Oil and Gas Pipeline Industrial Security Reference Design

Foreward

Now more than ever, technological innovations are advancing at a dizzying pace, going mainstream, and changing the world in the process. This is in part due to increased competition, rising regulatory pressures, and public expectations. For Industrial Control Systems (ICS), these factors have increasingly affected pipeline operations and maintenance. Recent technological developments are addressing many complex issues, driving efficiencies, and lowering costs. And these improvements come with risks, such as theft and unauthorized disclosure of proprietary information. Design flaws and technical vulnerabilities in information systems, which are used to manage and control the flow of pipeline products and their associated information, are often exploited. Numerous examples of cyber breaches, which have caused major damage to what is considered to be critical infrastructure, appear in the news. Globally, laws, regulations, and standards have become more stringent in an attempt to address the ever-increasing need to thwart cyber attacks. The public at large, as well as regulators, have formed a rallying cry, compelling the pipeline community to secure their assets to avoid safety hazards, security breaches, penalties, sanctions, and embarrassing news headlines.

As a SCADA Integrator in the ICS space, I have worked with many pipeline companies over the years, addressing the layers of complexity involved in securing their assets. This isn't just a technical issue. To prepare for and prevent current and emerging cyber attacks, organizations must balance technology with human-centric defenses. As cyber threats become increasingly prevalent and more sophisticated with each new technological innovation, the efforts to thwart them must adapt. As an organization, security must be integrated into the culture from the Board room to the Production environment. Only a multi-layered defense security strategy (human, physical, and cyber factors) will ensure that attackers penetrating one layer of defense will be stopped by a subsequent layer.

Protecting your company and ensuring security requires significant investment and clear guidelines for training, data integrity, and security. Given the general consensus to secure all manner of assets within pipeline operations, the authors of this paper have endeavored to present a comprehensive reference guide to securing your pipeline operation. This document is a source of information to help you understand the complexity of securing operations and provides a detailed technical solution approach to doing so. It is a well-written, thoughtful, and systematic discussion of all things cybersecurity and lays out the approaches that are in common use today and considered to be standard within the industry. This reference guide is peppered throughout with invaluable commentary from industry experts on best practices, techniques, and relevant technologies. You will gain considerable insight into today's key information security management challenges and concerns as your organization undertakes this formidable task of laying down the groundwork and managing a modern pipeline information security program.

The effort to create this document was the brainchild of a cross-disciplinary team from Cisco, Schneider Electric (SE), and AVEVA. The original intent was to build on the concept of the Smart Connected Pipeline, a fully Tested Validated Documented Architecture (TVDA) solution for pipelines, which includes all components of the solution from SCADA to devices to supporting systems, with a discussion on how security plays into the overall solution and the benefits of a jointly delivered solution. Having worked in this industry over twenty years, I was invited to be a part of this effort as a

reviewer of the document, providing feedback and insight into the value it would bring to its intended audience. The authors of this document have created an all-in-one solution reference that can be leveraged to establish a robust cybersecurity strategy for your organization. They have outlined in detail the various elements of a cybersecurity management program, which aligns with many security standards used throughout the world.

Today's business climate has created a demanding landscape where people and companies are more connected than ever and technology is transforming the organization. My hope is that the insights offered by this document will provide a reference to help create a cybersecurity strategy for your organization.

-- Jeff Whitney, Berkana Resources Corporation, October 25, 2018

The Authors

Rik Irons-Mclean—Senior Business Development Manager - Office of the CTO, Industry Solutions Group, Cisco

Kevin J. Rittie—Director, Solutions and Cybersecurity Management, AVEVA

Jason Greengrass—Solution Architect, IoT Solutions, Cisco

Jacques van Dijk—Director, Industry Solution Validation, AVEVA

Robert Albach—Product Manager, Security Business Unit, Cisco

Jose Manuel Pienado—Global Solutions Architect, Schneider Electric

Firas Ahmed—Architect, CX Advanced Services, Cisco

Preface

This reference document describes the Cisco Systems, AVEVA, and Schneider Electric approach to cybersecurity in the Oil and Gas (O&G) industry, specifically for Pipeline Management Systems (PMSs). The following key principles drive the guidelines in later sections:

- Security, an essential component of any properly designed and implemented Industrial Control System (ICS), forms a core part of the strategy to ensure the safety and reliability of O&G pipeline management solutions.
- Systems and architectures are continuously evolving as technology changes and in response to an increasing attack surface. The accepted security mindset is that O&G PMSs will be subject to cyber threats or attacks and, as such, organizations should prepare accordingly.
- Standards and guidelines are an essential foundation, but they do not describe how to secure specific systems. As all systems are different, standards and guidelines should be leveraged as a best practice framework and tailored specifically to business needs.
- The best security strategy is achieved through information technology (IT) and operational technology (OT) teams collaborating with technology vendors and standards organizations (regulatory bodies and industry trade organizations) to understand how individual strengths can be leveraged to best address control system risks.
- Any solution is only as strong as its weakest part. The best strategy to mitigate risk is to embrace “ecosystem security,” where all components of a system are designed, built, tested, validated, and certified wherever possible, taking end-to-end cyber and physical security into consideration.
- Security is a continuous process, not a single, isolated effort. Every design phase should include a set of security steps to be followed, integrating security directly into the solution throughout its lifecycle. To be most effective, security must be included in the lifecycle design from the outset. By building the system with a robust security architecture at its core, integrating with broader organizational compliance and governance efforts, a more effective, lower-cost security approach can be achieved.
- Security incidents will inevitably occur. Having a well-documented set of processes and procedures on how the organization responds to incidents is essential. It is not only the speed with which a threat is discovered, but also the speed with which security threats are mitigated and remediated that controls the potential risks and costs arising from an incident.

Intended Audience

The primary intended audience for this document is anyone with a responsibility or interest specifically in pipeline security or more generally in O&G security, as these principles are equally applicable to all areas of the O&G value chain. The audience would include those involved in security design, architecture, standards and compliance, and risk management.

> A 2016 Cisco and Schneider Electric Customer Advisory Board Survey found that 100% of customer respondents highlighted cybersecurity as their top-of-mind priority over the coming years.

Industry Perspective and Requirements

Cybersecurity threats and breaches continue to make headline news with impact across all industries and sectors. O&G, like other critical infrastructure environments, rely on highly-available ICSs and supporting infrastructure. In this document, the focus is on PMS; however, the guidelines are applicable to any ICS. The consequences of cybersecurity breaches, such as station shutdown, utilities interruption, production disruption, impact to the environment through detected or undetected leaks, and even the loss of human life, all mean cybersecurity is a critical area of concern within industry.

A 2017 study[1] found that industrial cybersecurity is difficult for even the most technologically advanced O&G companies for a number of reasons, including:

- Long life cycles of operational assets
- Inaccurate and outdated asset technology inventories
- 24/7/365 continuous operation times (barring turnarounds and shutdown)
- No single approach to security in the regulations or standards

These factors, coupled with a rapidly evolving technological landscape, pose a serious risk to the industry. This is not merely a concern for the future, but a current reality. A study[2] found that sixty-eight percent of respondents to an O&G survey admitted that their organizations had experienced at least one cyber compromise in 2016. For large organizations, the same study found that there were two to five such incidents per organization.

The potential for disruption and damage from cyberattacks is real and a threat that the industry must proactively address to protect the critical infrastructure of a foundational economic industry.

This reference document aims to help organizations address this threat by providing a simplified overview of industry best practices to help protect O&G pipelines from intentional or accidental security threats. While multiple standards and guidelines exist to offer perspectives on this subject, this document addresses the most consistent themes highlighted throughout the standards and guidelines, as well as introduces some of the latest developments that may pose a threat to reliable pipeline operations.

A key theme throughout this document, beyond describing standards, guidelines, and the nature of threats, is to make organizations recognize that they must have the appropriate personnel, internally or externally, to effectively support their cybersecurity practices. The industry is taking steps to meet this need as shown in Figure 1, but additional progress is still required.

1. https://newsroom.accenture.com/news/accenture-report-oil-and-gas-companies-cybersecurity-strategies-are-evolving-but-monitoring-and-responding-quickly-to-cyberattacks-remains-a-challenge.htm
2. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Figure 1 Challenges of Managing ICS Security[1]

A recent SANS Institute report[2] found that four out of ten organizations lack appropriate visibility into their ICS networks to monitor assets and operations to identify potential threats. This creates the risk of not being able to recognize and respond to attacks. How do you secure what you do not understand?

Cisco, Schneider Electric, and AVEVA work with a wide range of organizations involved in the design, construction, and operation of critical pipeline assets in midstream and downstream environments. We are consistently asked to help plan a comprehensive security strategy and roadmap, helping organizations navigate through the growing security threat landscape.

This document provides the foundation to develop a strong security posture and roadmap, with practical advice and recommendations as to what to do and when throughout the security lifecycle.

Document Scope

In order to provide best practice guidance versus design and implementation techniques. Cisco, Schneider Electric, and AVEVA services teams are available to jointly build on this guidance and deliver detailed individual customer designs, architectures, roadmaps, and implementations.

The key standards covered in this document that relate to O&G pipelines and ICS security include:

- IEC 62443 Industrial Control System standard
- API 1164 Pipeline Supervisory Control and Data Acquisition (SCADA) Security standard
- NIST 800-82 Guide to Industrial Control System Security
- IEC 27019 Security Management for Process Control
- Chemical Facility Anti-Terrorism Standards (CFATS)
- NERC-CIP where interfacing with the power grid, and remote station best practice electronic and physical perimeters
- TSA Guidelines

1. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf
2. https://www.sans.org/reading-room/whitepapers/ICS/securing-industrial-control-systems-2017-37860

This document is designed to complement and enhance the security advice provided in the jointly-delivered validated design and implementation guides for control centers and operational pipeline communication networks that can be found at:

- Smart Connected Pipeline—Control Centers: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-control-center.html
- Smart Connected Pipeline—Operational Telecoms: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-operational-telecoms.html

Introduction and Industry Overview

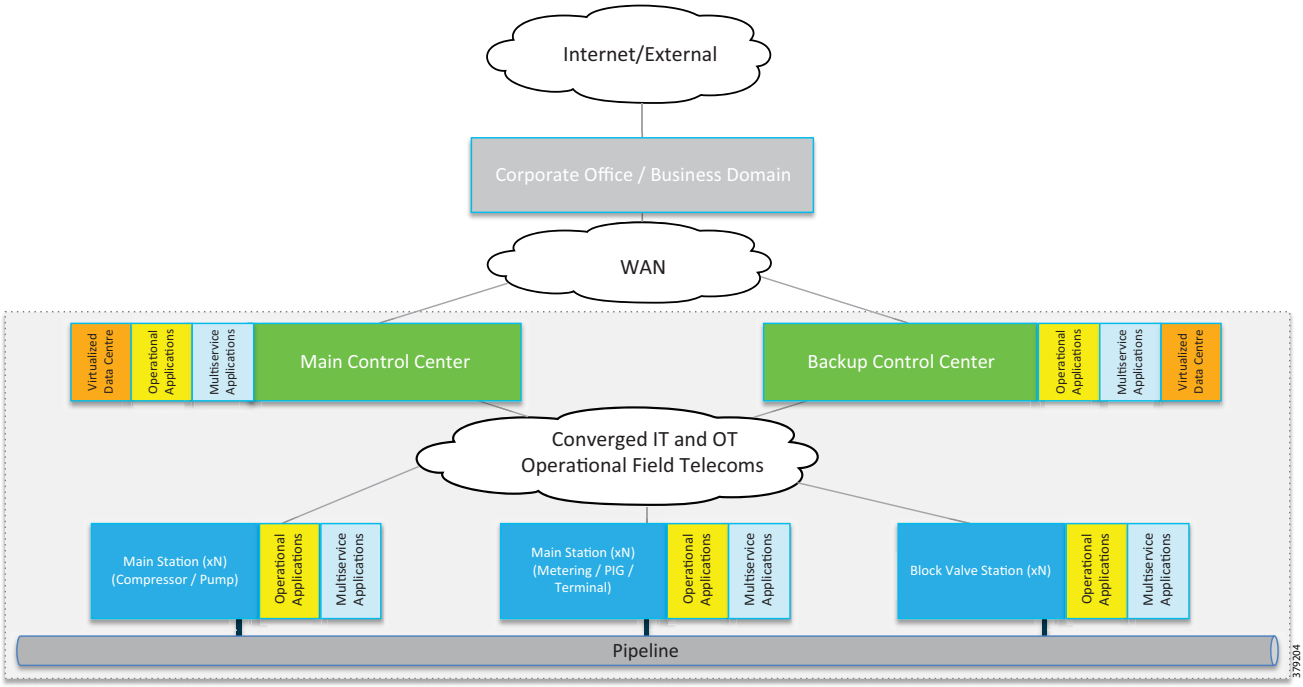
Transmission and distribution pipelines are the key transport mechanism for the O&G industry, operating continuously outside of scheduled maintenance windows. Pipelines provide an efficient, safe, and cost-effective way to transport processed or unprocessed oil, gas, and raw materials and products both on and offshore. It is essential that they operate as safely and efficiently as possible. When problems occur, they must be able to expeditiously restore normal operation to meet environmental, safety, quality, and production requirements.

Oil and Gas Pipeline Environment

For all pipeline operators, the safety and high availability of PMSs and underlying infrastructure is paramount. O&G pipeline management is challenging, with pipelines often running over large geographical distances, through harsh environments, and with limited communications and power infrastructure available. In addition, pipeline operators must operate their lines safely, following regulatory requirements such as Pipeline and Hazardous Materials Safety Administration (PHMSA) and industry best practices, to include ensuring compliance with stringent environmental regulations, while also addressing growing cyber and physical security threats.

The O&G pipeline architecture (Figure 2) includes operating processes and safety and energy management functions geographically spread along the pipeline for a set of stations.

Figure 2 High-Level Pipeline Architecture



Stations vary in size and function, but typically include compressor or pump stations, metering stations, Pipeline Inspection Gauge (PIG), terminal stations, and block valve stations. Each asset must be linked with the applications and processes at the Control Center(s) (main and backup) and sometimes at other stations through operational field telecoms infrastructure. The infrastructure must be implemented in a reliable and efficient way, avoiding communications outages and data losses. The Control Center(s) should also be securely connected to the enterprise to allow users to improve operational processes, streamline business planning, and optimize energy consumption. It is important to note that some of these services may reside in the operational control center.

Pipeline Applications

The traditional approach to safe and efficient pipeline operations is achieved through real-time monitoring and control using the collection of data to a centralized PMS. The PMS combines SCADA with real-time applications specific to the O&G industry such as leak detection and flow measurement.

These integrated applications provide pipeline operators with:

- Real-time or near real-time control and supervision of operations along the pipeline through a SCADA system based in one or more Control Centers
- An accurate measurement of key performance indicators (KPIs) such as flow, volume, and levels to ensure correct product accounting
- The ability to detect and locate pipeline leaks, including time, volume, and location
- Safe operations through instrumentation and safety systems where included
- An energy management system to visualize, manage, and optimize energy consumption within main stations
- Asset performance management such as condition-based monitoring and predictive analytics to proactively assess and address asset health

In addition to the pipeline management applications, non-production applications that support pipeline operations, such as physical security, voice, Public Address and General Alarm (PAGA) safety announcements, video, and wireless, also exist.

Both types of applications are mentioned because both are subject to threat and may potentially disrupt pipeline operations. As such, they need to be included as part of a holistic security strategy. Furthermore, many of these applications are bridging operations and business. Customers are leveraging solutions that are exclusively on-premise, exclusively in the cloud, or various hybrid solutions. This introduces new areas of security concerns that must be included in any security analysis and planning. The use of the cloud introduces new security concerns, along with the architecture of cloud-based solutions. A true SaaS offering where multiple users share the same common application introduces the risk of cross-user data exposure along with accessibility using the web to sensitive data stored in the cloud. This increases the attack surface and requires both the user and the supplier to consider how data is protected.

The last few years have seen an explosion of new technologies that can help improve the efficiency, availability, and safety of pipeline operations, including:

- Leveraging fiber for acoustic sensing for leak detection and tamper and intrusion prevention
- Virtual reality
- Big data and analytics
- Fog and edge computing
- Advanced integrity management
- Enterprise asset performance management (EAPM)
- Cloud computing
- Industrial Internet of Things (IIoT)

Although they bring new benefits, the challenge is that they also bring potentially new security attack surfaces and expose pipeline operations to new risks.

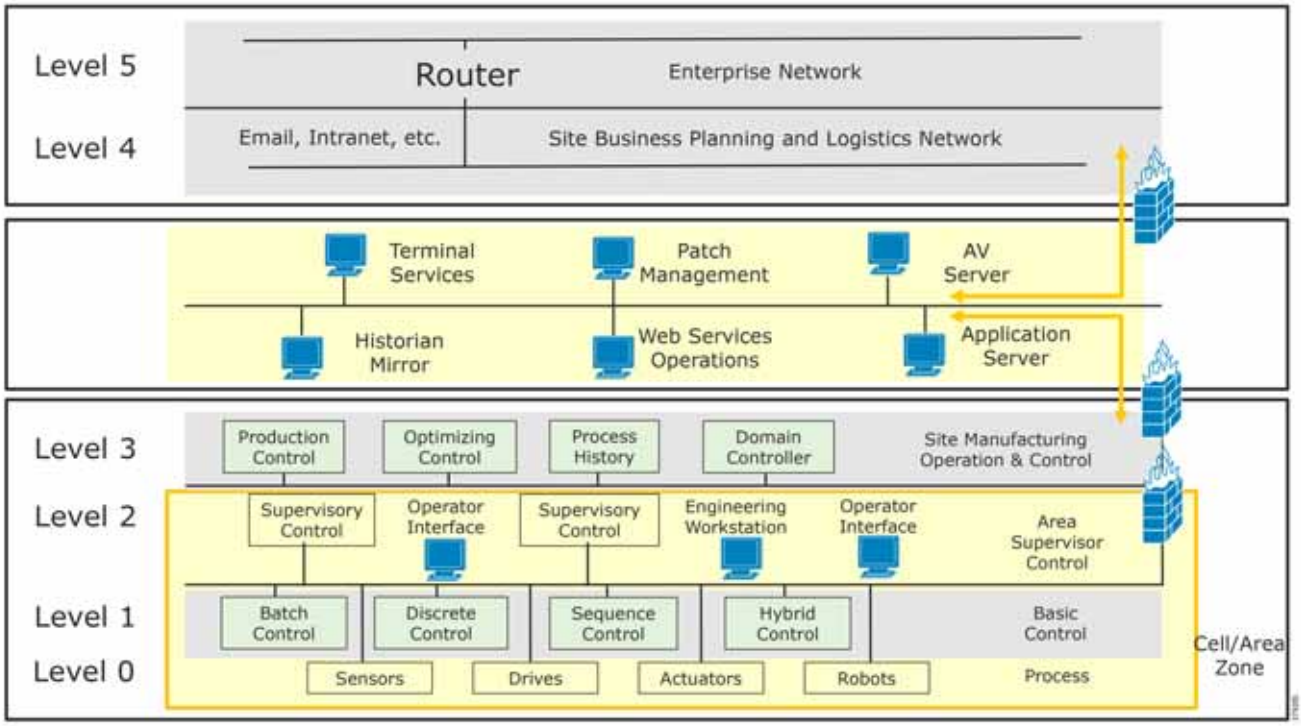
Traditional Security Architecture Approach

Secure architectures for both the operational and the enterprise layers associated with a pipeline are critical components of any design.

IEC 62443 is the most widely adopted cybersecurity standard globally for ICSs and is the *de facto* standard in the industry, evolving from the 1990s when the Purdue Model for Control Hierarchy (Figure 3) and ISA 95 established a strong emphasis on security architecture using segmented levels for ICS deployments. This was further developed through ISA 99 and IEC 62443, bringing additional risk assessment and business process focus. This segmented layered architecture forms the basis of many industrial system architectures and ICS security architectures.

The Purdue Model for Control Hierarchy also describes a hierarchical data flow model, where sensors and other field devices are connected to the ICS. The ICS serves the dual purpose of controlling processes or machines and serving processed data to the operations management level of applications. Level 3 applications feed information to the enterprise business system level through Layer 3.5.

Figure 3 Example Purdue Model for Control Hierarchy Architecture



The model has seen an additional level informally integrated, mainly due to the divide between the OT and IT domains. The Level 3.5 Industrial Demilitarized Zone (IDMZ) provides a strict segmentation zone and boundary between layers. However, services and data need to be exchanged between the enterprise layer and the ICS. Systems located in the IDMZ, such as a shadow historian, bring all the data together for company personnel in a near real-time system, publishing near real-time and historical information to the enterprise layer for better business decision-making.

No direct communication is allowed between the enterprise layer and the ICS layer. The IDMZ provides a point of access and control for the provision and exchange of data between these two layers. The IDMZ provides termination points for the enterprise layer and the operational domain and hosts various servers, applications, and security policies to broker and police communications between the two domains.

The traditional model has focused on segmentation and restricted traffic flows, but this is not enough to secure an operational domain. More recently, the National Institute of Standards and Technology (NIST) Cybersecurity Framework—with its charter to protect critical infrastructure—has strongly emphasized the human component of cybersecurity. A number of industry-specific regulations and guidelines for pipeline operators, such as API 1164 for SCADA security, also exist.

The reality is that technology itself can only address about half of the cybersecurity threat, whereas people and process play a critical part in every aspect of threat identification and monitoring. This means that guidelines and standards are not concrete measures to provide protection, but do provide a solid foundational base from which to work. The most comprehensive approach to securing the PMS combines technology, people, and processes, both cyber and physical.

A properly designed standards-based architecture to secure use cases and systems, bringing together the operational (Levels 3 and below) and enterprise (Levels 4 and above) domains, is critical. The architecture should provide an understanding of all components of a use case, map these elements together in a structured way, and show how they interact and work together. A properly designed architecture not only brings together IT and OT technologies, but also includes vendors and third-party content; in other words, it secures the ecosystem. Gartner[1] believes that security can be enhanced if IT security teams are shared, seconded, or combined with OT staff to plan a holistic security strategy.

1. http://www.gartner.com/newsroom/id/1590814

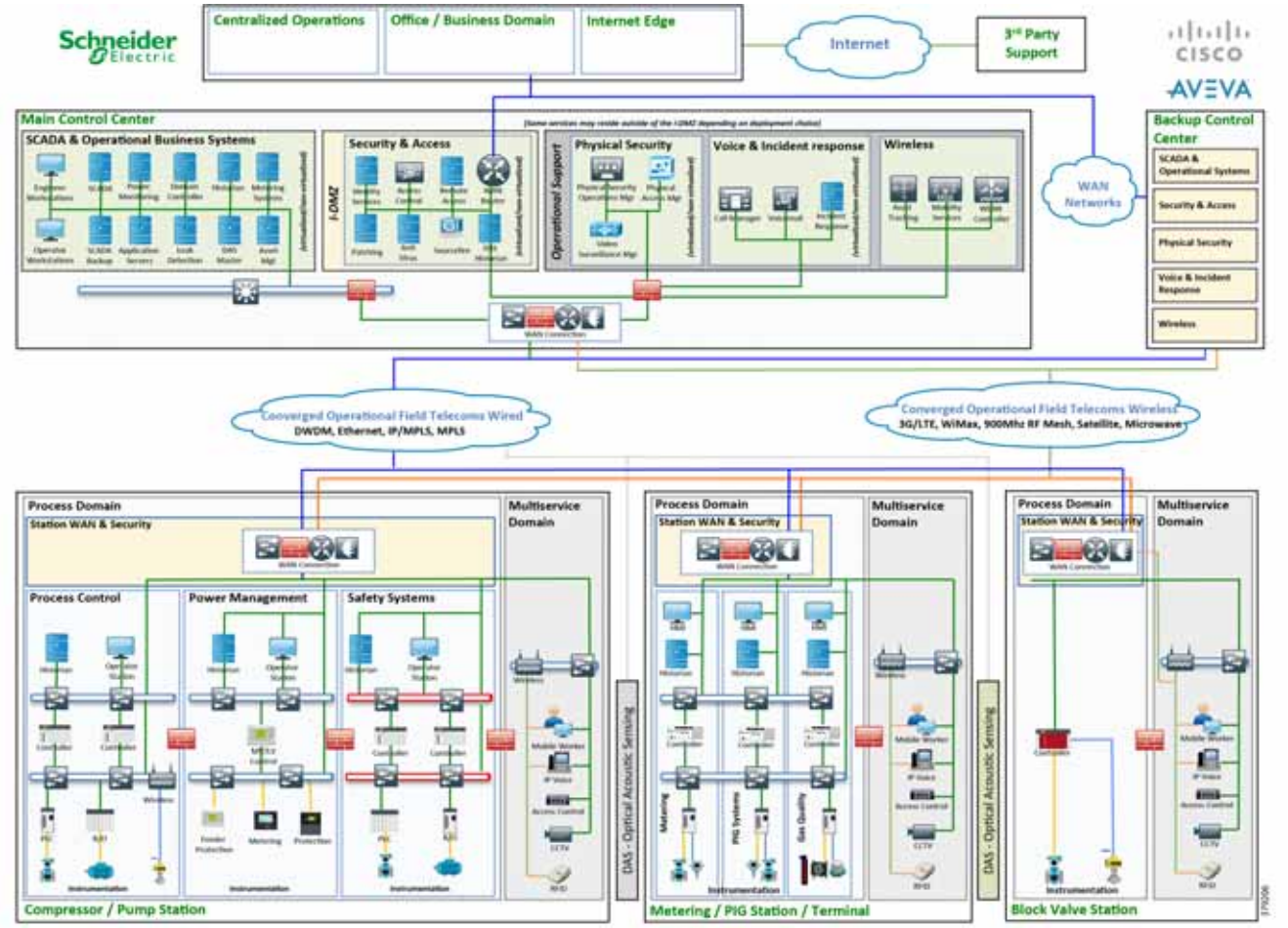
Cisco, Schneider Electric, and AVEVA Joint Reference Architectures

As part of the initial validation efforts for the Smart Connected Pipeline, Cisco, Schneider Electric, and AVEVA created a foundational reference architecture following the principles of IEC 62443. This represents a forward-looking functional architecture for end-to-end pipeline infrastructure. The aim is to provide a flexible and modular approach, supporting a phased roadmap to O&G pipeline operational excellence.

The architecture is based on a three-tier building block approach as defined in the joint Cisco and Schneider Electric reference architecture (Figure 4).

- **Control Center**—Virtualized, geographically separate, redundant Control Centers
- **Operational Telecoms Network**—End-to-end communication from field device to Control Center application for operational and multi-service applications
- **Pipeline Stations**—Local area networks inside the stations for operational and multiservice applications

Figure 4 Cisco, Schneider Electric, and AVEVA Reference Architecture



This solution architecture has been implemented in a number of deployments. It provides a strong foundation, following recognized security standards, and as it is jointly validated, helps to reduce risk for operators. However, due to the changing industry discussed in the next section, it is already evolving to include a number of new areas.

It is important to note that the reference architecture should be considered as a framework for a comprehensive PMS, but for operators that have less complex solutions, their needs are still recognized within the overall reference architecture. The design components and security infrastructure define a best practices structure that is recommended for midstream systems, thus the security concepts are applicable regardless of the complexity or design of the system in relation to the presented reference architecture.

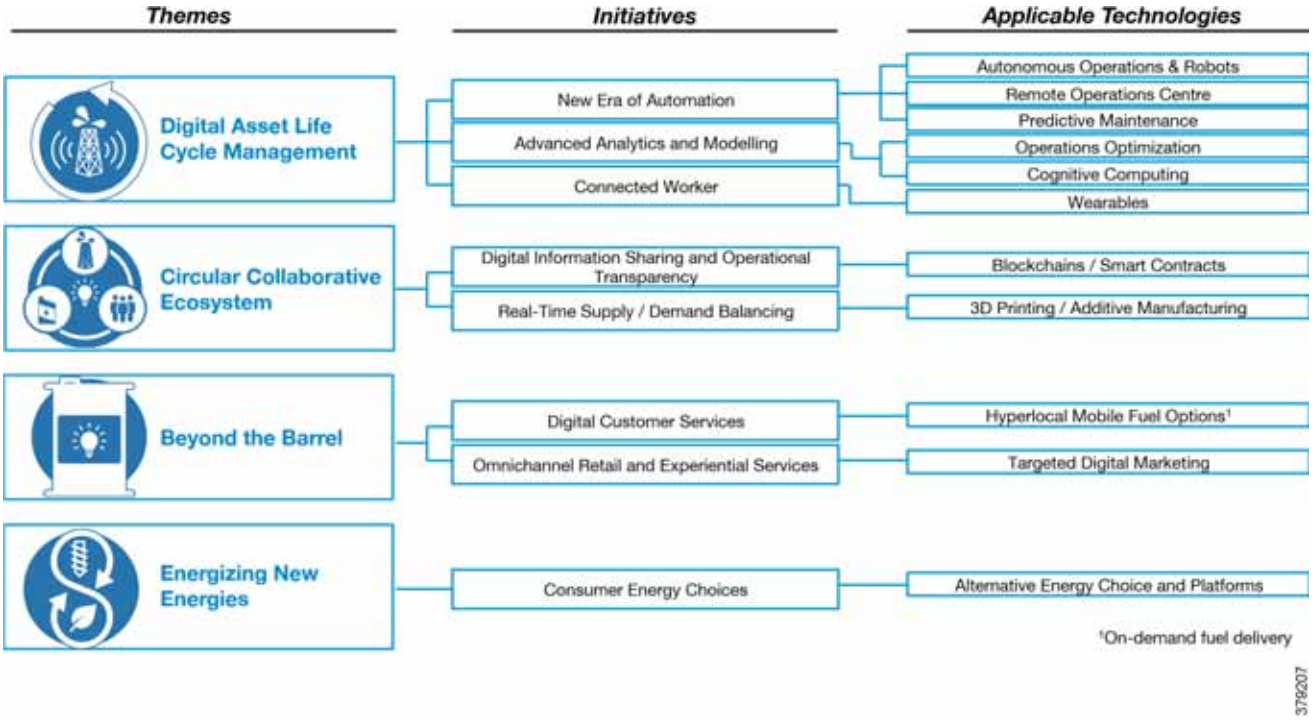
An Evolving Industry

The continuous evolution of technology directly affects the O&G segment. Most of the global technology trends are producing significant changes in the way the industry faces current and future challenges.

Most industrial environments, including O&G, are subject to transformation due to digitization and the benefits it brings, a number of which are shown in Figure 5. A 2017 World Economic Forum report[1] highlighted operations optimization and predictive maintenance as the two leading opportunities to provide value to the industry, with both residing in the digital asset life cycle management category. Remote operations centers, the connected worker, and autonomous operations and robots came third, fifth, and sixth, respectively. All of these areas that are needed to provide additional value to an evolving industry require new technologies to be realized, all of which need to be considered from a security perspective.

A number of enabling trends that are associated with digitization are discussed in Figure 5.

Figure 5 Digital Initiatives in the Oil and Gas Industry (Source: World Economic Forum)

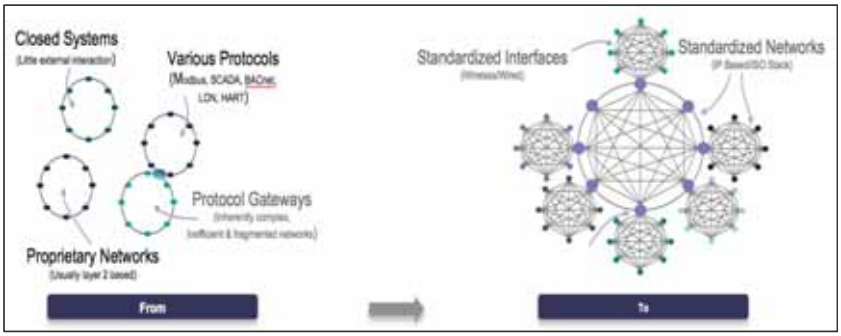


1. http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-oil-and-gas-industry-white-paper.pdf

Interoperability and Openness

The standard security architecture model has historically been a security-by-obscurity approach with physically isolated networks. Control systems were standalone with limited public access and proprietary or industrial-specific protocols, which were deemed too difficult to compromise. This approach may have been appropriate for control systems with highly restricted access (communications and people) and limited connection to IT; however, changes become necessary as systems developed with new features and functions to enhance performance and efficiencies and organizations seek to take advantage of newly available data. In addition, newer enabling technologies such as cloud computing, distributed fog and edge computing, real-time streaming analytics, and IIoT platforms are leveraging open interoperable protocols along with standardized interfaces. This means both traditional and newer systems communications architectures are based by default on Internet Protocol (IP) and Ethernet wired and wireless infrastructure (Figure 6).

Figure 6 Digitization and Evolving Architectures



Commercialization

Commercial off-the-shelf (COTS) technology is increasingly being introduced into the pipeline environment to perform monitor and control tasks, replacing devices that were built specifically for the operational environment. Devices such as mobile handsets and tablets, servers, video cameras, and wearable technology, as opposed to specifically designed ICSs hardware, are being implemented. These devices are necessary to enable new use cases, but their deployment that they achieve, along with operational technology, need careful consideration and appropriate architectural implementation to ensure the same levels of security as the operational systems to which they contribute.

Industrial Internet of Things

The O&G industry has experienced the connection of a proliferation of new devices to systems to replace existing functions or perform new ones. IIoT technologies are being used to connect pipeline networks, sensors, leak detection devices, alarms, and emergency shutdowns allowing companies to analyze and interpret data to reduce major risks.

As pipeline operators continue to adopt new technologies and use cases, new and diverse devices are being connected to the network, which provides potential new areas of security vulnerability.

Big Data and Analytics

Big Data and analytics (streaming, real-time, and historical) trends are leading to increased business intelligence through data derived from connecting new sensors, instrumentation, and previously-unconnected devices to the network. In parallel, business units and external vendors need secure remote access to operational data and systems to provide additional support and optimization services. These business requirements lead to a multitude of new entry points with the potential to compromise PMS security.

IT and OT Convergence

Organizationally, a shift has occurred to an increasing convergence between historically separate IT and OT teams and tools. This has led to more IT-centric technologies being leveraged for PMS. Information derived from operations is typically used to make physical decisions such as closing a valve, IT data is typically leveraged to make business decisions, and convergence enables the business to perform tasks such as process optimization or measurement. Regardless of the type of technology or information, the business must treat any security challenges in a similar manner. As the borders continue to blur between these traditionally separate domains, strategies should be aligned and IT and OT teams should work more closely together to ensure end-to-end security. At a minimum, this means organizations need to rethink how they address architectures, management, administration, policies, and infrastructure.

However, OT and IT security solutions cannot simply be deployed interchangeably. The same technology may be leveraged, but how it is designed and implemented may be very different. Although IT and OT teams may be a part of the same organization, they have very different priorities and often skill sets. The reality is that some organizations still have a gap between IT and OT, with some being very siloed while others are much more closely aligned. Regardless, this separation, and in some cases, antagonism, is unlikely to disappear in the short-term. Gartner research[1] argues that a shared set of standards, platforms, and architectures across IT and OT offers the opportunity in some circumstances to reduce both risk and cost and cover external threats and internal errors. However consideration must be made for some of the differences related to high availability and architectural reliability for OT.

Virtualization and Traditionally IT-centric Technologies

In line with operational efficiencies introduced with virtualization and hyperconvergence, the advancement of these technologies has begun to affect system architectures. Historically, control systems were deployed on servers dedicated to specific applications or functions and on separate communication networks to isolate specific operational segments. In addition, multiservice applications supporting operational processes had separate dedicated infrastructures.

In current deployments, we now see virtualized data center server infrastructures not only being introduced, but actually becoming the standard deployment offering for PMSs and adopted by ICS vendors and end customers. The operational field telecoms and WAN networks also leverage virtualization technologies like VPNs, VLANs, and Multiprotocol Label Switching (MPLS) to logically segment traffic across common infrastructure.

Although there are many examples of physically separated systems, due to customer philosophy, standards, and compliance requirements, virtualized implementations are on the rise. As such, the security requirements and necessary skills to implement and manage these deployments are moving away from being operations-based (i.e., OT) and becoming more IT-centric. This aligns to the aging workforce in the industry, where many newer engineers come with more of an IT-centric approach due to their education, experience, and daily engagement with technology.

New Approaches to Security Design

Even with the Level 3.5 IDMZ, the traditional segmented architecture poses challenges for a digitally evolving PMS. Neither current nor future data are hierarchical in nature. Data has many sources and many clients that will leverage it, so that we are already seeing “smart” systems that can autonomously leverage data and initiate processes. Federated data structures with storage exist all over the organization, not just in central locations. Even though the segmented approach has been the de facto manner to architect PMS, it segregates IT/enterprise and OT services, with physical or heavily virtualized segmentation implemented. This separation is inevitably blurring and use cases may often need a combination of IT and OT services to provide the optimal business benefit. The ICS environment for pipeline operators is changing, but the need for secure data management and control of operating assets is still a primary concern.

These trends continue to drive the need for a more connected ICS, along with a more open architecture. In whatever manner we look at it, the need for a comprehensive approach to security that acknowledges the need for control system protection, while facilitating the open data demands of the new digitization era, has never been stronger.

1. http://www.gartner.com/technology/research/infrastructure-operations-management.jsp

> *"This may reveal an awakening to the degree of exposure inseparable from the increasingly connected nature of control systems. As the process of migrating from analogue equipment to digital and networked devices that communicate with each other - as well as with monitoring and control systems distributed across the boundaries of operations, enterprises, vendors and manufacturers - continues inexorably forward, organizations must recognize that the concept of the perimeter as primary safeguard is obsolete, and they must adapt their security practices to the new reality."* **SANS Institute**

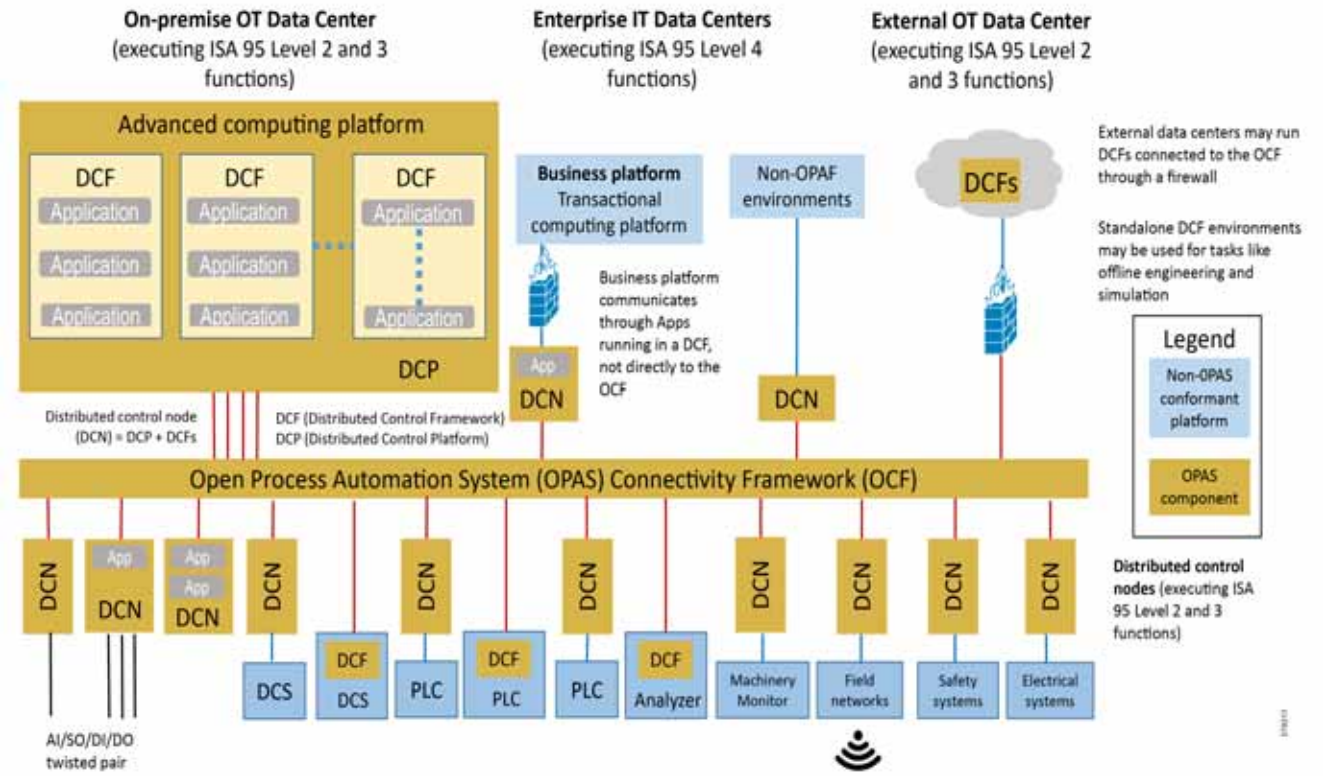
Newer Architectural Approaches

IT and OT convergence is inevitable, although the extent of this convergence, and to which parts of the business it will be applied, is not well understood. As shown in Figure 7, to deliver transformational operational use cases, such as real time analytics for machine health monitoring, the full IIoT stack (infrastructure, OS, applications, data pipeline, service assurance, security, and so on) is required. This means integrated IT-centric services must be deployed alongside OT services to generate business value. As such, IT capabilities are now becoming operationalized and pushing the boundaries of traditional security architectures, like the Purdue Model for Control Hierarchy and IEC 62443, where we are seeing more converged approaches based on easier sharing of data.

Figure 7 Addressing the Full IoT Stack Along the Edge to Cloud Continuum

These newer approaches focus on open architectures for peer-to-peer, scalable systems that support edge analytics, local monitoring, decision-making, and control. Recent standardized approaches such as Open Process Automation (Figure 8) are defining open and interoperable architectural approaches.

Figure 8 Open Process Automation Reference Architecture[1]



In many current traditional industrial environments, different vendor offer multiple control systems, each with its own set of protocols, philosophies, interfaces, development ecosystems, and security. This makes the introduction of new technologies challenging and more expensive to integrate and implement. The Open Process Automation approach is to develop a single industrial architecture to address these challenges. At its core is an integrated real-time service bus, open architecture software applications, and a device integration bus.

The central focus of the architecture in these approaches is a software integration bus acting as a software backplane that facilitates distributed control. Capabilities that include end-to-end security, system management, automated provisioning, and distributed data management build out the rest of the architecture.

Fog and Edge Computing

Another fundamental shift in the industry is the adoption of fog and edge computing, with microservices and analytics being deployed as close as possible to the edge of the network. In this way, information can be analyzed live at its source and real-time decisions can be made without data being sent across networks to a centralized resource to be actioned. These types of architectures are increasingly critical and leveraged in systems with low bandwidth links (e.g., 3G). Low bandwidth links make it impossible to transfer large amounts of data to a central location that is geographically dispersed or isolated (e.g., an offshore production platform or oilfield wellhead) or where information may need to be shared between devices at the edge in order to make a coordinated decision (oilfield wellhead cluster for reservoir optimization).

Typically these distributed architectures have multiple applications and functions hosted on an edge device, usually a mix of IT and OT. As an example, a single ruggedized server may be deployed that houses virtualization services for operator optimization applications, a virtualized controller from a process control vendor, and data normalization and protocol adaptor services from an industry software company. In addition, it may also include infrastructure services such as a virtualized router, switch, and security functions from a communications vendor, and real-time streaming analytics from another vendor.

1. http://albertadataarchitecture.org/data/documents/Open-Process-Automation-Standard.pdf

This approach requires securing multiple applications, functions, devices, and operating systems for multiple parties, including IT and OT functions.

This shifting landscape means that a different approach to the security posture may be required for the operational domain PMS. It also means a shift in the technical skill set, with a growing emphasis on having a well-rounded IT/OT engineer responsible for operating, maintaining, and securing today's control systems.

Increasing Threat Landscape

With digitization driving the connection of a plethora of new devices that can be leveraged for monitoring or control, the attack surface for cyber threats is increasing dramatically. Additionally, much of this new equipment is COTS, such as handsets and tablets, servers, video cameras, and wearable technology, versus specifically designed control systems hardware. These devices are necessary to enable new use cases, but careful consideration and appropriate architectural implementation—alongside traditional operational technology such as remote terminal units (RTUs) and programmable logic controllers (PLCs) needs—must be given to their deployment to ensure the same levels of security as operational systems. For example, IoT-enabled video cameras appear to readily address physical security needs easily and cost-effectively, but in actuality can open a network to compromise or be used as a malicious device in botnets.

A 2015 Accenture study[1] found that investment in big data, IoT, and digital mobility technologies is set to increase over the next five years. As organizations continue to evolve due to the recent oil price drop, the study found that the largest investments across the industry will be in mobility, infrastructure, and collaboration technologies. These will be leveraged to differentiate and improve competitiveness by enhancing operational processes through automation and business intelligence through new data sources. The study also found that cybersecurity and internal work processes will be the biggest barrier to deriving benefits from these technologies.

In parallel to these changes, non-operational business units, remote workers, and external service or vendor support companies require secure remote access to operational data and systems to provide support and optimization services. Again, these needs give rise to potential entry points, increasing the surface by which operational security may be compromised.

Threats may come from internal or external sources and may be accidental or malicious. The reality is that easy access to cyber information, resources, and tools have increased, making it simpler for hackers to gain an understanding of legacy and traditional protocols with the aim of gaining access to ICSs.

A DNV survey[2] found that, although companies are actively managing their information security, just over half (58%) have adopted an ad hoc management strategy, with only 27% setting concrete goals.

To maintain the high availability and reliability pipeline operators require, security cannot be a bolt-on afterthought or a one-off effort and it cannot be dealt with by technology alone. To best secure the PMS, a holistic approach needs to take place at an ecosystem level and it needs to be a continual process built into the governance and compliance efforts of any pipeline operator organization.

1. https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_15/Accenture-Microsoft-Digital-Energy-Survey-2015.pdf
2. https://www.safety4sea.com/dnv-gl-reveals-top-ten-cyber-security-vulnerabilities-for-the-oil-and-gas-industry/

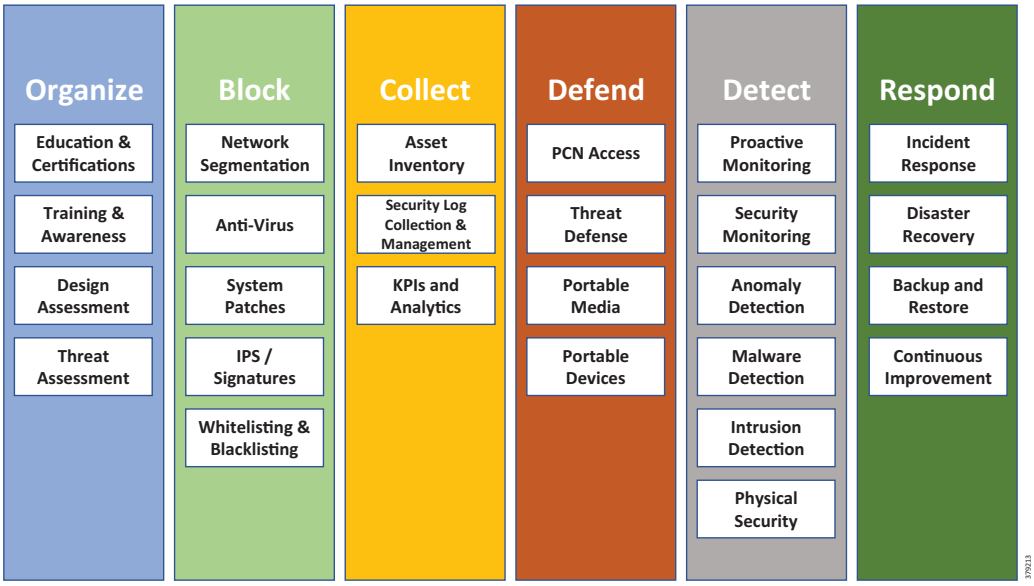
> *"A study of oil and gas companies in the US found that 61 percent of respondents say their organization's industrial control systems protection and security is not adequate, and only 41 percent of respondents say they continually monitor all infrastructure to prioritize threats and attacks.* ***In fact, an average of 46 percent of all cyber attacks in the OT environment go undetected, suggesting the need for investments in technologies that detect cyber threats to oil and gas operations."*** **Ponemon**

Security Process Lifecycle

Historically, security has been focused on keeping out potential attackers through a perimeter-based defense strategy. Today, the standard thinking is to anticipate a successful attack and to design and defend a network with a defense-in-depth approach to minimize and mitigate damages. This approach involves a multi-layered, multi-technology, and multi-party strategy to protect the organization's critical assets.

However, security cannot be a one-off incident and reactive response; it must be treated within the context of a life cycle involving everything from awareness to response, with the security life cycle being addressed through an appropriate Risk Control Framework (Figure 9).

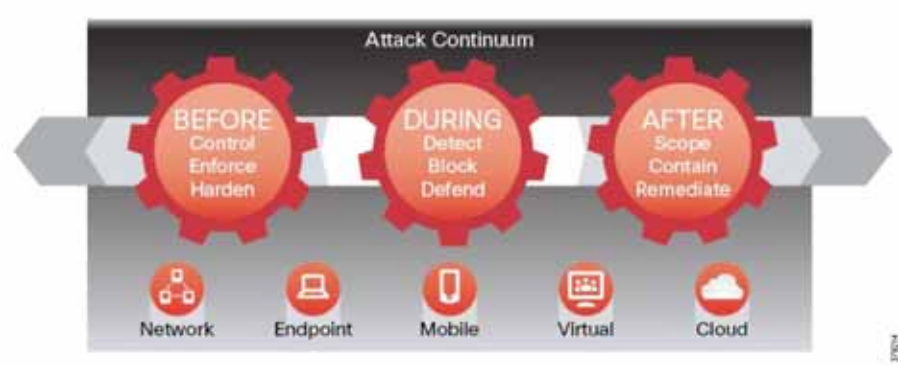
Figure 9 Example Risk Control Framework (Source: Cisco)



Attack Continuum

As this document has highlighted, a sound security process cannot be a reactive and isolated concept, but must take a holistic view of the system, addressing security in all areas of the system. In Figure 10, the attack continuum is shown consisting of three phases: before, during, and after an attack. In each phase, take note of the actions associated and how they identify activities that should be undertaken to reduce the risk of a successful attack proceeding undetected. Remember, an attack can come from many different sources, therefore, a broad perspective should be maintained throughout the lifecycle process.

Figure 10 The Security Attack Continuum



The reality is that no single security technology can address all security threats and point-in-time technologies are often bypassed as threats are designed to evade initial detection. The security approach must address detection and the ability to mitigate impact after an attack occurs. The security model for pipelines should not just concentrate on the endpoints that are often cited as the most vulnerable, but across the extended network from the edge to the control center to the enterprise, considering the entire attack continuum before an event occurs, during the event, and after the event.

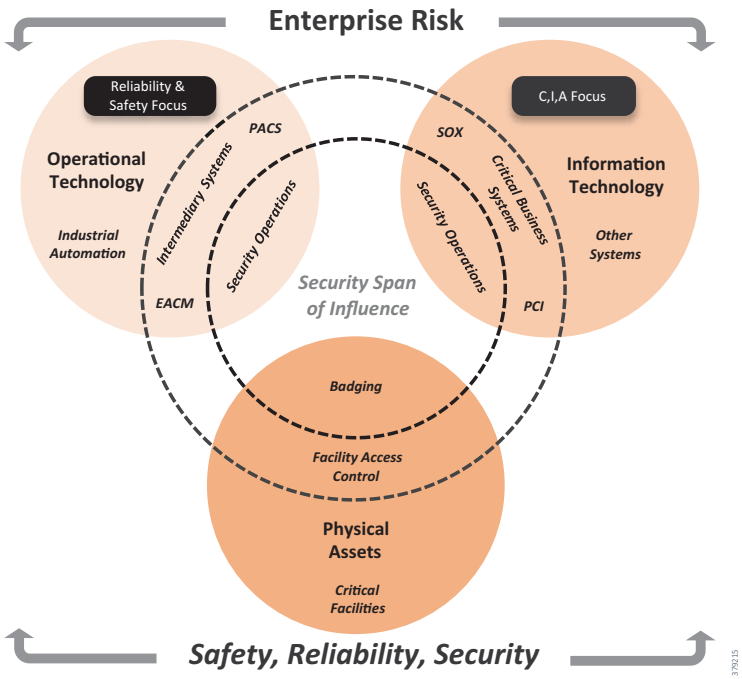
As noted, the full attack continuum can be broken into three phases: before, during, and after. Security measures must not only address detecting and blocking threats, but also include ongoing analysis following an attack to adapt the environment before the next one occurs. No system is truly secure and security cannot be guaranteed. Therefore, to most effectively address customer security and compliance needs, any security approach must offer protection along all phases of the attack continuum for both the PMS and the underlying infrastructure.

Addressing Enterprise Risk

Security for pipelines should take a holistic approach for all parts of the organization that touch the pipeline and associated systems and processes. This may sound obvious, but often security approaches are specific and implemented by a particular part of the organization, even though the system comprises many different components and may be used by many different areas.

The security capability should span the enterprise (Figure 11) and should interweave with existing processes and strategies in addition to being linked to the compliance effort. An organization needs visibility into any and all potential operational risks across a PMS to achieve a comprehensive, effective, and sustainable security program. The security span of influence should encompass OT, IT, and physical assets to best address risk and meet safety and reliability goals and standards.

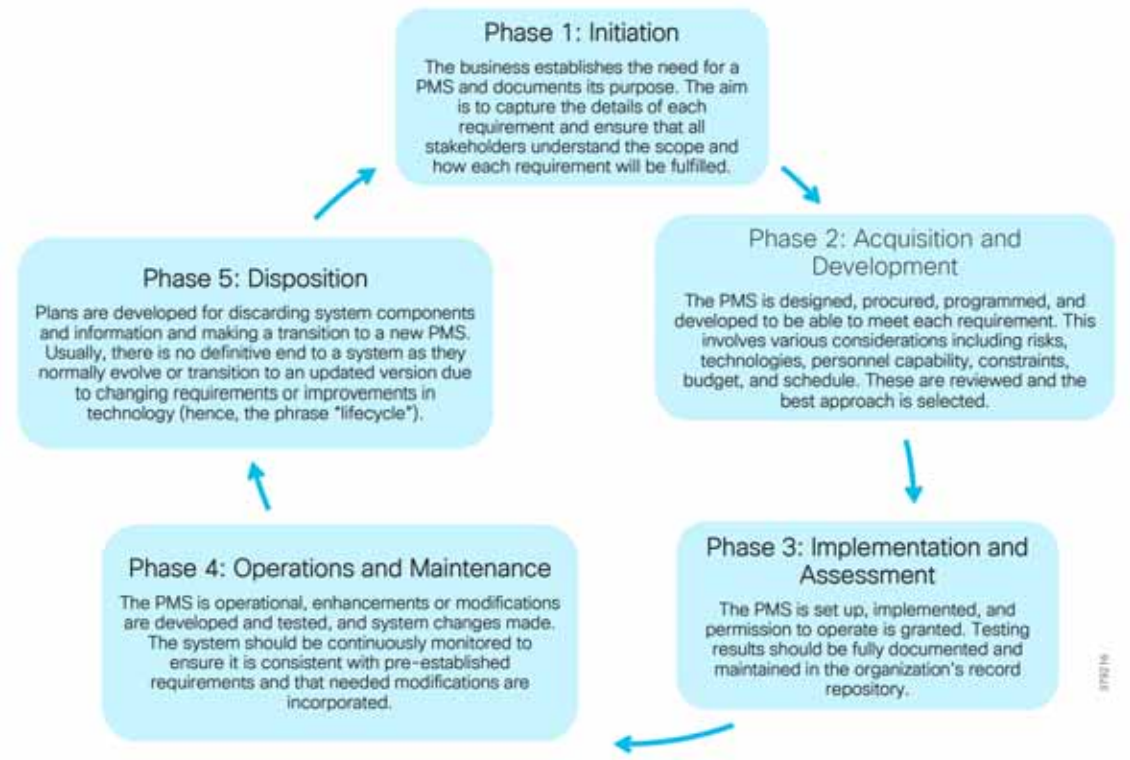
Figure 11 The Enterprise Security Risk



System Development Lifecycle

Best practice means that we need to consider how to take a practical and procedural approach to securing the system before deciding on the technologies, products, and processes we will use. System design and best practice usually follows a phased approach known as System Development Lifecycle (SDLC), as outlined in NIST SP 800-63 and IEC 62443-4-1 Product Development Requirements. A general SDLC includes five distinct phases as shown in Figure 12, although this could be further broken out.

Figure 12 Secure Development Lifecycle Phases



Each SDLC phase should include a set of security steps to be followed integrating security directly into the PMS throughout its lifecycle. To be most effective, security must be included in the SDLC from the outset. By building the system with a robust security architecture at its core and integrating with broader organizational compliance and governance efforts, a more effective as well as a more cost-effective development process can be achieved.

NIST recommends this early integration to maximize return on investment through:

- Identifying and mitigating security issues early, resulting in lower cost of implementing security controls
- Awareness of potential engineering issues created by mandatory security controls and addressing in advance
- Identifying opportunities for shared security services and reuse of security strategies and tools, reducing the cost and time taken to implement
- Aiding informed decision-making through risk management in a timely manner

Phase 1—Initiation

This includes security categorization based on potential impact in the event that a security breach occurs, a preliminary risk assessment to define the environment(s) the PMS will operate in, and initial basic security needs of the system. All system components, including process assets, computing, network infrastructure, and physical security should be considered in this phase.

Phase 2—Acquisition and Development

This phase has a number of security-focused areas including:

- **Formal Risk Assessment**—Security risk assessments allow organizations to assess, identify, and amend their overall posture and to enable stakeholders from all parts of the organization to better understand organizational risk from security attacks. The goal is to obtain leadership commitment to allocate resources and implement appropriate security solutions. A security risk assessment helps determine the value of data throughout the business. Without full awareness of how data is used and shared, it is incredibly difficult to prioritize and allocate resources where they are most needed. The risk assessment is a formal process, which builds on the preliminary assessment, identifying and documenting protection requirements for the PMS.

- **Functional Requirements Analysis**—These are security services that must be achieved by the system under inspection. Examples could include the security policy, the security architecture, and security functional requirements. These can be derived internally or through best practices, policies, regulations, and standards derived from regulations.

- **Non-Functional Security Requirements Analysis**—These are requirements like high availability, reliability, and scalability and are typically derived from architectural principles and best practices or standards. This might also involve assessing whether security was defined the right way according to best practice, ease of use, and minimization of complexity.

- **Security Assurance Requirements Analysis**—This process should provide credible evidence that justifies a level of confidence in the system and assurance that it meets its initial security requirements. Security assurance refers to security requirements. Assurance must provide evidence that the number of vulnerabilities are reduced to such a degree that it justifies a certain amount of confidence that the security properties of the system meet the established security requirements and that the degree of uncertainty has been sufficiently reduced. Based on both legal and functional security requirements, the analysis determines how much, and of what kind, assurance is required. The focus should be on minimizing vulnerabilities, since there can never be a guarantee that these have been eliminated.

- **Cost Considerations and Reporting**—Determine how much of the development cost of hardware, software, staff, and training can be associated with information security over the life of the system.

- **Security Planning**—Formal planning that defines the plan of action to secure a system. It includes a systematic approach and techniques for protecting a system from events that can impact the underlying system security. It can be a proposed plan or a plan that is already in place. The aim is to fully document agreed upon security controls, a description of the information system, and all documentation that supports the security program. Examples include a configuration management plan, a physical security plan, a contingency plan, an incident response plan, a training plan, and security accreditations.

- **Security Control Development**—The goal of security control is to protect critical assets, infrastructure, and data. This step ensures that the described security controls are designed, developed, implemented, and modified if needed.

- **Developmental Security Test and Evaluation**—Ensures the system security controls developed are working properly and are effective. These controls are typically management and operational controls.

Phase 3—Implementation

This stage includes:

- **Inspection and Acceptance**—Ensuring the organization validates and verifies that the described functionality is included in the deliverables.
- **System Integration**—Ensuring the system is integrated and ready for operation based on vendor and industry best practices and regulatory requirements.
- **Security Certification**—Ensuring implementation follows established verification techniques and procedures, typically provided by third-parties, providing confidence that the appropriate measures are in place to protect the PMS. Certification also describes known system vulnerabilities.
- **Security Accreditation**—Having a senior member of staff provide the necessary authorization of the system to process, store, or transmit information. For PMSs, common criteria include secure configurations for operating systems, device identity and inventory, key management and trust relationships, operational security verification, and capturing of required audit data.

Phase 4—Operations and Maintenance

This phase includes three main areas:

- Procedural aspects of security including training and awareness.
- **Configuration Management and Control**—Ensuring adequate consideration of potential security impacts caused by changes to a system. Configuration management and configuration control procedures are critical in establishing a baseline of hardware, software, and firmware components for the PMS and subsequently controlling and maintaining an accurate inventory of system changes.
- **Continuous Monitoring**—Ensuring controls are effective through periodic testing and evaluation. Examples would include verifying the continued effectiveness of controls over time, reporting the security status of the PMS to system operators, developing real time automated adaptive and continuous monitoring of devices to automate threat mitigation, and automating security tasks such as vulnerability assessments and penetration testing.

Phase 5—Disposition

The final phase involves:

- **Information Preservation**—Ensuring necessary information is retained for internal compliance or to conform to legal or regulatory requirements, as well as to accommodate future technology changes.
- **Media Sanitization**—Ensuring data is deleted as necessary and following proper disposal protocols as specified for the data type.
- **Hardware and Software Disposal**—Ensuring hardware and software is disposed of as per internal compliance and any legal requirements.

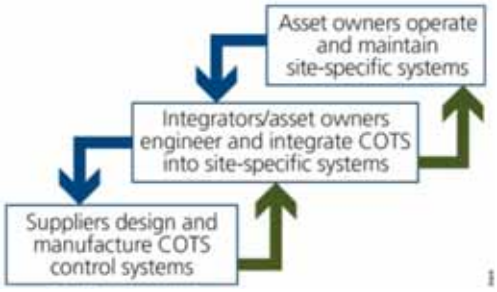
Establishing policies and procedures for the secure disposition of devices that held sensitive information or data is critical. Devices that have held sensitive information should be securely wiped of all data along with any associated certificates or identifiers.

> *"Life-cycle phases are important because the challenges and responses are different, but also interrelated, in each phase. The recommended cybersecurity responses must match the issues for each phase, and in almost every case, must address people, process, and technology."* **Andre Ristaino, ISA Secure**

In addition to the recommended steps, it is imperative that all parties in the PMS have a shared role for all phases of the cybersecurity lifecycle. ISA Secure recommends the relational approach (Figure 13) where:

- Product suppliers must securely develop COTS components that include security capabilities to support the intended use of the products in integrated operation and control solutions.
- System integrators must use practices that result in secure site-specific solutions to support the cybersecurity requirements for the intended deployment environment at operational sites.
- Asset owners or their designees must configure, commission, operate, and maintain the deployed solution in accordance with the solution's documented cybersecurity instructions, thereby ensuring that the solution's cybersecurity capabilities do not degrade over time.

Figure 13 Lifecycle Phases and Audiences[1]



Security Process

Cyber security programs are challenging. Now more than ever, organizations are leveraging digital strategies to optimize their businesses. This involves embracing new technologies, with each new device and associated configuration adding further complexity to an already complex attack surface.

As technology adoption accelerates, the recognized industry shortage of security expertise leads many organization's cybersecurity teams to struggle to effectively deal with cybersecurity issues and communicate these to leadership.

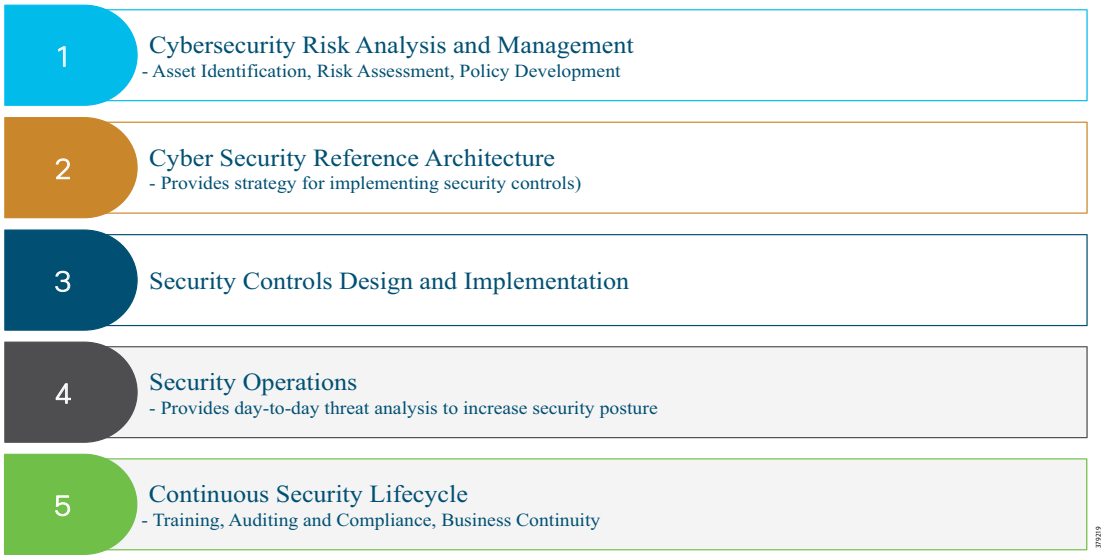
As pipeline companies evolve, cybersecurity management has become an essential and integrated business function. This requires the appropriate set of people, processes, and technologies to help understand the organization's current security posture. Following this, determining a target state for an improved profile is needed, all while managing budget constraints prior to creating a plan and recommending a roadmap to help deliver said target state. This should involve:

- Evaluation of the current PMS's cybersecurity management programs and underlying controls
- Identification of security gaps, ineffective operational processes, and poorly designed technology security controls
- Defining a security strategy and roadmap to address current and emerging threats to the pipeline system
- Developing and prioritizing security improvements to maximize return on investment and protect data and assets

1. https://www.isasecure.org/en-US/Articles/Industrial-automation-cybersecurity-conformity-ass

The security lifecycle follows the recommended steps in Figure 14.

Figure 14 Steps in the Security Lifecycle



The aim of the security process is to create a security strategy roadmap (Figure 16) to achieve an end goal best practice implementation architecture. This will take the PMS operator from the current to the desired state through a mixture of management, operational, and technology projects. This aligns the cybersecurity strategy with the business objectives and priorities by quantifying the financial impact of cybersecurity risks. In a 2017 Kaspersky report on OT and ICS security[1], of 359 companies surveyed worldwide, over half reported a cybersecurity incident in the past 12 months, with large companies suffering annual losses of $497,097. The majority reported having experienced between two and four incidents in that same period. The table in Figure 15 shows where these incidents originated.

1. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Figure 15 Sources of Cybersecurity Incidents

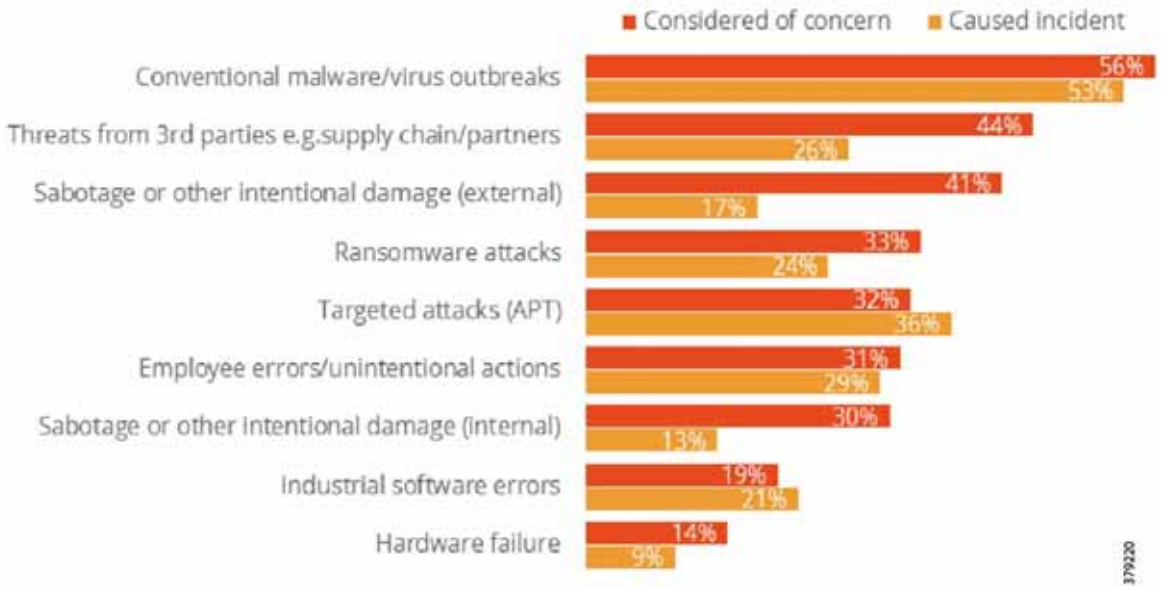


Figure 15 highlights malware as the most typical source of an incident, but targeted attacks were at 36%, a significant risk. The aim in this preventative process is to identify risk-mitigating security controls and financially quantify residual risk, then map security controls to business and technical objectives at specific places in the pipeline architecture.

The cost of an IT-related data breach can be significant, with the 2017 average, as reported by IBM[1], reaching $3.62 million at an average cost of $141 per compromised record containing sensitive data. This could be operations or commercial information that provides competitive advantage to your operations or those of your customers.

The result should be to securely integrate IT and OT domains and minimize risk, establish a baseline for security operations and compliance, and justify investments in security solutions to business leaders by rationalizing the implementation of specific security controls that mitigate the business' largest identified security threats.

1. https://www.ibm.com/security/data-breach

Figure 16 Example Security Strategy Roadmap

Administrative Components of a Security Program

To successfully bring security into the basic culture of the organization requires the engagement of its personnel, at all levels, along with the creation of policies that define the framework and enforcement actions required to institutionalize the security program into and throughout an organization.

Personnel

As noted, policies and procedures do not create a successful security profile for any operations company without the full participation of its people. This means that from the executive team to each employee, an organization must be fully engaged in creating a strong security culture. The following sections highlight the roles of individuals and departments in midstream and downstream organizations and how they contribute to the security profile and lifecycle, but these roles are found in all operational companies.

Chief Information Officer (CIO) and Chief Information Security Officer (CISO and CSO)

Generally, executive and managerial support must exist for the security policies and procedures to be implemented within an organization. The CIO or equivalent is generally responsible and accountable to ensure that the security policies and procedures are adequate and enforced throughout the organization. Security hardening is a component of the overall security policy and strategy within an organization. In some organizations, the role of the CIO will also have a focus on supporting operational LOB leaders to secure their environments.

IT and OT Staff

The two categories for discussion within the IT and OT organizations are:

- **Implementers**—Responsible for the creation, deployment, maintenance, and architecture of the network infrastructure
- **Users**—Use the network infrastructure to execute the business of the company

Implementers—Network and Security Administrators and Architects

The network and server staff are generally responsible for the overall design, implementation, and maintenance of the communications infrastructure and system. With the borders of separation between OT and IT now merging, security strategies should align and the teams should work more closely together at this level. Security policies adopted through regular IT security hardening are now filtering into OT standards (such as the NIST Energy Sector Asset Management and

IEC 62443-2-3[1]) to help secure ICSs and enable the IT staff to understand OT business flows and SLAs to help align the security implementation. Teams that support the multi-service systems (pipeline communications, physical security, business-enabling applications) must work closely with the teams responsible for the SCADA and PMSs.

This team or staff are the workhorses and technical experts for the system hardening policies and procedures. They are involved in all three phases of the attack continuum—before, during, and after. Related to hardening, the team needs to provide:

- Installation and configuration of systems aligned to security hardening policies
- Maintain system updates, patches, and backups on a continual basis
- Security risk assessments
- Continuous monitoring of the system for system integrity and security events
- Provide mitigation to security incidents and recovery from a security compromise
- Security testing of patches, updates, and any security mitigation before deployment
- Planning for improvements to the system hardening
- Continuously update technical knowledge to understand the latest threats and provide mitigation policies and procedures
- Document all procedures and policies
- Work with third-party vendors associated with the pipeline system

Users—Pipeline Operators, Plant Personnel, and Contractors

Users of the system have to comply with the policies and procedures of the security hardening and should be trained and regularly updated on all security policies. As this relates to hardening, access to the system is a good example where users need to follow security procedures. An end user should have neither the permission nor the ability to connect non-approved devices and applications to the SCADA system. For example, a contractor should use a laptop provided by an operator or only have access to the system through a dedicated terminal.

Roles and Program Alignment

A significant indicator of the success of a security program is found in the engagement of the members of the organization—from executive management to the summer intern. It is imperative that leadership sets the tone by their full participation and involvement. For example, there should be no exception to security policies such as Bring Your Own Device (BYOD) for executives versus “normal” employees. The process should start at the top and flow throughout the organization.

Policy Development

Policies form the framework upon which the organization functions and control what procedures and processes are defined and used. They define the rules related to security activities and help to characterize how the various organizations within an operational center work together. They also include potential corrective actions needed when policies are violated. Policies, like other components of the SDLC, must be regularly reviewed and updated to reflect organizational and operational changes and recommended best practices.

A policy should contain the following components:

- **Policy Statement**—Clearly denotes which security components it addresses.
- **Purpose of the Policy**—States why the policy is required.
- **Definitions**—Ensures that words and acronyms are clearly defined and unambiguous.

1. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-am-project-description-draft.pdf

- **Responsible Executive or Department**—Identifies the executive sponsor of the policy, along with relevant partners and peer organizations that must align with the policy.
- **Entities Affected by the Policy**—Specifies all members of the organization that are impacted by and must follow the specified policy.
- **Procedures**—Specifies the details of the policy, which may include sections such as general rules of behavior, training and enforcement, a comprehensive outline of actions, and rules and guiding principles necessary to implement the desired policy.

By clearly stating the procedures and identifying the parties that must participate and cooperate, the organization can remove ambiguity from the process and create a clear framework to guide and support the continuously improving security posture of the OT organization. Examples of security policies include:

- Passwords, their definition, frequency of change, and how they should be protected
- The types of devices that may be used within the OT environment, including wireless and other mobile technologies
- On boarding and off boarding processes as they relate to security and access control
- User access control philosophies

These examples serve to highlight how security needs to be considered throughout the organization. Security should be an integral and pervasive component of the culture. It contributes to the successful and secure delivery of services to customers while serving the company and protecting the environment.

The security policy should also be extended to third-party vendors who are involved with any aspect of the pipeline. This may be an internal process that details how third parties should be handled from a security perspective or a formally documented and agreed contract.

Cybersecurity Risk Analysis and Management

The intent of the Risk Analysis phase of the security process is to identify risks to the OT environment by looking at the vulnerabilities of the system and considering how they may be exploited, by whom, and the impact to the system in the event of a successful attack. A threat can either be an internal or external attack originating through malware, phishing attacks, human error, or other industrial cyber threats. It can also be related to environmental threats such as earthquakes, fire, water, or building security violations. These vulnerabilities can be found in the control systems themselves, the network infrastructure, the communications and field device systems, and the processes and procedures that frame how the system should be interacted with and managed.

Figure 17 Risk Management Process

Following the identification and investigation of vulnerabilities related to the control environment, the next step is to identify the impact to the PMS through an exploited vulnerability and to quantify the cost to the company. This weighted cost analysis helps to focus the company on where to apply their security focus given limited resources and budget.

This activity is not a one-off process, but an activity that should be performed annually, at a minimum, enabling the pipeline operator to address changing system demands, configurations, and the ever-changing threat environment.

Asset Discovery and Identification

Asset discovery and inventory is conducted using on-site workshops and asset discovery assessments, including reviewing any pre-determined security objectives, understanding the organizational structure, and using an automated asset discovery tool. The tool detects and visualizes IT and OT assets including Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), users, applications, switches, routers, and security devices. It also performs a protocol inspection to detect the protocols that are being leveraged in the PMS and to document communication flows between devices or endpoints. The aim is to build a complete picture of the operational environment and a baseline of standard “normal” operation.

Vulnerability Assessment

After identifying the base infrastructure, the next step is to investigate the system for vulnerabilities. Either internally or through an external consultant, industry standard tools are used to evaluate the PMS in light of potential vulnerabilities, including items such as open ports or unneeded services, weak or default passwords, USB access, clear text communication or tool usage, or weak access control definitions. Beyond these technical vulnerabilities, it is recommended that environmental vulnerabilities be identified, such as planning for disaster recovery, business continuity, and physical security.

Threat Assessment

The next step in a risk analysis is to quantify the threats by identifying the actors that could perpetrate an attack along with how it might be accomplished. For example, an internal actor could be an employee that acts on a phishing email and shares his password to an outsider believing the email was from the organization’s IT department. An external actor could be a support person bringing an infected USB drive and inadvertently installing malware on the system. Other attacks could spring from an ad hoc wireless network providing unintended access to the control network. It is important to note that not all attacks are intentional, but rather the result of poor training, naiveté, and unintentional actions which can open a system to exploitation.

Risk Assessment

After gaining a clear understanding of how the system is configured and how it operates and performs under normal circumstances, identifying system vulnerabilities, and identifying who might initiate and how exploitations might occur, risk assessment moves to a quantitative phase.

Fundamentally, the formula that is used to quantify a particular risk is:

Risk = Asset * Vulnerability * Threat

Where:

- Asset is the dollar value of the asset at risk.
- Vulnerability is the likelihood of it happening (0–100%).
- Threat is the impact of the threat: High (100%), Medium (50%), Low (10%).

In addition to this formula, it is necessary to identify the following items:

1. **Situation**—Specifies how a vulnerability could be exploited, for example, a fire in the control room or a compromised password.
2. **Threat and Vulnerability**—These designate the source of the threat and combine with the vulnerability; e.g., the same vulnerability could exist as both an internal and external threat.
3. **Area**—Specifies the security control area to which the risk pertains, e.g., policy, process, technical.
4. **Remediation**—Corrective actions that would mediate the identified risk.

By bringing these pieces of information together (Table 1), a risk assessment helps to quantify the impact that cyber risks may present to an organization and provides a guide for prioritizing the actions to be taken to improve the overall security posture of the system.

Table 1 Example Risk Assessment

Situation	Users accessing data that is not within their role and responsibility	Passwords easily compromised	Database information visible in Clear Text	User deletes data or software from personal servers or databases	Management and/or Auditors approach you to report on the status of the network with regards to attempted breaches, login failures, attempted probes, viruses, etc. Unfortunately, you have no information to provide.	A fire in the server room or other part of the facility.
Threat / Vulnerability	Internal / Access Control	External / Weak Passwords	External / Clear Text	Internal / Disaster Recovery + Access Control	Internal + External Auditing & Reporting	Environment / Disaster Recovery
Asset (Value)	$1,000,000	$500,000	$1,000,000	$1,000,000	$250,000	$500,000
Vulnerability (Likelihood)	20%	30%	10%	5%	50%	1%
Threat (Impact)	50%	50%	50%	50%	10%	100%
Risk (Valuation)	$100,000	$75,000	$50,000	$25,000	$12,500	$5,000
Area	Technical	Policy	Technical	Process	Technical	Process
Remediation	Implement a robust role-based access control paradigm that leverages Active Directory and is used to control data access universally.	Establish a password policy aligned to Microsoft best practices for critical sites.	Implement encryption on both the data and the communicatio n methods to remove Clear Text transmissions.	Establish contingency plans, including backups and assuring that access controls are in place to prevent data damage from unauthorized users.	Activate system eventing and audit trail information.	Establish a continuity plan in order to recover from a physical loss of equipment and data.

Cybersecurity End State

An end goal of a cybersecurity reference architecture (CSRA) is to provide a comprehensive, documented, formal model that overlays the Smart Connected Pipeline reference architecture mentioned later in this document. The CSRA also describes a methodology and an associated set of security controls that are mapped to business and technical objectives at specific places in a PMS.

In the context of this document, it provides:

- A defined security architecture for industrial pipeline requirements
- Secure integration of IT and OT domains
- The foundation for building secure operations
- Justification for investments in cybersecurity solutions to business leaders by rationalizing implementation of security control measures
- Minimization of risks by applying specific cybersecurity controls to mitigate well-known cybersecurity risks

The aim is to take an operator from their current state to a desired end state by identifying management, operational, and technology projects and determining when and how they should be implemented over a target timeline.

Design and Implementation of Security Controls

Security controls are safeguards or countermeasures implemented by an organization to protect itself from an incident that may result in the compromise of electronic information. When discussing security, a compromise of electronic information means any event that reduces the availability, integrity, or confidentiality of that electronic device. In a rapidly evolving technological and cybersecurity landscape, the conventional wisdom is that any organization can and will suffer a security incident—this it is a matter of when, not if. This very premise is what makes the strategic and effective implementation of cybersecurity controls so important.

Security controls may be of several types. Some are preventive and some are detective. Some are automated with configurable technical safeguards and some are manual procedures. It is through an effective balance of security controls across people, process, governance, and technology that an organization may not only enhance its ability to defend against a compromise, but also increase its ability to detect the inevitable security compromise while at the same time limiting its exposure and impact.

Security controls design may:

- **Prevent**—An organization performs these activities to make it more difficult for an attacker to compromise its systems, including vulnerability testing and server hardening, network segmentation, password hygiene, and user access provisioning controls.
- **Detect**—These controls include activities that an organization performs to discover security incidents in progress and alert them to cybersecurity support personnel. Detective controls may involve reviews of firewall and server logs, intrusion detection system (IDS) logs, and changes to system configurations.
- **Respond**—Response and recovery controls are critical as they are performed once a breach or other incident has occurred. These controls include the creation of an incident response plan:
  - A communication plan to notify authorities, management, and affected stakeholders (including end users, trading partners, and insurance carriers)
  - An approach to restore affected services
  - Performance of a root cause analysis of the compromise
  - Implementation of controls or system changes to prevent a recurrence

Seven Steps to Security Control Implementation

When implementing security controls, an organization should follow seven key steps:

1. **Select Control Standard**—Several respected industry groups have prepared cybersecurity standards that organizations can implement. Organizations can use these standards like a "controls catalog" to select the controls relevant for their specific risk profile and environment. The standards offer extremely useful guidance for organizations given their comprehensiveness. Organizations may not be fully aware of cybersecurity management processes and procedures. These standards offer critical insight into the specific controls that may be implemented as well as the management processes that an organization may follow to govern and oversee the cybersecurity efforts of the organization.

2. **Align Controls with Data Classification and Risk Assessment**—An organization may decide to follow a risk-based approach to implement controls; i.e., more valuable assets require more protection than less valuable assets. Resources are limited for all organizations, so when planning for a security control implementation, organizations need to decide which controls offer the most efficient protection and work to implement those controls.

3. **Prioritize**—Implementing security controls can be a time-consuming and sometimes expensive process. For example, technical safeguards like encrypting data at rest and in processing may require application architecture changes. Network segmentation could require the acquisition of new networking infrastructure. Other procedural changes may not have a hard cost associated with the implementation, but the changes could require significant resources and time to implement. Organizations need to align anticipated control benefits with available resources and prioritize the order of implementation.

4. **Design Controls**—While control standards provide a "controls catalog" approach for organizations to follow, the specifics of how an organization performs any given control needs to be designed. For technical safeguards, device-specific configurations need to be researched and defined. For manual procedures, discrete aspects like responsible performer, frequency of performance, required documentation, specific activities, and control documentation need to be defined.

5. **Train Control Performers and Users**—Before controls can be successfully implemented, an organization must train control performers on their responsibilities. Additionally, if certain controls require end user participation to help identify potential security incidents, the users need to be trained and understand the roles and responsibilities expected of them.

6. **Implement**—With all the planning, design, and training completed, this is the phase in which the control owners can put the new procedures into place and begin following the new controls. In the implementation phase, robust technical configurations are put into place for applications, servers, and network infrastructure. For manual or procedural controls, organizations implement the new workflows and review activities and performance documentation specified in the control designs.

7. **Integrate with Monitoring Function**—A major challenge for all process implementation and improvement projects is ensuring the new processes continue to be performed over time.

Security Operations

Operational Security Policy

Operators need to have clear guidelines on what they are and are not allowed to do. Escalation paths need to be defined that outline the steps to follow if an operator does not have the authorization required for a specific action. The operational security policy should clearly define the responsibilities and authorization, and, in case of breaches, disciplinary actions. The policy also acts as a deterrent against deliberate misconfigurations.

Change Management Process

Every company running a network should create precise processes that define and control how changes to the network are executed. The state of the hardware, operating system, and configurations should be monitored and all changes should be logged and executed in a controlled way. The logs should be evaluated and checked for potential misconfigurations. The logs can also be used to demonstrate a deliberate breach of the operational security policy. (For this, the concept of dual control is important and is discussed below.)

Access Control

It is a good practice to restrict access to network devices. Access restrictions are traditionally implemented in networks using authentication, authorization, and accounting (AAA) authentication. This security measure is typically executed, although in many networks too many operators have access to network devices. Restricting this number to the minimum number of operators necessary reduces the risk.

Authorization

Operator access should be restricted to the minimum access needed for them to do their job. In most cases, it is not a good idea for all operators to have full-enable access to devices. This practice can be more difficult to implement; however, simple distinctions, for example, who can and cannot enter configuration mode, can be very effective.

Dual Control

Security control and network control should not be the responsibility of the same group. Ideally, a security group controls who has access to what and a network group executes the configuration actions. Typically the logs are controlled by the security group. This setup makes it much harder to deliberately misconfigure devices, since the security team could recognize a misconfiguration in the log files.

Secure and Verify

All of the above measures are active attempts to detect a change in the network, such as a configuration change. It is also possible to detect policy violations by analyzing the traffic on the network or the state of dynamic information such as routing tables and address resolution protocol (ARP) tables. For example, IDSs can create alerts when flows are seen on the network that do not correspond to the policy. Many other ways exist to monitor for traffic anomalies. For example, Cisco IOS NetFlow can be instrumental in detecting misrouted packets on the network and routing tables can be checked for missing or unknown routing prefixes.

Automation

It is generally recommended to automate processes and procedures, specifically recurring verification processes, because humans tend to overlook details in log files and similar processes. Automated processes are also less prone to errors, although if an error does occur, it is often systematic and therefore easily detectable.

It can be very difficult to implement a comprehensive operational security environment and some measures (such as dual control) can require a certain organizational size to work properly. The goal should be to carry out incremental improvements to the overall operations process. For example, precise command level authorization schemes can be difficult to deploy and expensive to operate in large networks. Other parts of the operations process are much easier to enforce.

Continuous Security Lifecycle

The Risk Management process is not a static event that occurs once and then never again. Continuous Improvement is key to a successful security program, facilitating an ever-improving security profile. It is critical that a regular cycle of security and risk assessments be performed on the PMS, occurring at least annually.

At each review (typically annually although it may occur more frequently due to a specific event such as a discovered attack or a known cyber threat), it is important to consider how risks have changed and what sort of efforts should be undertaken to address those risks.

As part of this continuous program, it is important to acknowledge where you are in light of where you wish to be. It is not practical to attempt to create a new and pervasive security culture when a weak or non-existent one is currently in place. It is critical that you take the time to migrate through the various hardening stages in a logical and incremental manner. For example, you might want to consider initial improvements in password, physical, and email security, evolving into improved access control. Next, add network asset management and improved network security controls such as IDSs, along with enhanced next-generation firewalls. Follow this with other enhancements that include stricter policies, multi-factor authentication, and perhaps smartcards and improved authentication methods. Patch management, both operating system and applications, and virus protection are also tools that improve the security profile of an operations center.

Audits and security assessments are supporting methodologies that help you understand the state of your network and system security, guiding the decision-making process with clearly identified issues that improve security when addressed. Training helps to create a security mindset within the operations center culture, with people becoming an active component in the secure operation of the control system and associated OT environment. Lastly, the members of an organization are also key to the successful implementation of a security culture, with required contributions from the executive level down to an intern. Everyone has a part to play; otherwise, the security program will not be successful.

Training

Employee errors are a common cause of cybersecurity incidents, whether they are due to carelessness or simply not understanding the implications of a particular action. Without regular training to set expectations and explain the consequences of employees' security-related responsibilities and actions, avoidable incidents will continue to happen, potentially enabling a significant cyber event. Up until recently, external threats were seen as the number one cause of security threats; however, from 2017 onwards, this trend has changed with internal extended enterprise threats now being the number one cause[1].

Training is not a one-off activity, but something that occurs regularly. To establish a program, the following approach is a model to consider:

- Develop a training program that clearly outlines the strategic components of your security profile and then transition into the daily activities with which users interact regularly.

  Consider explaining passwords, email scams, and possible phishing attacks, physical security, encryption, and other policies that are directly related to the midstream business.

- Begin the training regimen by holding an introductory class through an online format, with a verification phase at the end. This way, each user can complete training at their own pace, but completion time frames can be enforced. In this training, clearly explain the risks and the user's part in contributing to the security profile of the company.

  This training should be an annual requirement and should be part of the onboarding process for new employees.

- As new policies and processes are implemented, new training sessions should be published and taken by the user community. This ensures that new threats and new or updated policies are always at the top of mind.

  Not all changes require training, but consider a communication process that facilitates information dissemination to the complete user community.

1. https://www.clearswift.com/about-us/pr/press-releases/insider-threat-74-security-incidents-come-extended-enterprise-not-hacking-groups

Training is one component of the overall security communications process. Employees need to be kept aware of threats, new policies, new IT structures, and procedure updates through a defined communication strategy. To reiterate, training and communication are a continuous process, occurring throughout the year, year over year.

Auditing and Compliance

Auditing is the process that is used to verify the current state of your security profile based on pre-established criteria. There are two forms of auditing, internal and external.

- The internal audit process, which is used to assess the current security profile at a given moment in time, is used as a checkpoint along the way to an improved and comprehensive security profile, providing information that is used to guide the decision-making process by assessing where you are and where you want to be. It is also used to prepare a company for external certification audits. It is critical that the resources performing the audit have the proper skills to make valid assessments, because a poor assessment will not move the PMS along the pathway to improved security and it might even create a false sense of security, facilitating a network compromise.
- The external auditing process uses third-party auditors to verify the network and system security profile against a set of requirements, with a formal report generated and provided for the controlling authority. These requirements, as with the internal ones, could be based on an acknowledged industry standard or best practice guidelines, an internally derived set of requirements, or a combination of both. In later sections of this document, we discuss many of the components that would need to be in place and evaluated as part of an audit, including hardening concepts, asset discovery and management, access control, authorization policies, confidentiality, and defensive mechanisms implemented through architecture and system components.

To help form your assessment criteria, the US-CERT has created evaluation level criteria defined as The Common Criteria Evaluation Assurance Levels (EALs)[1]. The higher the level, the more confidence that the functional security requirements have been met. The levels are as follows:

- **EAL1: Functionally Tested**—At this level, certitude in the product's operation is required; however, security threats are not considered important.
- **EAL2: Structurally Tested**—In this stage, the developers, or users, require reasonably self-sufficient security.
- **EAL3: Methodically Tested and Checked**—Users or developers, in this level, apply a moderate level of security to their products and security evaluations.
- **EAL4: Methodically Designed, Tested, and Reviewed**—This level applies when applications are required to have middle to high, independently verified security within standard products and will pay extra for additional efforts to promote improved security if needed.
- **EAL5: Semi-Formally Designed and Tested**—This level applies when applications are required to have a high and independently verified security, implemented and developed through a rigorous security forward development program, leveraging external security specialists as needed to achieve this level of security.
- **EAL6: Semi-Formally Verified Design and Tested**—This level augments the requirements of EAL-5, with the addition of creating specific security criteria for applications in high-risk situations where the return on this investment justifies the additional expense.
- **EAL7: Formally Verified Design and Tested**—This is considered the best evaluation level, whereby the security targets and validation programs are required to be formally tested and confirmed. This formality generates additional costs, but the security risks justify this additional financial impact to the development programs.

This information helps to give your assessment process a level of compliance that is relatively reasonable to achieve. As progress is made in a security program, levels will increase strategically throughout the assessment process, demonstrating improved security along with an improved defensive posture.

Further augmenting the security assessment process are the Security Level designations created as a component of the IEC 62443 standards. There are four Security Levels (SLs), ranging from 1 to 4, with the higher levels engendering higher costs, longer validation, and greater deployment time:

1. https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

- **Security Level 1 (SL1)**—Prevents the unauthorized disclosure of information by eavesdropping or casual exposure.
- **Security Level 2 (SL2)**—Prevents the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation.
- **Security Level 3 (SL3)**—Prevents the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS-specific skills, and high motivation.
- **Security Level 4 (SL4)**—Prevents the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS-specific skills, and high motivation.

As you progress from low to high, you are continually improving the security profile of the control system and surrounding environment. PMSs, as a component of the U.S. Critical Infrastructure, are gaining focus by international actors that are looking at ways to compromise key assets of the U.S. energy infrastructure. It is these concerns that are driving the need for a continuously improving security profile, whereby a comprehensive security life cycle is a strategic component of an overarching security program.

Business Resilience

Business resilience enables the operations center to mitigate disruptions and disasters. The Federal Emergency Management Association (FEMA) has identified four key steps to consider in business continuity[1]:

1. Perform a business impact analysis to identify critical functions and processes.
2. Determine the resources needed to recover critical business functions and processes.
3. Create a business continuity team, followed by the compilation of a business continuity plan.
4. Ensure the business continuity team is properly trained.

Disaster Recovery

A disaster recovery plan is a set of procedures that enables an organization to:

1. Respond to a disaster using a pre-defined identification and recovery plan.
2. By identifying resources to address specific areas ahead of time, operations can quickly evaluate the damage and estimate the time to repair and restart operations.
3. Following the short-term recovery, consider what equipment might be salvaged or that requires further repair to facilitate a sustained recovery.

Mission Continuity

Mission continuity addresses the recovery of a damaged facility or system components by restoring them to normal business operations. Multiple paradigms can be chosen to ensure business continuity:

- Sustain business operations by implementing redundancy and replication that enable failover of operations to a working facility or site.
- Recover and resume business operations by ensuring that valid archives and backups are readily available for immediate restoration.

Business continuity planning protects business assets, including people, reputation, and tangible assets so that in the event of a disaster, operational and commercial data and equipment are protected from environmental damage.

1. https://www.ready.gov/business/implementation/continuity

Project Phase Security Considerations

Introduction

Cybersecurity challenges create business risk caused by threats that exploit the systems, network, and vulnerabilities that exist on the network. The cybersecurity risk of a bad actor compromising an ICS directly affects the reliability of the operations, reputation, financial results, and potentially the safety of employees, vendors, customers, and the general public.

AVEVA and Cisco have extensive experience working with O&G, Energy, and manufacturing customers globally on all aspects of PMSs including their communications networks.

AVEVA and Cisco have cooperated in the creation of Joint Reference Architectures for the Smart Connected Pipeline, which ideally should be used as a starting point for any O&G pipeline project.

However, it is still imperative that the implementation of a PMS has a separate cybersecurity project or stream and that specific attention is given to cybersecurity issues during all phases of the implementation.

Regardless of whether the O&G pipeline project is a “Greenfield” or “Brownfield” project or whether or not the Smart Connected Pipeline Reference Architecture is used as the fundamental approach, a security project has the following phases:

- ICS Cybersecurity Advisory and Consultation Services
- Cybersecurity Risk Assessment
- Risk mitigation
- Cybersecurity Reference Architecture

Note that the Cybersecurity Reference Architecture is specific to the project, as it defines the target Cybersecurity Architecture for the implementation, and should not be confused with the System Reference Architectures for Smart Connected Pipeline systems.

Defining a cybersecurity risk assessment framework, as shown earlier, and then calculating a point-in-time quantitative risk assessment is the foundation upon which to build a security reference architecture that is justified by the line-of-business need. The cybersecurity reference practice then rationalizes investments made in design and implementation of specific technological cybersecurity solutions, as these solutions are the technical controls used to mitigate the business-impacting cybersecurity risks identified in the original assessment.

Several benefits are realized by first developing a reference architecture before developing cybersecurity policies, some of which must align with existing IT policies while ensuring unique OT requirements are met:

- Any newly-created or updated policies are better aligned to the ongoing security strategy.
- Policies are created that are more practical to implement and enforce.
- Such pragmatic policies ease the operational security burden and set a standard for new solutions being implemented.

In an implementation of a PMS, it is also important to address cybersecurity during the various implementation phases of the project to ensure that practices and project phase infrastructure setup do not compromise the security of the system in the longer term. Allowing intrusion through poor cybersecurity practices during implementation would open the door for malware or other vulnerabilities to be introduced. A simple act such as using “standard” known passwords could result in a system being compromised before it is operational.

Overview of Cybersecurity Services

Advisory and Consultation Services

AVEVA's Cybersecurity or Cisco's ICS Cybersecurity Advisory and Consultation service provide a peer to advise and balance the workload of the enterprise-level security architect, or similar role, during strategy, development, or deployment of a new security architecture. During this time of significant changes, the enterprise security architect is intensely involved in:

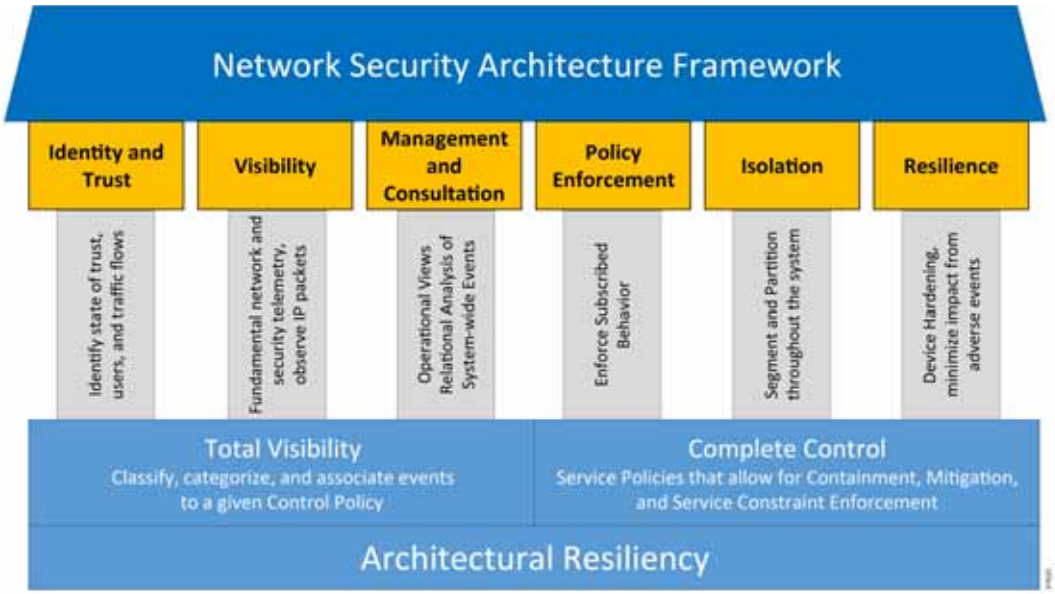
- Ensuring the alignment of the security program and initiatives to business goals
- Defining the security architecture for the computing environment
- Ensuring the security policy is properly designed, implemented, and enforced

To implement any new architecture, you must consider current and new security controls, processes, policies, and the impacts on your security posture by providing controls and visibility across the attack continuum.

Security Architectures

A number of standards and guidelines recommend the creation of a security reference or end state architecture (an example is shown in Figure 18). Both Cisco and Schneider Electric/AVEVA have worked with multiple pipeline owner operators to create these documents. From a guidelines, standards, and practical perspective it is essential to understand there is no "one size fits all" approach and these must be specific to the organization and its requirements.

Figure 18 Network Security Architecture Framework



In constructing a security architecture that reliably and securely connects the relevant communication systems, a number of network-based constructs, security controls, and other security features must be considered in addition to the inherent security features of the devices and their applications.

Cisco's architectural framework (Figure 18) is known as the "Network Security Architecture Framework" and comprises six pillars, which align with the fundamental requirements of a secure network.

Network Security Architecture Framework

The Network Security Architecture Framework is appropriate to use as the basis of any high-level architecture. Some of the features of the security architecture are described below.

Security Architecture Principles

Defense-in-Depth

Never assume that a single control can provide sufficient risk mitigation for a specific threat. Deploy multiple layers of controls to prevent, identify, and delay attacks in order to contain and minimize damage while an organization responds.

Service Availability and Resiliency

Ensure service availability through device hardening and by strengthening the resiliency of the network to adjust to and recover from abnormal circumstances.

Segregation and Modularity

Infrastructure is organized in functional blocks with distinct roles facilitating management, deployment, and securing of the devices and business assets within each block.

Regulatory Compliance and Industry Standards

Follow industry standards and best practices to facilitate the achievement of regulatory compliance. Many security standards are in use today. Specific to the pipeline vertical, these include the ISA-95 Model, ISA99/IEC-62443 Security Framework, NIST 800-82 R2, CSA Z246.1-17, INGAA for Industrial Automation and Control Systems (IACS).

Cybersecurity Service Components

Each component builds upon the previous one to ensure tight cohesion between the business need and the technical solution provided. When founded on a quantitative cybersecurity risk assessment and implemented according to a best practice security reference architecture, cybersecurity solutions can be selected, prioritized, and rationalized against both the business need and the customers existing OT and IT infrastructure strategy.

Should a more tactical approach be desired, the customer may choose to consume any of the latter components individually or in succession without performing a cybersecurity risk assessment. For example, it is understood that comprehensive planning, design, and implementation services are needed to provide an updated firewall solution for the entire OT network and interface with IT network. Should this be the customer's only and most critical cybersecurity concern, as part of comprehensive planning, designing and Implementation, components would be selected to complement the four (4) components. In such cases where cybersecurity services are consumed ad hoc, it is strongly recommended that the customer consider a cybersecurity risk and vulnerability assessment in the not-too-distant future to ensure that implemented technologies are effectively mitigating the highest impacting cybersecurity risks to the environment.

Cybersecurity During the Implementation Project

A typical PMS project consists of a number of phases and the Cybersecurity Reference Architecture for the project needs to be established to address both the issues common to all phases as well as the unique needs of each phase.

Typical phases include Front End Engineering and Design (FEED), Detailed Design, Development (with embedded Testing), Factory (Preliminary) Acceptance Testing, Site Acceptance Testing, Commissioning (including Point-to-Point verification), and then Service and Support.

Front End Engineering and Design

During this Front End Engineering and Design (FEED) phase, which is a common initial project phase, but may not always be a part of an implementation project, information is shared between the pipeline company and vendor(s) on various aspects of the planned PMS, including details of existing systems, existing communications infrastructure and planned infrastructure, and networking. As a result, information that can be used for malicious infiltration is being shared between various external parties.

It is imperative to put measures in place to protect this information (which is not making use of the infrastructure of the planned system and must therefore be applied using infrastructure already in place with the vendor(s) and pipeline company). A cybersecurity project should be launched to ensure that these measures are defined and executed.

Measures would include, for example:

- Dictating a policy where no files containing IP addresses, passwords, system names, domain names, etc. should be shared in the clear.
- Locking down access so that information stored in corporate systems at the vendor(s) or pipeline company should be accessible to only the appropriate parties within the organizations. (This prevents both intentional as well as unintentional leakage of information, which could be used to compromise the system at any stage of the project).
- If Test and Development systems are used for the FEED to test aspects of the design, the systems used in the FEED must be treated as a Production system (they are typically treated as test systems today, meaning they may not receive the same level of security consideration) to both remove the possibility of any contamination of the final system from the FEED system, but to also ensure that opportunities for later exploitation are not being created.

Detailed Design

During the detail design phase, the specific details of implementation are discussed (if there was no FEED phase, the scope would be large). Generally, the vendor(s) and interested parties in the pipeline company would be preparing for installation of the system, or at least, the test and development systems.

The threats and concerns during this phase are relatively the same as for a FEED, although generally the issues are magnified as more parties become involved. In short, these early phases are about securing the sharing of information so that sensitive information for either the current or planned system is not exposed to potential malicious actors or unintentionally facilitating data leakage.

Installation

Before the installation of the project infrastructure, prior to SAT, the Cybersecurity Reference Architecture must be finalized to ensure that the installation implements the Cybersecurity Reference Architecture to the extent agreed upon from the outset. Typical concerns that need to be addressed include:

- Disallowing “standard” password use for internal systems when implementing any aspect of the system (whether the Test and Development Environment, Decision Support, or Production environments). Where default user names are used, it is particularly important to make sure the passwords are unique to every system: generated passwords should be the norm.
- When implementing the systems using virtualized technology at a vendor location, it is important that all Domain Controller (DC) VMs (after the domain is created) generated for the project are used once and only once for that customer and not on multiple projects to provide cross project exploits.
- When the system is installed at the vendor prior to being shipped to the pipeline company facility, issues such as physical access to the system in the staging area should be strictly controlled to prevent infected media inadvertently being attached to the system.
- All media attached to the system must be scanned for virus and malware before being connected to the system.

- If the system is installed at one of the pipeline company's facilities, the same concerns regarding facility security and media apply.
- Where remote access to the system is available, whether at the vendor's facility or the pipeline company, this must be done through security appliances with individual user logins (with minimal privilege) for each user.
- The entire staged system should be isolated from the vendor's corporate network, ensuring that no unauthorized users may access the controlled project network and systems therein.

Development—With Embedded Testing

During this phase, both development of software and development of displays (Human-Machine Interface or HMI), configuration of points used for SCADA, as well as other configuration of applications and the SCADA platform itself can occur. Repeated updates of the environments with new software, configurations, and displays during the development phase will potentially occur.

During this phase, the system may be at the vendor(s) premises with the development performed in the environments of the system or at systems external to the project development network. In addition, testing will in all likelihood be performed within the system to ensure that the system is ready for Factory Acceptance Testing (FAT) or Preliminary Acceptance Testing (PAT).

A key concern would be access or authorization bypasses that are implemented to make it simpler to perform development and testing—for example, installation of additional (temporary) software and users to allow additional users to develop on or test the system simultaneously. The Cybersecurity plan should explicitly discourage these installations and users. If additional software is installed or new users are added, the plan should ensure that such installations are approached with the same rigor as the installation of the system for delivery, and have a clear plan for the removal of any and all additional users and/or software installations created for development and testing after testing is completed.

Factory (Preliminary) Acceptance Testing

The FAT phase (when on vendor's premises) or PAT phase (when at the Pipeline company's premises) is a phase in the project where the software, configuration, displays, and other applications are tested, including third-party interfaces to the system.

Concerns that need to be addressed are similar to those for the development phase, with the additional concerns of interfaces to corporate and third-party systems. For example, tests may be conducted against data sources such as weather interfaces, corporate scheduling systems, and so on, requiring a clear plan on securing the interfaces and data exchanges such that the attack surface is not increased.

The system must be treated as a production system to ensure the validity of the results as well as protecting the system from being exposed to potential vulnerabilities. To address this risk it is recommended that a security audit be conducted prior to shipment.

Site Acceptance Testing

During Site Acceptance Testing (SAT) the system under test is validated within the exact environment in which it will be executing once in production. This may include connecting to the actual field for testing or enabling data feeds from third-parties or listening in on an existing system, if one exists.

Specific concerns include having adverse effects on existing systems, including the cybersecurity aspects, since vulnerabilities in the newly introduced infrastructure can unintentionally bring vulnerabilities into the existing (production) systems. Careful planning and diligence must be applied to prevent this. For example, test accounts may still be available for project team members to access the system to make corrections, set up tests, or complete configuration in order to prepare for the test, requiring a plan for their controlled removal prior to final system activation.

As with FAT, the system must be treated as a production system to ensure the validity of the results as well as protect the system from exposing the production environment to vulnerabilities or from being exploited prior to startup. As part of the finalization process, a final security audit should be carried out.

Commissioning—Including Point-to-Point Verification

Commissioning leading to cut-over is a phase in which the system is tested to ensure that all functionality is working and the new system is transitioned to replace an existing system, if one exists.

A critical part of this phase is ensuring that displays (HMI) and devices are in synchronization using point-to-point testing. This requires coordination between central control personnel and field personnel. Any and all changes made to the system must be done through a Management of Change process to ensure that the system, configuration, and remote access are tightly controlled. All test accounts must have been removed and product processes with regards to password policies, user access, and role enforcement must be present and active.

The system is now, for all purposes, ready for cutover after this phase.

Service and Support

Once the system is in production (i.e., is cut-over and becomes the PMS of record), the system will be administered through Management of Change processes to ensure that a clear record and accountability for display, configuration, and system changes, including user and privilege management, exists. This also extends to the installation of patches, OS upgrades, virus management, and other IT-related activities. The new PMS is also part of the overall customer's corporate IT environment and, although typically isolated, it often is managed in conjunction with the IT staff, conforming to a combined OT and IT security and IT policy if the client has one. If not, one should be created to address this.

Specific concerns during this phase are ensuring that remote access and any remote user accounts used by the vendor(s) for the purpose of remote support access, are tightly controlled.

Project Team Communications

Throughout the lifetime of a project of this complexity, communications, both electronic and paper, share potentially sensitive and compromising details about the PMS, requiring additional considerations related to security. For example, the proper disposal of paper records must be implemented (e.g., a lockbox for secure shredding). Encryption of sensitive data should be mandatory when transmitted electronically or when stored. Consider that a laptop used by the project manager, if lost or compromised, could expose sensitive data. Therefore, team members should encrypt data stored on their local systems to prevent unauthorized access. Lastly, electronic records for a project need to be prepared for long-term storage. Records of individual team members should be reviewed and expunged of sensitive data no longer required as part of their project responsibilities. Long-term storage should be prepared, with proper access controls implemented to ensure that unauthorized access is not granted.

Arguably, one of the weakest areas in a cybersecurity program centers around the long-term storage and disposal of electronic records. Both the vendor and customer need to cooperatively share the responsibility of securing electronic and hardcopy communications following the completion of the project.

Customer Maturity, Risk, and Best Practices

Maturity, Risk, and Best Practices Defined

A growing number of regulatory directives aimed at critical infrastructure security, combined with uncertainty about how they might affect the business, are creating an urgent need for stronger cybersecurity in ICSs and their associated OTs. A key driver behind these concerns is the recent ICS-CERT report that found:

> According to the US Department of Homeland Security, within the ICS-CERT year in review report[1], that out of the 290 incidents that the ICS-CERT response team completed work on, 59 impacted the Energy Sector, approximately 23%!

With statistics such as this, pipeline operators need to determine how they may assess their current cybersecurity posture, determine the most important risks, and use this information to drive programs that move the organization along an ever-maturing pathway to an improved cybersecurity profile.

- **Maturity** is a term used to define how far along industry recognized standards an organization is with regards their OT cybersecurity profiles.
- **Risk** defines those things that could adversely impact the system through cyber vulnerabilities that are then exploited by malicious actors. These are not always technology related, but can be process, policies, or people. When determining and evaluating risk, it is important to consider a broad spectrum of activities and potential vulnerabilities and align them with the probability of them happening along with what type of actor may exploit.

Best practices are those activities that help a pipeline operator to address their risks, improve their maturity, and develop a continuously improving cybersecurity strategy and profile.

What We are Trying to Solve

In earlier sections, we introduced many concepts, highlighting the complexity and many facets that compose a cybersecurity profile for a PMS. In this section, we provide the context that a user must consider in order to determine where they are on their cybersecurity journey, where they wish to be, and what steps they should take to get there.

The topics highlighted in this section provide the framework for which a pipeline operator should consider establishing to track and guide their overall cybersecurity journey; and recognizing that last word—journey—is critical to this discussion. It is important to acknowledge that an organization does not move from the most basic cybersecurity profile to a highly mature posture overnight. It takes time to build a knowledgeable staff, perform the initial evaluations that defines your starting point, perform an initial risk assessment, develop a multi-phase program to address the risks, harden the system, and establish a continuous program to cyclically review and improve the PMS's security posture.

Maturity Level

Security Maturity Levels

Maturity, in this context, is an objective means of assessing where your cybersecurity program is in relation to recommended best practices and implemented process, procedures, and technology. One way to help an organization assess their maturity is to use an independent scale and perform an internal audit to provide a baseline of their current cybersecurity maturity level. The NIST Computer Security Resource Center (CSRC), as part of their recommended Program Review for Information Security Assistance (PRISMA), provides the following IT Security Maturity Levels[2]:

1. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf
2. https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels

Level 1—Policies

- Formal, up-to-date documented policies stated as “shall” or “will” statements exist and are readily available to employees.
- Policies establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness.
- Policies written to cover all major facilities and operations agency-wide or for a specific asset.
- Policies are approved by key affected parties.
- Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance.
- Policies identify specific penalties and disciplinary actions to be used if the policy is not followed.

Level 2—Procedures

- Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies.
- Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed.
- Procedures clearly define IT security responsibilities and expected behaviors for:
  - asset owners and users
  - information resources management and data processing personnel, management, and
  - IT security administrators.
- Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance.
- Procedures document the implementation of and the rigor in which the control is applied.

Level 3—Implementation

- Procedures are communicated to individuals who are required to follow them.
- IT security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training.
- Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged.
- Policies are approved by key affected parties.
- Initial testing is performed to ensure controls are operating as intended.

Level 4—Test

- Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations.
- Tests ensure that all policies, procedures, and controls are acting as intended and that they ensure the appropriate IT security level.
- Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual IT security incidents or through IT security alerts issued by FedCIRC, vendors, and other trusted sources.

- Self-assessments, a type of test that can be performed by agency staff, by contractors, or others engaged by agency management, are routinely conducted to evaluate the adequacy and effectiveness of all implementations.
- Independent audits such as those arranged by the General Accounting Office (GAO) or an agency Inspector General (IG) are an important check on agency performance, but are not viewed as a substitute for evaluations initiated by agency management.
- Information gleaned from records of potential and actual IT security incidents and from security alerts, such as those issued by software vendors are considered as test results. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk.
- Vulnerabilities and provide insights into the latest threats and resulting risk. Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented.
- The frequency and rigor with which individual controls are tested depends on the risks that are posed if the controls are not operating effectively.

Level 5—Integration

- Effective implementation of IT security controls is second nature.
- Policies, procedures, implementations, and tests are continually reviewed and improvements are made.
- A comprehensive IT security program is an integral part of the culture.
- Decision-making is based on cost, risk, and mission impact.
- The consideration of IT security is pervasive in the culture.
- There is an active enterprise-wide IT security program that achieves cost-effective IT security.
- IT security is an integrated practice.
- Security vulnerabilities are understood and managed.
- Threats are continually reevaluated and controls adapted to changing IT security environment.
- Additional or more cost-effective IT security alternatives are identified as the need arises.
- Costs and benefits of IT security are measured as precisely as practicable.
- Status metrics for the IT security program are established and met.

Maturity Level Evaluation

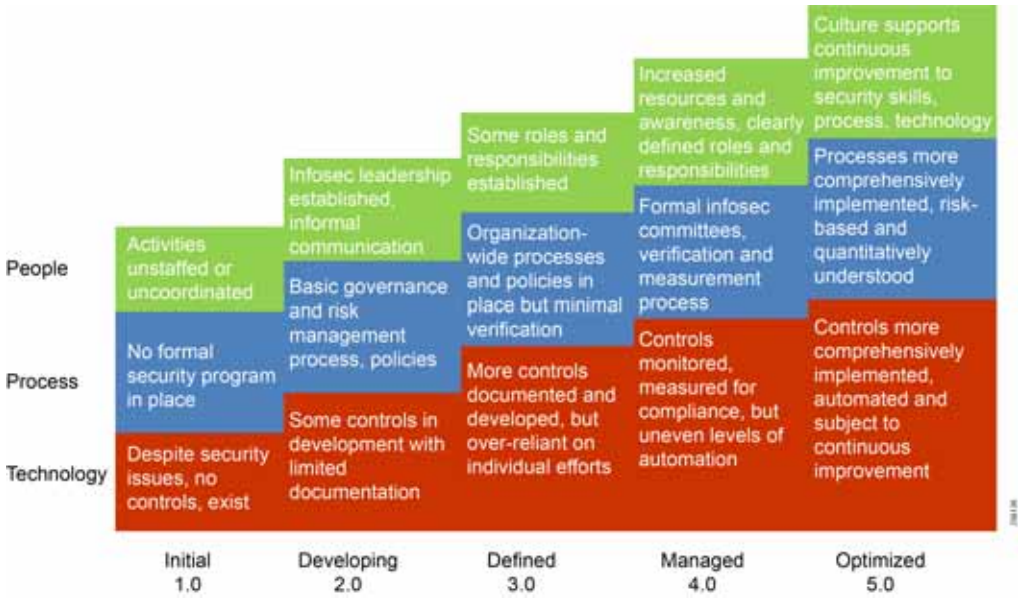
A Maturity Level Evaluation (MLE) is a high level preliminary evaluation of a PMS's security posture based on an assessment against a standard maturity model. The MLE aids in the scope and focus of the assessment activities, assisting system owners as to what is needed to increase their maturity level. The following suggested steps can help lead one through an MLE process:

- **Establish the Baseline**—Take a comprehensive inventory of all assets. Design defenses based on the premise that a successful attack is inevitable. Defensive capabilities are required before, during, and after an attack.
- **Achieve Visibility (and Control, if possible)**—Ensure visibility of the assets, protocols, users, applications, and traffic patterns on the control network to develop a picture of what is "normal" for that environment. This can be done without disrupting real-time communications or increasing loads on sensitive OT devices.
- **Implement Controls and Automation**—Prioritize assets and systems based upon their value to maintaining operations and build out defenses for the critical assets and systems first. Implement a combination of IT security and ICS/OT security to limit the attack surface and attack window as much as possible. Since security is a lifestyle, firms should identify tasks that are tedious, error prone, and repetitive and look to deploy automation in these instances in order to minimize the risk of human error.

- **Strive for Continuous Improvement**—Regularly test, review, and update defenses and policies through automation. Being "secure" is temporal, as threats and attack techniques constantly evolve. Therefore, defenses should be regularly tested and modified, as needed, and as just one component of comprehensive cybersecurity program.

An example is shown in Figure 19.

Figure 19 Example Maturity Level Evaluation[1]



Risk

For risk maturity, management needs to develop a governance structure that allows it to think about risk proactively and align its risk profile and exposures more closely with its strategy. Its governance leadership group and supporting management should clarify the company's risk appetite, define its risk universe, determine how to measure risk, and identify which technologies could best help the company manage its risks. Aligning risk to strategy by identifying strategic risks and embedding risk management principles into business unit planning cycles enables the company to identify and document 80% of the risks that have an impact on performance. The payback on this effort is multifaceted. Surveying risk so thoroughly gives the company the confidence to openly communicate its risk strategy to external stakeholders without worrying that the transparency would shake investor confidence. Most importantly, the alignment of risk awareness and management practices from strategy to business operations enables the company to monitor risk developments more effectively. Managers could keep the organization within acceptable tolerance ranges, driving performance to plan. Mature risk management allows companies to improve their financial performance, strengthen stakeholder communication, and build greater trust in the market[2].

An effective end-to-end cybersecurity approach delivers many advantages, including increased business agility and risk awareness, lower cost of operations, and reduced downtime. These translate into tangible economic benefits. However, to secure, harden, and defend a PMS in the world of the Internet of Things (IoT), one must truly understand IoT at its core. In the era of IoT, everything is connected, therefore determining the best protection methodology for the type of systems, data, and communication pathways that compose the PMS is a challenge. Assets are to be protected, but their information is needed to manage and improve operations; therefore, it must be accessible while being acknowledged as a possible attack vector that must also be protected. It is a balancing act that occurs throughout the entire PMS, from field to control center to corporate. This introduces the junction where the IT and OT worlds become conjoined and must fight together, acknowledging the unique demands of each sphere of influence.

1. https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/
2. https://hbr.org/2012/06/how-mature-is-your-risk-manage

Best Practices

This document covers a number of key cybersecurity standards that are applicable to oil and gas pipelines. However, a wealth of options are available. Using the US as an example, NIST has developed the Framework for Improving Critical Infrastructure Cybersecurity, which is a set of standards and best practices to assist organizations in managing cybersecurity risks and promoting the protection of critical infrastructure. To implement an effective cybersecurity strategy, pipeline operators should consider the approach outlined in the NIST Framework and the guidance issued by DHS and the Department of Energy, along with industry-specific or other established methodologies, standards, and best practices.

The following is a list of planning and implementation guidance developed by various industry or Federal government entities. Operators should consult the current edition of these and other cybersecurity references on a frequent basis while developing and reviewing their company's cybersecurity program.

- American Chemistry Council, Guidance for Addressing Cyber Security in the Chemical Industry
- American Gas Association (AGA) Report Number 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan
- American National Standards Institute (ANSI) and International Society of Automation (ISA) -99.00.01 - 2007, Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models
- ANSI and ISA - 99.02.01 - 2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control System Security Program
- American Petroleum Institute (API) Standard 1164 Pipeline SCADA Security
- ANSI and API Standard 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries
- U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
- U.S. Department of Commerce, NIST, Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security
- U.S. Department of Homeland Security, Office of Infrastructure Protection, Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards, May 2009
- U.S Department of Energy, Office of Electricity Delivery and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance, January 2015
- U.S Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance, June 2015

Throughout the standards and guidelines, consistent security mitigation techniques are designed to support the key pipeline requirements for availability, reliability, and safety. This can only be achieved through a properly architected, tested, and validated solution.

The Smart Connected Pipeline reference architecture and validated design mentioned earlier in this document is an example of an open, end-to-end solution for pipeline management that provides future-ready secure communication architectures for integrated, automated pipeline operations through the use of modern IT technologies.

Summary

These previous four sections provided the background to this document and the approach pipeline companies should consider as part of their security program and posture. The following thirteen sections dive deeper into the security mitigation techniques that are consistent among the most well-known standards and guidelines and provide practical recommendations for best practice.

Asset Discovery and Inventory

Asset Discovery and Inventory Defined

At its simplest, asset discovery and inventory is the capture and identification of the components of the PMS to be secured. An additional step is to identify the component relationships and security needs, for example, the current security state and risk profile.

This activity is necessary since securing an environment is most efficiently achieved when the things to be secured are known. This section discusses topics relevant to the process of discovery and inventory:

- Discovery is the capture of PMS components and their attributes.
- Inventory is the aggregation and classification of what was discovered.

With an inventory of discovered components in place, management and security policy can then be applied with greater effectiveness.

What We are Trying to Solve

Understanding the connected pipeline elements enhances the ability to protect them along with the broader system.

Distributed systems, such as pipelines and electric utilities, have had sophisticated attacks applied to components that defenders had never considered as valuable to the overall system. In the 2015 attack on the Ukrainian electric utility, the attackers initiated a telephone Denial of Service (DoS) against the outage reporting phone number, thus disabling the utility from finding the range of customers impacted. While this was not an operating component of the electrical distribution system, it was a valuable, parallel input to understand the operation of the system from a customer perspective. It is reasonable to think that it was, in fact, the most relevant feedback mechanism, particularly if you had to prioritize efforts for response. Several US gas pipelines were affected after a cyber-attack targeted a third-party supplier that supplies electronic data interchange (EDI) services. The computer-to-computer exchange of documents at the third-party allows providers to do business with their customers. This affected a number of pipeline customer operations.

The need to discover and inventory the participants within a system is referenced in multiple standards and best practices. These needs and standards span both informational and operational technology spaces. Examples of such standards referencing asset discovery are: NIST Guide to Industrial Control Systems (ICS) Security; and the US Transportation Safety Administration's Pipeline Security Guidelines.

Policy-driven protections are incomplete when knowledge of the scope of risks and threats is limited. Understanding the range of pipeline components and those who work on them and their associated risks enables a more complete mitigation policy. Completeness may not be your immediate need. What if an incident triggered this process? Consider the scope and timeliness of your need when initiating discovery and inventory.

Asset Discovery and Inventory Process

Having a process with flexibility to be applicable to PMSs at different stages of maturity, under multiple forms of managerial and regulatory oversight, is key to success. Conditions, such as the vendors providing automation equipment or sub-contractors performing identical tasks in different locations, may vary, therefore a flexible approach is important. The following are some questions and tasks on which to focus.

Visibility into the Pipeline Inventory

If it represents a security risk that we can address, then it needs to be accounted for in our pipeline inventory. Even items that do not represent obvious risks are worth noting because what looks innocuous to you may represent to another an opportunity for mischief.

The most commonly referenced class of inventory objects are network connected devices. The devices may work directly or indirectly on specific needs such as RTUs, PLCs, motors, sensors, and valves. The devices may be generic equipment, such as a generic computer or wireless access point, that supports pipeline equipment communication or other ancillary roles.

While software may be independent of a specific piece of equipment (its physical presence could be virtualized or relatively independent of a specific hardware host), its participation can still be critical. However, if software is deployed, it is a risk that needs to be addressed.

System users and participants qualify as “things” that need to be known. Management of system users is an important component of the inventory population.

In the discovery of the higher order systems, it should not be assumed that the systems will be interconnected by a common network. Some may be wholly separate yet remain vital to the system’s operation. One set of devices, software, and users may be unable to communicate directly with other devices, software, and users of another subsystem.

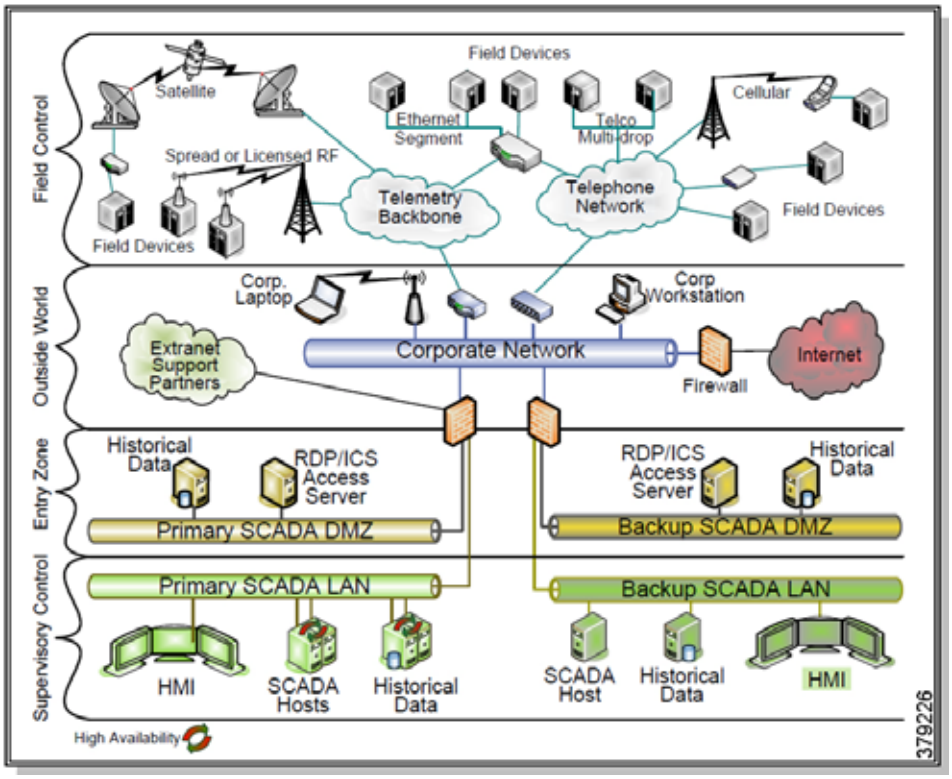
Numerous overlapping best practices and standards exist that are applicable to pipeline operation. Terms and references do not always use identical terms or focus on the same scope. For the purposes of this section and the desire to be inclusive, multiple standards are referenced.

The American Petroleum Institute’s Pipeline SCADA Security Guide (API Standard 1164) is wholly focused on the SCADA components and therefore limits its realm of focus to that class of devices and their supporting infrastructure. The standard, which goes beyond the act of discovery and inventory maintenance, suggests derivative attributes be associated with inventoried items to reflect their criticality as well as risk.

The North American 2018 pipeline shutdown, when a breach was discovered in an electronic document interchange between suppliers, transmission, and distribution entities, provides a valuable lesson. While no actual control systems were touched, the lack of a viable EDI system caused the delivery of goods to stop. So external third-party systems are a type of asset/participant system that needs to be considered even if it is beyond the operator’s direct control.

Pipeline Security Guidelines[1] describes a reference architecture that comprises the following broad areas: Field Control; Entry Zone; Supervisory Control; and Outside World, as shown in Figure 20.

Figure 20 Pipeline Architecture Domains Overview

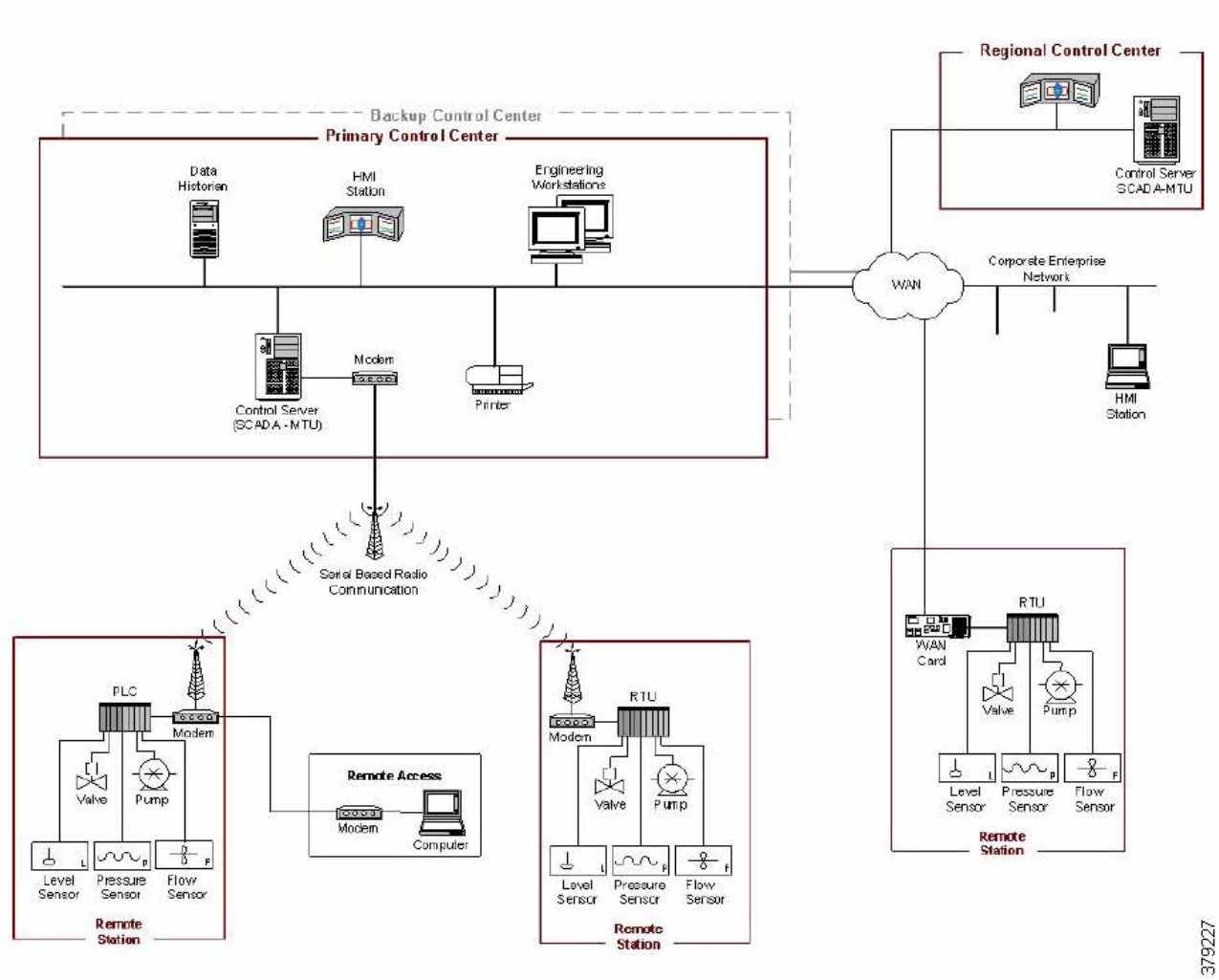


The US Transportation Security Administration's Pipeline Security Guidelines places the scope of applicability based on its criticality to the pipeline system. Risk Assessment Approach and Methodology, page 62 explicitly notes that the range of assets to be identified and classified according to their criticality to “safety and/or reliability.” What the standard does not do is to provide guidance on where to search for these assets. This lack of specificity provides flexibility and ambiguity.

1. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

Another representation of a remote industrial design can be found in NIST's Guide to Industrial Control Systems (ICS) Security. Their representation (Figure 21) is less detailed but shows a different communication structure as regards the field elements and the rest of the control environment. Clearly, the general business network is segregated from all field type elements.

Figure 21 NIST's Guide to Industrial Control Systems High Level Architecture



Mechanics of Discovery

The discovery and inventory process is a constant and ongoing activity. There is no "finished" as long as any change to the devices, software, or users is possible. Even when you may not believe it is possible, unintended or unknown changes justify a constant re-evaluation of the environment. As such, consider this the initial instance of a recurring activity. It is important to perform discovery not only to keep what is thought to be known up to date, but to confirm that unexpected or rogue devices have not appeared on the network.

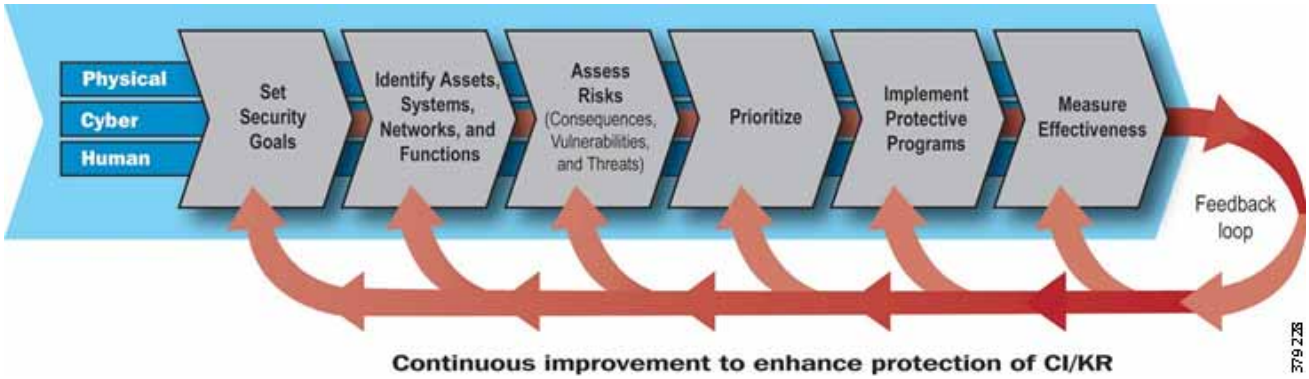
This subsection discusses discovery and inventory as discrete items with a clear relationship to the other.

Discovery is the first step to understanding the assets we wish to protect. It does not necessarily mean that the actors involved in creating the desired inventory are starting with a collection of assets without those assets included in some form of inventory. It is likely that inventories of assets within the scope of this work already exist. In short, this is as much a validation of existing inventory information as it is a confirmation that the network exists physically, according to the network architecture plan.

Table 2 Department of Homeland Defense–Continuous Diagnostics and Mitigation

CDM–Phase 1	CDM–Phase 2	CDM–Phase 3
Asset Control –What is the state of the endpoints I must secure?	Manage People and Services–Who can do what?	Process Planning–What to do and how do we improve?

Figure 22 National Infrastructure Protection Plan Risk Management Framework



The discovery process, as noted in the prior section, begins with people. A list of individuals and groups with responsibilities for the PMS must be created and recorded. That group should define the scope of the PMS, which is the focus of this exercise. The desired depth of organizational control and additional individuals is then defined. With the correct breadth and depth of participants, the next step is to identify existing inventory systems and artifacts.

Management systems with pipeline operation or infrastructure control, i.e., SCADA, are the highest value sources for inventory discovery. If the management systems are believed to be operationally valuable, then they must have control over known assets on which the pipeline depends. Often, operations control systems have separate asset inventory components. The operation's control tools should reference the inventory subsystems and systems. This implies that the discovery process has a manual component, along with technological approaches that aid the discovery process.

For our pipeline, we focus on the Schneider OASyS DNA Enterprise SCADA for Pipelines. OASyS, as is true of most SCADA systems, provides an extensive configuration database that may be used to identify the many operational devices along with the type of interface used and location. Additionally, information contained in displays can augment the research process. By analyzing data flows and user credentials, it is also possible to draw correlations to who, why and from where data is being accessed, further contributing to the overall asset inventory process. Asset Management systems may be associated with the control system that will also provide corroborating information to the configuration data within the system. Through analysis of configuration, data flow, and human input, a comprehensive control asset landscape can be created.

Parallel management systems that may be deemed as relevant to the scope of this exercise need to be included. In some environments, physical security systems are not directly associated with the operational systems. Safety Instrumentation Systems (SIS) may also be purposely parallel and not directly connected. Both, however, should have asset listings that are monitored and operated on.

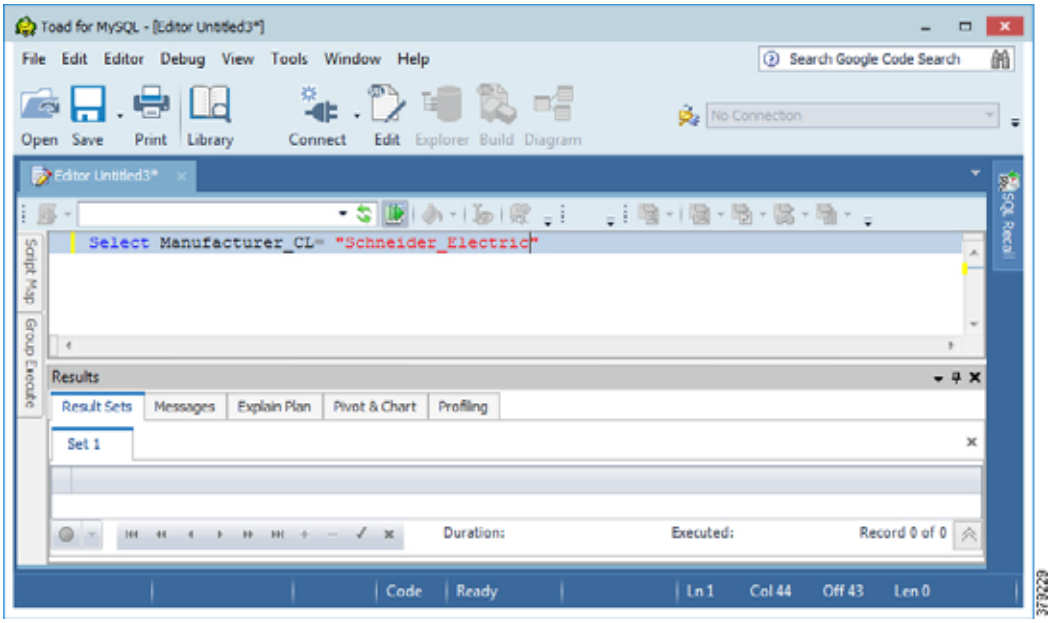
The next level of systems to be assessed is those that act as supporting infrastructure, but are not necessarily explicitly or uniquely designed for pipeline operation. The difference as to whether it is inherent in pipeline management or not is an arbitrary decision. The value to the systems operation is not diminished if one decides to think of it as supporting infrastructure rather than a pipeline explicit function. One class of functions that may be considered infrastructure are communications systems. Based on recent cyber attacks, it is important that the complete attack surface be evaluated, even if it is not specifically control system related.

Be sure to consider any part of an ICS that has communications with other components within their respective zones of a security-segmented architecture. Communication elements also exist that tie those zones to other zones and systems higher in the network architecture. For purposes of a simplified reference, we call communications that exit a station *telecommunications* and intra-station communications *local communications*. While technologies involved in the respective communication chains differ sometimes, these pieces are usually managed by network management tools. Network management tools, such as SolarWinds or Cisco Prime or Cisco DNA Center, are important sources of inventory information. Further, those network management tools may also present opportunities to determine the end-points that they monitor in order to populate the pipeline-specific pieces.

Operational support assets such as voice, CCTV/video, wireless, and PAGA are used to support the operations of the pipeline and the employees, but are not mission-critical applications and should not affect operational applications and processes. These may be independent systems that should be considered for inventory inclusion. Older systems may be based on internal PBX architectures or even local dial up lines (POTS). If so, their management and inventories are separate from the network in general. In newer deployments, voice communication may be video over IP (VOIP) based. In this case, the VOIP-specific equipment is simply additional network end-points to inventory and manage, with the infrastructure largely shared with the rest of the telecommunications infrastructure.

The PMS includes what appears to be a typical IT set of technological assets with operationally-focused applications. As with the telecommunications asset groupings, many of the existing management tools have standard inventory pieces. However, some additional specializations may exist.

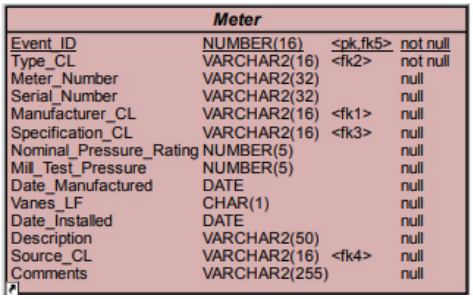
Let us look at a historian as an example. Historians and inventories themselves are typically built on COTS databases. These relational databases, in turn, have supporting tools that have the ability to manage and manipulate their operation and content. The number of tools in these IT-like environments are likely to be less proprietary and numerous. For example, the number of tools that can interact with a MS SQL Server or MySQL database would number in the dozens, while the tools that work directly with a flow meter would be far less. These tools are less likely to contain inventories of pipeline specific elements, but they are a good source for discovering the potential propagation of operational data for other security uses. For that reason, they are worthy of investigation with database query tools. You can cull that data for asset information that, in turn, can be placed into the broader asset inventory being constructed.



The second class of inventories to reference are non-dynamic documents that describe the systems. These can come in many forms, but we will focus on just a few. An original engineering design with a bill of material provides a good initial snapshot on the component assets and their connectivity. Such artifacts are valuable for potentially identifying assets that are no longer active or are invisible to the management tools higher in the system control tree for whatever reason. Another location may be follow-up purchases or change orders, which may be either electronic or paper based. If your organization undertook or underwent a formal audit, then additional details may be available in there. Network diagrams are another common example of this. All of these may represent snapshots in time that show the evolution of the system being studied.

A third class of inventories are those in their operators' knowledge that have not been formally documented. By engaging the people working on the system, we learn what the workers associated with the system know of what they believe is present at the locations and their relationship to the environment.

With the set of electronic repositories discovered above, the next step is to combine their contents with the goal of a unified view of the PMS's assets. The challenge in this case is to normalize the data and find a suitable common structure, location, and relationship. The amalgamation of diverse data sources into a common form and repository is a well-known challenge in the IT and OT worlds. For the sake of brevity, we leave that exercise to the respective teams involved by whatever means they select to do so. Such data models have been in place in the IT world since the last century. Most notably the Web-Based Enterprise Management (WBEM) Common Information Model (CIM) models and numerous operational groups have used the CIM model to great success. In pipelines, one such model is Pipeline Open Data Standards (PODS); this inherently relational model represents critical elements in a standard fashion. One example would be a meter in this object schema, as seen below.



Meter			
Event_ID	NUMBER(16)	<pk,fk5>	not null
Type_CL	VARCHAR2(16)	<fk2>	not null
Meter_Number	VARCHAR2(32)		null
Serial_Number	VARCHAR2(32)		null
Manufacturer_CL	VARCHAR2(16)	<fk1>	null
Specification_CL	VARCHAR2(16)	<fk3>	null
Nominal_Pressure_Rating	NUMBER(5)		null
Mill_Test_Pressure	NUMBER(5)		null
Date_Manufactured	DATE		null
Vanes_LF	CHAR(1)		null
Date_Installed	DATE		null
Description	VARCHAR2(50)		null
Source_CL	VARCHAR2(16)	<fk4>	null
Comments	VARCHAR2(255)		null

379230

It may be helpful to be able to align with some set of known data model, if possible. Some control system asset models can be referenced and clear, well documented models for information technology systems do exist.

Understanding the relationship between the discovered assets influences further discovery activities and incident investigation and helps create a more comprehensive security policy. The relationship is preferably defined explicitly in discoverable attributes, but often it must be inferred from other attributes such as the non-dynamic documents mentioned earlier. Some attributes that define relationships are physical locations, locations within the network topology, similarity in function, vendor affiliation, technology type, known combinations within a functional area.

Automating the Discovery Process

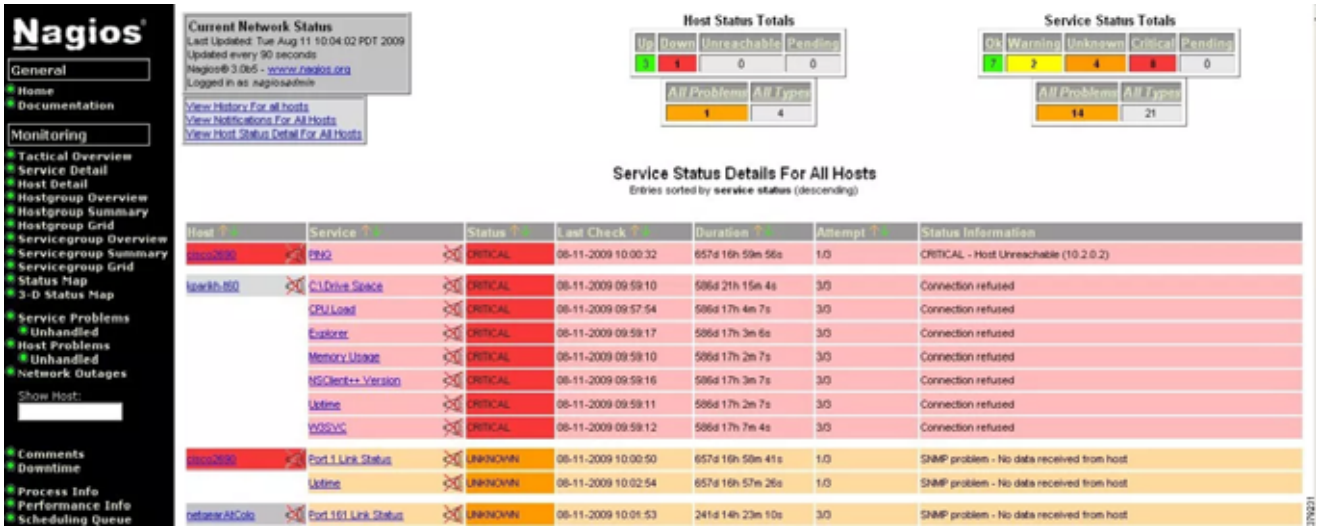
System-based discovery is the process whereby a set of tools is used to automatically discover assets in the system. This discovery process may be active or passive. Both active and passive means have their advantages and they can be used together to capture a timely and complete understanding of the assets of interest. To clarify:

- Active means using a tool that is perusing the network proactively, such as exploring all IP addresses across a specified range through pings or other probing technologies.
- Passive means that the tool is monitoring the network in a monitoring and listening mode and analyzing the visible traffic to determine what systems are speaking and to whom they are speaking.

Some operational technologists will express some concern with the idea of active asset discovery. Stories of network scans negatively affecting operational systems are common. Like all processes, potential dangers exist in their use if not done with the sensitivity appropriate to the environment that they target. When done with care, active asset discovery can be done safely and effectively, providing unparalleled levels of visibility into what comprises the pipeline system and who talks to whom, when, and how.

Most operations automation management tools have a discovery function. Those same tools, which we originally discussed as identifying existing sources of assets, should be your first option for active discovery. Some tools are driven by manual scan options, while others may offer scheduled discovery processes. Among active discovery actions, use of the native management tools is least likely to elicit concern from the operations teams.

The technologies of some classes of assets are composed of traditional IT technologies. For those assets, traditional IT tools are optimal, with many available, depending on the types of IT assets one wishes to discover. As an example, if you wish to find computational endpoints such as a workstation or a server, you might look at directory services or an authentication server such as RADIUS for the MAC and IP address of devices that were authenticated onto the network. If you were seeking to identify network infrastructure within the IT and OT space, then specialized protocols such as Cisco Discovery Protocol (CDP) could be used to find Cisco switches, routers, and firewalls. Free tools that perform an admirable job in this area exist if you choose not to utilize commercial offerings.



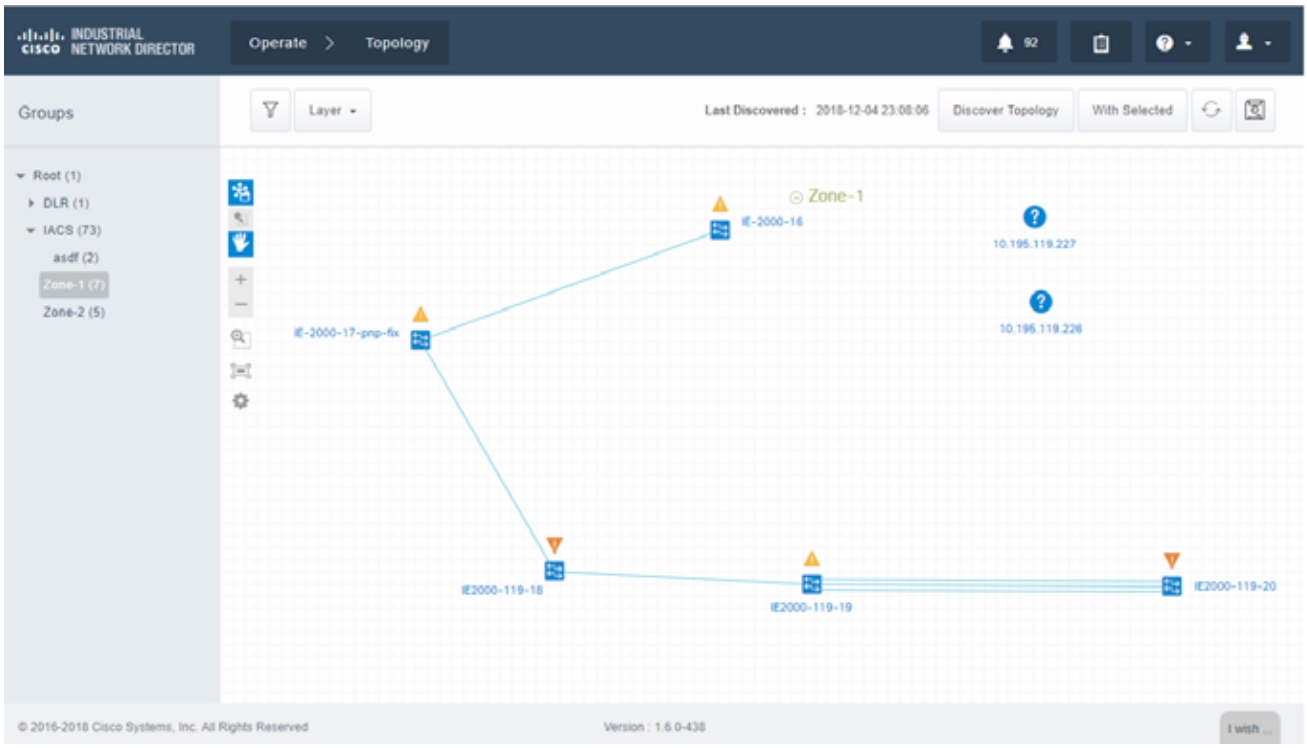
Within non-IT technology spaces, active discovery outside the use of traditional OT tools must be done carefully. A valuable step in this process is to consider what has already been found through the prior discovery and inventory activity. Finding clusters of automation technologies within network subnets suggests associations that should be confirmed through interviews with responsible workers. Taking what is known or suspected about likely assets within the subnet, the decision can be made whether it is worth the potential risk for active scanning of assets. If active scanning is determined as an option to be undertaken, it is imperative that pipeline operations be consulted in order to reduce the risk that operations may be negatively affected.

What you plan to do with the asset inventory from a security perspective should influence your discovery process. If the goal is to create an access control policy using your IP-based assets, then no need exists to find and discover non-IP-based assets. As such, active scans pursuing serial connected systems are unnecessary and a minimum amount of IP-based capabilities in the asset set can be assumed.

Port scans with the Nmap utility, which are a very common step for IT discovery, has a very rich set of options that can automate the discovery process and drive either greater or lesser amounts of asset attribute discovery. Other tools exist that can also augment Nmap with additional details on ICS and SCADA. Care must be taken with its use; however, it is important that the options that create the least amount of impact are selected. Consider the following if you gain acceptance to perform port scanning:

- First understand the need to slow down your scans. Older OT endpoints may have a low limit to the number of connection attempts that they can handle in a given time period. If using Nmap, try the scan-delay option to reduce the ports being scanned to one at a time for each target. Further time-sensitive settings to consider would be the use of the T2 setting with a preferred value of 0.5 seconds.
- Direct attempts to determine the target OS should be avoided. Capturing ARP table content and then reviewing the MAC address' OI values is a reasonably safe means of gaining vendor information.
- Service identification on ports is a desired attribute for establishing risk and potential access policy. Scanning for services is viable in most cases. When using Nmap, your lighter touch option would be the -sV setting should you feel it safe to pursue.

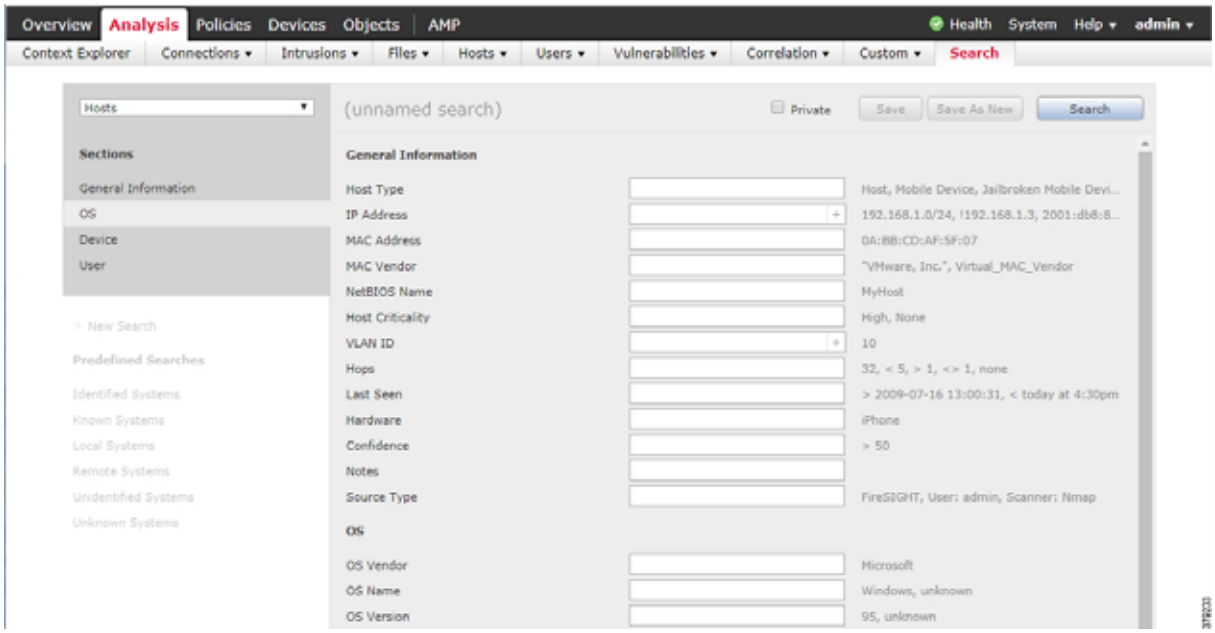
Tools that can safely scan the environment using native industrial protocols are another means of safely discovering assets in the operational space. An example of one such tool is Cisco's Industrial Network Director (IND). This tool is designed to perform network management at operational levels and part of that duty includes the discovery of assets through native management protocols. IND uses a two-step process to discovery. First is a lightweight Simple Network Management Protocol (SNMP) scan of the target environment. Based on the initial scan results, the tool queries the target device through the appropriate protocol such as Modbus or Control and Information Protocol/EtherNet/IP (CIP/EIP). Device attributes are then stored and displayed in the tool. IND also shares this information with a Network Access Control (NAC) system such as Cisco's Identity Services Engine (ISE). Policy can then be applied to the infrastructure and network participants.



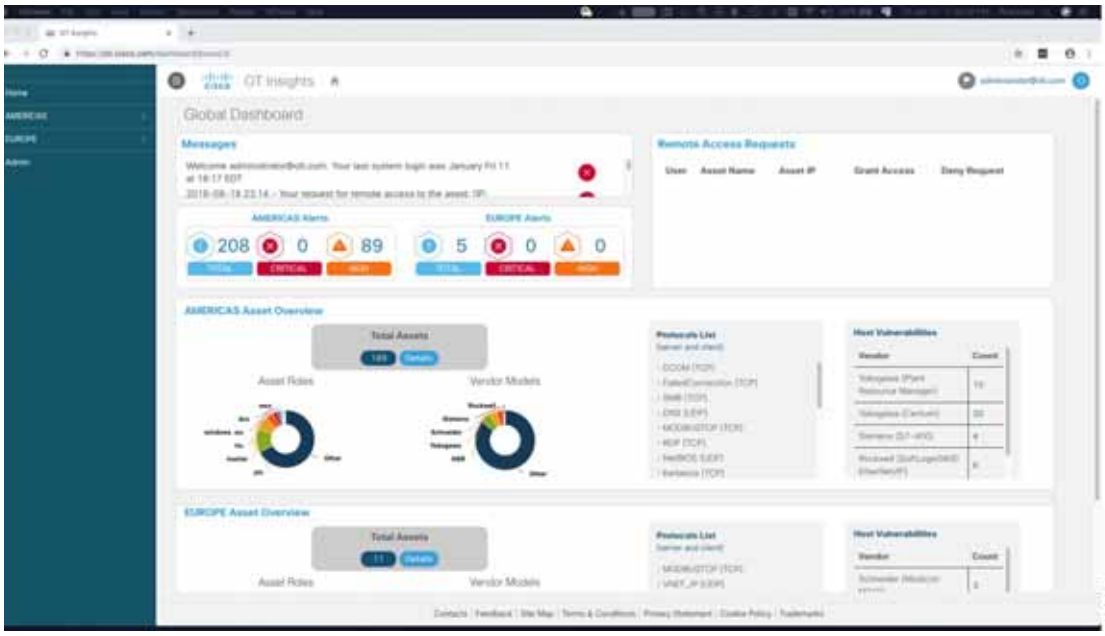
Cisco ISE itself is fully capable of discovering systems on the network through both passive and active means. ISE is particularly valuable for classic IT class elements such as workstations, servers, phones, tablets, and printers. It is a valuable repository of asset inventories and can receive inputs from other sources.

Passive scanning, which is a safer but longer process, requires the capture of data over the network or a review of data generated by devices in the area of interest over an extended period of time. Asset identification supporting content can be captured passively in multiple ways. One common method is to inspect network traffic through DPI tools such as an Intrusion Detection System (IDS) or an Intrusion Protection System (IPS). The IDS/IPS may be in-line or operating on copies of traffic. There are alternative services which operate on a span.

The Cisco FirePOWER system is an IDS/IPS that has the ability to capture device traffic and identify end points. This service is effective for typical IT stack devices. It notes common protocols associated with the device, services used, and potentially application-related traffic to suggest the operating system of the device.



Some tools attempt to infer the device attributes through a number of detected behaviors. An IDS/IPS type system with deep packet inspection (DPI) might do so by alerting on a particular traffic type and associated content. Another example could be using the CIP/EIP protocol to identify communication between two points. Some communication types are responses to queries. Using that logic of query and response conversations, one can normally determine the relationship and suggest a device type. In some cases, known vendor unique protocol extensions that more closely identify the device type and vendor exist. If your observation period is long enough, then a body of evidentiary content is built up, increasing the probability of an accurate identification. An example of such a tool comes from the OT Insight service which has a span port to capture the traffic and identify assets.



Flow data generated by modern network infrastructure can provide additional evidence to suggest a device type that can then be added to the inventory. Using a NetFlow-based tool such as Cisco Stealthwatch can provide information to suggest an endpoint type.

Log information generated by network infrastructure and security tools can provide information on devices in the network. ARP tables from switches and routers can provide information about end points. Firewall connection tables can also be mined for device discovery.

In some cases, the end devices themselves generate logs that may be forwarded to log servers, like syslog repositories. Analyzing these logs can provide further information to identify devices and their attributes.

Summary

The discovery and aggregation of end-point attributes into a comprehensive inventory is vital to proper security policy definition and enforcement. Inventory information is equally valuable to investigation activities and remediation planning as well, as it provides an understanding of the network's structure and expected communication which, in turn, support the identification of potentially anomalous traffic.

The process of generating an inventory of assets has multiple steps and can be achieved in a number of ways. Key to any inventory creation is the communications between the different teams needed to operate the pipeline and manage the associated infrastructure. The scope of the teams involved should touch the operations group, networking, physical security, IT, and external contractors.

Tools can automate and accelerate inventory creation. Some tools are ready made for operational elements, while others are targeted to IT type asset types. The mode of operation may be active or passive in nature. In all cases, it is important to recognize the safest and most complete practice to succeed in safely generating an asset inventory to facilitate further security actions.

Industry Standards Cross-Reference: Asset Discovery and Inventory

Key Industry Standards and Guidelines
ISO 27001 Section A8 Asset Management
ISO 55001 Asset Management, Management, System Requirements
ISO 19770 IT Asset Management
NIST SP 800-53 PE-20 Asset Monitoring and Tracking
ENERGY SECTOR ASSET MANAGEMENT for Electric Utilities, Oil & Gas Industry
NERC-CIP CIP-002 Cyber Asset Identification
TSA Pipeline Security Guidelines, Section 7.2 Pipeline Cyber Assets Identification

Risk Analysis

Risk Analysis Defined

The U.S. Department of Homeland Security[1] states that the intent of risk analysis is to bring a risk-based approach to the application of security measures throughout the pipeline industry. As stated in the National Infrastructure Protection Plan, oil and gas companies need to assess risk as a function of threats, vulnerabilities, and consequences. With this in mind, the most effective security programs employ a risk management approach that takes this information and distills it into a quantifiable and comparable structure allowing pipeline companies to determine their risk profile and make decisions based on quantified priorities.

What We are Trying to Solve

We are trying to define a risk assessment approach and methodology that fits your organization. Such a program is a risk-based corporate security program that should be established and implemented to address and document the organization's policies and procedures for managing security related threats, incidents, and responses. In addition, an organization should:

- Develop a corporate security plan
- Ensure sufficient resources, to include trained staff and equipment and budget, are provided to effectively execute the corporate security program
- Ensure identified security deficiencies have appropriate financial resources allocated in the corporate budgeting and purchasing processes
- Assign a qualified primary and alternate staff member to manage the corporate security program
- Develop and maintain a cyber/SCADA security plan, or incorporate cyber/SCADA security measures in the corporate security plan
- Develop and maintain security elements within the corporate incident response and recovery plan

Risk Assessment

Risk Assessment is the process that facilitates planning and decision making to mitigate risks for pipeline assets. General elements include:

- Assessments used to determine facility criticality
- Threat assessments identifying known or potential adversaries
- Vulnerability assessments identifying security weaknesses
- Risk assessments (based on threat, vulnerability, and consequence, considering facility criticality assessment findings)
- Risk mitigation to determine and implement appropriate risk reduction countermeasures
- Ongoing risk management to monitor, reassess, and modify the program

Recognizing that multiple risk assessment methodologies exist, the process and methodology most appropriate for implementation of the corporate security plan at the facilities comprising your pipeline system should be determined. This is one of the challenges related to the IT/OT convergence; a " give and take" must occur between the two since OT cannot always directly (or at all) converge with an IT security program.

1. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

Criticality Assessment

Determining facility criticality is an essential first step in the OT security risk management process. Information and findings gathered in the criticality assessment assists an organization in prioritizing assets and implementing risk reduction countermeasures. Each operating facility within the organizational system should be evaluated using the facility criticality criteria to determine or validate criticality, including:

- Conducting facility criticality assessments on a periodic basis, not to exceed 18 months, for all facilities. For example, a facility normally has safety, protection and control assets; safety and protection is considered a high criticality as compared to control assets.
- Documenting the methodology used and retaining the criticality assessment until no longer valid.
- Conducting a Security Vulnerability Assessment (SVA) or the equivalent for facilities determined to be critical.
- Maintaining and securing the company's list of critical facilities.

Security Vulnerability Assessment

Among the available risk assessment methodologies, an organization may choose to use a Security Vulnerability Assessment (SVA). The SVA serves as a planning and decision support tool to assist security managers with identifying, evaluating, prioritizing risks, and determining effective security measures to mitigate threats and vulnerabilities to their critical facilities. Common steps performed while conducting an SVA include:

- **Asset Characterization**—Identification of hazards and consequences of concern for the facility, its surroundings, and its supporting infrastructure; and identification of existing layers of protection.
- **Threat Assessment**—Identification of possible internal and external threats.
- **Security Vulnerability Analysis**—Identification of potential security vulnerabilities and existing countermeasures and their level of effectiveness in reducing identified vulnerabilities.
- **Risk Assessment**—Determination of the relative degree of risk to the facility in terms of the expected effect on each asset and the likelihood of success of an attack.
- **Countermeasures Analysis**—Comparison of methods that reduce the probability of a successful attack or reduce the possible degree of success, capabilities that enhance the degree of risk reduction, the capabilities and effectiveness of mitigation options, and the feasibility of the options. As an example, consider a Process Control Network (PCN) that is a flat network. If an attacker gains access to a low critical asset, he can laterally move and compromise a high critical asset; therefore, create a segmentation strategy that provides more granular traffic control and gives greater visibility into the network and applications.

Critical pipeline facilities should:

- Conduct an SVA or the equivalent on a periodic basis, not to exceed 36 months, and within 12 months after completion of a significant enhancement or modification to the facility.
- Conduct an SVA or the equivalent for newly identified or constructed critical facilities within 12 months of designation or after achieving operational status.
- Document findings from each assessment and retain them until no longer valid.
- Implement appropriate findings from the SVA in a timely fashion but no later than 24 months after SVA completion.

Risk Assessment Approach and Methodology

Some organizations have a defined methodology for asset discovery and risk assessment. Others will use a third-party vendor approach that multiple previous engagements have proven.

Best practice approaches in all engagements are to ask a series of key questions to ensure that the recommendations, roadmap, and strategy are tangible and able to deliver business value to the customer. For security-related engagements, some of the questions include (stated introspectively as the customer):

- Do I have the right strategy, security architecture, operational plan and governance model in place to support my business goals?
- What is the impact on these assets in the event of a cyber-attack or incident?
- What is the scope? Am I purely concerned, and focused, on the risk of a cyber-attack? Or should I be concerned (more broadly) about human errors and system failures as well?
- Who is accountable and responsible?
- How do I respond to an active cyber attack or incident? What processes do I have in place prior to such an incident?
- How does my approach compare to that of my peers, industry standards (such as ISA-99/IEC 62443) and best practices?
- What is my defined architecture? How much is automated and proactive?
- What is my current state of Security Maturity and how can that be improved?
- How do I ensure that my strategy and overarching plan evolves to the changing landscape?

The National Institute of Standards and Technology (NIST)[1] has developed the Framework for Improving Critical Infrastructure Cybersecurity, a set of standards and best practices to assist organizations in managing cybersecurity risks and to promote the protection of critical infrastructure. To implement an effective cybersecurity strategy, consider the approach outlined in the NIST Framework and the guidance issued by DHS and the Department of Energy (DOE) along with industry-specific or other established methodologies, standards, and best practices.

Pipeline Cyber Assets Classification

Evaluate pipeline cyber assets and classify them using the following criteria:

- Critical pipeline cyber assets are OT systems that can control operations of the pipeline. Baseline and enhanced security measures should be applied to these assets.
- Non-critical pipeline cyber assets are OT systems that monitor operations of the pipeline. Baseline security measures should be applied to these assets.

1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Security Measures for Pipeline Cyber Assets

Figure 23 shows the baseline and enhanced cybersecurity measures that should be applied to pipeline cyber assets based on their criticality designation. The cybersecurity guidelines that follow are organized according to the relevant functions and categories presented in the NIST Framework.

Figure 23 Baseline and Enhancement Cyber Security Measures 1

	Baseline Security Measures	Enhanced Security Measures
Identity	**Asset Management**	
	Establish and document policies and procedures for assessing and maintaining configuration information, for tracking changes made to the pipeline cyber assets, and for patching/upgrading operating systems and applications. Ensure that the changes do not adversely affect existing cybersecurity controls.	Employ mechanisms to maintain accurate inventory and to detect unauthorized components.
	Develop and maintain a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third party connections, and information flows.	Review network connections periodically, including remote and third party connections. Develop a detailed inventory for every endpoint.
	Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months.	
	Business Environment	
	Ensure that any change that adds control operations to a non-critical pipeline cyber asset results in the system being recognized as a critical pipeline cyber asset and enhanced security measures being applied.	
	Governance	
	Establish and distribute cybersecurity policies, plans, processes and supporting procedures commensurate with the current regulatory, risk, legal and operational environment.	
	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 36 months, or when a significant organizational or technological change occurs. Update as necessary.	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 12 months, or when a significant organizational change occurs. Update as necessary.
	Risk Management Strategy	
	Develop an operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks.	

379472

Figure 24 Baseline and Enhancement Cyber Security Measures 2

	Baseline Security Measures	Enhanced Security Measures
Identify	**Risk Assessment**	
	Establish a process to identify and evaluate vulnerabilities and compensating security controls.	Ensure threat and vulnerability information received from information sharing forums and sources are made available to those responsible for assessing and determining the appropriate course of action.
Protect	**Access Control**	
	Establish and enforce unique accounts for each individual user and administrator, establish security requirements for certain types of privileged accounts, and prohibit the sharing of these accounts. In instances where systems do not support unique user accounts, implement appropriate compensating security controls (e.g., physical controls).	Restrict user physical access to control systems and control networks using appropriate controls. Employ more stringent identity and access management practices (e.g., authenticators, password- construct, and access control).
	Ensure that user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or who are no longer employed by the company.	
	Establish and enforce access control policies for local and remote users. Procedures and controls should be in place for approving and enforcing policy for remote and third party connections.	Monitor physical and remote user access to critical pipeline cyber assets.
	Ensure appropriate segregation of duties is in place. In instances where this is not feasible, apply appropriate compensating security controls.	
	Change all default passwords for new software, hardware, etc., upon installation. In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), implement appropriate compensating security controls (e.g., administrative controls).	Employ mechanisms to support the management of accounts.

379473

Figure 25 Baseline and Enhancement Cyber Security Measures 3

	Baseline Security Measures	Enhanced Security Measures
Protect	**Awareness and Training**	
	Ensure that all persons requiring access to the organization's pipeline cyber assets receive cybersecurity awareness training.	Provide role-based security training on recognizing and reporting potential indicators of system compromise prior to obtaining access to the critical pipeline cyber assets.
	Establish and execute a cyber-threat awareness program for employees. This program should include practical exercises/testing.	
	Data Security & Information Protection	
	Establish and implement policies and procedures to ensure data protection measures are in place, including identifying critical data and establishing classification of different types of data, establishing specific handling procedures, and protections and disposal.	
	Protective Technology	
	Segregate and protect the pipeline cyber assets from enterprise networks and the internet using physical separation, firewalls and other protections.	
	Regularly validate that technical controls comply with the organization's cybersecurity policies, plans and procedures, and report results to senior management.	
	Implement technical or procedural controls to restrict the use of pipeline cyber assets for only approved activities.	
Detect	**Anomalies and Events**	
	Implement processes for generating alerts and log cybersecurity events in response to anomalous activity. Review the logs and respond to alerts in a timely manner.	
	Security Continuous Monitoring	
	Monitor for unauthorized access or the introduction of malicious code or communications.	
	Conduct cyber vulnerability assessments as described in your risk assessment process.	Use independent assessors to conduct pipeline cyber security assessments.

Figure 26 Baseline and Enhancement Cyber Security Measures 4

	Baseline Security Measures	Enhanced Security Measures
Detect	**Detection Processes**	
	Establish technical or procedural controls for cyber intrusion monitoring and detection.	
	Perform regular testing of intrusion and malware detection processes and procedures.	
Respond	**Response Planning**	
	Establish policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignment of the specific roles/tasks to individuals and teams.	Conduct cybersecurity incident response exercises periodically.
	Establish and maintain a cyber-incident response capability.	Establish and maintain a process that supports 24 hour-a-day cyber incident response.
	Communications	
	Report significant cyber incidents to senior management; appropriate federal, state, local, tribal, and territorial (SLTT) entities; and applicable ISAC(s).	Pipeline operators should follow the notification criteria in Appendix B
	Mitigation	
	Ensure the organization's response plans and procedures include mitigation measures to help prevent further impacts.	
Recover	**Recovery Planning**	
	Establish a plan for the recovery and reconstitution of pipeline cyber assets within a timeframe to align with the organization's safety and business continuity objectives.	
	Improvements	
	Review the organization's cyber recovery plan annually. Update as necessary.	

379475

Automated Risk Assessment Tools

Many pipeline companies have started looking for automated risk assessment and planning tools that will help their companies build a more robust security posture. These automation tools will require other security products like asset inventory coupled with monitoring and detecting tools; for example, passive or active asset discovery with anomaly detection.

Risk assessment automation tools use:

- The data generated by existing asset discovery and monitoring tools, which enables the customer to more easily pinpoint vulnerabilities and then create action plans that will ultimately lead to better protection.
- Big data analytics and sophisticated artificial intelligence (AI) algorithms to present the risks the customer may face through an intuitive, actionable fashion useful for both executives and operations teams.

Risk assessment is a complicated and time-consuming process, with many pipeline companies performing an annual risk assessment. However, automated risk assessment tools can provide value without adding agents, infrastructure, or substantial resource commitments, meaning companies can maximize the value of their current existing security investments with little to no additional operational overhead.

Conclusion

The risk assessment helps by identifying of risks, vulnerabilities, actors, cost implications, and the likelihood of the risk occurring. By bringing these items together across the various system components, including networks, servers, physical security, and users, an organization can quantify its risk profile. From there, mitigation strategies necessary to remove these risks and improve the overall security profile can be considered. It is important to note that all risks may never be removed, but the point of the process is to clearly identify your risks, thus helping reducing those risks to an acceptable level. Additionally, the necessary documentation is produced that clearly quantifies the risks, enabling justification of the request for resources, both people and budget, to establish the programs needed to address these key risks.

Industry Standards Cross-Reference: Risk Discovery

Key Industry Standards and Guidelines
IEC 62443-3-2 Security Risk Assessment and System Design
ISO 27001 Risk Management Section 6 Planning
ISO 27005 Information Technology, Security Techniques, Information Security Risk Management
ISO 31000 Risk Management
NIST SP 800-30 Guide for Conducting Risk Assessment
NIST SP 800-53 Risk Assessment Control Family
NIST Framework for Improving Critical Infrastructure Cybersecurity
API 1164 Section 3.3 Risk and Vulnerability Assessment
CFATS Section C Approval or disapproval of site security plans, (3) Site security plan assessments, (A) Risk assessment policies and procedures
TSA Pipeline Security Guidelines, Section 4 Risk Analysis

Cybersecurity Practice & Philosophy

Cybersecurity Practice and Philosophy Defined

The following key security philosophies, while not presented in any particular order or hierarchy, are important philosophies of cybersecurity practices and reference architectures that should guide system design for any pipeline company:

- **Philosophy #1**—Include Security Early and Often in your Projects. Unfortunately, security is not an add-on; the cost of fixing a problem after a project has been implemented and underway is much more expensive than addressing the need in the design phase. It is in an organization's long-term interest to adopt security practices during the course of the project, especially during design review, architecture analysis, and threat modeling, versus retrofitting it later.
- **Philosophy #2**—The First Line of Defense is the Individual User (zero trust policy). Every employee at a company who uses, moves, transports, files, disposes, or creates information and data is critically important to the success of the data and information security program. A user's actions, or failures to act in some instances, can result in exposing the company to some very risky situations or creating a cyber incident or enabling an opening to be exploited later.
- **Philosophy #3**—Protect the Data! In today's pipeline digitization world, a pipeline company runs on its *data*. Without the data and its protection, the organization cannot be successful. This data can include different forms of electronic media as well as documents and portable devices. As important as this issue is, and even with the widespread awareness of its criticality, data and networks often lack fundamental security infrastructure that will reduce the possibility of data exposure or compromise.

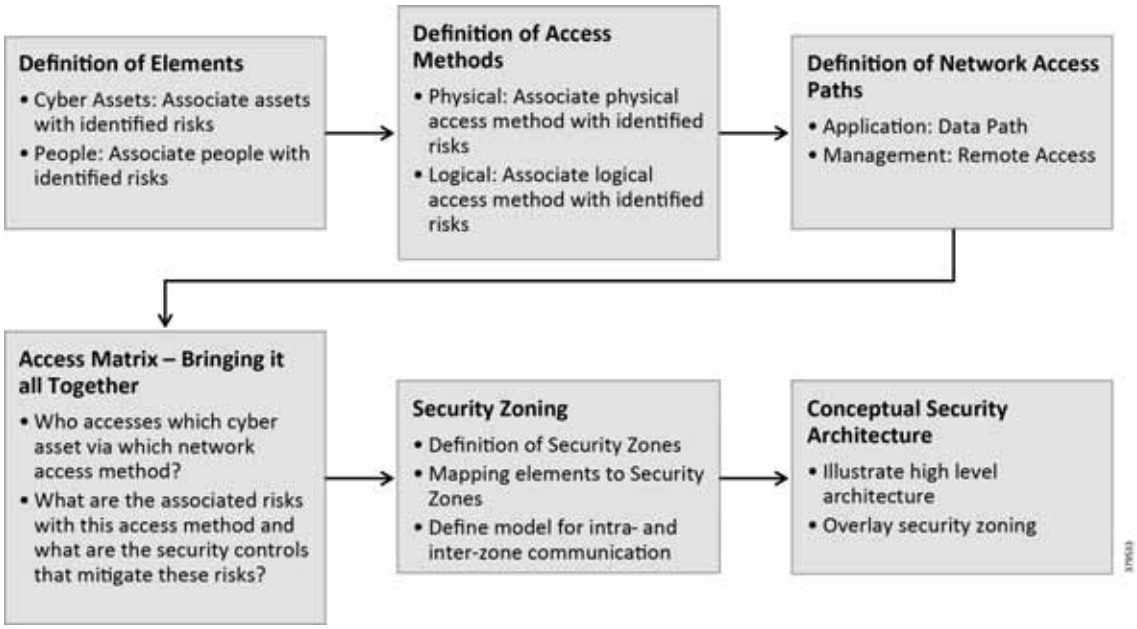
What We are Trying to Solve

This chapter describes the people and systems that are the key elements, how they access the different networks, and how they interact with each other. Previously, we identified security risks and control measures and how they are mapped to various operational areas. We also illustrated in an end-to-end conceptual security architecture the controls that can be used to mitigate identified risks.

Risk Assessment

The development of the Conceptual Security Architecture is based on a logical process that ensures continuity of the Risk Assessment Framework and Risk Assessment, as illustrated in Figure 27:

Figure 27 Example Risk Assessment Framework



Cybersecurity Elements

In the context of cybersecurity practice, *elements* are the entities that either need protection or pose a risk to systems. Categorization of elements, which is as follows, is described below.

Technology

Systems, in the context and scope of this chapter, are those systems, devices, hosts, or networks that are part of the overall architecture and require some form of network security protection.

Technology, in the context of ICS cyber security, is all about the technical security controls in place to uphold its availability, integrity, and confidentiality (aka the CIA Triad). These would include traditional solutions for authentication, access control, and encryption, as well as other technical measures that are applied to reduce security risks to the ICS. The objective of ICS-related technology is to ensure that security risks are reduced and security-related business processes are automated where feasible.

Processes

The objective is to establish a set of business processes and tasks to be completed, such as change control, access management, patching, inventory management, and security testing.

Processes can be implemented in several ways, but they are generally built upon smaller components of documentation and are based on policy foundations:

- **Policy**—A policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedure criteria for a specified subject area.

- **Standards**—A standard is a formal document that establishes mandatory requirements, engineering, technical criteria, and methods. A standard is meant to convey a mandatory action or rule and is written in conjunction with a policy.
- **Process/Procedures**—A process or procedure document typically describes the act of taking something through an established set of procedures or steps to convert it from one form to another, such as processing paperwork to grant physical or cyber access or converting computer data from one form to another.
- **Guidelines**—Guidelines are not required as part of a policy framework; however, they can play an important role in conveying best practice information to the user community. They are meant to **guide** users to adopt behaviors, which increases the security posture of a network but are not yet required (or in some cases, may never be required). In the context of the IEC-62443 series, the specific structure and content of policies, standards, and guidelines are left to the discretion of the ICS asset owner. However, the series organizes the subject areas associated with ICS processes in the following clauses, categories, and domains.

People

People, in the context of this document, are individuals that gain access to cyber assets for one or more of the following reasons:

1. Work conducted as part of regular maintenance or operations.
2. Work conducted as part of fault isolation, troubleshooting, and repairs.
3. Informational purpose as part of the service (for example, customer access to customer portal).
4. Malicious intent or other illegal activity.

Systems and networks require appropriate protection from access by people, depending on the individual's role, task, access method, and access path.

Cybersecurity Access Methods

Access methods specify the methods through which cyber asset elements can be accessed. These methods are generally either physical or logical.

Physical Access

Physical access is the manner in which a person accesses a cyber asset through manual or physical means (for example, a field worker gaining access to a customer's switchboard and the smart metering assets housed within it).

A person with malicious intent may gain physical access in order to manipulate a cyber asset for unauthorized purposes.

Logical Access (or Remote Access)

Logical access is a way of accessing a cyber asset through non-physical (or non-direct) means. Leveraging the various network-based access methods through which the cyber asset is connected or through other parts of the cyber-based infrastructure is a typical example.

Logical access methods use a variety of technologies and network protocols for communication. The logical access methods under consideration include:

1. Ethernet/IP
2. Wi-Fi
3. 2G/3G/4G
4. ASDN/Dial-up

Logical Access Matrix

The positioning of the various logical access technologies aids mitigation of the various risks in the interfaces between the elements.

The Security Risk Assessment Framework has identified the communication interfaces between elements. Building on this, we can position the various logical access technologies in their correct context as they apply to the overall system architecture.

The Risk Assessment section previously outlined the risks to be mitigated that are associated with the logical access methods for each given interface. Identified risks (or rather, vulnerabilities) are not confined to a given device itself; rather, the vulnerability is a result of the communications interface to the device.

For instance, a smart gas meter communicates over Ethernet. While the smart meter itself is susceptible to exploitation of vulnerabilities that exist within the element itself, the risks outlined here apply specifically to the network connectivity of the element. For example, a DoS attack doesn't exist on the device; it is initiated via the network connection to a system.

Cybersecurity Security Controls

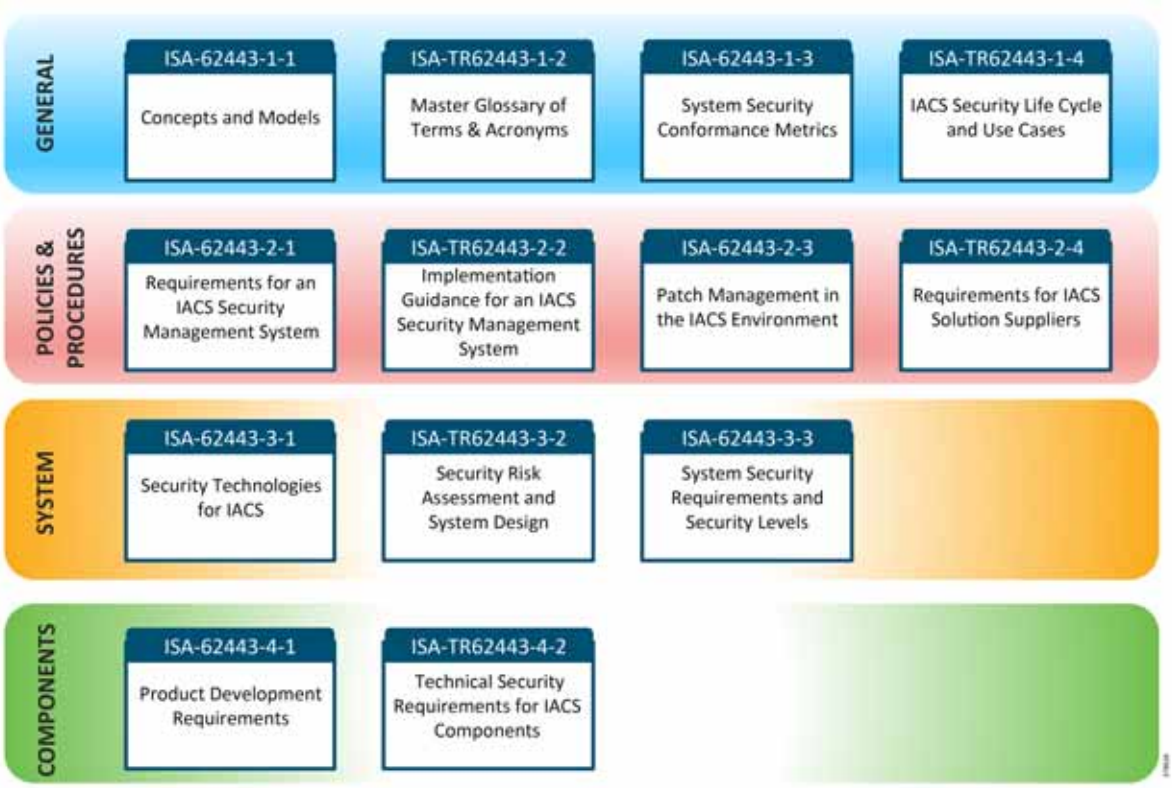
This section outlines the security controls used for the mitigation of identified risks. These security controls are in alignment with the eight security dimensions of the IEC-62443 framework.

IEC-62443 Overview

The IEC-62443 series builds on established standards for the security of general-purpose information technology systems (e.g., the ISO/IEC 27000 series), identifying and addressing the important differences present in an ICS.

Many of these differences are based on the reality that cyber security risks within an ICS may have Health, Safety, or Environment (HSE) implications and that the response should be integrated with other existing risk management practices addressing these risks.

Figure 28 ISA 62443 Series Elements



Security dimensions provide the framework and context by which security controls can be applied within a given system architecture.

Access Control

Access control, which protects against unauthorized use of network resources, ensures that only authorized personnel or devices have access to network elements, stored information, information flows, services, and applications. In addition, Role-Based Access Control (RBAC) provides differentiated access levels to guarantee that individuals and devices can only gain access to and perform operations on those network elements, stored information, and information flows for which they are authorized.

Authentication

Authentication confirms the identity of a communicating entity or individual. Authentication serves as a common means of ensuring that only legitimate users of the available data gain access to a cyber-based asset or resource.

Non-Repudiation

Non-Repudiation fundamentally proves the integrity and origin of data. It provides a means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions. It ensures that evidence proving that an event or action has taken place is available to a third party.

Data Confidentiality

Data Confidentiality protects data from unauthorized disclosure. Data confidentiality ensures that unauthorized entities cannot intercept the data content.

Communication Security

Communication Security ensures that information flows only between the authorized endpoints. That way the information cannot not diverted via alternative paths or intercepted because it flows between the communicating endpoints.

Data Integrity

Data Integrity ensures the correctness or accuracy of data, which is protected against unauthorized modification, deletion, creation or replication.

Availability

Availability ensures that events affecting the network do not compromise authorized access to network elements, stored information, information flows, services or applications. Disaster recovery solutions are included in this category.

Privacy

Privacy provides for the protection of information that might be derived from the observation of network activities. Examples of this information include web sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network.

Cybersecurity Controls Matrix

A Control Matrix identifies elements, access methods, network access paths, security controls, and associated risks. It describes who has access to a given cyber asset, which security risks are associated with this access, and the security controls for addressing these risks.

Cybersecurity Security Zoning

Security zones logically separate certain segments of a network from each other based on the level of trust that is associated with them. Multiple factors such as physical location, line of business, technical function, and access from internal and/or external resources can be the basis of this separation.

No specific 'best practice' exists for the number of zones an organizational security model should have. The zone model can be simple or complex in nature, but the recommended approach is to distinguish between elements/areas that are exposed to external factors (e.g., the Internet) or internal factors (e.g., corporate network users).

Another goal of security zones is to clearly identify the security controls that must or should be in place between elements that communicate with each other, either within a zone or across zones.

The following provides an overview of the suggested zones and their definitions, followed by a graphical illustration of these zones and their elements.

Zone Definitions

The security architecture includes the following suggested zones:

Figure 29 Security Zone Definitions

Zone	Description
Externally Uncontrolled	System Elements that are not controlled by the Customer. These systems may be visible to the pipeline company but are physically located on customer premises and potentially owned and operated by customers/end-users and/or 3rd parties.
Externally Semi-Controlled	System Elements that are partially controlled by the Customer. These systems may be visible and generally controlled by the pipeline company; however, due to their physical locations on customer premises, not all aspects of the system can be controlled by the pipeline company.
Externally Controlled	System Elements that are controlled by the Customer. These systems are only accessed by Customer staff; however, these devices are located in uncontrolled locations, with potential exposure to strangers or people with malicious intent.
Internally Controlled	System Elements that are controlled by the Customer. These systems are only accessible by Customer staff. These devices are located within Customer-secured locations.

Security Zone Model

The definitions of security zones allow for the broad categorization of network assets so that they can be grouped by their security threat posture.

Intra and Inter Zone Communications

Once cyber assets are assigned to a security zone, the communication flows between the assets can be overlaid, highlighting the flows that are both intra-zone and inter-zone based. Communication flow functionality does not change based on the placement of the asset within a given security zone; rather, the establishment of security boundaries or control points becomes more clear.

These control points act as enforcement points for security policies and technologies, such as stateful packet inspection firewalls and deep packet inspection (e.g. IDS/IPS).

Communication Rules

The zone communication rules provide high-level guidance on the management of communications between cyber assets within a zone (intra-zone) or across zones (inter-zone) from a security standpoint. Each security zone and the elements within each zone are associated with a certain level of trust.

In the suggested zone model above, the *Externally Uncontrolled* zone is the least trusted zone and the *Internally Controlled* is the most trusted zone.

The general approach with zoning models is that elements within a given zone should only communicate with elements in another zone that has the next higher level of trust.

In a communication path, as a high-level rule, a zone should not be by-passed or 'jumped over' by a single communications flow. For example, in the given model above, elements in the externally uncontrolled zone should not directly communicate with any element in the externally controlled zone.

As with any network, exceptions to the rule always exist, but this general approach is recommended with security zone models.

1. **Intra-Zone Communication**—From a zoning perspective, cyber assets within a zone can communicate with each other without restrictions; however, security controls are still required on each element to mitigate any vulnerabilities that may pose a risk that originates from malicious or non-legitimate activity.
2. **Inter-Zone Communication**—Communication across security zones with different trust levels should follow a stricter control model although, because of the complexity of some communication channels, some exceptions may be required.

Given the zoning model shown earlier, a cyber asset within a given zone should only be required to communicate directly with a cyber asset of another zone that has the next higher trust level.

For example, a cyber asset in the *Externally Uncontrolled* zone should not communicate directly with a cyber asset of the *Externally Controlled* zone because it would bypass the *Externally Semi-Controlled* zone. Likewise, no cyber asset in the *Externally Controlled* zone should directly communicate with a cyber asset of the *Externally Uncontrolled* zone.

Since network environments and communications can become very complex, organizations can make exceptions to these general rules described above. However, any such exceptions must be properly documented with a valid business and technical justification underpinning these decisions.

The application architecture and the requirements of various cyber assets to communicate with each other governs the application of these high-level guidelines or rules. Commonly, many application vendors do not consider security zones when application solutions are developed. In deployment of a given solution, whether to prioritize application functionality or security controls when a given application is unable to fit within a security zone model, is a business-based decision.

Allocating assets to a particular zone can be a subjective exercise.

Cybersecurity Conceptual Security Architecture

The Cybersecurity Reference Architecture Document will include:

- Recommended network designs document.
- Recommended firewall configuration document (network implementations document).
- User authorization and authentication document.
- Interconnecting different process control networks document.
- Remote access management document.
- Use of wireless communications document.
- Domains and trust relationships document.
- Patch management (including authentication) document.
- Anti-virus management document.
- System hardening in terms of closing software ports, disabling or avoiding unused or dangerous services, and disabling the use of removable storage devices document.
- Access to external networks (i.e., the internet) document.

Industry Standards Cross-Reference: Cybersecurity

Key Industry Standards and Guidelines
IEC 62443-1-4 Security Lifecycle and Use Cases
ISO 27001 Section A14, System Acquisition, Development And Maintenance
NIST SP 800-53 System and Services Acquisition Control Family
NIST Framework for Improving Critical Infrastructure Cybersecurity
NERC-CIP CIP-003 Security Management Controls
CFATS, (a) Program established, (b) Security measures
TSA Pipeline Security Guidelines, Section 3 Corporate Security Plan
OWASP Security by Design Principles

System Access Control

Access Control Defined

The first level of applied security is the control of access to assets. Depending on the capabilities of the assets and available points of control, access control can be applied to multiple levels of a system.

Control of access depends on knowing about the assets whose access an organization wishes to control; therefore, the successful capture of assets and an understanding of their relationships is critical to the process. In addition to the technical relationships, the definition of proper access policies depends on business needs and their relationship to the system. This chapter will discuss topics relevant to the process of defining and applying access control policies.

- Policies are the collection of rules, which define access rights to the assets within the system.
- Access rights can define who or what can access which assets with what level of participation.

What We are Trying to Solve

The ability to control access to pipeline assets is the first level of actionable security.

Industrial systems are a set of discrete assets assembled for purpose. The pipeline system is itself comprised of different subsystems, which, in turn, may have further subsystems and discrete items that make up those subsystems. This decomposition of systems logically continues down to the lowest identifiable element within each piece. At some point, however, the ability to control the use or access of those pieces reaches a pragmatic level that is under the direct control of the organization. Contractual obligations, organizational constraints, regulations, skill sets, and resources limit some of these constraints.

The first widely known cyber-attack on an industrial system was the result of improper access control. A disgruntled contractor attacked the Maroochy Shire sewage system by simply accessing the system remotely and initiating commands to dump tons of sewage into the local waterways. Such access control errors continue. In 2017, a fired system administrator, who was able to access a paper plant remotely, caused over a million dollars of damage.

Multiple standards and best practices reference controlling system access. These needs and standards span both informational and operational technology spaces. Examples of such standards referencing access control include NIST Guide to Industrial Control Systems (ICS) Security; the US Transportation Safety Administration's Pipeline Security Guidelines, and IEC 62443 / ISA 99 (via zone / conduit discussion).

Access Control, like most security initiatives, begins with policy, which depends upon understanding the goals and operation of the system under consideration. Discovery of the goals and operational procedures of the pipeline are outside the scope of this chapter so we will assume that policy is established and ready to be applied. An Access Control policy is enabled through AAA. Authentication and Authorization primarily focus on enablement. Accounting is the history of actions associated with network participation.

Process

As stated earlier, having a flexible process that organizations can apply to pipelines at different stages of maturity, unforeseen circumstances, and under multiple forms of managerial and regulatory oversight, is key to success. Conditions, such as the vendors providing automation equipment or sub-contractors performing identical tasks in different locations, can vary. Therefore, a flexible approach is important.

Consider the following lifecycle view of a security process, which the Department of Homeland Defense calls Continuous Diagnostics and Mitigation (CDM).

Table 3 Continuous Diagnostics and Mitigation (CDM)

CDM - Phase 1	CDM - Phase 2	CDM - Phase 3
Asset Control—what is the state of the endpoints I must secure	Manage People and Services—Who can do what?	Process Planning—What to do and how do we improve?

What should be noted is that the process of access control will either be affected or take place across all three of the above CDM phases. The assets to be accessed are determined in Phase 1, participants that may access those assets are discussed in Phase 2, and the constant re-evaluation of our security state is discussed in Phase 3. In short, access control, like all other security related processes, rarely, if ever, reaches a *done* state.

To get started, the following sections provide some questions and tasks on which to focus.

Access to What?

If access to an asset (hardware, software, or other) represents a security risk that can be addressed, then the organization's pipeline access control policy needs to account for it. Even items and access conditions that do not represent obvious risks are worth noting because what looks innocuous may represent an opportunity for mischief.

As a given, if it is in the inventory of objects created during asset discovery, then the organization should have an access control policy and a means of enforcement.

Looking back at Asset Discovery and Inventory, page 49, we see that the most commonly referenced class of inventory objects are network-connected devices. The devices may operate directly on the pipeline itself or have ancillary roles, which indirectly drive pipeline behavior.

Software is also within the inventory. Software, which may be independent of a specific piece of equipment, is likely to be the most dynamic of all assets and thus merits special attention, especially concerning capability coverage. A software package, which may be dynamic in location, is the controlling element that determines the organization's ability to remotely see or operate any physical element of the system.

System users is one of the attributes that an access control policy should reference. Management of the system's users via access control is an important component of pipeline security.

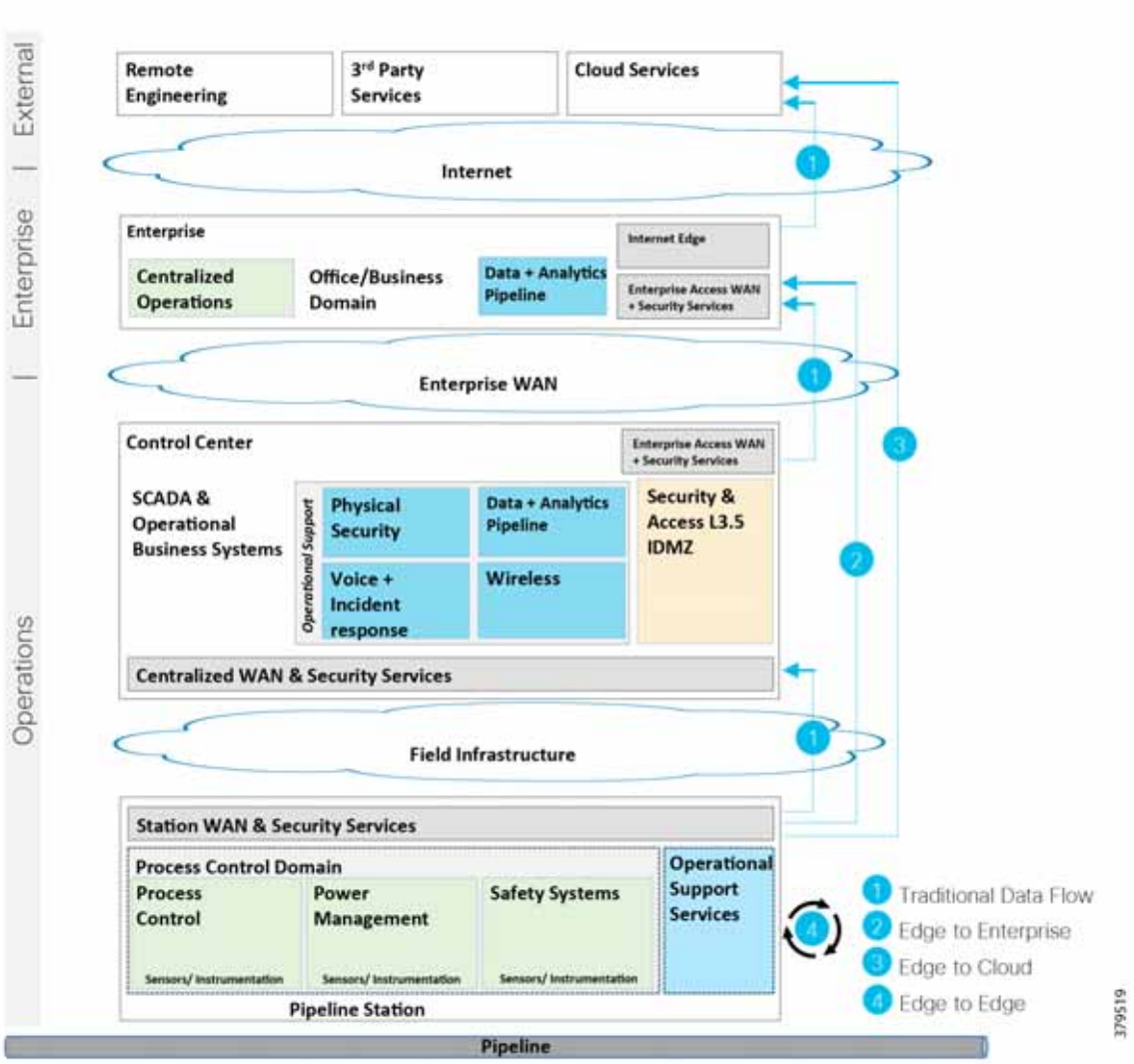
Referencing again earlier themes in the document, numerous overlapping best practices and standards are applicable to pipeline operation. Terms and references do not always use identical terms or focus on the same scope. For the purposes of this chapter and the desire to be as inclusive, we will reference multiple standards.

The question of scope or range of control, which we noted previously, is a consideration for access control discussions. What are the boundaries of the System under Consideration (SUC)? Considering if access to a system formally outside the SUC may imply or directly result in access to a sub-system within the SUC is a valuable exercise.

Multiple published pipeline-related guidelines with varying degree of scope or boundaries exist. The *Security Guidelines for Natural Gas Pipeline Industry* describes a reference architecture comprised of the following broad areas: Field Control, Entry Zone, Supervisory Control, and Outside World. The *US Transportation Security Administration's Pipeline Security Guidelines* places the scope of applicability based on its criticality to the pipeline system. Risk Assessment Approach and Methodology, page 62 explicitly notes that the range of assets to be identified and classified (and in turn have access control policy applied) is done according to their criticality to *safety and/or reliability*.

We will reference the base pipeline architecture in Figure 30 below.

Figure 30 Cisco, Schneider Electric, and AVEVA Base Pipeline Architecture



Consider the following additional systems and participants for assessing the needs of your access control policies:

- ERP Systems such as SAP/HANA; Oracle Business Systems
- Manufacturing Execution Systems (MES) Systems
- System Integrator and engineering firms
- Major equipment vendors
- Cloud-based repositories of telemetry information
- Telecommunication providers

Our recommendation here is to define scope according to your working conditions, but make note of potential risks/threats that may exist beyond your specific SUC.

Enabling Access Control—AAA Systems

To enforce access control policy, a clear mapping between the participants (users, applications, devices, services) plus a means of enforcement must be made. For many instances, an AAA server provides these needs. In older systems, RADIUS is a popular means of establishing the needed relationships for network participation. Systems that are more modern will typically use a directory service such as Active Directory to provide the requisite relationship definitions. Depending on the age of the organization's pipeline control system, it is very possible that both systems will offer a blend of benefits when working in conjunction with one another.

A Note Regarding Access Level Needs

The following concepts are important to consider for access levels:

- Least privilege is the minimization of rights or permissions to an accessed object or function. The minimum necessary levels of capabilities necessary to perform the role should be authorized.
- Uniqueness of rights associated with the system and its components is desirable as well.
- Separation of duties is also a key concept to be applied to access control policies.

Access Control Types

Access control is as dynamic as are the participants associated with the pipeline system. Varying levels of systems within pipelines means varying levels of access control needs. As with all things related to security, as long as any change to the devices, software, or users is possible, security is never " finished." Workers leave, subcontractors switch jobs, software components change, and devices are upgraded with new features. Thus, we must understand that access control management is a recurring activity. Access control activities are built on policy and are applied to items within your asset / participant inventory. Changes to the inventory of assets and participants should trigger questions about whether those changes should require an access control action.

This section of the chapter will focus on the different types/levels of asset access control.

Role Based Access Control

Before discussing the levels and means of enforcing access control, we will discuss a common means of describing the relationships, which determine access policy. RBAC provides a level of abstraction to make these necessary security definitions more efficient and, in turn, more manageable.

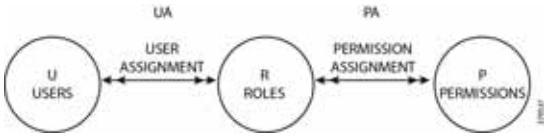
The goal of RBAC is to establish access or permissions to an asset or capability based on roles within the system. In short, users are assigned roles, which then determine the scope of permissions relative to an asset or capability.

Many ways exist to determine what the relationships are between roles and the asset capabilities. It could depend on tasks the user or device must perform. Organizational hierarchy could influence the model, qualifications (user is certified to use certain equipment), or other attributes of the user. The specifics are the responsibility of the organization with influences from the standards and regulations under which they must operate.

RBAC is referenced in multiple best practices associated with petrochemical and pipeline operations. Example reference documents are DNVGL-RP-G108 (a classification enterprise based in Norway); NIST Guide to Industrial Control Systems (ICS) Security; and Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry from the Interstate Natural Gas Association of America.

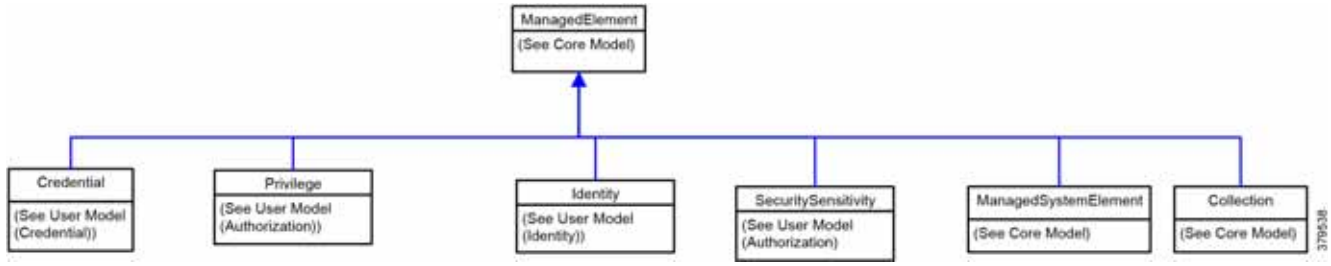
NIST researchers, who formally defined RBAC in *The NIST Model for Role Based Access Control* provide the following simplest representation (Figure 31) of the relationship between users, roles, and permissions.

Figure 31 RBAC Relationships (Source: NIST)



The Common Information Model (CIM) of the Distributed Management Task Force (DMTF) (Figure 32) provides formal models for describing the relationship between roles/users and the resources they would use:

Figure 32 CIM Model[1]



The NIST official reference is *INCITS 359-2012: Information Technology - Role Based Access Control* at https://standards.incits.org/apps/group_public/project/details.php?project_id=1658 that you can purchase for deeper understanding in a more formal format.

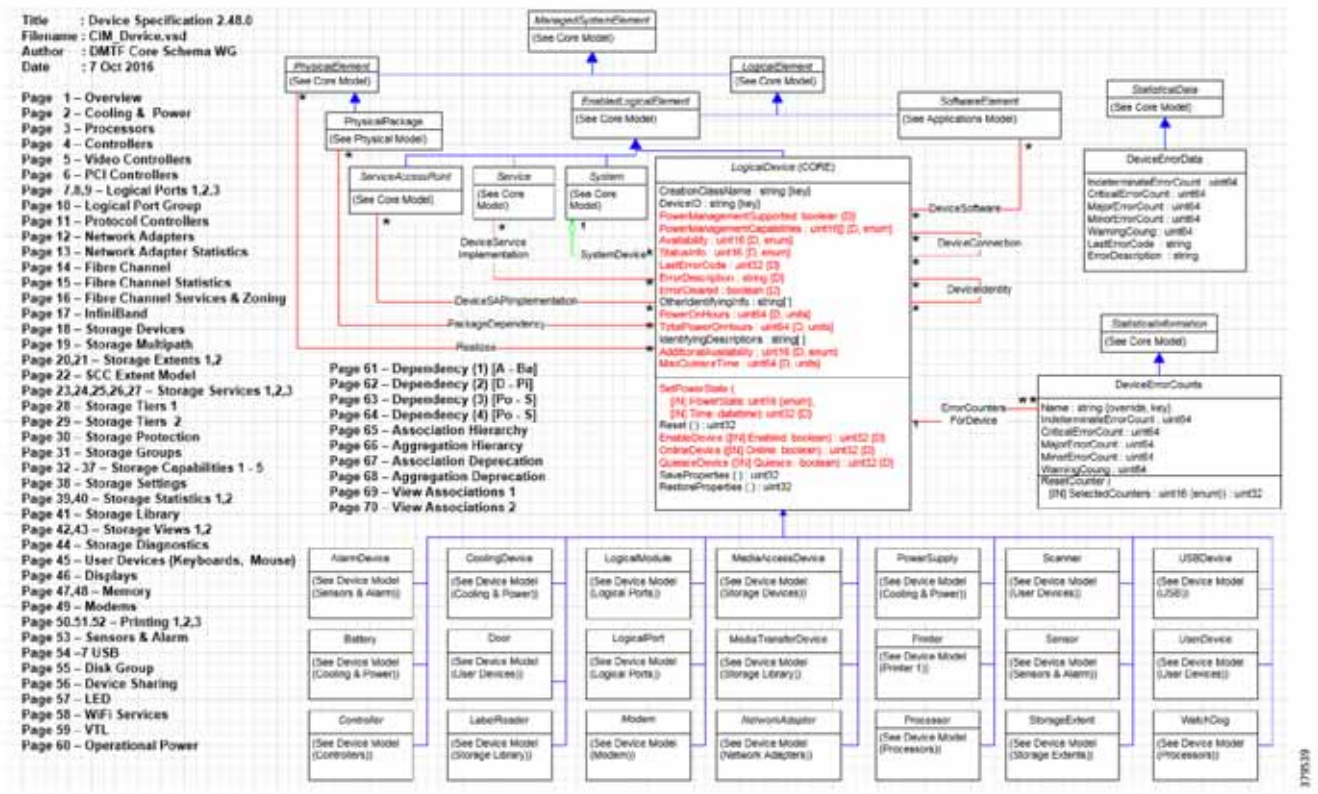
1. https://www.dmtf.org/standards/cim

Device/Object Access Control

Every system and every device is comprised of sub-parts, which may have their own forms of accessibility. A standard PC, which is often categorized as an endpoint, has multiple means of access and thus might be considered yet another set of sub-devices that may require levels of access control policy.

Consider for a moment the DMTF CIM for a device, as shown in Figure 33:

Figure 33 Device Common Information Model[1]



Note that this has 70 pages of specifications, multiple pages of which describe potentially externally accessible components. Some of these do present options for external access to the base system; e.g., USB and User Devices. The scope of access control on a micro level suggests these questions:

- To what level of specificity do you wish to create policy that reflects access to this specific device and then the different levels of the device?
- Are these within your organization's ability to define and maintain specificity and enforcement?

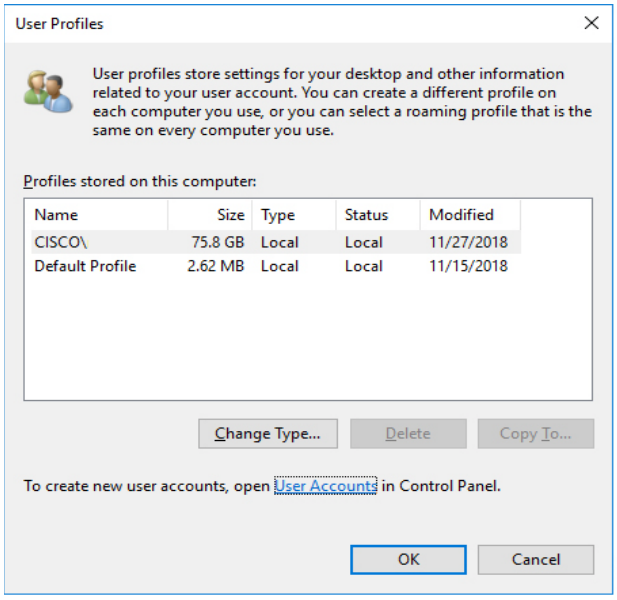
System hardening, discussed in System Hardening, page 90 of this document, may address some of these issues. Some potential overlap occurs between access control and endpoint hardening. Formally, they have different meanings, but the goal is the same: strengthening the security state of the endpoint.

Discussions of physical media and physical access are outside the scope of this chapter.

To achieve control over the diverse needs of device users, devices should have multiple unique and access-controlled accounts on the device. Figure 34 shows how this is done in Microsoft Windows User Profiles. As noted earlier, minimal necessary access across uniquely functional roles should be applied. This is also known as the principle of *least privilege*. This is part of the system and device hardening process, which later sections of this document will cover.

1. https://www.dmtf.org/standards/cim

Figure 34 Microsoft Windows User Profiles



Recognize that access rights within a compute-capable endpoint, such as a desktop, laptop, or server, should vary according to the role and needs of the user.

The person with responsibility for maintaining the operational state of the device (usually called the Administrator) should have the means for manipulating all of the elements described in the above example CIM model. These represent components of the device itself. The operating system controls are likely under the control of the same administrator.

Administration rights on a device should not automatically equate to full rights for the applications present or accessible from that device. Implementation of a secondary authentication / authorization service for hosted applications produces a greater degree of access control. We discuss application-level access control later in this section.

Providing multiple appropriate OS level accounts, which provides for greater segmentation opportunities, is safer, but also requires greater administrative overhead unless they are automated and/or centralized.

Device-level access control can be achieved with either broad or finely tuned policy work. Policy will only succeed with proper investment in management and device capabilities that support the level of policy desired.

Network Access Control

Network Access Control (NAC) is a security practice that applies policy to an endpoint for network participation conditions.

An endpoint may connect to the network through physical or wireless communication ports; policy then is applied to the port, which determines the conditions in which that device can participate on the network. At its most stringent, a deny action may be applied. More commonly, some set of access definitions are applied allowing for some subset of the network topology, either physical or virtual, to be reached.

NAC came into general commercial availability around 2005, with adoption largely driven by standard IT environments and focused on PC-based architectures. As personal computing endpoints continued to expand, the administrative burden of dealing with the proliferation of new endpoints drove network administrators to consider the value of automating network participation. Handling transient compute such as laptops in wireless environments and visiting guests were early drivers for NAC's adoption.

NAC is enabled normally through features commonly found on modern networks and computing endpoints. The basic model has a supplicant on an endpoint connecting to a switch, which acts as an authenticator and access enforcement mechanism. The switch communicates with an authentication system, which provides the appropriate verdict, and, in some cases, special access policies appropriate to the endpoint.

Most modern networks use the 802.1X standard protocol to enable NAC. Common platforms such as Windows, Linux, and Apple-based products have appropriate supplicants available. Similarly, network infrastructures are capable of working with these standards.

In some cases, the endpoints may lack the ability to work with 802.1x. In this case, MAC Authentication Bypass (MAB) may be an option. With MAB, a predefined list of MAC addresses is on the authentication server along with appropriate network access condition policies. If the MAC address is found, then policy is normally applied allowing for network participation. If the MAC address is missing, then the appropriate policy is applied with a likely constraint such as no access or highly constrained access.

NAC policies can be highly flexible depending on the capability of the policy source and enforcement points. Access policies can consider the security state of the endpoint. As an example, if the device is a Windows class machine, it can be checked for patch updates and the presence of advanced malware protection software as a condition for access to certain assets. Some policies and tools could restrain the ports over which the device can communicate such as SMBv1, the protocol by which the Petya/Not-Petya malware propagated itself.

Mobile connectivity requirements and third-party participation in a connected system, such as a distributed pipeline environment, make NAC a potentially valuable technology for addressing access control needs. In this case, access control refers to participation on a network. Automating policy provides inherent efficiency improvements and the 365/24/7 pipeline operating conditions makes that value all the greater. In an urgent situation at a remote site, a previously unplanned activity cannot be delayed awaiting a manual intervention by a network administrator yet at the same time, it can be challenging to differentiate between legitimate ad hoc access and undesired access. NAC can help in these conditions by automating access policies for these situations.

A challenge for NAC is likely to exist amongst devices with direct connectivity to pipeline equipment. The age of the devices and their compute resources may constrain them from using the more advanced capabilities of NAC.

Some platforms such as Windows XP may be constrained in their ability to work with 802.1x; Windows releases that are more modern have default operations with full support.

Reviewing the asset inventory that has been built to determine those assets that are likely to benefit from a NAC deployment is a valuable exercise. The more modern and "IT like" the asset set and environment, the more probability that NAC can contribute.

As noted though, some assets, including some relatively modern TCP/IP-based controls such as sensors, may not provide for 802.1x supplicant support.

This does not preclude the use of NAC, since an accurate and robust asset inventory can provide enough information for using MAB, but that assumes your asset inventory exercise has been successful.

NAC has powerful and automated policy capabilities using the network infrastructure itself to determine and enforce participation in the pipeline system network. NAC requires a generally modern level of endpoints and network infrastructure to succeed and, as such, may be applicable to a subset of the overall pipeline environment. NAC's power also means that it needs to be used judiciously in environments where communications are critical. A best deployment approach would be to phase this capability in starting with standard IT equivalent environments.

Device/Network-Based Application Control

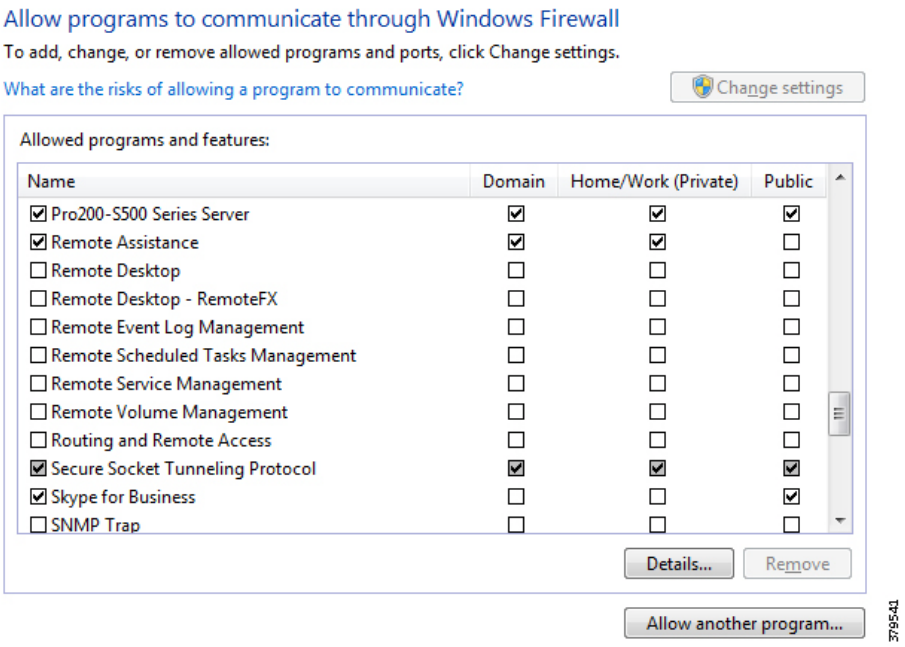
Applications can be local to a device or operate across a set of devices. Evaluate any application that can directly influence pipeline operation or that represents a risk to the pipeline for inclusion within a formal access control policy. Therefore, in these cases, access refers to use of the device or system's applications.

Some assets, such as compound applications, are distributed across multiple physical compute devices and in some instances, such as virtualized environments like the cloud, have no user discernible association with a particular device. In these conditions, control of access to the applications can be applied locally, over the network, or within the application itself (as covered in the next section).

At the device level, the operating system may allow applications to be accessed according to device user account settings. It cannot be assumed, however, that all applications are under that level of granular control. In those instances, the question comes to whether the application should be allowed on the device.

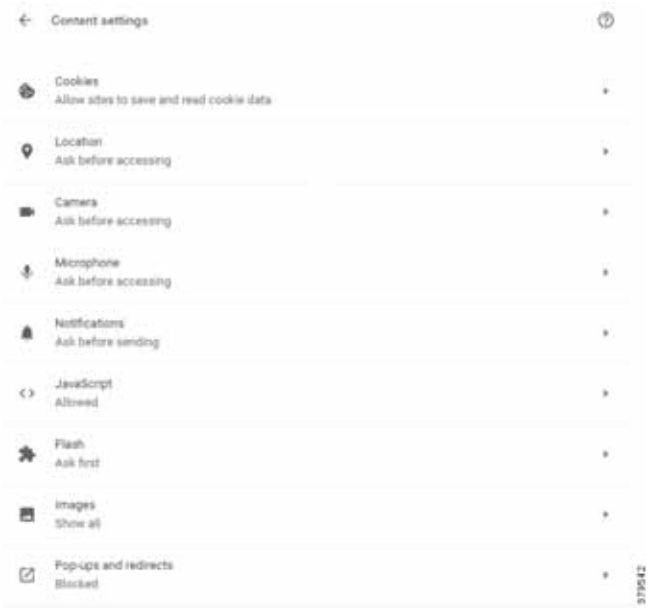
As an example, on Windows, one can optionally select applications present on the device and determine if they can communicate outbound from the device via the Windows Firewall, as shown in Figure 35.

Figure 35 Windows Firewall Application Settings



For web-based applications, opportunities exist to blacklist and whitelist URLs and classes of downloadable content, as shown in Figure 36.

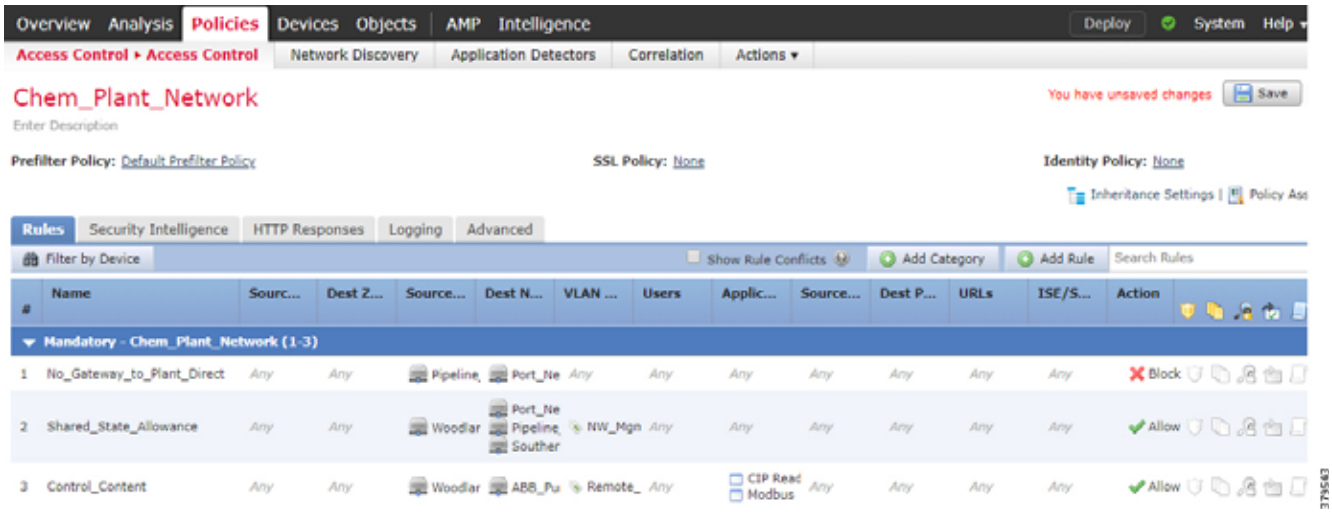
Figure 36 Google Chrome Content Settings



While the Windows Firewall can be used in these areas, the impact of leveraging such features on the control systems must be validated. Control system applications include many outbound communication activities via ports (some well-known and some not), which need to be properly configured or they will negatively affect the stability and operational integrity of the Control System.

Outside of the end device, network control elements such as Next Generation Firewalls (NGFW) can control applications through inspection of traffic as it traverses the environment. As the application traffic crosses the network, NGFWs can see the traffic and determine whether the application itself or even individual behaviors meet policy conditions. Applications can be limited in a number of ways with such simple controls as denying a particular port to be used between two devices, all the way determining if a set point value is outside of a desired range. The method to do this can be as simple as a port-based access control statement or the use of DPI to detect information that is more detailed. Once a match condition is met, the control point can take action. Figure 37 illustrates this capability.

Figure 37 FirePOWER Network Access Control Rules



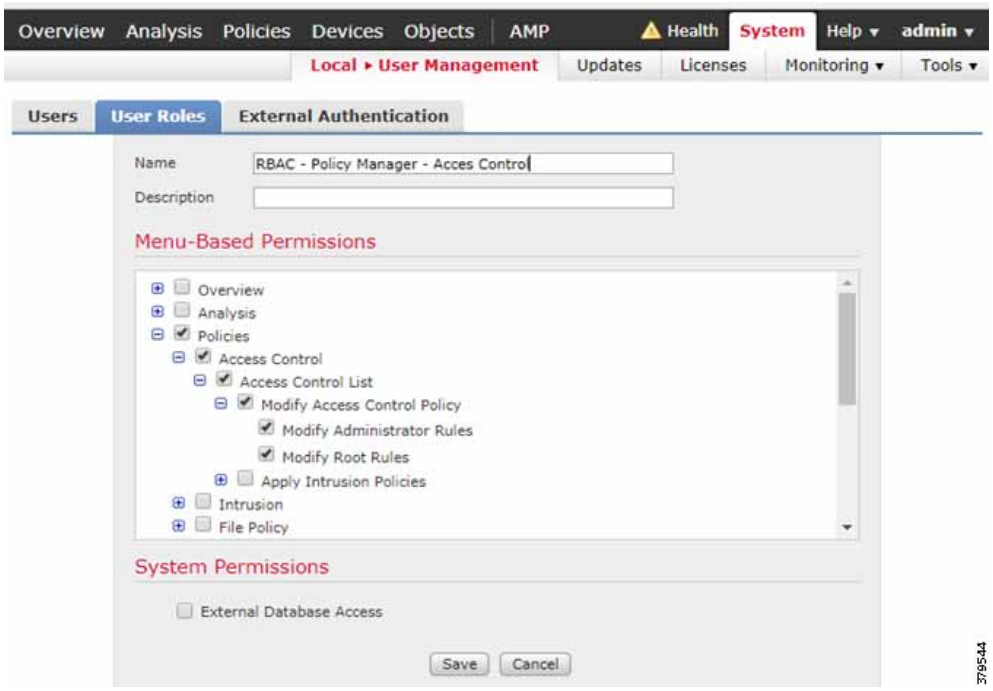
Application controls on devices and within the network provide layers of control to ensure that necessary applications are available to the right local users and can access the correct network elements. From a protection perspective, these controls provide for application-independent enforcement on the endpoints and the broader network. As applications become more distributed, the ability to understand and act on desired and undesired application behaviors could be the final layer of protection as communications progress to endpoints, which lack the sophistication or resources to provide their own defense.

Additionally, these features can figure prominently in enforcing network segmentation, helping to control/restrict the flow of traffic between the segments, enforcing design objectives such as traffic flowing from higher to lower security segments (e.g., Production to IDMZ).

Application Level Access Control

In addition to the physical device components, software applications, which could be independently managed or operated, exist. Keeping focus on the discrete, non-distributed applications unique to the specific device, a user account may be needed that lacks the administrator's device level controls, but is allowed to use specific applications that run on top of the operating system. Management of this level of access can be more precise. It could mean OS level accounts to access the application and/or associated activity and object access rights within an application. As shown in Figure 38, a fine level of control can be seen all the way down to individual capabilities on a screen.

Figure 38 FirePOWER Management Center's User Management



The RBAC discussion earlier in this section largely covers the core concepts aligned with application-level access control. In short, within the application, functions and data sets exist whose exercise and access the RBAC capabilities associated with the application should determine and enforce. The authentication and authorization mechanism may be external to the application itself, but the application should understand the attributes of the user in order to enforce it.

A pipeline operator may use the operator workstation/console to simply monitor the state of the system, but may not be authorized to make any changes to the system. The application understands the end user's role and the logic comprising the application ensures that proper role access is enforced. It is important to note that device level and network level controls often do not know or enforce application-level controls, as they largely are unaware of those constraints.

In AVEVA systems, RBAC is based on Active Directory security group membership where users inherit privileges from the groups of which they are members. These groups are aligned with the role of each particular user and these roles (aka security groups) can then be assigned to Authorities, which define the desired level of Control System application access each user should be permitted:

- An Authority represents a set of required application rights, or Permissions, that the application software validates to enable or disable specific access rights. Permissions are capabilities or rights that define application-level control over user/application actions or functions.
- User groups define access to system objects such as files via Access Control Lists (ACLs), infrastructure applications such as MS SQL Server, or Control System applications and embedded rights related to control.

Policy Definitions

Policy definitions are structured to reflect the environment they operate in and the detection / enforcement mechanics of the associated control point.

As an example, the Chrome Browser allows for control of browser access for a particular application within its control realm—the specific instance here was whether Flash-based content could run without manual intervention. The policy definition was limited to a simple set of options. Similarly, the Windows firewall-placed local control rules regarding the environment with which application components could communicate outwardly, using simple generic references to the environment within which the computer was operating.

In the Network Access control reference, the image referenced a standard source/destination design, but applied an application-level awareness for communications accepted or denied through the NGFW.

Given the different levels of access control and the equally different policy statements needed to enforce access control, it becomes apparent that the full range of controls may be beyond any one individual for an entire pipeline. It is likely that multiple groups with administrative rights exist on the asset sets comprising the pipeline. From devices, to local applications, to networked assets, to compound applications the complication will simply multiply.

The security practitioner must determine what is within their ability to scope, execute, and manage, and whether to manage those access control policies centrally or delegate controls to appropriate groups. Centralization has the benefit of knowledge, which helps with coordination and debugging or communications issues. Decentralization has the benefit of allowing local expert knowledge that is unique to the specialized needs or operations of the environment.

Establishing Identity and Permissions

Access control assumes that:

- Proper identification of assets and their users
- Policies associated with the roles aligned with assets and users are available to the enforcement elements.
- The enforcement of those policies is possible with the control mechanisms available.

Directory services are common tools to provide authentication and authorization of users; e.g., the user is whom they said they are and therefore is authorized to exercise permissions associated with the asset set described in the policy.

This chapter will not discuss the infrastructure implementation details other than to note that that functionality should be available to every element to which one wishes to offer control.

Special Challenges to Access Control within Industrial Control Systems

Access control policies will only work when the group desiring to enforce them has the technical tools and is itself authorized to act.

In some cases, assets or systems are off-limits to access control changes beyond what was originally in the box. A specialized machine or functional area may have been accepted with contractual obligations preventing manipulation of certain or all sub-elements. Such conditions are much more common in the ICS space than in IT and security practitioners should be aware of any examples within the pipeline system, making the capturing of these subtleties part of the overall asset inventory process.

Summary

Access Control is a fundamental security practice for any system and is of particular value for such physically distributed and diverse participant sets as seen in pipelines.

Successful access control builds on the asset inventory. The more complete the asset inventory, the more likely is the completeness and success of an asset control exercise.

The diversity of the assets involved makes for a complex set of policies and controls in order to enforce access control. Organization, contractual, and technical impediments may exist within the broader pipeline system. The organization's willingness to invest in policy creation, enforcement mechanisms, and ongoing maintenance will determine the likelihood of success.

Industry Standards Cross-Reference: System Access Control

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 5 (FR1) Identification and Authentication Control
IEC 62442-3-3 Part 6 (FR2) Use Control
NIST SP 800-53 PE-20 Asset Monitoring and Tracking
NIST Guide to Industrial Control Systems (ICS) Security, Section 6.2.1.1
NIST Guide to Industrial Control Systems (ICS) Security, 6.1.6 Access Control
NIST Model for Role Based Access Control: Towards a Unified Standard
NIST Assessment of Access Control Systems
ISO 27001 Section A8 Asset Management
ISO 27001 Section A9 Access Control
ISO 27001 Section A9 Business Requirements of Access Control (subsection A.9.1)
ISO 27001 Section A9 User Access Management (subsection A.9.2)
ISO 27001 Section A9 User Responsibilities (subsection A.9.3)
ISO 27001 Section A9 System and Application Access Control (subsection A.9.4)
API 1164 5 System Access Control
API 1164 8 Field Communication, System Access
TSA Pipeline Security Guidelines, Section 5 System Access Control
Cyber security in the oil and gas industry based on IEC 62443 DNV-GL September 2017

System Hardening

System Hardening Defined

System hardening, within the realms of Cyber Security, can be defined as reducing the attack surface or vulnerability of a system and making it more resilient to attack through hardening measures. Hardening activities typically include disabling unnecessary services and applications, providing least privilege user access to systems, and adding additional security features such as anti-malware, anti-virus, and endpoint security systems. For the connected pipeline, protection needs to be applied across servers, workstations, PLCs, applications, operating systems, networking, user access, and at the physical layer of devices across the end-to-end architecture. This includes the control centers, the WAN communication infrastructure, and the pipeline stations. Generally, the hardening policies and procedures can be applied to multiple areas:

- Mitigation techniques such as patching a system and installing anti-malware software
- Removal of unneeded users and high privilege users during install and configuration of the system
- Locking down and removing unnecessary services and ports
- Restriction of Privilege so that each task, process, or user is granted the minimum rights required to perform their job and are not allowed access to functions or information that is not necessary or beyond their roles.

Also, these areas require ongoing maintenance and review and should not to be considered a one and done set of activities. For example, as users transition in and out of roles; e.g., because of promotion or change of department, users' security access controls must be reviewed and updated as necessary.

A system is only as strong as its weakest component and therefore system hardening needs to adhere to a defense-in-depth methodology with multiple layers of protection to shield the operations of the pipeline.

What We are Trying to Solve

Traditionally, ICSs relied on air gap security measures to help secure their systems. Pipeline systems may be far more open and susceptible to attacks because of the following: the adoption of IoT, shared infrastructure between operational and non-operational systems, and connectivity or integration to corporate networks, the internet, and COTS systems now entering the industrial domain. Pipeline operators that choose to adopt the *air gap* approach are not eliminating all risk. Vulnerabilities exist that can still be exploited locally. Therefore, security measures such as system hardening are still relevant in these deployments as well. The aim of system hardening is to eliminate as many security risks as possible by reducing the attack surface. Hardening procedures and policies must be applied to protect against intentional attacks such as an attacker accessing a server through a back door for information or unintentional attacks such as when a user unknowingly plugs an infected USB stick into a server.

In alignment with the key standards, it is clear that technology plays a major part in securing the system; however, technology only provides about half of the coverage for security threats. People and process play a critical, and often unrecognized, role in all aspects of securing the system. The pipeline system must combine all three areas-technology, people, and process-to provide a comprehensive strategy and implementation for system hardening.

Process

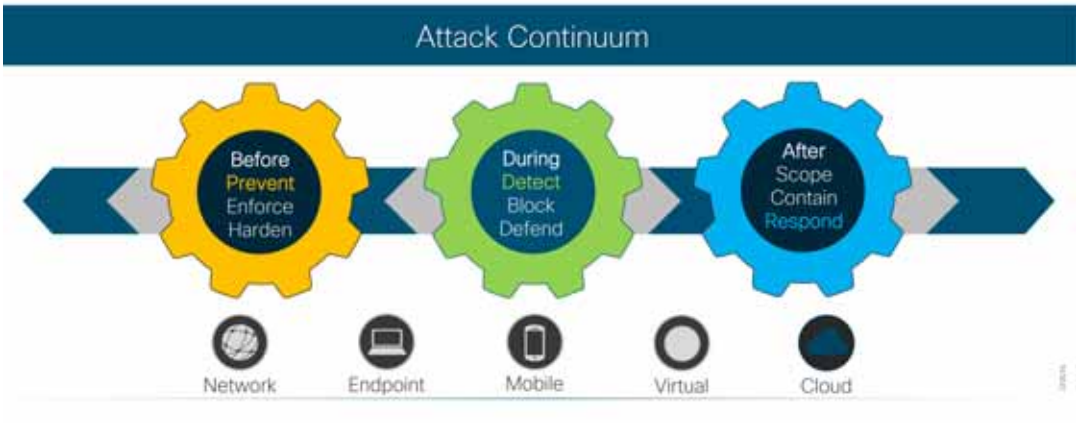
For a greenfield implementation, it is generally easier to add security and security hardening when designing the system, and as such, hardening activities should be identified as part of the initial planning and designing of the system. It is much more difficult, and generally more expensive, to implement security after a system has been deployed, such as in a brownfield installation.

Security Process Lifecycle, page 17 highlights that the security process cannot be isolated and reactive, but must take a proactive and holistic approach to addressing system security. In alignment with these objectives, the process can be broken into three phases that address the attack continuum and protect the system.

The application of security controls is how hardening happens. SANS defines security controls as technical or administrative safeguards or countermeasures that are used to reduce the risk of attack, data loss, or system unavailability. The process is to match a control to the vulnerability or risk, thereby creating a way to clearly address individual security risks in an industry-recognized manner[1].

Using the Prevent (Identify and Protect), Detect (Detection and Monitoring) and Respond (Respond and Recovery) security controls (as shown in Figure 39) we can align components of the process for security hardening. Although most of the implementation of hardening is defined and deployed in the Prevent phase, system hardening practices and procedures hit all three phases of the security methodology.

Figure 39 The Security Continuum - Prevent, Detect and Respond



Prevent

In order to start the hardening process, as with most of the other functional areas, it is extremely important to have an inventory of components, users and data flows for the system. The inventory discovery, previously discussed in Asset Discovery and Inventory, page 49, is a component of an overall Security Risk Assessment. This inventory of data collected for the pipeline system will then help define which system hardening policies, procedures, and processes to implement based on a vulnerability assessment. The asset inventory and vulnerability assessment, aligned with any governance or business practices, forms an overall risk management strategy with policies and procedures for implementation. Ultimately, at this phase, system hardening for the pipeline system should be well planned, tested, and documented before implementation.

The Protect function will implement the technologies and procedures to protect the pipeline system, such as removing unnecessary services from the SCADA servers and PLCs and implementing anti-malware technologies and endpoint security. Again, these areas should be addressed before initial deployment and then regularly reviewed throughout the system's lifecycle. These continuous reviews prevent a scheduled upgrade or expansion from inadvertently opening a port or enabling an unnecessary service.

Detect

Ongoing maintenance, monitoring and detection of the system are extremely important activities. This is covered in Security Operational Management and Monitoring Defined, page 132 through which the information feeds into the system hardening strategy, such that a plan for mitigation and improvements of any detected anomalies can be planned and implemented. It is important to remember that security is a continuous improvement process, requiring ongoing activities that address new system threats and emerging risks. Based on a review of Common Vulnerabilities and Exposures (CVE) details, more than 14,600 vulnerabilities were reported in 2017, versus 6447 in 2016[2]. These numbers, which are truly astonishing, serve to highlight the need for continuous vigilance.

1. Northcutt, S. (2009, September 1). Security Controls. Retrieved from SANS: https://www.sans.edu/cyber-research/security-laboratory/article/security-controls

Respond

Following a compromise of the pipeline system, resolution of the incident (cyber, environmental, or other), and restoration of the system to operation, a plan for improvements to the comprehensive system hardening strategy needs to be made. An After Action Report (AAR) will help to consider what actions could have been taken to have prevented the attack, mitigated damage, and improved the business' overall response to the incident. An example of a finding could be that a vendor may need to provide a security patch or a Windows update may need to be applied to the SCADA system. This would need to go through evaluation and testing in a non-operational but representative environment before implementing into the operational pipeline system. As part of the incident postmortem, it is necessary to consider if shortcomings occurred in the existing security processes. For example, was there a weakness in the patch management process, or was there an unintended network connection that violated network sectionalization, enabling an attacker to access systems that should have been unreachable? Lastly, were there weaknesses in physical security or access controls at the field level, enabling an attacker to move up into the system via proprietary pathways? Whatever the reason, it is paramount that the vulnerability at the root of the compromise be honestly addressed in order to prevent future compromises by a similar attack vector.

Technology

The same principles, and to an extent a large amount of the same procedures, are required to harden both the network and the devices accessing the network in a SCADA environment. This next section breaks down the hardening technologies and procedures into Server, PLC, and network hardening, as well as possible approaches to consider with legacy devices, which generally have few, if any, hardening capabilities.

SCADA Server, PLC, Engineering and Operator Workstations, Industrial PCs

Patching and Upgrading Operating Systems

To reduce vulnerability to attacks, systems should be patched to the latest vendor-recommended software and firmware levels. This is particularly true with computer systems, such as SCADA hosts, that provide an element of control, access, and isolation for the deeper layers of the industrial control networks. It is also true of devices on the control and field level networks.

A plan for implementation of patches should be considered. A secure, trusted, and regular retrieval and deployment of patches from the vendor or supplier should be implemented. Where possible all patches should be tested and evaluated before pushing into the production network. A plan for an infected server should be considered until it can be patched (backup, quarantine, isolation). This latter step should be part of a broader and more comprehensive incident response plan, aligned with an overall business continuity process.

Malware and Anti-virus Protection

In a well-defined secure system, the people factor, whether intentional or unintentional, still plays a major role in attacks. For example, a user could open an attachment from his Gmail account on a Decision Support workstation, which triggers some form of malware, which is now infecting his system or possibly other systems within the IDMZ. Anti-malware and anti-virus software on the host could help to defend against this type of attack. It is recommended that a comprehensive anti-malware program be instituted and that any system with an interface to the ICS be required to have it installed and up to date.

Removing or Disabling Unnecessary Services Applications and Network Protocols

Remove or disable (when unable to remove) all services, applications, and network protocols so that the server is reduced to a minimum configuration for its purpose. Examples include IPv6, Web servers and services, email services, Telnet, print services, and remote services if not required.

2. Mendoza, M. (2018, February 5). Vulnerabilities Reached Historic Peak in 2017. Retrieved from We Live Security: https://www.welivesecurity.com/2018/02/05/vulnerabilities-reached-historic-peak-2017/

Removing Unnecessary Hardware and Secure Physical Ports (USB ports, CD/ROM)

System hardening must provide guidance to disable access mediums, as open ports may provide unsecured access to the system. For example, removing or disabling USB ports will reduce the entry into the system for potentially infected software or for someone to take data off a server or device.

OS User Authentication, Least Privilege Access.

Access Control, page 99 includes the bulk of coverage of user access configuration and least privilege access. However, aspects of providing user authentication should be covered under System Hardening and be listed as part of the policy and procedures. This includes removing unneeded default accounts that come with a system, such as those where the names and passwords are well known (guest accounts, admin, or root level accounts). If these accounts are required, then severely restrict their access. Provide accounts for only necessary functions. This includes vendor accounts that are used to grant general access during the project implementation–these must be managed with access control in mind as the system moves into production.

Create user groups and user accounts and assign least privilege access depending on the function or support required. This should be performed in coordination with the access control policy and procedures. For example, a pipeline operator would not require debug access to troubleshoot SCADA servers, but would still require access to the servers to retrieve data. As such, the operator would configure access controls in order to align with this policy directive.

Policy should also address passwords. It is important to consider the frequency that passwords are changed, their complexity versus convenience, the minimum time between changes, and other related configuration that helps to create a password policy that addresses the needs of your specific organization.

Network Structural Security

The following items are used to help create a robust network infrastructure, enforcing segmentation and defense in depth, restricting the flow of traffic between segments, and helping the OT/IT staff charged with managing and protecting the network:

- Host-based Intrusion Detection Systems (IDS) and Vulnerability Management software to detect any attacks performed on the server such as denial of service attacks or changes to any critical files within the system. The Host IDS will generally monitor log analysis, file integrity checking, and Windows registry monitoring and resource monitoring to help identify attacks. It is necessary to note that Intrusion Prevention Systems (IPS) should not be used within the production environment, as it could identify control traffic during an upset condition or other normal traffic as malicious and take actions to protect the system, possibly isolating the control system from the field and preventing the ability to control the pipeline. Both host and network-based IDS systems are used to help identify potential attacks; therefore, it is crucial that active monitoring and alerting on attack warnings be a component to the overall strategy to identify and respond to potential cyber incidents quickly.
- Firewalls should be used to facilitate the isolation of functionally secure network segments, for example, between the primary and backup control centers, the control networks from the Decision Support segments (aka IDMZ), and to protect the Production environments from the Test and Development segments, ensuring that no cross-network traffic that could affect operations. The firewall rules should ensure that traffic moves from most secure to least secure network segments. Rules should consider traffic protocol restrictions, along with controlling network address sources and targets.
- Smart Switches should be leveraged to isolate network segments via VLANs, in that way helping to create secure areas within the operational networks and to control traffic from moving into areas that should support only related traffic. All of this helps to prevent unauthorized access to/from certain areas of the network.

Data at Rest Security/Encrypted Hard Drives

A need may exist to encrypt data stored on the hard drives so that data is protected from attackers that may gain access to the physical system. The distributed nature of the pipeline architecture may enforce encryption of data at rest in unmanned environments where a potential threat to remove hard drives/data exists.

In many ICS environments, data encryption for data at rest carries performance risks; therefore, some vendors do not leverage these types of features. For example, if a server or workstation had an encrypted drive that required password approval to make accessible at boot, a pipeline operator could find that a server or operator workstation would not recover from a restart failure, possibly prohibiting or restricting the secure operation of their assets. This is not an option for many operators; as a result, it is important for organizations to consider the risk/reward equation, which will help decide which policies fit your risk profile.

Alerting, Logging, and Integration to the Security Information and Event Management (SIEM)

Logging is a cornerstone of a sound security posture. The endpoints, in alignment with their feature sets, need to be configured with logging capabilities and reporting functions to a centralized security management system. Syslogs, along with SNMPv3, should be enabled to report any events or incidents discovered at the endpoints. The type of agents and/or reporting approaches should be considered holistically, specifically as they relate to overall system performance and their possible negative impacts. Again, consider this all within your risk/reward framework.

Secure Networking Protocols and Data in Motion

If File Transfer Protocol (FTP) communications or access to devices are required, the use of secure encrypted versions of any networking protocols to access servers are recommended: for example, Secure File Transport Protocol (SFTP), Secure Copy Protocol (SCP), Secure Shell (SSH), and Simple Network Management Protocol version 3 (SNMPv3). For communication within the operations network and between related segments, organizations should consider IPSec (Internet Protocol Security), Secure Socket Layer (SSL), Transport Layer Security (TLS), and Hypertext Transport Protocol Secure (HTTPS) for securing operational data exchanged between nodes within the operational system.

Device protocols should also be considered in this area, although this presents a greater challenge since many typical devices and their protocols have limited (or no) in-built security capabilities. Where encryption or protocols that support advanced features are available, the vendors of the control system and the devices should be engaged to explore how to deploy advanced features within the operational system. Common protocols or devices have been exploited because of misconfigured network components; for example, internet access within L1 and/or L2 opens up external access to these network components. In brownfield solutions, older devices will not have secure features in their communications nor will they support external security options like bump-in-the-line encryption; therefore, isolation and defense-in-depth approaches are going to be critical in protecting the field from exploitation.

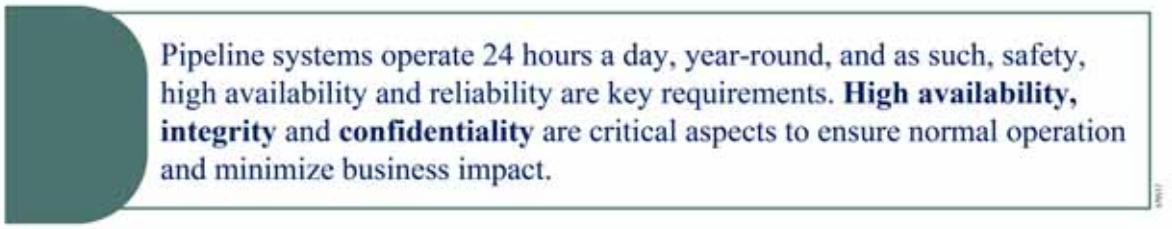
Vulnerability Scanning

Vulnerability scanning usually involves using an automated vulnerability scanner to scan a host or group of hosts on a network for application, network, and OS vulnerabilities. Organizations should conduct vulnerability scanning to validate that OSs and server software have up-to-date security patches and software versions. When choosing a solution, be aware that some of these tools may be invasive or negatively affect the network (i.e., performance); therefore, the timing of their use and their configuration should be considered when used in the Production environment. As with all aspects of managing the control environment, Test and Development environment verification should be undertaken before deploying the tools and processes into production.

System Availability for Critical Components

Pipelines must operate 24 hours a day, year-round, and as such, PMSs and the supporting infrastructure require safety, high availability, and reliability. Availability, integrity, and confidentiality are three critical aspects that ensure normal operation of the operations system and help avoid negative effects on the business. Ensuring availability through critical component and resource redundancy is a cornerstone of any system hardening design:

- Redundant Hardware, Servers, Workstations, Storage etc.
- Redundant power
- Server Backups
- Data Backups and redundancy



Network System Hardening

The majority of the hardening mechanisms mentioned in the previous section carry over into the network hardening implementation. Least privilege access control, disabling or removing unused services, logging, and secure protocols are all configured in some capacity and need to be configured across the three functional planes within a networking system. These three functional planes of a networking system that require hardening and securing are the Management Plane, the Control Plane, and the Data Plane.

- **Management Plane**—The management plane provides access to the networking devices to allow for management of the networking system. The management plane manages traffic that is sent to a networking device and is made up of applications and protocols such as SSH and SNMP.
- **Control Plane**—The control plane of a network device processes the traffic that is critical for maintaining the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, which include the routing protocols.
- **Data Plane**—The data plane forwards data throughout a networking system, traversing the networking devices. The data plane does not include traffic that is sent to the local networking device.

The following provides an overview of the hardening technologies and guidelines that should be adopted for the operational systems. More details can be found at the following links:

- https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- https://www.cisco.com/c/en/us/about/security-center/securing-nx-os.html

Management Plane

The management plane consists of functions that achieve the management goals of the network. This includes interactive management sessions that use SSH, as well as statistics gathering with SNMP or NetFlow. When you consider the security of a network device, it is critical that the management plane be protected. If a security incident undermines the functions of the management plane, it may be impossible for you to recover or stabilize the network.

The management plane is used to access, configure, and manage a device, as well as monitor its operations and the network on which it is deployed. The management plane is the plane that receives and sends traffic for operations of these functions. You must secure both the management plane and control plane of a device, because operations of the control plane directly affect operations of the management plane.

The following sections highlight some of the key technologies that help secure the management plane.

Disabling Unused Services

A number of unneeded services, especially those that use User Datagram Protocol (UDP), are infrequently used for legitimate purposes, but can be used to launch DoS and other attacks that are otherwise prevented by packet filtering. TCP and UDP small services must be disabled, but SSH, SNMP, and Network Timing Protocol (NTP) are essential services for running and managing a network and are enabled by default. If unneeded, they can be individually disabled.

Access Control and Least Privilege Access

The following list describes in further detail what types of access controls are applicable at this level:

- **Least Privilege Access and AAA**—User authentication must be covered under system hardening and listed as part of the policy and procedures. This includes removing unneeded default accounts that come with a system where the names and passwords are well known (guest accounts, admin, or root level accounts). If these accounts are required, then severely restrict their access. Provide accounts for only the functions that are required. The AAA framework, which is critical in order to secure interactive access to network devices, provides a highly configurable environment that can be tailored based on the needs of the network

- **Configure a Management Interface**—Add a loopback interface as a management interface to each device. This interface is a logical interface so, unlike a physical network interface, is essentially always seen as available. It should be used exclusively for the management plane. Secure with Management Plane Protection such as infrastructure access control lists or an equivalent technology to designate and allow management communications to only this single interface.

- **Configure Infrastructure Access Control Lists**—Devised to prevent unauthorized direct communication to network devices, infrastructure access control lists (iACLs) are one of the most critical security controls that can be implemented in networks. The access control lists filter network traffic by controlling whether data is forwarded or blocked at the network device interfaces. Your device examines each packet or data frame to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.

Configure Secure Networking Protocols for Access to the Networking Equipment

Because an interactive management session can disclose information, this traffic must be encrypted to prevent a malicious user from gaining access to the transmitted data. Traffic encryption allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in cleartext, an attacker can obtain sensitive information about devices, operations, and the network. SSH and SNMPv3 encrypt packets over the network, thus providing security from inadvertent disclosure to unauthorized users.

Network System Logging

In order to gain knowledge about existing, emerging, and historic events related to security incidents, networking devices should be logged and monitored. Ultimately, the organization should move to a centralized logging implementation and develop a structured approach to log analysis and incident tracking. Based on the needs of your organization, this approach can range from a simple diligent review of log data to advanced rule-based analysis, which will include more than just network device based monitoring/logging.

Backup Device Configuration

All network device configuration should be backed up after initial installation, setup, and following modifications. Depending on the frequency of configuration changes, a policy should be put in place to determine how often backups of the devices should be made. Backups provide a quick way to restore a previously known good configuration, resulting in less downtime when replacing network devices after failures or providing for quicker implementation when new devices are added.

Control Plane

The CPU of a network device processes the traffic that is critical for maintaining the functionality of the network infrastructure within the control plane. The control plane consists of applications and protocols between network devices, including routing protocols. It is important that events in the management and data planes do not adversely affect the control plane. Should a data plane event such as a DoS attack affect the control plane, the entire network could become unstable. In addition, control plane traffic needs to be understood and protected so that abnormalities do not affect the performance of the network device's CPUs, thus making the networking device unstable and creating/contributing to network-wide instability.

Process-switched traffic or traffic that requires processing by the CPU are attack surfaces for network instability. Some data plane traffic requires CPU processing. This traffic may not seem high within the Data Plane, but if all packets need to be redirected to the CPU for processing, this could affect the CPU, which wouldn't be able to fulfill its primary functions.

Control Plane Protection or Policing

Most routers and switches can protect the CPU from DoS-style attacks through functionality equivalent to Control Plane protection or policing. This functionality can be used in order to restrict or police control plane traffic that is destined for the CPU of the network device such that it is not overrun with Control Plane traffic.

Limiting the CPU Impact of Data Plane Traffic

It is recommended to monitor for CPU spikes above 80% while passing " normal" traffic. These events may require a call to action for further design changes. Although not explicitly the Control Plane and more of a monitoring function, this option should be configured on devices in this layer. Firewalls may be more susceptible to CPU performance issues based on packet inspection technologies and other features that may be deployed.

Infrastructure Access Control Lists (ACLs)

ACLs filter network traffic by controlling whether data is forwarded or blocked at the network device's interfaces. Your device examines each packet or data frame to determine whether to forward or drop the packet, based on the criteria you specify within the access lists. Leveraging ACLs can help protect the control plane functional layer of network devices.

Router/Routing Protection

Routing can be compromised in various ways, from the injection of illegitimate routing table updates to DoS attacks specially designed to disrupt routing. Attacks may target the router devices, the peering sessions, and/or the routing information itself. Fortunately, protocols like Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol version 2 (RIPv2) provide a set of tools that help secure the routing infrastructure. The following lists a few mechanisms that will help to harden the router infrastructure:

- **Neighbor Authentication**—When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted source.
- **Routing Peer Definition**—The same dynamic peer discovery mechanisms that facilitate deployment and setup of routers can potentially be used to insert bogus routers into the routing infrastructure. Disabling such dynamic mechanisms by statically configuring a list of trusted neighbors with known IP addresses prevents this problem. This can be used in conjunction with other routing security features such as neighbor authentication and route filtering.
- **Control Plane Policing/Protection**—This option should be configured to help protect routing sessions by preventing the establishment of unauthorized sessions, thus reducing the chances for session reset attacks.

Switched Networks

Within switched networks, it is important to protect the overall switched network from things that cause overall network instability. Mechanisms are deployed in these types of networks to protect the integrity of the Layer 2 switched domains. For example, the Spanning Tree Protocol (STP) can be used within these switched domains to help maintain a loop free topology in a redundant Layer 2 infrastructure. Within Layer 2 networks, root devices exist that help provide information about the stability of the network. Guard mechanisms need to be configured so that these root devices are not changed. Bridge Protocol Data Units (BPDU) Guard and Root Guard are examples that should be configured to help protect the Layer 2 domain and prevent Spanning Tree instability. Through additional configuration options, most modern switches also provide protection of the Control Plane and should be considered for enabling.

Data Plane

The data plane contains the logical group of "customer" application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other similar devices that are supported by the network. Within the context of security, and because the data plane represents the highest traffic rates, it is critical that the Data Plane be secured to prevent exception packets from punting to the CPU and affecting the control and management planes.

Network Encryption

Network encryption technologies should be deployed to protect the integrity and confidentiality of data throughout the pipeline network. At a minimum, encryption should be deployed over WAN links that a Service Provider or another entity outside of the pipeline operator may provide. Encryption should also be considered for use between the control centers and field devices (if practical), between tasks and components of the operations system itself, and between the operations system and other layers such as the IDMZ and corporate networks.

Anti-Spoofing Protections for Layer 3 Network Devices

Many attacks use source IP address spoofing to be effective or to conceal the true source of an attack and hinder accurate traceback. In addition, ACLs are often deployed as a manual means of spoofing prevention. Layer 3 devices such as routers or Layer 3 switches should be configured with the following anti-spoofing protection features:

- **Unicast RPF**—Provides source network verification and can reduce spoofed attacks from networks that are not under direct administrative control.
- **Disable IP Source Routing**—IP source routing leverages the Loose Source Route and Record Route options in tandem or the Strict Source Route along with the Record Route option to enable the source of the IP datagram to specify the network path a packet takes. This functionality can be used in attempts to route traffic around security controls in the network.
- **Disable ICMP Redirects**—It might be possible for an attacker to cause the network device to send many ICMP redirect messages, which results in an elevated CPU load. For this reason, disabling transmission of ICMP redirects is recommended.

Anti-Spoofing Protections for Layer 2 Network Devices

Layer 2 devices such as switches should be configured with the following anti-spoofing protection features:

- MAC spoofing prevention should be configured as protection against Layer 2 traffic storms (for example, an unusually high number of Broadcast or Multicast packets). These are configured at the edge port where servers or devices enter into the network. Examples of these anti-spoofing features deployed on a switch are seen below. Anti-MAC-Spoofing methods can be used to protect against MAC spoofing and Content Addressable Memory (CAM) overflow attacks, and can restrict the number of devices on a single port. You can use this to limit and identify MAC addresses of the stations allowed to access the port.
- Traffic Storm Control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces
- Dynamic Host Configuration Protocol (DHCP) snooping prevents unauthorized (i.e., rogue) DHCP servers offering IP addresses to DHCP clients.

- Dynamic ARP Inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.
- Virtual LANs (VLANs) are used extensively to assist with segmentation and restricting of data flow within the network infrastructure. The following are a sample of several best practices for helping harden VLAN and switched deployments:
  - Disable all unused ports and put them in an unused VLAN. Any enabled open port provides an access medium into the network. Therefore, disable all unused ports.
  - Do not use VLAN 1 for anything. VLAN 1 is the default VLAN and is enabled on all ports by default; therefore, it is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1.
  - To assist with preventing VLAN hopping attacks, whereby an end station can spoof as a switch, configure all user-facing ports as non-trunking. This prevents the port from going into trunking mode unless explicitly configured.
  - Explicitly configure trunking on infrastructure ports. For ports connecting switches, trunking is used to extend VLANs throughout the network. Explicitly configure only the VLANs required to be extended to other switches.
  - Force tagging for the native VLAN on trunks and drop untagged frames to assist with preventing VLAN Hopping.

Access Control

This section explains the mechanisms used to secure and control access to the Operations System. The types of access that occurs at the networking level can contribute a large amount to the overall access control security policies and procedures. Within the networking components and the confines of the Data Plane, access to the network is primarily controlled at the edge. This primarily governs access to servers, Ethernet-enabled devices, and end stations to the network switches where these devices plug into the network:

- Port security at the edge, explained earlier, provides a way of limiting devices connected to a port.
- ACLs applied to the ports at the edge can be used to filter and control data based on source address, destination address, and protocol. This can permit or deny traffic to specific destinations and applications based on the rules applied to the networking access port.
- Building on top of ACLs, newer technologies can be applied; for example, 802.1X is an IEEE standard for port-based access control. It provides a mechanism to assist with authentication of the end system to a centralized policy system or server and dynamically apply network access control to an end device based on its defined policy. This requires that the end system have support for the 802.1x protocol, as such older devices may not support this policy and would need to fall back to a more manual access method such as statically-defined ACLs or hardware address authentication using the MAC address.

The following sections provide further details.

Legacy Edge Devices and Limited Security Devices

Some edge devices might have limited security technologies, therefore, hardening of these devices is going to be limited. However, technologies exist that can apply a level of hardening from an end-to-end system perspective. Understanding the type of device and baselining its function is key to this. Having flow-based technologies within a network provides the necessary visibility for understanding if these devices are performing in an anomalous fashion. Active Defense, page 156 provides descriptions supporting Active Defense. Access control mechanisms and restricted data flow mechanisms can also contribute here and are described elsewhere in this document.

Network Availability for Critical Network Components

Network availability is a key component in system hardening. Organizations should implement redundant equipment and redundancy of paths through a network by leveraging certain networking protocols. These will provide the year-round availability that a PMS would require.

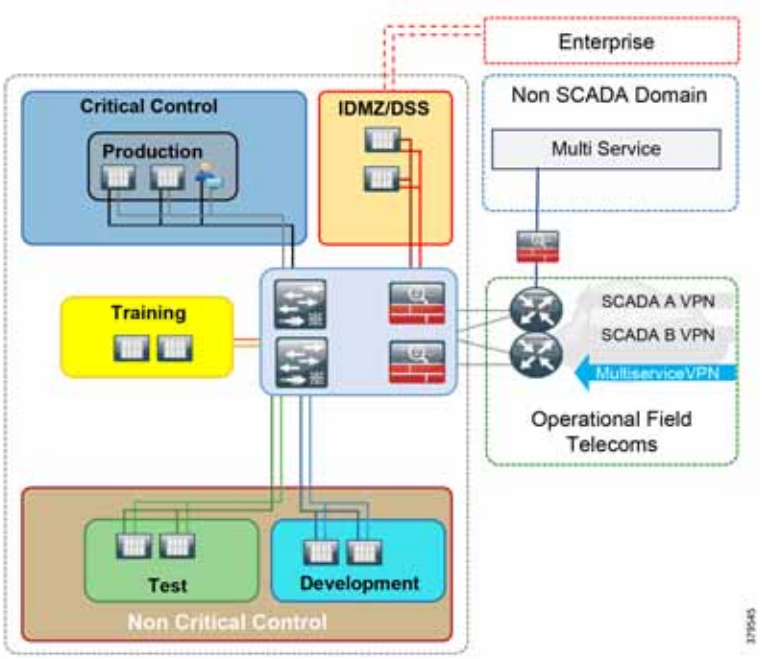
Practical Considerations for SCADA Hardening

The prior sections have provided a discussion of the framework (servers, users, access control, field devices, field communications, and the various LAN and WAN components) that can be used to harden an operational infrastructure. While we have given operational system examples throughout that discussion, this section will look at some ways that these recommendations can be applied practically to improve the security profile of a Pipeline SCADA system.

Hardening the Control Center

The Control Center is the core of the operations control system. In it resides the servers and operator stations that are used to control the operations of an industrial process. Hardening is the processes for accomplishing the protection of the many layers, components, and sections. In the next several sections, we will make recommendations about how to improve the protection of this core control (and business) component.

Figure 40 Smart Connected Pipeline - Simplified RA



Security Zones

Network segmentation is crucial to protecting your operational system and enforcing a defense-in-depth architecture. It ensures that only authorized users may take specific actions within these zones in a safe and secure manner. This zone approach is a core design feature of the SCP Reference Architecture. Additionally, while each zone leverages network infrastructure to enforce the segmentation, separate Windows Domains are also used to further improve the segmentation, which helps to protect possible cross-domain operations that could interfere with production. We recommend that firewalls be used to facilitate and enforce the segmentation, protecting and controlling the flow of information in and out of each zone.

It is important to note that each Domain has its own set of users, groups, and access control definitions. Group Policies should be managed within each Domain/Zone.

Test and Development Zone

This zone contains the system components used to help implement and validate system changes (e.g., database changes or OS and application patches) before deployment into the production environment. Typically, this zone contains a representative subset of the production and IDMZ systems. The level of redundancy and the type of representative field communications is aligned with each organization's specific priorities and capabilities. As part of the Domain segmentation, the T&D zone has its own Windows Domain and users, separate from other Domains and with no domain trusts.

Three types of systems typically exist in this zone: the Test Environment, the Development Environment, and if one exists, a copy of the IDMZ or DSS.

Production Zone

The Production Zone contains the actual full production environment, including the field components, the Primary Control Center (PCC), and the optional Backup Control Center (BCC). Operational display systems are also a component of this Zone. As with other zones, a unique and independent Windows Domain exists for the Production Zone.

System types in this zone include the main control systems, real-time historians, real-time supporting applications for gas and liquids, and leak detection systems. In some configurations, a deployment system, which is used to distribute patches and system configuration changes, might be configured.

Operator Training Zone

In systems where a formal training environment has been deployed, an Operator Training zone may be created. The importance of this segment's existence is to ensure that no chance exists that an operator may confuse training with production and *vice versa*, eliminating the chance of production-training cross-domain traffic. We recommend having a corresponding unique Windows Domain.

I/DMZ and/or DSS Zone

These zones can exist in parallel or can be collapsed into one or more segments, depending on how the exchange of information is intended, along with the corresponding integration demands of corporate. Several configurations can exist regarding the Domain structure. In some instances, the Domain for the DMZ/Decision Support System (DSS) can be unique (parallel to the other security zones) or it can be aligned with the Corporate Domain (completely depending on the needs of the user community and IT's expectations).

Software Tools and Applications

It is important to consider the use and location of certain vendor-supplied software tools, also known as utilities. For example, a protocol monitoring utility that is used to review and troubleshoot field traffic may exist. Depending on how it is implemented, the network parameters might need to be configured in a way that opens the network to easier sniffing or other protocol insertion or mimic attacks.

Another area for consideration about exploitation opportunities are information uploads or configuration downloads to field devices from the production environment. The pathways that are used to implement these features might or might not open an exploitable pathway to the field devices, creating another vulnerability to consider in a risk assessment.

The takeaway here is that it is important to ascertain from the vendor how tools and processes like these are implemented and to consider their use; e.g., who may use them and under what circumstances-along with the risk versus value within the overall security profile of the system.

Data Flow Enforcement

By using firewalls and access control, it is possible to enforce the flow of information to move from most secure to least secure security zones. Low security zone layers should not be able to send information directly into a zone of higher security. The operational environment should be structured and products deployed within it that enforce this process through its implementation model. It is important for the OT staff to ensure that, as new applications and features are added to the environment, this secure data flow model continues to be enforced. Arguably, this could become a policy statement as well, ensuring that those maintaining the network infrastructure do not implement rules or exceptions that violate this directive.

Application Signing and Management of Change (MOC)

It is imperative that the OT management staff can ensure the legitimacy of elements that comprise the executable infrastructure of the operations system, such as executables and DLLs. It is recommended that application signing be enforced and only properly signed and validated software be installed on a production system. This too, could be considered a candidate for a security policy and something that OT could demand of their vendors.

Aligned with ensuring the validity of product components, is ensuring that a complete audit trail or record of changes be maintained. As part of such a process, formal approvals would be required before any changes are made to production systems, or for that matter, to other system components.

Patch Management

Patches and updates are a critical part of a comprehensive security program and maintaining the software that forms the actual control system at both the OS and Application levels is important. Microsoft has a documented release schedule for security patches. While it is recommended that the production system be isolated via an air gap, this is not always assured; therefore, keeping the base OS infrastructure up to date is critical. While no industry requirements exist, it is important to establish a regular deployment of approved OS patches after ensuring that they have been validated in the T&D environment prior to Production deployment. The same is necessary of vendor patches. While they may not be released on the same cadence as the OS, they may also contain security-related updates that will improve the overall security profile of the operational systems.

While software most often comes to mind when thinking of patching, hardware devices today contain a great deal of software and these must be maintained and updated as well to correct identified security flaws and exploited vulnerabilities.

Anti-Malware

Despite the best management practices, processes, and policy directives, compromises can and will occur, exposing operations systems to malware. Imagine that if a ransomware exploit was successful, you would be managing a major cyber incident that might have easily been avoided with anti-malware software. Many traditional signature-based anti-malware systems solutions (such as McAfee and Norton) exist, but new options such as Cylance, which uses a machine learning approach, are also available. Whitelisting and blacklisting exist, but they require a lot of direct and ongoing management to define and maintain and with the complexity of many control systems, they can be a challenge to successfully operate consistently.

In all cases, it is imperative that the vendor be consulted concerning anti-malware systems and the configuration of these packages. For example, it is important that files not be deleted or moved automatically, negatively affecting the running of the system, due to a false positive. Tools like whitelisting or blacklisting can cause the system to prevent a valid file from running although it had been legitimately changed without the configuration being updated. These packages can produce on a system a negative impact to performance. For example, an on-demand scan at program startup might delay a critical piece of software from starting during an emergency.

These are examples that highlight the challenges to implementing and maintaining an anti-malware program within an ICS environment and how security needs to be a partnership between the asset operator and their vendors.

Internet and Related Access

It is critical that Internet access be restricted to areas other than the Production zone. Such connectivity, while enabling on one hand, can be debilitating on the other. Opening the Production zone, including the field infrastructure, to the Internet should be a non-starter. Any access to the Internet and the cloud features that are driving much of this demand should be through the DMZ and higher.

It is imperative that the continuous review cycle include confirmation that this policy is strictly being enforced.

Firewall Considerations

While each operational system has its own port and service constraints, the following are recommendations derived from AVEVA experience in configuring and deploying enterprise-level SCADA solutions:

- Use VPN tunneling between control centers to leverage the built-in encryption (IPSec) provided by the tunnel. Rules then must be applied within the components supporting this connection such that only authorized traffic is exchanged.
- Network Segmentation is one of the key uses for firewalls, which, as outlined in earlier sections, should be used to enforce segmentation and be configured to ensure that only authorized traffic for authorized source and destination systems occurs between segments. Smart switches with VLANs can assist in this segmentation.
- Least Privilege firewall configuration is the driving philosophy behind how SCP-RA uses and configures firewalls. This means that only the ports and protocols necessary for a functioning operational system should be enabled on the firewall, while all others are disabled by default. As a result, only the minimal openings are supported, ensuring that unintended exchanges cannot be successfully initiated.
- Most Secure to Least Secure Initiation should be enforced to ensure that processes initiate connections from high security zones to lower security zones.
- As noted, the ports and protocols that should be enabled are specific to the deployed solution, but the following are typical items to consider:
  - At a minimum, MS SQL, ports 1433, 1434 over TCP/UPD, and application-driven ports.
  - RPC Endpoint Mapper port 135 should be evaluated as needed, and if so, ensure that all OS patches are installed to prevent exploits against known vulnerabilities.
  - NTP, port 123, used for time sync, an important component for correct Kerberos functioning.
  - Domain Name Server (DNS), port 53 over TCP/UDP, is used for DNS lookup.
  - Internet Control Message Protocol (ICMP) protocol should be reviewed for its need within the operational network, since it facilitates exploration of the network by attackers and provides useful tools.
  - HTTPS (SSL/TLS) leverages port 443 for secure web traffic.

Many other ports and protocols will need to be considered, but this list should help to establish what needs to be considered in this review process. Additionally, the requirements of each third-party application that is a component of the operational system, should be included as part of the review process.

Baseline OS Hardening Considerations

These recommendations to help secure an operational control system do not cover every requirement, nor are they mandatory—they are only examples. When developing the security plan for the control system during either system design or hardening of a deployed system, these are the sort of things that should be evaluated and considered.

Here are some general OS items to consider disabling or removing when working through a hardening program:

- Windows applications, such as games
- Restricting unprivileged users from installing software
- Restricting access to the command line or general windows components typically available through the start menu
- Unneeded device drivers
- Hardware devices such as USB, CD/DVD drives, and other removable media devices
- Unnecessary wireless features
- Internet services
- Unused and unsecure protocols such as HTTP and Telnet
- Unnecessary administrative utilities, diagnostics, system, and network management
- Utilities, applications, and other tools that are used for scripting or other development/testing work

By applying these additional components to the other hardening recommendations, an organization can devised and successfully deployed a comprehensive security plan across the entire operations environment.

Baseline Network Hardening Considerations

To provide extra levels of security, basic network infrastructure mechanisms exist to protect each of the functional communication planes as described earlier. The guidelines described earlier to secure the Control Plane, Management Plane, and Data Plane should be followed. Using the network switches as an example, this would include shutting down unused ports, properly configuring trunk ports to secure against VLAN hopping, DHCP snooping, dynamic ARP inspection, port security, traffic storm control, infrastructure management, and Control Plane Policing (CoPP). Each of the firewall routers (if deployed) and switches within the control center have detailed documentation examples in the Appendix for securing the network infrastructure.

Availability in the Control Center

To provide redundancy of all components using a primary and backup control center deployed in two geographically separate locations, the SCADA system can be provided in a single redundant model or, more commonly, in a distributed model. This should include applications, compute, storage, and networking components in the control center. No Single Point of Failure (SPOF) should occur on any critical component of the SCADA system. A critical component is any component whose failure directly and adversely affects the SCADA system's overall performance or its ability to continue performing the critical SCADA functions of monitoring and control.

The SCADA system should make use of modular components so that the failure of a single component does not make other components inoperative. It also provides redundancy for all critical SCADA functions for monitoring and control.

The SCADA system redundancy model should be self-monitoring with critical functions and devices under constant evaluation as to their availability. This is a key requirement for SCADA system robustness and for ease of support and administration. Automated monitors check all critical components for failures and take the least disruptive course of action to recover from any disruption or failure. In all cases, component failure and recovery should not compromise SCADA system integrity.

The implemented solution equipment and software should include mechanisms capable of providing automatic failover to redundant equipment or software services. This ensures protection from any SPOF, which would cause a general SCADA system failure due to the failure of critical SCADA system functions.

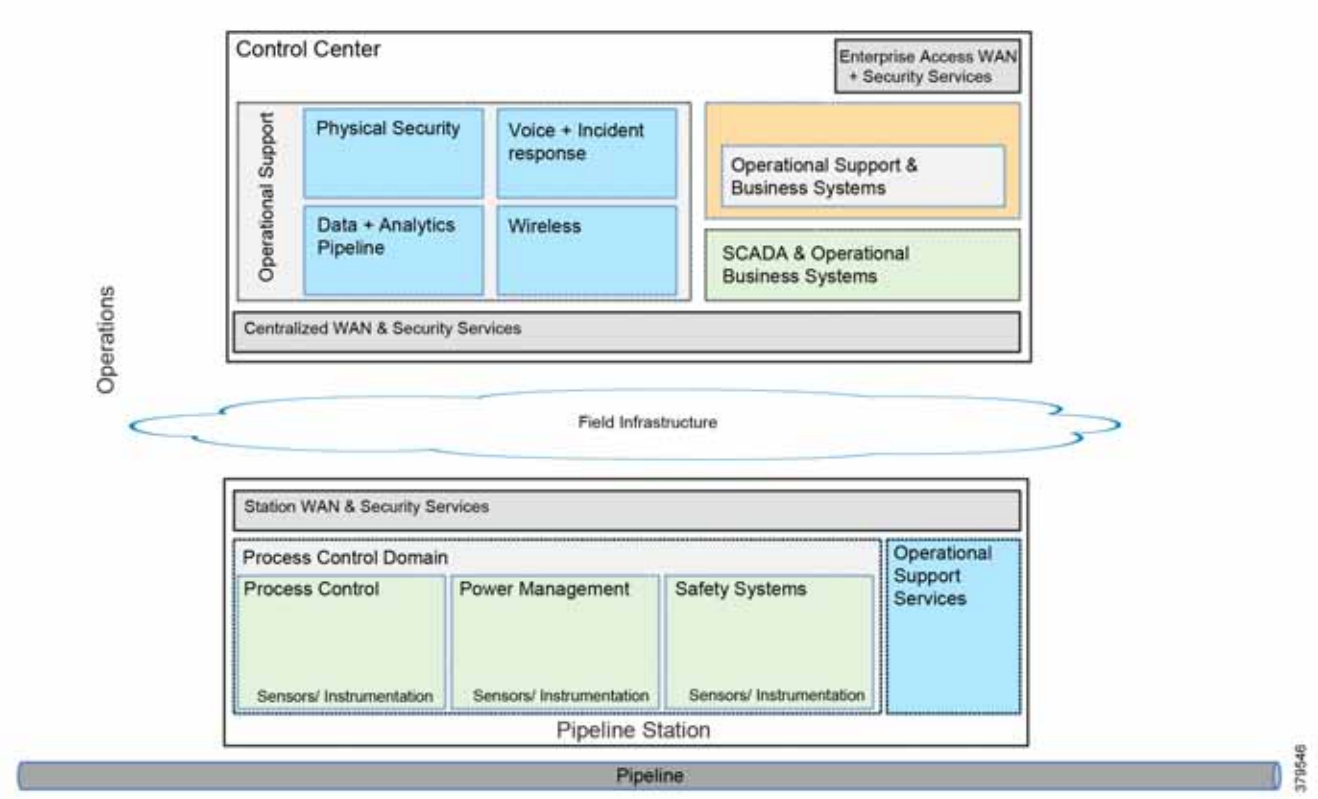
Hardening the WAN and Field Infrastructure

In relationship to operations, network hardening is the focus within the confines of the WAN.

The WAN must provide the year-round availability for the operations of the pipeline. Network redundancy, through redundant hardware and paths, needs to be engineered within the WAN communications infrastructure between the station WAN block and the Control Center Centralized WAN block.

Communications integrity and confidentiality are deployed within the WAN using network encryption. For example, deployment of VPN encryption should be configured over WAN links provided by a Service Provider or another entity outside of the pipeline operator. In figure X, this would be between routers deployed in the control center in the centralized WAN and security services block and at the Layer 3 boundaries at the Station WAN and Security Services Block.

Figure 41 Communications Infrastructure in the Connected Pipeline Architecture



Integrity and Data Confidentiality

Network-based encryption can provide integrity authentication and confidentiality of data. This is typically deployed where data is traversing a public infrastructure such as wireless LTE or 3G deployments.

IPSec provides a standardized framework for the security of communications over an IP network. The principal feature that allows it to support varied applications is the encryption or authentication of all IP layer traffic below the transport and application layers of the OSI model. Regardless of the application, all data that passes over the IPSec segment can be secured. Within IPSec, the Encapsulating Security Payload (ESP) provides confidentiality, integrity, and authentication and has anti-replay capabilities. ESP is recommended for SCADA deployments as it provides the highest level of security

Resource Availability

A robust, highly available communications network is essential to support the control and operations of the pipeline. Redundancy is provided at all layers of the architecture. Dual platforms, dual networks paths, and dual SCADA networks provide separately addressed networks for communications between the Control Center and the RTUs in the pipeline stations.

QoS should be enabled to provide priority of SCADA communications above all other traffic. In architectures or technologies where the physical infrastructure is shared, and especially with technologies such as 3G or satellite where bandwidth is restricted, SCADA communications must be prioritized. Classification and marking should be applied at the edges of the network with policy applied throughout the network infrastructure. QoS techniques can be used to help identify and or mitigate anomalous behavior related to oversubscription of traffic types. If the network has been profiled, then bandwidth utilization per service should be well known. Techniques such as traffic policing should be implemented to suppress abnormal traffic levels for a service that might be used as a point for a DoS attack.

Baseline Network Hardening

The general best practice for helping protect the routers from becoming oversubscribed for resources should be implemented. When considering router attack scenarios, both malicious and non-malicious events can overwhelm router processor resources. Malicious events include crafted packet attacks or simply high rates of packets directed at the control plane. Non-malicious events may result from router or network misconfigurations, software bugs, or, in some circumstances, network failure re-convergence events. To protect the control plane from a network-based DoS, and to restrict access to the router management and resources, network hardening of the three functional planes (Control, Management, and Data) should be deployed.

Identification, Authentication, and Use Control

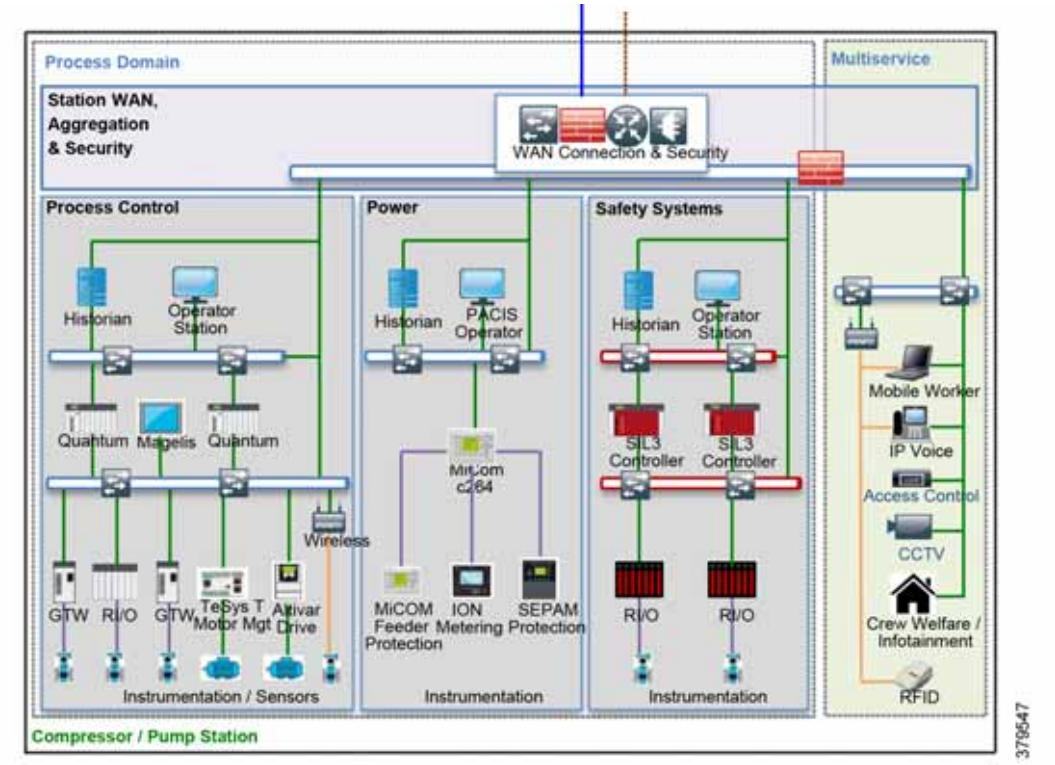
RBAC is configured to provide authentication and access to the network infrastructure components. A user is identified by authentication, and based on policy, is provided access to certain devices. A security admin can maintain network firewalls while a dedicated network engineer maintains the routed infrastructure of a WAN. Terminal Access Controller Access Control System (TACACS+) provides further granularity to ensure command level control and management of a networking device. This is, in fact, a component of securing the management plane described earlier.

Hardening the Pipeline Stations

The stations, which are usually the system structures closest to the physical assets and are typically located in remote locations, consist of control devices (e.g., PLCs and RTUs), communication equipment, and pipeline control components such as values, pumps, and compressors. Along with the expected list of pipeline control components, security cameras, security access control devices, lighting, and possible environment control components-more related to the IoT portion of the operations equation-will exist. In addition, physical structures such as fencing and other possible security barriers can be found.

What this demonstrates is that hardening a station can involve more than just locking down the related SCADA and network components. It can also involve a broad array of equipment and physical security. The next few sections will consider these items.

Figure 42 Pipeline Station Architecture



Baseline Network Hardening

The same fundamentals for hardening the network infrastructure described earlier should be followed for hardening the baseline network. To provide extra levels of security, basic network infrastructure mechanisms exist to protect each of the functional communication planes as described earlier. The guidelines described in this section to secure the Control Plane, Management Plane, and Data Plane should be followed.

Restricting Data Flow

Applications can be categorized as operational (those directly involved with supporting pipeline operations such as the SCADA or leak-detection systems) and multiservice applications (those that support pipeline operations such as video surveillance, voice, and mobile worker data access). Within the pipeline station, we need to segment these systems using the zoning and segmentation guidance created from the initial risk assessment. Physical segmentation or logical segmentation using VLANs should be deployed with firewalls to police communications between systems.

Firewalls

Two deployment and use cases for firewalls within the station architecture are:

- At the point in the network where traffic is taken from the WAN infrastructure, as seen in Figure 42. This may include boundaries between transition points in the pipeline points where pipelines may intersect other pipelines, and where control of the pipeline switches between operators or geographic boundaries, such as between countries.
- Within the station environment to police and protect communications between zones and boundaries described previously in the restricted data flow description. Least privilege access and policing traffic between network boundaries should be used to enforce segmentation and be configured to ensure that only authorized traffic for authorized source and destination systems occurs between the zones.

Resource Availability

Defense-in-depth recommendations include routine backup of data, programs, and settings. Network device configurations, server, program backups, and documentation should be routinely saved and stored at an offsite location. Data should be encrypted before it leaves the site. These backups can facilitate remediation if a system is compromised. Backups should be taken before and after any change of a device.

The same principles and guidelines that are described earlier in this section to protect the infrastructure and provide high availability are administered in the pipeline stations. Dual platforms, dual networks paths, and dual SCADA networks provide separately addressed networks for communications between the Control Center and the RTUs in the pipeline stations. QoS is enabled within the pipeline stations to prioritize SCADA and control traffic above all other traffic types. This is especially important in architectures or technologies where the physical infrastructure is shared and with technologies such as 3G or satellite where bandwidth is restricted. Traffic should be classified and marked as close to the edge of the network as possible.

Security Plan

Per PHMSA recommendations, a security plan for those transporting hazardous materials is required. In this plan, comprehensive risk assessment, plans for security duties related to each department/position responsible for implementation, and formal procedures for notifying employees when implementation of the plan is required, should exist. The plan must be in writing and retained while in effect. Copies should be available, based on need and authorization, to all responsible parties. Finally, the plan should be reviewed and updated at least once a year. Be sure to include training as part of the preparation activities[1].

Physical

This can consist of multiple areas, as the risks to a station are not only cyber, but also environmental, for example, hurricanes, flooding, tornadoes, and other natural occurrences.

Structural improvements can be made to the exterior structure of the walls of the pump station to improve the buildings resiliency against hurricanes and other natural disasters. This can be accomplished through rebar anchors and filling internal block cells with concrete.

Controlling Access

Beyond the building's structure, it is important to consider other activities that might occur at a station[2], including:

- Routine inspections or audits
- Verification of layout drawings or building plans
- Material delivery
- Facility tours

All of these activities require controlling authorized access, which includes unescorted (for trained and approved workers), escorted (for unusual repairs or audits), and special escorts (people that are highly skilled and familiar with the station supporting special activities).

Preventing unauthorized access includes providing structures such as proper lighting, surveillance systems, alarms, enclosures, and fences along the perimeter with warning signage. Adding either security key access or lock codes will also help in restricting unwanted access into potentially hazardous areas by careless or malicious individuals.

Using the network (for example, leveraging the IoT capabilities of security devices) could facilitate security monitoring and improved alerts around suspicious activities.

1. U.S. DOT - PHMSA. (2012, February 22). Hazardous Materials Transportation Security Requirements. Retrieved from PHMSA: https://hazmatonline.phmsa.dot.gov/services/publication_documents/Enhanced_Security_02_22_12%201.pdf
2. Substation Safety. (2018, June 27). Safety Factors to Consider for Substation Accessibility. Retrieved from Substation Safety: https://www.substation-safety.com/latest-news/safety-factors-consider-substation-accessibility/

Redundancy

Considerations should be given to employing redundant solutions for critical components to ensure that high availability of control capabilities is maintained in the event of a failure. Redundancy can be at the level of the device or sub-device (encompassing things such as dual power supplies). At the network components level, creating fault tolerant networks can help ensure continuous connectivity to the control centers.

Power Stability

Depending on the criticality of the station on the pipeline control model, a consideration for backup power or power control should be made. Backup generators, along with power conditioners as part of Uninterrupted Power Supplies (UPS) can provide assurance that transient power issues do not affect or compromise operational stability.

Local Operations

In today's connected environment, many technologies are available that provide local connectivity to connected and disconnected devices. For example, meter information may only be uploaded intermittently through smart devices carried by technicians that visit the device on a regular schedule. Maintenance and configuration activities can occur remotely or control lockouts when devices are physically accessed. These smart devices require the same type of role based access control and authorization. The security for these devices should be connected directly to the central security configurations. Additionally, the rules and access control must be applied to prevent an unauthorized device or user connecting to devices with which they should have no responsibility. This can include an internal or external threat and should be controlled.

Auditing and logging of access and any changes should be logged, ensuring that no unexpected or unapproved changes have occurred, either through intentional or unintentional means.

Care should be given to maintaining account management best practices, such as no account sharing, devices being shut down after failed login attempts, and ensuring that employees that have left the company have their credentials ended quickly.

Lastly, portable devices also create a concern around theft or loss. These situations could expose the pipeline to unauthorized access; therefore, having the means to remotely disable and/or purge these devices should be available. This will remove the risk that a lost device is used to grant unauthorized access to the control system through the field.

Communication

One last topic to consider is if the possibility exists that field level devices will be compromised such that spoofing of traffic or the unauthorized issuing of commands is possible. Many of the protocols that are still in use (e.g., Modbus) are not secure by nature and can be subject to man-in-the-middle, spoofing, or replay attacks. Part of a comprehensive risk management plan for field level structures is consideration of the security of the communication lines between device, control device, and control station. Consider where physical or logical access might be possible and move to secure this critical risk area. Examples exist of these situations arising within control systems where one or more of these attacks have created compromised and unsafe operating conditions.

Industry Standards Cross-Reference: System Hardening

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 7 (FR3) System Integrity
IEC 62443-3-3 Part 11 (FR7) Resource Availability
NIST SP 800-53 SI-7 Software, Firmware, and Information Integrity
NIST Framework for Improving Critical Infrastructure Cybersecurity
ISO27001 Section A12, Operations Security
NIST SP 800-53 Risk Assessment Control Family
API 1164 3.7 Operating System and Application Updates
API 1164 3.8 Application and Software Restrictions
NERC-CIP CIP-007 System Security Management

Confidentiality

Confidentiality Defined

Confidentiality is the protection of information associated with pipeline operations so that it is not exposed to those internally who are unauthorized or to those outside the company.

Confidentiality within a pipeline environment is necessary to protect the pipeline itself along with the multiple constituencies associated with the pipeline. The following are examples of areas where confidentiality should be considered for pipeline operations:

- Information that could be used to negatively impact safe operation of the pipeline
- Data that could expose personal information of employees
- Price, volume, and delivery information regarding product conveyed by the pipeline
- Purchasing or operational data associated with future transactions
- The security of operational traffic for monitoring and control

What We are Trying to Solve

We are trying to prevent the exposure of information that could be used to the detriment of the pipelines' operators, employees, partners, customers, and the public.

Pipelines are typically geographically distributed with many jurisdictions, communities, employees, vendors, and customers sharing some amount of information, which could be used to harm the legitimate interests of those same communities and entities either purposefully or accidentally.

Confidentiality can be a challenge due to a common misconception that industrial environments should simply invert the Confidentiality, Integrity, and Availability (CIA) acronym to Availability, Integrity, and Confidentiality (AIC). The reason that this is problematic is that confidentiality, while not an explicit goal for operations, is overlooked as a critical enabler for both integrity and availability. In other words, the ability to achieve operational integrity and availability is not possible without proper confidentiality.

To expand on the need, consider other dependencies and obligations associated with the business, which operate the pipeline. These include legal and contractual obligations between entities, which require confidentiality of information, associated with participants of pipeline operation. Employment records and supply chain data have legal protections and, in some cases, have become levers for abuse.

Process

As with all planned security activities, the first step is to either establish or consult appropriate policies. It may be the case, however, that an incident, which neither policy nor a specific action has covered up to then, triggers the need for confidentiality. Clearly, it is preferable to have proper policy and process in place, but in ad hoc conditions, a triage activity may be required. For the purposes of this document, however, we will focus on planning and implementation rather than a reaction.

The first step is to establish proper policy related to confidentiality associated with the pipeline environment. Having established or referenced the proper policy, the organization will need to determine what information is covered by the policy. Finally, a set of plans are to be established and acted upon. Some of these plans will represent initial control efforts and ongoing maintenance of those controls. Others will be ad hoc play-books focused on responses to potential incidents.

With time, investment, and experience, the organization will grow to higher levels of maturity in both its practices and its ability to execute.

Confidentiality Policies

An organization typically already has some set of confidentiality policies in place. We will assume that pipeline operations are obligated to follow these as employees of the company. Secondly, varying jurisdictions likely exist in which the organization operates which may have their own unique confidentiality dictates, which must also be followed. Finally, general guidelines, which may have business influences such as the cost of insurance or the sale of a system or assets, exist. Some examples are:

- DNV GL's[1] Cyber security in the oil and gas industry based on IEC 62443"—DNVGL-RP-G108. DNV GL is a global quality and risk assurance organization based in Europe.
- US Department of Homeland Security—Transportation Security Administration Title 49 Part 1520

Regulatory conditions exist that are unique to pipeline operations and determine what must be published and what can and should be kept private. Organizations have individual contractual obligations with which the company may need to comply. All of these are examples of potential pre-defined requirements that will drive a confidentiality policy.

Outside of regulatory and legal compliance, however, are confidentiality practices, which are simply best practices to protect the safety and security of the pipeline itself. These can be gleaned from a variety of best practice guidance available from a number of sources. Some are simply general security best practices; others may be targeted at ICS / SCADA systems. Additional sources may come from parallel industries with similar operational attributes (electric transmission entities, for example), and finally pipelines may have unique data guidance.

The US NIST has published a guide that offers a valuable guide for protecting general operational information. NIST Special Publication 800-171 titled *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. A valuable general guide to confidentiality of Personally Identifiable Information (PII) class information is available from NIST in publication 800-122 entitled *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

1. https://www.dnvgl.com/about/index.html

Definitions of Confidential Information

Let us arbitrarily identify classes of information that must be kept confidential: operational data, general business data, and personally identifiable information (PII).

Broadly speaking, the information discussed in this document, which focuses on the uniqueness found with the operation and security of a specific pipeline, must be kept confidential. The specific details, as implemented, would be valuable to someone wishing to cause harm or gain an unfair competitive advantage.

The operational information necessary to operate and secure the pipeline is the data most valuable to create both positive and negative results. On the security side, there is a class of information generally referred to as Sensitive Security Information (SSI), which could enable or disable security controls for pipeline operation. Because of the gravity of that information, the US Department of Homeland Security has detailed best practices guidance regarding its handling - some of which is mentioned in this chapter.

Much of the competitive advantage information is covered in contractual obligations. The following lengthy definition is found in a business contract associated with a US pipeline company.

> " Confidential Information" means any proprietary or confidential information that is competitively sensitive material or otherwise of value to a Party or its affiliates and not generally known to the public, including trade secrets, scientific or technical information, design, invention, process, procedure, formula, improvements, product planning information, marketing strategies, financial information, information regarding operations, consumer and/or customer relationships, consumer and/or customer identities and profiles, sales estimates, business plans, and internal performance results relating to the past, present or future business activities of a Party or its affiliates and the consumers, customers, clients and suppliers of any of the foregoing. Confidential Information includes such information as may be contained in or embodied by documents, substances, engineering and laboratory notebooks, reports, data, specifications, computer source code and object code, flow charts, databases, drawings, pilot plants or demonstration or operating facilities, diagrams, specifications, bills of material, equipment, prototypes and models, and any other tangible manifestation (including data in computer or other digital format) of the foregoing; provided, however, that Confidential Information does not include information that a receiving Party can show (a) has been published or has otherwise become available to the general public as part of the public domain without breach of this Agreement, (b) has been furnished or made known to the receiving Party without any obligation to keep it confidential by a third party under circumstances which are not known to the receiving Party to involve a breach of the third party's obligations to a Party or (c) was developed independently of information furnished or made available to the receiving Party as contemplated under this Agreement.

It is further valuable to note to whom the obligation to treat the above data as confidential applies to:

> *its affiliates and its and their respective directors, managers, officers, employees, agents, consultants, advisors, contractors, and other representatives (collectively, " Representatives")*

Despite the explicit confidentiality statements made in the above contracts, the US Government's Federal Energy Regulatory Commission (FERC) dictates transparency rules for public post-delivery information associated with both in-state and cross-state pipelines. To quote the FERC ruling, *" pipelines are required to post daily scheduled volumes for delivery points dedicated to a single customer."* While FERC allowed for some obfuscation of the specific customer, the dictate to make the general information available for the sake of market visibility is clear.

Pipeline employee personal information, commonly referred to as personally identifiable information (PII), also constitutes a class of data requiring confidentiality by laws across multiple jurisdictions. PII is likely the most explicitly protected class of protected data from a regulation perspective. While this class of data is not the primary focus of this document, it is included for completeness sake and must be addressed. Employee expectations of privacy may also be set contractually and by corporate policy. The definitions of such data and an employer's obligations vary across jurisdictions. Some examples to consider are employee home information, images, and national identification data, such as passports or social security numbers. Medical information is almost universally protected and financial statements and benefits plans may be as well. Look to the explicit protections defined in jurisdictions such as the US state of California's California Civil Code §1798.140(o)(1); the European Union's GDPR.

A Note Regarding Data Retention Needs

Numerous regulatory and potentially contractual obligations require the retention of data for a set period. Depending on the volume of data under those obligations, it may become necessary to store that information in a repository that is not a part of the pipeline system itself. As a result, pipeline operators will need to be aware of the location of that data and how it is secured. Thus, the scope of required control is likely to expand beyond the boundaries of the system that operates the pipeline.

The obligations regarding data retention will be limited to those uniquely aligned with pipeline operations. General human resource class records will be assumed to be the responsibility of the appropriate functions within the company.

US Federal Pipeline safety regulations (*Code section §192.947*) note requirements for the retention of operational records. It is advised that the full range of content should be targeted for confidential access controls.

Application of Confidentiality Controls

With policies defined and applicable data identified, the next step is to execute controls for confidential data.

Access Control

Data is generated within the context of a system or application and access control activities associated with that system or application inherently define confidentiality controls. For these reasons, the controls defined within the access control system must be applied with data in mind.

It is important to note, however, that data may be stored in a way that does not guarantee that access is limited by a particular system or application. Systems may generate data in a commonly accessible form such as clear text or it may be stored in a general database management system (DBMS). In the first case, the operating system on which it is stored will dictate the primary means of controlling access. Access control can be applied to a file, directory structure, or the device itself. In the case of a DBMS, controls exist that may be applied to individual field levels or depend on the values within the structure itself. In this manner, the logic of the application's access control policy is actually applied to the data structures. This is not guaranteed and should not be assumed unless you have confirmed it to be true. There are numerous commercial and free database query and DBMS management tools, which can access data directly without going through the logic of an application server and its logical controls.

Figure 43 Windows Access Control Settings 1

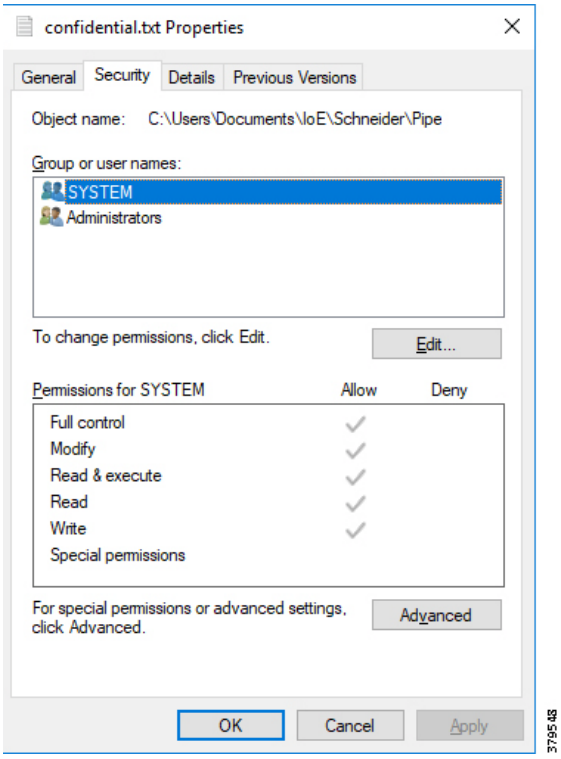


Figure 44 Windows Access Control Settings 2

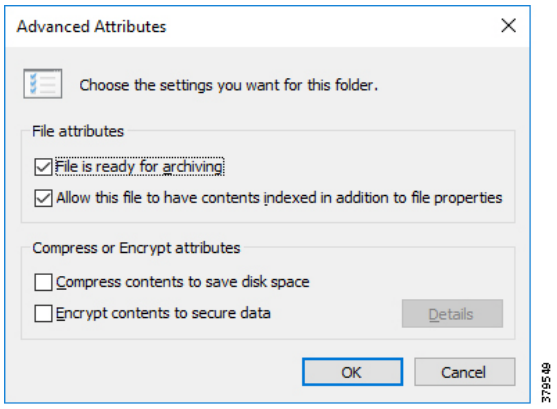
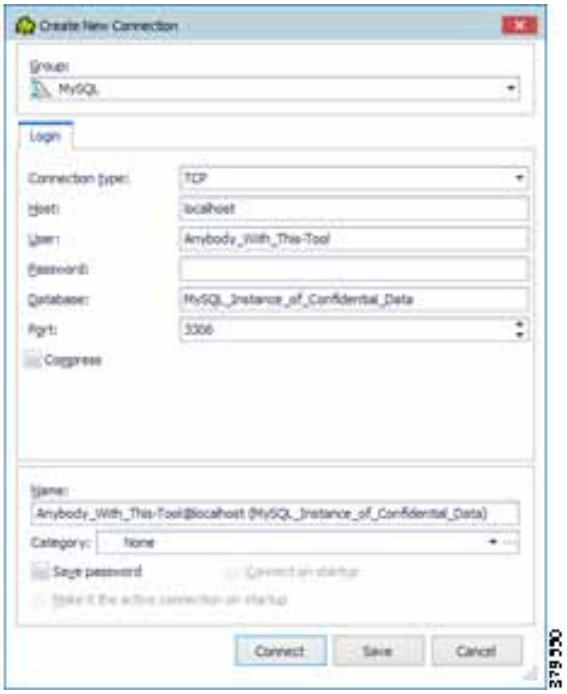


Figure 45 Windows Access Control Settings 3



Credentials, Authentication, and Authorization

Access control to applications and systems is largely based on the credentials used. Those credentials may be evaluated locally within the system being accessed or they may be validated through additional credentialing tools such as Microsoft Active Directory and RADIUS.

To expand the protection of the user's credentials, consider the addition of multi-factor authentication. This requires two forms of information to be provided to authenticate the user. One may be something known to the user and the authentication system (such as a password or password hash); the other traditionally is something in possession of the user that is accepted by the authentication system as evidence that the requester is who they claim to be. A common tool is an electronic device, which generates numeric values algorithmically that align with the expected algorithm outputs on the authenticating side. Associated applications, which request an approval from a separate system, also exist. An example of this is shown in Figure 46:

Figure 46 Example Secondary Login Screen as part of Multi-factor Authentication

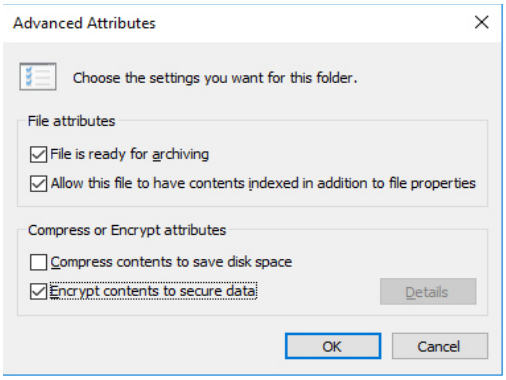
Given that these systems act as the decision makers for access and capabilities aligned with access to pipeline controls systems, they themselves should be properly secured.

Encryption of Data at Rest

It is desired that data at rest be protected. One means of protection is by encryption. As discussed earlier, this means that implementation will depend on the form of the data.

Pipeline management does not have any known unique explicit encryption requirements, but general industrial standards such as IEC 62443-2-4 /2 make mention of it in section SP.03.08 and in other sections.

Optional third-party tools can perform tasks related to OS level protections and encryption of application elements.

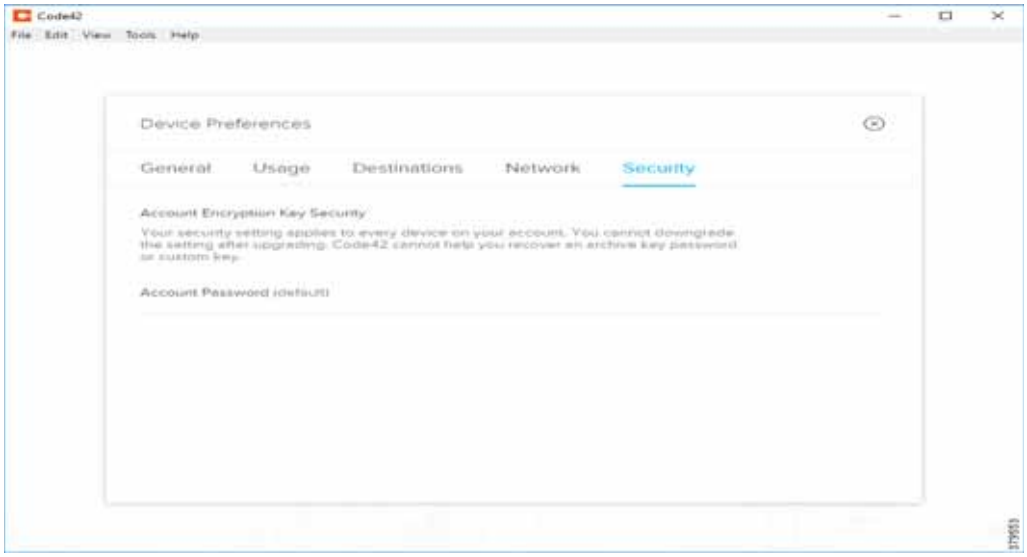


Modern database management systems will provide for data encryption. That does not necessarily mean that the applications for which the database is being used will be configured for such. It will be important to check with your automation control vendors to determine what the state is and what can be configured if encryption is not enabled by default.

It is worth noting that a valuable practice for system resiliency will include having regular and recoverable backups of data for systems. In that case, there are copies of data, which must be protected. Encryption is a valuable option here.

Event and system logs are worth special attention as they reflect an official record of activities. Organizations may need to investigate or provide proof regarding an incident. Given that most logs are generated and stored in a clear-text format, the ability to ensure irrefutability of a record may be difficult. Enabling encryption of events soon after their generation can help in that regard.

Figure 47 Enabling Event Encryption



Encryption of Data in Motion

To protect data as it is transmitted within the system, some form of encrypted communications is advised when it is viable. Like all security decisions, a risk to cost analysis should be performed to ascertain the proper security stance. Encryption helps to protect the data associated with the environment and additionally protects system communications in general. All ICS guidelines describing the need for secure conduits referenced in IEC 62443 and ISA 99 standards are applicable guides. The most likely and appropriate data exchange conduits to secure would be those communication channels between critical control areas and remote operating areas. These are the paths for control activity to be communicated and the telecommunications equipment available are more likely to support the appropriate levels of encryption.

Within a self-contained system where serial communications are common and in direct touch with older kinetic equipment, encrypted communications may be both resource prohibitive and potentially inhibiting to the operation itself.

Traditional means of protecting communications is done via VLANs (not necessarily encrypted) and VPNS that use encryption.

Destruction and Disposal of Confidential Data

Data may leave the range of your direct control unknowingly during device replacement cycles. The pipeline operator, once aware of where confidential data may live, must look at that data from a complete life cycle management perspective. That life cycle management should consider the potential exposure of confidential information at the point of equipment's end of life.

TSA Pipeline Security Guidelines call for plans to secure data through the entire lifecycle, including its eventual destruction when the host environment it resides on or its own inherent usefulness ends. The guidelines found in Figure 23 specifically call for *the secure disposal of equipment and associated media*.

Detecting Behaviors of Data Hoarding and Exfiltration

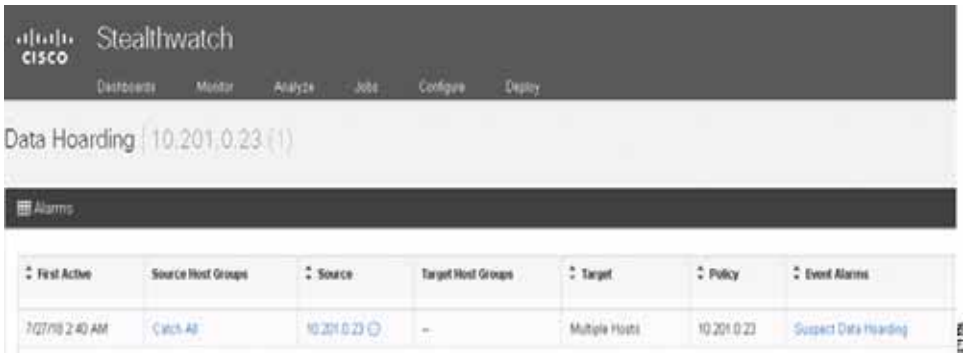
The practice of network security monitoring can provide evidence of data hoarding, which is frequently a precursor to data exfiltration. Data exfiltration is the process by which an attacker takes data from the target environment.

The earlier an activity in a multi-step process can be detected, the more likely the end step of data loss can be averted, and thus detection of data hoarding is desired.

With network security monitoring, a number of network activity data points are captured and analyzed for undesired and/or unusual behaviors. Some of those behaviors may be related to unusual communication patterns determined by frequency of connections, the participants in a connection, the protocols spoken, volume of data exchanged and others.

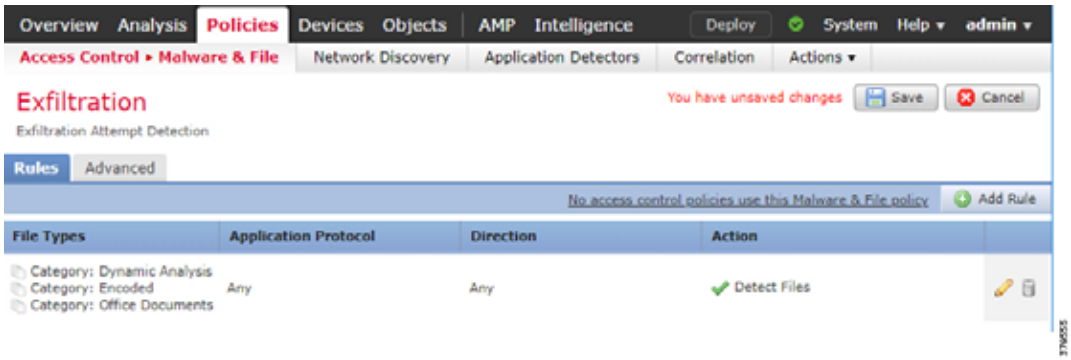
The process can be potentially data intensive and thus automating detection is desired. Tools that can perform those tasks are available and can make the detection of data hoarding and potential exfiltration attempts much easier. The following is an example of a tool that performs that analysis and can automate alerts of data hoarding and exfiltration.

Figure 48 Example Behavioral Analysis Tool



Not all risky behaviors are malicious however. Sometimes large-scale file transfers are made to enable out of band analysis within a spreadsheet or other tools. At other times, configurations are shared about the network as well. Being able to track these file transfers could be beneficial.

Figure 49 Example Tracking File Transfers



It would be valuable to log data transfers at key control points within the network. Of particular value would be any demarcation point where your segmentation policy merited some form of access control such as a firewall. In these cases, the outbound communication logs are most worthy of analysis.

Summary

Pipeline data confidentiality is a special case of access control focused on content associated with operations and participants. Pipeline security can be compromised if those with malicious intent know key operational details. Policies dictating the handling of the data may come from multiple sources such as political jurisdictions, contractual obligations, and organizational requirements. It will be important to understand the nature of the data and where it exists during its entire lifecycle. The type of data and its residence will influence the type of controls that can be applied to maintain confidentiality.

Industry Standards Cross-Reference: Confidentiality

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 8 (FR4) Data Confidentiality
NIST SP 800-30 Guide for Conducting Risk Assessment
NIST SP 800-53 SC-13 Cryptographic Protection
NIST 800-112 Guide to Protecting the Confidentiality of Personally Identifiable Information
ISO27001 Section A10 Cryptography
ISO/IEC 27002 Section 8
API 1164 Section 6 Information Distribution
NERC-CIP CIP-011: Information Protection

Restricted Data Flow & Infrastructure Design

Restricted Data Flow Defined

Restricted data flow is described in IEC 62443 as *"Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources."* In alignment with IEC 62443-3-3, the foundational requirement for restricted data flows lists the following system requirements, which provide guidance for restricting data flow:

- **Network Segmentation**—*"The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control systems networks from other control system networks."* Examples of implementation could be logical or physical segmentation. Logical are VLANs to provide the network segmentation on a shared infrastructure and physical is using a completely separate set of actual networking devices per system.
- **Zone Boundary Protection**—*"The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model."* This would include managed network boundary devices such as firewalls or routers to deny or permit communications between zones.
- **General-purpose Person-to-Person Communication Restriction**s—*"The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system."* No Facebook or Twitter within the operational domain!
- **Application Partitioning**—*"The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model."* As with network segmentation, physical or logical means using machine virtualization or specific bare-metal compute and storage can accomplish application partitioning.

Within the context of the Connected Pipeline, the above system requirements form the basis of restricting the flow of data between control and non-control systems and between critical and non-critical systems within the control system.

What We are Trying to Solve

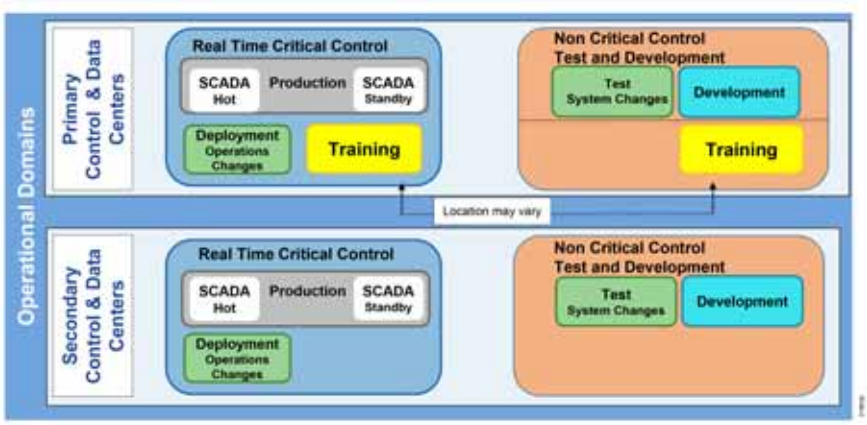
Security issues arising in one zone must be restricted from affecting or cross-pollinating into other zones, with only permitted traffic passing between zones using conduits. If a system is compromised, means and countermeasures must exist to prevent the proliferation of the compromise to other systems. These protect systems from intentional security incidents and unintentional mishaps caused by human error such as misconfigurations applied to devices, which cause networking issues. If communications need to flow between zones then this should be through some form of zone boundary control.

The operational SCADA traffic is segmented from any other traffic that may be traversing the network and should be prioritized over non-operational, thus less critical, traffic. This segmentation must be carried through the architecture from the instrumentation reporting data within the pipeline stations into the Control Center. Prioritization within the SCADA system is also a requirement. In an application such as leak detection, information must be relayed to a decision point within the system at a priority above all other SCADA traffic.

Looking at Figure 50 and Figure 51 provides a view of the zoning and segmentation that is applied in the pipeline control center. The zoning isolates data, applications, services, and communications between different domains in the pipeline system. In the following, we are isolating critical control systems, non-critical control systems, and non-control systems.

Applications and services running across the pipeline should usually be divided into Operational domains (Figure 50) and Operational Support domains (Figure 51). Please note that the segmentation can be further refined through the creation of Demilitarized Zones (DMZ)/Decision Support Systems (DSS) that isolate the control system from the needs of the corporate support and related business applications.

Figure 50 SCADA System Zones 1

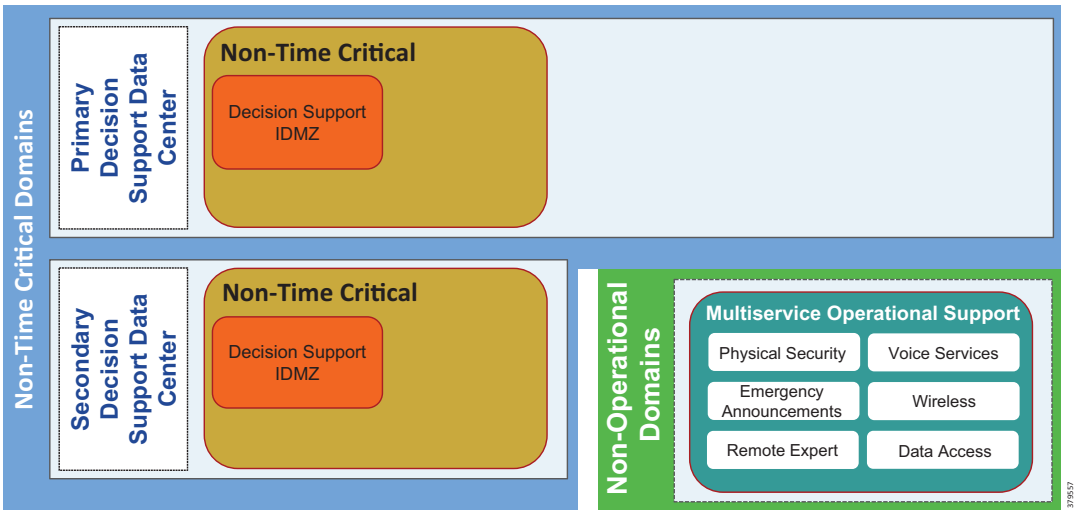


Inside the Control Center environment, these domains would typically be segmented into real-time critical control systems and test and development zones (Figure 50).

- The real-time zone is further segmented into production (including SCADA and engineer workstations) and deployment.
- Test and development is segmented into test and development zones.
- Training and simulation may reside in either main zone, depending on customer philosophy and practice.

Non-Control Systems designed to support the operational activities for the pipeline are also segmented into the Decision Support/L3.5 IDMZ and multiservice (Figure 51). Although not essential to real-time control and operational process control of the pipeline, these are vital services for supporting operational activities and providing access to information from the Enterprise and outside world, where appropriate.

Figure 51 SCADA System Zones 2



Process

In the 1990s, the Purdue Reference Model and ISA 95 created a strong emphasis on architecture using segmented levels between various parts of the control system. ISA99 and IEC 62443, which brought focus to risk assessment and process, developed these further. The security risk assessment will identify which portions of the PMS are defined as critical control systems, non-critical control systems, and non-control systems. The architecture should segment and isolate these management systems accordingly. Inventory awareness is key in this process and should be well understood when evaluating zoning and segmentation. Another key factor of risk analysis is determining the security levels and targets as part of the risk assessment. Factors such as simplification versus over complexity of the implementation, as well as price point for implementation, are key parts in determining the level of risk a pipeline is willing to take. This point is especially poignant when assessing segmentation strategy with virtual or physical segmentation deployments.

- **IEC 62443-1-1**—Security for Industrial Automation and Control Systems "Models and Concepts" provides information on Zones and Conduits with examples.
- **IEC 62443-3-2**—Risk assessment guidelines to help determine philosophy and architectural design are available in this standard "Security for Industrial Automation and Control Systems - Security Risk Assessment and System Design."
- **IEC 62443-3-3**—Specific Restricted Data Flow requirements can be found in this standard under Foundational Requirement 5.1.

After implementation, continual assessment is required to ensure devices that are added to the system maintain the level of security associated with the zone. Devices already zoned must be verified too as software updates may change the security level of a device.

Security Levels

IEC 62443 defines further enhancements to the System Requirements (SR) that provide guidance to the security levels. Security levels (SL) provide a way to measure the level of security that are applied or targeted to a particular zone or conduit. Security levels are defined as follows in IEC 62443-3-3 when discussing Restricted Data Flow:

- **SL 1**—Prevent the casual or coincidental circumvention of zone and conduit segmentation.
- **SL 2**—Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills, and low motivation.
- **SL 3**—Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
- **SL 4**—Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS-specific skills, and high motivation.

Further enhancements are given to the System Requirements using Requirement Enhancements (RE), if applicable. These strengthen the security implementation and are mapped to one of the four security levels. Specifically, this applies to network segmentation and boundary control within the construct of Restricted Data Flow and is an important evaluation that needs to be considered when assessing the level of risk that the pipeline operator is willing to take.

Segmentation Virtual versus Physical

Segmentation can be achieved using physical or virtual techniques. Traditionally, a network infrastructure has been separated physically, but with the advent of virtualization technologies and increased security mechanisms, logical separation of services is also an option. This can be applied not just to the network using VLANs or VPNs but also to the compute and storage, where virtualization such as virtual machines (VMs) for compute and virtual storage networks are deployed. Virtualization technologies all run across a shared physical infrastructure and, depending on a risk assessment, an operator may choose to deploy completely separate hardware and infrastructure for each of its zones and conduits. Factors that influence the decision for deployment include:

- Cost of total physical infrastructure versus a shared infrastructure model with logical segmentation.
- Complexity of running multiple networks for a physical deployment versus a single shared network.
- SPOFs: If a network device on a shared infrastructure is compromised or misconfigured, the potential may exist to affect other zones. Segmenting physical networks where another level of protection will remove the potential of the SPOF case is recommended.
- Consider the possibility of a shared virtual or physical architecture that could enable crossover or spillage in traffic between zones and how this fits into your risk profile.

Depending on the design, the Security Level achieved will change according to the definition in IEC-62443-3-3. Refer to IEC 62443-3-3 FR Restricted Data Flow for the details related to Network Segmentation, Security Levels, System Requirements, and Requirement Enhancements.

Infrastructure Design

A well-designed solution infrastructure following industry-standard guidelines should be able to support physical, logical, or mixed application segmentation implementations, depending on the end user philosophy. The key requirement is that solutions interoperate inside and among architectural tiers. Creating a secure Control Center is pointless if devices at the field level are compromised and are sending inaccurate or corrupted information. The following sections describe the infrastructure design highlighting zoning, segmentation, and restricted data flow.

Control Center

Virtualization has transformed the data center environment over the past decade, allowing consolidation of multiple standalone bare-metal servers and applications onto smaller and more powerful nodes. The primary business push for virtualization was the aim to achieve better server usage from powerful and smaller physical servers, thus leading to an improved Total Cost of Ownership (TCO) and additional operational efficiencies (such as power, cooling, and space). The deployment of fully or partially virtualized solutions has increased in recent years, and industrial security standards and guidelines such as IEC 62443, NERC-CIP, and the NIST Cybersecurity Framework have an increasing focus on the deployment of virtualization technologies.

The choice of deployment depends on end user requirements and philosophy. However, any deployment must focus on high availability, redundancy, and security. A holistic security strategy should include risk assessment, change management, recovery processes, training, information protection, and incident response, all of which will determine the deployment architecture.

A high-level view is represented to provide a view of how the zoning might look within the control center. Figure 52 and Figure 53 show each one of the SCADA system environments.

Operational Zones

- Production, including domain controllers, real-time, historical and leak detection servers, and operator workstations.
- Test is the non-production replica of the operational SCADA system, allowing software and system changes to be validated prior to production without disrupting production.

- Development area for reports, displays and database changes.
- Training area is built upon the environment that a pipeline controller lives in every day, via a fully functional SCADA control system together with accurate simulation of the pipelines they control.
- Decision Support/Industrial DMZ (L3.5):
  - Decision support domain controllers and real-time historical and remote access services.
  - The Operational system isolated from any external systems or users.
  - Synchronized with real-time and historical data from the Production system to provide a secure method of providing real-time data to external users.
  - With firewalls creating a DMZ, secure services are enabled to provide the external environments exposure to the data.

Non-operational Zones

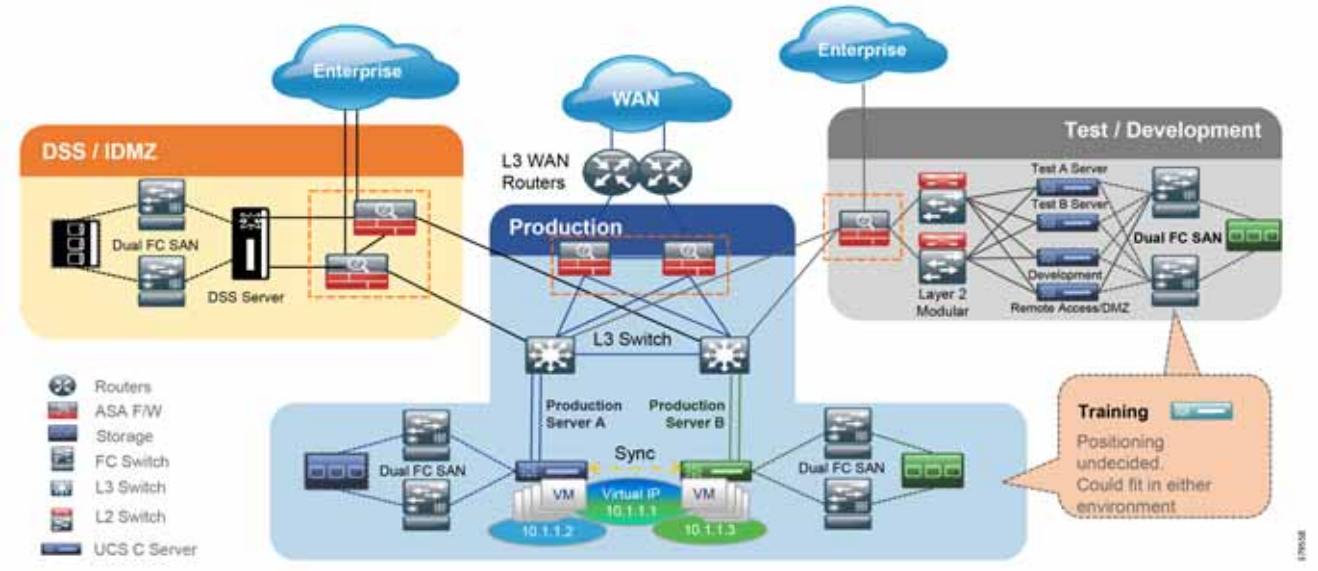
- Multi-service, which are non-production applications that support the operation of the pipeline such as physical security, voice, PAGA safety announcements, video, and wireless.

These building blocks are core components of a SCADA architecture design that can be deployed in one or more Control Centers. Customer philosophy and individual requirements will dictate how these zones are created and into which sites they are deployed. These are typically based on an internal risk assessment to ensure safe and reliable operations. Risk assessment guidelines to help determine philosophy and architectural design are available in the IEC 62443-3-2 standard " Security for Industrial Automation and Control Systems - Security Risk Assessment and System Design."

SCADA Deployment—Physical Segmentation and Zoning

Figure 52 is a suggested architecture, which aligns more with less virtualization and dedicated servers and physical infrastructure.

Figure 52 SCADA Deployment Physical Separation



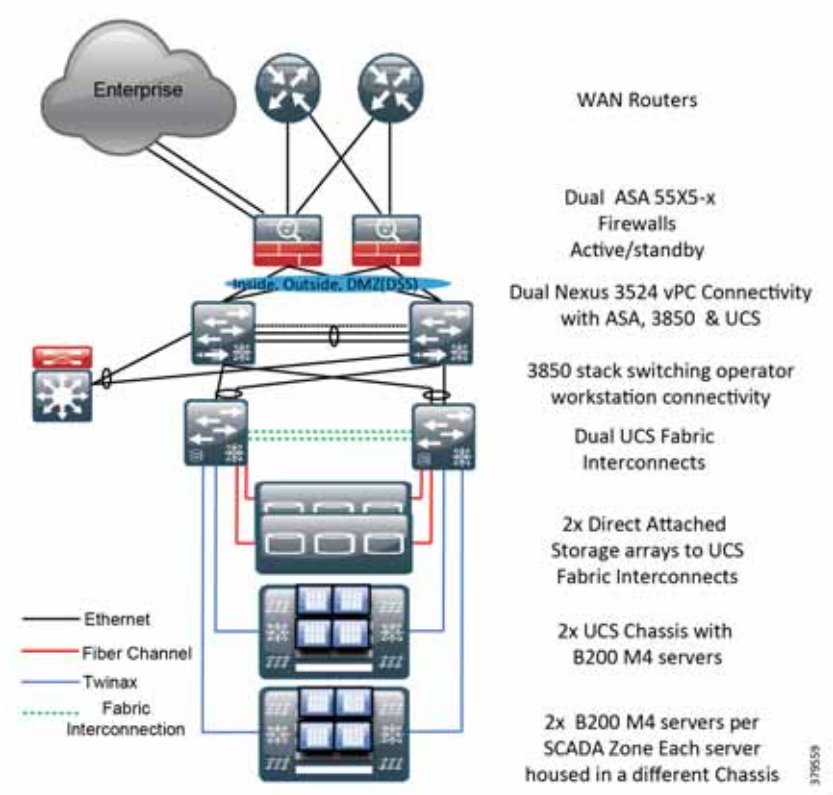
The Infrastructure design for the control center depicted in Figure 52 provides a view of a deployment of physical segmentation for the Control Center. The emphasis is on reducing as much shared infrastructure as possible reducing the risk of impact on one system affecting another system. The expense of this deployment may deter customers from implementing this option, as the below options will increase cost and potentially complexity:

- Each of the Production, DSS, and Test/Development Zones within the operational domain have their own dedicated set of equipment.
- Dedicated storage devices and storage networks. The Production zone (critical control) deploys separate storage systems per redundant environment.
- Dedicated switching equipment and physical links per zone.
- Dedicated firewalls per environment where zone boundary control between each of the zones and external networks is policed.
- Redundancy is provided for all components within the Production zone.
- Virtualization is deployed in this design. Within the environments (highlighted in the Production zone), multiple VMs are deployed for each of the SCADA servers (e.g., Real Time servers monitoring and control, Domain Controller, and the historical server). Ensure that redundant pairs are structurally separated on physical hardware, reducing the risk of a SPOF failing the redundancy configuration.

SCADA Deployment–Virtualized Segmentation and Zoning

A different approach is to go for a shared infrastructure model where cost of implementation and confidence in maintaining and operating the virtualized system are results of the pipeline operator's risk assessment. Figure 53 and the bulleted information that follows provide an overview of the implementation related to restricted data flow and segmentation.

Figure 53 Baseline Integrated SCADA System (BLISS) Architecture



- VLANs providing the segmentation on a per-zone or system level within the Control Center. The production environment seen here will have its own dedicated VLAN as will the test, development and IDMZ/DSS, and training.
- Shared Infrastructure Firewalls, Ethernet switches, Storage networks, and Server Chassis.

- Segmentation for the networking using VLANS extended from the virtual switch in the servers through the switched infrastructure to the zone boundary devices (Firewalls).
- Shared Firewalls providing zone boundary protection per zone and interface to the external networks.
- Storage Segmentation is enhanced with the configuration of Fiber Channel zoning and Virtual Storage Area Networks (VSAN) in a Fiber Channel storage network. These technologies allow the physical SAN fabric to be segmented into smaller logical domains. Each of the environments (production, test, development DSS/IDMZ) will have dedicated VSANs and Fiber Channel Zoning.
- Redundancy of all components.

IDMZ/DSS

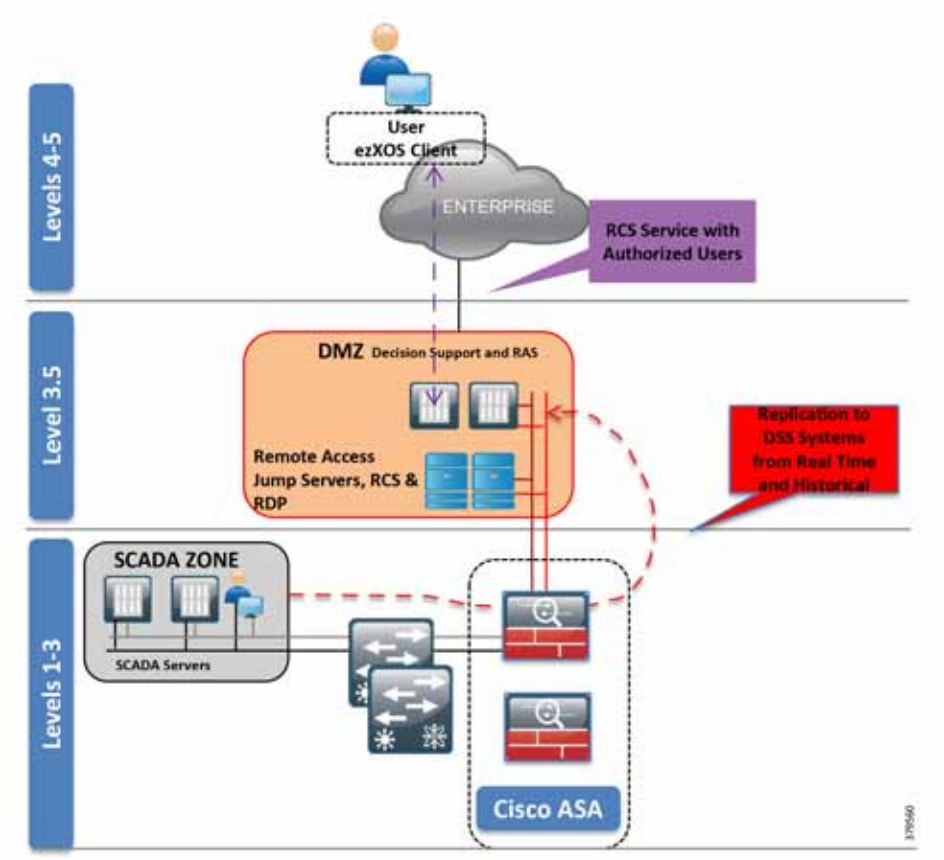
Services and data need to be exchanged between the untrusted Enterprise network and the trusted Process Control Network (PCN). This exposes near real-time and historical information to the Enterprise and allows for better business decisions. Systems located in the Industrial DMZ bring all the data together for company personnel in a near real-time system, allowing the forecasting and change of daily operations that will generate the most revenue for the company.

In aligning with standards such as IEC 62443/ISA99 and ISA 95, the Process Control Domain (PCD) has a requirement to provide strict policy enforcement between the trusted Levels 1-3 of the PCD and the untrusted Levels 4-5 of the Enterprise/business domain. No direct communications are allowed between the Enterprise and PCD. The IDMZ commonly referred to as Level 3.5 provides a point of access and control for the access and exchange of data between these two entities. The IDMZ architecture provides termination points for the Enterprise and the process domain and then has various servers, applications, and security policies to broker and police communications between the two domains.

The following are key IDMZ guidelines and concepts:

- No direct communications should occur between the Enterprise and the PCD. Firewalls act as the zone boundary between the Enterprise and the PCD, following the practice of denying any service unless explicitly configured.
- The IDMZ needs to provide secure communications between the Enterprise and the PCD using mirrored or replicated servers and applications.
- The IDMZ provides for remote access services from the external networks into the PCD.
- The IDMZ should establish a security barrier to prevent unauthorized communications into the PCD and, therefore, create security policies to explicitly allow authorized communications.
- VLAN segmentation within the IDMZ. The DSS/IDMZ could be deployed with extra VLAN segmentation within the environment to provide further isolation of servers.

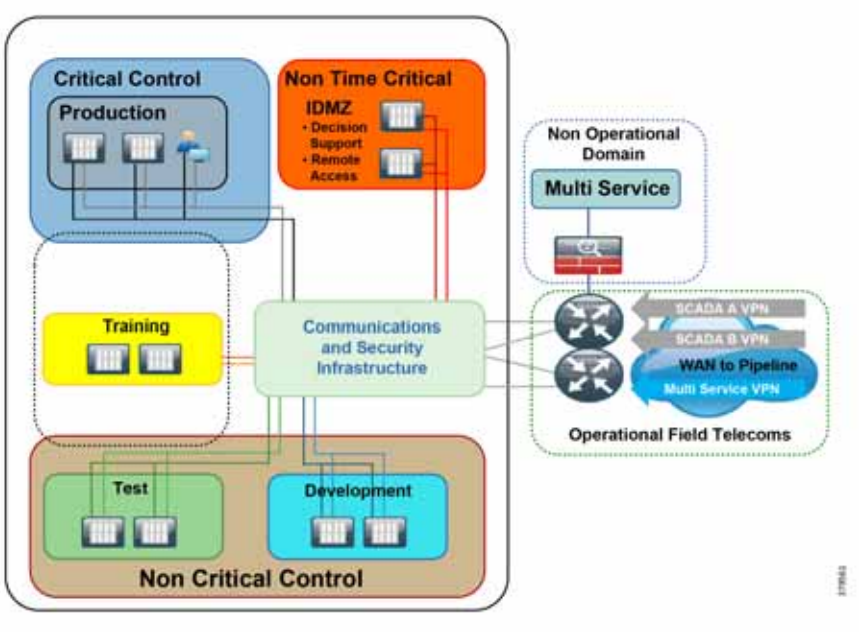
Figure 54 IDMZ High Level Architecture



Multi Service Domain

Multiple services will be deployed to support pipeline communications, physical security, and business-enabling applications within the pipeline architecture. Segmentation of the multi-service applications from the operational communications is a common requirement. Regulatory demands, security concerns, and confidence of the pipeline operator to house the multi-service on the same infrastructure as the SCADA servers will drive the Control Center multi-service architecture. The typical deployment is shown in Figure 55 where the nonoperational domain is physically separated from the operational infrastructure.

Figure 55 Control Center Multiservice Architecture



Operational Pipeline Telecoms and WAN

With pipeline networks increasingly deploying multiservice architectures, securely restricting and isolating services to protect the integrity of the traffic is essential. Intentional or accidental cross-pollination of traffic between untrusted entities must be restricted. Services are segmented (physically or logically) and prioritized so that SCADA networks (operational traffic) and multiservice traffic (non-operational traffic) will not affect each other under normal operations, security incidents, upset conditions, or network congestion. Both logical and physical path isolation techniques can be provided to promote a dedicated infrastructure per service.

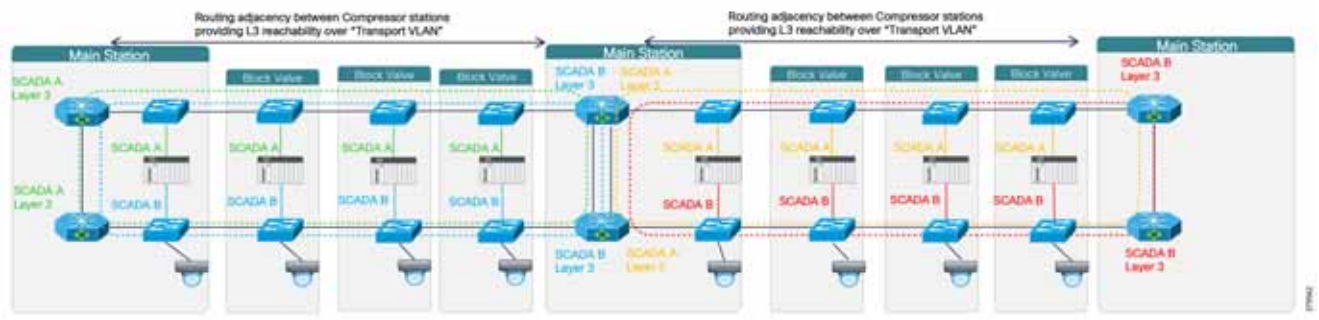
Various connectivity options such as Ethernet, MPLS, dense wavelength-division multiplexing (DWDM), cellular, and wireless can comprise the communications network. Factors that influence the choice of the communications technology include power and space availability at the various sites, physical aspects relating to the environment such as ruggedization, no moving parts, extended temperature ranges, capital and operational costs, the customer's preferred technology, and ultimately, from a security perspective, the results of a risk assessment.

Ethernet

Within an Ethernet architecture, Layer 2 VLANs allow for logical segmentation of operational and non-operational services over the same physical infrastructure. If the physical architecture allows, a dedicated infrastructure per service aligned to VLANs, can be deployed. MPLS is typically deployed in the core. End-to-end logical proven security options through Layer 2 or Layer 3 VPNs from the Control Center to the pipeline stations provide station-to-control center security segmentation and isolation per service. A VPN is also enabled per service. This provides effective use of fiber pairs where logical separation can be employed.

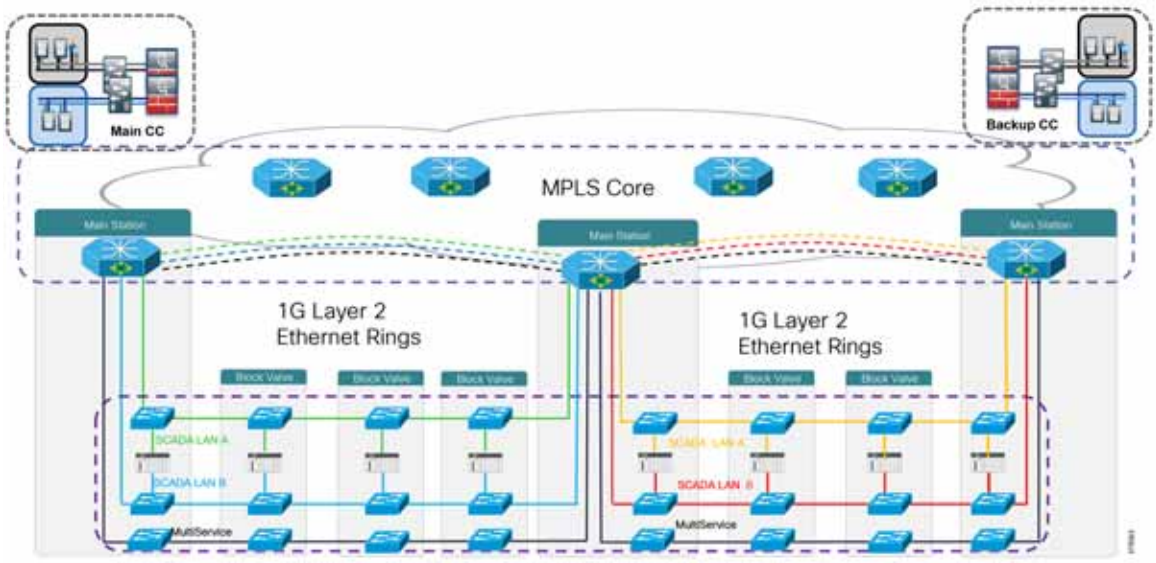
Figure 56 provides a view of a deployment where Ethernet rings were deployed to provide the communications along the pipeline infrastructure. In this example, fiber use was limited and cost was a factor in the deployment so a shared infrastructure deployed with a VLAN per service (SCADA A LAN, SCADA B LAN, multiservice LAN) was run over a single fiber pair and VRFs (VPN) provide reachability back to the Control Centers.

Figure 56 Ethernet Ring Example Deployment



Segmentation shown below in Figure 57 is supported with dedicated fiber per service along the pipeline. Each LAN had its own fiber pair. MPLS VPNs supporting L3VPN services from the pipeline main stations to the Control Centers and for communications between the Control Centers. The SCADA networks and multiservice networks will have reachability through separate L3VPN instances, promoting segmentation and availability. This also provides effective use of fiber pairs where logical separation can be employed.

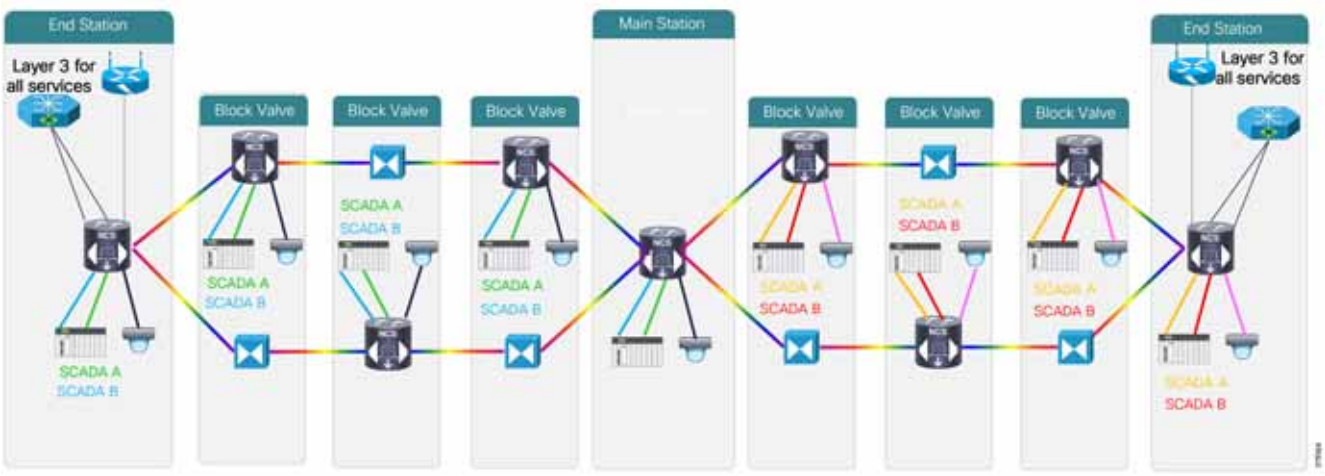
Figure 57 MPLS Example Deployment



Dense Wavelength Division Multiplexing

Dense Wavelength Division Multiplexing (DWDM) is an optical transmission technology that transmits signals at different wavelengths over a single fiber optic cable. With amplification and error correction, the transmission capacity can be extended to 1000s of KM. Proven end-to-end segmentation and isolation can be obtained through wavelength/Lambda separation from the Control Center to pipeline station. Each wavelength will provide a different service.

Figure 58 DWDM Example Deployment



Secure wireless or cellular-based services such as WiMAX, 3G, LTE, and satellite are available for brownfield retrofit in areas where fiber is not available, and as backup to wired technologies. These technologies still allow for the transport of Ethernet and IP, but with restricted capabilities because of bandwidth availability. VPN technologies such as Dynamic Multipoint Virtual Private Network (DMVPN) or FlexVPN provide confidentiality and integrity.

Zone Boundary Protection

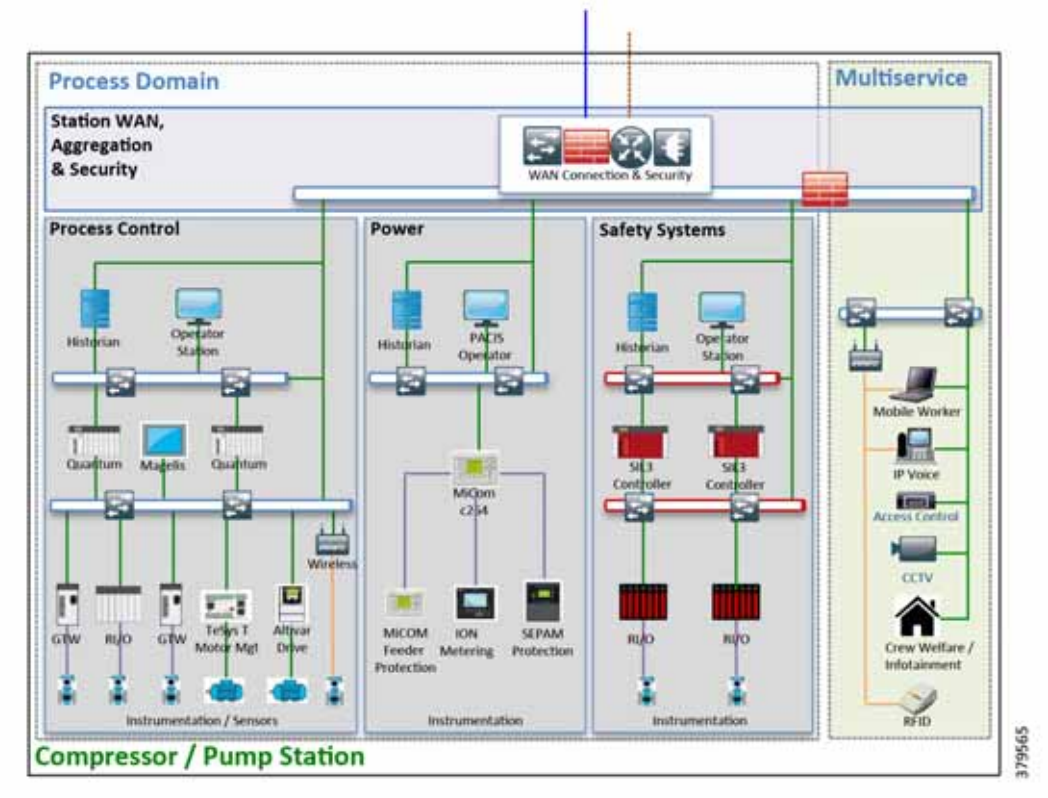
Zone Boundary protection can be provided in any of the architectures and technologies discussed using firewalls deployed at routed boundaries or Layer 3 routers with firewall services and/or access control lists. An example of this within the Operational Telecoms Network is through the introduction of a firewall at the pipeline station edge. Firewalls act as the Layer 3 gateways providing access and policy to the SCADA RTU networking segments from the WAN and between adjacent interconnecting pipeline segments. The Purdue Model of Control does not formally identify this but typically refers to it as a Level 2.5 firewall sitting between the operational domain of Level 3 and PCD Level 2 and below. Within the architecture, the firewalls provide the following functions:

- Inter-zone security protecting the SCADA LANs
- A policy and security point between pipeline segments, which can be used for inter-pipeline security that protects the Layer 2 SCADA networks from the WAN

Station

A compressor/pump station is shown in Figure 59. Here the process domain is completely isolated from the multi-service domain. Within the process domain, each of the Process Control, Power, and Safety systems are further segmented. This would typically be deployed with separate networks and switches. Firewalls at the main station level provide zone boundaries between systems within the station and interface with the WAN and other pipeline networking segments. These are the Level 2.5 firewalls previously discussed in the operational pipeline Telecoms section under Zone Boundary Control.

Figure 59 Large Pipeline Station Architecture



Industry Standards Cross-Reference: Restricted Data Flow & Infrastructure Design

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 9 (FR5) Restricted Data Flow
NIST SP 800-30
NIST SP 800-163
NIST SP 800-53 - SC-5 Denial of Service Protection
NIST Framework for Improving Critical Infrastructure Cybersecurity
ISO27001 Section A13, Network Security
API 1164 Section 6, Information Distribution
API 1164 Section 7, Network Design and Data Interchange
NERC-CIP CIP-005 Electronic Security Perimeters
TSA Pipeline Security Guidelines, Section 7.3 Security Measures for Pipeline Cyber Assets
IETF RFC 7452 Architectural Considerations in Smart Object Networking

Security Operational Management and Monitoring

Security Operational Management and Monitoring Defined

The security architecture of an ICS must incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks. Monitoring and logging activities are imperative for understanding the current state of the ICS, and validating that the system is operating as intended and that no policy violations or cyber incidents have hindered the operation of the system. Auditing provides a means to assess the overall effectiveness of the security implementation as well as provides proof of alignment to any regulatory or compliance audit. Management within the context written in this section involves the auditing of end systems to verify the correct configuration and software versions and provide a process for updating and validating any patches or security updates to the system.

What We are Trying to Solve

To understand what we are trying to achieve it is important to understand the phases of a cyber-attack or incident. A cyber-attack has essentially three overarching phases:

- **Phase 1** is basically an information gathering or reconnaissance phase. The attacker will identify a target and search for vulnerabilities in the system or organization. This could include process and people as well as technology.
- **Phase 2** is when the system is infected though the searched for vulnerabilities and are being exploited, perhaps expanding the foothold within the network and leading to the exploitation of other vulnerabilities within the system or organization.
- **Phase 3** is essentially the result of the cybersecurity incident and is the successful implementation of the hacker's attack. This includes data manipulation and data loss to disrupt the operations of the pipeline, or ultimately the loss of the control of the pipeline system.

The main goal of the security management and monitoring is to identify any threats to the system as early as possible. Security management procedures involve continual threat assessments, software updates, patching, consistent logging, and a monitoring solution that performs monitoring and auditing of the system. Most systems do not discover an incident until Phase 2 at the earliest; however, a thorough management, logging, and monitoring initiative should provide protective measures and incident discovery to highlight incidents starting in Phase 1. The security design and system implementation depends on the risk assessment, which then drives the path for the management and monitoring processes and procedures that are implemented.

Process

Security Operational Management and Monitoring cannot be isolated and reactive, but must take a proactive approach within the lifecycle of the security system. Using the Prevent (Identify and Protect), Detect (Detection and Monitoring), and Respond (Respond and Recovery) security controls, we can align components of the process for security operations' Management and Monitoring.

- **Prevent**—On the surface, the subject seems very much aligned with the Detect phase of the security lifecycle, but all the groundwork and planning needs to be in place in order to determine what needs to be managed and monitored. The risk assessment and associated risk tolerance for the control system will determine the various security technologies and systems deployed to prevent and mitigate any security threats. Once the risk assessment has been created and systems identified that must be managed and monitored for security incidents, the plan for the Detect phase needs to be prepared. Process and people in addition to technology need to be applied. Change management and control, monitoring and auditing processes, plans defined for incident response, and software and patch update testing procedures are all examples of the management component of the security system that are identified in this phase. The last point here leads to the Protect function, which needs to implement the technologies and procedures for security management. Once the procedures and technologies have been identified, these need to be regularly reviewed through the security management lifecycle.

- **Detect**—The risk assessment during the Prevent phase should have identified what is going to be monitored and which technologies we have available. Ongoing maintenance and monitoring are extremely important to maintaining the security health of the system. The Event logging and management strategy and plan is key to identifying any security incidents and, once detected, working with the overall security strategy to help decide mitigation and improvements to the overall security design and implementation. The logging and management not only become integral to the security management and design, but are a major factor for compliance and audits, and after incident activities that provide critical lessons learned.

- **Respond**—Following compromise of the pipeline system, the incident being resolved, and the system restored to operation, a plan for improvements to the comprehensive system hardening strategy needs to occur. An After Action Report (AAR) will help to consider what actions may have been taken that could have prevented the attack, mitigated damage, and improved the business' overall response to the incident. Any documents created in the Prevent phase as part of specifying security procedures or policies would need to be addressed to reflect any updates required. Any security updates or changes must go through evaluation and testing in a non-operational but representative environment before implementing into the operational pipeline system.

Security Management, Monitoring & Logging Requirements

The pipeline system needs to be managed and monitored from a security standpoint to protect against various types of security incidents. Not all incidents are malicious and not all incidents are attacks from external bad guys outside of the operator or company. Internal attacks could be from disgruntled employees who have access to systems to create an incident or who accidentally misconfigure a device, which then behaves erratically and interrupts a process or operation. With this in mind, we need to ensure that configuration control correctly configures and monitors any change in systems. Software patch policies and procedures also need to be managed, ensuring that systems are updated without impact on the operations of the pipeline. Audits of the system should be run to validate that systems are at the correct patch or security level. Along with the configuration control and patch management, the system needs to be monitored continuously to provide an overall security status or risk view of the system. Monitoring the system, networking events, and logs are all key contributors for providing security awareness to those responsible for the system.

The following two sections provide guidance for Security Management and for Monitoring Events and Logging.

Security Management

We break security management into two areas: Configuration Management and Patch Management and Software Updates. Although Patch Management is a component of Change Management, NIST does provide guidance for it to reside outside of Change Management, which we have followed.

Configuration Management

As a component of security management, a configuration management program must be created and maintained. This is to ensure that all modifications or changes are aligned to the security requirements outlined in the asset evaluation and risk analysis. Any modifications, configuration changes, or additions to the pipeline systems and networking devices must be linked to a risk assessment as part of the change management program. This includes addition, deletion, and modification of hardware, software, firmware, and any configuration settings. The NIST SP 800-53 Configuration Management (CM) family provides policy and procedures for establishing baseline controls for information systems. Logging and monitoring any changes provides tracking and auditing capabilities for any compliance, but also provides awareness of any security incidents malicious or accidental in nature. There are eleven configuration management controls to be referenced and applied to the pipeline systems. The following are highlights for each of the Configuration Management control family recommendations from NIST SP 800-53.

- **Configuration Management Policy and Procedure (CM-1)**—Create a documented configuration management program to facilitate the implementation of a configuration management policy and associated configuration management controls.

- **Baseline Configuration (CM-2)**—The pipeline operator establishes the baseline known configuration for all the systems and components. This includes maintaining an up-to-date configuration status of the system as well as backups to support the rollback of any required configurations. This baseline configuration would be used in the test environment, as specified in the pipeline architecture, when looking at testing any updates, patches, or configuration changes.
- **Configuration Change Control (CM-3)**—Document, approve, and test any proposed changes to the baseline system before implementing/deploying into the operational system.
- **Security Impact Analysis (CM-4)**—Conduct an assessment of changes to determine and test (in a test environment) the impact of any changes to the security of the asset changed along with any impact to the overall system.
- **Access Restrictions for Change (CM-5)**—Any changes to the assets of the system can potentially have impacts on the overall security of the system. The organization must implement and enforce access restrictions so that only authorized personnel are initiating changes or modifications to the system. The system must monitor and maintain records to monitor/identify any unauthorized transactions or changes.
- **Configuration Settings (CM-6)**—Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Responding to any unauthorized changes must follow any incident response plan and the operational availability of the pipeline must be paramount.
- **Least Functionality (CM-7)**—As detailed in System Hardening, page 90, the configuration of the assets and systems must only provide functions that are necessary and restrict the use of unnecessary ports, applications, and services.
- **Information System Component Inventory (CM-8)**—The configuration management system must have an updated inventory of all assets on the system to provide a current baseline of the system. This provides identification of all assets that are subject to configuration control and provides awareness of any rogue devices or systems that are not at the required security level (i.e., assets not at the stated baseline approved software level). Asset discovery and inventory management must take care to not affect systems when running any asset discovery services. More details on asset discovery can be found in Asset Discovery and Inventory, page 49.
- **Configuration Management Plan (CM-9)**—Addresses roles, responsibilities, and configuration management processes and procedures to maintain the configuration management plan.
- **Software Usage Restrictions (CM-10)**—Defines the requirements for the tracking and usage of software to ensure that said usage is in alignment with the license agreement, including quantities. Also controls file-sharing technology to ensure that materials are not distributed without proper authorizations.
- **User Installed software (CM-11)**—No direct user-installed software should be permitted within the pipeline system. This process should be monitored so that only authorized and tested software or patches are permitted onto any assets.

Patch Management and Software Updates

Highlighted in System Hardening, page 90, a comprehensive Patch Management process must be a major component of a security management strategy when maintaining and operating a connected pipeline. Patches and updates are generally applied to correct security or software vulnerabilities, but could be in the form of new features and functions to an application. Patches and software updates should be maintained to the vendor's latest recommended software and firmware levels where possible. There are a few challenges that should be considered when applying a patch management process in an industrial environment and specifically here in pipelines.

NIST SP 800-40 Revision 3 [40] provides guidance responsible for designing and implementing security patch and vulnerability management programs and for testing the effectiveness of the programs in reducing vulnerabilities. NIST SP 800-82 "Guide to Industrial Control Systems (ICS) Security," Section 6.2.17.3 provides ICS guidelines and considerations for patch management. The following are considerations for patch and software updates for a connected pipeline.

Software Inventory Management

One of the primary challenges for patch management is understanding what needs to be updated or patched in the system. Without thoroughly inventorying the system's assets and associated software, it is very difficult to provide a comprehensive patch management process. All assets within the system must be discovered in order to create a successful patch management process. Once assets are discovered, the operator must determine which systems require updates or are missing patches based on a vulnerability assessment of the software or firmware levels.

Asset Discovery and Inventory, page 49 discusses the process and method for creating a successful asset discovery process for the pipeline. It's important that this inventory be regularly updated and maintained on an ongoing basis to assist with the patch management process.

Threat Awareness

As well as awareness of vulnerabilities of the pipeline's operational and networking assets, the security systems that monitor the assets also require updates and patches. Updates to IDS systems, anti-malware, and anti-virus systems must be included in the patch management process. Threat awareness assessments are provided for those systems that provide guidance on current threats and vulnerabilities. The operator should factor these into their comprehensive patch management process.

Timing, Prioritization, and Testing

Timing, prioritization, and testing have interdependencies when evaluating when and what requires patch or software updates. In an ideal situation where patches were trusted to perform without affecting the pipeline operations, all new patches would be applied to systems the moment they became available in order to minimize any security vulnerabilities. However, in the real world, this really isn't possible. Patches installed without verifying that operational systems are unaffected pose a serious risk and potentially could have more of a security impact than if the system was never patched. Which patches should be applied and when to apply them is closely related. A risk analysis should be considered as a major component of determining patch updates. The following provides a brief guideline for patch management.

- **Testing**—It is the responsibility of a vendor to evaluate any software updates or patches before introduction to the environment, although potential impacts to the systems still exist when applying the patches. All patches and software updates should go through testing by the operator before applying to the system. In the reference architecture, the control center has a test and development environment, which is used to help validate any updates to the control center such as changes to the OS, application patches, and security updates to systems. Similar processes would be required to verify other systems throughout the architecture so that any patch or system updates are vetted properly. Pipeline station environments out in the field would also require a similar process.

- **Timing and Prioritization**—Not all updates are required to be applied immediately. As mentioned, the timing and prioritization are interlinked. Determining the criticality of the update is dependent on multiple factors that contribute to the overall risk analysis that is considered for all patch updates. For example, is the update required to be applied to critical operational systems? Is the update required immediately as the exploitation is known to be occurring and therefore has a high level of prioritization?

- **System Availability**—A component of the assessment related to timing, system availability is a fundamental issue when looking at when to apply an update. Once the update has gone through testing, it may be identified that the patch requires a system reboot or that one or more applications or services will require restarting. Within a pipeline operational system, operational control must always be maintained. As such, careful planning needs to be done in order to establish a plan of action for the update. For example, systems may need to be switched to backups prior to installing the patch or update and this has to be factored into the update equation when evaluating timing and prioritization for the update.

Legacy Systems

The policies and procedures of the patch management process need to address legacy systems within the operational domain. Some legacy systems may still be in use (for the basic reason that " it works") despite the operating system or software application being beyond its support window. Procedures should include contingency plans for mitigating vulnerabilities where patches may never be available. Regular vulnerability assessments of these systems and monitoring should be planned in order to understand the threats that these outdated assets pose to the overall system. Ideally, a plan should be put in place to address updating or changing the system to remove any potential threat; however, this needs to be evaluated and addressed as part of the overall risk analysis to the operations of the pipeline, ensuring that the decision is in alignment with the amount of risk an organization is prepared to accept.

Patch Distribution

Following best practice guidelines, any security servers such as patch management or anti-virus servers should be located in the IDMZ. Direct communication from the outside world into the operational domain (Level 3 and below) must be restricted. These systems should be set up to be dedicated for the operational environment so that updates can be tailored for the pipeline systems.

Updates should not be automatically applied as is sometimes the case in traditional IT environments where wide distribution is applied to all systems after testing. As mentioned earlier, the security admins must factor in the operational state of the pipeline when applying the updates. In short, tighter control of the update process must be applied in targeting specific systems that require the update.

Monitoring Events & Logging

A thorough management and logging program provides awareness and helps identify any security incidents during Phase 1 of an attack/incident. At a high level, important organizationally-defined security events should be monitored and logged to a central system and provide real-time awareness of the security state of the pipeline system so that incidents can be easily analyzed and acted upon in a timely manner. Logs, which can be useful for performing auditing and forensic analysis to aid any organizational investigations, can be used in establishing baselines to help identify issues over a longer period. Besides the inherent benefits of log and event management for security; regulatory or compliance requirements may exist that compel an organization to store and provide logs.

The pipeline operator should perform testing and validation activities periodically to confirm that the organization's logging policies, processes, and procedures are being followed properly, both at the infrastructure level and the system level, throughout the organization. Log management audits can identify deficiencies in policies, procedures, technology, and training that can then be addressed. Audits can also be helpful in identifying effective practices, such as particular configuration or filtering settings, which may be beneficial for use on other systems.

Log and Event Sources

Fundamentally, in an ideal world, you would want to log everything within your system. This isn't achievable on a practical level with the vast amount of data that is generated by today's control systems. Pipeline systems have many log sources or data points; security alone includes assets, users, IDS systems, network equipment, firewalls, and applications, while the control system will provide other sources of operational logs such as alarms, events, and operator tracking. The log management system and tools can be easily overwhelmed by the sheer amount of data that could be generated. Careful planning and assessment of what needs to be monitored and prioritized for the pipeline are required first steps. The following provides a view as to the various sources that could be logged and monitored, but is not an all-inclusive list.

OT Assets

OT assets that can create events and logs should be enabled. The OS, application, or file system can generate logs that help provide security awareness of an asset. If critical OT assets do not have a logging capability, then other systems could be used to provide this needed, but missing functionality. For example, flow-based metrics to look at traffic patterns on the network or using data posted to the historian are potential avenues for logging against these types of devices.

Historians

Historians could be used to provide additional awareness of non-network connected assets or those not available to network flow-based technologies. If the RTUs do not have the ability to produce logs or event data to the SIEM, then historical data from these systems or devices could be used to provide input into the SIEM and then could be normalized.

Applications

Applications generally generate their own log files and vary significantly in the logs generated as they are application specific. Items include account information, usage information, and changes.

OS Monitoring

Operating systems for servers, workstations, and networking devices (e.g., routers and switches) usually log a variety of information related to security. System events and audit records are the most common:

- System events are operational actions performed by OS components, such as shutting down the system or starting a service.
- Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes, and use of privileges.

Firewalls

Firewalls provide boundaries between zones in the pipeline environment. They are able to detect any traffic attempting to traverse zones and are ideally situated to help identify anomalies in the network.

IDS Systems

Host-based or network-based IDS systems monitor the network or system for advanced threat detection using packet inspection techniques to detect suspicious data based on pre-defined signatures and settings. These systems must alert the SIEM when a security event is discovered. DPI to the protocol level is now enabled on industrial firewalls. Industrial firewalls have the capability to look deeper into packets of industrial protocols helping to improve anomaly detection.

Networking Equipment

Logs and events from networking equipment such as routers and switches can provide data related to the availability aspects of a network (e.g., failed network interfaces) or by using security events such as configuration changes or high CPU or memory metrics to trigger alerts with regards a possible security incident.

Network Flows (sflow)

Network flow data, which is generated from networking equipment, provides details of communication flows with source IP, destination IP, source port, destination port, and packet/byte count. These network flows can provide data for advanced anomaly detection systems and turn the data into actionable intelligence, effectively turning the network into a sensor itself. This anomaly detection system would then forward logs and events triggered to the SIEM.

Users, Logins, and LDAP

Auditing and tracking access to systems as well as the assets and information a user has accessed is a key security requirement. It can be used for real-time monitoring for security incidents such as unauthorized access or multiple failed password attempts. It can be used for investigative or forensic analysis, post-event. User monitoring generally requires correlation between multiple systems. Monitoring who has accessed a system and what they accessed or modified would need contextual awareness and normalization of the data from LDAP and application logs. These are key attributes of SIEM.

Configuration Management

As part of change management, the logging system should monitor any changes to configurations on systems along with identifying who made these changes. This would need to be considered for all systems.

Please note that this is focusing on the security aspects of monitoring and logging. As noted, control systems have other requirements for logging and archival storage from the operational perspectives. It is important to note that some of this information could be summarized or used as a component of overall system monitoring and health, which would provide additional triggers that could alert on an unusual circumstance, warning the OT team of a possible security incident.

Evaluating that the log sources generating information are not affecting the system should also be tested and evaluated. An example might be a host-based monitoring system, for example, a host-based IDS affecting the performance of a critical asset. As with everything that is deployed to the production environment, even the security tools must be evaluated with regards to security and system performance impacts.

Security Incident and Event Management (SIEM)

The following challenges and requirements need to be met when addressing security monitoring, logging, and event management:

- The first challenge for the pipeline operator to address is compliance and regulatory requirements along with addressing any internal policies that may be required for audits.
- The second is to use logging and event management to enhance and address security monitoring across the pipeline systems, assets, and infrastructure.
- Finally, the management of the sheer volume of data from the many sources of data generating real-time events that require both short and long-term storage requires significant effort and planning.

With all of the various systems and technologies involved, no underlying way exists for normalizing, aggregating, and correlating the data across these systems and technologies. A SIEM system, which provides centralized real-time monitoring and longer-term analysis for security events and compliance, can help address these challenges.

Normalization

Normalization of data needs to address the various formats and information that is sourced from logging and events. Normalization provides a mapping of log messages and events from multiple assets or systems into a common data model. This provides an organization with the ability to correlate and analyze related events even when created in different data formats or across different sources.

Aggregation and Correlation

Aggregating the data to a centralized system so that all events can be correlated provides benefits for reducing the volume of event data and consolidating duplicate records from multiple systems for the same event. This event correlation helps speed up detection of possible security incidents in order to create an actionable item for the operator or administrator.

Contextualization

Providing context to the data beyond event and log correlation is essential. When events have greater context, it becomes easier to assess the relevance of any threat and its impact on security or the operations of the pipeline. An example for context could be interaction with a user database to provide a mapping of a user-id to name and access privileges. Another source could be a threat intelligence database to add context to a detected threat and determine if the threat is critical or not.

Log and Event Sources

The vast amount of data generated for logging and monitoring requires careful planning and fine-tuning of what assets should be monitored. As mentioned previously, a risk assessment should be performed that will determine what assets and systems will be configured to generate events and logs. Within these assets and systems, finer tuning is required to determine what events generate a log or what level of logging is required. This needs to be reviewed over the security lifecycle of the system with regular tuning being addressed as part of this cycle. To help assist with data normalization and correlation, the messages should have common fields or data attributes where possible (for example, timestamp, IP address, source port, protocol, and device/hostname for any data flow-related event). Another example for user logins to a system could be IP-address, username, timestamp, and device/hostname.

Timing

The exact timing of any events or logs is extremely important for correlating information from multiple sources. Where possible, all systems providing information should have a trusted common synchronized timing source. The NTP is a common timing method that is used to synchronize time across all networking, hosts, applications, and systems.

Storage, Data Retention, and Data Security

The vast amount of data collected requires a large storage repository and a process to monitor the data. Determining the length of time to collect data and what the long-term data strategy for auditing and compliance should be, are all part of the planning conversation. The data needs to be securely stored and must be prevented from being accessed by unauthorized sources. The organization cannot afford for any of the data to be changed, manipulated, or lost; therefore, appropriate backup mechanisms must be considered.

Reporting

Finally, the SIEM must provide capabilities for providing real-time alerts to those responsible for the security of the pipeline. Part of the incident response plan should designate who should be notified about a security event. This could be the pipeline operator, although this would typically be another entity such as an OT/IT network admin or security administrator. Generally, a risk management dashboard should be provided that gives insight into the security state of the pipeline that includes logging and monitoring data, but also patch level and asset awareness data.

Historical analysis and reporting functions are part of the SIEM. Security analysts will want to see an audit trail of any event and forensic analysis that can be used as part of the response phase to assist in creating an After Action Report (AAR).

Managed Security Service Providers

Security management, logging, and monitoring of the pipeline system may be overwhelming, costly, and too complex for an operator to administer and manage. Therefore, the required task of a security team to constantly monitor, evaluate, and quickly respond to incidents is sometimes contracted to a Managed Security Service Provider (MSSP). MSSPs have correlation and analysis engines for processing the vast amounts of events logged per day and reducing them to a small subset that needs to be manually evaluated. They can take on the asset discovery and assist in providing risk and vulnerability assessments. The operator must work with the provider to understand the operational and security requirements of the system in providing the security management plan and processes.

Industry Standards Cross-Reference: Security Operational Management and Monitoring

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 10 (Foundational Requirement 6) Timely Response to Events
NIST SP 800-30 Guide to Risk Assessment
NIST SP 800-53 Security and Privacy Controls
NIST SP 800-92 Computer Security Log Management
NIST Framework for Improving Critical Infrastructure Cybersecurity
ISO27001 Section A12, Operations security
ISO 27031 Section 8.1.2
API 1164 Part 3 Management System
API 1164 Part 7 Network Design and Data Interchange, Network Management
NERC-CIP CIP-008 Incident Reporting and Response

Business Continuity Planning and Disaster Recovery

Business Continuity Planning and Disaster Recovery Defined

In many instances, people will equate Business Continuity Planning (BCP) with Disaster Recovery (DR) and struggle to understand why they should be treated as separate components within risk management and mitigation. BCP is the process for creating a plan for how the business will continue to provide its services in case of a disaster. On the other hand, DR is the process followed to recover the business activities after a disaster occurs. The former is strategic, while the latter is tactical. Combined, they form the backbone of a comprehensive program aiming to help a business survive any form of disaster.

In the early days of IT and OT, a disaster would normally imply the occurrence of a natural disaster, such as weather, flooding, or fire. However, in today's digital era, disasters have been expanded to include cyber-based events, such as ransomware, malware, compromised data, and DoS attacks, in addition to insider threats or internal errors. Depending on a company's security profile, the impact of these events can be every bit as devastating as a natural disaster.

Through these two activities, Business Continuity Planning and Disaster Recovery, a business can know where to focus its recovery activities, and thus implement the correct Disaster Recovery activities in order to restore business operations as quickly as possible.

What We are Trying to Solve

BCP and DR are key components of a comprehensive Risk Management program. In earlier sections, we highlighted how a risk assessment identifies risks to the business and the type of actors or events that might trigger the risk becoming a reality. In this process, mitigation strategies and cost profiles would be developed, assigning priority in such a way as to guide the risk mitigation activities.

When a disaster strikes, warnings rarely occur. Therefore, for a business to successfully weather a severe impact to its operations successfully, it must take steps to establish a plan on how to recover from major incidents and quickly resume operations. For example, if your primary control center is affected with flooding from a hurricane or unexpected heavy rains, what is the process for continuing to operate your assets and what is the plan for returning the primary center to control status following the storm's passing? An important component of Business Continuity Planning is understanding what type of downtime your business can tolerate and how to speed the restoration of key internally- or externally-facing services.

Disaster Recovery is the process of restoring business functions as identified by the BCP. These actions, which must be planned ahead of time, include personnel assignments and roles, so that when a disaster strikes, the plan is ready to be implemented. The team needs to know what needs to be accomplished and where to focus their activities to restore key components of the business rapidly. This will enable other business areas that have interdependencies to recover quickest.

BCP and DR go hand-in-hand. Examples of issues that could trigger the need for DR activities and that should be identified within a BCP include drive failures, data deletion, malware incidents, power failures, natural disasters like hurricanes, snow storms, and tornadoes, as well as operational emergencies such as a leak or explosion. It is critical that operators plan for how each of these categories of events should be addressed when and if they happen. In the following sections, we will make recommendations on how to progress in these areas.

Business Continuity Planning

The first steps in creating a comprehensive Business Continuity Plan is assessing your business processes, determining vulnerable areas and how they become vulnerable, and determining what losses the business will suffer if one of these processes failed for hours, a day, several days, a week or even longer. This will frame the items that are most important to the business and will guide the BCP in terms of priority.

Process

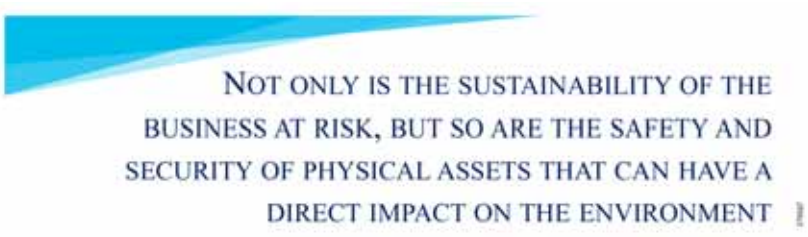
The process of creating a BCP consists of several steps, as found in the following table[1]:

BC Planning Steps	Description
Clearly determine the scope of the plan.	You cannot boil the ocean; therefore, it is necessary to focus on the critical components of the operation, what dependencies exist, and a system's or function's importance to the overall business in a crisis. For example, field communications and operations are critical; however, corporate connections may not be as high a priority and are therefore lower on the recovery chain. Therefore, scope needs to be about what types of scenarios to address, the crisis they might create, the systems affected, and then a framing of the steps that follow.
Document the key business areas that need to be addressed.	Having identified the scope of the BCP, the next step involves clearly identifying the business areas that are fundamentally strategic to business operations. For example, field communications, which are critical, would rank high on recovery efforts.
Determine each area's critical functions.	This step is aligned with the scope step, but is intended to be a deep dive into each identified business area's functionality and the impacts to the business overall. By clearly identifying the areas of the business that are truly strategic, you reduce the recovery risk to a manageable level.
Identify the dependencies that exist between these areas and key functions.	This step helps to clarify the recovery order and to help establish the order in which activities need to happen to ensure the most rapid recovery possible. When looking at these elements, it is conceivable that what might have been thought to be a minor component, for example internet access, might suddenly become significant as a nexus for several other core activities and therefore needs to be addressed quickly to enable other key components to be restored.
Determine how much downtime is acceptable for each area and/or function.	This is a difficult step, because everyone will want to say that they cannot be down for even a second or the business will collapse. This we know from experience is not true across the board, therefore take the time to consider downtime of components based on how you determined their significance in the business along with where they fall in the dependency chart and consider the cost/impact to the business related to downtime. This will help to address the importance of key components and provide you with reasonable time frames for recovery.
Define a plan to recover each area and/or function.	This moves us into the actual recovery process. In this phase, based on the prioritization, downtime tolerance, and dependencies, a plan is created for the recovery of services in proper order to achieve the most rapid restoration of services that is possible. Please note that no disaster will ever align 100% with the plan, but having a framework upon which a business can react with established plans will help it respond to an incident, either natural or cyber, with confidence that it's been thought through and properly planned.

1. Lindros, K., & Tittle, E. (2017, July 18). How to Create an Effective Business Continuity Plan. Retrieved from CIO: https://www.cio.com/article/2381021/best-practices/best-practices-how-to-create-an-effective-business-continuity-plan.html

Why BCP Matters

The ability to recover from a natural or cyber disaster directly affects the long-term viability of a business. In the OT space, not only is the sustainability of the business at risk, but so are the safety and security of physical assets that can have a direct impact on the environment. For example, when field communications are unavailable and operations are unable to safely see and operate the assets, people are put at risk potentially, either those near the lines or those that might have to respond to manually operate or shutdown the lines. In addition to the people, the environment can be placed at risk, affecting business reputation and placing the business at significant liability, both in human and financial terms, as well as harming the environment.



The energy sector is a component of most nations' critical infrastructure, which means that national security is directly affected when O&G pipelines become inoperable for any reason. Coupled with the liability issues associated with impacted operations, the ability to restore operations quickly ensures that the safety and security of large portions of a country's population will be able to recover from a shared disaster quickly and with minimal impacts to society.

Lastly, cyber incidents are a form of disaster that can affect not just your own operations, but have a potentially direct effect on the operations of your customers and business partners. For example, a cyber incident that exposes customer financial data or operational constraints that are part of their competitive advantages will damage reputations and affect financials. A cyber incident could take operations down, creating a situation similar to a natural disaster, or it could falsify commercial information bringing into question the validity of commercial invoices.

In the end, the business needs to consider a broad set of scenarios, and then narrow them to those that will have the greatest impact and to create plans that address the most critical components of the business, ensuring the quickest recovery of operations and business functions.

Disaster Recovery

Having considered the concepts related to the BCP, it is now time to turn to the creation of a DR plan. This is where the strategic components of the BCP meet the tactical process of actual recovery and bring the critical assets back online while restoring their functionality to the business, even if in a reduced capacity.

At this stage, you select a scenario or related scenarios and put a team in place to consider how to address the incident. Items to consider include:

- **Roles and Responsibilities**—Be sure that each team member knows what they are responsible for when planning and during the actual crisis. Review the team membership at least annually, and consider a backup if someone is not available.
- **Communications**—The team must communicate across various arrangements, internally, with those that have dependencies, and the rest of the organization. This is not necessarily simple, as cellular networks may be down or overwhelmed, or internet access may not be available, eliminating or reducing social media and email. This points out that the team must be creative when considering how they will communicate and have several options.
- **Equipment**—Clearly specify the tools, supplies, and spare equipment that you will need for executing the recovery plan. Consider where it will be stored and how the team will be able to retrieve it during an emergency. For example, if spare routers, firewalls, or servers are part of the expected recovery plan, storing them in the same building that would be subject to isolation or disaster may make the spares unavailable, thus causing the plan to fail prior to it even starting.

- **Preventive or Preparatory Activities**—In this area, the planners must consider what actions should be regularly a part of the actions (e.g., system backups or backup centers with valid system images) that will prevent, mitigate, or prepare the organization for recovery. Without the proper preparatory activities in place and their results regularly verified, the pieces needed for a recovery process will not exist and the business will have a much greater challenge in recovery.
- **Document**—Fully and formally document the DR plan. Consider where the plan is stored and how team members will access it. As noted in the next section, be sure to stress test the plan at least annually so that team members are familiar with their obligations and that the plan addresses the current needs of the business.
- **Budget**—Each of these activities requires a cross-organizational commitment of time, resources, and budget. It is imperative that these activities be clear line items in both the budget process and activity planning. Without a formal commitment of time and dollars, these activities will not be given the priority that they require. Consider how to actively include these tasks into your overall operations plans, ensuring that when a disaster strikes, your DR activities will be current and ready to execute.

DR plans will change and must be reviewed and updated throughout their lifecycle. Equipment changes, software upgrades, and operational structure changes all contribute to the need for plans to be updated to reflect these changed states. If this is not done, when the crisis arises, the plan will not address the need and the critical services may not be able to be restored in the anticipated time frames. This could result in catastrophic damage to the business or the operating assets.

Validating the Plan

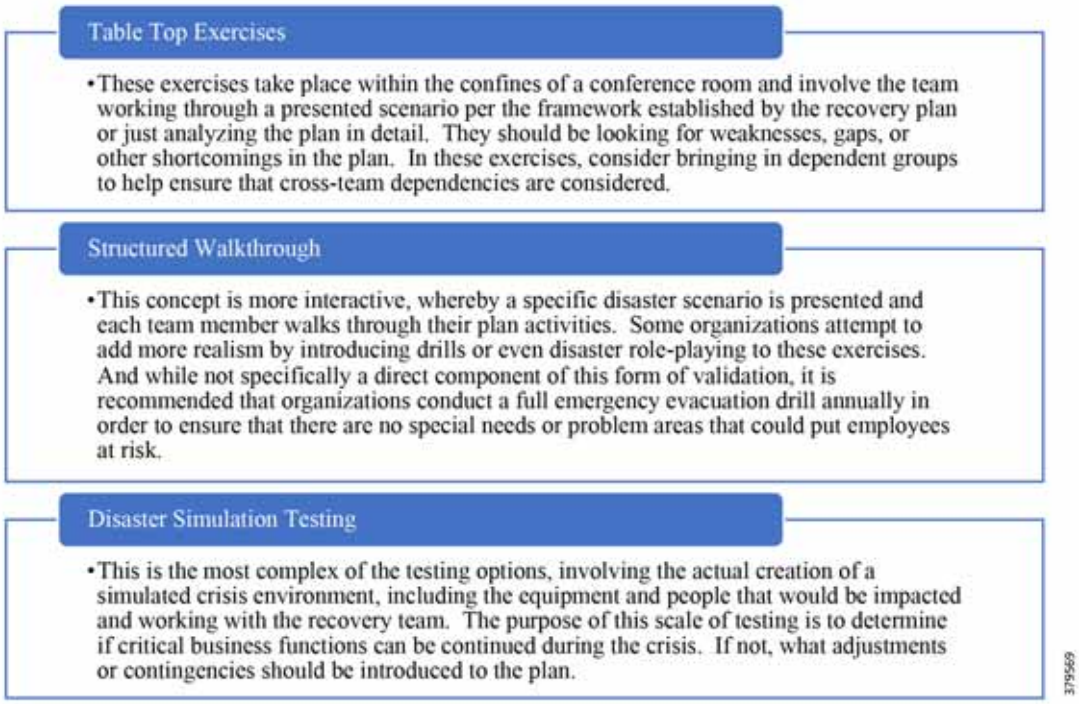
Developing a plan, but failing to validate the plan to ensure that it addresses the issues it was designed for, means that you only have a wish list. Regular reviews of the various BCPs must be performed. Some organizations execute active tests two to four times a year[1].

When considering your test objectives, it is important to make them realistic and with measurable goals. If you oversimplify the test scenarios, you risk not identifying key weaknesses that during an actual crisis could cause the recovery plan to fail or be significantly delayed and therefore cause unnecessary risks and costs to business operations. As such, make the exercise challenging, stretching the capabilities of the assigned teams. As the testing cycles progress, consider swapping in new personnel in order to gain a fresh perspective, potentially identifying an overlooked component in the plan. In addition, outsiders can help challenge the designated recovery team, pushing the teams to look at areas of the plan that they may be overly comfortable with, again helping to de-risk the plan by addressing possible weaknesses.

1. Lindros, K., & Tittle, E. (2017, July 18). How to Create an Effective Business Continuity Plan. Retrieved from CIO: https://www.cio.com/article/2381021/best-practices/best-practices-how-to-create-an-effective-business-continuity-plan.html

Testing can take several forms (Lindros & Tittle, 2017), as shown in Figure 60:

Figure 60 Example Validation Exercises



Following any of the test exercises, it is necessary to produce AARs that capture the positives and negatives along with identified improvements. A formal review and action plan to apply lessons learned to the various plans is required; otherwise, the business risks wasting the opportunity. It is important to remember without all parts of the business being active participants, the plans will not be fully vetted and that places the recovery process in a time of real crisis in jeopardy.

ICS Considerations

ICS companies may believe that their operations system is structured in ways that makes a comprehensive BCP and DR program unnecessary. Most ICSs have hot redundancy as a native component, which enables the system to support single component failures. This redundancy is found within hardware such as redundant power supplies, in the system architecture with redundant servers, and in the network with fault tolerant network infrastructures. Many, especially those that follow the recommended SCP Reference Architecture, will have Backup Control Centers (BCCs) that will enable them to maintain operations if the Primary Control Center (PCC) becomes inoperable. Additional organizations add engineering and test and development systems to their architecture, enabling them to perform tests on patches, upgrades, and the like, reducing the risk of an issue once installed in the main operations center.

All of this is necessary to help reduce the risk of an operational system failure. However, these structures do not necessarily protect against incidents like a ransomware attack, device compromise such as man-in-the-middle spoofing, or malware that spreads throughout the system causing system failures, even across redundant systems. Other scenarios, including natural disasters, or possibly attacks beyond the organization's self-determining scope, such as when a strategic partner is hit, can cause the business to lose access to business systems, either through Distributed Denial-of-Service (DDoS) style attacks or through system failures at the cloud level. These may not affect the operations system and the safety of the assets, but it will affect the business overall and requires consideration in BC planning.

As such, the OT and IT organizations need to form a hybrid team as part of BCP activities. Each brings a unique perspective and set of tools that can help identify weaknesses or incidents, cyber or natural, that could create serious downtime for the business, requiring implementation of selected recovery plans or contingency actions.

In addition, where operational systems have complex redundancy and backup sites, formal plans to regularly validate these systems and their abilities to function need to exist. Do plans exist to address what happens if multiple points of failures occur and are the steps needed to restore functionality clearly identified? What if the backup satellite links are inoperable at the same time a cellular communication outage occurs? One can argue that these are rare situations, but disasters are those rare instances that a business must be ready to address.

Conclusion

The key takeaways from this discussion is that it is critical for an ICS operator to consider the various types of disasters that might befall not only the OT system, but the IT infrastructure and the business components that rely on it. By openly and honestly creating first a BCP, the business can clearly identify the critical components of its business, the parts that depend on them, its downtime tolerance, and how to quickly and effectively recover from a failure to restore critical business components and continue operations.

Validation is also a critical component of the BCP and DR process. Without proper vetting of the plans, the organization will have no confidence that in a time of emergency, people will execute the desired recovery processes quickly and as pre-planned. If crisis actions are left unplanned, the people needed to address them may not be available at the time, further risking the business.

Lastly, ICS operators often have extensive redundancy and backup plans and/or architectures in place. However, while these are robust, they are often limited in scope to just the OT and, even so, may not survive multiple points of failures. It is important to question your continuity plans and consider how they may be tested during a disaster and to clearly answer whether they are sufficiently comprehensive to weather a natural disaster or damaging cyber-attack.

Industry Standards Cross-Reference: Business Continuity Planning and Disaster Recovery

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 11 (FR7) Resource Availability
NIST SP 800-30 Guide to Risk Assessment
NIST SP 800-53 Incident Response Control Family
NIST 800-61 Computer Security Incident Handling Guide
ISO27001 Section A16, Information security incident management
ISO 27031 Business Continuity Section 9.2
ISO 27031 Business Continuity Section 7.3
ISO 27035 Security Incident Management
API 1164 3.4 Business Continuity Plan (BCP)
API 1164 3.5 Incident Response Plan (IRP)
NERC-CIP CIP-009 Recovery Plan for Critical Cyber Assets

Physical and Environmental Security

Physical Security Defined

Physical security is central for preventing unauthorized persons from entering a physical facility or stealing something of perceived value. The safety of personnel should not be overlooked in this respect.

Physical security shall include but not be limited to:

- Protection from burglary
- Theft
- Vandalism
- Tampering

Environmental threats including fire, flood, natural disasters and contamination from spilled food/drink should be considered as well.

The following is a brief overview of some of the subsystems normally used to physically secure and protect the operations in the O&G operating environment.

Integrated Architecture for Premises' Physical Security

An integrated architecture for a premise's physical security is a requirement in a properly designed pipeline architecture. It should consider how critical facilities are to be monitored and identify areas such as doorways, entrances to the plant, external fences, critical rooms, and assets as key components of a monitoring and control strategy.

Analytics and artificial intelligence can be used to improve the level of integration of the different security systems, providing a means to reduce false alarms by crosschecking possible incidents using several sources of information.

Physical Access Control

The physical Access Control System (ACS), which is one of the key components of an Integrated Security System (ISS), is a key component of a global strategy of physical protection of information resources. The traditional workflow of these systems is the following:

1. A credential is presented to a reader.
2. The reader sends the credential's information to a control panel.
3. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database.
4. When access is denied based on the access control list, the door remains locked.
5. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door.

Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The process explained above is for Single-Factor Authentication (SFA). SFA, however, is considered too weak to protect critical facilities or infrastructures, which is why today it is recommended to use some form of Two-Factor Authentication (2FA). In this kind of procedure, a second factor of authentication is required. The second factor can be a PIN, a second credential, operator intervention, or some biometric credential.

Security experts, normally talk about three types of factors when considering authentication:

- Something the user knows, like a password or PIN
- Something the user has, like a badge or a smartphone
- Something the user is, such as a fingerprint, verified by biometric measurement

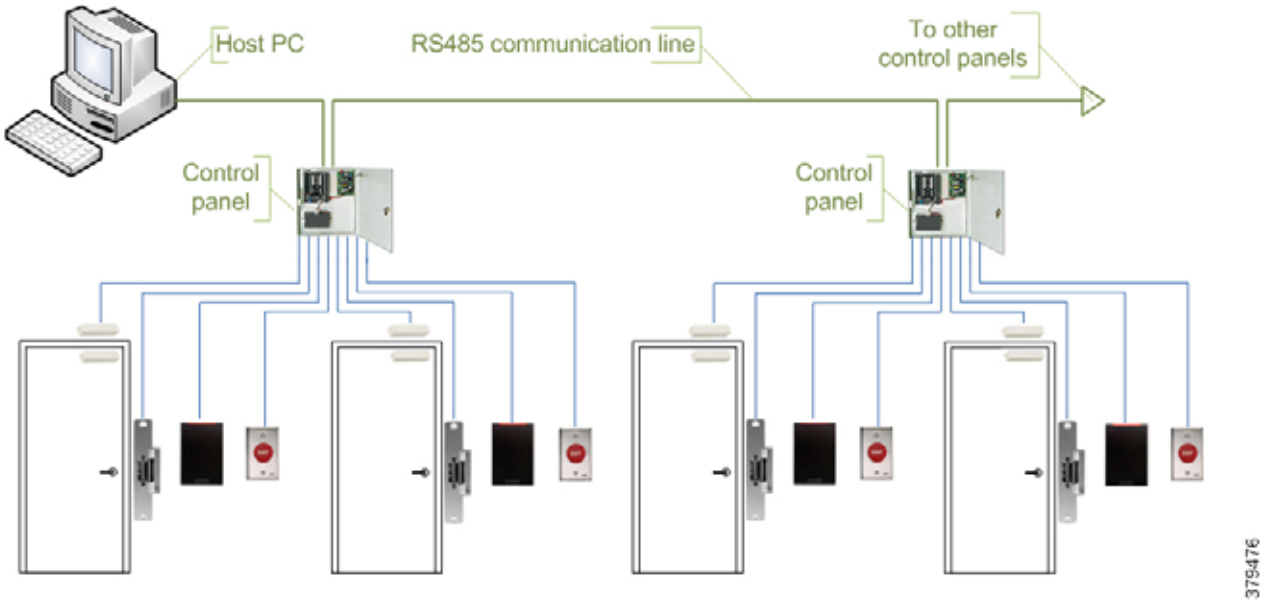
A strong secured access control system normally involves two or three different types of factors to make it more robust. For example, using a password you know and a PIN code you will receive via your smartphone, or a password and a biometric confirmation via your smartphone.

Typical Topology

Figure 61 below shows a typical topology of a traditional Access Control based on badge readers.

The IoT is having a major effect on ACSs. In addition, most of the technologies and systems now available on the market are fully based on IP, where the card reader and the locks can be directly connected through IP to a central server where all the information about the users is stored. While the use of IP could arguably expand the attack surface, these new systems also allow the use of cryptographic technologies to add a new layer of security.

Figure 61 Badge Reader Based Access Control



Security Risks

The four most common risks of intrusion through an Access Control System today are:

- Following a valid user through a door
- Levering a door open
- Natural disasters
- Cyber attacks

Cyber attacks are not so common today because of the nature of the technologies traditionally used in this industry, but the cyber attacks will become increasingly relevant in the coming years, which is why considering the link between the physical and cyber security explained in another part of this section is very important.

Personnel Tracking System

The physical ACS helps ensure that only validated users have access to certain areas within your facilities, but, by itself, cannot tell who is in each area at a certain moment in time.

This is the main goal of a Personnel Tracking System (PTS), which from a security perspective, has a double purpose:

- Information about the number of people in each area in the case of a security or safety event.
- Ensuring that everyone reaches a safe area in the case of a security or safety event.

Typical Topology

PTSs typically have a link to the ACS and, in most cases, they can share some of the components such as the card reader. Sometimes the PTS is an additional function of the ACS. Some commercial solutions consider it as an add-on, but in Oil and Gas, it normally implies some additional components to track the employees in order to be sure that they have reached safe areas in the event of a safety-related incident.

Security Risks

This system, which is highly linked to safety, is normally identified as a critical subsystem, even more critical than the ACS itself.

This is a good reason to include it in the Risks Assessment procedures of the company and to review the cyber-security associated with it.

Video Surveillance and CCTV

Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a set of monitors and record the videos in a secure way for further analysis with different purposes. In the O&G environment, a CCTV system is used for many goals, mainly:

- Operations
- Safety
- Security topics, like live monitoring, motion detection, intrusion detection, etc.
- Tracking people through video analytics

This section will focus on the security topics as the main goal of a CCTV system.

Historically, CCTV systems in O&G have been based on analog cameras requiring a large amount of cabling and are considered difficult to install, deploy, and maintain.

However, today nearly all Greenfield systems are IP based, a fact that helps customers to reduce the time to deploy these systems, facilitating the installation and the maintenance of a CCTV system and multiplying the number of applications that can benefit from such a system, thanks to the adoption of video analytics and advanced cloud services.

With IP-based CCTV systems, additional aspects need to be considered to ensure the proper design of the system. These aspects are right-sizing and the design of the communications network used by the CCTV system along with the cybersecurity aspects mentioned above as a component of the overall security risks in this section.

Many types of camera options are available, depending on the environment, the location to be installed, and the kind of information you want to capture. The main types are:

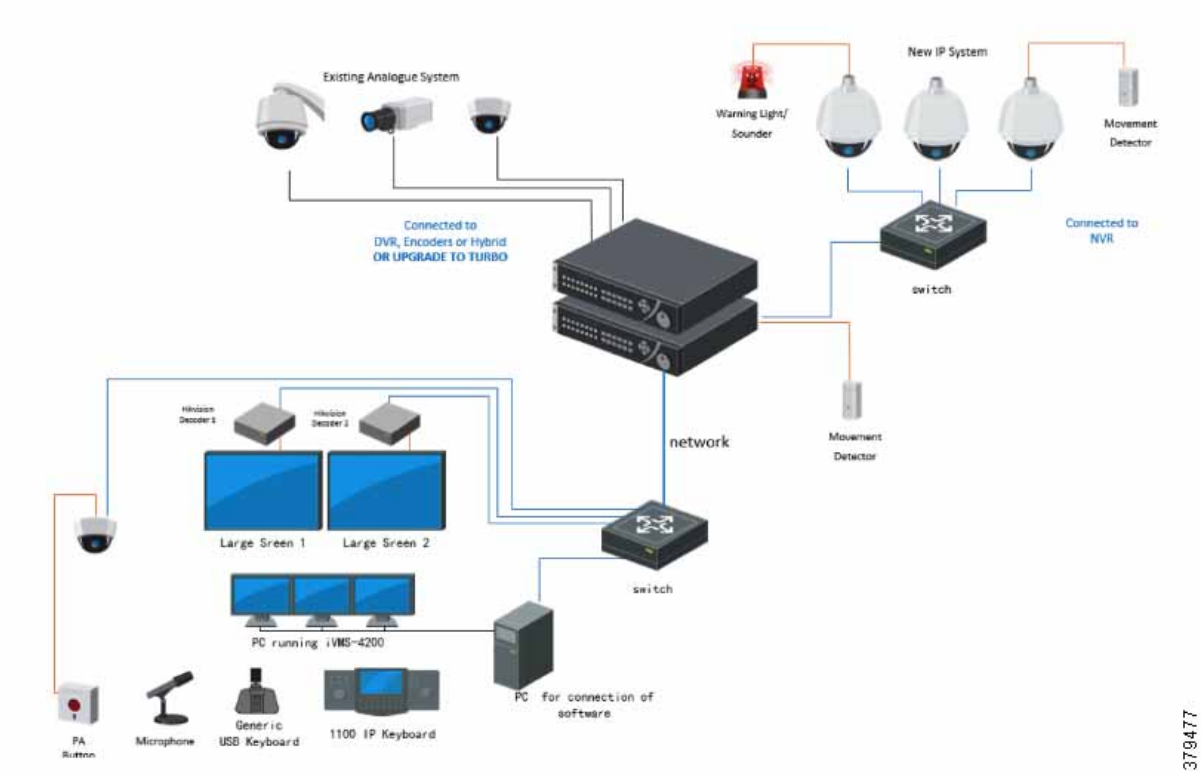
- Fixed cameras
- Domo Cameras
- Pan, Tilt, and Zoom (PTZ) cameras
- Bird-eye cameras
- Explosion Proof Cameras
- Thermal and thermographic cameras

Typical Topology

When CCTV systems that were fully based on IP were introduced, the topology and architecture of the CCTV systems changed. CCTV applications generally consume a lot of bandwidth compared to typical industrial applications. Because of this demand, it is very important to involve expert teams to do the sizing and the design of the networks, ensuring that they consider all cybersecurity and performance aspects associated with this technology being used within an industrial control setting.

IP-based CCTV systems allow video to be sent on demand, which is much more flexible than the traditional analog CCTV systems. For example, we can send the data to the control center only when an incident occurs instead of sending the stream continuously. Figure 62 shows a typical topology of an IP-based CCTV system:

Figure 62 Example IP-based CCTV Architecture



Security Risks

CCTV systems have three main security risks:

- **Vandalism**—Cameras are normally one of the first targets of vandals. Modern cameras implement algorithms to detect vandalism actions and to send alarms to the control center or directly to the security staff.
- **Environmental Conditions**—Choosing the right type of cameras as well as the correct accessories is critical for achieving good performance.
- **Cybersecurity**—As already explained in previous sections, while new IoT technologies and IP-based devices come with improved features and flexibility, they also present new cybersecurity challenges that need to be considered. This is vital today and will be even more important in the future.

Public Address and General Alarm

Public Address and General Alarm (commonly called PAGA or PA/GA) is aimed at providing voice and alarm audible/visible signals throughout different facilities. The PAGA industrial application is critical for personnel safety and during an emergency needs to be fully operational to facilitate the safe evacuation of the facility; therefore, a field-proven design should be used.

The PAGA distributes alarm tones, pre-recorded messages, emergency voice messages, and routine voice messages to all or selected areas of the facility via loudspeakers. In areas with a high ambient noise level, flashing lights (beacons) complement voice messages and audible alarms.

Alarms can be initiated either manually from any one of the dedicated access panels or automatically from the Fire and Gas Detection System or Emergency Shutdown System main panel via dedicated hardwired interfaces between the two systems. Voice messages can be generated either from the microphones at dedicated access panels or from telephones in the facility.

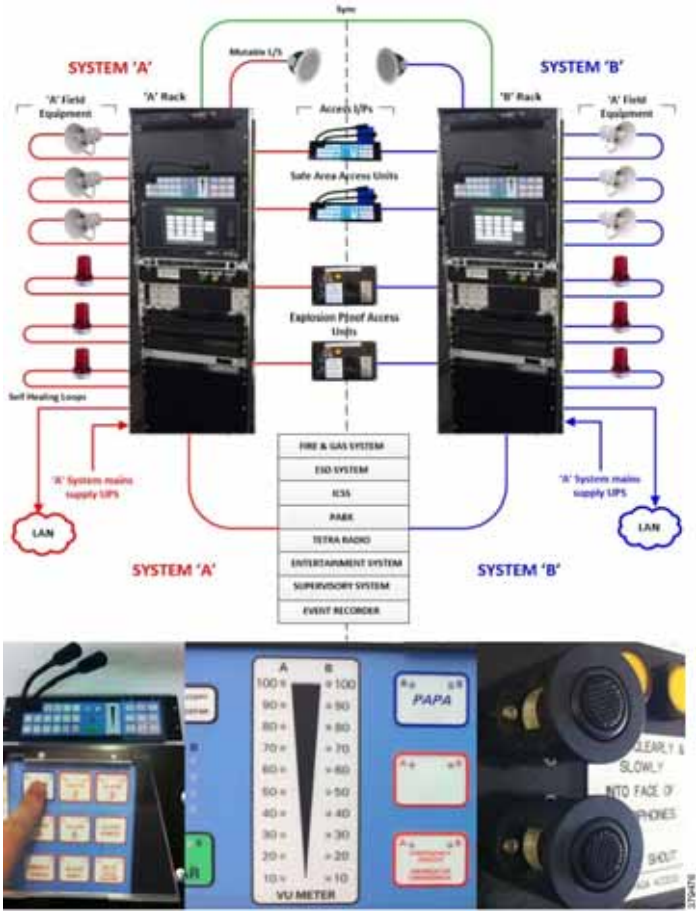
The main elements of a PAGA system are:

- Central servers, which centralize the management tasks as well as the interfacing with other systems
- Field devices, which are mainly amplifiers, loudspeakers, and flashing beacons

Typical Topology

A PAGA system can be designed in a number of architectures depending on site criticality. Normally these systems are hardwired to the field elements. Figure 63 shows an example architecture of a PAGA system:

Figure 63 PAGA System Architecture



Security Risks

No particular security risks are associated with this subsystem; however, with that said, we need to ensure the reliability of the system because it plays a key role in crisis situations.

Physical Intrusion Detection System

The main goal of a Physical Intrusion Detection System (PIDS) is to detect and locate attempts to dig, cut, move vehicles, or breakthrough along or climb over the perimeter fences surrounding the protected areas and facilities.

A PIDS consists of a set of sensors and/or cameras connected to a system capable of analyzing the data and generating alarms when a trigger occurs. It also allows for locating the source of the breach with reasonable accuracy when an intrusion has been detected. The location of the breach shall occur in predefined areas of the systems. Several technologies are available and shall be chosen giving consideration for:

- The nature of the land
- The performance of the technologies
- The security risks
- Any local constraints

Typical PIDS technologies include:

- Fence-mounted sensors:
- Fiber optic fence sensors
- Vibration sensors
- Taut wire fences
- Strain-sensitive and microphonic cables
- Electrostatic or capacitance sensors
- Buried sensors:
  - Buried fiber optic sensors
  - Coax buried sensors
  - Buried pressure tube sensors
  - Buried geophones
- Volumetric sensors:
  - Buried fiber optic sensors
  - Coax buried sensors
  - Buried pressure tube sensors
  - Buried geophones
- Video sensors based on video analytics

For highly sensitive facilities, several different intrusion detection technologies can be used to minimize false alarms and optimize the detection capabilities.

Typical Topology

Because of the large number of technologies available in the market today, it is very difficult to provide a typical topology for this subsystem. With that said, Figure 64 shows a typical field installation of a fence-mounted controller as an example of the technologies available.

Figure 64 Fence-Mounted Controller as part of a PIDS

Security Risks

Regardless of the cybersecurity aspects that have been mentioned several times before and that are common to all systems based on IP, PIDS have particular security risks associated with them. The risk that applies depends on the selected technology or combination of technologies. The most critical security risks are all those associated with physical attacks to the devices and components of the system. That is why buried and hidden technologies are normally considered to be more secure.

Cyber Security Aspects of Physical Security Subsystems

As has been highlighted throughout this section, many new cybersecurity threats are associated with the devices normally used to build these physical security subsystems. Once again, this fact reinforces the need to approach cybersecurity policies holistically. All aspects need to be considered along with the many device and system interactions as well.

Detailed studies, strategies, tools, and recommendations about how to implement the best practices for cybersecurity activities and policies can be found in the other chapters of this document.

Environmental Security

Environmental issues center on conflicts over access to natural resources compromising security interests. Considering that conflicts over natural resources are among the greatest challenges in 21st century geopolitics and present serious threats to human security, O&G corporations should align with other Critical Infrastructure stakeholders to promote collaboration between industries to better understand and address the consequences of environmental catastrophes.

Environmental Security is another aspect that needs to be clearly addressed as part of the security policies, ensuring natural resource protection and controlled access.

Industry Standards Cross-Reference: Physical and Environmental Security

Key Industry Standards and Guidelines
IEC 62443 62443-2-1, Sections 11.1 and 11.2
NIST SP 800-53 Physical and Environmental Protection Control Family
NIST SP 800-53 Tamper Resistance and Detection
NIST SP 800-53 Access Control Policy and Procedures
ISO27001 SectionA9, Access Control
ISO27001 Section A11, Physical and Environmental Security
ISO/IEC 27002:2013 Section 17
ISO 27019:2013 Section 14
API 1164 Section 4, Physical Security
NERC-CIP CIP-006 Physical Security Perimeter of Cyber Systems
NERC-CIP CIP-014 Physical Security

Active Defense

Active Defense Defined

Active Defense, which originates from the defense world, refers to techniques that deny positions or strategic resources to adversaries, making their battle efforts more difficult to carry out. In the cybersecurity world, the goal is the same: to make the success of security attackers as difficult as possible through proactive monitoring, outmaneuvering of attack activities, and denying access to key resources. Slowing down or derailing the attacker so they cannot advance or complete their attack increases the probability that the attacker will make a mistake and expose their presence or reveal their attack methods.

Organizations in the industrial space are beginning to move from a reactive perimeter-based security approach to one that proactively focuses on threat identification and incident response. The techniques in active defense are designed to primarily detect and slow down attackers, but may also include striking back at an attacker. Doing the latter has potential legal ramifications and an industrial pipeline environment would not typically do this.

The change of mindset from prevention-only methods to active deterrents is becoming widely accepted as an additional layer in a strength-in-depth security posture. However, deploying technologies is not enough. A combination of technology, people, and processes, following the consistent theme we have described throughout this document, is required. Figure 65 shows the typical building blocks for an active defense program.

Figure 65 Preparing an Active Defense Program (Source: Ernst & Young)

The process covers four main steps:

1. Identify critical assets.
2. Define the context and standard behavior.
3. Use intelligence to identify the most likely attack sources.
4. Test active defense techniques.

It is essential to leverage proactive strategies, which should use contextual intelligence to better prepare for future attacks, to detect and stop both external and internal threats. The described combination of technology, people, and process is essential for success.

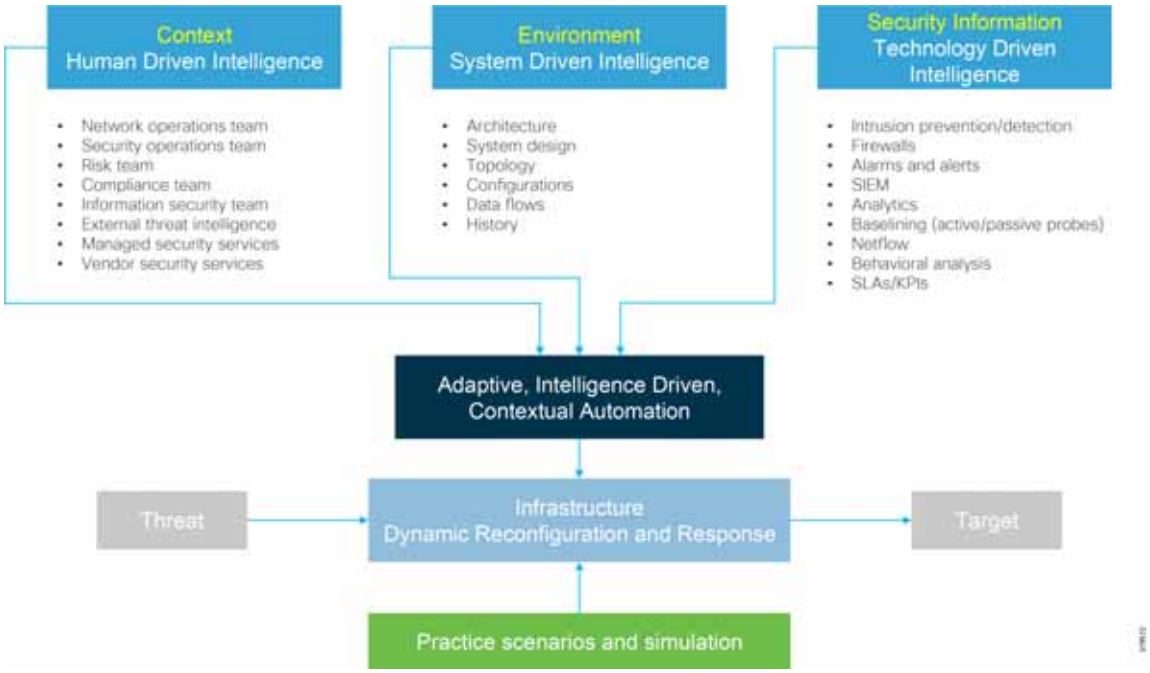
What We Are Trying to Solve

The ARC Advisory Group[1]suggests that the passive (or even active) monitoring technologies used in most cybersecurity programs today are only adequate for lower risk parts of an organization. In any area deemed medium-to-high risk, and especially for those deemed part of critical infrastructure such as pipelines, the recommendation is to supplement the traditional method with active monitoring and management by qualified people.

As critical infrastructure becomes increasingly appealing to cyber attackers, a contextually aware and intelligence-driven approach is needed to provide the best strategy to deal with threats.

The challenge is that many organizations do not have resources with the right skill sets, and in those rare instances when they do, they lack the necessary number of people to adopt an active defense approach. The result is that most pipeline operators today have and will continue to deploy passive and defensive technologies, making them more susceptible than those using active defense. This can be perceived as a major risk, since pipeline owner-operators cannot afford disruption to the operation of the pipeline because of monetary, environmental, and safety considerations. The most robust security program should combine human-driven intelligence with technologies that feed into automation systems to respond to threats rapidly, supplemented with practice and process to test the mitigation capabilities (Figure 66).

Figure 66 Active Defense Overview



Active defense programs should be considered an extension and enhancement of and not just a replacement for traditional security programs (from which they leverage technology and data). They should be the outcome of blending timely threat and risk intelligence with planned and deployed proactive technology and process measures created around specific threat scenarios. Active defense is used to solve the problem of traditional security approaches that often lack context and integration with other elements for producing an automated or standardized response to a threat.

By providing integrated and more accurate intelligence, it is easier to detect anomalies, identify threats, improve response times, and increase the capability of resources to respond and contain attacks.

1. https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

Visibility and Analysis

All four steps of the active defense model shown in Figure 66 above require visibility and analysis. The first two steps are critical to building up a baseline of assets to protect and identifying/defining their expected normal behavior. After all, you cannot protect what you cannot see and understand. As part of the first two phases (identifying critical assets and defining context and standard behavior), technology plays an essential role.

Visibility and analysis are fundamental enablers for providing the data that can be turned into intelligence. Visibility provides insight into the elements of the pipeline system, including sensors and instrumentation, devices such as PLCs and RTUs, network infrastructure including routers, switches, and firewalls, application infrastructure such as servers and storage, and the applications and services running across these elements. It also allows insight into the protocols used, and the data flows between endpoints. This builds up a baseline picture of all the actors and communications within a system, describing normal operation (providing the system has not been compromised during the baseline assessment). Once the baseline is established, tools can be used to continually monitor and assess the system before, during, and after security incidents, providing real-time anomaly detection and incident response forensics for post-attack analysis. Figure 67 shows a number of methods that can be used to identify threats, with various depths of visibility. Note that this is not an exhaustive list.

Figure 67 Visibility and Analysis

It is essential that these tools are used with the operational domain in mind. For example, a passive monitoring tool is likely the preferred option when baselining networks. This ensures that no impact is made on the industrial system or associated operational processes.

The following areas are used to provide visibility, analysis, and context for both known and unknown threats.

Intrusion Detection and Prevention

Intrusion detection and prevention solutions (IDS/IPS) are used to identify unusual patterns in network traffic that could signal a security threat. Industrial systems face different requirements and constraints compared to IT networks. Deployed IPS/IDS technology should be capable of supporting industrial protocols that include Modbus, DNP3, CIP, and IEC61850, in addition to traditional IT protocols. The support should also include both serial and IP-based protocols, with detection capabilities for not only infrastructure devices such as servers, but also to detect vulnerabilities (weakness in code) and exploits (malicious code) in endpoints such as PLCs and HMIs.

Technologies should provide policy enforcement and visibility for industrial protocols, including readability into parts of the protocol such as commands, and provision of protocol normalization. They should also address vulnerabilities that are known publicly and for which exploits may be publicly available. However, in all evaluations, it is critical that performance not be affected and that the reliable and safe operation of assets is always maintained.

When considering the deployment of IPS/IDS, a series of questions must be considered:

- Does a need exist for prevention or detection/reporting, or both?
- Do different segments require different protection?
- What software/applications are running?
- What devices are connected to the network?
- What security (policy, devices) is currently in place?
- What is the patch/update policy?
- What is most critical to the business?
- What is the potential for damage?

An IDS is designed to only detect vulnerability exploits against a target, and would typically be deployed out-of-band on a network supporting the pipeline, receiving traffic information via a Catalyst Switched Port Analyzer (SPAN) port or Terminal Access Point (TAP) so that it does not sit in the path of real-time communications between the sender and receiver of information. This way it does not introduce latency or affect the applications or processes of the pipeline system.

On the other hand, an IPS provides the same functionality as IDS, but is architected in-line between source and destination and is capable of actively dropping traffic packets in response to what it considers a detected attack. This affects the exchange of information in the control environment and therefore such a response is not currently a recommendation.

Both IPS and IDS systems are able to detect a range of security threats, such as DDoS attacks, virus activity, and worms. This is achieved through pattern matching where the IPS/IDS system will use DPI to look into the content of the traffic, and use signatures to detect certain malicious activities and respond with predefined actions. IPS/IDS systems also have protocol analysis capability, which allows them to inspect the protocol for threats. Some IDS/IPS solutions are constantly updated to ensure their signatures include the latest threats identified on a global basis. This ties back into the threat intelligence gathering from other sources mentioned earlier in this section.

The DPI examining traffic traversing a network can detect both attacks and anomalies, including both accidental and malicious ones. IPS/IDS devices interpret network traffic in much the same way as the endpoints that receive the traffic in question. Once a packet has been processed by a device, it is passed to optimized signature engines for further inspection. If the device determines that an attack is in progress, it can stop the attack or issue an alert containing information that can be used for investigation, or both.

When making a choice of technology, a number of areas should be considered:

- IPS/IDS device selection, including performance, connectivity, availability, and security
- Network insertion point, including location, connectivity, availability, and scaling
- Configuration/tuning, including compliance, security, and management
- Allowing/denying connectivity to the external world (via an IDMZ) for continuous threat updates
- Skill sets of security personnel to monitor and interpret events
- Protocol support for industrial environments
- Impact of actively responding to a suspected threat on the ability to monitor and control the assets

IPS/IDS solutions can be deployed in a number of ways depending on the use case to be addressed. For example, technology could be placed in the Level 3.5 IDMZ to monitor traffic passing between the Enterprise and PCD, and inside a security zone in a station process network to passively monitor traffic flowing between devices and looking for anomalies. Typical locations would include monitoring of connections terminating in the IDMZ, between Level 3 and 4 (Level 3.5), between Level 2 and 3 (Level 2.5), and inside zones.

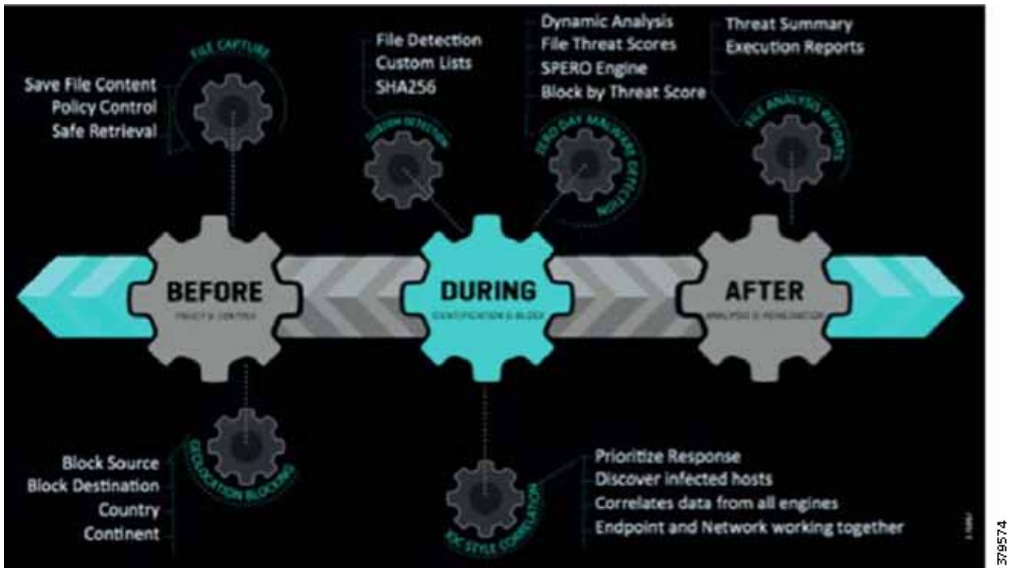
Some IPS/IDS solutions extend beyond the traditional signature recognition (Figure 68), with the ability to provide anomaly detection and leverage intelligence from both inside an organization and from external resources.

Figure 68 IPS/IDS Capabilities

IPS/IDS technologies running in monitoring or span mode, and flow-based technologies such as NetFlow, are very useful tools for building up baseline views inside or between architectural security zones and traffic patterns. The baselining and profiling of the network and data flows is conducted in a passive manner, which is good for operations; however, it is enacted on boundaries. From the baselining results, anomalies to normal operation can be detected and acted upon.

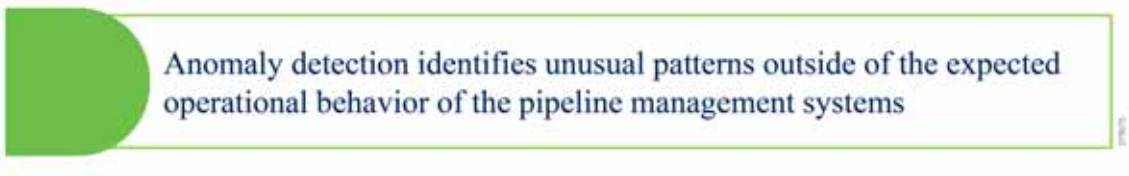
However, regardless of where the IPS/IDS is deployed, it is essential to understand that it forms part of the attack continuum and can enact multiple roles in the before, during, and after phases (Figure 69).

Figure 69 IPS/IDS as Part of the Attack Continuum



Analysis and Anomaly Detection

Anomaly detection, which identifies unusual patterns outside of expected behavior called *outliers*, would typically be used after a standard operational baseline has been established against which analysis can occur. In ICS networks, it can be used for intrusion detection, system health monitoring, and fault or error detection in operating environments.



Anomalies are usually defined in three ways:

- **Point**—A single piece of data that is different from the rest of the data.
- **Contextual**—A data instance that is anomalous in only specific contexts, and is often seen in time-series data. Also referred to as a conditional anomaly.
- **Collective**—A collection of related data instances identified as anomalous compared to the entire data set. The individual data instances may not be anomalies by themselves, but their occurrence together as a collection is seen as anomalous.

Data irregularities are normally identified by flagging the data points that deviate from common statistical distribution properties. These include mean, median, mode, and quantiles.

It is also possible to apply advanced techniques such as machine learning (ML) to the anomaly detection to provide automated learning and identification of anomalies. ML methods would include density-based, clustering-based, and support vector machine-based approaches.

In the pipeline environment, ML combined with industrial anomaly detection can provide both the baselining service and a self-learning system that can then detect anomalies against the baseline when the system is operating. Anomalies detected may indicate threats such as hacks or data theft/manipulation, but could also flag internal actions such as configuration changes or software updates, thus providing capabilities to detect internal and external threats.

Much of the analysis and information gathering is created by turning the pipeline communications infrastructure into a "sensor" that ingests and analyzes traffic metadata collected from infrastructure and workstations and creates a baseline of the normal system communication of an organization and its users. From this baseline, it is then much easier to identify infections or sophisticated attackers infiltrating the network. Anomaly detection can identify malware, DDoS attacks, advanced persistent threats (APTs), and insider threats. Anomaly detection can monitor both north-south and east-west (lateral) movements to detect the widest range of attacks, and it can quarantine attackers through integration with identity and access control systems so long as it does not affect safety. As an example, we can tie in Cisco Stealthwatch for behavioral analysis, and if we find deviation, we can communicate with Cisco ISE to quarantine an attacker by restricting access to any network devices based on identity. By providing a secure link to the internet via the IDMZ, it is also possible to gather external threat intelligence that can be used to continually match against known threats, or identify new outbreaks.

Although analysis and anomaly detection can provide a lot of benefit to a business, it is not an exact science. Oracle [X] identified a number of challenges that may occur when using this technique:

- The data contains noise, which might be similar to abnormal behavior because the boundary between normal and abnormal behavior is often not precise.
- The definition of abnormal or normal may frequently change, as malicious adversaries constantly adapt themselves. Therefore, the threshold based on a moving average may not always apply.
- The pattern is based on seasonality. This involves more sophisticated methods, such as decomposing the data into multiple trends in order to identify the change in seasonality.

Network Infrastructure Monitoring

Network security through hardware and/or software is any activity designed to protect the usability and integrity of the pipeline communications network infrastructure and data. It targets a variety of threats and stops them from entering or spreading on a network.

Typically expected threats to the network infrastructure include DoS, DDoS, unauthorized access, session hijacking, man in the middle (MITM) attacks, privilege escalation, intrusions, botnets, routing protocol attacks, spanning tree attacks, and Layer 2 attacks.

Designing a secure infrastructure to defend against complex threats and malicious attacks, which continue to change in behavior and characteristics, is essential today more than ever in critical infrastructure. High service availability, reliability, and quality are critical attributes that pipeline owner-operators must consider when deploying network infrastructure. As part of the active defense process, network infrastructure should follow a three-step approach and:

- Be based on a multi-layered defense system, i.e., defense-in-depth.
- Control network-based behavior through passive and proactive means. Careful assessment of proactive means must be considered to ensure no impact to operational activities.
- Support visibility into network behavior.

The multi-layered approach should consider access control, anti-virus and anti-malware software, application security, behavioral analytics, data loss prevention, email security, firewalls, intrusion prevention/detection systems, mobile device security, encryption and VPNs, web security, and wireless security.

Wrapped around all of these defense-in-depth tools must be the capability to manage and monitor them, with alarming, event management, and forwarding to SIEM tools that pull together the information security staff need to identify and respond to threats.

Integrating the security capability into the network infrastructure and providing tools to manage potential threats proactively in the context of the domain in which it occurs (e.g., mobile device and process control switching zone) provides a series of advantages as part of an active defense posture:

- Functionality without affecting overall network and system performance.
- Operation with existing high-availability services.
- The ability to identify, classify, and trace back anomalous behavior network wide.
- Increasing the overall security posture of the network.
- The ability to distribute countermeasures to multiple ingress points of the network. What and how these countermeasures are deployed needs consideration in the design phase to minimize or negate any operational impact.

By integrating security functionality within the network infrastructure, the same operational tools to manage data services can also be used to support security operations. Common tools such as AAA services, SNMP, Syslog, routing protocols, device counters, and packet analysis tools enforce and monitor security policies required to ensure reliable operation of the pipeline applications. As the network devices become more intelligent, operational processes can become more proactive in identifying and mitigating threats.

This proactive approach to network infrastructure design and monitoring ensures two crucial design goals in active defense:

- Control network behavior
- Maintain visibility into network behavior

These are not one-off approaches, but part of the continuous security lifecycle of the pipeline system network. IP-based networks have three planes of operation that need to be considered:

- **Data Plane**—The data plane receives, processes, and transmits network data between network elements, and represents the bulk of network traffic that passes to and through the network devices.
- **Control Plane**—The control plane is where all routing control information is exchanged, making the control plane and its components a target. Because control plane resiliency depends on CPU processing power and scalability, *out-of-resources* attacks against the CPU are not uncommon.
- **Management Plane**—The management plane is the logical path of all traffic related to the system management of the routing platform. In a distributed and modular environment such as a pipeline system, the management plane offers new levels of complexity, and increased requirements to maintain secure access.

Each plane of operation must be properly secured and monitored (i.e., control and visibility) to ensure the reliable operation of the network. Typical network threats are listed below. As part of an active defense approach, these can be built into the " test active defense techniques" step, with organizations conducting simulations, penetration testing, and so on. These can be done before network infrastructure or systems are deployed, against test environments for the pipeline system, or be specific portions of the live system subject to a comprehensive risk analysis to ensure no disruption to operations.

- **Reconnaissance**—Scan network topologies to identify vulnerable devices (e.g., open ports, no passwords, and OS vulnerabilities).
- **Distributed Denial of Service/Infrastructure**—IP packet-based attacks launched at the network infrastructure to compromise network performance and reliability.
- **Break-ins**—Usually follows reconnaissance and unauthorized access to a given device with intention to compromise device security.
- **Theft of Service/Fraud**—Unauthorized use of network resources.

These are typically identified and mitigated using the following techniques:

- **Network Control—Policy**:
  - Policy Enforcement - Access Control Lists, QoS policy actions
  - Isolation / Segmentation - QoS Resources
  - Instrumentation and Management - Control Plane Protection
- **Visibility—Classification**:
  - Protocol and Application Awareness - NetFlow, Access Control List, QoS classes
  - Identity and Trust - AAA services, management of Access Control Lists, Anti-Spoofing
  - Correlation - Network-wide Monitoring (SNMP, NetFlow records, Syslog)

Application and Application Infrastructure Monitoring

Connected to, and running across the communications network infrastructure, is the application infrastructure, the pipeline management system, and operational support applications. Like the network infrastructure, applications and their supporting infrastructure can also be baselined, monitored, and tested as part of an active defense approach.

Application Performance Management (APM), which is not new, is based on the premise that applications that provide value and which an organization must protect and maintain, should have their performance measured and managed. It is increasingly difficult to monitor, assess, and protect application performance because of increased environmental complexity as new operational applications are added to the pipeline network, additional operational support applications are introduced, and new use cases and technologies are deployed through digitalization.

Digital Transformation and IoT lead to increased connectedness and automation, with interconnected applications, services, and infrastructure for delivering better business outcomes. Orchestrating and monitoring applications across a distributed environment can enable competitive value; however, the complex application stack and supporting infrastructure can also pose performance and security challenges to an organization.

As part of an active defense strategy, gathering as much information about the performance of applications, systems, and processes, and putting it into the real-time context of critical business services, provides an additional level of visibility that can be monitored and controlled to mitigate potential security threats.

APM can act as a monitoring tool for the security environment, helping to identify and prioritize real-time threats. As security concerns grow and organizations struggle to improve their responsiveness, having early insights becomes critical to actively managing and defending systems in a number of ways:

- By integrating APM into a security strategy, the impact of an attack on an organization can be estimated. APM also provides a holistic view of all applications (operational or operational support), for both operations and security teams.
- APM can monitor the performance and security of applications in real-time, protecting against unwanted variations or breaks in performance. Alerts can be created to notify security teams when unusual behavior occurs from the edge environment through to the enterprise and cloud.
- Real-time monitoring capabilities integrated into security response processes enable a timely and direct response to threats. Potential or real threats can be identified in seconds or minutes (instead of hours or days using traditional methods), investigated and triaged as needed.
- In the event of an attack, APM will help identify and prioritize applications that have been affected, highlighting what needs to be fixed first. Many traditional tools and processes are unable to provide the business context (active defense requirement) needed around application issues.
- Some APM tools (e.g., Cisco AppDynamics) have security integration framework modules that reports on and feeds directly into security and regulatory compliance requirements. This includes end-to-end management of security threats to an organization, from detection to remediation, creating an unbroken audit trail for risk remediation and regulatory compliance.

APM tools can provide a set of capabilities to help with an organization's active defense strategy. These include:

- Application performance, such as Cisco AppDynamics, monitoring for end-to-end visibility into the performance of applications:
- Working with popular programming languages including Java, .NET, Node.js, PHP, Python, and C/C++, allowing security and operational teams to troubleshoot problems such as slow response times and application errors.
- Automatically discovering application topology and how components in the application environment work together to fulfill key business transactions for users.
- Measure end-to-end business transaction performance, along with the health of individual application and infrastructure nodes.

- Receive alerts based on custom or built-in KPI/SLA rules, including rules against dynamic performance baselines that alert on issues in the context of business transactions.
- Analyze applications at the code execution level using snapshots.
- Application modeling to fulfill requests from users of applications including:
  - Web applications served from an application server.
  - Databases or other data stores.
  - Remote services such as message queues and caches.
- Dynamic application agents that can automatically discover common application frameworks and services. Using built-in application detection and configuration settings, agents collect application data and metrics to build interaction flow maps. A flow map visually represents the components of your application to help you understand how data flows among the application components.
- Business transactions that represent the data processing flow for a request, typically a user request.
- Business applications that contain a set of related services and business transactions.
- Nodes that correspond to monitored servers or virtual machines in the application environment.
- End-user monitoring (EUM) provides end-to-end visibility on the performance of applications, enabling the ability to troubleshoot problems such as slow web, mobile network requests, or IoT application errors. EUM provides metrics on application performance and user activity, such as:
  - The impact of application performance on server performance
  - The impact of third-party APIs on application performance
  - The origin of the heaviest resource consuming loads
  - How users connect to and navigate applications

While application performance monitoring measures user interaction starting at an application server entry point, EUM extends visibility all the way to the web browser, mobile, or IoT application.

- Database monitoring and visibility provide insight into the performance of a database, providing the ability to troubleshoot slow response times and excessive load. The visibility provides metrics on database activity, such as:
  - Which SQL statements or stored procedures are consuming the most system resources
  - Statistics on procedures, SQL statements, and SQL query plans
  - Time spent fetching, sorting, or waiting on a lock
  - Activity from the previous periods such as day, week, or month
- Infrastructure monitoring (from the application perspective) provides visibility of the performance of the hardware running applications. It helps to identify and troubleshoot problems that can affect application performance such as server failures, virtual machine crashes, and network packet loss. Infrastructure monitoring provides metrics such as:
  - CPU busy/idle times, disk and partition reads/writes, and network interface utilization
  - Packet loss, round-trip times, connection setup/teardown errors, TCP window size issues, and retransmission timeouts
  - Disk/CPU/memory utilization, process, and machine availability

Threat Intelligence

The above sections describe multiple ways to baseline operational systems and gather data and information on what is happening in the ICS. However, information becomes intelligence through context. This requires either the correct people or automation tools (or both) who are able to recognize and react to threats. Many organizations do not have adequately trained staff or available tools, meaning additional investments are required in technology, people, and active defense processes.

ARC[1] advises that anomaly and network infrastructure tools are a good starting point, but active defense requires additional capabilities including:

- Detection based on intelligence-driven context, instead of context-less anomalies that put the investigation on the analyst.
- Detections that account for multiple devices and types of data, instead of just network traffic.
- Historical records of the kinds of events and network messages that defenders need in order to understand the context of suspicious behavior.
- Tools and workflows that support efficient investigation and management of suspicious behavior. This includes the ability to perform data queries for patterns that attackers might use to disrupt system operation (e.g., the steps in the ICS Cyber Kill Chain model).
- The ability for defenders to implement specific ad-hoc detection and evaluation queries that incorporate information from threat intelligence sources monitoring emerging threats and changes in attacker tradecraft.

Training operational staff, developing shared security services in the wider organization, and working with external security service providers and external security threat intelligence services such as Talos may address these additional capabilities. The contextual expertise needed must span cybersecurity, ICS, and industrial processes, and provide the correct tools to gather the right information that can be contextualized.

The Process

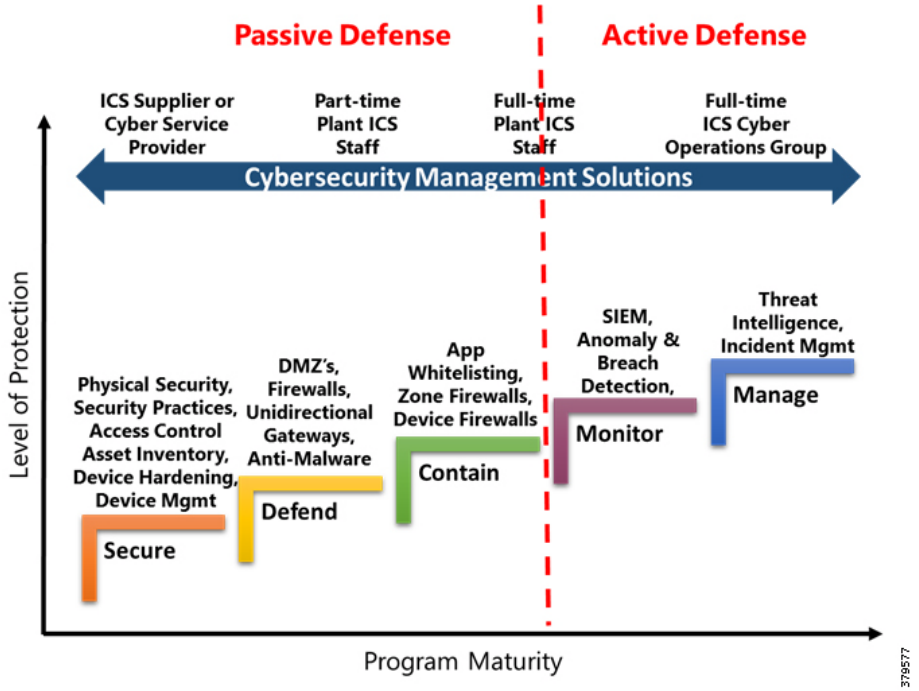
Ernst and Young[2] describes three main steps in the active defense process. Security teams must:

1. Ensure that they clearly understand which assets are most susceptible to attack and likely to be attacked by potential attackers, and which assets are most critical to the business. Discussion between security teams and business leads will produce a list of key assets to be defended, which are typically associated with critical business functions. These will include applications, infrastructure, and corresponding data repositories.
2. Understand what constitutes normal system operation. Typically, this is referred to as a baseline in the context of security. Active defense requires strong analysis capabilities by both systems and people to understand any deviations from the baseline that may constitute a threat.
3. Be able to contextualize information and understand the threat actors that are likely to target their organization.

1. https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model
2. https://www.ey.com/Publication/vwLUAssets/EY-active-defense-cybersecurity/$FILE/EY-active-defense-cybersecurity.pdf

Figure 70 describes the journey from passive to active defense and covers the different phases, processes, and technology described in this section.

Figure 70 Active Defense Security Posture (Source: ARC Advisory Services)



McKinsey [X] believes that most organizations lack the budget to build fully self-sufficient security teams to deliver an active defense program. However, by engaging outside resources, participating in information-sharing partnerships, and using intelligence tools, businesses can still mount a strong active defense. Their advice is to:

- Anticipate attacks before they happen using an intelligence-heavy, data-driven process. Where skill sets are missing or resources stretched, engage external cybersecurity experts and third parties that specialize in threat intelligence.
- Detect and respond to attacks in real time. Early detection depends on an organization's ability to track network patterns and user behavior that deviate from the norm. Use both IDS/IPS technologies that look for threats based on known patterns, and anomaly detection technologies that detect unknown threats based on changes to normal baseline operation. The combination provides more comprehensive threat detection.
- Look beyond the network and communications infrastructure, incorporating application and threat intelligence.
- Establish traps and alarms to contain attacks.
- Use defense-in-depth architectures to protect critical assets. Penetration in any one layer will set off alarms.

Active defense also requires risk planning that organizes and prioritizes security-related technology spending. It can be tempting to try to protect everything, resulting in creating vulnerabilities when spending and systems cannot be maintained.

From a practical process perspective, organizations can follow two approaches: Observe, Orient, Decide, Act (OODA) and Plan, Do, Check, Act (PDCA).

OODA is used to provide continuous improvement in the analysis of traditional intelligence:

- Observe each stage of the attack lifecycle as highlighted earlier in this document. Collect and process all captured data and information from any technology or process in the system.

- Orient on the attacker's methods and technologies used, analyzing the data and information available.
- Decide if this is a new attack, a new attacker, or a known threat, and produce an outcome via a threat intelligence report. Threat intelligence using contextual information can provide actionable information on the tools and processes and how to respond accordingly.
- Act on the information in the report and feed it back into the Active Defense security posture.

As part of the final tier of active defense, it is essential to build learnings from the OODA approach into actionable and recordable measures as part of a security posture. This can be realized via a PDCA approach:

- Plan actions based on the gathered threat intelligence for each stage of the attack. Actions can be technical and process based, and may even be human based through training or allocation of budget/additional resources.
- (Do) Implement the planned actions.
- Check the quality of the implemented actions, including the reliability of the intelligence, and the effectiveness of any mitigation techniques over time. Use the outcomes of these check measures to improve active defense across technology, people, and processes.
- Act by providing feedback on the quality of threat intelligence and effectiveness of countermeasures to continuously improve the security response lifecycle.

Summary

By organizing and integrating the existing security operations in a business with new capabilities, an Active Defense approach can enhance security monitoring and incident response, reduce the number of successful attacks, decrease the amount of time that attackers operate before being discovered and removed from a system, and crucially minimize the impact to critical business applications and services.

Industry Standards Cross-Reference: Active Defense

Key Industry Standards and Guidelines
IEC 62443-3-3 Part 9 Restricted Data Flow
IEC 62443-3-3 Part 10 Timely Response to Events
NIST SP 800-30
NIST SP 800-50
NIST 800-137 Continuous Security Monitoring Information Security Continuous Monitoring
NIST 800-94 Guide to Intrusion Detection and Intrusion Prevention Systems
NIST SP 800-53 - Incident Response Control Family
NIST SP 800-53 - Awareness and Training Control Family
NIST Framework for Improving Critical Infrastructure Cybersecurity
ISO27001 Section A16, Information Security Incident Management
ISO 27031 Sections 7.3 and 9.2
ISO27001 Section A7, Human Resource Security
NERC-CIP CIP-007 System Security Management
TSA Pipeline Security Guidelines, Section 7.3 Security Measures for Pipeline Cyber Assets

Secondary Security Functions

In addition to the core security capabilities that run across the standards, guidelines, and best practices, a number of additional functions should be considered as part of a well-rounded security approach:

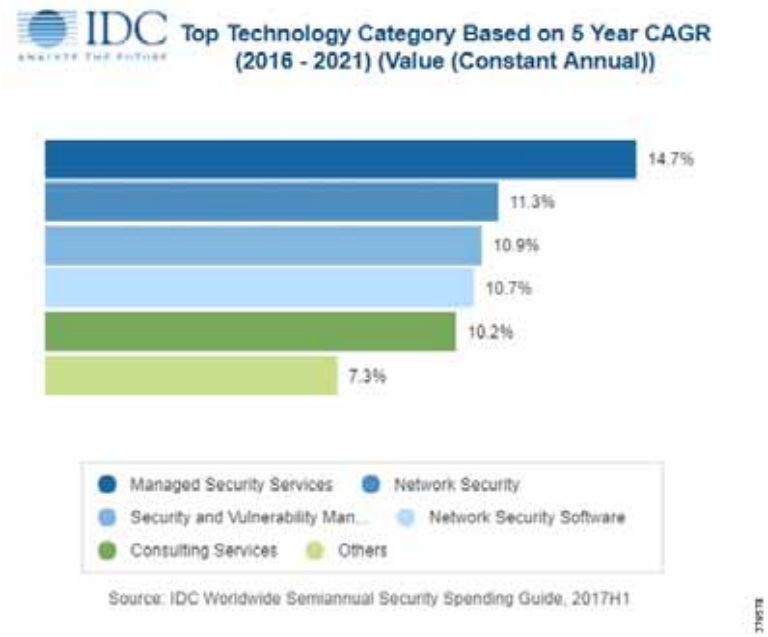
- Managed security services
- Organization of information security
- Compliance
- Security vulnerability and penetration testing
- Shared operations and handoff points
- Human resource and personnel security

We outline these over the next few sections, which provides a general (versus a deeper dive) introduction for pipeline companies to consider.

Managed Security Services

In line with the increasing threat surface and expanding attacks aimed at energy companies, to say nothing of the gap in qualified cyber security professionals in the industry, outsourcing of security services has grown. IDC Research[1] believes Managed Security Services (MSS) will be the fastest growing security area in terms of spending (Figure 71) in the years up to 2021. Process manufacturing is included in the top six industries for security spends including MSS.

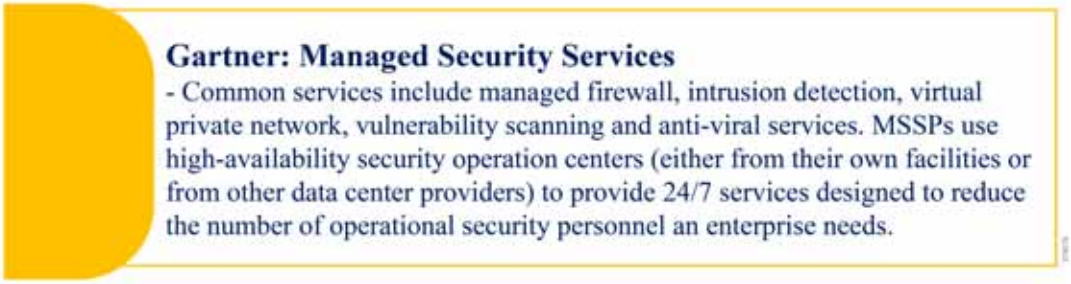
Figure 71 Top Security Technology Categories (Source IDC)



The skills challenge is not just about the shortage of trained people, but also includes the amount of security skills a workforce would require. This means that it is difficult to hire or train and then retain these personnel to meet an acceptable security posture.

1. https://www.idc.com/getdoc.jsp?containerId=US41320917

Gartner[1] defines a company providing these outsourced services as a MSSP, with services including round the clock monitoring and management of security devices and systems, patch management, security assessment and audits, and cyber incident response. In the case of pipeline environments, this would also include infrastructure supporting the pipeline management applications and services in the operational environment.



The reason managed security services are attractive is that MSSPs specialize, providing more capabilities and advanced security services to assist organizations in defending against security threats. However, they are not a replacement for an organization's security posture, but should complement in-house capabilities consisting of the security strategy, security blueprint, security reference architecture, and cybersecurity practice. Before engaging an MSSP, the core competencies, cost-effectiveness versus in-house solutions, the need for 24/7/365 service, and customization of the service, needs to be considered.

IDC argues that as organizations become more digitally enabled, they will fundamentally change their technology, architectures, and data value chain, along with their fundamental approach to risk. All of this creates new security challenges that an organization may find difficult to address and therefore will require outside support.

Although this may seem a costly solution, it will be lower than training and employing an equivalent set of employees. It also allows staff to focus on the key security issues that cannot be outsourced due to things such as company IP and data sensitivity. Other advantages include vulnerability and penetration testing, routine security scans, and focused security operation centers (SOC) to support the business. As cyber threats and attacks evolve at pace, being able to respond at speed is a challenge, and Gartner[2] argues that leveraging an MSSP and their SOC is a better and ultimately more cost-effective way to approach security.

IDC believes that the following areas will drive the MSS market forward while providing vendors the opportunity to provide differentiated propositions:

- Complementary services that provide customizable opportunities for assistance in security transformation and maturity; these can include enabling security within a customer's journey to the cloud.
- Cloud monitoring, visibility, and management capabilities that seamlessly enable hybrid implementations.
- Flexible consumption models that match customers' preferences for integrating MSSP expertise, processes, and technology.
- Pricing models that support the end customer's buying preference.
- Mobility and IoT solutions.
- Advanced detection methods and analytics techniques, including advanced detection and response capabilities, threat intelligence, and big data.
- Robust customer support, including incident response (IR) and forensics, to assist with recovery from breaches.
- Customer portal and reporting capabilities.

1. https://www.gartner.com/newsroom/id/3815169
2. https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

- Security orchestration and automation technologies to provide more efficient incident response workflow.
- Security operations centers.

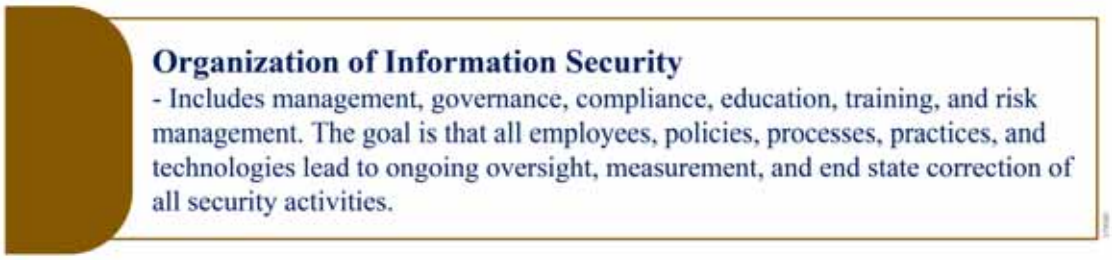
As solutions become increasingly complex, the more they attempt to address this long list of capabilities, PWC[1] believes the MSS capability and cross-border footprint is best-positioned to address these evolving needs. This will also help provide consistency of approach to security across different parts of the organization.

In the operational space, it is essential to evaluate the MSSP, not only for their capability offering (e.g., use cases, staffing, capabilities, location, SLAs, portal capabilities, payment options, complementary services, and technologies), but also for their experience in providing security as a managed service, and security for the operational domain. Often MSS partnership approaches provide the best of both worlds, so long as the offering and roles and responsibilities are clearly understood and documented.

A critical consideration for pipeline operators is that outsourcing security capabilities to an MSSP does not hand responsibility over to the MSSP. The pipeline company is still responsible for its own security, and should be prepared to closely monitor and manage the MSSP in the relationship, while ensuring the MSSP is accountable for the services for which it is contracted to provide.

Organization of Information Security

Regardless of an organization's size, a formal documented plan to ensure the security of information assets should be in place. This organization of information security is known as the security program. This is essential as organizations think holistically about their security throughout a lifecycle approach. It will include fundamental areas that allow a company to meet their security level or appetite for risk, through a framework that includes the potential risks faced, how risks will be mitigated, and procedures and practices for how the security program will stay up to date.



This will combine the technical protections with business processes, resulting in an overall security approach. It is essential to not only focus on technology, but also include people, processes, data/information, and environments in which the business takes place. It should also be a continuous process, not a one-off exercise. This must cover both external (including third parties) and internal needs in alignment of the company's tolerance for risk.

1. https://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf

Table 4 provides a broad overview of the different activities associated with the organization of information security.

Table 4 Organization of Information Security Example Activities (Source: Carnegie Mellon University)

Department	Sub-function	Example Activity
Program management office	Information security program / plan	■ Develop, implement, and maintain an information security program and plan ■ Allocate adequately trained/skilled resources to implement the information security program and plan ■ Measure and monitor cost, schedule, and performance
Governance, risk, and compliance	Information security program / plan	Define, implement, and enforce information security policies
	Risk management	Establish an information security risk management strategy, process, and program
	Governance and compliance	■ Govern/oversee the information security program and plan (includes CCB and other oversight boards/groups) ■ Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements ■ Conduct audits
Personnel and external relationships	External relationship management	■ Manage relationships with third parties (vendors, suppliers, contractors, partners, and critical infrastructure owners/operators) ■ Manage relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, and the press)
	Personnel management	■ Manage the employment lifecycle and performance of personnel in accordance with security requirements (background checks, vetting, transfers, risk designations, success planning, disciplinary action, and termination) ■ Manage knowledge, skills, capabilities, and availability of the information security team ■ Implement an enterprise-wide role-based information security awareness and training program

How Information Security fits into the broader organization is important to consider. Fundamentally, it is not an isolated function, but rather a part of an overall approach to risk management in the organization, overlapping with a number of areas, as shown in Figure 72:

Figure 72 Information Security Alignment in an Organization (Source: Advisera)

Who owns this function in an organization will vary depending on the company philosophy. As pipeline companies move further into their digital journey, and as IT and OT take on different or new responsibilities, different ownership approaches may emerge. The introduction of IoT and digital technologies allows companies to realize benefits, but as systems continue to merge and process data as a more readily available commodity, the overall threat landscape is increasing as OT technologies and applications mix with Business Enterprise applications. We have seen the creation of Chief Information Security Officer (CISO) and Chief Digitalization Officer (CDO) roles where ownership often lies.

Compliance

Security is a priority topic for pipeline companies and is a critical subject in the public eye. As such, pipeline security programs are evolving and updating to cover increased technological, operational, and regulatory risks. Not only is the industry tightly regulated, but regulations are evolving and changing on an ongoing basis, with new regulations regularly being introduced.

An example is the Network and Information Security Directive (NISD) in Europe[1], where energy companies, including Oil and Gas, must ensure network and information systems meet minimum standards of cyber security. The directive introduces " appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems," in addition to compulsory reporting of incidents that occur.

Pipeline companies must ensure that they have technologies, processes, and people in place to effectively monitor and respond to legal, regulatory, and operational risks. This is to ensure that they not only minimize their own liability, but also minimize the risk of damage to the environment, property, human injury, or loss of life. We are seeing a move in the industry where investments are being made early and before incidents occur to improve security posture, coupled with structures to adequately investigate incidents and show evidence of such actions when reporting.

In addition to external regulations that organizations must meet or exceed, pipeline companies will have their own set of internal compliance procedures that must also be met. Being compliant is a challenge for the industry due to tight internal and external targets. Compliance requires an auditing process (internal or external) to provide an independent view that you are indeed doing what you say you are doing. In addition, compliance carries financial implications that need to be

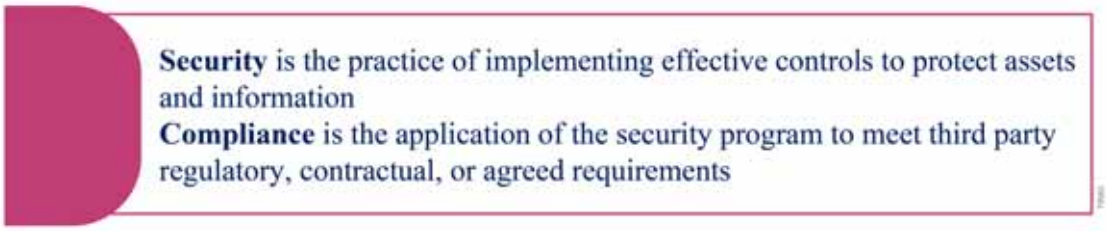
1. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

measured against internal appetite to risk, and the cost of fines and reparations when targets are not met. Insurance policies are now available to protect companies against the damages related to cyber incidents and should be considered as a financial hedge against potential losses.

In light of this, companies need to consider whether current security programs that include technologies, management systems, risk management systems, and supply chains, are capable of detecting, preventing, and managing the lifecycle of security risk.

Compliance and security are intertwined, yet they are still two distinct areas:

- **Security** is the practice of implementing effective controls to protect assets and information. It is a program delivered not to satisfy third party needs, but for its own sake. It delivers against the need to protect from continual threats to an organization and it is a continuous lifecycle, being maintained and improved on an ongoing basis.
- **Compliance** is the application of the security program to meet third party (external or internal) regulatory, contractual, or agreed requirements. Compliance is complete (at least for a moment in time), when the third party is satisfied. In the context of security, compliance is a demonstration or reporting function, of how a security program meets the specific regulatory, contractual, or agreed requirements.



Both use formal practices within the day-to-day operations of a business, but compliance on its own does not equate to meeting security needs. A mistake we have seen is organizations using compliance requirements as a blueprint for the entirety of their security program. The challenge is that this is a prescriptive approach, targeting a static goal, and security as a discipline is continually evolving. An effective security program should be foundational, that is baked-in, and based on the needs of the organization versus a third party. Compliance should be an outcome of a security program.

The most effective security programs go beyond the box checking exercises and leverage robust best practices to safeguard assets and information, including defense and detection in depth, user awareness and training programs, and external third-party testing to ensure the security controls are working. Compliance programs do not necessarily require these critical functions, meaning a compliance-centric security program may not address key security needs.

Compliance should not be viewed as a negative task, focusing on doing only what is necessary. Even without regulatory needs, it still has a useful purpose and certain certification programs (such as ISO 27001) can actively enhance an organization's reputation. It may also play a role in identifying gaps in a security program. A former president of the Canadian Energy Pipeline Association (CEPA) argues that it is essential for pipeline companies to go beyond compliance[1] to improve their performance, and gain public trust. Using innovative technology and management systems to continuously improve the way pipelines are designed, built, operated, and secured, this improved public perspective can be achieved.

One of the best ways to meet compliance requirements is to leverage technology to digitize and automate the process. This will include baselining assets and data to paint a picture of how the pipeline system operates (as discussed in detail in Asset Discovery and Inventory, page 49), monitoring for variations against a baseline, taking automated actions, and automating processes to get this data into centralized compliance systems so that it can be reported on. This provides both compliance data and a security audit trail if incidents occur.

Security and compliance are inter-related and provide complementary aspects to one another. With a focus in both areas, ensuring there are ties between both, pipeline companies can not only meet the regulatory, contractual, or agreed requirements for compliance, but they can also demonstrate a commitment to exceeding compliance and enhancing the security program.

1. https://www.aboutpipelines.com/en/blog/pipeline-safety-why-compliance-isnt-enough/

Security Vulnerability and Penetration Testing

As part of an organization's strength in depth and compliance efforts, a security assessment should be conducted. This may include both vulnerability assessments and penetration (also known as *pen*) testing to help with the overall security posture.

A vulnerability assessment focuses on identifying vulnerabilities in a system. It provides an estimate on how susceptible a network is to a range of vulnerabilities. An assessment can be a manual process, or via automated scanning tools to find, document, and report on discovered vulnerabilities. Information, which is collected from the system, is compared with documented issues to understand if the system has known vulnerabilities or weaknesses as well as to identify potential challenges.

Penetration testing takes the approach one step further in that it not only identifies vulnerabilities, but it will also attempt to exploit them. Penetration testing is conducted regularly in the IT domain, leveraging similar techniques to those that attackers might use to exploit the environment. Penetration testing in OT is much less common, but works in the same way, but with a focus on the operational environment.

The aim of these processes is to proactively identify and address issues and vulnerabilities, and prevent them from being exploited by security attacks. This will include recommendations on the best ways (technology, people, and process) to address the gaps.

These techniques fit with the US TSA Pipeline Security Guidelines, advocating pipeline operators to:

- Identify all assets in the system, such as operator stations, servers, and network equipment. Record information, including the type of operating system, IP address and subnet mask, and the vendor software each asset uses.
- Identify all the risks within the environment; i.e., perform a risk assessment. This involves pinpointing possible threats and associated security vulnerabilities.
- Create an action plan that prioritizes all the vulnerabilities identified during the risk assessment. The action plan must outline the necessary remediation steps to minimize or eliminate the risk. Time lines should be included.

Although penetration testing is common in IT, it is not as widespread in the OT domain, and there is often a question as to whether a penetration test should be included for the operational side of the pipeline systems. A number of reasons exist for why it may not happen, including:

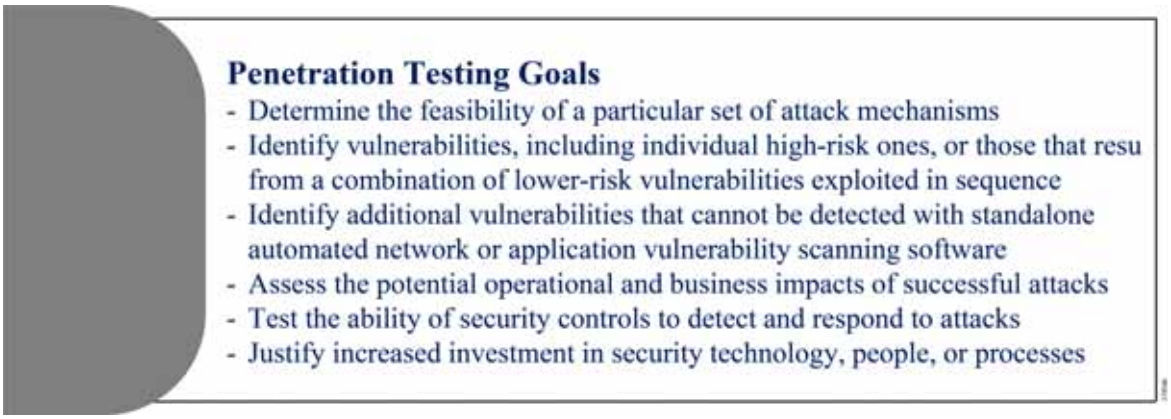
- Pipeline management systems need to stay as available as possible, operational 24/7/365: there is not the same opportunity to take systems offline as there is for IT.
- Unintended consequences relating to the test can damage systems or assets, resulting in:
  - Financial implications from downtime resulting in significant losses
  - Environmental or safety issues that prevent the safe operation of the pipeline

Any of the above or in combination have caused pipeline companies to be hesitant about conducting tests that could potentially affect operational systems. An alternative approach to penetration testing the actual pipeline environment is to establish a sandbox that avoids the disruptions from performing such tests in the production environment. The sandbox is representative of the pipeline, potentially leveraging a copy of the training systems, and uses this created environment as the basis for more extensive testing.

As has been outlined in multiple sections of this document, pipeline management systems are evolving and have more IT-centric technologies and IoT technologies, including the need for data sharing and remote access via the IDMZ to the Enterprise and outside world. This means potentially new threats to the operational system, and a need to address these threats in a different way. This increased risk demands a more in-depth approach to OT (similar to IT), including regular reviews of the infrastructure, data and information flows, remote access, and management and monitoring tools that are associated with the OT environment. This is where penetration testing, if properly and professionally conducted, can help.

A penetration test usually consists of four distinct phases:

- **Discovery**—The initial phase where the system applications and infrastructure are baselined with the aim of learning as much as possible about assets, networks, applications, data, and information flows, etc. A topology of information and assets is created as a result, as well as other IT-related information such as IP addresses, protocols spoken, manufacturers of devices, and bandwidth utilization. The aim is to create a picture of how the system looks during normal operation.
- **Vulnerability Identification**—Working from the normal operational baseline, the tester will begin to probe different areas and aspects of the system, looking for potential vulnerabilities (known and unknown). This is usually carried out via an automated scan. The scan can be active or passive, where the making of an informed choice is essential in operational environments where there is potential to disrupt operating assets and cause downtime or operational issues. Based on the information returned from the scan, a list of potential vulnerabilities is created.
- **Exploitation**—Sometimes referred to as *hacking* or *ethical hacking*, the tester will use attack tools and techniques to exploit agreed upon vulnerabilities. This will allow the tester access to vulnerable devices that the attacker will try to leverage to escalate their access privileges or breadth of attack. Other techniques may include extracting confidential data or information whilst leaving the system intact and operational so it appears that no attack took place. The aim is to determine how far a system can be exploited and understand the potential damage or outcomes. It is essential that only professionals who understand all aspects and potential impact of the test process handle the penetration testing.
- **Reporting**—The final stage is producing the agreed deliverable for the security, risk, and management teams. This should include:
  - A list of all vulnerabilities that were exploitable
  - A list of potential or theoretical vulnerabilities
  - A set of actions the organization can take to mitigate the identified risks.



The penetration testing process can assess many different areas. The British Standards Institute highlights the following areas:

- Infrastructure testing
- Application testing
- SCADA and ICS testing
- Build review
- Mobile applications and devices
- Network device reviews

- Wireless penetration testing
- Secure code review
- Virtualization testing
- Stolen laptop review
- Golden build image review
- Database review
- Environment breakout

With proper planning, it is proven and possible to carry out meaningful testing in the operational environment and provide the same benefits that are seen in IT or in the enterprise today. To do so, one must have:

- Clear objectives and desired outcomes
- Detailed project plans and test scenarios
- Correct skill sets using a mixture of IT, OT, and security professionals
- Appetite for risk
- Level of knowledge on available information: What level of information (restricted, confidential, intellectual property) can be provided to aid testing

Pipeline companies, like all industrial operators, are subject to cyber threats, and this often comes in the form of attackers probing for known vulnerabilities or weakness in security depth. A challenge that sometimes occurs is that organizations do not act on the results of the penetration test to bolster security posture. This may come down to lack of finance, appetite for risk, or lack of knowledge. Penetration testing will only provide the vulnerability information, but it is up to the business to implement the appropriate mitigation techniques and provide themselves with the best level of protection.

Shared Operations, Handoff Points, and Supply Chain

Not all pipelines are owned or operated by the same company. For example:

- The pipeline may be co-owned as part of a joint venture
- The pipeline may be operated by a different organization to the owner
- The pipeline may run through multiple geographies with different owners or operators for each geography
- Pipelines can intersect one another
- Pipelines connect to other operational environments such as refineries, processing facilities, and terminals.

For each of these scenarios, the parties involved have a number of differing factors that could potentially contribute towards a security threat. It is important for the pipeline companies in these scenarios to understand the various security postures compared to their own, and the risks this might impose.

Some regulations exist for these scenarios, such as the UK Gas Act 1986, where gas transporters are required to develop and maintain an efficient and economical pipeline system, with security an extension of this requirement. A similar obligation is imposed on interconnector operators, under the terms of the interconnector operator license. However, these regulations are not widespread, nor consistent, and where a pipeline runs through two countries, as an example, the same levels of security may not be applicable at interconnection or handoff points.

As the pipeline IT and OT systems are increasingly integrated with those of other companies within the supply chain, the attack surface is increased. Pipeline operators should consider issuing contracts that explicitly contain security terms where responsibility and liability for security is outlined, in addition to the types of security mitigation techniques, processes or trained people that should be leveraged. Pipeline companies should increasingly recognize that just allocating liability in a contract for security incidents is not adequate. Companies should negotiate the right cyber security behaviors of any other parties at handoff points or in the supply chain in order to avoid incidents in the first place.

Human Resource and Personnel Security

Cyber security is not just a technology problem. People and processes play an essential part, with the success of the program ultimately dependent upon the human factor. The role people play in cyber security is probably the most important in mitigating and managing threats and risks, but at the same time, people are potentially the greatest threat (deliberately or inadvertently) to security.

An area of concern highlighted in this document were the different IT and OT security skill sets. The OT environment has a lot of capability, but with the newer technologies and architectures bringing more IT-centric technologies into the operational domain, the OT skill set needs to be expanded. In some instances, security has also primarily been seen as a function of IT, and services and support have been borrowed into the OT environment. The tool sets and technologies used in these two domains may also be different.

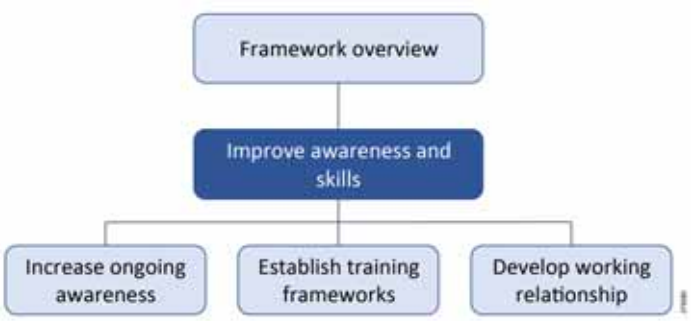
These differing areas all point towards the role of people in the security practice. Addressing threats comes down to an understanding of the risks as they relate to production, operations, and safety, in combination with security awareness and how employees (internal and external) behave.

Many security programs focus on technology, but they don't necessarily build in the human element. People may take deliberate action, or make mistakes, but in the operational environment, the resulting outcomes from these potential security threats can affect both human safety and the environment. Some of the human factor challenges we have seen that may affect security include:

- Lack of ICS security knowledge, security policies, and security training
- Vulnerability to social engineering attacks
- Deliberate actions from disgruntled employees (current or former)
- Human error or negligence

The Center for Protection of National Infrastructure (CPNI) in the UK provides a set of guidelines for improving internal staff awareness and skills on security in industrial environments. They identify three key areas to improve the security of ICS (Figure 73) through increasing awareness, improving skills through training, and by developing closer relationships between OT and IT security personnel.

Figure 73 Good Practice Principles to Improve Awareness And Skills (Source: CPNI)



- Programs to increase awareness should highlight the vulnerabilities, threats, and risk to ICS, as well as the potential impacts of security failures on the business. Awareness programs should also provide insights into the technical and procedural solutions that can be deployed to prevent cyber security attacks from succeeding.
- Personnel, including from third parties, should be trained to give them the appropriate level of knowledge to understand the risks and adequately protect the ICS environment. The training should cover technical areas (IT and ICS), policies, processes, and procedures. An increasing number of training courses exist that are designed for these specific areas and organizations should select courses that suit their own training strategy.
- Awareness and training can also help develop a close working relationship between ICS and IT departments, and provide a common language and processes that can be used to develop an effective ICS security program.

Centre for the Protection of National Infrastructure (CPNI) also has a strong recommendation that organizational leadership must recognize that the topic is relevant to a wide audience within an organization. In other words, the security program will only be as strong as is executive commitment to it.

The potential impact to an organization from insider threats may include financial and reputational losses, as well as environmental impact and human safety. Internal threats range from fraud and theft of intellectual property or sensitive data, to the sabotage of key sites, systems, or equipment.

In addition to internal employees, the pipeline environment will have a range of external contractors working in the operational domain, and in certain situations, having access to key operational assets and data/information. While the use of contractors is essential to business operations, it can increase the security attack surface through human means. Contractors may not have the same sense of loyalty as regular employees, or have been as thoroughly screened, as internal employees. They may also be outside the security management and monitoring processes, meaning ways to identify potential issues may be missed.

Best practice guidelines[1] for an effective personnel security regime include:

- Personnel security measures have been applied in a way that is proportionate to the risks, and reduce those risks to an acceptable level.
- The personal information provided by the contractor is genuine.
- Only personnel who are unlikely to present a security concern are allowed to work on the contract.
- The opportunity for the contractor to abuse their access to the organizations assets has been limited as far as possible.

1. https://oilandgasuk.co.uk/wp-content/uploads/2015/05/EM009.pdf

- Measures are in place to detect if a contractor becomes a security concern and processes are in place to manage this accordingly.

This clearly shows that pipeline organizations should be as vigilant with their own employees as they are with external threats, but who is responsible for this inside an organization? As so many problems arise resulting from a company's own employees, the human resources (HR) team, working closely with security, operational, and IT professionals, can play a fundamental role.

HR having a formal role in a cyber security program means they have the ability to:

- Help IT, OT, and security professionals develop and distribute security policies, associated procedures, and guidelines.
- Train employees, and the HR staff themselves, on security issues and company posture.
- As part of the on-boarding process, ensure new employees have not brought sensitive data or information, or physical hardware such as laptops and thumb drives, from their previous employer, and are properly trained in OT/IT security practices.
- Close any internal and external access to accounts of former employees immediately.
- Be responsible for stressing and enforcing the disciplinary policies for employees that do not comply with security guidelines, up to and including termination.

The aim for pipeline companies should be to treat internal and external people as an extension of the security threat landscape. This will allow them to be part of the risk process, with the appropriate mitigation techniques implemented to best protect the organization. Employees want to do the right thing. When educated in proper security practices, they will work to ensure security is part of the culture and not an afterthought. Additionally, it is important that security practices be rational in how they are implemented, adding value, versus adding complexity and frustration that leads to the need or desire to circumvent them, once more opening the operational world up to avoidable risk.

Industry Standards Cross-Reference: Secondary Security Functions

Key Industry Standards and Guidelines
IEC 62443-2-4 (requirements for system integrators)
IEC 62443-2-1
IEC 62443-2-2
NIST 800-53 PS1 Personnel Security Policy
NIST 800-53 PS7 3rd Party Personnel Security
ISO/IEC 27001 Personnel Security
ISO 27799 Section 6 Personnel Security
ISO/IEC 27002 Human Resource Security
API 1164 Part 3.1 Personnel
API 1164 Part 5.10 Personnel Administration
NERC-CIP CIP-004 Personnel & Training
CFATS 622. Chemical Facility Anti-Terrorism Standards Program b) Security measures, (d) Compliance, (2) Personnel surety
CFATS 623. Protection and sharing of information
OpenFog Consortium Reference Architecture
Open Process Automation
Cloud Security Alliance
Industrial Internet Consortium Reference Architecture
Internet of Things Reference Architecture (IoT RA)
Industrial Internet Consortium Security Framework
oneM2M - Standards for M2M and the Internet of Things

New Architectures

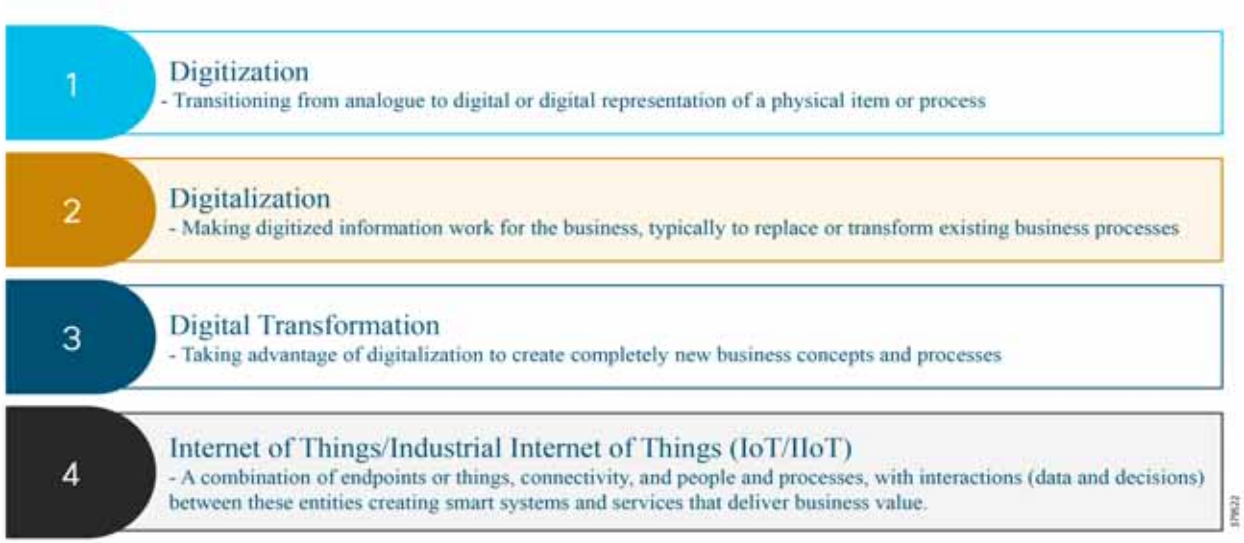
A 2015 Deloitte whitepaper[1] argues that digital transformation through IIoT is the best approach for helping petroleum organizations meet their key focus areas:

- **Improving reliability and managing risk**—Minimizing the risks to health, safety, and the environment by reducing disruptions.
- **Optimizing operations**—Increasing productivity and optimizing the supply chain through the cost and capital efficiency of business operations.
- **Creating new value**—Exploring new sources of revenue and competitive advantage that drive business transformation.

The above use cases have an impact on traditional architectural and security requirements as pipeline owner operators drive innovations to ensure uptime of the pipeline assets through advanced condition-based monitoring and predictive maintenance, leak detection, and worker mobility and productivity.

Use of the terms *digitization*, *digitalization*, and *digital transformation* in organizations, however, is confusing. In addition, *IIoT* is often interchanged with these terms. For clarity, see Figure 74:

Figure 74 Digital Capability Overview



In practice, the responsibility for digital capabilities and transformation should reside with line of business (LOB) owners, with IT responsible for enablement through technology.

New IIoT and digital capabilities can be used to provide better operational and business insight, and to make faster and better decisions. This approach is not a new concept to the petroleum industry: owner operators have had the ability to measure and collect increasing amounts of data for some time. The difference is that the majority of data generated has been unused, whether through choice or ease of technology use. A 2016 world economic forum found that 90+% of data generated remained unused. New advances in digital technology, primarily driven by IIoT, is making the use of data easier to collect, consume, and use for the benefit of businesses.

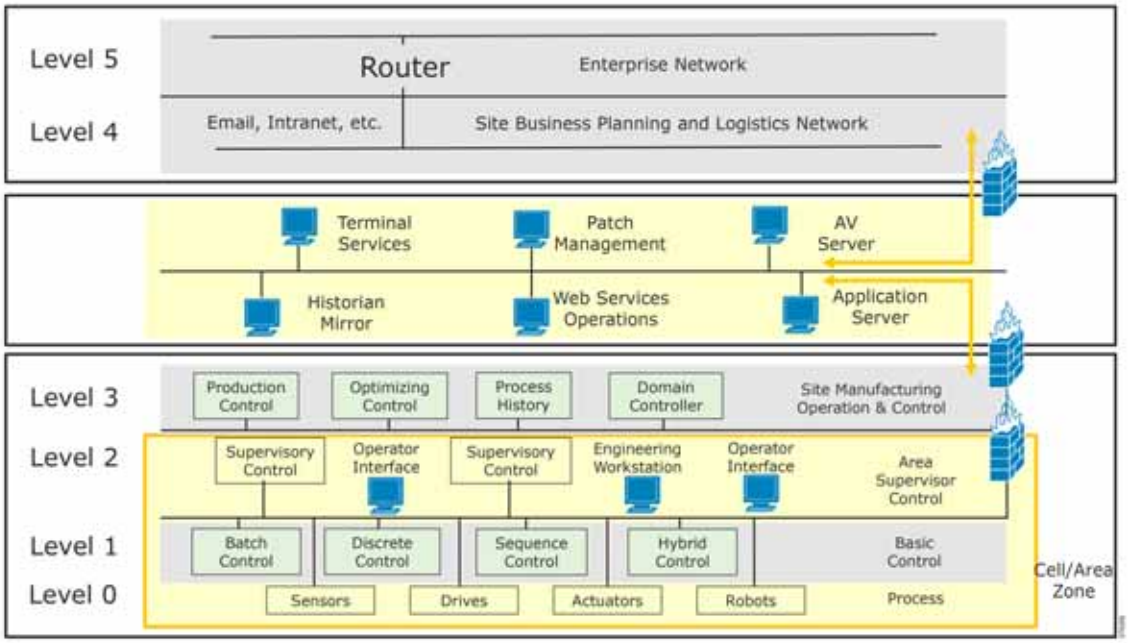
However, it is not as simple as just adding new IIoT technologies in order for digital transformation to take place. As discussed in Cisco, Schneider Electric, and AVEVA Joint Reference Architectures, page 10, both current and end-state architectures of the use case environment need to be carefully considered since the introduction of any new technology or service will expand the security attack surface and risk to the pipeline system. As outlined in the first section of this

1. https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

document, a new approach to architecture and associated security must be considered such that businesses can gain the most advantage from the introduction of new technologies into the pipeline environment. In the rest of this chapter, we will introduce some of the key architectural trends and the associated standards, including IIoT, cloud, edge/fog compute, and open process automation. We will also discuss how deployed projects have typically leveraged the adoption of these newer technologies.

Before exploring the emerging architectures for pipelines and the oil and gas environment in general, it is necessary to revisit how most pipeline control systems are architected today. The prevalent standard that most architectures follow in critical pipeline environments is based on some flavor of IEC 62443 or the Purdue model of control reference model in Figure 75:

Figure 75 Segmented Architecture Based on the Purdue Model of Control



The approach describes various " levels" of applications and controls in an industrial system. It describes components from the physical levels of the plant (Level 0) through localized control equipment (Level 1) and local supervisory control (Level 2), with safety critical applications defined in a separate layer.

Level 3 comprises the system level operations and management control for the pipeline and provides a system level view of applications that " control" operations. Level 3 is often referred to as 'operations management' because of the various applications inside this level. This is also the domain of the pipeline system IT professionals. Level 3 and below comprise the OT domain.

Levels 4 and 5 are referred to as the enterprise or business level, including connections to the outside world, and are the domain of corporate IT.

The Purdue model also describes a hierarchical data flow model, where sensors and other field devices are connected to the control system. The control system serves the dual purpose of controlling processes or machines, as well as serving processed data to the operations management level of applications. Level 3 applications, in turn, feed information to the enterprise business system level.

The model has seen informal integration of an additional level, which arises from the historical divide between OT and IT domains. The Level 3.5 IDMZ provides a strict segmentation zone and boundaries between OT and IT domains. However, services and data need to be exchanged between the IT and OT domains. Systems located in the IDMZ, such as a shadow historian, bring all the data together for company personnel in a near real-time system, exposing near real-time and historical information to the enterprise for better business decision making.

No direct communications are allowed between the enterprise and operational domains. The IDMZ provides a point of access and control for the provision and exchange of data between these two environments. The IDMZ provides termination points for the enterprise and the operational pipeline domain and hosts various servers, applications, and security policies to broker and police communications between the two domains.

Even with the Level 3.5 IDMZ, this architectural approach imposes potential challenges for a modern digital pipeline environment leveraging IIoT. The data of today, and the data of the future, is not necessarily hierarchical in nature. Data has many sources, and many clients that will leverage the data, and we are already seeing systems that can automatically leverage data and initiate processes without human intervention. In addition, federated data structures with localized storage situated in multiple places of a pipeline system, not just in central locations, often exist. Although this approach has been the de facto way to architect pipeline industrial networks, it divides IT and OT services with physical or heavily virtualized segmentation implemented to achieve separation. As pipeline owner operators look to integrate new technologies to enable their digital transformation strategy, this separation is blurring, and use cases may often need a combination of IT and OT services to provide maximum business benefit, yet the security of the data and of the OT environment must continue to be ensured.

With IIoT-generated data providing the basis for most new digital projects for the pipeline, real opportunity exists to improve end-to-end operational integrity for remote operations and management in real time. Pipeline operator goals include fast resolution of issues with pipeline assets, ensuring worker safety and meeting industry, environmental, along with their own internal compliance and regulatory goals. To achieve this, pipeline operators need technologies that can interoperate between edge, operational domains, the enterprise, and often in the cloud. They also need to understand that a process and culture change will also be required inside the organization.

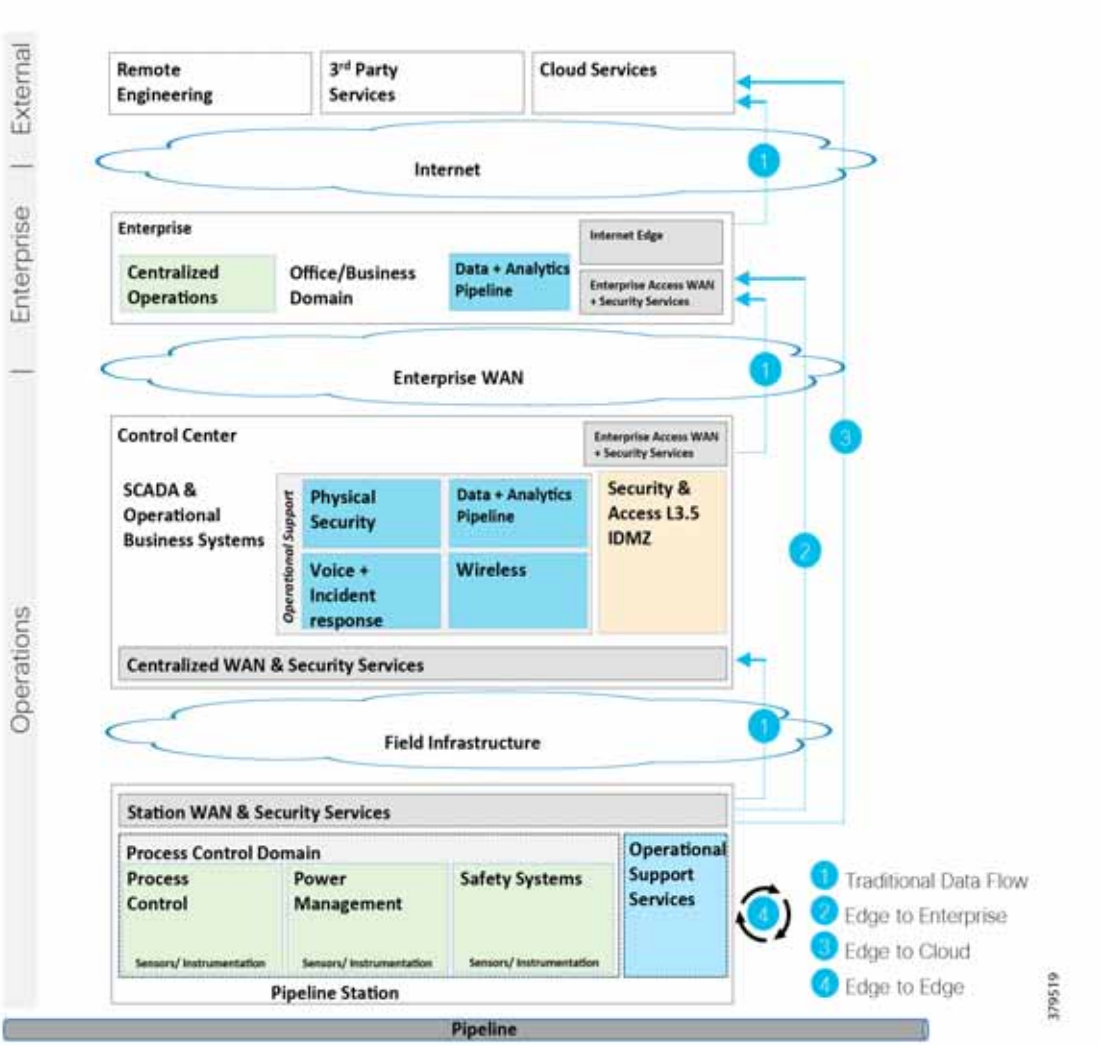
As mentioned frequently in this reference document, IT and OT often have differing perspectives and mindsets, resulting in the separated and siloed architectures we see today. Importantly though, the pipeline industry is starting to see these areas coming together, particularly when driven by IIoT and digital, but IIoT and digital bring their own challenges.

Organizationally, we have seen a shift to increasing convergence between historically separate IT and OT teams and tools. This has led to leveraging more IT-centric technologies for operational activities. Where operationally derived information is used to typically make physical decisions to complete a process such as detecting a leak, IT information is typically leveraged to make business decisions such as optimization of a process. However, regardless of the type of technology deployed or the type of data or information produced, the pipeline operator must treat any security challenges in a similar manner. Strategies should be more aligned and teams should work more closely in order to ensure a consistent approach to end-to-end security is achieved. This will include traditional standards-based and emerging architectures, and the management, administration and policy, and infrastructure needed to implement new use cases and supporting technology.

IT/OT convergence is occurring although we don't understand very well the extent of this convergence or to which parts of the business it will yet be applied. To deliver digital operational use cases for the pipeline, such as real time analytics for asset health monitoring, a full IIoT stack (such as infrastructure, OS, applications, data pipeline, and security) is needed. This means pipeline solutions will see integrated IT-centric services deployed alongside OT services, to directly enable business value. As such, IT capabilities, which are now becoming operationalized, push the boundaries of traditional security architectures like the Purdue Model of Control and IEC 62443.

As a result, we are seeing more converged standards based on the easier sharing of data with data flows following edge-to-enterprise or edge-to-cloud rather than the traditional path (Figure 76). These newer approaches focus on open architectures for peer-to-peer, scalable systems that supports edge analytics, and local monitoring, decision-making, and control, in addition to the centralized models of today.

Figure 76 Changing Data Flows in Industrial Environments



It is essential to point out that these digital use cases are currently typically used for monitoring applications and not control applications. Often these monitoring applications are deployed on separate networks outside of operations; however, we have seen projects where operators are already experimenting with using this data to provide real-time control and actuation at the edge, or automated feedback loops into operational pipeline systems. As these digital technologies increasingly provide benefit to the business, they are also increasingly likely to be operationalized and considered critical elements of the pipeline business. At the same time, oil and gas companies are also announcing digital strategies that include non-traditional architectures such as cloud as a foundational element.

An example of this[1] is Chevron, where they are using new cloud-based solutions in data-intensive areas such as exploration, midstream, retail operations, and the management of oil wells. Chevron's goal is to be able to access real-time operational data, handle the volume and scale, and apply analytics to provide predictive maintenance and create smarter workflows.

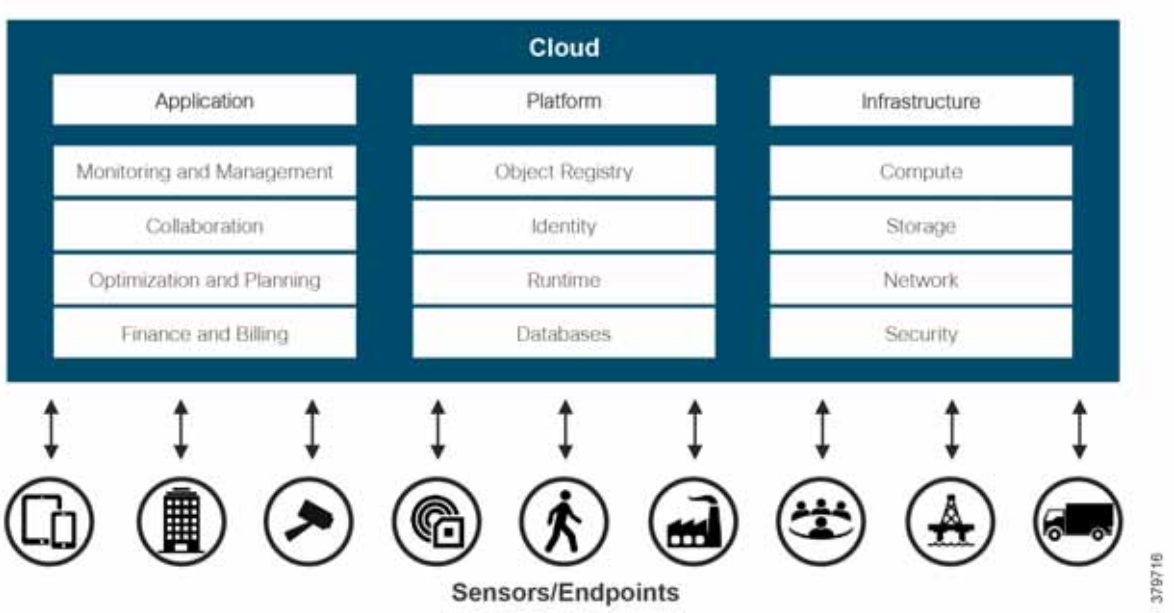
1. https://news.microsoft.com/transform/chevron-fuels-digital-transformation-with-new-microsoft-partnership/

The following content describes some of the key technologies that we are seeing introduced to help pipeline operations with IIoT or digital projects. It is included to provide awareness (versus an in-depth explanation and application).

Cloud Computing

Centralized cloud computing as a concept has been around for decades, referring to applications and services hosted and delivered remotely from the internet rather than via local servers or personal computers. Cloud computing provides shared computer resources (Figure 75), such as processing, storage, data, and analytics, to users and devices on demand. The basic premise is to enable on-demand access to a shared pool of resources that can be quickly and automatically scaled up or down, allowing individual users or organizations to process and store information in a cloud data center that may be located anywhere.

Figure 77 Cloud Computing High Level Architecture



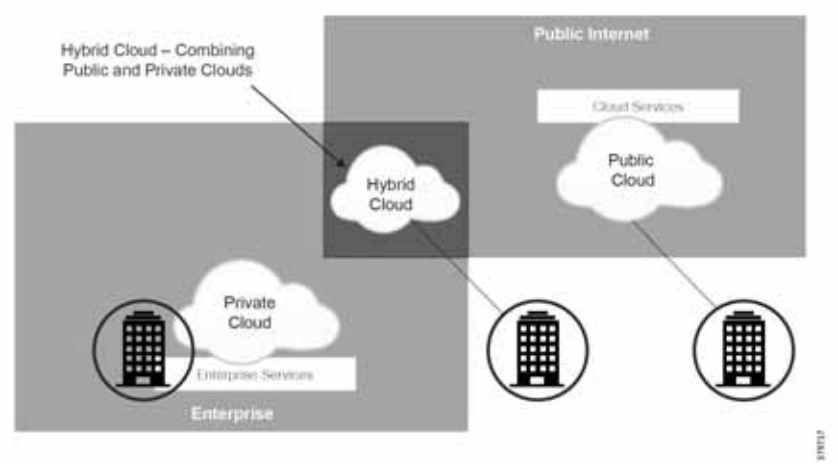
Three main types of deployment model exist:

- **Private cloud** where infrastructure is deployed, operated by, and maintained for a single organization
- **Public cloud** where infrastructure is available on a commercial basis by a cloud service provider
- **Hybrid cloud** where infrastructure combines two or more clouds (private, public, or community) that remain distinct entities, but are connected together, offering the benefits of multiple deployment models

In addition, the three main service deployment models defined by NIST (Figure 78) are:

- **Software as a Service (SaaS)**, which allows the consumption of a provider's applications running in a cloud infrastructure
- **Platform as a Service (PaaS)**, which allows the deployment of applications into the cloud infrastructure using tools supported by the provider
- **Infrastructure as a Service (IaaS)**, which allows the provisioning of infrastructure computing resources to deploy and run applications

Figure 78 Cloud Computing Deployment Models



A number of potential benefits for pipeline companies associated with cloud computing exist, including reduced cost, scalability and extensibility, reliability and availability, accessibility, reduced support and maintenance and potential environmental benefits through lower power consumption, and less equipment used.

Pipeline companies should consider the challenges associated with cloud computing, although some of these may be resolved with careful consideration at the planning stage. Challenges include lack of cloud interoperability standards, the continuous evolution of cloud which may not fit static industrial environments, compliance of where data is processed and stored, dependence on an external cloud service provider, and of course security and privacy of data.

Owner operator examples of cloud-based technologies for pipelines include:

- Abu Dhabi National Oil Company (ADNOC), who are leveraging it to increase the speed and efficiency of new application development as they move into new markets, including natural gas pipelines.
- Pacific Gas and Electric (PG&E), who currently leverage analytics on sensor-based data to help identify compressor, valve, and pipeline issues and to use predictive and proactive maintenance techniques to address these potential issues before they become problems.

The pipeline ecosystem vendor also uses cloud-based architectures and technologies to transfer a wealth of data for pipeline inspection machinery to its own applications that are hosted in the cloud in order to generate information and value from the captured data.

Cloud and IIoT are closely aligned for many use cases and industries, driven as the amount of data produced by IIoT devices has rapidly expanded, and needs to be processed, stored, and accessed. Cloud computing technologies were designed to address these needs, and, for many use cases, cloud is the main solution today for big data and high-computational analytics requirements. IoT and cloud are likely to see a growth for pipeline companies introducing new monitoring services, along with projects that will trial real-time control for non-critical applications.

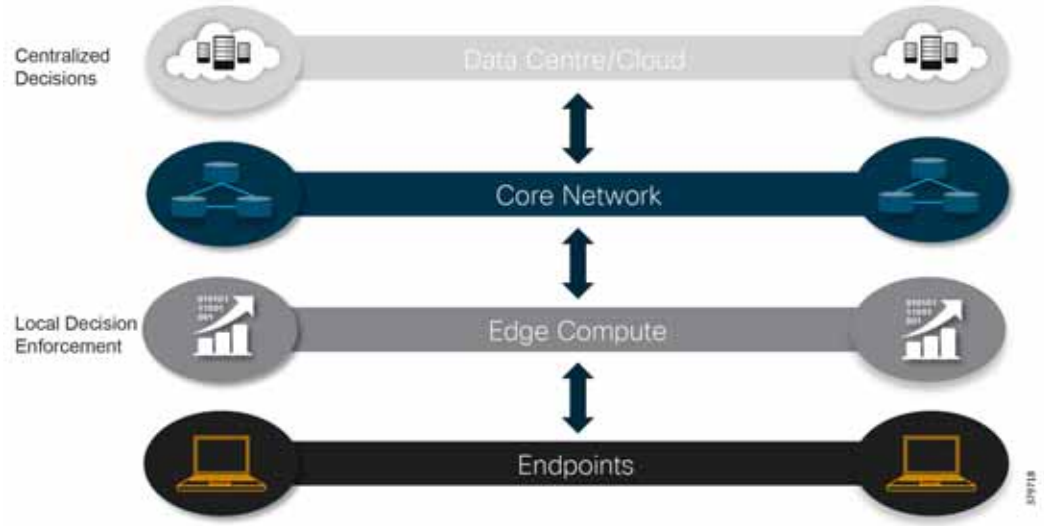
The goal of digital projects leveraging IIoT is to turn data into business insight, and the cloud can deliver against this depending on the use case. This use case consideration is ultimately the decision point for cloud suitability. For real-time and critical, privacy-sensitive use cases, the lack of reliability due to minimal (if any) end-to-end QoS, service assurance, security, and the typical OTT deployment scenarios will mean cloud does not fit all IIoT architectural requirements or deployments.

Fog/Edge Computing

Fog and Edge compute are more recent developments for addressing a number of the challenges highlighted for cloud services. Fog computing can address those problems by providing resources and services to end devices and users at any level of an IoT architecture, although it is more commonly (and incorrectly) positioned for the edge of network only.

Fog and edge compute are often used interchangeably, which often makes sense; however, a difference exists. Edge computing is an old concept that has been modernized as part of the fit with IIoT. Edge computing pushes most of the data processing to the edge of the network, as close to the data source as possible. In the edge compute model, data is still centrally stored, and, as a result, all data is moved to centralized systems for permanent storage and future processing. Edge compute therefore means we replicate centralized processing and data storage close to the source, but the architecture is master/slave in nature (Figure 79), with the edge processing being merely an extension of a centralized system.

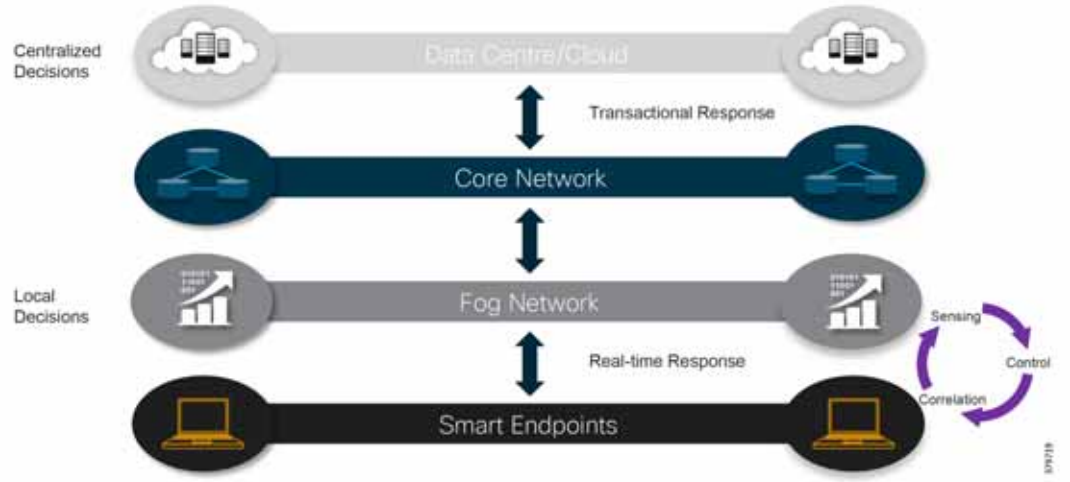
Figure 79 Edge Compute Architecture



While edge compute refers to performing processing at the edge of a system, fog computing performs processing anywhere from the centralized application to the edge of the system. Many IIoT applications are latency-sensitive, mobile, and geographically coordinated, and this presents a challenge for cloud or purely edge-based solutions. Some use cases require mobility support and geo-distribution in addition to location awareness and low latency, and this is where fog fits. Where cloud compute provides centralized compute, storage, and application resources over public and private networks, fog moves these resources to the most appropriate locations anywhere from edge to cloud.

Fog computing, therefore, extends the cloud computing paradigm closer to the things that produce and act on IIoT data (Figure 80). The devices that perform this function are called fog nodes, which can be deployed anywhere with a network connection and can be any device with computing, storage, and network connectivity such as industrial controllers, switches, routers, embedded servers, and video surveillance cameras. Fog provides distributed compute, storage and network services, and, as a result, enables a new breed of applications and services. Fog extends cloud services.

Figure 80 Fog Computing Architecture



According to Gartner[1], by 2022 75% of generated data in an enterprise petroleum company will be created and processed outside of the traditional data center or cloud and driven by new digital projects. This compares to 10% today.

Fog is not an adapted version of cloud computing, but it is a complementary technology, and interaction will occur between the cloud and the fog, particularly when it comes to data management and analytics. While fog technologies provide localized compute and correlation, enabling low latency and contextual awareness, cloud provides centralization, coordination, federation and orchestration. A number of digital projects in the petrochemical industry, such as predictive analytics and remote monitoring and management, require both fog localization and cloud centralization, through their use of analytics, optimization services, and Big Data.

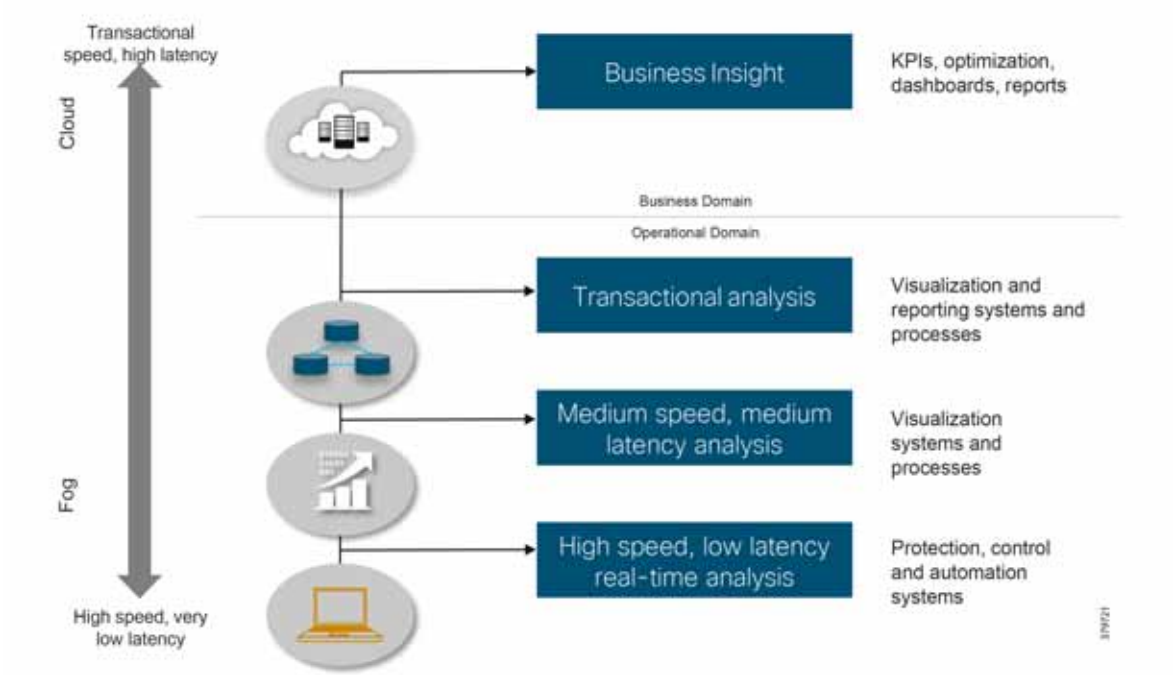
> *"Organizations that have embarked on a digital business journey have realized that a more decentralized approach is required to address digital business infrastructure requirements. As the volume and velocity of data increases, so too does the inefficiency of streaming all this information to a cloud or data center for processing."* - Santosh Rao, Principal Research Analyst, Gartner

Fog computing is often considered when projects need to minimize latency, face bandwidth restrictions, have security concerns associated with moving and centrally storing data, need operational reliability, must collect and secure data across a wide geographic area, and where there is a wide-spread geographic distribution of a large number of nodes that have scalability and manageability requirements. Fog computing provides an advantage over cloud-only technologies for certain use cases. Centralized analytics are typically used for post-event analysis to tell you what went wrong, whereas the near real-time analysis enabled by fog as the data is produced means measures can be taken before a problem actually occurs.

1. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/

Figure 81 shows how data is transacted in a fog architecture. The fog nodes closest to the edge ingest data from sensors and devices, and the fog application has the capability for consuming data, normalizing data, and sending different types of data to the optimal place for analysis. Time-sensitive data is analyzed on the fog node closest to the things generating the data. Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action. Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage.

Figure 81 Data Transactions in a Fog Computing Architecture



By leveraging fog-based architectures, pipeline operators can benefit from the proximity of processing at the right place, speed, mobility, cost (by reducing the amount of data needed to be transmitted), and security and governance. By combining fog with cloud, use cases can also take advantage of centralized computing power to collate and analyze data from all remote locations to provide trending on optimization services over time.

The best-known standard for fog computing comes from the OpenFog Consortium[1], which has now been formally adopted by the IEEE.

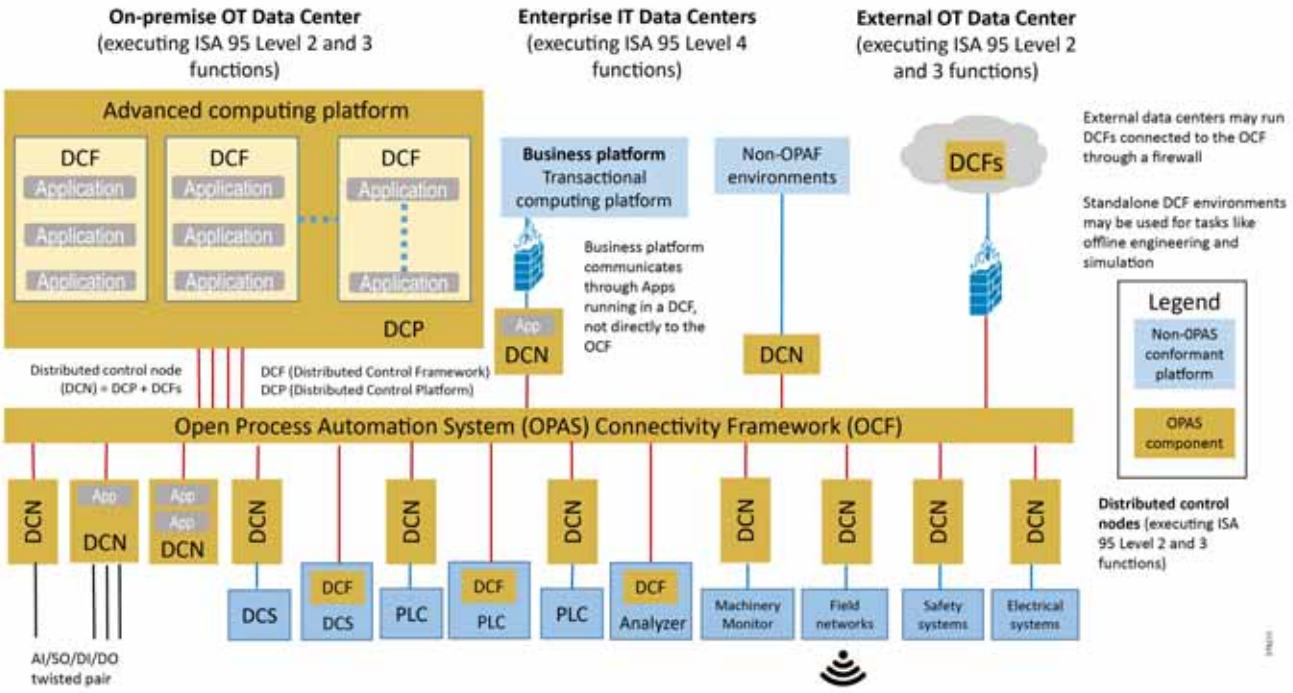
1. https://www.digitalistmag.com/cio-knowledge/2018/06/21/edge-computing-cloud-for-remote-operations-part-2-06177273

Open Process Automation

A recent standardized approach driven by ExxonMobil has resulted in the Open Process Automation initiative. In industrial environments, different vendors typically have multiple control systems, each with their own protocols, philosophies, interfaces, development ecosystems, and security. This makes the introduction of new technologies or digital use cases potentially challenging and more expensive to integrate and implement. The Open Process Automation approach is to develop a single IIoT-based architecture to address these challenges.

The central focus of the architecture (Figure 82) is a software integration bus that acts as a software backplane that facilitates distributed control. Building out the rest of the architecture are capabilities including end-to-end security, system management, automated provisioning, and distributed data management.

Figure 82 Open Process Automation Architecture



Practically speaking, the fact that the majority of security technologies deployed in operational environments are IT-centric (typically enforced as part of IEC 62443-3-3 (system security requirements and security levels)), operational staff have a skill set challenge since IT-centric skills are needed to deploy the networking, infrastructure, and compute technologies that OT needs to operate. This also raises the challenge of who (IT or OT) owns which use cases and services, and where the IT and security skills should reside.

Standards for IIoT and Digital

We have highlighted some examples of the many changing architectural approaches that are already affecting the operational environment. Each of the standards mentioned, along with the other industrial frameworks, factor in the inherent need for security and include either integrated guidance or separate design documents. At the end of this chapter, we provide a comprehensive list of the most applicable standards and guidelines in this domain. One of the big challenges with IIoT and digital transformation is the multitude of competing standards, guidelines, and consortia, and the lack of alignment and consistency among them.

As digital and IIoT offerings evolve, the need for a standardized approach to not just allow devices to communicate, but to perform common IIoT backend tasks such as security, automation, analytics, and business insight, is becoming increasingly relevant. Industrial companies will continue to drive this need through new use cases and technology

adoption, creating a need for IIoT solutions for the operational domain to interoperate with common backend services, guaranteeing levels of interoperability, portability, serviceability, and manageability, in conjunction with today's control system technology.

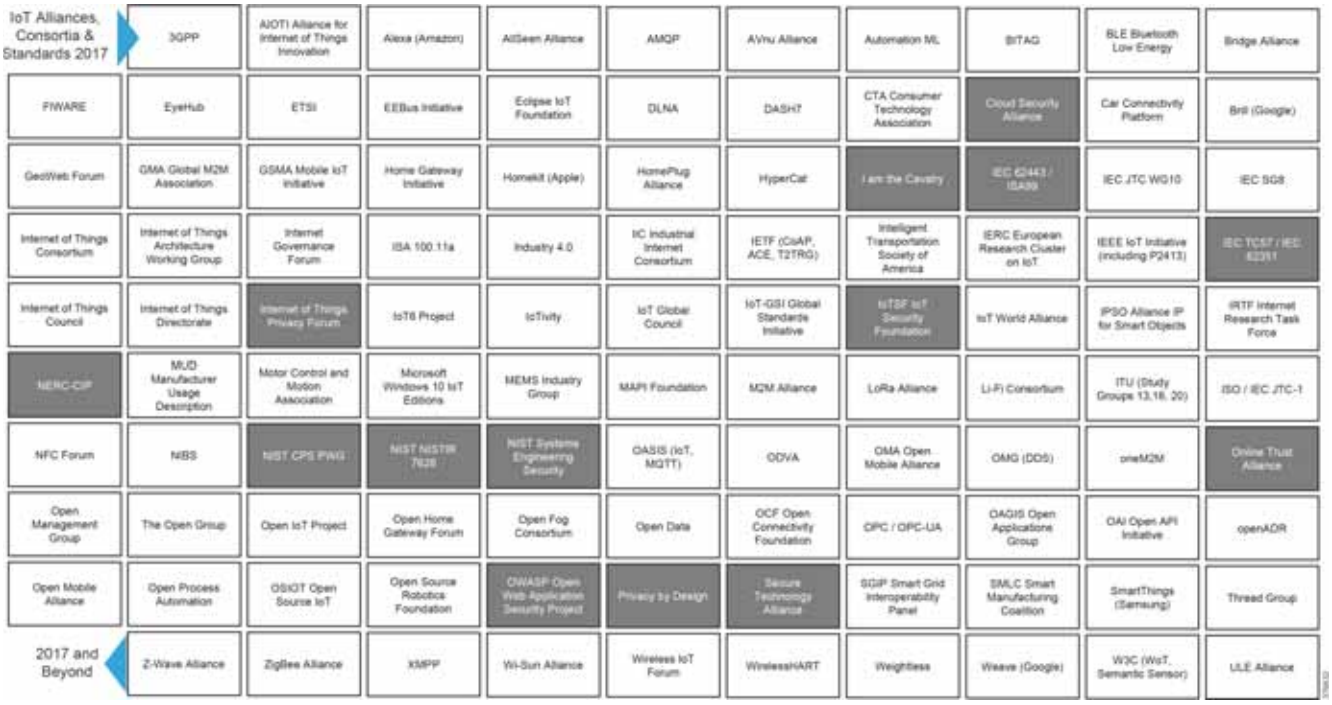
As pipeline companies look to architect, design, and build new systems that include digital technologies, we need to carefully consider the standards that exist today in conjunction with those emerging, and choose wisely. A broad collection of standards, alliances, consortia, and regulatory bodies are already in play, as shown in Figure 83. How the path forward is determined is critical and how it affects security must always remain at the forefront. Standards will help to minimize the attack surface, realize better visibility of security incidents, and provide consistent and usable tools to defend, detect, remediate, and report security incidents.

Practical considerations for pipeline companies looking to introduce digital and IIoT technology include:

- Do not create something that already exists. The US Department for Homeland Security advises, that as part of a strategy to secure IoT, to build on recognized architectural and security practices. Many tested practices that are used in the operational environment today, in addition to traditional IT and network security, can be applied to IIoT.
- Start with a basic, consistent architecture augmented with cybersecurity standards and best practices, applying them to not only the IIoT use case, but to the entire IIoT ecosystem that may form part of a solution.
- Leverage sector or market-specific best practice and guidelines where available. Unique architectural and security approaches, or regulation, will exist.
- Try to assess industry indicators to determine which standard will win out longer term. Backing the wrong standard may mean a system could become non-interoperable or obsolete, resulting in a waste of time and money. A method to achieve this is to back the standards bodies that the large vendors and industry players are backing. This could, however, be a challenge where a number of industry leading IoT companies, such as Cisco, Intel, IBM, GE, and Microsoft, appear to be hedging their bets and working across multiple consortia.

The standards, guidelines, consortia and alliances landscape is broad with a wealth of options. The likelihood is that, in the short term, this may increase, but the industry will eventually need to converge if we are to realize the IoT vision. Figure 83 shows the main groups in 2017; note that this is not an exhaustive list, and that a number of specific security groups are highlighted.

Figure 83 The IoT Standards and Guidance Landscape (Source: Orchestrating and Automating Security for the Internet of Things)



As mentioned, we didn't design this reference guide to be a detailed guide into the standards that currently exist or are emerging for this space, but to emphasize that the industry is continuously adapting to meet the ever arising new use cases and technologies that drive the IIoT ecosystem.e. From a security perspective, readers are recommended to familiarize themselves with the various companion guidelines or integrated sections (as seen in the OpenFog consortium, and Open Process Automation standards). However, we are including the following example, which is one of the more common and comprehensive approaches to security in the operational environment as IIoT and digital technologies become more widespread and integrated.

Industrial Internet Security Framework (IISF) IIC Reference Architecture

One of the best-known approaches to IoT for the industrial environment is the IIC Security Framework document (and associated reference architecture), which is an integrated element of the Industrial Internet Consortium (IIC) reference architecture. IT and OT have elements that interact, and can often conflict, with each other. To be most successful, these different elements must converge and be reconciled with each other into overall system trustworthiness. This is clearly essential in the operational pipeline environment as companies look to balance new use cases with existing pipeline management systems.

The IISF is a guide for industrial environments aimed at addressing security, privacy, safety, and reliability issues caused by the addition of new connectivity to historically disconnected devices or segmented systems. The main goal is to set a significantly higher security level than that seen for consumer and COTS devices.

The new framework articulates a standard for *trustworthiness* in industrial IoT systems and provides standard definitions for concepts like *risk*, *threats*, *metrics*, and *performance indicators*. Unlike traditional industrial control systems, IIoT systems are inherently connected to other systems and people, increasing both potential complexity and attack surface.

The framework divides the IoT environment into three areas: component builders who create hardware and software, system builders who build solutions on top of the hardware and software, and the owners and operators of those systems. To ensure end-to-end security, industrial users must assess the level of trustworthiness of the complete system, including all three of these areas. This reflects the ecosystem approach mentioned in the first section of this guide.

The IISF describes characteristics that affect the trust decisions of an IIoT deployment and must be considered:

- Top five (key system characteristics): security, safety, reliability, resilience and privacy
- Others (non-key characteristics) include scalability, usability, maintainability, portability and composability

The focus of the architecture is to provide assurance of the key system characteristics. Assurance requires the collection and analysis of evidence that supports the design, construction, deployment, and test of an IIoT system, and the activities that take place during operation. The correct blend of innate system capabilities, and compensating security controls, must be demonstrable through evidence. Assurance comprises risk analysis to identify hazards and prevent incidents or accidents, including rigorous design and validation testing. The key system characteristics are the following:

- **Security** is seen as the condition of the system being protected from unintended or unauthorized access, change, or destruction, and is seen as a continuum. The document recognizes that no IoT system can be fully secure in every context, so the specific contexts deemed relevant must be explicitly outlined in the design or risk assessment, along with the mitigating security controls that the stakeholders expect.
- **Safety** is defined as the system operating without causing, directly or indirectly, unacceptable risk of physical injury or damage to the health of people or to the environment.
- **Reliability** is seen as the ability of the full system, or parts of it, to perform as specified, under normal operating conditions, for a determined period of time. System availability is also called out, taking into consideration planned scheduled maintenance, updates, repairs, and backups. When these tasks take place, reliability is reduced as the system is not operating; however, they do not affect reliability if properly scheduled.
- **Resilience** refers to how a system behaves to avoid, absorb, and manage dynamic and challenging conditions, while still completing pre-defined activities. It is recommended to design the system so that failures are compartmentalized, meaning a single function failure does not affect other functions.
- **Privacy** is defined as the right of an individual or group, to control or influence what information related to them may be collected, processed, and stored. This also includes by whom, in terms of collecting or to having access.

In addition, the reference architecture includes a number of recommendations:

- The architecture of the system must provide end-to-end security from the edge endpoint to the cloud. This includes endpoint hardening and onboarding, protecting communications, policy and update management, secure remote access, and leveraging analytics to monitor the entire security process. Wherever possible, security and real-time situational awareness should cover IT and OT, without affecting operational business processes.
- Security should be fully integrated into the architecture and system design as opposed to being added as an afterthought. Security must be built into the design and risks should be evaluated early, rather than trying to bolt-on security as an afterthought. Achieving this is understood to be easier for greenfield deployments, while much more difficult for existing scenarios.
- Any design should include an ecosystem approach, where anyone who is part of the system—vendors, systems integrators and equipment owner/operators—must be involved in any security risk assessment, architecture, or design.
- No single "best way" exists to implement security and achieve adequately secure behavior. Technological building blocks should support a defense-in-depth strategy that maps logical defensive levels to security tools and techniques.

- No " one size fits all" solution exists. Multiple sub-networks and differing functional zones may have different operating technologies and security requirements. Security tools and techniques built for IT environments may not always be well suited for OT environments.
- An essential element is that IIoT system security should rely on automation as much as possible, with provisions for users to be able to interact with the security implementation to monitor status, review analytics, make decisions when needed, and plan modifications and improvements. There is recognition that humans may cause security challenges through misconfiguration and errors.

The functional viewpoint of the security framework consists of six interacting building blocks that are organized into three layers, as shown in Figure 84. The top layer includes the four core security functions of security configuration management, security monitoring and analysis, communications and connectivity protection, and endpoint protection. A data protection layer and a system-wide security model and policy layer supports these core functions.

Figure 84 IISF Functional Building Blocks

The IISF document describes the role of each of these functions in creating and maintaining the overall security of the system. Endpoint protection implements defensive capabilities on devices wherever they are located in the system, and emphasizes physical security of the device, cyber security techniques, and identity of the device through an identity management system or authority.

The communications and connectivity protection leverages the authoritative identity capability to authenticate and authorize data traffic. Cryptographic and information flow control techniques should be used to protect communications and connectivity.

When endpoints are protected and communications secured, the system state must be preserved throughout its operational lifecycle with security monitoring and analysis, and controlled security configuration management for all system components.

The data protection function covers data-at-rest in the endpoints, data-in-motion in the communications, and encompasses any data generated through the monitoring and analysis function, and all system configuration and management data.

The security model and policy orchestrates how the functional elements work together to deliver an end-to-end security strategy. This layer governs how security is implemented, and the associated policies that ensure confidentiality, integrity, and availability of the system are maintained throughout the lifecycle.

These six building blocks provide guidance for implementing security end-to-end across IIoT systems in the context of trustworthiness. To translate these blocks into a specific implementation, the reference architecture recommends the following eight design principles, any number of which may be applied when implementing each of the functional building blocks:

- **Principle of economy of mechanism**: Keep the design as simple and small as possible.
- **Principle of fail-safe defaults**: Base access decisions on permission rather than exclusion.
- **Principle of complete mediation**: Every access to every object must be checked for authority.

- **Principle of open design**: A design should not be secret. The mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific, more easily protected, keys or passwords.
- **Principle of separation of privilege**: Where feasible, a protection mechanism that requires two keys to unlock is more robust and flexible than one that allows access to the presenter of only a single key.
- **Principle of least privilege**: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Principle of least common mechanism**: Minimize the amount of mechanism common to more than one user and depended on by all users.
- **Principle of psychological acceptability**: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Conclusion

OT and IT security solutions cannot simply be deployed interchangeably. The same technology sets may be used, but the architecture and implementation strategy may be different. And although IT and OT teams may be part of the same organization, they may have different priorities and often skill sets. Due to these changing needs, in conjunction with the growing number of regulatory legislation aimed at critical infrastructure protection, an urgent need exists for stronger cyber security in OT environments, which should be designed with a defense and detection-in-depth approach to mitigate potential damage. This must involve a multi-layered, multi-technology, and multi-party (IT, OT, and vendors) strategy to protect critical assets. The reality is that most petroleum organizations still have a gap between IT and OT, some still very siloed and with others more closely aligned, which is unlikely to disappear in the short term.

New use cases, technologies, and architectural approaches for IIoT are constantly being introduced into the pipeline environment. Although most of these today are based on monitoring capabilities only, and are often deployed on separate infrastructure, pilots are already in place focused on control and leveraging common infrastructure to best meet the needs of the overall organization. The resulting deployments sometimes break the traditional segmented hierarchical approach followed, with connectivity directly from the edge to the enterprise or the cloud, and even localized closed-loop control with no centralized decision making in the process. In reality, this is likely to only increase over time, meaning security considerations will be at the forefront of design for some time.

This is, however, not an overnight process. It will be a slow and gradual change from legacy SCADA to real-time data driven support systems. However, as organizations benefit from outcomes such as predictive or condition-based maintenance, optimized flow, and real-time leak detection, more and more assets will become connected with more and more sensors in the effort for organizations to become more efficient and keep assets operational.

This means a properly designed standards-based architecture to secure use cases and systems, bringing together the operational domains with IIoT and IT approaches, is critical. Architecture will provide an understanding of all components of a use case, map these elements together in a structured way, and show how they interact and work together. Architecture will not only bring together IT and OT technologies, but should also include vendors and third party components to complete the full system architecture – in other words, secure the ecosystem.

As reference and solution architectures are developed, they must provide a foundation, leveraging an end-to-end approach with technologies designed to operate together, minimizing risk and operational complexity. These requirements should be implemented across both existing and new use cases, and for control systems and emerging technologies such as IoT, big data, mobility, virtualized infrastructure, and collaboration. However slow the change, it is an inevitability.

References and Related Documentation

References Cited in Footnotes

- Accenture Report: Oil and Gas Companies' Cybersecurity Strategies Are Evolving, But Monitoring and Responding Quickly to Cyberattacks Remains a Challenge
  https://newsroom.accenture.com/news/accenture-report-oil-and-gas-companies-cybersecurity-strategies-are-evolving-but-monitoring-and-responding-quickly-to-cyberattacks-remains-a-challenge.htm
- Cost of a Data Breach Study
  https://www.ibm.com/security/data-breach
- Digital Transformation Initiative—Oil and Gas Industry
  http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-oil-and-gas-industry-white-paper.pdf
- DNV GL reveals top ten cyber security vulnerabilities for the oil and gas industry
  https://www.safety4sea.com/dnv-gl-reveals-top-ten-cyber-security-vulnerabilities-for-the-oil-and-gas-industry/
- Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry
  https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-am-project-description-draft.pdf
- FEMA—Business Continuity Plan
  https://www.ready.gov/business/implementation/continuity
- Gartner Says the Worlds of IT and Operational Technology Are Converging
  http://www.gartner.com/newsroom/id/1590814
- Infrastructure & Operations—Infrastructure agility: The I&O imperative
  http://www.gartner.com/technology/research/infrastructure-operations-management.jsp
- Insider Threat: 74% of security incidents come from the extended enterprise, not hacking groups
  https://www.clearswift.com/about-us/pr/press-releases/insider-threat-74-security-incidents-come-extended-enterprise-not-hacking-groups
- ICS-CERT Year in Review. Industrial Control Systems Cyber Emergency Response Team 2016
  https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf
- Oil and Gas Digital and Technology Trends Survey
  https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_15/Accenture-Microsoft-Digital-Energy-Survey-2015.pdf
- Securing Industrial Control Systems-2017
  https://www.sans.org/reading-room/whitepapers/ICS/securing-industrial-control-systems-2017-37860
- The State of Industrial Cybersecurity 2017
  https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf
- US-CERT—The Common Criteria
  https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria
- Program Review for Information Security Assistance (PRISMA) Security Maturity Levels
  https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels
- How Mature is Your Risk Management?
  https://hbr.org/2012/06/how-mature-is-your-risk-manage
- TSA—Pipeline Security Guidelines
  https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

Other Related Documents

- Accenture—Energy
  https://www.accenture.com/us-en/energy-index
- Cybersecurity in Energy: The Implications of a Security Breach on an Oil & Gas Company
  http://energy.sia-partners.com/20170727/cybersecurity_in_energy_implications_of_a_security_breach_on_an_og_company
- Digitization and cyber disruption in oil and gas
  http://www.ey.com/Publication/vwLUAssets/ey-wpc-digitization-and-cyber/$FILE/ey-wpc-digitization-and-cyber.pdf
- Industrial automation cybersecurity conformity assessments
  http://www.isasecure.org/en-US/Articles/Industrial-automation-cybersecurity-conformity-ass
- Ponemon Institute—The State of Cybersecurity in the Oil & Gas Industry: United States
  http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf
- Smart Connected Pipeline—Control Centers:
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-control-center.html
- Smart Connected Pipeline—Operational Telecoms:
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-operational-telecoms.html
- Special Report: Cyber security becomes critical concern
  http://www.arabianoilandgas.com/article-17922-special-report-cyber-security-becomes-critical-concern/

Glossary

Term	Description
#	
2FA	Two-Factor Authentication
A	
AAA	authentication, authorization, and accounting
AAR	After Action Report
ACLs	Access Control Lists
ACS	Access Control System
AI	artificial intelligence
APM	Application Performance Management
APT	advanced persistent threat
ARP	address resolution protocol
B	
BCC	Backup Control Center
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Units
BYOD	Bring Your Own Device
C	
CAM	Content Addressable Memory
CCTV	Closed-circuit television
CDM	Continuous Diagnostics and Mitigation
CDO	Chief Digitalization Officer
CDP	Cisco Discovery Protocol
CEPA	Canadian Energy Pipeline Association
CFATS	Chemical Facility Anti-Terrorism Standards
CIA	Confidentiality, Integrity, and Availability
CIM	Common Information Model
CIO	Chief Information Officer
CIP	Control and Information Protocol
CISO	Chief Information Security Officer
CM	Configuration Management
CoPP	Control Plane Policing
COTS	Commercial off-the-shelf
CPNI	Center for Protection of National Infrastructure
CSO	Chief Security Officer
CSRA	cybersecurity reference architecture
CSRC	NIST Computer Security Resource Center
CVE	Common Vulnerabilities and Exposures

Term	Description
D	
DBMS	database management system
DC	Domain Controller
DDoS	distributed denial-of-service
DHCP	Dynamic Host Configuration Protocol
DMTF	Distributed Management Task Force
DMVPN	Dynamic Multipoint Virtual Private Network
DMZ	Demilitarized Zones
DNS	Domain Name Server
DOE	Department of Energy
DoS	Denial of Service
DPI	deep packet inspection
DR	Disaster Recovery
DSS	Data Security Standards
DWDM	dense wavelength-division multiplexing
E	
EALs	Evaluation Assurance Levels
EDI	electronic data interchange
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
EUM	End-user monitoring
F	
FAT	Factory Acceptance Testing
FEED	Front End Engineering and Design
FEMA	Federal Emergency Management Association
FTP	File Transfer Protocol
G	
GAO	General Accounting Office
H	
HMI	Human-Machine Interface
HSE	Health, Safety, or Environment
HTTPS	Hypertext Transport Protocol Secure
I	
iACLs	Infrastructure Access Control Lists
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDMZ	Industrial Demilitarized Zone
IDS	intrusion detection system
IED	Intelligent Electronic Devices

Term	Description
IND	Cisco's Industrial Network Director
IoT	Internet of Things
IPS	Intrusion Protection System
ISE	Cisco's Identity Services Engine
IS-IS	Intermediate System to Intermediate System
ISS	Integrated Security System
IT	information technology
K	
KPI	key performance indicators
M	
MAB	MAC Authentication Bypass
MES	Manufacturing Execution Systems
MITM	man in the middle
MLE	Maturity Level Evaluation
MPLS	Multiprotocol Label Switching
MSS	Managed Security Services
MSSP	Managed Security Service Providers
N	
NAC	Network Access Control
NGFW	Next Generation Firewalls
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	
OODA	Observe, Orient, Decide, Act
OSPF	Open Shortest Path First
OT	operational technology
P	
PAGA	Public Address and General Alarm
PAT	Preliminary Acceptance Testing
PCC	Primary Control Center
PCD	Process Control Domain
PCN	Process Control Network
PDCA	Plan, Do, Check, Act
PHMSA	Pipeline and Hazardous Materials Safety Administration
PIDS	Physical Intrusion Detection System
PIG	Pipeline Inspection Gauge
PII	Personally Identifiable Information
PLC	Programmable logic controllers
PMS	pipeline management systems
PODS	Pipeline Open Data Standards

Term	Description
PRISMA	Program Review for Information Security Assistance
PTS	Personnel Tracking System
PTZ	Pan, Tilt, and Zoom
R	
RBAC	Role-Based Access Control
RE	Requirement Enhancements
RIP	Routing Information Protocol
RPF	Reverse path forwarding
RTU	remote terminal unit
S	
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protocol
SDLC	System Development Lifecycle
Secure Socket Layer	SSL
SFA	single-factor authentication
SFTP	Secure File Transport Protocol
SIEM	Security Information and Event Management
SL	Security Levels
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SOC	security operation centers
SPAN	Catalyst Switched Port Analyzer
SPOF	Single Point of Failure
SR	System Requirements
SSH	Secure Shell
SSI	Sensitive Security Information
SUC	System under Consideration
SVA	Security Vulnerability Assessment
T	
TACACS+	Terminal Access Controller Access Control System
TAP	Terminal Access Point
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TVDA	Tested Validated Documented Architecture
U	
UDP	User Datagram Protocol
V	
VM	virtual machines

Term	Description
VOIP	video over IP
VSAN	Virtual Storage Area Networks
W	
WBEM	Web-Based Enterprise Management