tankers. The much higher anticipated traffic volume is also expected to cause congestion and delays.

- Fog events and other increasing severe climatic events in recent years have resulted in significant closures of industrial ports of the U.S. Gulf Coast leading to substantial disruption in the supply chain and associated revenue streams.

The USCG Commandant issued the 4-year 2018 USCG Strategic Plan,[27] in November 2018, where it recognized the need to be innovative and prepared to challenge existing processes and systems to maximize their support in an ever changing and evolving environment.

The LNG shipping and ship transfer operations have operated safely largely due to sharing best practices and standards through nonprofit trade organizations. Adhering to a combination of applicable international regulations, codes, and standards has led to the LNG shipping industry's exemplary safety record.

Finding: The United States is constructing new LNG terminals with robust safety and reliability designs, with strong quality assurance and self-assessments to ensure that all applicable international standards and guidelines are met (SIGTTO, OCIMF, GIIGNL, PIANC, etc.).

LNG marine facilities are highly regulated under several statutes, including the key standards from organizations cited above. These regulations cover a wide range of activities, from design and construction of terminals, safety equipment, operations, maintenance, training, security, fire protection, and firefighting. LNG vessels are regulated under 46 CFR 154 and Subchapter O requiring inspections to ensure that substandard vessels do not enter U.S. waters.

Part 127 also requires preparation of a Waterway Suitability Assessment (WSA) to demonstrate that the waterway is suitable for LNG carriers and passage can be safely handled, and the supporting marine infrastructure is adequate. The WSA also requires consideration of the risks regarding maritime safety and security and the consideration of risk management and mitigation strategies.

Local regulations, established by the USCG, may require a safety/security zone around the vessel during the transit or alongside—this is enforced through regulations either during the transit and/or alongside. Refer to 33 CFR Part 165 Regulated Navigation Areas.

Emergency Response Plans (ERPs) are developed and exercised routinely at LNG terminals. ERPs while typical for the LNG industry, are driven in the United States by regulations; 33 CFR Part 127.019 requires an Emergency Manual to be approved by the captain of the port.

c. LNG Transfer Technologies

Ship-to-shore operations and transfer of LNG is a tightly controlled process that is designed and conducted in accordance with the requirements and principles of SIGTTO for handling liquefied gases.[28] The LNG transfer operations must also comply with Part 127, and NFPA 59A requirements included by reference. The design incorporates emergency shut down systems that are intended to ensure adequate protection to the LNG carrier and the terminal, covering a wide range of possible upset conditions. The transfer of LNG between the

27 Coast Guard Strategic Plan 2018-2022, https://www.uscg.mil/Portals/0/seniorleadership/alwaysready/USCG_Strategic%20Plan__LoResReaderSpreads_20181115_vFinal.pdf?ver=2018-11-14-150015-323.

28 Society of International Gas Tanker and Terminal Operators. (2016). Liquefied Gas Handling Principles on Ships and in Terminals (4th ed.), London: Witherby Seamanship.

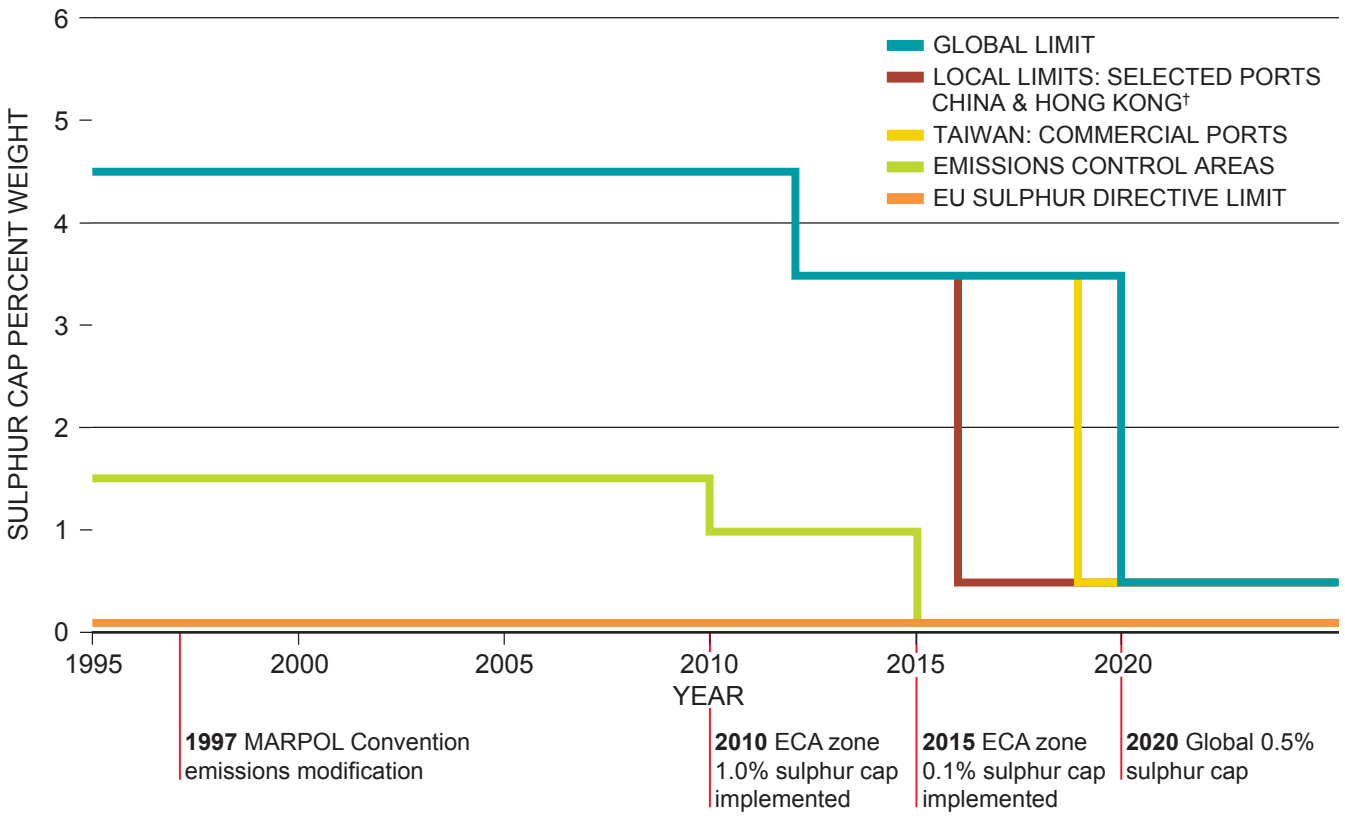
terminal and the carrier is via specialized marine loading arms that have swivel joints to accommodate a range of ship motions.

Integrated into the LNG loading arms are emergency release couplings that are intended to provide a clean break-away in case of emergency separation between ship and shore and if deployed would result in a negligible spill of LNG.

Effective from January 1, 2020 the IMO will require that all ships burn fuel with a sulfur content of no more than 0.5% m/m (mass by mass) compared to current levels of 3.5% m/m (mass by mass). Reduced sulfur limits have already been imposed on a number of emission control areas throughout the world. This new global emission level creates demand for cleaner burning fuel, or alternatively ships would have to install expensive cleaning systems for the exhaust gas to limit the emissions to the required amount (Figure 4-28). The annual global marine fuel demand is in excess of 400 million tons, with projected 2020 demand exceeding 500 million tons. As a result, the demand for low sulfur compliant fuel oil or LNG as a low sulfur fuel alternative for ocean-going vessels is expected to rise.

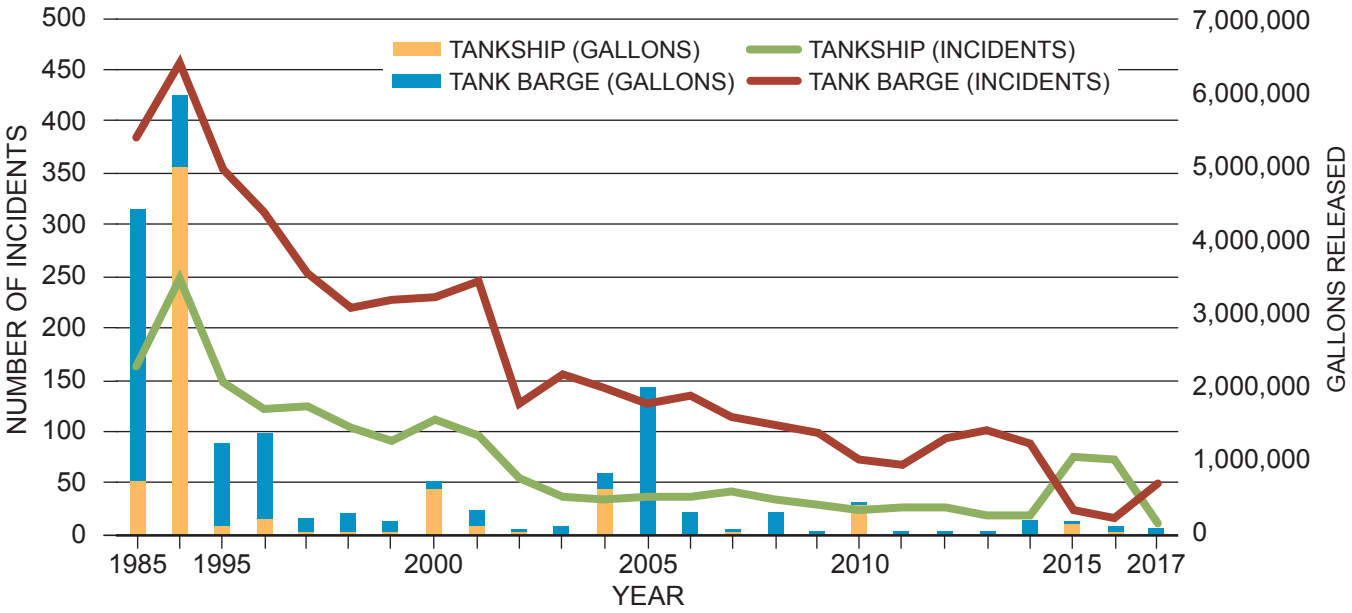
Advances in cryogenic flexible hose technology offers significant benefits for ship-to-ship transfer of LNG as well as potential risk mitigation for ship-to-shore transfer of LNG in exposed marine conditions. LNG ship-to-ship transfers are now considered "normal operations" with more than 2,000 completed inclusive of floating storage and re-gas operations.

Finding: Cryogenic flexible hose technology currently provides for safer bunkering of LNG carriers and other ocean-going vessels, given the increasing demands for cleaner burning fuels on ships but is not yet widely used in the United States.



† Key ports in Pearl River Delta, Yangtze River Delta, and Bohai Sea.
Source: BP, *MARPOL 2020 and Beyond*, October 2018.

Figure 4-28. *Global Sulfur Emissions Cap per IMO MARPOL Annex VI*



Notes: Incidents and gallons spilled

1995: Bouchard 155, Balsa 37, Maritrans Ocean 255 collision Tampa Bay: 336,000 gallons

1996: Barge North Cape grounding after tug scandia engine room fire: 828,000 gallons

2000: Tanker Westchester 11-28-2000 grounding: 567,000 gallons

2004: Selendang Ayu grounding: 337,000 gallons.

2005: DBL 152. > 1,900,000 gallons (ran over submerged oil rig)

2008: DM 932 tank barge collision with Tintomara New Orleans: 156,500 gallons

2010: Eagle Otome collision with Gull Arrow and collision with Dixie Vengeance: 462,000 gallons

2014: Kirby 27706/Summer Wind collision Galveston HSC: 168,000 gallons

2015: Carla Maersk/Conti Peridot HSC collision: 88,200 gallons

Source: U.S. Department of Transportation, Bureau of Transportation Statistics, "Petroleum Oil Spills Impacting Navigable U.S. Waters."

Figure 4-29. *Tankship and Tank Barge Incidents and Oil Spill Trends*

B. Marine Industry Technologies

1. Marine Industry Overview

The marine industry has been a leader in advancing safety performance improvements since 1990 and has made continued improvements in vessel safety and environmental performance since then. The total oil spill volume from tankers and barges in the U.S. navigable waters over the past decade through 2017 was 77% less than was spilled in the year 1990 (Figure 4-29). More than 50% of the oil spill volume during this decade ending in 2017 was caused by three collision events.[29]

Unintentional vessel impacts by collision, allisions,[30] and material failures are the leading accident types.[31] Deploying existing navigational technologies more consistently and broadly can be used to help reduce human-factor accidents. Additional advancements in navigational technologies should provide promising valuable tools for vessel captains to detect impact threats earlier to reduce risks. Application of these existing and new technologies to improve navigational safety performance is the primary focus for preventing marine accidents.

International shipping is a well-regulated industry encompassing international, national, local, and voluntary organizations operating under what is known as the Maritime Regulatory and Industry Framework (Figure 4-30). Maritime regulations have developed out of experience and tradition, along with lessons learned from marine incidents

29 U.S. Department of Transportation, Bureau of Transportation Statistics, "Petroleum Oil Spills Impacting Navigable U.S. Waters," https://www.bts.gov/content/petroleum-oil-spills-impacting-navigable-us-waters.

30 A collision is the impact of two moving vessels. An allision is the striking of a moving vessel against a stationary object. A grounding is the unintentional impact of a vessel with the bottom or side of a waterway.

31 U.S. Coast Guard–American Waterways Operators Annual Safety Report, July 31, 2018, p. 8-9, https://www.americanwaterways.com/sites/default/files/2018%20USCG-AWO%20Annual%20Safety%20Report%2031Jul2018.pdf.

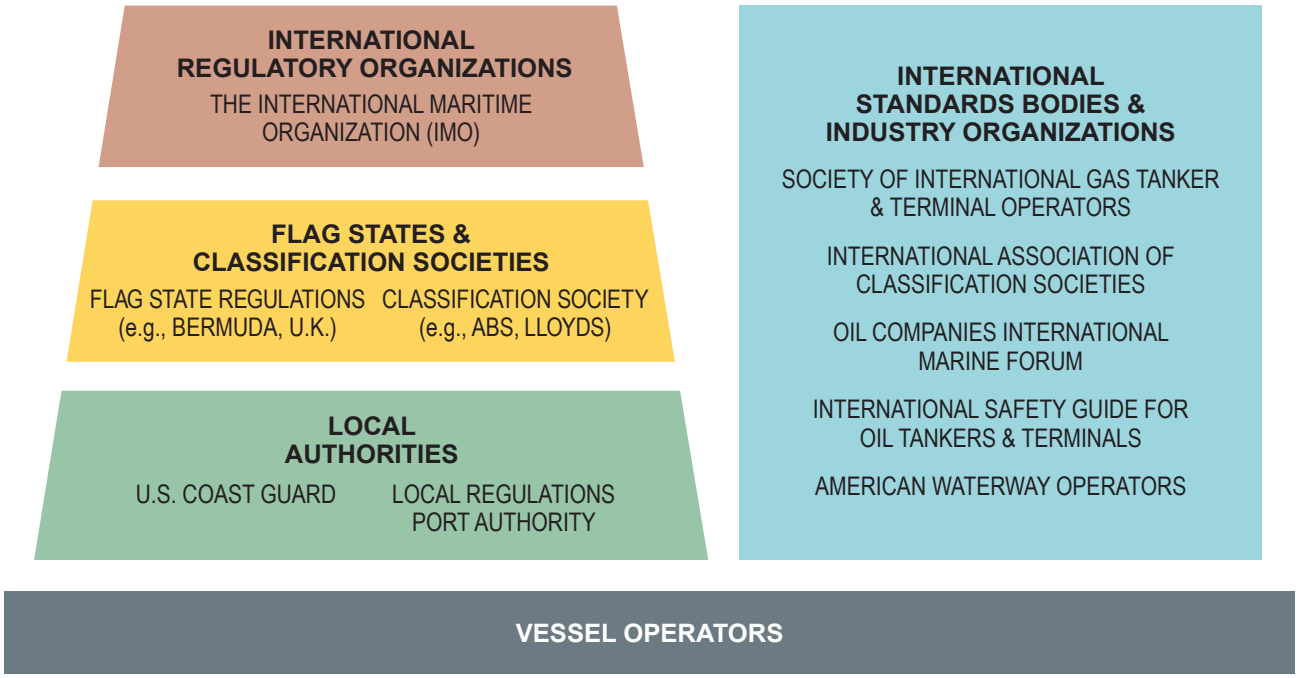


Figure 4-30. *Maritime Regulatory and Industry Framework*

throughout history. As such, these internationally trading vessels are subject to an ongoing and continuously evolving series of regulations and requirements to improve overall performance of the industry.

Figure 4-30 shows the Maritime Regulatory and Industry Framework to which international trading vessels operating in/out of U.S. ports are subject. The framework for U.S. inland and coastal fleets is significantly different primarily regarding regulatory training required to maintain licenses.

The shipping industry has achieved sustained improvement since 1991, after the onset of the Oil Pollution Act of 1990 and the industry's continuous improvement in the use of safety management systems, see Figure 4-29 and Figure 4-31. Tank vessel design and construction improvements such as double hulls have reduced the number and volume of oil spills. Routine frequent standardized ship inspections like Oil Companies International Marine Forum-Ship Inspection Report Exchange (OCIMF-SIRE) ensure vessel operators maintain robust preventive maintenance systems within their safety and quality management systems. Finally, vessel classification societies verify vessel structural and essential machinery integrity. All of these provide vessel charters with standard measurements of vessel and vessel operator quality to make informed decisions when chartering vessels. The oil and natural gas industry has supported regulatory entities to drive safety and environmental performance excellence in marine oil and natural gas transportation by implementing stringent industry standards.

Findings:

- Marine vessel safety has improved, largely from Oil Pollution Act of 1990 implementation and an industry commitment for vessel operators to implement and improve a robust safety management system. Vessel oil spills to water were reduced dramatically beginning in 1991 and have remained essentially flat through 2017 apart from infrequent high consequence events.
- Additional advancements in navigation technologies and training systems offer the best opportunities to mitigate marine vessel accidents.

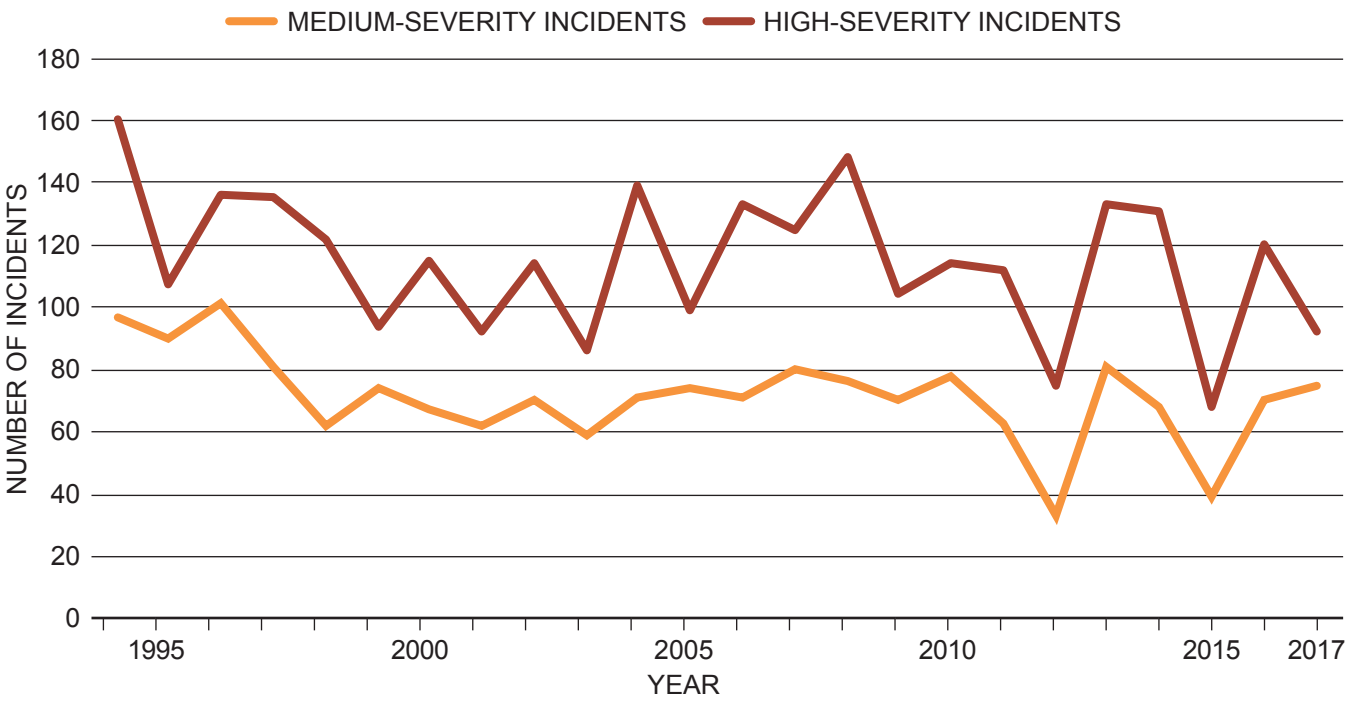
Important contributors to the marine transportation industry operational safety performance are classification societies, safety management systems, and OCIMF-SIRE vessel inspections.

Classification societies were initially started to provide an independent technical assessment for issuing insurance. Today the objective of ship classification is to verify the structural strength and integrity of essential parts of the ship's hull and its appendages, and the reliability and function of the propulsion and steering systems, power generation, and those other features and auxiliary systems that have been built into the ship to maintain essential services on board.

Classification societies aim to achieve this objective through the development and application of their own rules and by verifying compliance with international and national statutory regulations. A Classification Society may also be a Recognized Organization and perform statutory certification and services on behalf of a flag administration.[32] For example, in the United States, the American Bureau of Shipping is one of the classification societies that is authorized to act on behalf of the United States government to ensure that ships comply with international and flag state requirements for certification from initial design plans throughout the build, and then periodically throughout the life of the vessel.

An example of technology used to verify vessel structural integrity is nondestructive ultrasonic steel thickness measurements, which is a well-established and proven technology. The newest technologies are being approved by flag states on a case-by-case basis. Some of these technologies include unmanned aerial vehicle internal tank inspections in gas-free environments and advanced analytics based on remotely operated

32 Office of Design & Engineering Standards, "Status of Classification Society Recognition, ACP Participation, and Authorizations Delegated by the U.S. Coast Guard," revised April 5, 2018, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/Alternate%20Compliance%20Program/ClassSocietyAuths.pdf?ver=2017-10-18-091452-957.



Notes: Medium severity = Damage: $50,001 to $250,000, no injuries or deaths, and 11 to 1,000 gallons of oil spilled.
High severity = Damage: $250,001 or more, ANY injuries or deaths, and 1,001 or more gallons of oil spilled.

Figure 4-31. *U.S. Coast Guard–American Waterways Operators Severity Classes for Towing Vessel Incidents (including Barges)*

vehicles UWILD (underwater inspection in lieu of dry-docking) inspection.

Major oil companies remain committed to maritime safety and environmental protection by supporting continuous improvement efforts of IMO, OCIMF and the Society of International Gas Tanker and Terminal Operators. The International Safety Management Code (ISM) was the first safety management system standard introduced to the international marine oil and natural gas tanker industry in 1998 by the IMO. American Waterways Operators developed the Responsible Carriers Program in 1997 to provide the U.S. towboat and barge industry with guidance to develop SMS specifically for this segment of the industry. OCIMF released Tanker Management and Self-Assessment (TMSA) in 2004. TMSA builds upon ISM principles to provide a quantified measurement of a vessel operator's safety management systems level of attainment. The OCIMF TMSA program encourages companies to assess their own SMS against set key performance indicators and provides a minimum expectation (level 1) and three further levels of increasing best practice guidance, which companies may wish to apply to their SMS to improve ship management safety performance,[33] see Table 4-8.

2. Navigational Technologies to Address Human Factors

This section will focus on collision avoidance technologies that exist today. All the technologies discussed are collision avoidance aids that provide the vessel operator with critical information to make timely, informed navigational decisions. Navigation technology has made impressive advancements in the last 15 years providing commercial vessel operators with competent technology providing excellent reliable data to make sound navigation decisions. Vessel operators today are working in complex work environments, frequently involving high-stress decision-making while working irregular hours. Today, mariners have reliable technology to fix their position and track the course and heading of their vessels and of vessels within the range of automatic identification systems (AIS), radar, and very high frequency (VHF) broadcast of nearby vessels and U.S. Coast Guard.

Technologies and practices that address operations safety and integrity include U.S. Coast Guard Vessel Traffic Service, simulator training technologies, GPS, eATON, AIS, Electronic Chart Displays (ECS) and Information Systems (ECDIS), Automatic Radar Plotting Aid (ARPA), and E-Navigation. New technologies that address operations safety and integrity include the National Ocean Service (NOS) Physical Oceanographic Real Time System service that provides mariners with real-time oceanographic and weather data. AIS-based vessel-monitoring service can monitor and alert vessels that might be slowing or anchoring over pipelines by messaging "PIPELINE BELOW."

Findings:

- An effective means to expand capacity of ports will be the application of navigational technologies that would support reliable two-way channel traffic. Advancements in route planning and integrated navigational system technologies offer strong potential for maximizing channel capacity.
- Accurate underwater infrastructure mapping is important for vessels to identify nearby pipeline infrastructure. Where accurate map locations are not available, advancements in technologies that could recognize nearby pipeline infrastructure could provide an even higher level of safety. The National Oceanic and Atmospheric Administration, Coast Guard, and Army Corps of Engineers may offer collective expertise and information to better locate and alert mariners to underwater pipeline infrastructure.

Vessel Traffic Service. U.S. Coast Guard Vessel Traffic Service is a shore-based surveillance and communication system comprising a network of 12 centers around the country with the authority to ensure the safe, efficient movement of marine traffic in hazardous and/or congested waterways in the United States. The systems primary mission

33 Oil Companies International Marine Forum. (2017). Tanker Management and Self Assessment 3: A Best Practice Guide, London: Witherby Seamanship, p.4.

Management System Element	Technology Driver	Examples of Technology Applications
Leadership	Sets goals for improving performance that encourages the use of new technologies	Approve investment in technology to achieve safety and environmental excellence Vessel new-build program incorporates with the best available technology beyond statutory requirements Advanced employee training beyond the statutory requirements
Reliability Maintenance	Reputation, marketability	Computerized planned maintenance defect reporting system Condition-based maintenance technology examples to improve tank vessel reliability: • Hull stress monitoring • Ultrasonic steel thickness measurements • Vibration analysis • Intermediate engine top end inspection • Lube oil analysis • Vessel integrity robotics
Navigation Safety	Protection of people, environment, assets, and reputation	Advanced technology ship handling simulator and manned model training Navigational skills assessment and development programs using the newest simulator technologies and techniques
Cargo Operations		Collaborate with cargo Original Equipment Manufacturers to design new technology to improve safety performance and environmental care
Safety Management	The primary key to being successful in the marine oil and natural gas transportation industry	Enhanced safety management identifies or predicts operational, procedural, and environmental risk and threats before they occur. Adoption of new technology is a key component in the attainment of safety and environmental excellence
Measurement Analysis	Verify new technology is an improvement, identify opportunities to implement new technology	Measurement is essential to verify new technology is effective and indeed an improvement over previous technology

Table 4-8. *Safety Management System Elements that Support and Advance Technology*

is to reduce the risk of allisions, collisions, and groundings. Mission success requires the system to detect and resolve unsafe traffic situations in a timely manner.[34]

The 2016 National Transportation Safety Board (NTSB) assessment of the effectiveness of the U.S. Coast Guard Vessel Traffic Service (VTS) system[35] found that although the USCG system has enough authority to manage vessel traffic, many watch supervisors were reluctant to exercise their full authority and direct a vessel. Decisions on how and when to exercise VTS authority have been influenced by local stakeholders, economic considerations, and varying management practices at the 12 VTS centers.

During the years 2010 through 2014, an average of 18% of all reportable collisions, allisions, and groundings involving vessels meeting the requirements of a VTS user occurred while they

34 National Transportation Safety Board. (2016). "An assessment of effectiveness of the U.S. Coast Guard Vessel Traffic Service System." (NTSB/SS-16/01). Washington, DC. https://www.ntsb.gov/safety/safety-studies/Documents/SS1601.pdf.

35 Ibid.

were operating inside a VTS area. The most common causal factor assigned to these incidents by the Coast Guard was inattention errors by mariners involved, which suggests an opportunity exists for the VTS system to further reduce risk of these types of incidents by taking a more proactive role in traffic management. Collision, allisions, and groundings inside VTS areas during this 5-year period resulted in two fatalities, 179 injuries, and more than $69 million in damage to vessels, facilities, infrastructure, and the environment.[36] Three years after this NTSB assessment industry continues to experience significant accidents involving a commercial collision, allision, and groundings inside VTS areas. The 2016 NTSB assessment reported 14 findings and 21 recommendations that could improve this strategic navigation safety system.

The NPC recommends that the U.S. Coast Guard should:

- Fully implement NTSB recommendations that could improve VTS system ability to consistently achieve its primary mission to reduce the risk of allisions, collisions, and groundings within VTS areas.
- Implement additional traffic separation schemes and traffic rules such as speed limits, one way, and tethered escort tugs, particularly in non-vessel traffic service areas, to reduce marine traffic risk of allision, collision, and grounding.

3. Training and Development to Reduce Accidents Caused by Human Factors

As discussed in the previous section, marine vessels delivering energy have demonstrated sustained improvement in safety and environmental performance since 1991. Collision, allision, and grounding incidents have not improved at the same rate as other incident types. Safe navigation of marine vessels requires skilled, competent mariners working in bridge teams to safely direct vessel movement. Investigations of navigational incidents find human factors to cause, at least in part, a high percentage of these type of accidents.

U.S. maritime deck officer licensing is under the jurisdiction of the U.S. Coast Guard as described in 46 CFR Part 10. Deck officer candidates are required to pass a written exam after meeting experience and training requirements. Pursuing a career as a licensed deck officer can be accomplished by attending one of the U.S. maritime academies or by beginning as an unlicensed seaman and working up to licensed deck officer (hawsepiper).[37]

Developing competent deck officers with enough navigational skills to be in charge of a navigation watch has traditionally been the responsibility of the vessel operators. Traditional on-the-job navigational skill development works well for ships with larger crews that have bridge[38] teams supported by robust documented training programs. Smaller commercial vessels operating with one person on the bridge require navigation skills development as an extra crewmember training under the direction of a training master,[39] or a similar apprenticeship program. Similarly, training pilots who will need the navigational skills to direct the movement of vessels of all types and sizes will initially serve in an apprenticeship capacity. The apprenticeship may take several years to master the considerable skills and gain enough experience needed to be promoted to pilot.

Finding: The U.S. Coast Guard Deck Officer examination process for original and raise in grade licenses does not include a comprehensive simulator assessment to verify that candidates have the skills required to oversee a navigation watch.

36 Ibid., Executive Summary, paragraph 4.

37 Informal maritime industry term used to refer to a merchant ship's officer who began his or her career as an unlicensed merchant seaman and did not attend a traditional maritime college/academy to earn the officer license.

38 The *bridge* of a ship is the room or platform from which the ship can be commanded.

39 What is the difference between a ship's captain and a ship's master? In contemporary usage, not much, but historically, the titles represented quite distinct roles. Captain is more common in modern usage, but master is more historically accurate.

To illustrate human factors role in vessel collisions, the three collisions (Figure 4-32) occurred in the Houston channel in the area of Morgan's Point; all involved one of the meeting vessels sheering across the channel resulting in a collision. The two completed NTSB investigations, the 2011 Elka Apollon/MSC Nederland,[40] and the 2016 Conti Peridot/Carla Maersk[41] determined the probable cause to be pilot error for inadequately responding to bank effect[42] resulting in a collision.

- High Consequence Incidents in a Common Area include those incidents impacting people and the environment. All incidents occurred within a precautionary area in the Houston ship channel known as the Bayport flare.
  - The USCG has identified the vicinity of the Houston Ship Channel/Bayport Ship Channel intersection as a precautionary zone. This zone is codified in the Federal Code of Regulations 33 CFR §161.35. Precautionary zone is defined as "a routing measure comprising an area within defined limits where vessels must navigate with particular caution and within which the direction of traffic may be recommended."
- Ships unable to adequately respond to bank effect/bank cushion were being commanded (conned) by highly qualified federal/Texas State licensed pilots.
- USCG VTS did not exercise their authority to manage *vessel traffic*.

Subsequent pilot commission/pilot board investigations of these two incidents found no willful misconduct or actions against any pilots. The Conti Peridot/Carla Maersk investigation did propose several recommendations that included reminders to all pilots about communication and logging vessel deficiencies. The pilot board also recommended that the Conti Peridot pilot be assigned to a project tasked with developing a bridge resource management pilot training module that emphasizes the pilot leadership role on the bridge team.

Vessel operators have made significant improvements in conducting incident investigations over the years, but there is still a tendency to stop the incident analysis once some form of human error is identified at the sharp end.[43] This partial investigation does little to distinguish corrective, preventive, and opportunities for improvement at the organizational level to support the improvement of human performance.

The NPC recommends that the U.S. Coast Guard should extend requirements for vessels to be outfitted with automatic identification systems (AIS) to all commercial towing vessels with accurate tow-dimension input. In addition, operator training should be required on model-specific AIS technology in use.

Training program goals must be to prepare newly licensed deck officers to make consistent, sound, informed decisions in today's complex navigational environment. The training, licensing, and license renewal process should be robust to ensure that deck officers maintain their qualifications.

a. Existing Navigational Technologies

Marine navigation has undergone many different advances and developments over the last few decades, and out of that, many different technologies have emerged (Table 4-9). While advances in marine navigation technologies continue, many of the advancements address how these technologies are able to be connected and integrated with other technologies to provide the mariner with an enhanced situational awareness improving the safety of navigation.

40 National Transportation Safety Board, Marine Accident Report, "Collision of the Tankship Elka Apollon With the Containership MSC Nederland, Houston Ship Channel, Upper Galveston Bay, Texas, October 29, 2011," https://www.ntsb.gov/investigations/AccidentReports/Reports/MAR1202.pdf.

41 National Transportation Safety Board, Marine Accident Report, "Collision between Bulk Carrier Conti Peridot and Tanker Carla Maersk, Houston Ship Channel near Morgan's Point, Texas, March 9, 2015," https://www.ntsb.gov/investigations/AccidentReports/Reports/MAR1601.pdf.

42 "Bank effect" refers to the tendency of the ship's stern to swing toward the near bank when the ship is operating in a river or restricted waterway. "Bank cushion effect" is when a ship is near the bank, the water is forced between the narrowing gap between the ship's bow and the bank.

43 "Sharp end" refers to the people who were working at the time and in the place where the accident happened.

Elka Apolon – MSC Nederland 10/29/2011	Conti Peridot – Carla Maersk 3/9/2015	Genesis River – Towboat Voyager 5/10/2019
The National Transportation Safety Board (NTSB) determines that the probable cause of the collision between the *Elka Apollon* and the *MSC Nederland* was the failure of the pilot conning the *Elka Apollon* to appropriately respond to changes in bank effect forces as the vessel transited the Bayport flare, causing the vessel to sheer across the channel and collide with the *MSC Nederland*. Contributing to the accident was the combination of the narrow waterway, bank effects at the Bayport flare, and traffic density at the time, which increased the challenges in a waterway with a limited margin for error.	The National Transportation Safety Board determines that the probable cause of the collision between bulk carrier Conti Peridot and tanker Carla Maersk in the Houston Ship Channel was the inability of the pilot on the Conti Peridot to respond appropriately to hydrodynamic forces after meeting another vessel during restricted visibility, and his lack of communication with other vessels about this handling difficulty. Contributing to the circumstances that resulted in the collision was the inadequate bridge resource management between the master and the pilot on the Conti Peridot.	The National Transportation Safety Board is investigating the liquid propane gas carrier Genesis River, collided with the towboat Voyager as it pushed two 25,000-barrel tanks barges of reformate, a high-octane gasoline blend product near Bayport, TX on 10 MAY 2019. One barge capsized and the other was split open by the impact, releasing part of its cargo into the waterway, causing officials to close the Houston Ship Channel.

Figure 4-32. *Examples of Marine Incidents*

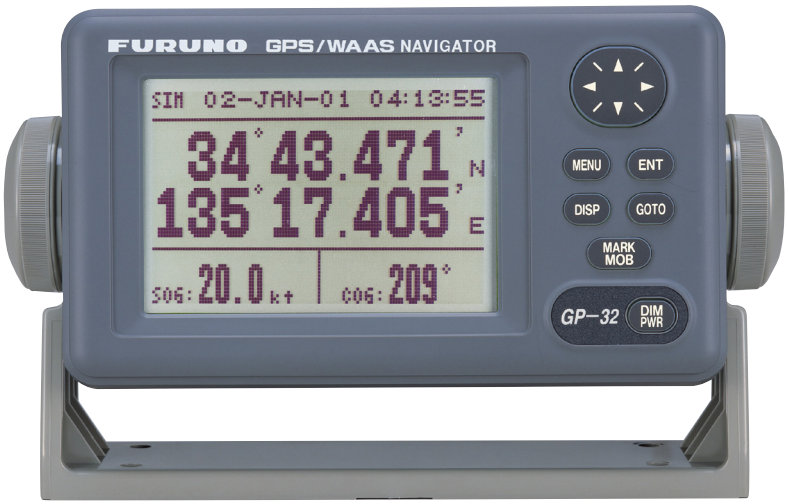
	Navigational Technology	Highlights
 https://www.furuno.com/en/products	Global Navigation Satellite System	• GPS receivers operate continuously and can receive position and time with high accuracy, reject wrong measurements, and estimate receiver speed and direction. GPS transmitters emit positional information to integrated equipment on average every 2 seconds.

Table 4-9. *Marine Navigation Technologies*

	Navigational Technology	Highlights
 https://www2.vespermarine.com/products	Automatic Identification System (AIS)	• AIS transceivers automatically broadcast information via a VHF transmitter built into the transceiver. • AIS information broadcasted include: Heading information and course and speed over ground, rate of turn, angle of heel, pitch and roll, and destination and estimated time of arrival. • AIS can be a means to transmit information to ships in port or underway that contributes to safety-of-navigation.
  https://www.furunousa.com/en/products/commercial	Electronic Chart Display and Information System (ECDIS)	• Navigational chart system used by commercial vessels. • ECDIS greatly eases the navigator's workload with its automatic capabilities such as route planning, route monitoring, automatic estimated time of arrival computation, and electronic navigation chart updating. • ECDIS provides many other sophisticated navigation and safety features, including continuous data recording for later analysis.

Table 4-9. *(continued)*

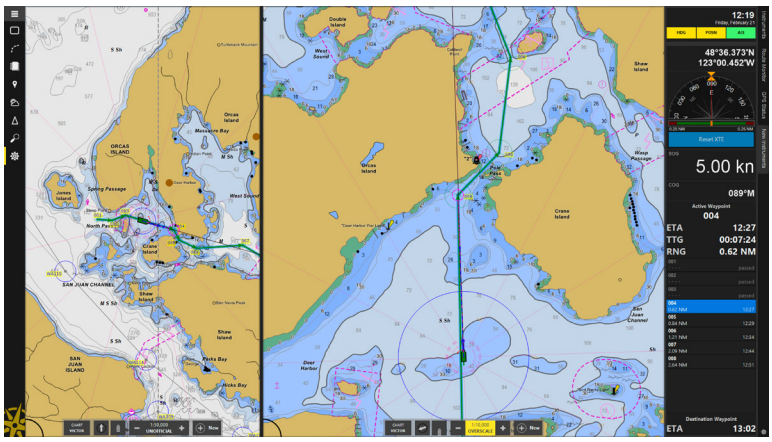
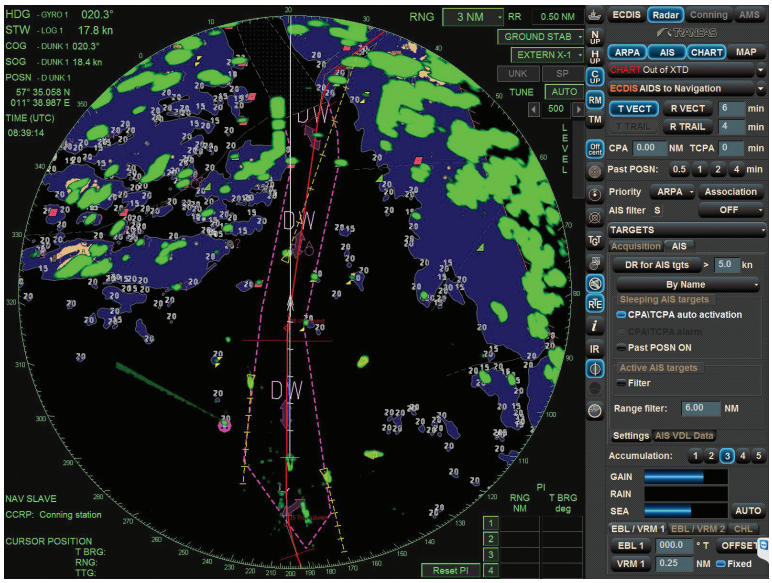
	Navigational Technology	Highlights
 https://www.rosepoint.com/rose-point-ecs/	Electronic Chart Display (ECS)	• ECS system is fundamentally capable of all the same functions as an ECDIS system; however, IMO refers to systems not meeting IMO Regulation. • Inland towing vessels by nature of design that do not leave U.S. waters are not currently subject to any of the governance of IMO or Safety of Life at Sea SOLAS are not required to adhere to any of the electronic charting requirements.
 https://www.furunousa.com/en/products/commercial	Automatic Radar Plotting Aid (ARPA)	• A marine radar with ARPA capability can create tracks using radar contacts. • The system can calculate the tracked object's course, speed and closest point of approach, thereby knowing if there is a danger of collision with the other ship or landmass. • The system can acquire automatically and constantly monitor many targets, plot their speeds and courses, present these as vectors on the display screen, updated with each sweep of the antenna, and calculate their closest points of approach to own ship and the time before that will occur.

Table 4-9. *(continued)*

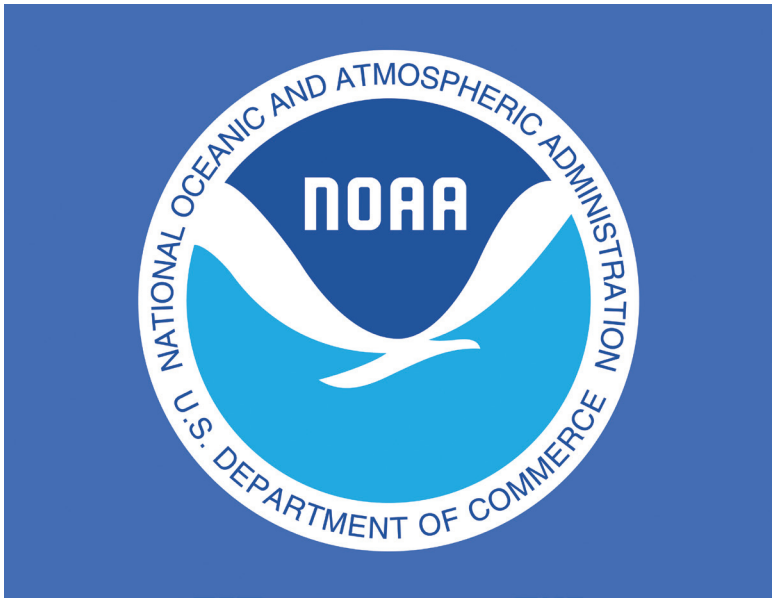
	Navigational Technology	Highlights
 https://tidesandcurrents.noaa.gov/ports.html	National Ocean Service (NOS)	• NOS is responsible for providing real-time oceanographic data and other navigation products to promote safe and efficient navigation within U.S. waters. One component of NOS's integrated program for safe navigation is the PORTS data system. • PORTS is a decision support tool that improves the safety and efficiency of maritime commerce and coastal resource management through the integration of real-time environmental observations, forecasts, and other geospatial information.

Table 4-9. *(continued)*

The deployment of PORTS at Corpus Christi demonstrates how the LNG shipping industry has worked with the National Oceanic and Atmospheric Administration to implement a system that meets the needs of all stakeholders toward improving the safety of navigation.

The NPC recommends that local port authorities should adopt National Ocean Service (NOS) real-time oceanographic data and other navigation products to promote safe and efficient navigation within U.S. waters. One component of NOS's integrated program for safe navigation is the PORTS data system.

Maritime simulators have been used in the United States to complete the International Convention on Standards of Training, Certification, and Watchkeeping training for many years. Training facilities require USCG approval before offering this regulatory training. Many vessel operators are utilizing simulators (Figure 4-33) to determine if individual mariners have enough navigation skills to be competent officers in charge of a watch and develop personal remedial training to correct performance deficiencies.[44] The additional benefit of simulator training is the ability to provide stress exposure training to provide simulated experience to begin to improve human performance in emergencies.[45] Simulation software is being developed to teach best practice for ship maneuvering and improve vessel handling. Advances in the software are delivering new aspects to training, such as multi-vessel operations and equipment interaction. Hydrodynamic model maneuvering simulation and three-dimensional physical models are part of the next generation of simulators.

Electronic aids to navigation (eATON) are an electronic system of marking channels that update

44 "The 21st Century Maritime Workforce: Recruiting and Training the Next Generation," The Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council, January-April 2017, http://digitaleditions.walsworthprintgroup.com/publication/?i=408860#.

45 Gregory, D., and Shanahan, P. (2017). Being Human in safety critical organizations, TSO. Norwich: UK.

Source: Wärtsilä Corporation.

Figure 4-33. *Marine Training Simulator*

AIS. USCG plans to deploy a risk-based mix of traditional aids to navigation and eATON.

A virtual aid to navigation itself does not physically exist unlike buoys and beacons but comprises a signal broadcast to a location in a waterway. It can be described as digital information transmitted from an AIS station located elsewhere for a specified location without being itself present in that specified location, an electronic virtual marker of hazards.

A virtual aid to navigation can be used in situations when it is not practically possible to equip, or due to the limitation of time a physical aid to navigation such as a buoy, beacon or a lighthouse cannot be set up. In this case, an AIS coast station can be configured to send information to mark its location with a virtual aid to navigation, providing navigating officers with updated information real time.

E-navigation (Figure 4-34) defined by the IMO as "the harmonized collection, integration, exchange, presentation and analysis of maritime information onboard and ashore by electronic means to enhance berth-to-berth navigation and related services, for safety and security at sea and protection of the marine environment."

The strategic implementation plan has five prioritized e-navigation solutions:[46]

- Improved, harmonized and user-friendly bridge design
- Means for standardized and automated reporting
- Improved reliability, resilience, and integrity of bridge equipment and navigation information
- Integration and presentation of the available information in graphical displays received via communication equipment
- Improved communication of VTS service portfolio (not limited to VTS stations)

46 Annex 7, Draft E-Navigation Strategy Implementation Plan, http://www.imo.org/en/OurWork/Safety/Navigation/Documents/enavigation/SIP.pdf.

E-Navigation is designed to provide navigators with smart, easy to understand navigational safety information using existing electronic navigation equipment. In the United States, both government and industry groups are working on the implementation. Details of the implementation timeline is uncertain currently.

The NPC recommends that the U.S. Coast Guard should require that all vessels that are required to carry AIS "type A" under 33 CFR 164 should also be required to be fitted with electronic chart systems. Additionally, the U.S. Coast Guard should require that chart system training is specific to the technology model being used.

C. Rail Industry Technologies

1. Rail Industry Overview

Freight railroads move vast amounts of products critical to commerce and quality of life, including products such as fertilizer, chlorine, ethanol, and petroleum products (e.g., crude oil), which are all classified as hazardous materials. Technology helps railroads achieve increasing levels of safety performance and minimize their impact on the environment and helps the United States maintain a competitive edge in the global economy.

Transport of these commodities is subject to strict oversight by the Federal Railroad Administration (FRA), PHMSA, and Department of Homeland Security (DHS). Railroads work in partnership with these agencies, shippers, and other local, state, and federal entities on train routing, security, tank car design, emergency response, and more.

Railroads and shippers are committed to safe operations and work diligently to secure and transport every commodity incident-free. The resources, operating practices, and policies surrounding the rail transport of hazardous commodities are categorized in the focus areas of accident prevention, accident mitigation, and emergency response.

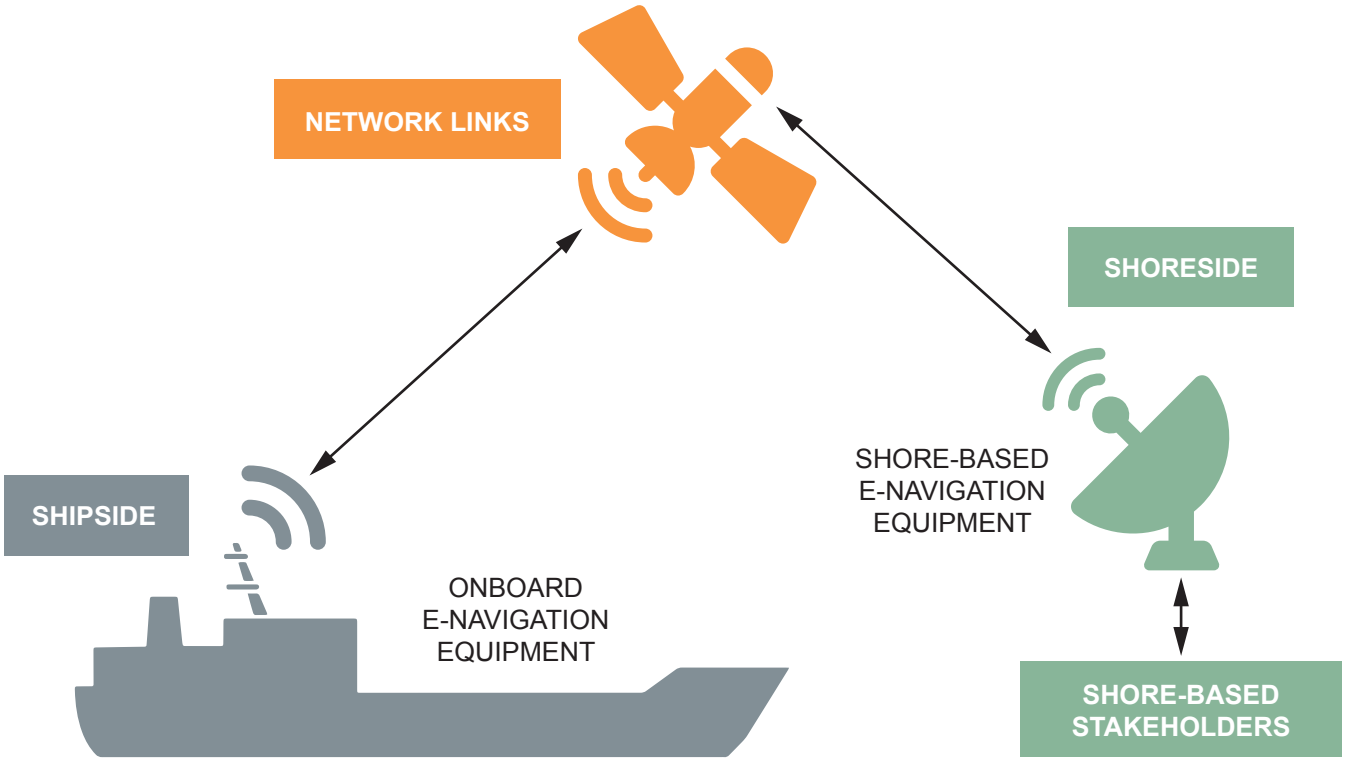


Figure 4-34. *E-Navigation System*

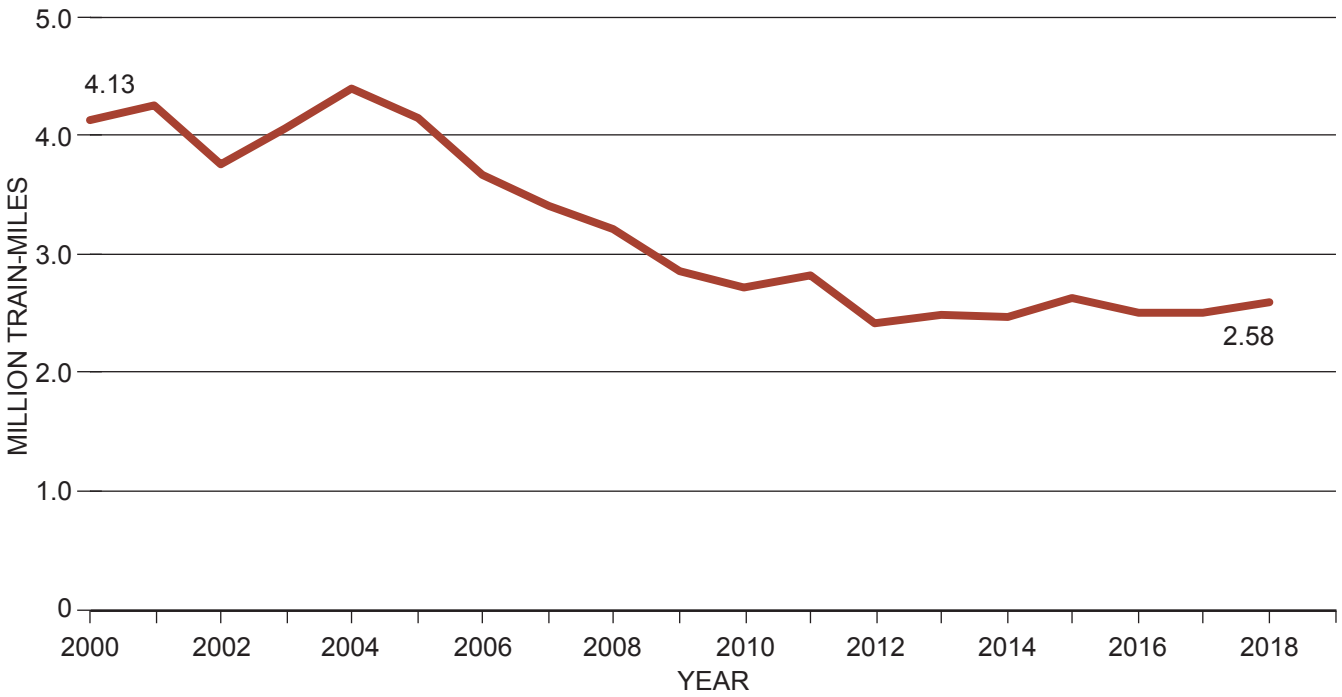
FRA safety statistics demonstrate the rail industry's commitment to safety and show a 37% decrease in train accidents since 2000 (Figure 4-35). By many measures, recent years have been the safest in history. Railroads today have lower employee injury rates than most other major industries. Further improvements in railroad transportation safety are possible by harnessing advancements in technology development.

The rail industry continues to have a long-term goal of zero injuries and accidents. To accomplish this goal, freight railroads have taken a strategic approach, focusing on the leading causes of incidents—track, equipment, and human factors—while harnessing innovative solutions to reduce accidents. The railroad industry has implemented additional standards and processes, including the use of new technologies, to address the causal factors related to these accidents. These technologies are further discussed in this section.

Finding: Railcars transporting petroleum-based commodities safely reach their destinations with high reliability. Infrequent accidents do occur. The railroad industry has implemented additional standards, processes, and new technologies to address the causal factors related to these accidents.

To further reduce train accidents, the industry is focused on the three primary areas of railroad management (Table 4-10): (1) the track structures that provide the ground support of railroad operations, (2) the equipment that powers the trains to carry the commodities, and (3) the people involved with operating the trains. Looking at each of the three primary areas of focus provides examples of the industry's efforts to improve railroad safety, both from a historical and forward-looking perspective.

The railroad industry is developing and advancing technologies to further improve safety performance by pursuing the three primary cause categories of accidents. These technology areas of development include enabling railroads to inspect track and equipment faster, more frequently, and more reliably as well as technologies



Note: Excludes grade crossing accidents. Data for 2018 are preliminary as of March 2019.
Source: Federal Railroad Administration, Office of Safety Analysis, "Accident Trends – Summary Statistics."

Figure 4-35. *Accidents per Million Train-Miles Have Been Reduced 37% since 2000*

	Percent of Total Train Accidents (2018)	Accident Rate Reduction Since 2000	Performance Improvement Drivers
Track	29%	48%	• Record investment in track maintenance and replacement • Improved component design and development • Use of advanced inspection technologies
Equipment	14%	30%	• Locomotive and railcar design standards • Advanced equipment inspection technology • Industry-wide asset management programs
Human Factor	37%	40%	• Rigorous employee training • Safety management system programs • Fatigue management programs • Deployment of technologies such as positive train control
Miscellaneous	20%		• Focus on grade crossing and trespassing incidents through education, engineering and enforcement initiatives and activities. • Identification and communication of weather-related activity (e.g. wind, flooding, slides) through technology.

Table 4-10. *Rail Industry Safety*

that can assist rail employees in making better decisions by giving them insight well beyond human limitations.

Railroads, government agencies, shippers, and suppliers coordinate activities, and conduct their own programs, to develop technology to address opportunities in the industry. For instance, the FRA's Research, Development & Technology (RD&T) employs basic and applied research, and development of innovations and solutions to ensure the safe, efficient, and reliable movement of people and goods by rail. The FRA's RD&T program is founded on an understanding of safety risks in the industry. Key strategies include stakeholder engagement and partnerships with other researchers, prioritization of projects, and conducting research through cost-effective procurement. The FRA has a specialized focus around the safe transportation of hazardous materials. The increased harmonization of regulations, better data, and new technology, and cooperative efforts between shippers, carriers, tank car builders, and government agencies influence safe transport practices for hazardous materials.

Additionally, many of the industry's technological advancements are developed at the Transportation Technology Center (TTC). At present, the Association of American Railroads (AAR) manages this facility for the FRA under a care, custody, and control agreement. This world-class transportation research testing facility and organization provides emerging technology solutions for the railway industry throughout North America and the world. Research and development programs converge at this facility headquartered in Pueblo, Colorado. The site includes extensive track facilities (approximately 48 miles), state-of-the-art laboratory facilities, and an accompanying engineering and support staff. These unique assets enable the testing of locomotives, railcars, track components, and signaling devices. Additionally, one-of-a-kind test machines and computer models provide research engineers with the tools to test and evaluate railroad products and/or improvement concepts. Research initiatives to improve the safety, reliability, and efficiency of rail transportation is prioritized through a strategic research initiative process.

Finding: Further improvement in advancing technological innovations will rely on effective collaboration between shippers, regulators, and the industry.

The power and promise of rail technology will become even more evident in the years ahead as the railroad industry seeks to apply technology solutions to their ultimate goal—an accident-free future. The industry is on the verge of an exciting new era of innovation. Advanced algorithms and data analysis software will enable railroads to harness massive amounts of data collected nationwide to enhance safety, reliability, and customer service. Next-generation automation technology will reduce the impact of human error and limitations.

> "Regulators should start with the premise that technological progress can solve many problems. They should therefore welcome technological development, and act to speed the process of making it safe and reliable and introducing it into markets, rather than act as gatekeepers who slow the pace of innovation."
>
> —Joe Kennedy, Information Technology & Innovation Foundation

Looking ahead, federal regulations should both permit and encourage the railroad industry to continue to develop and deploy these vital technologies. Realizing the full benefit of future technologies will require modernization of regulatory processes from the current historical perspective to one which actively encourages the development of safe and productive technological solutions.

Finding: Technological innovations will require continued modernization of regulatory processes from prescriptive methods to a system that accommodates and incentivizes the development and deployment of new advanced technological solutions.

A regulatory environment based on today's technology—and flexible enough to embrace future innovations—will enable the railroad industry to meet the challenges of today and tomorrow. Meaningful dialogue with railroads and other interested parties is essential to identify beforehand any specific safety concerns that a new rule is meant to address and ensure the new rule would address the safety concern efficiently and effectively.

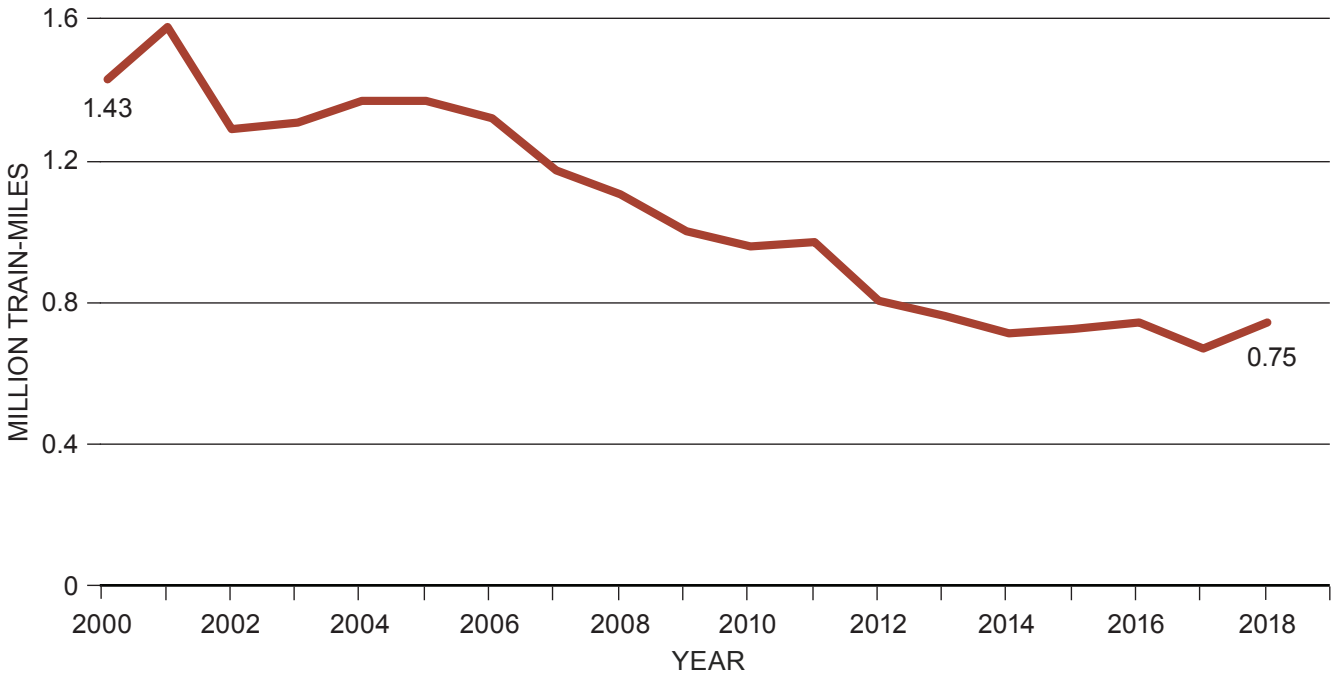
The NPC recommends that Federal Railroad Administration should include the following considerations in their rulemaking and guidance documents:

- Avoid locking in existing technologies and processes so that new innovations, including new technologies, that could improve safety and efficiency are not stifled.
- Validate results with technical data and ensure benefits of a new rule exceed costs with supporting performance metrics.
- Give meaningful opportunity to review and comment on new rules.
- Track and Structures.

Preventing accidents starts with sound engineering, robust construction practices, and the use of high-quality materials. This includes advanced railroad track construction and maintenance technologies and leveraging technologies to ensure the integrity with those components. Supplementing those sound construction practices are asset integrity systems that involve inspection technologies of track and structures, and the utilization of software and algorithms to evaluate the collected data. Railroads use these evaluations to identify potential problems before they occur and proactively schedule maintenance. By utilizing these construction, maintenance, and inspection technologies, railroads have achieved a nearly 50% reduction in track-caused rail accidents since 2000 (Figure 4-36).

a. Construction and Maintenance

The components of railroad track (the rails, crossties, fasteners, and ballast) are the foundation of the 135,000+ miles of the U.S. freight rail network. Together, the tracks support the trains



Note: Excludes grade crossing accidents. Data for 2018 are preliminary as of March 2019.
Source: Federal Railroad Administration, *Railroad Safety Statistics: Annual Report*, 2008, 2009, and 2010.

Figure 4-36. *Track-Caused Accidents per Million-Train Miles*

carrying thousands of tons as they move across the country.

- Rails – Steel has been the foundation of railroads since the inception of the industry. Improved metallurgy and improved fastening systems have improved steel integrity and enhanced track stability, reducing the risk of track failure that can lead to accidents.
- Ties – Wood is the predominant material used to support the rails, but ties made of composites, concrete, and other materials are used in some rail applications as well. Technology investments in improving the quality and life are important to continued safety improvements and reduced life cycle costs.
- Ballast – The ballast supports the base track structure. Varying rock type and maintenance of ballast structures is key to maintaining the support and integrity of the rail and ties.

b. Asset Integrity

Tiny flaws imperceptible to the human eye can lead to accidents, so railroads rely on technology such as ultrasound and radar to look deep inside rail, crossties, and other elements of the track structure. In addition, systems such as unmanned aerial vehicles (drones) and inspection vehicles are used to search for flaws in tracks. The information provided by these technologies allows railroads to identify potential problems, proactively address issues, and schedule maintenance.

- Defect detector vehicles detect internal flaws in rails. The AAR and the FRA fund a rail defect test facility at the TTC that tests new methods for detecting rail flaws. A prototype of the world's first laser-based rail inspection system is being developed and tested at TTC. In addition, a new in-motion ultrasonic rail joint inspection system developed at TTC is being tested on a major railroad.
- Advanced track geometry cars (Figure 4-37) use sophisticated electronic and optical instruments to inspect track alignment, gauge, curvature, and other track conditions. Railroads have developed onboard computer systems that provide even more sophisticated analyses of track

Source: BNSF.

Figure 4-37. *Track Geometry Car and Sensors*

geometry and predict the response of freight cars to track geometry deviations. This information helps railroads determine when track will require additional maintenance.

- Ground-penetrating radar and terrain conductivity sensors are being developed that will help identify problems below the ground (such as excessive water penetration and deteriorated ballast) that hinder track stability.

- Unmanned aerial vehicles are being deployed by freight railroads for a variety of safety and environmental purposes. In remote areas, these systems are being employed to explore thousands of miles of track to ensure that freight trains continue to safely traverse challenging terrain. Unmanned aerial vehicles are also being used to inspect bridges and telecommunications infrastructure.

- Track stability and washout detection systems are deployed in potentially unstable geographical areas where tracks are exposed to natural hazards such as slides resulting from slope failures and washouts, which causes failure of a track's ballast and substructure. While those events are rare, they represent a high potential of very severe consequences to railroads. These systems detect the presence of an obstruction or hazard when electrical conductors are interrupted, which can provide warning to train personnel through a signal system.

Enabled by next-generation technology and modifications to federal regulation, railroads will be able to conduct safety inspections more frequently, detect more flaws more reliably, and respond more quickly to remediating potential defects.

2. Equipment

Similar to track and structures, preventing equipment-caused accidents starts with sound design engineering, robust construction practices, improved inspection and securement processes, and the use of high-quality materials. These areas are further supported with railcar inspection technologies and data processing support systems. By focusing on these segments, railroads have realized a nearly 30% reduction in equipment-caused rail accidents since 2000 (Figure 4-38).

a. Construction and Maintenance

Freight cars come in a variety of sizes and types, but tank cars are by far the most important type for the transport of crude oil and refined petroleum products. The North American tank car fleet consists of more than 400,000 cars; nearly all of them are owned by rail customers and leasing companies, rather than by railroads themselves.

U.S. federal regulations pertaining to tank cars that carry crude oil and other petroleum products are set by PHMSA, an agency within DOT. In addition, the industry advocacy group's AAR Tank Car Committee sets rail industry standards regarding how tank cars used in North America are designed and constructed.[47]

For many years, better tank car design standards have been a key focus of enhancing crude oil transport safety. In May 2015, DOT released a final rule for "Enhanced Tank Car Standards and Operational Controls for High-Hazard Flammable Trains." This rule set forth new, tougher tank car standards and generally applies to high-hazard flammable trains (HHFT). HHFTs are defined as trains with either a continuous block of 20 or more tank cars loaded with a flammable liquid or at least 35 tank cars loaded with a flammable liquid dispersed throughout the train.

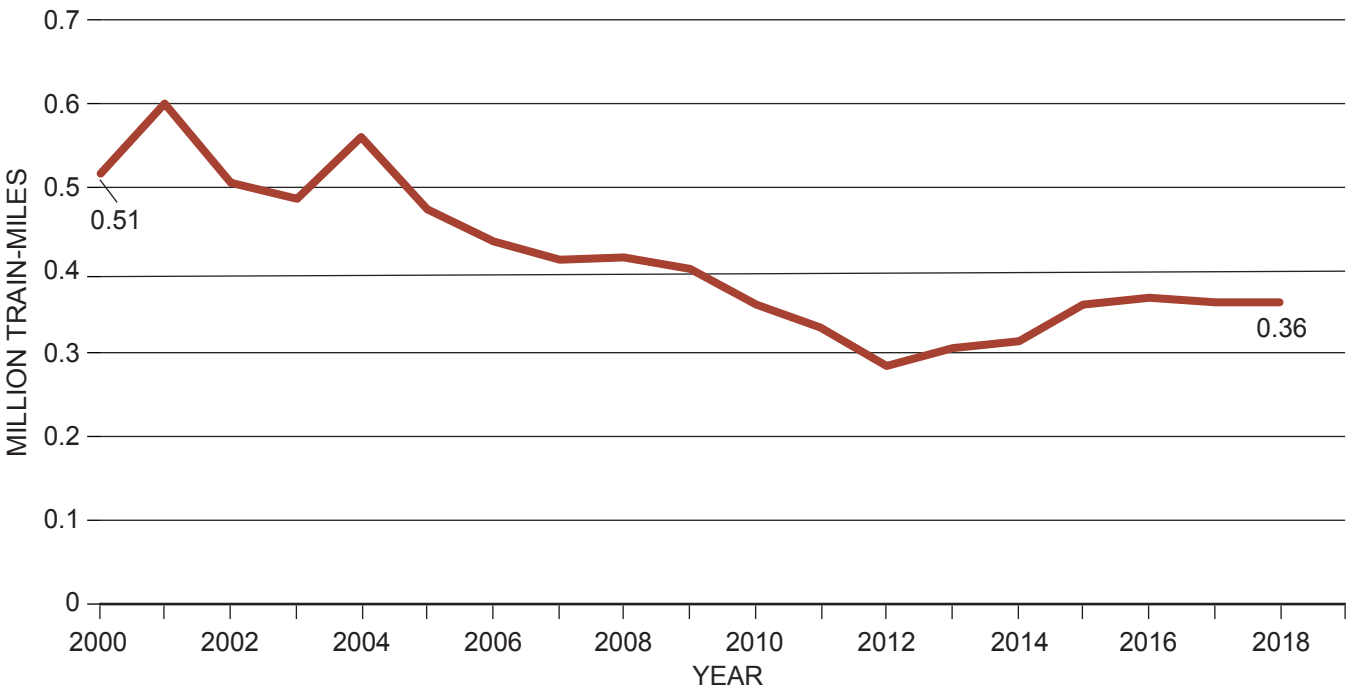
47 The committee comprises railroads, tank car owners and manufacturers, and rail hazmat customers with active participation from DOT, Transport Canada, and the National Transportation Safety Board.

According to the final rule, tank cars built after October 1, 2015, used to transport flammable liquids, including crude oil and ethanol, in HHFTs must meet the following provisions:

- New tank cars constructed after October 1, 2015, are required to meet enhanced DOT Specification 117 design or performance criteria for use in an HHFT.
- Existing tank cars must be retrofitted in accordance with the DOT-prescribed retrofit design or performance standard for use in an HHFT.
- Retrofits must be completed based on a prescriptive retrofit schedule. The retrofit timeline focuses on two risk factors, the packing group and differing types of DOT-111 and CPC-1232 tank car.

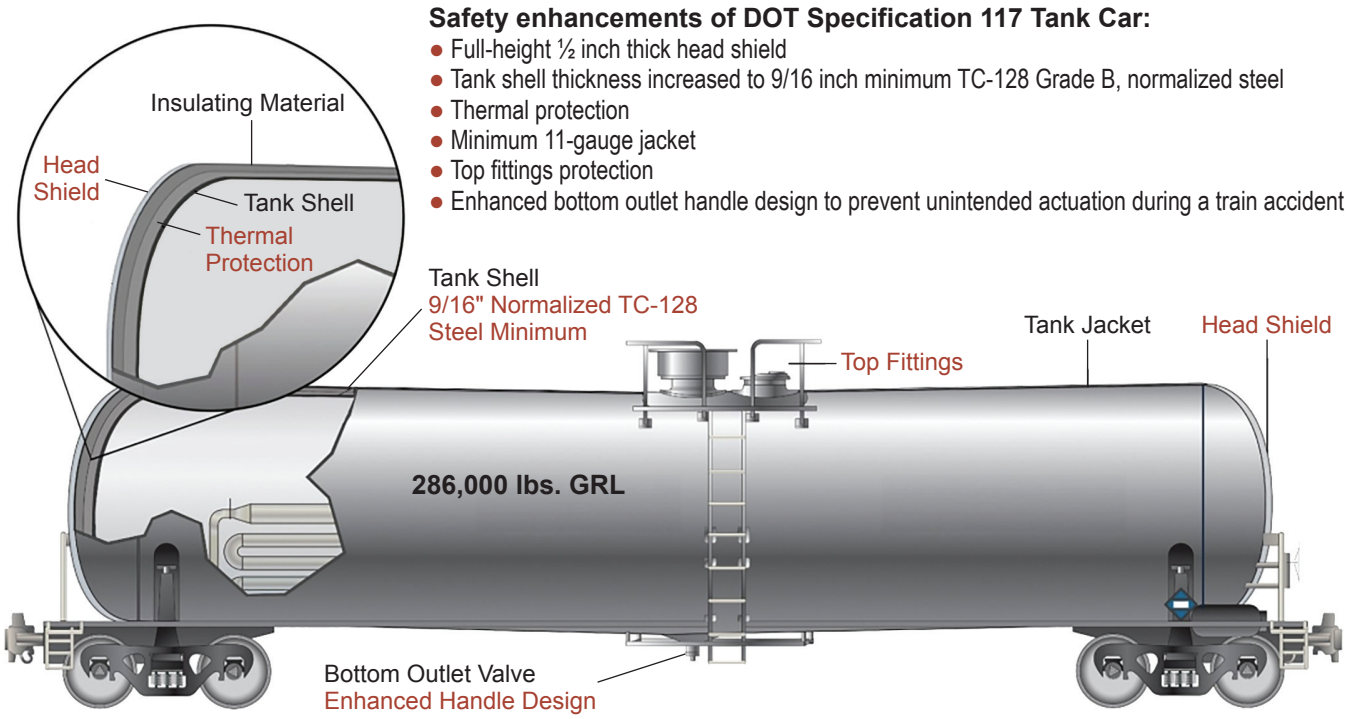
The DOT calls tank cars that meet these standards a DOT-117 car (Figure 4-39).

The tank car design, construction, and resulting robust improvement to the DOT-117 standard translates into a 50% to 70% lower conditional



Note: Excludes grade crossing accidents. Data for 2018 are preliminary as of March 2019.
Source: Federal Railroad Administration, Railroad Safety Statistics: Annual Report, 2008, 2009, and 2010.

Figure 4-38. *Equipment-Caused Accidents per Million Train-Miles*



Source: U.S. Department of Transportation.

Figure 4-39. *Example of DOT-117 Tank Car*

probability of release (CPR) in the event of an accident compared to the DOT-111 model that was most prevalent in crude oil movements previously. The CPR measure estimates the expected number of lading releases, given a tank car design and a number of carloads shipped, by comparing various tank car packaging options. This measure can be part of a larger risk analysis of a locality, route, operation, or annual traffic, but notably it is not a reliable predictor for one specific accident.

The May 2015 rule also requires that existing tank cars used to carry flammable liquids but that do not meet the new standards, must be retrofitted to higher standards if they are to continue to carry flammable liquids. The phaseout is underway ensuring that after May 1, 2025, all tank cars used to carry crude oil will have to meet or exceed the DOT-117 standards.

The primary focus on reducing incidents in the rail transport of petroleum products relies on prevention and mitigation strategies discussed in this section. The increasing shipments of tight oils transported by rail over the last decade coupled with high-profile crude oil train accidents, raised questions about the role of oil properties in affecting the severity of related crude oil fires.

A recently released report[48] by Sandia National Laboratories of a DOE/DOT/Transport Canada Crude Oil Characterization Research Study detailed an experimental study of physical, chemical, and combustion characteristics of selected North American crude oils. The crude oil samples used for the experiments were obtained from several U.S. locations, including tight oils from the Bakken region of North Dakota and Permian region of Texas, and a conventionally produced oil from the U.S. Strategic Petroleum Reserve stockpile. The results indicate that all the oils tested have comparable thermal hazard distances and the measured properties are consistent with other alkane-based hydrocarbon liquids. The similarity

48 Luketa, A., Blanchet, T. K., Lord, D., Hogge, J., Cruz-Cabrera, A. A., and Allen, R. (2019). "Pool Fire and Fireball Experiments in Support of the U.S. DOE/DOT/TC Crude Oil Characterization Research Study," U.S. Department of Energy, Office of Scientific and Technical Information, https://www.osti.gov/servlets/purl/1557808.

of pool fire and fireball burn characteristics pertinent to thermal hazard outcomes of the three oils studied indicate that vapor pressure is not a statistically significant factor in affecting these outcomes. Thus, the results from the study did not support creating a distinction for crude oils based on vapor pressure with regards to these combustion events.

b. Asset Integrity

Using smart sensors, advanced analytics software, and industry-wide data sharing, railroads and shippers currently monitor the health of rail equipment frequently if not continuously. Detectors positioned along track use multiple technologies—such as infrared and lasers—to assess the condition of bearings, axles, wheels, and springs as trains pass.

Existing railroad equipment asset integrity sensor and detector technologies include the following:

- Wayside detectors identify defects on passing rail cars—including overheated bearings and damaged wheels, dragging hoses, deteriorating bearings, cracked wheels, and excessively high and wide loads—before structural failure or other damage occurs. Some of the newest wayside detectors use machine vision and digitized images to perform high accuracy inspections of car safety features (such as handholds, ladders, and uncoupling levers) and car underframes. Following tests at TTC, one railroad recently installed a system that uses ultrasonic probes to inspect wheels of moving trains.
- Wheel profile monitors use lasers and optics to capture images of wheels. The images show if wheel tread or flanges are worn and, consequently, when the wheels should be removed from service.
- Trackside acoustic detector systems use acoustic signatures to evaluate the sound of internal wheel bearings to identify those nearing failure. These systems supplement or replace existing systems that measure the heat bearings generate to identify those in the process of failing.
- Wheel temperature detectors, using infrared technology, scan locomotives and freight cars on passing trains to determine if their brakes are properly set or are applied when they should not be.
- Because a relatively small percentage of freight cars cause an inordinately high percentage of track damage and have a higher than usual propensity to derail, TTC is working on ways to use truck performance detectors and hunting detectors[49] to identify poorly performing freight cars.
- Nondestructive inspection techniques that use fluorescent magnetic particles to identify defects in rail car castings and coupling systems are being developed.

To provide a view of the health of rolling stock available to all stakeholders, particularly to the railroads on which the cars and locomotives are operating, the rail industry uses the innovative industry-wide collaborative AAR Asset Health Strategic Initiative (AHSI). AHSI is a multiyear program that pools the immense amount of data collected from the detector network to identify and address industry-level issues that can be addressed with information technology solutions and processes that will enable safer, more reliable service and cost-effective operations through more effective asset health management. The program builds on existing industry defect detection systems and capabilities—such as equipment databases, component identification, car repair procedures, and detector alerts—to develop a common foundation for solutions aimed at reducing mechanical service interruptions, improving the quality of railcar inspections, and increasing rail yard and repair shop efficiency.

3. Train Operation Safety

a. Train Control Technology

Train safety is enhanced through the development and deployment of various train control technologies. These technologies are layered on top of already stringent operating practices employed in the transport of crude oil that include various operating restrictions, including speed.

49 In terms of rail cars, "truck" refers to the completed four-wheel assembly that supports the car body. "Hunting" is an instability, more prevalent at higher speeds, that cause a rail car to weave down a track, usually with the flange of the wheel striking the rail.

The most prominent and technologically advanced train control technology today is positive train control, or PTC. PTC describes technologies designed to automatically stop a train before certain accidents caused by human error occur.

Though PTC had been in development and testing by railroads for years, it was mandated by the Rail Safety Improvement Act of 2008. The act called on railroads to install PTC by the end of 2015 on certain mainlines used to transport passengers or toxic-by-inhalation materials. In October 2015, the statutory deadline for PTC installation was extended to the end of 2018, with further extensions available up to the end of 2020 to allow time for railroads to adequately test their systems.

As mandated by Congress, PTC must be designed to prevent train-to-train collisions; accidents caused by excessive speed, unauthorized incursions by trains onto sections of track where maintenance activities are taking place, and the movement of a train through a track switch left in the wrong position.

To accomplish these mandates, a PTC system (Figure 4-40) consists of three main elements:

- An onboard or locomotive system monitors a train's position and speed and activates brakes as necessary to enforce speed restrictions and prevent unauthorized train movements.
- A wayside system monitors railroad track signals, switches, and track circuits to communicate data on this local infrastructure needed to permit the onboard system to authorize movement of a locomotive.
- A back-office server stores all information related to the rail network and trains operating across it (e.g., speed restrictions, movement authorities, train compositions, etc.) and transmits this information to individual locomotive onboard enforcement systems.

These three elements are integrated by a wireless data communications system that moves massive amounts of information back and forth between the back-office servers, the wayside equipment, and the locomotive's onboard computers.

PTC development and implementation has been an unprecedented technological challenge, on a

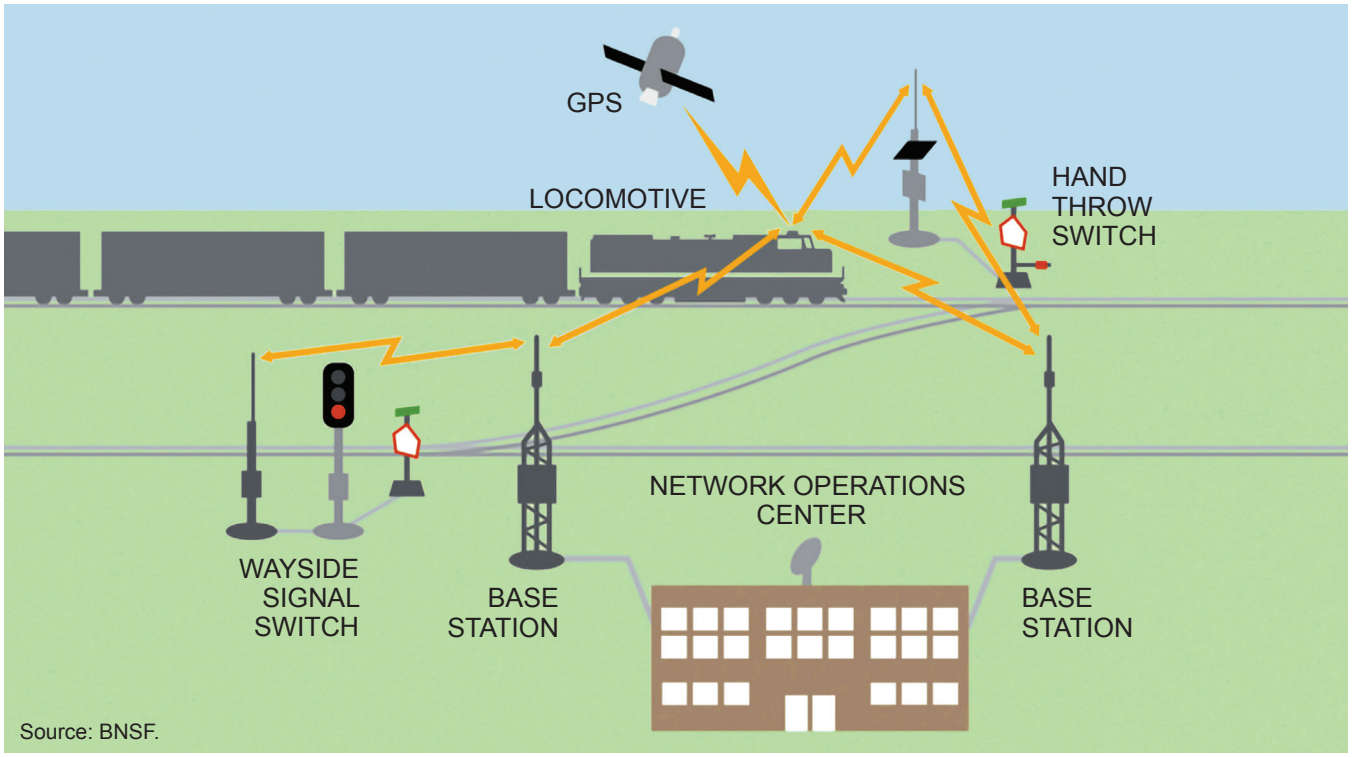


Figure 4-40. *Positive Train Control*

scale never attempted on railroads anywhere in the world. Necessary tasks for Class I freight railroads include:

- A complete physical survey and highly precise geomapping of the nearly 54,000 freight route-miles on which PTC technology will be installed, including more than 450,000 field assets along the right-of-way (e.g., mileposts, curves, rail and highway grade crossings, switches, signals, track vertical profiles and horizontal geometry).
- Installing more than 28,500 custom-designed wayside interface units that provide the mechanism for transmitting information from signal and switch locations along the right-of-way to locomotives and railroad facilities.
- Installing PTC technology on nearly 16,400 locomotives.
- Developing, producing, and deploying a new radio system specifically designed for the massive data transmission requirements of PTC at tens of thousands of base stations and trackside locations, and on nearly 16,400 locomotives.
- Upgrading some 2,100 switches in nonsignaled territory and completing signal replacement projects, including upgrades to PTC-compatible signal technology, at some 14,500 locations.
- Developing back-office systems and upgrading and integrating dispatching software to incorporate the data and precision required for PTC systems.

Railroads have invested enormous human and financial resources to the effort and because of this, Class I railroads have met all 2018 PTC-related statutory requirements. As of the end of 2018, PTC was operational on 44,695 miles, or 83%, of the 53,732 route-miles that will eventually be equipped with PTC. Moreover, each Class I railroad installed 100% of PTC wayside, back-office, and locomotive hardware, and completed all required employee training, by the end of 2018, as statute required.

As of the end of 2018, Class I freight railroads in aggregate had spent $10.6 billion—their own funds, not taxpayer funds—on PTC development and deployment. Maintaining the PTC systems once they are installed will cost hundreds of millions of additional dollars each year.

Each Class I railroad expects to be operating trains in PTC mode on all their PTC routes no later than 2020, as required by statute. In the meantime, railroads are continuing to test and validate their systems thoroughly to ensure they work as they should. Every day, as railroads expand PTC operations, additional accident avoidance becomes possible.

b. Locomotive Cab Technologies

Additional locomotive technologies are being employed by railroads to improve the safety of operations. Various technologies include devices such as alerters and locomotive outward and inward facing cameras. These technologies help identify and remediate incidents and potential incident causes.

Locomotive alerters are a type of safety technology designed to verify that the locomotive engineer remains capable and focused on safety critical tasks. The alerter will initiate a braking application to stop the train if the locomotive engineer does not respond properly to certain operating conditions. Next-generation technology might include cognitive alerters that could require demonstrating an increased level of operator alertness.

Inward facing cameras can be used as another tool in rail safety and could be used during investigations after an incident. Additionally, information can be used to identify electronic device use and other rail operating rule noncompliance. Railroads are implementing inward facing camera technologies.

c. Route Modeling

To additionally identify and mitigate risk of operations, several years ago the rail industry and various federal agencies jointly developed the Rail Corridor Risk Management System (RCRMS), a sophisticated routing model designed to help railroads analyze and identify the overall safest and most secure routes for transporting highly

hazardous materials. The model uses 27 risk factors—including hazmat volume, population density along the route, trip length, emergency response capability, and availability of alternate routes—to assess the overall safety and security of rail routes. Major U.S. railroads are now using the RCRMS for trains carrying large amounts of flammable liquids and security-sensitive hazardous materials.

4. Emergency Response

Railroads have extensive emergency response capabilities in which railroad personnel work in cooperation with federal, state, and local governments to assist communities in the event of an incident involving crude oil, ethanol, or other hazardous materials.

Railroads' emergency response efforts begin internally and utilize technology to improve those capabilities. For example, major U.S. freight railroads use a web-based application called AskRail that allows emergency responders to input the identification number of a rail car and immediately determine whether the car is loaded or empty, if loaded the commodity contained in the car, its hazard class, the handling railroad, the handling railroad's emergency contact phone number, and emergency response information associated with the commodity.

Technologies supplement many other response efforts, including deployment of full-time personnel focusing on hazmat safety and emergency response, placement of emergency response inventory across their networks maintaining hazmat response contractors and environmental consultants, strategically located throughout their service areas to handle issues, and enforcement of standard of care protocols to ensure that community impacts, such as evacuations, are addressed promptly and professionally.

Outreach processes include the TRANSCAER (Transportation Community Awareness and Emergency Response), which is a voluntary national outreach effort that focuses on assisting communities to prepare for and to respond to a possible hazardous materials transportation incident. TRANSCAER members consist of volunteer representatives from the chemical manufacturing, transportation, distributor, and emergency response industries, as well as the government. TRANSCAER is focused in the specific areas of hazardous materials transport safety including:

- Promoting safe transportation and handling of hazardous materials
- Educating and assisting communities near major transportation routes about hazardous materials
- Aiding community emergency response planning for hazardous material transportation incidents.

Additional enhancements to railroad processes and regulations continue to be developed and include the recent final rule on crude oil spill response plans recently issued by the PHMSA. This rule requires that railroads develop oil spill response plans for routes traveled by trains carrying crude oil in a block of 20 or more loaded tank cars, or those with a total of 35 loaded tank cars spread throughout the train. Railroads will also be required to establish geographic response zones along various rail routes to ensure there are people and equipment staged and prepared to respond to an oil spill within 12 hours. In addition, railroads affected by the new standards will have to share certain railcar and cargo information with state safety agencies.

These technologies and processes are also supported by world-class training provided by railroads and the Security and Emergency Response Training Center (SERTC) in Pueblo, Colorado, that is operated by TTC. SERTC provides in-depth, realistic, hands-on hazmat emergency response training to tens of thousands of local, state, and tribal emergency responders and railroad, chemical, and petroleum industry employees. Most of the training at SERTC is advanced training that builds on basic training that responders receive elsewhere.

D. Trucking Industry Technologies

1. Trucking Industry Overview

Trucks provide a vital link for crude oil and refined petroleum products to other modes of

Fleet Size	# of Trucks	% Total Trucks	# of Fleets	% Total Fleets
1-4	9,445,400	33.17%	7,284,100	92.76%
5-20	6,469,200	22.72%	450,500	5.74%
21-50	3,451,300	12.12%	83,000	1.06%
51-99	1,912,900	6.72%	24,100	0.31%
100-499	2,887,200	10.14%	9,500	0.12%
500-999	889,200	3.12%	1,150	0.01%
1,000+	3,424,100	12.02%	690	0.01%
Total	28,479,300	100.00%	7,853,040	100.00%

Source: FleetOwner. (2016). Trucking Snapshot.

Table 4-11. *Commercial Trucking Industry Segmentation*

transportation (e.g., pipelines, rail terminals, etc.) as well as processing, storage, and points-of-sale locations. For the transportation of crude oil and refined petroleum products, trucking has small individual container capacities, compared to other modes of transportation for these products. The volumes that can be transported with one vehicle are much less than can be transported by other means such a rail, ship, or pipeline. However, trucks are also the most flexible means of transporting products because they can go where other transport options cannot and can deploy quickly to meet changing market needs.

Large trucks, those weighing more than 10,000 pounds, serve the U.S. economy by transporting and delivering a wide range of commodities, including crude oil and natural gas. These trucks are engaged in every segment of moving goods and commodities, from long haul transportation to last mile delivery. Trucks servicing the petroleum industry are usually large tanker trucks weighing up to 80,000 pounds. Over the 5-year period from 2012 to 2016 the trucking industry transported an average of 154 million gallons of crude oil per year, which accounts for 4.19% of all land-based crude oil transportation per year, resulting in approximately 789,000 trips per year.[50]

The commercial trucking industry[51] primarily consists of many small independent carriers. According to an industry snapshot from *FleetOwner* magazine produced in August 2016, of the 7.8 million trucking companies in the United States, 98% operate 20 or fewer trucks while 93% operate 4 or fewer trucks. While these carriers represent 98% of the total truck operators, they represent only 55% of the total trucks (Table 4-11).[52]

Large trucks with a gross vehicle weight rating of more than 10,000 pounds drove approximately 280 billion miles on U.S. roads in 2015 and were involved in a total of more than 400,000 crashes, which resulted in 116,000 injuries and 4,067 deaths.[53]

Advanced technologies allow the industry to address human error and physical limitations, whether by the truck operator or by the operators of other vehicles that creates risk to the truck operator. Sensors and computers available for trucks today can detect hazards, analyze more information, and respond to events much faster than any human being. These technologies—including

50 U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration. (2018). Report on Shipping Crude Oil by Truck, Rail, and Pipeline, https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/news/70826/report-congress-shipping-crude-oil-truck-rail-and-pipeline-32019.pdf.

51 The commercial trucking industry includes trucks weighing 10,000 lbs. or more and covers all commodities transported.

52 FleetOwner. (2016). Trucking Snapshot. https://www.fleetowner.com/fleet-management/article/21694137/trucking-by-the-numbers-2016-trucking-snapshot.

53 AAA Foundation for Traffic Safety. (2017). "Leveraging Large-Truck Technology and Engineering to Realize Safety Gains," Fact Sheet, https://publicaffairsresources.aaa.biz/wp-content/uploads/2017/09/17-0097_Truck-Safety-Report-Fact-Sheet_FNL-CX-2.pdf.

forward collision warning and avoidance, lane departure warning, and automatic emergency braking—can help eliminate thousands of deaths and injuries.

These new safety technologies can help reduce accidents. The trucking industry faces challenges to wide-scale deployment. The return on investment tends to be longer with retrofits compared to purchasing new trucks with the technology preinstalled. The cost of retrofitting is greater than the cost of a new vehicle with advanced technology already deployed. Due to the longevity of trucks, this results in a longer overall time to deploy these new technologies across the entire fleet. Some manufacturers are developing new programs to reduce the cost and simplify the process of retrofitting safety technologies to accelerate installations on existing trucks.

Smaller trucking companies have fewer resources to put toward evaluating and funding new technologies and overall tend to be slower to adopt new technologies. Larger carriers are typically more likely to be early adopters of emerging technologies and to dedicate resources toward testing new technologies. As such, many larger operators have made the investments to retrofit their existing fleets.

a. Types of Safety Systems

Active safety systems (also known as primary safety systems) include features that activate based on roadway conditions to reduce the chances of an accident or collision. Examples include traction control, collision warning system, antilock braking, and electronic stability control.

Passive safety systems react to the abnormal event (i.e., they activate after an accident has occurred) and reduce the effects of an accident. Examples include seat belts, passenger safety cell design, laminated glass, and deformation zones.

Independent safety systems provide most of their value without driver and/or management intervention. Examples include roll stability, automatic braking systems, automated collision avoidance system, speed limiters, etc. When properly installed and maintained, these systems work with no human intervention and require no training to operate correctly.

Dependent safety systems act through human (driver and/or management) intervention in conjunction with the technology. Examples include lane departure warnings, collision warning systems, speed monitoring, blind spot detection, video telematics with coaching or corrective action, electronic onboard recording devices, etc. Without human interaction or response to these systems, there is little or no safety enhancement. Training and strong management systems are critical to the success of dependent safety systems.

b. Challenges of Translating Safety Technologies from Passenger Cars to Large Commercial Trucks

The forces associated with large trucks are very different from those of smaller passenger vehicles. The center of gravity is higher, the overall weights greater, the stopping distances longer, and the vehicles larger than passenger vehicles. These factors also vary depending on the commodities being carried. These variances, due to different forces and commodities, make applying passenger vehicle safety systems to large trucks difficult. Additional research and development are needed to provide guidance on applying certain safety systems to large trucks.

c. Enabling Technology Implementation in Trucking Industry

Various challenges confront adoption of new technology, including but not limited to:

- Validating that the technology will achieve the expected results and is ready for widespread implementation.
- Disaggregated data and a lack of mechanisms for sharing data. This slows adoption of these technologies because the data proving the value of the technologies is not being widely shared and accepted.
- New and emerging technologies may have a higher initial cost of implementation and therefore smaller carriers may be less likely to be early adopters of these technologies and may wait

until installation costs decline or the technologies are required by regulation.

- Developing appropriate rules and specifications for requiring mandatory safety systems and technology.
- Cost to install, maintain, and repair or replace technology (i.e., does the benefit of the technology outweigh the cost). This is both a short-term and long-term question (i.e., How much impact is there on the short term, and how long will it take for the technology to pay for itself?).
- Driver resistance to change. Drivers will require training to understand how the technology works, what the benefits and challenges of the technology are, and how the technology will ultimately help to make their jobs easier or safer.

Drivers typically accept independent technology better than dependent technology, because it has less direct impact on the driver and their driving habits. With proper training and understanding of the independent technology, drivers should be able to easily adjust their habits to maximize benefits of the new technology.

Dependent technology requires driver and management engagement to maximize effectiveness. Engagement with the technology can make the driver more aware and engaged with the task of driving but might also distract the driver with ongoing interruptions if there are too many unnecessary audible or visual indicators. Finding the right balance is critical in these cases. This is similar to the concern of nuisance alarms in control room situations. Excessive false positive alarms can be a distraction and potentially cause an important alarm to be missed. Training, communication, and strong management systems become essential to the success of dependent technologies.

d. Data Collection and Sharing

Advanced Driver Assisted Systems (ADAS) have the potential to significantly reduce the frequency and severity of large truck accidents. Carriers expect an appropriate benefit versus cost for technology investments to justify voluntary implementation of additional technology systems. There is currently not enough consolidated data to provide real-world objective findings on the amount of improvement that could be achieved. Some large carriers who have voluntarily implemented these new technologies have data, but, in most cases, that data has not been published or shared. Independent objective research and data on ADAS implementation is also lacking, which limits wider acceptance of these lifesaving technologies.

Finding: Carriers need valid data to measure the cost/benefit of adding advanced driver assisted technologies to their trucks. There is limited sharing of objective data validating the successes of these systems. This limits support for wide-scale implementation of these important safety technologies.

The NPC recommends that National Highway Traffic Safety Administration (NHTSA), and any other appropriate federal agency, should sponsor a research study to confidentially gather performance data from current users of various advanced safety technologies on incident triggers and near miss incidents that avoided actual accidents. This should also include consolidating expert testimony and manufacturer data to further improve information sharing.

This research should provide valuable information that is needed to encourage companies and manufacturers to install the technology in commercial trucks or ensure that we have the data to support appropriate regulation of these lifesaving technologies.

2. Forward Collision Warning and Avoidance Systems

A variety of technologies, often integrated, reduce the risk of front-end and rear-end collisions. Forward collision warning (FCW) systems use sensors to monitor a vehicle's speed, the speed of the vehicle in front of it, and the distance between the vehicles. FCW systems can provide audible, visual, or other warning signals (depending on how the system is designed) to alert the driver to take evasive actions.

Automatic emergency braking (AEB) systems combine forward-looking sensors, driver alerts, and automatic vehicle braking. These systems are designed to reduce or prevent rear-end collisions. The forward-looking sensor is used to detect a lead vehicle within a preset distance or time-to-collision. The system alerts the driver of the lead vehicle's proximity through haptic (such as seat vibration), audible, visual, or a combination of warnings. The driver may maintain control of the vehicle and decide to reduce speed and/or steer to avoid the lead vehicle. If the driver does not apply the brakes or steer away from the lead vehicle and the system detects that a crash is imminent, the AEB system will assume active control of the truck's brakes to prevent or mitigate the imminent crash.[54]

Collision avoidance systems (CAS) combine AEB with FCW to manage the following distance and to provide emergency braking. CAS help to prevent crashes by detecting a conflict and alerting the driver. Many systems aide in automatically applying brakes. Some systems employ dynamic braking systems; however, these are not currently available on commercial trucks.

Warning systems that provide multiple types of feedback, such as audible, visual, and/or haptic, are most beneficial because quicker response times significantly reduce the potential for an incident to occur. Researchers consistently reported faster response times to sudden events when drivers were alerted by multimodal signals, such as an auditory/visual or auditory/haptic, rather than a single sensory cue.[55] The findings of the research into the efficacy of different warning cues to alert a driver to a potential collision, although conducted with passenger vehicles, also apply to commercial vehicles. While the timing of the warnings presented to a heavy-truck driver may differ from the timing posed to a driver in a passenger vehicle, the basic findings of the benefits of multimodal cues remain.

Though more research has been conducted on passenger vehicles than commercial trucks, the findings still support the benefits of FCW and AEB systems for all vehicle types (Table 4-12). While there are limited data on the level of safety improvement to be expected with large commercial trucks, when the systems are properly adjusted for and implemented in large commercial trucks, they will provide significant safety improvements to both frequency and severity of truck-related accidents.

Finding: Current studies indicate that collision avoidance technologies work as intended in the large commercial truck environment and have the ability to help prevent or mitigate rear-end crashes, thus reducing the number of fatalities and injuries related to rear-end crashes. An NTSB analysis of two-vehicle rear-end crashes during 2011–2012 found that up to 2,220 lives might have been saved had the vehicles been equipped with forward collision avoidance systems.[56]

The NPC recommends that DOT should consider sponsoring incentive mechanisms to the commercial trucking industry and equipment manufacturers, to accelerate deployment of safety technologies. These incentive mechanisms can include government/industry consortiums to invest in technology advancements, phased tax credit incentives, insurance, and regulatory requirements. In addition, petroleum company customers should consider requiring their trucking carriers to use driver-assist safety technologies by contract.

54 AAA Foundation for Traffic Safety. (2017). "Leveraging Large-Truck Technology and Engineering to Realize Safety Gains: Automatic Emergency Braking Systems," https://aaafoundation.org/wp-content/uploads/2017/11/Truck-Safety_-Braking-Report.pdf.

55 NTSB/SIR-15-01, "The Use of Forward Collision Avoidance Systems to Prevent and Mitigate Rear-End Crashes." Adopted May 19, 2015, https://www.ntsb.gov/safety/safety-studies/Documents/SIR1501.pdf; Kramer, A.F., N. Cassavaugh, W. Horrey, E. Becic, and J. Mayhugh. (2007). "Influence of Age and Proximity Warning Devices on Collision Avoidance in Simulated Driving," Human Factors 49: 935–949; Forkenbrock, G., A. Snyder, M. Heitz, R.L. Hoover, B. O'Harra, S. Vasko, and L. Smith. (2011). "A Test Track Protocol for Assessing Forward Collision Warning Driver-Vehicle Interface Effectiveness," DOT HS 811 501. Washington, DC: NHTSA.

56 NTSB/SIR-15-01, "The Use of Forward Collision Avoidance Systems to Prevent and Mitigate Rear-End Crashes." Adopted May 19, 2015, https://www.ntsb.gov/safety/safety-studies/Documents/SIR1501.pdf.

Study	Findings
Insurance Institute for Highway Safety, Highway Loss Data Institute. (May 2018). *Real-world benefits of crash avoidance technologies.*	• Forward collision warning could reduce front-to-rear crashes by 27%, front-to-rear crashes with injuries by 20%, claim rates for damage to other vehicles by 9%, and claim rates for injuries to people in other vehicles by 16%. • With the addition of autobrake, the study indicates that the technologies together could reduce front-to-rear crashes by 50%, front-to-rear crashes with injuries by 56%, claim rates for damage to other vehicles by 13%, and claim rates for injuries to people in other vehicles by 23%.
Grove, K., Atwood, J., Hill, P., Fitch, G., Blanco, M., Guo, F., … & Richards, T. (June 2016). *Field study of heavy-vehicle crash avoidance systems*. (Final report. Report No. DOT HS 812 280). Washington, DC: National Highway Traffic Safety Administration.	• One-year field operational study with 3 million miles of data • No rear-end crashes of the type collision avoidance systems (CAS) are designed to prevent • A total of 6,000 CAS activations were sampled and analyzed to evaluate their reliability • CAS user experience can be improved • Some activation types were found to be less reliable than others
National Transportation Safety Board. (2015). *The Use of Forward Collision Avoidance Systems to Prevent and Mitigate Rear End Crashes* (Special Investigative Report NTSB/SIR-15-01).	• National Transportation Safety Board (NTSB) analysis of two-vehicle rear-end crashes during 2011 to 2012 (with 3,491 fatalities, 2,700 of which were attributed to crashes in which a passenger vehicle, truck-tractor, or single-unit truck struck the rear of another vehicle) found that up to 2,220 lives might have been saved had the vehicles been equipped with forward CAS • A forward CAS might have prevented or lessened the severity of injuries in: – 93.7% of rear-end crashes when a passenger vehicle was the striking vehicle – 87.1% of rear-end crashes when the striking vehicle was a single-unit truck – 79.0% of rear-end crashes when the striking vehicle was a tractor-trailer, respectively • Study concluded that collision warning, particularly when paired with active braking, could significantly reduce frequency and severity of rear-end crashes. NTSB made six recommendations to accelerate deployment of these technologies.
Moore, M., and D. Zuby. (2013). "Collision avoidance features: Initial results." In 23rd Annual Proceedings: International Technical Conference on the Enhanced Safety of Vehicles, paper number 13-0126.	• Lower property damage liability claim frequency across all vehicles equipped with any type of forward CAS, compared to the same or similar vehicles without a forward CAS • Further reduction in liability claims for vehicles equipped with collision warning systems (CWS) and automatic emergency braking (AEB)
U.S. Department of Transportation. (2007). *Final Report: Evaluation of the Volvo Intelligent Vehicle Initiative Field Operational Test*, DTFH61-96-C-00077.	• Truck-tractors equipped with CWS alone, or in combination with other safety components, were less frequently (by 37%) involved in situations that had a potential to result in a rear-end collision. – More than 80% of drivers reported that they preferred driving truck-tractors equipped with a CWS. – Drivers reported that the systems made them more vigilant and improved their following distances. – Following distance when equipped with CWS was 15 feet longer than without CWS.
Con-way internal study (reported in NTSB/SIR-15-01).	• Drivers operating truck-tractors equipped with forward CAS (with AEB, electronic stability control, and lane departure warnings) exhibited a decreased crash rate for different types of crashes, as well as a decline in risky driving behavior: – 71% reduction in rear-end collisions – 63% decline in unsafe following behaviors

Table 4-12. *Summary of Research Supporting Adoption of Forward Collision Warning, Automatic Emergency Braking, and Collision Avoidance Systems*

3. Lane Departure Warning and Corrective Steering

Lane departure warning systems (LDWS) warn drivers when the vehicle begins to move out of its lane (unless a turn signal is on in that direction) on freeways and arterial roads, usually when operating over a certain speed. LDWS address driver error, distractions, and drowsiness. These systems (as they are currently designed for commercial trucks) are not intended to steer the vehicle or actively keep the vehicle in the lane but are only meant as warning systems that prompt the driver to make a correction. To be successful, LDWS requires good driver training and strong management systems to ensure that drivers properly use the information and react appropriately to the information provided by the LDWS.

LDW systems depend on good lane markings to ensure their accuracy. LDWS may not be able to recognize lane markings for reasons such as lack of or poor quality of lane markings, poor visibility, or a dirty/icy detection device. When lane markings are not visible on roads covered by mud, ice, or snow, the lane tracking indicator will show that the system is inactive.

LDWS technology consists of a forward viewing camera system that uses algorithms to interpret collected images to estimate a vehicle's lateral position, lateral velocity, and vehicle heading, as well as the roadway alignment based on the lane width and road curvature. When the vehicle drifts outside the road alignment markings to either the left or right, the driver is warned with an audible alarm notifying them to take corrective steering action. Some LDWS use audible warnings inside the cab of the truck that sound like rumble strips. They may also have a graphical display that indicates if the driver needs to steer right or left.

Other potential benefits from the use of LDWS include:

- Assisting in training the driver to consistently keep a vehicle in the lane, thereby reducing lane departure crashes
- Reinforcing driver awareness of vehicle position in the lane to maintain a more central lane position and improve the driver's attentiveness to the driving task
- Encouraging the driver to use turn signals when changing lanes (otherwise, a lane departure warning sounds)
- Collecting data from the vehicle to assist with driver behavior-based training sessions.

On average, large-truck LDWS may prevent 66 to 103 fatal crashes, 748 to 1,171 injury crashes, and 3,254 to 5,098 property damage crashes each year. These crashes were associated with 74 to 115 fatalities, 103 to 162 suspected serious injuries, 366 to 573 suspected minor injuries, and 371 to 581 possible injuries. When the costs of LDWS are averaged, and the discount rate is 0%, the estimated benefits of LDWS are 2.3 times the estimated costs.[57,58]

Finding: Infrastructure, primarily in the form of well-maintained lane markings, is critical to the effectiveness of lane departure warning and corrective steering systems.

The NPC recommends that:

- DOT should ensure adequate funds are provided for infrastructure improvements to ensure that roads maintain the proper markings to allow these LDWS technology systems to operate properly. If road markings are nonexistent or obscured, then the system will not work properly.
- NHTSA should support additional research and development to identify new technologies that improve LDWS ability to work properly on snow-covered roads or roads without proper markings.

57 Camden, M.C., Medina-Flintsch, A., Hickman, J.S., Miller, A.M., and Hanowski, R.J. (2017). "Air Disc Brakes: Leveraging Large-Truck Technology and Engineering to Realize Safety Gains. AAA Foundation for Traffic Safety," https://aaafoundation.org/air-disc-brakes-leveraging-large-truck-technology-engineering-realize-safety-gains/.

58 AAA Foundation for Traffic Safety. (2017). "Lane Departure Warning Systems: Leveraging Large-Truck Technology and Engineering to Realize Safety Gains," https://aaafoundation.org/lane-departure-warning-systems-leveraging-large-truck-technology-engineering-realize-safety-gains/.

4. Fatigue and Distracted Behavior Recognition

Fatigue and distracted behavior recognition systems use cameras and sometimes additional sensors to provide in-cab fatigue detection that instantly alerts operators and remote monitoring stations when fatigue or distraction is identified. Fatigue detection technology works by monitoring parameters such as head pose, body position, and eye-closure duration, blink rate, and redness. If the system detects a fatigue or distraction event, the operator can be immediately alerted through configurable in-vehicle seat vibration and/or audio alarm. New technologies are in development to use sensors and cameras to identify instances of distraction and/or fatigue and to immediately warn the driver via haptic, auditory, and visual warning signs. These events can also be recorded for training purposes. Cameras and data storage systems can also be configured to store footage recorded from a specified time period before and after a fatigue or distraction event is detected.

System Configuration	Benefits
Independent Configuration	• Providing real-time intervention for fatigued drivers • Integration with other truck technology to turn off cruise control and potentially slow the vehicle • Allowing drivers to focus on the job rather than interacting with the system • Alerting operators to distraction events to improve safe driving
Dependent Configuration	• Providing information to management to ensure follow-up training for drivers to recognize fatigue and change their behavior • Customizing data and reporting for continuous improvement and safety education • Configurable with live data feeds to management to ensure follow up and accountability

Table 4-13. *Eye Movement and Facial Recognition Technology Benefits*

Benefits of eye movement and facial recognition systems include those listed in Table 4-13.

Additional benefits include providing training on specific events recorded by the system to improve driver performance and recording and storing data that may be useful in incident investigations (including potentially reducing the time to settle civil disputes by enabling better root cause analysis).

According to the National Safety Council, 13% of all fatal truck crashes and 28% of single commercial vehicle crashes involve fatigue. The National Center for Statistics and Analysis found more than 10% of fatal crashes and 15% of injury crashes are related to distracted driving. NHTSA estimates that 3,166 people were killed by distracted driving in 2017. This represents 9% of the total fatalities on the road in the United States. Considering the 795 deaths from drowsy driving related crashes in 2017, these cameras have the potential to reduce up to 11% of fatal motor vehicle crashes.[59] The theory behind this technology appears sound: recognize predictive behavior and warn before an incident occurs. The challenge is that few independent objective studies exist to prove that the technology is advanced enough to be reliable. A 2016 study from researchers in Australia showed that cameras measuring eye movement and head pose and providing real-time feedback to the drivers had reduced fatigue events by more than 90% per km driven exposure.[60] Additional objective studies should be completed to verify that the technology is ready for wide-scale implementation.

EuroNCAP, a safety performance assessment program for new European passenger vehicles, has made these cameras a requirement to achieve a five-star vehicle safety rating in 2020. Consequently, original equipment manufacturers for light vehicles are starting to voluntarily include this technology to achieve the rating.

59 U.S. Department of Transportation, National Highway Traffic Safety Administration. (2019). "Distracted Driving in Fatal Crashes, 2017," Traffic Safety Facts Research Notes, https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812700.

60 Lenne, Michael G. and Fitzharris, M. "Real-time feedback reduces the incidence of fatigue events in heavy vehicle fleets." Paper number ITS-AN-SP0293. 23rd ITS World Congress, Melbourne, Australia, October 10–14, 2016.

Finding: The studies that are available show promising results in reducing distracted driving.

The NPC recommends that Federal Motor Carrier Safety Administration should work with NHTSA to sponsor additional research and development to advance promising fatigue and distraction detection technologies.

5. Vehicle Camera Systems

Video-based onboard safety monitoring systems incorporate in-vehicle video technology that records the environment in front of the vehicle, within the cab of the vehicle, and potentially surrounding the vehicle. Recording may be continuous or may be prompted by safety events. Some systems use algorithms to identify issues. Company's may then use the recordings to coach and train drivers to improve safety performance. Some systems record vehicle telematics data (e.g., speeding, hard braking, rapid acceleration, quick cornering, seat belt use, turn signal use, driver distraction, following distance, and lane departures).

This technology is considered dependent technology as the majority of the value comes from coaching and training drivers to change behaviors and become safer drivers. There may be additional value in behavioral changes that occur by drivers knowing that their behaviors are being recorded and subject to review. There may also be value in having video to either defend against a false claim or to quickly and amicably settle cases where liability is clear. Effective management systems, complete with processes and procedures for thorough and consistent review of data and training programs for management and employees, are critical to the effectiveness of video-based camera systems. Cost-effective, in-cabin camera systems are available for use today, and, when used properly and supported by management systems, help identify and reduce poor driver behaviors that are likely to contribute to accidents.

A 2017 study by AAA Foundation for Traffic Safety estimates that installing video-based monitoring systems on all trucks could prevent as many as 63,000 crashes, 17,733 injuries, and 293 deaths annually. Approximately 90% of all accidents result from driver error or risky behavior. Recognizing and documenting these risky behaviors is critical to being able to coach drivers and correct their behavior. Behaviors directly related to driver performance that could be monitored through a camera system include following distance, failure to yield or stop, unsafe lane changes, and distracted driving and cell phone use.

There are limited but promising data available on the industry's track record with camera systems (Table 4-14).

Company	Experience
AmeriGas	55% reduction in crashes and safety-related events
Cox Petroleum	80% reduction in at-fault crashes
Salmon Companies	44% reduction in drivers' risky behaviors

Source: AAA Foundation for Traffic Safety, "Leveraging Large-Truck Technology and Engineering to Realize Safety Gains: Video-Based Onboard Safety Monitoring Systems," September 2017.

Table 4-14. *Recent Industry Track Record with Camera Systems*

Finding: Camera systems reduce at-risk driving behaviors that contribute to accidents and provide coaching points to help improve safe driver skills.

The NPC recommends that carriers should install vehicle camera technologies where feasible and use as a tool for coaching and training drivers to help improve driver safety performance and reduce accidents.

IV. CYBERSECURITY

The purpose of this section on cybersecurity is to identify risks that threaten operational technology (OT) systems and network environments

impacting industrial control systems across the midstream and downstream oil and natural gas industries. IT systems and business networks are excluded from this scope.

The U.S. economy depends on and benefits from its extensive oil and natural gas infrastructure. Protecting pipelines from cybersecurity threats is becoming increasingly important as the majority of U.S. oil and natural gas is transported via pipeline. Decreasing proportions are transported via marine, rail, and truck. Pipeline, marine, and rail assets rely on OT systems for operations and control. A broad-based cybersecurity attack could target OT systems and potentially impair the transportation of oil and natural gas.

IT uses computer systems and networks to store and disseminate information, manipulate data, and support business processes across the enterprise. OT refers to hardware and software that detect or cause a change in physical processes through the direct monitoring of sensors and/or control of physical devices, such as valves, pumps, etc.

ICSs within OT environments receive data from sensors that measure process variables, compare these with established set points, and derive command functions that are used to control a process through the final control elements, such as control valves. They can range from a few modular panel-mounted controllers to a large interconnected and interactive system at a plant or a pipeline's control center with many thousands of field connections. The larger systems are usually implemented by supervisory control and data acquisition (SCADA) systems,[61] or distributed control systems,[62] and programmable logic controllers.[63] Such systems are extensively used in industries such as chemical processing, pulp and paper manufacture, power generation, oil and natural gas processing, and telecommunications.

61 Supervisory control and data acquisition: industrial control systems used to monitor or control chemical, physical, or transport processes, typically used in pipeline operations.

62 Distributed control systems: complex industrial control systems for advanced process control (e.g., plant automation).

63 Programmable logic controllers: stand-alone industrial systems that contain hardware and software used to perform control functions.

Industry and government have been working together for over a decade to strengthen cybersecurity controls in relation to OT assets and escalating threats. Credible cyber risk models used by companies for decision-making are based on the evolving frameworks and standards. The lack of impactful incidents relating to OT cyber events to date in the United States is in part a result of existing cybersecurity programs. Cybersecurity publications provided by industry groups are referenced in Section VI.C at the back of this chapter.

Threats against OT systems have increased in frequency and severity over the past 20 years with the potential to damage or disrupt oil and natural gas infrastructure. A series of recommendations have been defined for the DOE, DHS, and industry to pursue and implement to mitigate the increased risk to OT systems.

This is a collaborative report from multiple oil and natural gas companies, OT system vendors, U.S. government representatives, and private-sector cyber defense companies and consortiums. Within this section on cybersecurity, the convergence of OT systems, IT systems, and supply chain manufacturers is outlined. Longstanding threat actors, as well as emerging threats, are presented. A growing set of sophisticated, malicious actors are seeking to exploit U.S. oil and natural gas companies. A successful attack on an OT system could result in economic impact, operational shutdowns, damaged equipment, and significant environmental, health, and safety consequences. Nation-states present a considerable threat, but other threat actors, such as organized cyber criminals, continue to emerge with capabilities that match those of sophisticated nation-states.

In addition, topic papers have been provided that describe unique cybersecurity considerations covering specific transportation modalities. These topic papers provide options to build onto the foundation of this chapter's findings and recommendations.

A. Overview of Operational Technology and Cybersecurity

The substantial growth in Internet access and the proliferation of Internet-enabled devices and systems have enabled real-time access and

availability to large datasets to elevate productivity, obtain efficiencies, and make better decisions across all major industries. This extraordinary level of connectivity has introduced progressively greater cyber challenges to the oil and natural gas industry due to the convergence[64] of IT networks with OT industrial control system (ICS) networks. The growing number of connected devices within ICS networks and the further reliance on global supply chains has complicated the risk profile. Traditional IT system threats are targeted against OT systems as connectivity increases between IT and OT networks. This is propagated by threat actors with sophisticated capabilities and broader access to digital technology.

The threat of cyberattacks to the ICSs of industrial and critical infrastructure companies was exposed in 2010 by the Stuxnet computer worm. This was the first confirmed example of ICS-tailored malware leveraged against a target—Iran's developing nuclear capabilities in this case. It showed the capability to leverage the centrifuge process to make it do something it was not designed to do—operate at speeds above the safety tolerances and ultimately destroy the equipment.

In March 2015, the DHS issued a report listing the energy sector at the top of the list of U.S. industries under cyberattack. Symantec, a cybersecurity software company, is currently tracking at least 140 groups of threat actors actively targeting the energy industry, an increase from 87 groups in 2015. The energy sector includes electrical utilities, outside the scope of this report, but many of the threats and vulnerabilities faced by the oil and natural gas systems are the same that exist for other sectors because of common ICS components.

WannaCry and NotPetya, two of the largest global cybersecurity attacks, were not originally targeting OT environments, but exploited existing communications links to impact them. Incidents in the Ukraine have illustrated the systemic impact of widespread and escalated OT-based attacks. In 2018 and 2019, the Triton malware attack specifically targeted the safety systems of OT systems. A programming error within the malicious code resulted in a portion of a refinery in the Middle East entering failsafe mode and thus limiting the impact of the attack.

Targeted ICS attacks have increased in frequency and sophistication. While known cyberattacks relating to ICSs within the U.S. oil and natural gas industries have not resulted in significant safety incidents or operational disruptions, these attacks do indicate an increased focus on OT systems.

Finding: Cyber threats to control systems are increasing due to greater reliance on control technology to manage risk and optimize assets, additional connectivity to business systems, and increasing instances of cyber activity targeting industrial control systems.

1. Growing Nature of OT Cybersecurity Risks

Business IT networks possess a larger exposure to cyber threats than OT systems due to their connectivity to the Internet. For example, large U.S. financial institutions move trillions of dollars every day across many interfaces with customers, business-to-business partner networks, and other financial institutions. The Internet provides the ability to share sensitive data with customers regardless of location, from any device, at any time. This creates a different risk profile than OT networks, which are isolated from business networks by firewalls and other protective cyber controls. The greater exposure of IT systems increases the likelihood of an IT incident. An OT event carries more significant health, safety, or environmental consequences.

Oil and natural gas companies rely on OT systems to form the digital backbone of ICSs to ensure uptime, reliability, safety, and compliance. Many of these OT systems were designed at a time when cybersecurity and continuous change were not deemed to be necessary due to isolation and segmentation. Without robust and extensive protections, OT systems are susceptible to cyber threats.

The basic design of the OT systems results in an inherently more defensible environment

64 In this context, convergence is defined as (1) connecting OT data networks to IT systems for sharing data between the OT and IT environments and (2) increasing the use of IT protocols in OT networks/systems.

as opposed to IT systems. IT networks include a broad array of business applications, leveraging Internet-facing connectivity that supports many different business processes. The OT risk-mitigating design factors include:

- Isolation and segmentation (defined below)
- Additional layers of access control (physical and logical)
- Resiliency of operations via redundancy of control components (99.999% uptime)
- Additional protection of safety instrumented systems.

a. Historical Protections

Companies have been enhancing their IT cybersecurity controls to address cybersecurity threats for more than 20 years. Companies have historically focused on prevention of threats to their IT business networks by strengthening cyber controls to prevent threat actors from breaching the perimeter between the Internet and internal business networks. As the sophistication of these attacks increased, companies added more advanced preventive protections, but also increasingly realized an advanced, persistent, and targeted attack would eventually result in a breach. To address this, internal detection monitoring to manage and respond to a successful intrusion has increased. An effective program relies on multiple cyber controls that ensure a single vulnerability or exploit does not compromise critical business systems. It collectively addresses identification, protection, detection, response, and recovery through a comprehensive cyber management system.

Unlike IT, OT infrastructures and networks were designed decades ago and lack the maturity of the core IT cyber protection mechanisms, such as patching, access control, and identity management (e.g., multifactor authentication). Preventive and perimeter protections to keep the networks separate have been important for a long time. While many companies have very robust and sophisticated OT cyber preventive protections, increased detection monitoring, response, and recovery capabilities are more difficult in this area. Many cybersecurity enhancements cannot be implemented in OT environments without vendor approval. An extended disruption to critical functions to certify and make changes can jeopardize the OT functions' top priority of availability, and downtime can have significant consequences.

Cybersecurity enhancements that took place in traditional IT have not been rigorously adopted within OT systems. OT cyber protections have evolved differently based on an assessment of threats, the risk to each specific facility, and the availability of cybersecurity expertise. An understanding of the relative susceptibility to threats is important in determining what actions are prudent to mitigate potential risk.

Historically, isolation has been the preferred method for providing preventive protections of OT systems. Convergence of OT systems is forcing companies to reevaluate their isolation approach.

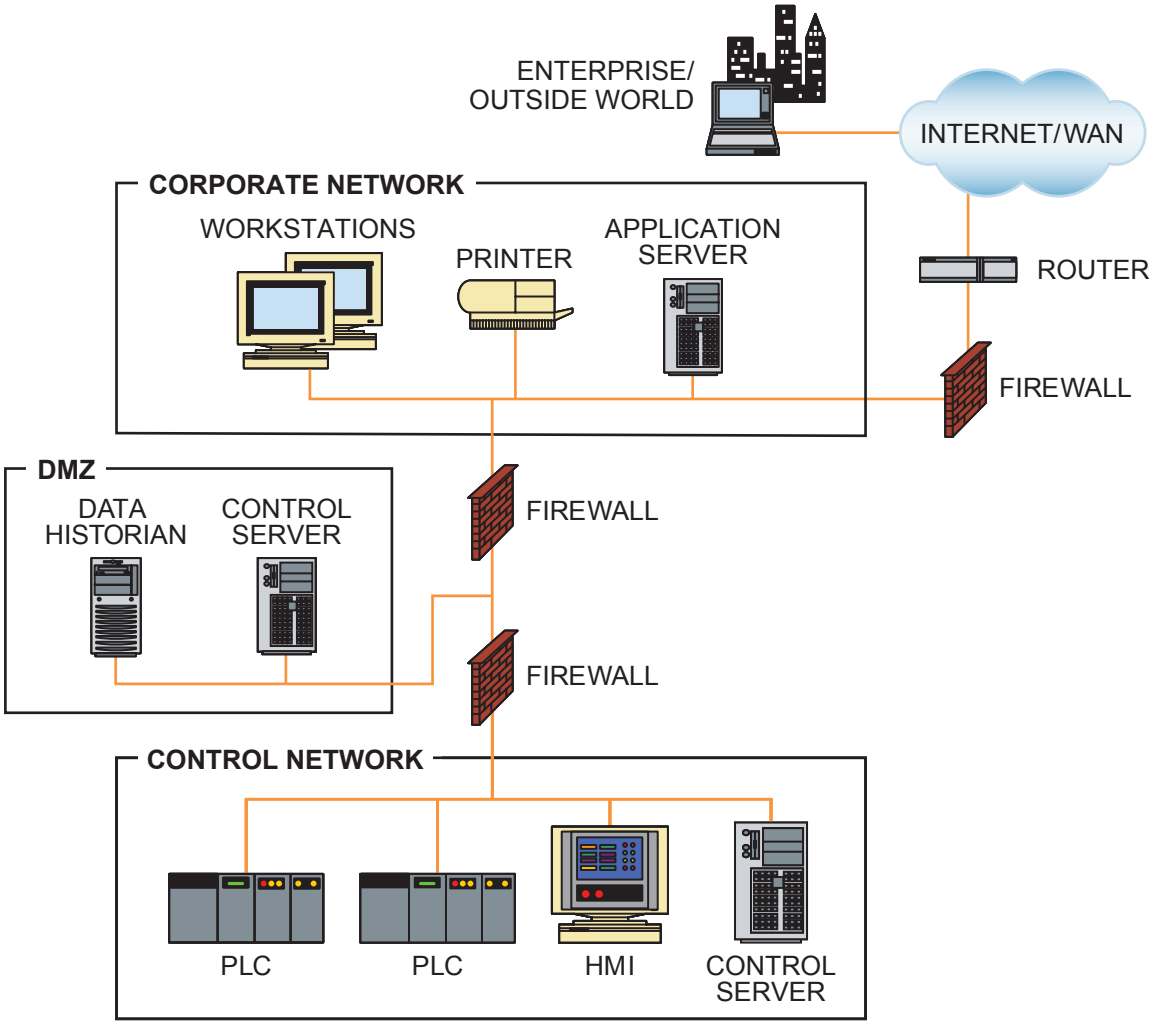
b. Erosion of Isolation and Increased Reliance on Segmentation

OT networks were initially designed to be isolated, to have no connectivity to the outside world other than periodic maintenance updates to the ICSs.[65] ICSs tend to be closed-source, stand-alone proprietary systems, which provides inherent isolation from IT.

Connectivity between IT and OT provides a pathway for cyber threats. Over time, connections to IT networks protected by firewalls or similar controls have been added (see Figure 4-41). In addition, the increasing use of IT technologies in OT enables easier exploitation. Older systems were protected by proprietary protocols, which attackers could not readily exploit. The drive for increased operational efficiencies has led to greater use of remote access by vendors, which increases the potential for cyber issues.

Segmentation is an important component of providing independent layers of protection within OT. As an example, segmentation is used to create resiliency within a plant by separating multiple control systems that operate different process units. Additional information on network

65 This is often referred to as "air-gapping," which is complete physical isolation of a computer system from other networks.



Source: NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).

Figure 4-41. *Firewall between Corporate Network and Control Network.*

segmentation can be found in the *Defense-in-Depth* publication by the National Gas Council[66] and also in applicable topic papers.

As isolation of control networks dissolves, the potential for attacks increases unless operators recognize and offset this increasing risk with mitigations. Best practices for protecting OT systems involve simplifying, reducing, and isolating network connections and virtually segmenting networks from one another. Those actions and capabilities include patching the legacy systems to the extent possible, monitoring and mitigating vulnerabilities, and putting in place breach response planning.

Finding: Industrial control systems were designed for safety and reliability through traditional approaches of isolation (air-gapping) and segmentation. These systems have demonstrated strong reliability. However, the isolation of these control networks is dissolving with advanced technologies, and relying solely on isolation and segmentation for cyber protection can create a false sense of security.

66 National Gas Council. (2018). Defense-In-Depth: Cybersecurity in the Natural Gas & Oil Industry, https://www.api.org/~/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

c. *Challenges to Protecting OT*

Without adequate protections, ICS can become a target. OT systems have long life cycles and many of the ICSs still in place were designed when security features were not as important. Applying updates to these systems without disruption is difficult and impossible to test in some cases. In cases where older systems cannot be patched, many companies rely primarily on isolation and segmentation for protection.

For end-of-life systems, vendors will not create patches against known vulnerabilities. This creates a variety of systems that largely must be isolated from the IT business networks and the Internet to be protected against cyber threats. It also creates a need for segmentation within that network. The ability to assess OT cybersecurity risk depends on multiple factors that are difficult to completely identify. These risks include vulnerabilities within firmware, hardware, software, and configuration data.

Many ICSs attacks involve standard IT intrusions between OT and IT networks. By introducing third-party machines that connect to ICSs, malicious code can be unintentionally installed. The business imperative to extract real-time process data increases the likelihood of human error that can result in the creation of a vulnerability that could be exploited from the IT network.

Due to the size, scale, uniqueness, and complexity of OT systems and networks, it is not realistic to expect complete coverage of cybersecurity improvements to be applied to all previously installed OT system components. To manage cybersecurity concerns, companies must evaluate potential points of vulnerability across the entire OT landscape. Assessments should ensure that companies have effective:

- Network strength (proper segmentation; configurations that avoid single points of failure and changes are monitored)
- System/server design, configurations, and processes (procedures for regular updates/patching and change; enterprise-level solutions such as antivirus and consistent disaster recovery or backup capabilities)
- Workstation protections (USB/remote media control, scanning practices for contractor devices)
- People/process discipline and controls (roles, responsibilities, and training in place; controls for remote connections).

Even if threat actors are not able to directly access and exploit OT systems, they can disrupt activities by targeting IT systems outside those networks. At least four companies that own interstate natural gas pipelines advised customers to temporarily switch to other systems because of the 2018 attack on Latitude Technologies—a third-party service used for pipeline scheduling and nominations. The cyberattack did not disrupt physical pipeline operations. But the hackers may have been seeking sensitive information like account numbers, transaction details, and email addresses of gas producers and their utility customers. This information could be used for destructive purposes, such as ransomware attacks on pipeline companies, spoofing transactions, seeking email addresses of key pipeline operations personnel that can later be used in phishing attacks.[67]

d. *OT Cyber Threats May Interfere with Safety System Protections*

Protection from events such as hazardous material spills, fires, injury is not new, and safety programs that identify and mitigate risks have been in place for decades. Process safety risk reduction programs have resulted in the increasing use of safety systems. Adopting digital software systems to address safety, reliability, and human-factor risks is introducing vulnerabilities that could lead to hazardous states that are not adequately addressed within current risk reduction programs. Cyber threats jeopardize this trajectory. If vulnerabilities within OT systems are exploited by threat actors, physical harm is a possible outcome that could result in a spill, release, or similar environmental event.

67 Where a digital intruder poses as a trustworthy source in an attempt to get sensitive information such as usernames, passwords, or other data.

The safety risk to the process industry from cyber threats is more difficult to quantify. From a safety perspective, risk is assessed by evaluating the probability and consequence of an event. Probability is measurable as a time-based event that is typically associated with design and material failures. Cybersecurity interprets probability as a function of motivation and opportunity. A growing motivation by bad actors toward the oil and natural gas industry increases the inherent risk over time and must be accounted for in additional protections. In other words, risk from cyber threats is not static.

Many of the threats posed by cyber activity, such as loss of process variable, controller malfunction, or equipment shutdown, have already been identified and mitigated through hazard analysis programs. In addition, risks associated with system-wide failures such as power outages, steam outages, and loss of view on distributed control systems are evaluated and mitigated. Because cyber is a new threat with different actors, traditional safety analysis of process hazards should be expanded to include known and credible cyber threat scenarios of the OT environment—referred to as a cyber PHA (process hazards analysis).[68]

Finding: Existing process hazard reduction programs address many, but not all, of the negative physical outcomes created by cybersecurity threats.

The NPC recommends that industry should develop a cyber PHA (process hazards analysis) standard that effectively evaluates risks from cyber threat scenarios and establishes appropriate levels of protection against cybersecurity attacks. DHS should work with DOE and industry to develop and maintain an evergreen catalog of cyber threat scenarios that can be evaluated within a cyber PHA.

68 A cyber PHA is a detailed cybersecurity risk assessment methodology that conforms to ICS standards. The name, cyber PHA, was given to this method because it is similar to the PHA or the hazard and operability study (HAZOP) methodology that is popular in process safety management, particularly in industries that operate highly hazardous industrial processes (e.g., oil and natural gas, chemical).

e. Growing Threat of OT Cyberattacks

There has been a sustained evolution of ICS-related malware over the course of the past 9 years. Stuxnet was the first confirmed example of an ICS-tailored attack leveraged against a target. The payload was specific to ICSs and demonstrated understanding of the industrial processes that it was targeting. OT cyberattacks demonstrate that the threat actors are patient and disciplined with some of the attacks taking years to execute. Successive ICS-targeted intrusions have increased in both frequency and severity (Figure 4-42), and include:

- BlackEnergy 1, BlackEnergy 2, BlackEnergy 3: malware specific to ICSs and targeted human-machine interfaces to enable access to the ICS control room to conduct effective reconnaissance and develop a launch pad from which to commence additional activities
- Havex or Backdoor: espionage malware attack constructed to collect information on ICSs, focused on Petrochemical and power generation sectors
- Industroyer or Crashoverride: malware specifically designed to attack electrical grids by disrupting the working processes of ICSs
- Triton/Trisis: malware designed to attack the logic controller that operates as a safety system for equipment in an industrial environment.

Finding: The progression of cyberattacks indicates an increased focus on OT systems and the potential of greater impact, which could be leveraged by a committed and motivated attacker. However, reported cyberattacks and incidents relating to industrial control systems within the U.S. oil and natural gas and/or midstream industries have not resulted in significant safety incidents or operational disruptions to date.

f. Sophisticated and Organized Threat Actors

Companies face threats from a growing set of sophisticated, malicious actors who seek to exploit cyberspace. The scale and complexity of oil and

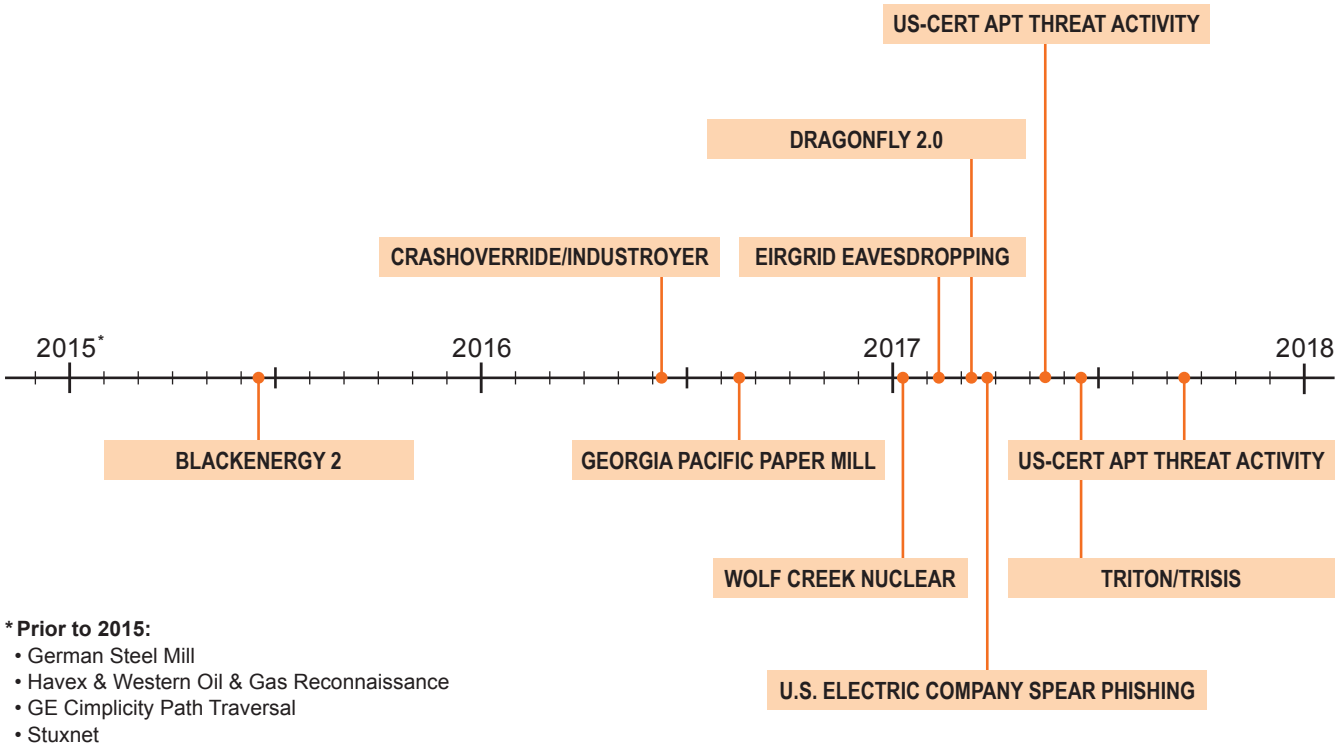


Figure 4-42. *Timeline of Recent Cyberattacks, 2015 to 2018*

natural gas ICS leaves companies challenged in defending against well-funded and sophisticated threat actors. Even with a disciplined approach in cybersecurity protections, a breach of controls may still happen.

Nation-states continue to present a considerable cyber threat, but nonstate actors are emerging with similar capabilities. Organized crime groups have executed the majority of cyberattacks against IT networks but, in recent years, have turned more toward OT infrastructure attacks to extort money from utilities and governments. The distinction between state and nonstate cyber activities is blurred, resulting in a combination of criminal and nation-state affiliations. The methods and techniques that successful threat actors deploy is becoming more accessible to less sophisticated actors. Criminal actors are increasingly empowered by modern information and communication technologies that increases their reach and impact.

U.S. intelligence officials reported in January 2017 that more than 30 countries are developing offensive cyberattack capabilities (see text box titled "Nation-State Cyber Incidents" for details on incidents). Developing the capabilities to be a leader in offensive cyber capabilities enables better advantage on a new battlefield and is cheaper than a military build-up. The most notable cybersecurity superpowers include the United States, China, Russia, Israel, the United Kingdom, Iran, and North Korea.

China's cyber capabilities are extensive. In November 2018, the Department of Justice started a China Threat Initiative to address cybersecurity attacks. A new Office of Commercial and Economic Analysis within the Pentagon is investigating defense contracts for Chinese companies. Chinese advanced persistent threat groups have targeted managed service providers (MSPs) so that one breach may enable access to many or all of the MSPs customers and partners.

North Korea, responsible for an attack that severely impacted Sony's operations in 2014, has remained active internationally. WannaCry paralyzed more than 150 companies globally and has been traced to North Korea.

Iran has focused on the OT space and has targeted more than 200 companies over the past 2 years, according to Microsoft, who deployed incident response teams to many of the companies. The threat group Holmium[69] caused damage estimated at hundreds of millions of dollars in lost productivity, including oil and natural gas companies, heavy machinery manufacturers, and international conglomerates in more than a half-dozen countries, including Saudi Arabia, Germany, the United Kingdom, India, and the United States.[70]

NATION-STATE CYBER INCIDENTS

- In March 2019, it was reported that hundreds of attacks from North Korea were directly monitored. Most of the attacks targeted the United States and specifically oil and natural gas firms. The hackers found profiles of energy industry job recruiters and sent emails that appeared to come from those recruiters' accounts promoting job opportunities. When the email recipient clicked on an attachment or link in the email, the hackers gained access to the target's computer. The hackers also were able to delete their digital movements and encrypt their traffic.[71]

- In 2017, an unplanned shutdown of a plant in the Middle East was identified as a new kind of cyberattack on the safety instrumented system (or SIS), which is the last line of defense for a safe stable shut down in the event of a process upset. Triton/Trisis is a malware that injects malicious code into the programmable memory of the Triconex SIS, through reverse engineering of the Triconex TriStation communication protocol. Due to a programing error (by the attacker) the malware caused two of the systems in the refinery to enter failsafe mode and shut the process down.[72]

- The latest campaign by Russia, with energy-critical infrastructure the focus area, was limited to access, with no physical impact identified. Intended targets were power generation, transmission, and distribution companies (targeting ICSs) that have sophisticated networks with more defensive cyber tools. The Russians deliberatively selected staging targets going back 2+ years that were smaller organizations with less sophisticated networks and preexisting relationships with intended targets (e.g., vendors, integrators, suppliers, and strategic R&D partners).[73]

Sophisticated threat actors will often leverage insiders to gain access, either wittingly or unwittingly, to do harm to the operational activity of a company, institution, or governmental organization. In most cases, the threat actor takes advantage of insider privileges to affect an attack. In addition, insiders might have access to resources that are not required to complete their job function

There are two primary vectors for insider attacks: (1) using the network and (2) direct physical access to devices. The latter occurs when a user plugs into an industrial device and distributes malware or uploads new malicious code. This type of an attack does not require digital access due to the user's physical access to the device. These types of attacks can evade network monitoring and require the detection of anomalous configuration changes and/or monitoring at the device level. Detecting these changes is only possible with an up-to-date inventory of devices and their status, including firmware versions, patch levels, serial numbers, and other information. Monitoring both network activity and device integrity are required to detect these two types of threats. (See text box titled "Department of Homeland Security Report on Insider Threat.")

69 Holmium: listed as Advanced Persistent Threat 39.

70 Radio Farda, "Iranian Hackers Caused Losses in Hundreds of Millions: Microsoft Researchers," https://en.radiofarda.com/a/iranian-hackers-caused-losses-in-hundreds-of-millions-microsoft-researchers/29808137.html.

71 Perper, R. (March 2019). "While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US and elsewhere," *Business Insider*, https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3.

72 Seals, T. (April 10, 2109). "SAS 2019: Triton ICS Malware Hits A Second Victim," *ThreatPost*, https://threatpost.com/triton-ics-malware-second-victim/143658/.

73 Blake Sobczak. (September 6, 2019). "Report reveals play-by-play of first U.S. grid cyberattack," *E&E News*, https://www.eenews.net/stories/1061111289.

DEPARTMENT OF HOMELAND SECURITY REPORT ON INSIDER THREAT

The Department of Homeland Security Science and Technology Directorate's Insider Threat project is developing a research agenda to aggressively curtail elements of the insider problem (see https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat). Although policy violations can be the result of carelessness or accident, the primary focus of this project is preventing deliberate and intended actions such as malicious exploitation, theft or destruction of data, or the compromise of networks, communications, or other information technology resources.

U.S. company Georgia Pacific experienced an insider threat attack from a recently terminated system administrator who had retained access to plant control systems. The attacker deleted all the onsite backups and then proceeded to update the distribution and quality control system configurations, which resulted in a complete production outage. Applying offsite backups did not restore production, resulting in a lengthy line-by-line investigation of the operational configuration to restart production.

g. Mechanisms of Exploitation

There are many different mechanisms of exploitation used by attackers. Some exploits leverage IT networks and move laterally into OT networks, whereas other exploits indirectly impact OT networks and systems. For example, phishing is an example of an indirect attack aimed at obtaining credentials, which can be used to access OT systems. Cybersecurity awareness training covering mechanisms of exploitation is important as employees are the front line against advanced, targeted attacks.

i. Social Engineering and Phishing

The most common instance of social engineering is phishing, where a bad actor will use deception to manipulate individuals into providing user credentials or other sensitive information that can be used to breach cyber controls. Social engineering is sometimes neglected within OT networks due to existing physical controls.

Phishing does not typically pose a direct threat to process control as communications applications (email or chat) should not be present on OT systems. Usernames and passwords are often reused across OT and IT networks so that a successful phishing attack on IT can be used to exploit OT. Companies address social engineering with a risk mitigation policy that features training, awareness, and layered defense.

ii. Ransomware

Ransomware can incapacitate a company's business operation until the ransom is paid or systems are manually restored, but thus far have not significantly affected OT systems in oil and natural gas. In May 2017, WannaCry, the biggest ransomware attack in history, spread across the globe in just a few hours. WannaCry affected the IT networks of many energy companies, but OT networks were not directly impacted. Some OT networks of non-energy companies were affected.

Despite the lack of cyber incidents within OT systems, companies remain vulnerable due to the interconnectedness with suppliers and contractors that support hardware and software. Attackers focus their attention on companies with the resources and motivation to pay ransoms. Operational shutdowns and health or safety issues are significant levers to exploit payment.

iii. Malware

The sale and exploitation of illicit and sophisticated software is readily available to threat actors. Malware kits and instructions are easy to locate and reconfigure for specific attacks against companies. Advances in technology have enabled this exchange of information and negatively affected the security landscape. Ukraine has been used as a testing ground for cyber weaponry and was experiencing more than 3,000 attacks a month at one point.

In 2015, an advanced persistent threat group known as Sandworm used malware known as BlackEnergy to target the Ukrainian power grid

with a goal of physical disruption. The use of BlackEnergy 3 was malware that migrated to the ICS network through the IT corporate network. The attackers used distributed management systems on the power grid to deliver malicious firmware updates that left operators without the automated systems for a sustained period.

In 2016, Crashoverride malware used knowledge from previous ICS attacks. Ultimately, this became a platform that was no longer vendor specific and demonstrated the advancement of ICS cyber weapons that bridged the connection between OT and IT networks and did not simply rely on exploitable vulnerabilities.

iv. Manipulation of Supply Chains

Attackers are targeting companies across the supply chain with a plan to ultimately access and exploit any weaknesses. Supply chain threats involve the injection of malicious software or hardware into third-party provided systems. These threats can expose highly sensitive data, create opportunities for bad actors to remotely access the system, or stop the device from functioning at a predefined date and time. This has affected contractors involved in national defense, essential services, and companies that supply vital hardware or software components. (See text box titled "Triton Malware.")

For maximum impact, ICS attackers need to understand the automation processes, equipment configuration, and design. Lack of standardization across vendors and existence of multigenerational equipment makes those environments more complex and difficult to decipher for the attackers, but also more difficult to defend. Customers may not be able to gain the support of vendors for partnering with them around cybersecurity threat protections. Vendors focus their research and development activities, including for patches and updates on more modern systems.

There are two notable examples where the supply chain of OT equipment suppliers was compromised. Telvent, owned by Aveva, an OT system vendor, has process control operating software that is widely used in the oil and natural gas industry and was the victim of a 2012 breach where system data was stolen. The threat actors behind the Triton malware framework had knowledge about the Triconex SIS controllers and TriStation, a proprietary network communications protocol.

TRITON MALWARE

Dragos publicly tracks eight ICS-focused activity groups and tracks more unlabeled activity of interest. These are summarized in the referenced *2018 Year in Review* report, and include XENOTIME, which was the group behind TRISIS, the malware targeting the Triconex safety systems in the Middle East discussed in this report. Triton/TRISIS specifics should be used to identify gaps and be applied to companies' own internal setups and evolving programs around OT. This includes:

- Anomaly detection might have been triggered in the attackers' early attempts and testing
- Unusual or unexpected actions investigated due to nonstandard commands from the attackers

Supply chain cybersecurity requirements are needed to ensure compliance to industry-relevant OT standards. Vendors should perform independent assessments regarding the effectiveness of their cybersecurity practices and provide these to their customers for assurance.[74] These audits should also address whether generally accepted system security and system administration practices are designed and operating effectively.

Collaboration between suppliers and operating companies is critical. There are various industry efforts now in play to encourage suppliers to standardize hardware, software, and protocols. Attackers are making advancements faster than vendors can identify and address vulnerabilities or companies can apply. OT professionals and suppliers need to partner on more innovative ways to ensure these systems are defensible.

74 Acceptable forms of assurance include an ISO27001 certification, SOC 2 Type II audit report, or a similar form of independent audit evidence.

Findings:

- Enhanced cybersecurity architecture and design specifications of OT systems are needed to establish effective systems and controls, including addressing human factors exploited by threat actors. Enhanced design specifications would prompt additional research and development in patching and detection and result in customers being more able and willing to upgrade and/or standardize their multigenerational equipment more efficiently to accept these updates.
- The supply chain threats need to be understood, designed, and managed as an entire system in a disciplined manner. Attackers leverage vendors with less sophisticated capabilities to build bridges into their ultimate targets.

The NPC recommends that companies involved in the production, manufacturing, and transportation of oil and natural gas should specify requirements in purchasing contracts with OT suppliers to adhere to industry cybersecurity standards and related development. OT suppliers must provide timely updates, such as patching, for cyber vulnerabilities.

2. Industry Response to Evolving Threats

The National Cybersecurity and Communications Integration Center (NCCIC) reported that the energy sector, which includes electrical power and transmission, nuclear, and oil and natural gas, experienced more cyber incidents than any sector from 2013 to 2015, accounting for 35% of the 796 incidents reported by all critical infrastructure sectors. In 2016, NCCIC reported that the energy sector was the third most frequently attacked sector. In March 2018, the NCCIC reported that a nation-state had targeted organizations within multiple U.S. critical infrastructure sectors, including the energy sector, and collected information pertaining to ICSs.

Energy companies have enterprise risk management programs, which have elevated cybersecurity risk as a top priority. The business risk and associated mitigations for cybersecurity threats are developed and presented to the executive management and boards. It is clearly recognized that energy is a core component of critical infrastructure and public safety is paramount for security programs. The increasing capabilities of nation-states and organized crime actors is driving the need for cybersecurity program improvements. (See the "World Economic Forum Report" text box regarding cyber resiliency principles.)

The *Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry* report acknowledges "... that cyberattacks can present 'enterprise risks' – risks that could compromise the viability of a company – and have developed comprehensive approaches to cybersecurity similar to industry's approach to managing safety; robust governance, systematic risk-based management, and multi-dimensional programs based on proven frameworks including the NIST [National Institute of Standards and Technology] Cybersecurity Framework (NIST CSF), best-in-class international cybersecurity standards including ISA/IEC 62443, and the Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2)."

Companies are continuing to adopt risk management cybersecurity frameworks (e.g., NIST, ISO, API). The private and public sectors are collaborating to align and improve the frameworks and the response to cybersecurity incidents. Expanding adoption of risk management frameworks is important to improve protection from cybersecurity threats. Performance-based standards will allow for more rapid and efficient adoption of new practices that are largely driven by technological advancement, emergence of new threat actors, and the resulting risk landscape. Expanded usage of technology within ICS networks requires additional compensating cybersecurity controls. For example, oil and natural gas companies are deploying more Internet of Things and Industrial Internet of Things sensors to closely track flows and data related to operations.

WORLD ECONOMIC FORUM REPORT: *CYBER RESILIENCE IN THE ELECTRICITY ECOSYSTEM: PRINCIPLES AND GUIDANCE FOR BOARDS*

"Cyber risk is business risk. In the electricity industry, cyber risk is also an ecosystem-wide risk. Cyber resilience is a challenge for all organizations, but it is of particular importance for the electricity ecosystem. A large-scale blackout would have socioeconomic ramifications for households, businesses, and vital institutions. For example, a six-hour winter blackout in mainland France could result in damages totaling over $1.7 billion. Traditionally, managing this risk has meant dealing with issues such as component failure or inclement weather via robust mitigation and recovery plans. Today, however, existing resilience plans in electricity delivery must integrate a carefully designed cyber resilience strategy."*

* World Economic Forum Report by Centre for Cybersecurity and Electricity Industry Community in collaboration with Boston Consulting Group. (2019). *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.

B. Improving Cybersecurity for the Oil and Natural Gas Industry

Defending against OT cyber threats requires coordination across the oil and natural gas sector. Attacks on ICSs differ based on several factors, including the adversary's intent, sophistication and capabilities, and familiarization with ICSs and automated processes. Understanding different adversaries and their technological capabilities enable companies to make better-informed decisions regarding defensive status and future planning.

Companies are at different levels of implementing robust and comprehensive cybersecurity programs focused on protecting OT systems. Individual components of cybersecurity programs may also have different maturity levels, such as the development of cyber incident response plans, periodically recurring cyber risk assessments, and penetration testing of both existing controls and the introduction of new technology.

1. Improvement of Cyber Management Programs

The goal of a comprehensive cybersecurity risk management program should account for well-designed system architecture and effective controls. The cyber program should set goals, objectives, and priorities to successfully execute the full range of the company's responsibilities. The program should be based on industry standards that leverage the expertise of cybersecurity industry professionals and frameworks such as the NIST Cybersecurity Framework.

Strategic cyber objectives and initiatives should align with frameworks and standards such as the NIST Cybersecurity Framework while applying a Defense-in-Depth approach. Industry adoption of a voluntary framework to address cybersecurity is resulting in overall cyber improvements as many oil and natural gas companies have adopted frameworks specific to the business functions. In the pipeline sector, API 1164 standard establishes a cybersecurity framework that has been adopted by many companies (refer to Section VI.B regarding API 1164 at the end of this chapter). API 1164 was last updated in 2009 and is under review to publish a current revision. As seen with health, safety, and environmental management systems adopted within the industry, voluntary programs are successful in driving improvement.

The cyber-related regulatory environment for oil and natural gas currently includes the Coast Guard (marine) and Transportation Security Administration (TSA) (pipeline). Adding new prescriptive regulations could complicate the goal of effective cybersecurity through a suboptimum allocation of resources, creating future issues with coverage, resources, effectiveness, and efficiency. One of the most significant issues at the regulatory level is a lack of resources, investment, and expertise. A more prescriptive environment stands to exacerbate the gap between the rapidly evolving cyber threats and current operating posture of the average oil and natural gas company. The most effective approach for cyber protection in the oil and natural gas industry is alignment and adoption of

proven risk-management-based frameworks and public-private collaboration rather than prescriptive regulation.

Cybersecurity improvements should be prioritized for the most critical OT assets and processes. Following are some examples of OT cyber-related best practices:

- Multifactor authentication for remote access requiring an additional step beyond user ID and password
- Cyber controls on contractor and engineering workstations
- Management of removable media control[75] such as USB ports to prevent unconstrained introduction of viruses or malware
- Integration of ICS logs into the security incident event monitoring systems[76]
- Intrusion detection systems[77] to report on anomalies
- Predefined cyber response plans specific to OT assets, including drills and tabletop exercises.

The NPC recommends that:

- Industry, in collaboration with trade associations and federal government agencies, should adopt and maintain up-to-date performance-based cyber security management standards. These standards should be continuously updated to keep pace with corresponding digital technology advancement and changes to the cyber threat landscape.
- Oil and natural gas companies with DHS-identified critical infrastructure should adopt industry-specific cybersecurity standards. Conformance with these standards should be verified through independent audits and assessments conducted by recognized or authorized entities, including but not limited to government-sanctioned entities. DHS and other regulatory agencies should update the assessment mechanisms to address any ongoing recommendations, including those relating to the potential limitations of a voluntary framework.

a. Inventory and Asset Management

Protecting OT begins with building and maintaining a comprehensive inventory of networked and nonnetworked (or isolated) assets. An accurate inventory of asset information (e.g., firmware, hardware configuration) is difficult to gather and maintain, given the breadth of some networks such as pipelines and remote field sites. Lack of up-to-date information, such as with older or proprietary legacy systems, is a significant challenge with companies that have these systems.

With an accurate inventory, visibility into the security status of the OT assets is achievable. An accurate and complete OT asset inventory is necessary for effective monitoring to reduce vulnerabilities across the organization to an adequate level of risk. The greatest risks to the OT system can be identified by focusing on the critical functions of the industrial control system. Once an accurate inventory is established, the operator then must manage change across devices and components within field devices.

Establishing visibility across both IT and OT networks by integrating security tools and the data they generate can help detect lateral attack activity or malware from remote access or USB transmits. The application of security tools should be prioritized based on process criticality and other risk-based considerations.

A detailed configuration baseline is a key component of the asset inventory. Configuring the industrial control system involves the operationalization of the processes that run in every OT environment, one of the functional benefits of the detailed asset inventory is that it enables both forensic analysis in the event of an issue and boosts the recovery capabilities should they be needed.

75 A form of computer storage that is designed to be inserted and removed from a system. Using removable media poses some risks, including data theft and the introduction of malware.

76 Security information and event management, software products, and services provide real-time analysis of security alerts generated by applications and network hardware.

77 An intrusion detection system is a type of security software designed to automatically alert administrators when someone or something is trying to compromise an information system through malicious activities or through security policy violations.

b. *Vulnerability Analysis and Threat Monitoring*

OT systems require different threat monitoring and vulnerability assessment tools than IT systems require. Conventional scans to discover and detect exploits or anomalous behavior can adversely affect OT systems as those systems were not designed to withstand such probing. Nonintrusive assessment is more effective as traditional security monitoring tools can create traffic on a network that could cause a control signal to be missed. Traditional signature-based security systems such as antivirus software are less effective against advanced threats. Current practices such as monitoring firewalls and perimeters of OT networks will not stop a persistent, skilled attacker. OT-oriented threat monitoring tools that are compatible with the protocols these systems use have started to develop in the marketplace.

Ongoing visibility and monitoring into both the IT and OT environments is critical for detecting the various stages of an intrusion. Threat detection and mitigation should monitor for anomalies that could represent cyber threats, operational issues, or configuration and programming mistakes.

Sources of vulnerabilities are a matter of continuous discovery. Examples of sources include OT cyber vulnerabilities published by third-party services, governmental sources, and supply chain vendors. Additional vulnerabilities may be reported by peer companies. These various sources can be merged and matched against each company's inventory of OT assets and programming to ensure all prioritized risks are identified and addressed.

Companies are ideally receiving regular reports of risk levels for the assets in their OT networks. However, enterprise visibility is difficult due to nonnetworked systems. Enterprise visibility of information allows for evaluation of OT risk and allows for prioritization of mitigation steps. For example, interstate pipeline assets are distributed across wide geography reaching thousands of miles. These pipeline assets typically have sensors and actuators in the field with remote terminal units[78] that can be hard wired or connected by satellite or cellular communications. One-way satellite and cellular communications from them will transmit variables, such as flow and other inputs for SCADA, but do not have visibility to all sensor data and firmware versions and changes. Because these are not connected to a network, operators are challenged with gathering security-related data and assessing risk. The lack of network connectivity helps protect them from Internet and email driven malware, but it also hinders companies' ability to gather security-related information. Threat behavior analytics provide insight into abnormal activity. This is important given the level of complexity and potential for false positives in the OT environment.

c. *Management of Change and Change Detection*

Management of change (MOC) is a mature industry discipline that enables safe and reliable operations and includes the design and operation of ICS. Without detailed analysis of changes, configuration of OT assets can inadvertently create vulnerabilities that can be exploited. A systematic approach to managing changes to the configuration settings provides the visibility needed to track authorized changes and identify, investigate, and correct unauthorized changes. This includes changes to the OT systems that control physical assets and industrial processes. A sophisticated OT attacker will try to adjust existing configurations without being detected by monitoring functions. The potential points of attack might be changing a set point or adjusting to a higher rate than normal.

Change protection involves tracking and logging configuration changes, whether executed by a human user or by malware, over the network or physically at the device. Each company should understand the system controls it has in the field and know when those controls are changed. This also is important for effective forensics to investigate and understand what is occurring during or after an event.

78 A remote terminal unit is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA system by transmitting telemetry data to a master system and by using messages from the master supervisory system to control connected objects.

Some companies outsource configuration or MOC regarding OT to third parties. In this case, documentation becomes crucial. Without the right MOC procedures this can create risk, particularly if there are multiple providers, because it increases the touchpoints and complexity. Third parties must be aligned with the owner's expectations, and the owner must train or educate third parties against these expectations prior to access being granted. Vendor screening is important to ensure organizational confidence in contracted or partnered companies.

d. Reducing Threats and Vulnerabilities

OT system patching practices are complicated and need improving. Unlike IT, it is not possible to reduce vulnerabilities by rolling out patches automatically. Many of these systems run 24/7, and operators cannot interrupt production to install a security patch or new firmware version. Installing a patch or new firmware is a configuration change that can have negative side effects, including downtime. Vendors do not have a consistent method for publishing approved patches; this complicates asset owners' responsibilities.

There are many challenges to having an effective patch management process in OT environments involving thousands of varying components. ICS vendors test and certify patches prior to deployment. These patches or firmware updates need to be checked for compatibility with installed software applications and libraries. The vendor is typically in control of the update life cycle.

Cybersecurity improvements must be prioritized based on risk. There is not an expectation to add cyber protections to all devices. In taking actions, companies need to consider factors such as criticality of the process, cost/benefit of the fix, and feasibility of patching the device. There are additional mechanisms to reduce threats and vulnerabilities beyond patching, such as access control, software management, and physical control.

Companies reduce cyber threats by increasing their detection, response, prediction, and prevention capabilities. Defenders must focus on understanding the required steps an attacker must take, from initial intrusion through ultimate effect, and build a robust security posture to impede those steps. Cyber teams perform a critical role in cybersecurity risk management by focusing on the threat and developing capabilities and resources to enhance investigative efforts and address evolving challenges, including the growing use of anonymous networks, and sophisticated attack strategies design for OT.

e. Incident Response, Recovery, and Investigation

Companies must enhance their incident response capabilities to minimize the impact following an incident by containing the unwanted intrusion, safeguarding critical functions, and coordinating with internal and external stakeholders. This is accomplished through cyber incident response teams, which play an important role in responding to cyber incidents to mitigate potential consequences by providing technical assistance to affected entities and other assets that are at risk as well as investigating the underlying causes.

Companies should develop response plans with the expectation that a breach of OT systems will occur. OT systems are not impenetrable. Breach preparation and incident response plans have been traditionally more focused on IT scenarios. Since most attacks have come from these sources, these plans will need to adopt OT-related scenarios given the potential impacts of such incidents. Backup configurations to restore operations and logs to analyze, monitor, and perform forensics are necessary for incident response and recovery.

OT cyber response plans should be coordinated with a company's emergency response organization. Emergency response plans will benefit from adoption of a unified incident command system that improves response effectives and coordination with regulatory agencies. Cybersecurity response plans can be included within existing plans such as incident response, business continuity, crisis communications, and disaster recovery.

Lack of transparent reporting of ICS cyber activity and incidents could lead to systemic threats across an industry sector. Companies should investigate cybersecurity incidents with the same rigor as safety incidents. The nature of the threat and

failure analysis of cyber protections are required to continuously improve cybersecurity controls. Establishing cybersecurity investigation requirements and protocols should ensure timely investigation, resolution, and actionable information sharing across the industry. Beyond regulatory reporting requirements, companies have discretion when information is shared within industry and governmental agencies.

f. Improving the Partnership between IT and OT Professionals

Proper cybersecurity assessments require collaboration between IT and OT professionals, business stakeholders, and third parties to gain an adequate understanding of overall cybersecurity risks, interdependencies, and evolving methods of exploitation. Different knowledge and technological tools are required to fully understand and assess industrial and process controls. Process control engineers may not have an adequate understanding of cybersecurity controls or techniques to perform risk assessments of ICSs.

Cyber protection experts need to be working hand in hand with SCADA/process control experts. This is a significant cultural change in many companies. Executive management should develop a strategy to ensure IT and OT professionals work together. Effective OT/IT partnerships will encourage the reporting of incidents and provide expertise to support incident investigation. Encouraging a culture of reporting, notification, and information sharing will increase the security and resilience of critical infrastructure.

Partnerships should be extended to supply chain vendors to enable more effective sharing of insight, challenges, and risk. This activity can help identify likely attack paths, enable risk mitigation actions such as risk assessments, drills, vulnerability analysis, and expansion of threat monitoring.

There are different priorities driving IT and OT organizations. IT personnel focus on the confidentiality, integrity, and availability of business systems and data. OT personnel prioritize safety, uptime, reliability, and optimization of processes. Rather than developing OT professionals with detailed knowledge of cybersecurity controls, many find it better to require IT and OT professionals to work collaboratively on OT solutions.

Finding: The effective design, installation, and maintenance of industrial control systems requires integration of cyber expertise, usually located within IT, with process control disciplines to ensure cyber risks are adequately addressed.

The NPC recommends that industry should revise and update existing standards, including API 1164, to incorporate the following elements into cybersecurity programs:

- Organizational Structure: Cyber and process control disciplines must jointly manage the design, development, and change management of process control systems.
- Asset Inventory and System Monitoring: Establish robust OT component, system, and process control network monitoring processes and practices, including effective management oversight and risk assessment. Incorporate the impacts of the impending convergence of IT and OT systems as well as future major technology planning elements such as Industrial Internet of Things architectures and technologies. Ensure appropriate integration with contractor/supplier management policies and practices.
- Emergency Planning: Based on criticality analysis of the ICSs that includes commitments to customers and/or reputational considerations, performance expectations for recovering compromised systems should be established and tested.
- Event Investigation: Establish cybersecurity investigation requirements and protocols. Establish a corporate compliance verification process to ensure appropriate closure and follow up of action items. Share internally while abiding by security classification requirements to promote learning and program improvement.

Cybersecurity expertise is in short supply around the world, with the shortfall of qualified cybersecurity professionals anticipated to be as much as 1.8 million globally by 2022.[79] Many of the professionals working on OT systems have been resourced from various engineering roles within the company. Industry and educational institutions can incentivize and subsidize new curricula and continuing education from academia and private industry for OT cybersecurity. This labor shortage also increases the need for more automation and broader use of advanced analytics and machine learning to address incident detection and response.

The NPC recommends that:

- Oil and natural gas companies should increase efforts to support staffing and training requirements and develop a consortium to address these needs, with guidance for common skills, transportable knowledge, and industry-wide growth in capabilities associated with automation systems, safety, and security.

- Oil and natural gas companies should increase efforts to work with education institutions to grow industry workforce knowledge and organizational capabilities in industrial cybersecurity technologies and practices as applied to oil and natural gas system design, development, and operations:

  – Professional education: Encourage and support university engineering degree programs to incorporate relevant curriculum on the essential elements of cybersecurity fundamentals, technologies, and practices. Specific priorities are those engineering disciplines directly related to the oil and natural gas industry, including (but not limited to) chemical engineering, petroleum engineering, process and mechanical engineering.

  – Workforce development and training: Encourage and support the development and delivery of educational and training programs by industry, academia, and government targeted to industry professionals and operations personnel. The objective is to significantly enhance individual and organizational capacities to effectively incorporate current and evolving cybersecurity technologies and practices into oil and natural gas asset development and operations.

2. Improving Collaboration with Key Stakeholders

Companies should proactively collaborate with governmental agencies, industry peers, and information sharing and analysis centers (ISACs) in establishing best practices and communicating on cybersecurity incidents. Cybersecurity risks are opaque due to the evolving and changing nature of the threats. The presence of better OT cyber metrics would provide a shared understanding of cyber activity to collaborate with supply chain providers, ISACs, and industry peers. Companies may be reticent to share this information at the risk of further exposing their vulnerabilities or creating reputational impacts. (See text box titled "Summary of U.S. Government Activity to Support Protection of Key Infrastructure.")

There are several governmental entities involved in information sharing and collaboration. Most notably, DHS's Risk Management Center assesses systemic and aggregate risks, including critical infrastructure. In response to recent concerns and areas of interest, DHS has recently been engaged with the pipeline industry and has initiated a program of assessments of ICSs for natural gas companies. The focus of the assessments includes analysis of architecture and network traffic. The assessments are intended to identify areas where proactive cybersecurity controls can be implemented or improved. DHS is finding that most of the companies have created or are establishing robust cybersecurity programs, layered defenses, and are aiming to improve cyber resilience. DHS assessments are one example of public and private collaboration occurring in the oil and natural gas

79 Crunpler, W., and Lewis, J. A., (January 291, 2019). "The Cybersecurity Workforce Gap," Center for Strategic and International Studies, https://www.csis.org/analysis/cybersecurity-workforce-gap.

industry. (See text box titled "Validated Architecture Design Review.")

VALIDATED ARCHITECTURE DESIGN REVIEW

In mid-2019 the DHS National Risk Management Center and TSA partnered with the pipeline industry, oil and natural gas companies to conduct cybersecurity reviews. The assessment platform was framed within the NCCIC's National Cybersecurity Assessments and Technical Services Validated Architecture Design Review (VADR). The Pipeline VADR is built on the NIST Cyber Framework, NIST-800, TSA Pipeline Security Guidelines and ICS Defense in Depth Practices. The VADR was intended to provide pipeline owners a comprehensive evaluation and discovery process, focusing on defense strategies associated with asset owners' specific control system's network design, configuration, interdependencies and applications.

A cybersecurity threat faced by one sector could find its way into other sectors due to commonalities in OT systems. The threat and vulnerabilities faced by the oil and natural gas are the same that exist for several other critical infrastructure sectors because of common ICS components. Attacks in other industries can be easily reengineered toward oil and natural gas companies. Correlating the potential of cross-sector ICS threats and vulnerabilities should be a focus of multiagency government councils. The National Risk Management Center should provide cross-sector collaboration on systemic risks. Collaborative assessments of cyber programs should be prioritized on natural gas delivery systems where geographic resiliency is most important.

The National Risk Management Center is working closely with other federal partners and the oil and natural gas industry to understand the types of assessments being conducted and the desired outcomes. DHS should continue to focus its efforts on coordinating cross-industry activities to improve system architecture, model attack scenarios, and conduct other analysis. Agencies should consider using accredited third parties to perform risk-based cyber assessments rather than bearing the entire cost. For critical infrastructure, there should be independent validation to ensure protection from systemic risks.

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the DOE's emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyberattacks, natural disasters, and human-made events. CESER also addresses emerging threats by improving energy infrastructure cybersecurity and supporting the DOE national security mission. CESER's focus is preparedness and response activities to natural and man-made threats to ensure a more secure future for the nation. CESER is tactically and strategically addressing the increased frequency and sophistication of cyber threats and is investing in industry-specific research and development. CESER leverages the National Labs to test components and configurations based on feedback from industry. Continuous monitoring tools and capabilities for information systems and control networks and identifying best practices are also supported by CESER's Cybersecurity Risk Information Sharing Program.

Being prepared and ready to respond quickly and effectively to all hazards is crucial. CESER partners with companies across the energy sector and occupies a critical role in coordinating federal and state government strategies with industry. Furthermore, CESER, along with energy sector partners, prepares for various types of emergencies through exercises such as Clear Path, Liberty Eclipse, and GridEx. These exercises help DOE, industry, and government partners test and improve plans, as well as provide insights for future R&D needs. When an incident occurs, CESER facilitates coordination across the government and with the energy sector to enhance response and recovery efforts while coordinating federal capabilities to mitigate the impact of energy disruptions.

Additional collaborative efforts to improve cybersecurity programs include the following:

- In 2018, TSA and FERC provided voluntary architecture and security reviews to pipeline companies. The program was modified in 2019

SUMMARY OF U.S. GOVERNMENT ACTIVITY TO SUPPORT PROTECTION OF KEY INFRASTRUCTURE

The National Infrastructure Protection Plan (NIPP) aims to unify critical infrastructure and key resource protection efforts. NIPP is a mechanism for developing coordination between government and the private sector. Department of Homeland Security (DHS) and Department of Transportation have oversight of the transportation systems sector. Each sector has a government coordinating council consisting of representatives from various levels of government, and many have a sector coordinating council consisting of owner-operators of these critical assets or members of their respective trade organizations. NIPP is structured to create partnerships between these government coordinating councils from the public sector and sector coordinating councils from the private sector for the 16 sectors DHS has identified as critical. The NIPP established a framework to conduct risk assessments to understand the most likely and severe incidents that could affect operations and communities and use this information to support planning and resource allocation.

Within DHS, the National Cybersecurity and Communications Integration Center (NCCIC) partners with other government agencies, the private sector, and international entities. The NCCIC analyzes cybersecurity information, shares timely and actionable information, and coordinates response, mitigation, and recovery efforts. The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical IT and communications networks. NCCIC's role is to serve as the federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings with federal and nonfederal entities, and to provide shared situational awareness to enable real-time actions to address cybersecurity risks and incidents to federal and nonfederal entities.

The National Risk Management Center (NRMC) was created in July 2018. The Pipeline Cybersecurity Initiative was established as one of the first NRMC efforts and announced to industry during the Oil and Natural Gas Sector Coordinating Council meeting in October 2018. Intended to enhance DHS risk management planning and response, the NRMC would provide sector and cross-sector critical infrastructure risk management and vulnerabilities analysis. In November 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency (CISA) Act. The law prioritizes CISA's mission as the federal leaders within the U.S. government for cyber and physical infrastructure security. CISA would continue to serve as the hub through which information sharing of cyber threat indicators occurs, such as from the ONG-ISAC to and from the U.S. intelligence community via DHS and the NCCIC, which is part of the new CISA.

to be administered by TSA and DHS and has been rebranded to the Validated Architecture Design Review.

- In 2018, representatives from the electric industry regional transmission organizations, the U.S. government (DOE, FERC, and TSA), and natural gas pipeline owners and operators met for a tabletop exercise to facilitate better understanding of how they would respond under a cyberattack affecting SCADA during a multiday cold snap that stresses natural gas and electrical power delivery and to support development of professional relationships.
- Several states have state-managed fusion centers[80] that serve as information sharing hubs.

80 Fusion centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial, federal, and private-sector partners.

- DOE and FERC cohosted a Security Investments for Energy Infrastructure Technical Conference in 2019 to discuss current cyber and physical security practices used to protect energy infrastructure. The conference explored how federal and state authorities can provide incentives and cost recovery for security investments, particularly the electric and natural gas sectors. (See text box titled "Shared Responsibility Model.")

The NPC recommends that DHS and DOE should increase capabilities and resources to support independent and secure cybersecurity assessments prioritized on critical infrastructure. Assessments should be conducted by authorized entities, including but not limited to government-sanctioned entities. Cybersecurity assessments should be informed by current threat intelligence information sharing and lessons learned from cyber incidents.

Federal policy has encouraged voluntary information sharing mechanisms between the federal government and industry. Among other consortiums, the Oil and Natural Gas Information Sharing and Analysis Center shares threat information from member organizations and governmental agencies. Timely threat information is vital in addressing new vulnerabilities and assessing indicators of a potential breach. Cyber committees within industry groups work closely with existing ISACs, governmental agencies, cybersecurity consulting companies, and industry members.

ISACs are self-directed and determine their own mission and scope. ISAC effectiveness depends on broad industry membership and on submission of threat intelligence by member companies. Challenges that hinder the quality of information sharing include visibility of asset inventory, vulnerability analysis, and monitoring OT cyber threats. As OT-related submissions increase and submission quality improves, ISACs can improve rapid response mechanisms to receive, analyze, and share cyber threat indicators and defensive measures with member companies.

There are new regional collaboration groups beyond ISACs that are forming to improve communications (see text box titled "Neighborhood Keeper"). As governmental agencies declassify actionable information more quickly and share with ISACs and regional groups, industry can better respond to emerging threats. The current backlog in granting security clearances is affecting the sharing of information in a timely manner.

Finding: Collaboration to share cyber threats is increasing between industry, trade associations, and federal governmental agencies. OT cyber threat sharing often lacks the necessary transparency among and within companies that is necessary to improve effective cyber management practices. Current practices can result in findings that are overly sanitized and are inconsistently shared.

The NPC recommends that the DHS, working with DOE, other federal agencies, and the oil and natural gas industry, should assist sector ISACs and regional groups to promote information sharing, including learnings from investigations. DHS should encourage increasing ISAC membership across industry sectors. DHS and other federal agencies should quickly share actionable information with ISACs and operators.

SHARED RESPONSIBILITY MODEL

"The threats against our nation's energy infrastructure, particularly the electric and natural gas sectors, continue to grow and the responsibility for protecting our energy infrastructure is shared across industry as well as states and the federal government. In light of this shared responsibility, we will join with DOE to explore current threats against energy infrastructure, best practices for mitigation, current incentives for investing in physical and cyber security protections, and current cost recovery practices at both the state and federal level."

—FERC Chairman Neil Chatterjee

NEIGHBORHOOD KEEPER

Recognizing that less sophisticated entities provide an environment for adversaries to train and prepare undetected, Dragos began work on Neighborhood Keeper, a research and development effort in concert with the DOE, Idaho National Labs, the Electric ISAC, Ameren, First Energy and Southern Company, to bring affordable threat detection technology and shared insight to a broader set of infrastructure providers.

3. Advancing Cybersecurity R&D within the Oil and Natural Gas Industry

Many cyber incidents involve exploitation of vulnerabilities or misconfigurations in software or hardware. OT system operators are also increasingly dependent on suppliers of off-the-shelf products or integrators of commercially available products and lack the capability to effectively manage supply chain risks. Efforts to research and develop technological innovations will result in more secure OT infrastructure.

Collaborative research consortiums will be required to advance OT cybersecurity technologies. A properly constructed consortium can foster innovations and improve security and resilience. Consortium members, including IT, communications, and cybersecurity services should collaborate to incentivize and enable cybersecurity outcomes such as minimizing vulnerabilities and addressing supply chain risks.

As an example, LOGIIC[81] was formed in 2004 to facilitate cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. After a successful first project, the LOGIIC consortium was formally established as a collaboration between DHS, the Automation Federation, and five of the major oil and natural gas companies. Industry should invest in research and development efforts that support the goal of decreasing OT cybersecurity risk leading to negative physical outcomes.

API Information Technology Security Subcommittee (ITSS) members have proposed to develop an ongoing process to provide ideas for research programs as part of an annual process. This could be the start of a research forum and be expanded to other industry groups (e.g., Interstate Natural Gas Association of America and American Gas Association). The API ITSS started to identify areas of research, involving the Industrial Internet of Things, software defined networking, patching/vulnerability management, resilient systems, artificial intelligence and machine learning, and next-generation networks, including 5G wireless.

The NPC recommends that DOE, working with industry, DOD, DHS, and DOT, should establish a collaborative process to identify and prioritize research and development aimed at sector-wide protection against nation-state and advanced persistent threat actors. The process should include the following:

- Centralized input to research entities according to established criteria based on current and anticipated threats.
- R&D efforts focused on the transportation types with the highest risk posed by cyber OT threats.
- Funding, partnering, or incentive opportunities to reduce cyber OT risks.

C. Cybersecurity Conclusion

The risk to OT has increased due to the convergence and growing interconnectivity between IT and OT networks along with the increased activity and focus of threat actors on the energy sector. Historical protections of isolation and segmentation are consequently being eroded due to these activities.

Defending against OT threats begins with a comprehensive cybersecurity risk management

81 Department of Homeland Security, Linking the Oil and Gas Industry to Improve Cybersecurity Program. (2016). "Improve Linking the Oil and Gas Industry to Improve Cyber Security," https://www.dhs.gov/science-and-technology/logiic.

program based on industry best practices and frameworks, applying a Defense-in-Depth approach that protects both IT and OT networks.

Companies within the oil and natural gas industry must expand and improve the focus of sector-specific ISACs that promote information sharing and learnings from cyber investigations. Improving the cyber skillsets that support ICSs and creating transportable knowledge between IT and OT professionals should be supported by industry. Improved collaboration and information sharing between governmental agencies, supply chain providers, and industry will enable oil and natural gas to improve cybersecurity protections.

Based on this analysis, the executive level recommendations are as follows:

- Cybersecurity protections should be advanced through:
- Industry, trade associations, and federal government agencies collaborating to maintain up-to-date performance-based Cyber Security Management Standards to be adopted by industry.
- Increased DHS and DOE capabilities and resources to support independent and secure cyber security assessments and audits prioritized on critical infrastructure.
- DOE, working with industry, DOD, DHS, and DOT, to establish a collaborative process to identify and prioritize research and development aimed at sector-wide protection against nation-state and advanced persistent threat actors.

V. SUMMARY OF FINDINGS AND RECOMMENDATIONS

This chapter has highlighted the technology advancements in the oil and natural gas transportation section that have continuously improved safety and environmental performance over the past several decades and have assisted in driving improvements in reliability, efficiency, and cost effectiveness. The following is a summary of the findings and recommendations identified through the study.

Finding	Recommendation
I.D.5 Technology Advancement and Deployment Challenges	
Industry, in cooperation with federal agencies, is advancing promising new technologies to prevent high-impact events. Adoption of new technology can be impeded by high early-adopter costs. Existing regulations, prescriptive and performance based, are designed to promote safety. However, some prescriptive aspects of existing regulations slow the adoption of new technologies. The sometimes-lengthy regulatory review and approval process for introducing new technology increases the cycle time for wide-scale adoption.	Congress should authorize DOT to lead a collaborative effort, with support from industry, to develop and prioritize pilot programs that can accelerate pipeline, storage, and LNG technology adoption based on performance-based rules with a goal of enhancing public safety. Upon successful completion of pilot programs, regulators should promptly update their regulations to allow use of new technology. Oil and natural gas transportation companies should establish a collaborative effort with participation from DOT, DOE, EPA, and industry research consortiums to prioritize promising, risk-based research opportunities, to establish consistent technical readiness processes, and to prioritize field validation testing needs. DOT should lead, while working with DOE, EPA, and U.S. Coast Guard, creation of an agile pathway for evaluation and regulatory acceptance of new technologies that can improve transportation safety and shorten the research, deployment, and adoption cycle time. The Federal Energy Regulatory Commission and state regulatory agencies should work with DOT, DOE, and others to promote laws, regulations, and public-private partnerships that support funding protocols and/or cost recovery for natural gas and oil pipeline safety research.
II.B.1. Asset Integrity Overview	
API RP 1173 has been vital to improving pipeline industry safety performance through standardization of key elements and expectations of management systems.	Pipeline companies should continue to seek opportunities to proactively implement safety management systems and strengthen industry-wide safety culture to continuously improve performance.
II.B.2. Inspections and Feature Detection	
Industry-led standards and recommended practices continue to be updated with the latest methods and a more streamlined regulatory acceptance process could promote accelerated risk reduction. Many of the in-line inspection technologies available to the pipeline industry collect large amounts of data that must be processed and interpreted. Currently, operating companies, working with their ILI supplier, do this validation and interpretation individually. With better collaboration between and among industry operators and ILI tool suppliers, the accuracy and validation cycle time could be accelerated.	PHMSA should accelerate its process for validating and incorporating safety and environmental performance aspects of the latest editions of industry standards and recommended practices that are referenced in the regulations, to the extent practicable.

Finding	Recommendation
II.B.3.a. Regulatory Pathways	
A subset of prescriptive requirements within PHMSA regulations have limited industry's ability to accommodate risk-based assessments which, if incorporated, would allow companies to improve resource allocation and speed adoption of technology. Certain prescriptive requirements within existing PHMSA regulations discourage field testing of new inspection technologies where the performance, accuracy, and repeatability of a technology is not yet proven. This issue can add significant costs to address regulatory requirements associated with conducting trial runs and thereby can slow the adoption of new technology.	
II.B.3.b. Industry Collaboration on Safety	
Additional participation and investment in joint industry projects could improve prioritization and speed development and deployment of new and promising technologies that address industry-wide challenges, such as those related to corrosion, cracking, and material pipe/weld failures.	Industry, working with PHMSA and ILI technology providers, should develop a collaborative pathway to support the testing and validation of new inspection technologies that can lead to acceptance into approved integrity management requirements.
II.C.2. Leak Detection Technologies	
Robust and effective leak detection capabilities exist today. Additional detection of the smallest release rates may be improved by validating newer linear monitoring systems and integrating them with other mature technologies.	Industry, working through research consortiums, should pursue a pilot program as recommended to be established by PHMSA to advance linear monitoring systems (e.g., fiber optics, hydrocarbon detection cables, hybrid discrete sensor cables) that could provide additional leak detection capabilities.
II.C.3. Geological Hazard Monitoring Technologies	
Desktop research continues as the foundational approach for geohazard management. A portion of the applicable data that is needed is publicly available but is not readily accessible from central repositories for consistent use across industry.	DOE and DOT should work with FEMA, NOAA, USGS, or other relevant agencies to organize an information sharing effort to increase collaboration on geohazard management among federal, state, and local agencies, and pipeline operators. This should drive use of consensus-based standards for storing data (e.g., Pipeline Open Data Standard or other similar standards) now used within the pipeline industry.
II.C.4.c. Geospatial Analytics	
Currently no industry-wide standards exist to support consistency in design of data analytics software or data management solutions for reliable and cost-effective remote sensing applications.	DOE, in cooperation with DOT and other relevant agencies, should organize an information sharing effort to assist with efficient acquisition and management of industry-specific geospatial data.

Finding	Recommendation
II.C.4.d. Applications by Platform	
The pipeline industry has not widely adopted space-borne remote sensing technologies because of the limited availability and selection of appropriate sensors, delayed frequency of data collection, and high costs of data acquisition. Field-level validation of sensors and analytical methods are necessary to advance their acceptance and use in integrity management programs.	DOE should work with industry to sponsor R&D programs to promote collaboration among data vendors (existing and emerging), operators, and government that can bolster regulatory and industry confidence and acceptance of RST-GA solutions to expedite the adoption and deployment of the technologies, and leverage improvements in data accessibility and costs.
II.D.2. Prevention of Pipeline Corrosion Failures	
	DOE, working with PHMSA, industry research organizations, and coating manufacturers, should support research and development on new pipeline and repair coating systems that are highly durable and damage resistant during construction and remain so throughout the expected life of a pipeline with minimal need for other protective measures.
II.D.3. Improvements to High-Strength Steels and Welding to Reduce Material Pipe/Weld Failures	
The development of a new generation of high-strength pipeline steels has allowed companies to build new pipeline infrastructure more cost-efficiently.	DOE, working with the pipeline industry, should sponsor research and development to improve stability of TMCP steel's physical properties that are exposed to high heat conditions above 500°F.
II.D.4. Improved Field Inspection Technologies to Reduce Material Pipe/Weld Failures	
	Industry and research consortiums should collaborate with PHMSA to complete technical development and validation of advanced field inspection technologies to accurately size features.
II.D.5. Assurance of Long-Term Pipeline Repair Integrity to Protect Against Corrosion and Material/Weld Failures	
The pipeline industry uses both steel and composite pipe sleeves as suitable, reliable repair methods for restoring integrity to damaged pipeline systems. When inspection of these sleeves may be needed, a visual inspection is the primary method, which can be challenging to access.	DOE should sponsor research and development on inspection technologies that would allow pipeline operators to inspect the condition of installed steel and composite sleeves throughout their life cycle without need for excavation and field inspection. Industry and research consortiums, working with PHMSA and DOE, should conduct research to establish the viability of using composite repairs for crack-like defects, planar flaws, and leaking defects. This research would entail full-scale destructive testing and qualification of repair methods appropriate to each of these flaw types.

Finding	Recommendation
II.D.6. Locating Underground Utilities to Prevent Excavation-Caused Incidents	
The leading causes of line strikes during excavation activities are from excavators not properly following procedures and from excavators failing to contact 811 Call Before You Dig to have underground utilities properly marked.	PHMSA, working with DOE and industry research organizations, should sponsor additional research and development to accelerate improvements in precise mapping of underground asset location (improved handling of GIS data). Oil and natural gas pipeline companies, working with DOE, PHMSA, industry research organizations, and technology providers, should expand research and development of excavator-based warning systems and proximity-based warning systems to use during drilling and digging operations to prevent pipeline strikes. These systems need to be reliable and cost effective for excavator owners and drill owners to install and use.
II.E.1.b. Underground Storage Reservoir Well and Reservoir Design and Integrity Management	
High-resolution casing inspection logging tools have size and availability limitations relating to the diameter of the casing. High-resolution logging tools for smaller diameter wells are still in development. In addition, it is important to continue to improve the accuracy and calibration of these tools, including the ability to assess the integrity of multiple concentric casings. Technology developments are underway on casing inspection log tools and analysis that may allow the inspection of the production casing without the removal of tubing. More work needs to be done to pinpoint specific metal loss in the outer string of concentric casings.	DOE should lead a collaborative effort with PHMSA and industry trade associations to determine the most effective measures of casing and cement integrity and explore opportunities for casing and cement logging improvements, including additional research and development opportunities. DOE should pursue additional research and development on well inspection technologies that can improve integrity logging, and reduce the frequency of tubing removals, which would reduce risk to personnel and the environment, as recommended by DOE's Interagency Task Force.
II.E.2.a. Aboveground Storage Overview	
Industry research and incident investigations have concluded that a sizable portion of floating roof incidents could have been prevented through earlier recognition of specific roof behavior patterns. Technologies have been developed to detect threats in real time, the threat that a floating roof may sink, but widespread field adoption is limited.	
II.E.2.b. Sensors	
	Industry and PHMSA should consider additional research and validation on tank integrity monitoring technologies, including camera technologies and associated pattern recognition software, wireless sensors, and unmanned aerial systems (drones) to measure floating roof stability and integrity.

Finding	Recommendation
II.E.2.c. Firefighting Foams	
The effectiveness of the new and environmentally friendly foams that are entering service warrants additional study and field testing. The ability to dispense foam rapidly when needed can mean the difference between a manageable incident and a crisis situation. Opportunities to transition to more environmentally friendly firefighting foams are under review.	
II.F.1. Pipeline Methane Emissions Overview	
Pipeline companies are committed to extending the progress made in reducing methane emissions through voluntary programs such as the Environmental Partnership, EPA's Methane Challenge, Natural Gas STAR, and ONE Future.	
II.F.2. Reducing Compressor Station Leaks	
Prescriptive elements of existing regulations (e.g., rod packing changeout requirements) create barriers to the advancement and deployment of new technology that could be used to more effectively reduce methane emissions. Compressor station fugitive methane emissions could potentially be further reduced though the use of new, innovative technologies for identifying, locating, and quantifying methane emissions. The development of a protocol to demonstrate regulatory equivalency is needed as well as test sites such as Colorado State University's Methane Emission Test and Evaluation Center (METEC) to verify the equivalency of the technology.	EPA, in collaboration with industry, should develop performance-based regulations that will encourage the advancement and deployment of new rod packing and real-time emissions detection technology to better manage and minimize methane emissions. DOE should work with industry and technology developers to fund the development of technologies to better identify, locate, and quantify methane emissions. EPA should work with industry to develop a protocol to validate when new technology is equivalent to or better than existing regulatory requirements. DOE should work with industry to continue funding the Colorado State University METEC site or other similar sites to test and prove the equivalency of technologies to support timely deployment of new proven technologies. The METEC site simulates real-world equipment, operations, and leaks.
II.F.3. Reducing Uncombusted Methane Fuel Gas from Reciprocating Engines (Methane Slip)	
Additional research on enhanced combustion processes and technologies could provide new opportunities to further reduce methane slip while also continuing industry's progress in reductions of criteria pollutant emissions from reciprocating engines. An efficient and cost-effective method for measuring methane slip is not yet available to support the development of enhanced combustion systems that could reduce methane slip.	DOE should fund research and development with research consortiums for combustion engines that will enhance combustion efficiency and reduce methane slip while not increasing criteria pollutant emissions. DOE should fund research and development to develop efficient and cost-effective methods for directly measuring methane in the exhaust.

Finding	Recommendation
II.F.4. Reducing Methane Emissions from Planned Pipeline Blowdowns	
Continued technology development advancements of in-line inspection technologies to better assess threats should enable a reduction of hydrostatic testing.	Industry, in coordination with PHMSA, DOE, and other agencies, should conduct research and development to improve in-line inspection tool capabilities for natural gas pipelines to address technology gaps, thus enabling the application of integrity management principles and technologies to replace hydrostatic testing and pipe replacement requirements of in-service pipelines where possible.
III.A.1. LNG Industry Overview	
There is a healthy and broad range of LNG operating experience in the United States spanning from the first U.S. export facility in Kenai, Alaska, peak shaving plants located in the Northeast and Midwest, to the new, large purpose-built LNG export facilities located on the Gulf and East coasts of the United States.	
III.A.2. Onshore LNG Storage and Containment Integrity	
Current DOT Part 193 regulations do not recognize updated design codes and standards used today for LNG production and export facilities. These requirements do not recognize relevant risk-based standards that are used internationally for LNG export projects, which can impair the cost competitiveness for U.S. LNG operators.	Pursuant to Executive Order 13868, PHMSA, working with the LNG industry, should jointly review and update 49 CFR Part 193 for design, construction, and operation of LNG facilities to ensure they align with world-wide best practices, advances in design codes and reflect risk-based standards. Industry, through its trade associations, should work with PHMSA to develop an inspection regime/protocol specifically for LNG tanks that are built to API 625 and ACI 376, and based on the failure mechanisms unique to LNG storage. This initiative could take the form of a standard similar to API 653 that is applicable to API 650 tanks.
III.A.3.b. LNG Shipping in the United States	
The United States is constructing new LNG terminals with robust safety and reliability designs, with strong quality assurance and self-assessments to ensure that all applicable international standards and guidelines are met (SIGTTO, OCIMF, GIIGNL, PIANC, etc.).	
III.A.3.c. LNG Transfer Technologies	
Cryogenic flexible hose technology currently provides for safer bunkering of LNG carriers and other ocean-going vessels, given the increasing demands for cleaner burning fuels on ships but is not yet widely used in the United States.	

Finding	Recommendation
III.B.1. Marine Industry Overview	
Marine vessel safety has improved, largely from Oil Pollution Act of 1990 implementation and an industry commitment for vessel operators to implement and improve a robust safety management system. Vessel oil spills to water were reduced dramatically beginning in 1991 and have remained essentially flat through 2017 apart from infrequent high-consequence events. Additional advancements in navigation technologies and training systems offer the best opportunities to mitigate marine vessel accidents.	
III.B.2. Navigational Technologies to Address Human Factors	
An effective means to expand capacity of ports will be the application of navigational technologies that would support reliable two-way channel traffic. Advancements in route planning and integrated navigational system technologies offer strong potential for maximizing channel capacity. Accurate underwater infrastructure mapping is important for vessels to identify nearby pipeline infrastructure. Where accurate map locations are not available, advancements in technologies that could recognize nearby pipeline infrastructure could provide an even higher level of safety. The National Oceanic and Atmospheric Administration, Coast Guard, and Army Corp of Engineers may offer collective expertise to better locate underwater pipeline infrastructure.	The U.S. Coast Guard should fully implement NTSB recommendations that could improve VTS system ability to consistently achieve its primary mission to reduce the risk of allisions, collisions, and groundings within VTS areas. The U.S. Coast Guard should implement additional traffic separation schemes and traffic rules such as speed limits, one way, and tethered escort tugs, particularly in non-vessel traffic service areas, to reduce marine traffic risk of allision, collision, and grounding.
III.B.3. Training and Development to Reduce Accidents Caused by Human Factors	
The U.S. Coast Guard Deck Officer examination process for original and raise in grade licenses does not include a comprehensive simulator assessment to verify that candidates have the skills required to oversee a navigation watch.	U.S. Coast Guard should extend requirements for vessels to be outfitted with automatic identification systems (AIS) to all commercial towing vessels with accurate tow-dimension input. In addition, operator training should be required on model-specific AIS technology in use.
III.B.3.a. Existing Navigational Technologies	
	Local port authorities should adopt National Ocean Service (NOS) real-time oceanographic data and other navigation products to promote safe and efficient navigation within U.S. waters. One component of NOS's integrated program for safe navigation is the PORTS data system. The U.S. Coast Guard should require that all vessels that are required to carry AIS "type A" under 33 CFR 164 should also be required to be fitted with electronic chart systems. Additionally, the U.S. Coast Guard should require that chart system training is specific to the technology model being used.

Finding	Recommendation
III.C.1. Rail Industry Overview	
Railcars transporting petroleum-based commodities safely reach their destinations with high reliability. Infrequent accidents do occur. The railroad industry has implemented additional standards, processes, and new technologies to address the causal factors related to these accidents. Further improvement in advancing technological innovations will rely on effective collaboration between shippers, regulators, and the industry. Technological innovations will require continued modernization of regulatory processes from prescriptive methods to a system that accommodates and incentivizes the development and deployment of new advanced technological solutions.	The Federal Railroad Administration should include the following considerations in their rulemaking and guidance documents: • Avoid locking in existing technologies and processes so that new innovations, including new technologies, that could improve safety and efficiency are not stifled. • Validate results with technical data and ensure benefits of a new rule exceed costs with supporting performance metrics. • Give meaningful opportunity to review and comment on new rules.
III.D.1.d. Data Collection and Sharing	
Carriers need valid data to measure the cost/benefit of adding advanced driver assisted technologies to their trucks. There is limited sharing of objective data validating the successes of these systems. This limits support for wide-scale implementation of these important safety technologies.	The National Highway Traffic Safety Administration (NHTSA), and any other appropriate federal agency, should sponsor a research study to confidentially gather performance data from current users of various advanced safety technologies on incident triggers and near miss incidents that avoided actual accidents. This should also include consolidating expert testimony and manufacturer data to further improve information sharing.
III.D.2. Forward Collision Warning and Avoidance Systems	
Current studies indicate that collision avoidance technologies work as intended in the large commercial truck environment and have the ability to help prevent or mitigate rear-end crashes, thus reducing the number of fatalities and injuries related to rear-end crashes. An NTSB analysis of two-vehicle rear-end crashes during 2011–2012 found that up to 2,220 lives might have been saved had the vehicles been equipped with forward collision avoidance systems.	DOT should consider sponsoring incentive mechanisms to the commercial trucking industry and equipment manufacturers, to accelerate deployment of safety technologies. These incentive mechanisms can include government/industry consortiums to invest in technology advancements, phased tax credit incentives, insurance, and regulatory requirements. In addition, petroleum company customers should consider requiring their trucking carriers to use driver-assist safety technologies by contract.
III.D.3. Lane Departure Warning and Corrective Steering	
Infrastructure, primarily in the form of well-maintained lane markings, is critical to the effectiveness of lane departure warning and corrective steering systems.	DOT should ensure adequate funds are provided for infrastructure improvements to ensure that roads maintain the proper markings to allow these LDWS technology systems to operate properly. If road markings are nonexistent or obscured, then the system will not work properly. NHTSA should support additional research and development to identify new technologies that improve LDWS ability to work properly on snow-covered roads or roads without proper markings.

Finding	Recommendation
III.D.4. Fatigue and Distracted Behavior Recognition	
The studies that are available show promising results in reducing distracted driving.	The Federal Motor Carrier Safety Administration should work with NHTSA to sponsor additional research and development to advance promising fatigue and distraction detection technologies.
III.D.5. Vehicle Camera Systems	
Camera systems reduce at-risk driving behaviors that contribute to accidents and provide coaching points to help improve safe driver skills.	Carriers should install vehicle camera technologies where feasible and use as a tool for coaching and training drivers to help improve driver safety performance and reduce accidents.
IV.A. Overview of Operational Technology and Cybersecurity	
Cyber threats to control systems are increasing due to greater reliance on control technology to manage risk and optimize assets, additional connectivity to business systems, and increasing instances of cyber activity targeting industrial control systems.	
IV.A.1.b. Erosion of Isolation and Increased Reliance on Segmentation	
Industrial Control Systems were designed for safety and reliability through traditional approaches of isolation (air-gapping) and segmentation. These systems have demonstrated strong reliability. However, the isolation of these control networks is dissolving with advanced technologies, and relying solely on isolation and segmentation for cyber protection can create a false sense of security.	
IV.A.1.d. OT Cyber Threats May Interfere with Safety System Protections	
Existing process hazard reduction programs address many, but not all, of the negative physical outcomes created by cybersecurity threats.	Industry should develop a cyber PHA (process hazards analysis) standard that effectively evaluates risks from cyber threat scenarios and establishes appropriate levels of protection against cybersecurity attacks. DHS should work with DOE and industry to develop and maintain an evergreen catalog of cyber threat scenarios that can be evaluated within a cyber PHA.
IV.A.1.e. Growing Threat of OT Cyberattacks	
The progression of cyberattacks indicates an increased focus on OT systems and the potential of greater impact, which could be leveraged by a committed and motivated attacker. However, reported cyberattacks and incidents relating to industrial control systems within the U.S. oil and natural gas and/or midstream industries have not resulted in significant safety incidents or operational disruptions to date.	

Finding	Recommendation
IV.A.1.g.iv. Manipulation of Supply Chains	
Enhanced cybersecurity architecture and design specifications of OT systems are needed to establish effective systems and controls, including addressing human factors exploited by threat actors. Enhanced design specifications would prompt additional research and development in patching and detection and result in customers being more able and willing to upgrade and/or standardize their multigenerational equipment more efficiently to accept these updates. The supply chain threats need to be understood, designed, and managed as an entire system in a disciplined manner. Attackers leverage vendors with less sophisticated capabilities to build bridges into their ultimate targets.	Companies involved in the production, manufacturing, and transportation of oil and natural gas should specify requirements in purchasing contracts with OT suppliers to adhere to industry cybersecurity standards and related development. OT suppliers must provide timely updates, such as patching, for cyber vulnerabilities.
IV.B.1. Improvement of Cyber Management Programs	
	Industry, in collaboration with trade associations and federal government agencies, should adopt and maintain up-to-date performance-based cybersecurity management standards. These standards should be continuously updated to keep pace with corresponding digital technology advancement and changes to the cyber threat landscape. Oil and natural gas companies with DHS-identified critical infrastructure should adopt industry-specific cybersecurity standards. Conformance with these standards should be verified through independent audits and assessments conducted by recognized or authorized entities, including but not limited to government-sanctioned entities. DHS and other regulatory agencies should update the assessment mechanisms to address any ongoing recommendations, including those relating to the potential limitations of a voluntary framework.

Finding	Recommendation
IV.B.1.f. Improving the Partnership between IT and OT Professionals	
The effective design, installation, and maintenance of industrial control systems requires integration of cyber expertise, usually located within IT, with process control disciplines to ensure cyber risks are adequately addressed.	Industry should revise and update existing standards, including API 1164, to incorporate the following elements into cybersecurity programs: • Organizational Structure: Cyber and process control disciplines must jointly manage the design, development, and change management of process control systems. • Asset Inventory and System Monitoring: Establish robust OT component, system, and process control network monitoring processes and practices, including effective management oversight and risk assessment. Incorporate the impacts of the impending convergence of IT and OT systems as well as future major technology planning elements such as Industrial Internet of Things architectures and technologies. Ensure appropriate integration with contractor/supplier management policies and practices. • Emergency Planning: Based on criticality analysis of the ICSs that includes commitments to customers and/or reputational considerations, performance expectations for recovering compromised systems should be established and tested. • Event Investigation: Establish cybersecurity investigation requirements and protocols. Establish a corporate compliance verification process to ensure appropriate closure and follow up of action items. Share internally while abiding by security classification requirements to promote learning and program improvement. Oil and natural gas companies should increase efforts to support staffing and training requirements and develop a consortium to address these needs, with guidance for common skills, transportable knowledge, and industry-wide growth in capabilities associated with automation systems, safety, and security. Oil and natural gas companies should increase efforts to work with education institutions to grow industry workforce knowledge and organizational capabilities in industrial cybersecurity technologies and practices as applied to oil and natural gas system design, development, and operations: • Professional education: Encourage and support university engineering degree programs to incorporate relevant curriculum on the essential elements of cybersecurity fundamentals, technologies, and practices. Specific priorities are those engineering disciplines directly related to the oil and natural gas industry, including (but not limited to) chemical engineering, petroleum engineering, process and mechanical engineering. Workforce development and training: Encourage and support the development and delivery of educational and training programs by industry, academia, and government targeted to industry professionals and operations personnel. The objective is to significantly enhance individual and organizational capacities to effectively incorporate current and evolving cybersecurity technologies and practices into oil and natural gas asset development and operations.

Finding	Recommendation
IV.B.2. Improving Collaboration with Key Stakeholders	
Collaboration to share cyber threats is increasing between industry, trade associations, and federal governmental agencies. OT cyber threat sharing often lacks the necessary transparency among and within companies that is necessary to improve effective cyber management practices. Current practices can result in findings that are overly sanitized and are inconsistently shared.	DHS and DOE should increase capabilities and resources to support independent and secure cybersecurity assessments prioritized on critical infrastructure. Assessments should be conducted by authorized entities, including but not limited to government-sanctioned entities. Cybersecurity assessments should be informed by current threat intelligence information sharing and lessons learned from cyber incidents. DHS, working with DOE, other federal agencies, and the oil and natural gas industry, should assist sector ISACs and regional groups to promote information sharing, including learnings from investigations. DHS should encourage increasing ISAC membership across industry sectors. DHS and other federal agencies should quickly share actionable information with ISACs and operators.
IV.B.3. Advancing Cybersecurity R&D within the Oil and Natural Gas Industry	
	DOE, working with industry, DOD, DHS, and DOT, should establish a collaborative process to identify and prioritize research and development aimed at sector-wide protection against nation-state and advanced persistent threat actors. The process should include the following: • Centralized input to research entities according to established criteria based on current and anticipated threats. • R&D efforts focused on the transportation types with the highest risk posed by cyber OT threats. • Funding, partnering, or incentive opportunities to reduce cyber OT risks.

VI. DEFINITIONS AND BACKGROUND INFORMATION

A. Terms and Definitions

Term	Definition
Blowdown	Practice of controlled venting of gas to atmosphere for maintenance, construction, integrity assessment, emergency relief, or other purposes
Breakout Tank	A tank used to (a) relieve surges in a hazardous liquid pipeline system or (b) receive and store hazardous liquid transported by a pipeline for reinjection and continued transportation by pipeline. (PHMSA, 49 CFR 195.2)
Cathodic Protection	Reduction or elimination of corrosion by making the metal a cathode by means of an impressed DC current or attachment to a sacrificial anode (usually Mg, Al, or Zn) (Corrosion Basics – An Introduction. NACE, 1984, p. 14)
Criteria Emissions	The six common air pollutants for which the Clean Air Act requires the Environmental Protection Agency to set National Ambient Air Quality Standards; the six are carbon monoxide, lead, nitrogen dioxide, ozone, particulate matter, and sulfur dioxide
Fugitive Emissions	Unintentional leaks from process equipment to the atmosphere
Haptic	Safety devices or warning systems installed in vehicles that operate through the sense of touch
Hydrocarbon	Often used as a generic term for oil and natural gas, a hydrocarbon is any compound comprised of only hydrogen and carbon. For example, CH_4, or methane, is composed of one carbon atom and four hydrogen atoms
Incident (Natural Gas Pipeline)	• A death, or personal injury, necessitating in-patient hospitalization; or • Estimated property damage of $50,000 or more, including loss to the operator and others, or both, but excluding cost of gas lost; or • Unintentional estimated gas loss of 3 million cubic feet or more
Incident (Oil Pipeline)	Tier 1 (independent of location): Fatality, injury requiring in-patient hospitalization, ignition, explosion, evacuation, wildlife impact, water contamination, or private property damage Tier 2 (location not contained on operator-controlled property): Unintentional release volume greater than or equal to 5 gallons and in a high-consequence area (HCA); or unintentional release volume greater than or equal to 5 barrels and outside of an HCA; or water contamination; or soil contamination
In-Line Inspection Tools	Tools (often referred to as ILI tools or pigs) inserted into pipelines to inspect a pipeline segment for anomalies and pipe integrity; ILI tools are equipped with varying technology packages, including MFL
Liquefied Natural Gas	Natural gas that has been cooled to −260°F; the liquefied gas takes up 600 times less space than when in a gaseous state and can be more easily stored or transported by specialized ships
Management System	The policies, plans, and procedures organizations use to manage a business or other organization; Plan-Do-Check-Act cycles are a critical component of management systems, as is continuous improvement
Methane Slip	Uncombusted methane in the exhaust stream of reciprocating engines
Natural Gas	Primarily consists of methane, but also includes a smaller percentage of petroleum gases such as pentane, butane, ethane, etc.
Pipeline	For the purposes of this report, the term “pipeline” means a pipeline transporting oil, natural gas, and refined products and that is regulated by PHMSA

B. API 1164

The original API 1164 standard was written in response to the September 11, 2001, terrorist attacks. The first and second editions were titled "Pipeline SCADA Security" and provided recommendations to oil and natural gas companies with pipeline infrastructure. As cybersecurity threats have increased in severity, API rewrote the third edition into a format that maps to the National Institute of Standards and Technology (NIST) framework and other related standards.

NIST publishes a Cybersecurity Framework (CSF) comprising three components (core, tier, profile) designed to assist companies with applying cybersecurity controls to specific risk scenarios. Further, the NIST 800-53 revision 5 standard maintains a catalog of security controls that address the full range of cybersecurity issues related to enterprise IT networks and systems.

API 1164 will build upon NIST CSF and 800-53 standards with cybersecurity controls specific to the pipeline system environment. This will include categories based on domain-specific relevance, business drivers, risk assessments, and OT manufacturer's priorities. The third edition of API 1164 will align with the elements of NIST CSF (see Table 4-15).

The implementation of the API 1164 standard will support a multilayered cybersecurity defense that can improve the cybersecurity posture for oil and natural gas companies with pipeline infrastructure. The initiatives within the standard will contribute to systemically improving a company's cybersecurity controls by providing proactive recommendations and flexibility to align to future technology deployments.

Identity	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Access Control
	Awareness Training
	Data Security
	Information Protection
	Maintenance
	Protective Technical Security Solutions
Detect	Anomaly and Event Detection
	Continuous Monitoring
	Detection Process
Respond	Response Planning
	Coordinated Response Activities
	Response and Recovery Analysis
	Containment, Mitigation, and Eradication
	Process Improvement by Lessons Learned
Recover	Planning Processes & Procedures
	Process Improvement by Lessons Learned
	Communicate Restoration to Stakeholders

Source: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, April 2018.

Table 4-15. *NIST CSF Core*

C. Key Cybersecurity Report References

1. Defense-in-Depth: Cybersecurity in the Natural Gas & Oil Industry – December 2018 – API and Oil and Natural Gas Subsector Coordinating Council. https://www.api.org/news-policy-and-issues/cybersecurity/defense-in-depth-cybersecurity-in-the-natural-gas-and-oil-industry
2. Article: Senators Call for Urgency on Energy Cybersecurity. February 18, 2019. By Michael Brooks.
3. WSJ article: Russian Hack Exposes Weakness in U.S. Power Grid – 1/11/19
4. Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management – U.S. Government Accountability Office Report – December 2018. https://www.gao.gov/products/GAO-19-48
5. National Intelligence Strategy of the United States 2019. January 2019. Dan Coates.

https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

6. Natural Gas Systems: Reliable and Resilient. Natural Gas Council. July 2017. https://www.ngsa.org/download/analysis_studies/NGC-Reliable-Resilient-Nat-Gas-WHITE-PAPER-Final.pdf

7. The Natural Gas Grid Needs Better Monitoring. By Jay Apt, Gerad Freeman, Michael Dworkin. Issues in Science and Technology. Vol. XXXIV, No. 4, Summer 2018. https://issues.org/the-natural-gas-grid-needs-better-monitoring/

8. AGA Natural Gas Resiliency. April 2014. https://www.energy.gov/sites/prod/files/2015/01/f19/AGA.Resiliency%20Metrics%20workshop.pdf

9. Dragos Year in Review 2018. ICS Activity Groups and the Threat Landscape. Industrial Controls System Vulnerabilities. 2 reports. https://dragos.com/year-in-review/

10. ICS-CERT Annual Assessment Report. Industrial Control Systems Cyber Emergency Response Team. FY 2016. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

11. AON 2019 Cyber Security Risk Report. What's Now and What's Next. February 2019. https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx

12. https://www.api.org/~/media/Files/Policy/Safety/ONG-Industry-Preparedness-Handbook-v2.pdf

13. http://naturalgascouncil.org/wp-content/uploads/2019/04/Natural-Gas-Reliable-and-Resilient.pdf

14. http://naturalgascouncil.org/wp-content/uploads/2018/10/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf

15. http://ongsubsector.com/documents/ONG-Cybersecurity-101-Factsheet.pdf

16. http://ongsubsector.com/documents/ONG-SCC-Regulatory-Matrix.pdf

17. Understanding the Oil and Natural Gas Industry: Cyber & Physical Security Practices, U.S. Department of Energy, Presented by the ONG-SCC, December 2017.

18. Natural Gas 101 – Operations & Resilience, American Gas Association, Presentation, September 2016.

19. Understanding the Oil and Natural Gas Industry: Security Regulatory Framework, U.S. Department of Energy, Presented by the ONG SCC, February 2017.

20. World Economic Forum Report by Centre for Cybersecurity and Electricity Industry Community in collaboration with Boston Consulting Group. Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards.