Working Document of the NPC Study
Dynamic Delivery –
America's Evolving Oil and Natural Gas Transportation Infrastructure
Made Available December 12, 2019

Topic Paper #4-15

THE API 1164 FRAMEWORK AND CYBERSECURITY CONSIDERATIONS FOR PIPELINE TRANSPORTATION AND STORAGE

Prepared for the

Technology Advancement and Deployment Task Group

On December 12, 2019 the National Petroleum Council (NPC) in approving its report, *Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation Infrastructure*, also approved the making available of certain materials used in the study process, including detailed, specific subject matter papers prepared or used by the study's Permitting, Siting, and Community Engagement for Infrastructure Development Task Group. These Topic Papers were working documents that were part of the analyses that led to development of the summary results presented in the report's Executive Summary and Chapters.

These Topic Papers represent the views and conclusions of the authors. The National Petroleum Council has not endorsed or approved the statements and conclusions contained in these documents, but approved the publication of these materials as part of the study process.

The NPC believes that these papers will be of interest to the readers of the report and will help them better understand the results. These materials are being made available in the interest of transparency.

The attached paper is one of 26 such working documents used in the study analyses. Appendix C of the final NPC report provides a complete list of the 26 Topic Papers. The full papers can be viewed and downloaded from the report section of the NPC website (www.npc.org).

This page is intentionally left blank.

Topic Paper

(Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure)

4-15	**The API 1164 Framework and Cybersecurity Considerations for Pipeline Transportation and Storage**
Author(s)	**Joey Hewitt (Plains All American)** **Curt Wiggins (Chevron Pipeline & Power)** **Thomas Penn (Enbridge Pipelines Inc.)** **Amy Bejtlich (Dragos, Inc.)** **Kent Knudson (Plains All American)**
Reviewers	**Al Lindseth (Plains All American Pipeline)** **Marty Willhoite (Miller Consulting Services)** **Wesley Malaby (Phillips 66 Company)** **Doug Sauer (Phillips 66 Company)** **Jay Churchill (Phillips 66 Company)**
Date: November 12, 2019	**Revision:** Final

SUMMARY

The API 1164 was initially developed after the terrorist attacks on September 11th, 2001 for pipeline and SCADA systems. The current framework is being broadened to apply to modern control systems being used within midstream companies. The framework primarily focuses on pipelines, but it could be expanded to other assets, such as storage. This topic paper provides guidance on the continued implementation of the API 1164 framework as the Technological Advancement & Deployment chapter recommends.

Overview: Pipeline Transportation & Storage Operations

Many companies operate the nation's pipeline systems. These are comprised of different assets – pipelines, storage tanks, compressor stations, and control centers. Pipelines involve long distances and traverse virtually every conceivable environment. The physical infrastructure is located above and below ground, and below bodies of water. All pipelines require at least one initial pump station or compressing facility providing the work that moves the raw product from the pipeline inlet to the ultimate termination. Frequently, depending on hydraulic factors (e.g., geographical constraints, distances, etc.), pipelines require more than one pump station or compressor station along its length and ends at the refinery, distribution facility or terminal.

Criticality

Defining critical infrastructure based on the extensive networks of interconnected pipelines and infrastructure adds to the complexity of evaluation for pipeline operators. Assisting the industry

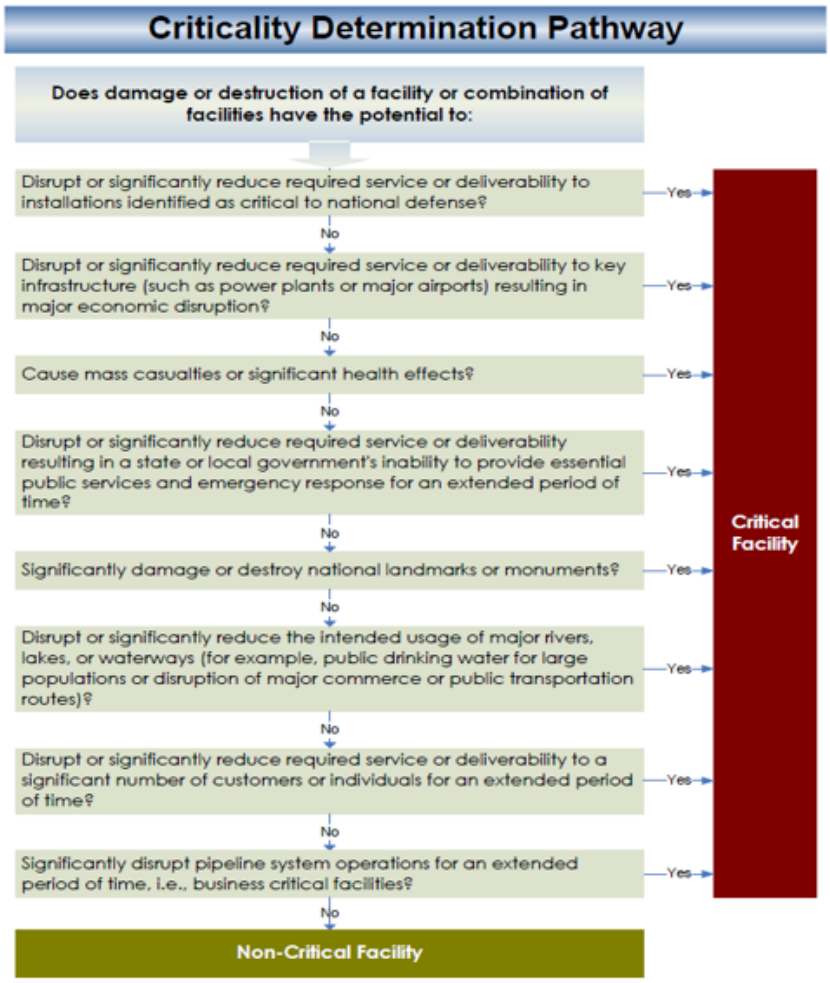


Figure 1: Transportation Security Administration (Pipeline Security Guidelines, March 2018)

in defining critical infrastructure, Transportation Security Administration (TSA) has established the *Pipeline Security Guidelines* (TSA, 2018) to assist in the determination and critical nature of pipelines and facilities to establish requirements and consistency when validating critical infrastructure. Other factors that may influence the determination of criticality are customer base, downstream deliverability and reliability commitments, resiliency, and operator risk tolerance. Based on identified factors and continuing changes infrastructure and business directives, pipeline operators should establish criteria for the evaluation of the assets on a standard interval acceptable to the operator and, or when changes require, TSA recommends periodic assessments not to exceed 18 months. The criteria as established by guidelines are structured to review where facilities or combination of facilities together would have a potential impact is identified and therefore defining critical facilities. Figure 1 provides criteria and pathways in determining the outcome in identifying a critical facility.

As described in Figure 1, a pipeline operator determines the assets and follows the flow of descriptive questions in determining the criticality of a facility in whether the outcome of the flow is "No", which leads to a non-critical facility or "Yes" identifying that its assets are critical.

These criticality assessments are necessary first steps for operators in the security risk management process.

Inherent safety of pipelines

The natural gas and oil pipeline environments today are managed and controlled through the use of automation and as such, are engineered and designed around safety and resiliency, including government requirements to assess operational pipeline safety, physical security, and risk. Many items of these safety and risk reviews are designed around failure or external factors affecting the controlling of a pipeline. Outcomes of these reviews provide methods and procedures to manually maintain control of the pipeline for a limited time before shutting down in a controlled fashion. Many factors, including the extensive network of interconnections of pipelines, redundancies, recovery options, routing capabilities, and increased availability through storage, contribute to minimizing large or long-lasting events, thereby reducing impacts to the distribution of a product.

Pipeline operators understand that their industry is the target of a range of malicious actors, including nation-states and other criminals wanting to obtain confidential data, breach industrial control systems for various reasons, including jeopardizing safety and systems. American Petroleum Institute (API) notes (API, 2018) that natural gas and oil companies realize that these attacks can affect the overall operations and threats that cyber-attacks can inflict could jeopardize the company. These industry-based approaches and frameworks assist in the reliance of the demonstrated and effective risk-based adoption and methodology among the operators.

Pipelines impact both upstream and downstream activities if the pipeline system is shutdown. Cybersecurity of pipeline operations is particularly critical, given the inability to physically secure or man miles of pipe. Data integrity ensures situational awareness and facilitates seamless, optimal operations. Advanced Operational Technology (OT) in pipelines often includes significant cybersecurity.

Most pipeline systems are monitored and moderated through automated Industrial Control System (ICS) or Supervisory Control and Data Acquisition (SCADA) systems using remote sensors, signals, and preprogrammed parameters to activate and deactivate valves and pumps to maintain

flows within tolerances. One of the most important aspects of cybersecurity in the pipeline space is ensuring the integrity and operability of the SCADA system of each pipeline against cyber compromise. From a cybersecurity perspective, pipeline functions are divided across an enterprise network and an operations network (which includes a control system, SCADA, and pipeline monitoring). These two networks are generally isolated from each other, and a portfolio of tools and mechanisms is used to improve the prevention, detection, and mitigation of cyber penetration. Pipeline safety regulations and standards state that back-up systems cannot be affected by the same incident that compromises the primary control system; thus, fail-safes and redundancies must be independent of the cause of the primary mechanism's failure.

For many pipeline operations, the monitoring and control location is remote from the pipeline pump station or compressor locations. The physical separation of the various components, which make up the pipeline OT system, requires extensive use of long-distance telecommunication services. In today's operating environment, these telecommunication systems are generally obtained from third-party commercial suppliers. Other pipeline threat vectors viewed as unique are:

- virtually no physical means to monitor the entire system on a 24x7x365 basis exists,
- The lack of network connectivity helps protect them from internet and email-driven malware, but it also keeps the parent companies from gathering information, and they cannot protect and monitor what they do not know.
- Third party access to the infrastructure is common,
- wireless telecommunications are increasing, and
- physical infrastructure frequently transverses unique geographic areas.

In addition, a partnership between the private sector and the federal and state governments is a key part of addressing physical and cybersecurity threats to the nation's critical infrastructure. Industry members participate in internal and industrywide security situation simulation exercises – training exercises that present real-world challenges – with government officials and others to ensure that the industry is better prepared for a cyber or a physical emergency.

Just as with pipeline safety, utilities, and other associated entities apply layers of resilience for cybersecurity by employing firewalls and other tools to improve the prevention, detection, and mitigation of cyber penetration. Further, the delivery systems are mechanical by nature and can still be run manually if necessary. For example, natural gas is moved by using pressure to control the amount entering and leaving the system.

Resiliency is designed into pipeline systems and has been an important topic relating to natural gas given the increase of gas-fired generation and concerns that a gas outage or interruption due to a cyber event or other causes could create power outages. Natural gas networks are highly diversified and interconnected. Significant spend and continuous attention are devoted to maintaining safety and reliability and increase resiliency. It is an industry constantly focused on coming back online quickly in the case of disruption/outage.

Operators have programs to improve the prevention, detection, and mitigation of cyber threats. Cybersecurity risk mitigations are taken into account within companies' risk management, safety, and emergency management programs. Measures and protocols exist to address disruptions from cyber threats. On a real-time basis, pipeline operators manage assets and activities that include supply, transportation, and storage contracts to provide security and reliability of product delivery.

API 1164

The original API 1164 Standard was first authored in response to the terrorist attacks on September 11th, 2001. Originally the 1st and 2nd editions were labeled "Pipeline SCADA Security" and were treated more like a "recommended practice" because of infancy. As cyber threats became more serious, the decision was made to refresh the document in a framework form just like National Institute of Standards and Technology (NIST), International Standards Organization (ISO), TSA, and other standards that are out there. This 3rd edition is using a standards/framework approach based on NIST and other frameworks. Pipeline profile development (including both hazardous liquid and natural gas), is to be developed as an actionable approach for implementing TSA Cyber Asset security requirements into a pipeline system. Profiles will be derived from the security

controls of the ISA/IEC 62443, with NIST SP-800-53 sourced for subcategories that have no corresponding ISA/IEC 62443 references.

NIST provides/maintains a catalog (NIST SP 800-53) of security control baselines addressing all types of cyber issues as they pertain to basic IT/OT functions and is currently on revision 5. This framework is voluntary guidance. NIST then also publishes a Cybersecurity Framework comprised of three components (Core, Tiers, Profiles) designed to assist the user with quickly finding specific controls as they pertain to specific situations. It is a policy framework of cyber guidance for operators to assess, and improve capabilities for prevention, detection and responsiveness to cyber events. The Core functions that drive this policy (and were mentioned previously in this report) are:

a. Identify: Develop an understanding of risk to systems, assets, data, capabilities, etc.
b. Protect: Implement safeguards to ensure the delivery of critical infrastructure services.
c. Detect: Implement tasks designed to properly identify an occurrence of a cyber event.
d. Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
e. Recover: Develop recovery plans for services impaired by a cyber event.

These five “core” functions and categories are just the beginning stages of using the CSF:

Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness Training
		PR.DA	Data Security
		PR.IP	Information Protection
		PR.MA	Maintenance
		PR.PR	Protective Technical Security Solutions
DE	Detect	DE.AE	Anomaly and Event Detection
		DE.CM	Continuous Monitoring
		DE.DP	Detection Process
RS	Respond	RS.RP	Response Planning
		RS.CO	Coordinated Response Activities
		RS.AN	Response and recovery analysis
		RS.MI	Containment, Mitigation and Eradication
		RS.IM	Process Improvement by Lessons Learned
RC	Recover	RC.RP	Planning Processes & Procedures
		RC.IM	Process Improvement by Lessons Learned
		RC.CO	Communicate Restoration to Stakeholders

Figure 2: NIST Cybersecurity Framework 2018, Function and Category Unique Identifiers

These five core functions collectively represent a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. The core functions provide detailed guidance for developing individual organizational or, as specified herein, industry Profiles. These are further clarified by the use of categories and sub-categories not illustrated here.

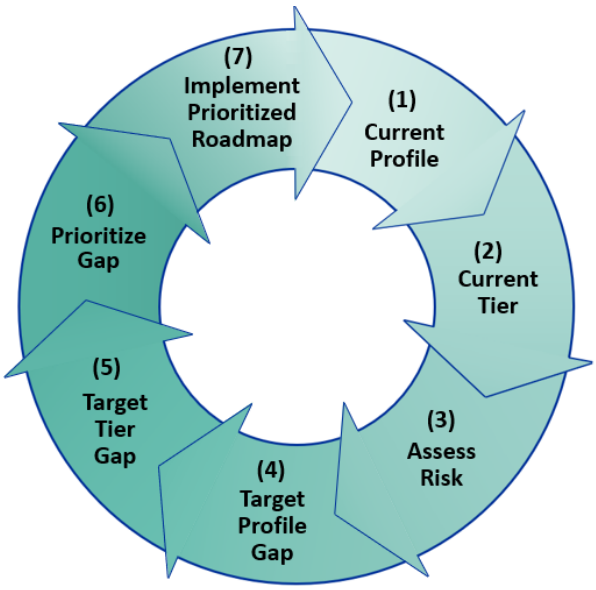
The proposed implementation tiers below assess a company's maturity against implementing the core functions of the framework. These tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives. They aid by illustrating the maturity levels of cybersecurity processes. They project an increasing degree of complexion and rigor in cybersecurity risk management. The tiers are a tool for internal communication between cybersecurity risk management and operational risk management. Regardless, higher tiers represent higher degree of sophistication and maturity in the management of cybersecurity risks and responses:

Tier	Name	Explanation
1	Partial	Informal practices; limited awareness; no cybersecurity coordination.

Tier	Name	Explanation
2	Risk Informed	Management approved processes and prioritization not implemented organization-wide; high-level awareness, adequate resources provided; informal sharing and coordination
3	Repeatable	Formal policy defines risk management practices processes, with regular reviews and updates; manage cybersecurity risk organization-wide with implemented processes; regular formalized coordination.
4	Adaptive	Practices actively adapt based on lessons learned and predictive indicators; cybersecurity implemented and part of culture organization-wide; active risk management and information sharing.

The framework profiles identify opportunities for improving cyber vulnerabilities by comparing current capabilities with desired target capabilities. They are an alignment of the "Core" as expressed by function, category, and sub-category with the business objectives and risk tolerance. Companies define their current profile for comparison to their desired target profile after internal risk assessment. Once defined, a gap analysis can be performed, telling each operator for each threat vector whether they should take action or not. The below diagram illustrates the CSF risk prioritized gap mitigation roadmap implementation model:

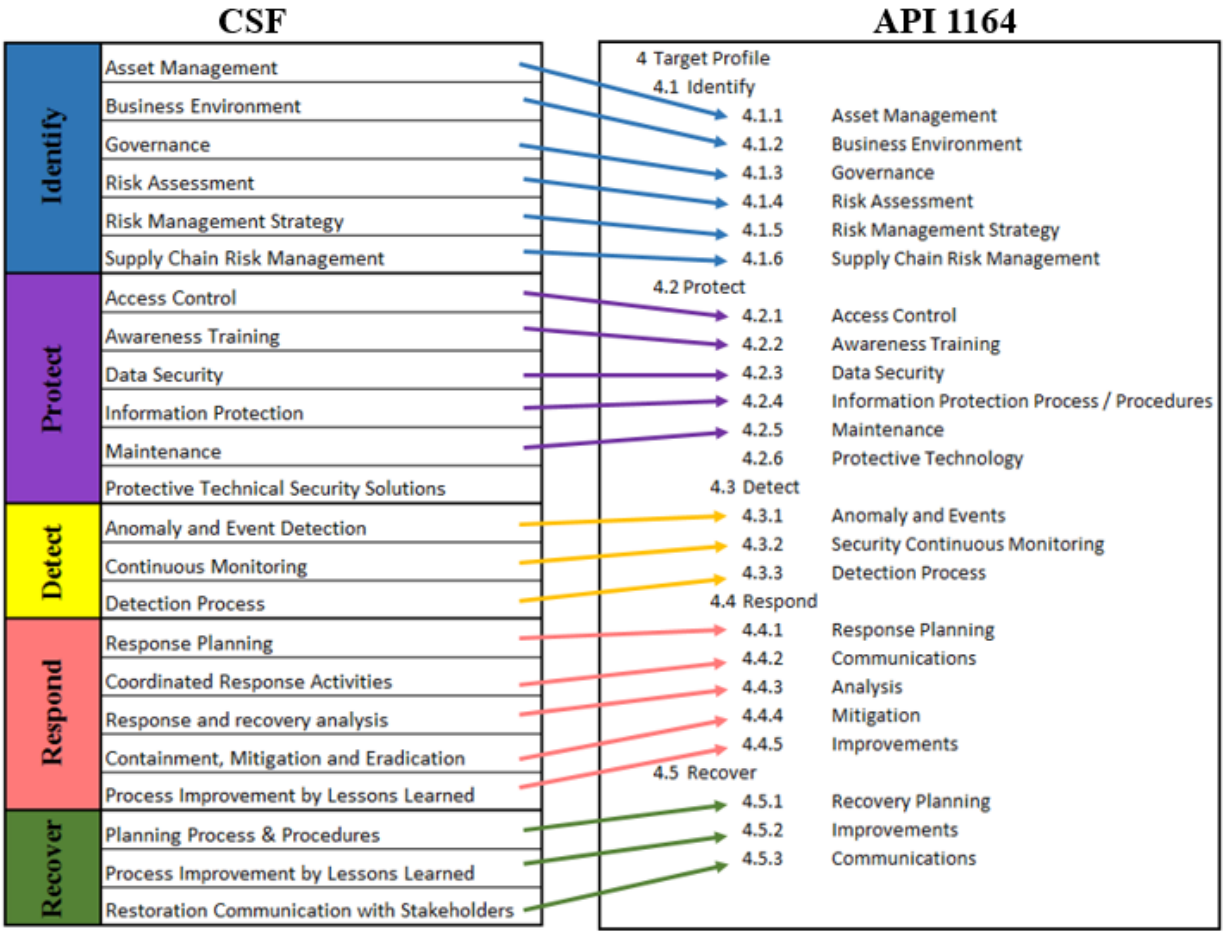
As related to the proposed API 1164 3rd edition, the framework approach defines pipeline profile development (including both liquids and natural gas) to be an actionable approach for implementing TSA Cyber Asset security requirements into a pipeline system. The specific statements in the subcategories will be derived from the security controls of the ISA/IEC 62443, and are customized to the pipeline domain using relevant, informative references. NIST SP-800-53 is sourced for subcategories that have no corresponding ISA/IEC 62443 references. For informative references to an entire control family or set of controls (such as subcategory ID.GV-1's informative reference to all "policy and procedures" controls), the approach takes a holistic view of the controls comprising the family/set. There will be an additional section providing customized CSF subcategory language developed using informative references relevant to the pipeline domain.



CSF Risk Prioritized Gap Mitigation Roadmap Model

This profile will express tailored values for cybersecurity controls for the pipeline system environment. These represent the application of the Categories and Subcategories from the Framework based on domain-specific relevance, business drivers, risk assessment, and the manufacturer's priorities. Users of the Profile can also add Categories and Subcategories as needed to address unique and specific risks.

The implementation of this standard will support a multi-layered security environment and identify a number of technical and management-level recommendations that could improve the security posture of those companies. These risk control initiatives will contribute to systemically improving each company's information and cybersecurity controls, providing a security infrastructure in a proactive nature and provide information assurance guidance and alignment to future technology deployments.



NIST provides a common framework that can be leveraged in a landscape of different cybersecurity and other related guidelines and framework systems, as it is with API 1164. It also offers a standardized approach for all critical infrastructure in the United States, outlining ways to employ five strategic functions: identify, protect, detect, respond, and recover.

Operators thus should review and consider their own plans and procedures to ensure they are consistent with the approved API 1164 framework. It is important to make a distinction between organizations simply complying with regulations and those implementing an effective approach and program relating to cybersecurity.

In the latest version, NIST has added self-assessing cybersecurity risk components within the framework and is being adopted into API 1164. Companies are encouraged to perform internal or third-party assessments using the framework. However, meaningful framework assessments

require knowledge of your current cybersecurity risk profile. Self-assessing by design is to drive discussions around what your company has in place and what it needs based on fact-based cyber risks that are specific to your company. Prudent pipeline operators should consider their business requirements and material risks, and then make reasonable and informed cybersecurity decisions using the framework to help them identify and prioritize feasible and cost-effective improvements.

Cyber References

A Key Documents/Studies List

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 Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management – US Government Accountability Office Report – December 2018. https://www.gao.gov/products/GAO-19-48

3 National Intelligence Strategy of the United states 2019. January 2019. Dan Coates. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

4 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

5 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/

6 AGA Natural Gas Resiliency. April 2014. https://www.energy.gov/sites/prod/files/2015/01/f19/AGA.Resiliency%20Metrics%20workshop.pdf