State of Operational Technology Cybersecurity in the Oil and Natural Gas Industry

APRIL 2014

energy API®

AMERICAN PETROLEUM INSTITUTE

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Suggested revisions are invited and should be submitted to the Tax and Accounting Policy department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

Page

Figures

Contents

Page

Tables

Executive Summary

Operational Technologies (OT) comprise hardware and software assets, tools, and procedures used to monitor and control physical processes. OT cybersecurity includes controls to protect and secure these assets as well as methodologies, methods, devices, and tools used to ensure the stability, resilience, and ease of recovery of these assets during and after a cyber event. This document is a detailed discussion of the current state of OT cybersecurity in the Oil and Natural Gas (ONG) industry. The result of cumulative research and analysis conducted within the industry, this report examines data, metrics, and trends to reach overarching ONG-specific conclusions about the state of security of OT assets and processes.

The ONG industry, as defined by organizations such as the U.S. Congress, is a foundational element of the U.S. economy and critical infrastructure (CI). Uninterrupted ONG operations must exist to ensure national stability and security as well as to support basic social functions. Like other national CI sectors, the ONG industry finds itself a target of almost constant cyber threats. OT technology continues to evolve and these threats create additional challenges and issues that transcend technology and processes. The ONG industry has already developed a framework of cybersecurity objectives and standards, with many methods for applying and maintaining fundamental and advanced security practices. This framework, which promotes secure operations and business continuity, includes protection, defense, resilience, and recovery methods. A number of risk management methodologies are also in practice today to prevent cyber events, increase resilience, and speed recovery. Methods of meeting objectives and applying security are constantly in flux and require commitment from industry sub-sectors, trade organizations, and individual asset owners and operators.

This document identifies common security approaches in Information Technology (IT) and OT, the unique aspects of the OT environment, potential consequences of security shortcomings in OT, and interoperability between IT and OT. OT systems used across the individual ONG sub-industries are described in detail, to include components and their respective cyber risks and diagrams of architectural interconnectivity

Over the past decade, asset owners have shown a significant interest in applying best-practice security controls to their OT systems. The realization that continuity of operations depends on OT system security is a generally shared view across the industry. A number of resources exist for asset owners to leverage in meeting security objectives. Typically an asset owner develops a security program that maps to the needs of their specific OT environment. This may involve developing a program in-house or with assistance from third parties or consultants, or choosing a set of guidelines or standards to leverage. Suitable guidelines are available from government and industry sources. The spectrum of choices allows industry to select a best-fit for their operational space, which typically considers many factors such as geographical location of the system, criticality of the system, and economic impact of the system. In addition to written guidance, asset owners have options for building programs that include assessments and audits, policy and procedure development, and incident response capabilities. A wealth of information regarding assessment science, options, and components has been developed by both industry forums and government entities to assist with this process.

Over the past decade, the body of knowledge around identifying and implementing best-practice security programs has expanded significantly with the benefit of artifacts from collaborative projects that provided guidance, methodologies, and research findings. As the cyber threat landscape grows to be areality of daily operations, the industry continues to adapt and respond to, and defend against these threats by implementing and maintaining security controls based on cutting-edge technology, and program and industry standards. The industry continues to employ advanced technologies while mitigating risk and continuing secure operations.

Finally, recommendations are presented in this document that outline productive roles for the ONG industry and federal government to play in promoting effective cybersecurity practice and strengthening the overall national CI.

Introduction

This document is a detailed discussion of the current state of Operational Technology (OT) cybersecurity in the Oil and Natural Gas (ONG) industry. The result of cumulative research and analysis conducted within the industry, this report identifies data, metrics, and trends to reach overarching ONG-specific conclusions about the state of cybersecurity of OT assets and processes.

State of Operational Technology Cybersecurity in the Oil and Natural Gas Industry

1 Scope

1.1 General

The scope of this document includes operational technology (OT) for the oil and natural gas (ONG) industry. Control system technology and operational processes are described in detail in later sections. The scope includes the current state of cybersecurity of OT within the ONG industry.

1.2 Document Purpose

The purpose of this document is to provide a detailed and critical examination of the state of OT cybersecurity within the ONG industry, at this point in time. It is intended to provide the report's audience with a full scope of OT cybersecurity that is inclusive of practices, controls, and risk mitigation techniques currently in use by industry asset owners.

This document is not intended to be a 'how-to' manual or to provide step-by-step instructions on how to design, implement, monitor, control, and upgrade OT cybersecurity systems. Each industry location, system and operational environment is unique. The corresponding OT cybersecurity approach is equally unique to the physical and operational environment, the risk level, the potential threats, and the type of system used. Instead, this document provides an overview of the present state of OT cybersecurity.

1.3 Intended Audience

The intended audience of this report is the American Petroleum Institute (API) membership and practitioners with a detailed, working-to-advanced understanding and knowledge of this topic gained through real-world experience. Managers and supervisors of OT, as well as risk managers and security managers, are included in the target audience. This paper is not intended for the general public or for individuals who have no understanding of OT cybersecurity.

2 Terms, Definitions, and Acronyms

2.1 Terms and Definitions

For the purposes of this document, the following definitions apply:

2.1.2
consequences
Result on the system if a threat has successfully exploited an vulnerability.

2.1.2
cyber
A prefix that means "computer" or "computer network".

2.1.3
cybersecurity
Measures taken to protect a computer or computer system against unauthorized access or attack. First known use occurred in 1994.

2.1.4
distributed control system
DCS
An automated control system that distributes autonomous monitoring and control capabilities throughout the network.

2.1.5
demilitarized zone
DMZ
An intermediary zone between trusted and untrusted networks, providing monitored and controlled access and data transfer [7]**.**

2.1.6
emergency shutdown systems
ESD
An ESD or safety instrumented system (SIS) is a system comprising sensors, logic solvers and actuators for the purposes of taking a process to a safe state when normal predetermined set points are exceeded, or safe operating conditions are violated [42].

2.1.7
field data acquisition
FDA
A system with the primary purpose to gather all assigned field data into a common device with no human interaction.

2.1.8
flow computers
FC
Computer-based devices which convert the raw flow meter data, such as that from turbine meter pulses, into information such as net and gross flow rates, as well as accumulated volumes.

2.1.9
human machine interface
HMI
A software application that presents information and data from a computer system to the user in a combination of forms (graphically, numerically, tabular, etc.).

2.1.10
incident command system
A set of personnel, policies, procedures, facilities, and equipment that are integrated into a common organizational structure designed to improve emergency response operations of all types and complexities.

2.1.11
industrial control systems
ICS
A broad term that often encompasses supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system components such as Programmable Logic Controllers (PLC). ICS are typically used to monitor and control industrial processes such as systems within a refinery, pump station, manufacturing facility, etc.

2.1.12
industry standards
Standards that are developed by industry organizations that are based on sound engineering principles and current industry best practices.

2.1.13
local area network
LAN
A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network [7].

2.1.14
non-redundant SCADA systems
SCADA systems that utilize a single computer, network, or field device. No redundancy exists within the system.

2.1.15
operational risk
Risk of losses resulting from inadequate or failed internal processes, people and technology or from external events.

2.1.16
operational technology
OT
A collective term referring to control systems (industrial control systems or ICS, distributed control systems, or DCS, production control systems or PCS, supervisory control and data acquisition or SCADA, etc.) that companies use to automate machinery that manufactures, produces or delivers a product.

2.1.17
operations control center
OCC
A physical location where personnel monitor the systems process, direct and control communications, initiate physical system changes, and coordinate the overall process operations.

2.1.18
process control system
PCS
A system designed to ensure a process is predictable, stable, and consistently operating at the target level of performance. It may include computers, field sensing and control devices, as well as a communications network that links all components together.

2.1.19
programmable logic controllers
PLC
Programmable logic controllers are hardened, special purpose zcomputer systems that are generally used for discrete control of specific applications and generally provide regulatory control. These systems often interface and interact with DCS, ICS, and SCADA systems as well as standalone process monitoring and control systems.

2.1.20
remote data terminal units/data concentrators
Devices which gather or concentrate various field input data such as valve status, motor status, flow meter data, relay status, etc. into a single device. The concentrated data is then transferred to the master terminal unit or distributed control unit.

2.1.21
remote terminal unit
RTUs
A remote device typically used to gather status, alarms and analog remote readings for transmission to the SCADA system and transfer controls from the SCAD system to a field device [7].

2.1.22
risk
Impact to the organization as a function of threat, vulnerability, and consequence.

2.1.23
risk assessment
The identification, evaluation and estimation of the levels of risk presented to safe and secure operations by security and safety issues, and the comparison of those levels of risk to benchmarks or standards to determine acceptability.

2.1.24
risk based performance
Integration of the corporation's risk management and performance metrics to support a decision framework that balances risk and performance.

2.1.25
safety instrumented systems
SIS
An engineered set of hardware and software controls that are specifically designed for monitoring and controlling critical process systems. The SIS is designed to ensure the system remains in a safe state under all operating, transitional and shutdown states. Often the term 'fail safe' is associated with these systems, which means that the system will always go to a safe state regardless of operational events.

2.1.26
SCADA host/master
A system comprising a computer and software that transfers data from the field systems to the Operator graphical user interface (GUI). The system may also initiate control commands and setpoint changes to the field systems from the GUI or the master terminal unit using automated control applications.

2.1.27
standards
A document or set of documents that defines terms; classifies components; delineates procedures; specifies dimensions, materials, performance, designs, or operations; measures quality and quantity in describing materials, processes, products, systems, services, or practices; defines test methods and sampling procedures; and/or describes fit and measurements of size or strength.

2.1.28
supervisory control and data acquisition
SCADA
A combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling dispersed assets using centralized data acquisition and supervisory control.

2.1.29
telecommunications infrastructure
Infrastructure that provides the electronic link between separate locations. In the context of OT, the telecommunications infrastructure links the central control center with all remote locations.

2.1.30
threat
An internal or external agent that may disrupt operations or cause harm to the organization, its systems or its data.

2.1.31
vulnerability
A weakness in a system that can be exploited.

2.2 Acronyms

AGA	American Gas Association
ANSI	American National Standards Institute
API	American Petroleum Institute
ARPANET	Advanced Research Project Agency Network
BYOD	bring your own device
CFR	Code of Federal Regulations
CI	critical infrastructure
CIKR	critical infrastructure and key resources sectors
CISA	certified information systems auditor
CISSP	certified information systems security professional
CPU	central processing unit
CSSLP	certified secure software lifecycle professional
CSSP	control systems security program
CWSP	certified wireless security professional
DCS	distributed control system
DHS	Department of Homeland Security
DMZ	demilitarized zone
DOT	Department of Transportation
EPA	Environmental Protection Agency
ESCSWG	energy sector control system working group
ESD	emergency shutdown systems
FBI	Federal Bureau of Investigation
FC	flow computers
FDA	field data acquisition
FFRDCs	federally funded research and development centers
FS	field systems
GAO	General Accounting Office
GSS-JAVA	GIAC Secure Software Programmer - Java

GUI	graphical user interface
HMI	human machine interface
HSIN	Homeland Security Information Network
I3P	Information Infrastructure Protection
ICS	industrial control systems
ICS-CERT	industrial control systems cyber emergency response team
ICSJWG	industrial control systems joint working group
ICT	information and communication technology
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INGAA	Interstate Natural Gas Association of America
IPS	intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standards
IT	information technology
LAN	local area network
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
MACT	maximum achievable control technology regulations
NIST	National Institute of Standards and Technology
OCC	operations control center
NRC	National Research Council
NRC Advisory	Nuclear Regulatory Commission Advisory
NTSB	National Transportation Safety Bureau
ONG	oil and natural gas
Onshore and Offshore E&P	onshore and offshore exploration and production
OT	operational technology
PCCIP	President’s Commission of Critical Infrastructure Protection
PCN	process control network
PCS	process control systems
PCS	production control systems
PLC	programmable logic controllers
PPD	Presidential Policy Directive
RTUs	remote terminal units
SCADA	supervisory control and data acquisition

SSAx	sector specific agencies
SIS	safety instrument systems
TSA	Transportation Security Administration
UK	United Kingdom
U.S. CERT	United States Computer Emergency Readiness Team
VPN	virtual private network
WAN	wide area network

3 Background

3.1 General

Operational Technologies comprise hardware and software assets, tools, and procedures and processes used in critical operations. OT cybersecurity includes controls to protect and secure these assets as well as methodologies, methods, devices, and tools used to ensure the stability, resilience, and ease of recovery of these assets during and after a Cyber event. "Society ultimately expects computer systems to be trustworthy – that is, that they do what is required and expected of them despite … attacks by hostile parties [i.e. cyber events]…" [44]. OT systems, once installed, have a long lifespan. Yet the uses and requirements of OT data elements are ever-changing and vital to an organization's operation. In essence, securing OT systems resembles taking aim at a moving target.

OT systems that are designed and used to remotely or centrally monitor and control a process have a long evolutionary history. The first application of a rudimentary operational technology, or by another name process control systems (PCS), is traced to the 1912 Chicago power industry, which relied on people who were located on either end of a telephone line to provide system status information and implement controls as required [157]. From that minimalistic foundation, OT systems evolved to a point where, in 1959, industrial control computer systems were first deployed at the Texaco Port Arthur refinery in Texas [52].

As OT technology evolves, it creates additional challenges and issues that transcend the technology and processes. This evolution increases the difficulty in fully describing and quantifying cybersecurity. Further, technology changes make it virtually impossible to predict and plan for the future. The risk map, potential attack surface, and even the protective mechanisms, are extremely difficult to forecast.

The ONG industry, as defined by organizations such as the U.S. Congress, is a foundational element of the U.S. economy and CI. Uninterrupted ONG operations must exist to ensure national stability and security as well as support basic social functions. Threats to the U.S. have changed over time and continue to change. Like other national CI sectors, the ONG industry finds itself a target of almost constant threats. However, ONG companies provide core products and services that form the cornerstone of American energy. As the basis for interdependent infrastructures such as electricity and mass transportation, and as an industry that directly serves the transportation needs of consumers every hour of every day, the ONG industry finds itself at higher risk for attacks seeking to damage core U.S. social, economic and defense operations.

All threats against the industry, from script kiddies to organized and well-funded threats, must be taken seriously. Protection from these threats must provide risk-based decision protection while facilitating continuity of operations and business. An incorrect approach to cybersecurity could impact operations and inhibit the seamless flow of energy, which in turn poses serious national consequences.

Technology and operational control systems have evolved significantly. Increased interconnectedness between enterprise networks and OT, and between operators, vendors, and third parties has greatly increased the operational footprint of networks that must be secured. Likewise, the post-9/11 world saw an increased focus on social engineering, phishing, and attempts to infiltrate networks through technology and personnel.

Stuxnet was perhaps the first fully recognized attack against a control system. Since then, Duqu and other events have reinforced the fact that control systems make attractive targets. Major corporations have also been hit by the Anonymous group, a costly nuisance. Threats cannot be controlled by CI organizations, so they must rely on technical defenses, on designing and maintaining resilient infrastructures, and on maintaining high levels of protection.

The ONG industry has already developed a framework of cybersecurity objectives and standards, with many methods for application and maintenance. This framework, which promotes operations and business continuity, includes protection, defense, resilience, and recovery methods. Methods of meeting objectives and applying security are constantly in flux, and it requires commitment from industry sub-sectors, trade organizations, and individual asset owners and operators. As the industry moves forward, we must examine the state of OT and cybersecurity to understand the options and potential risks that lie ahead.

3.2 Overview of Current Approaches

OT cybersecurity is an evolution in process. Early day OT systems contained a cybersecurity capability based on a combination of variables which included:

1) culture of trust, i.e. there was no "…need for particular protective measures to keep … [SCADA] systems safe from intentional attacks. After all, why would someone want to disrupt the operation of such systems?" [129];
2) the absence of direct data connections between the corporate infrastructure and the OT system;
3) OT systems having no connectivity to the internet;
4) OT systems having no wireless connectivity; and
5) OT operating systems relying on vendor proprietary software applications.

The combination of these variables is often referred to as security through obscurity or inherent cybersecurity [49]. That is, the OT system is secure as an external entity cannot obtain access to it. If they were able to gain access to it, they would require in-depth technical knowledge of the unique OT system, to include its proprietary software and its vulnerabilities. This severally limited the risk map to either trusted insiders or to a very small subset of external individuals who had the required knowledge and skill sets.

Since the 1960s, when computer-based control systems first appeared "…these systems have been migrating away from centralized mainframe-based architectures, stand-alone telecommunications systems, heterogeneous or platform dependent operating systems, and limited system access by users toward distributed PC and workstation-based distributed data processing architectures, integrated and internet-based telecommunications networks and communications systems, common computer operating systems, and greater desire of external users to obtain field data directly from the source" [49]. This migration and convergence of OT and IT technologies and software, and the need to interconnect, is the driving force for the current technological approaches.

The majority of OT cybersecurity influences resides within the IT organization. As Shaw states "… it is not surprising that many, if not most, of the techniques and technologies employed in security IT systems have direct applicability to modern SCADA systems" [129]. These security techniques and technologies are sometimes referred to as security protocols: "…Security protocols are the rules that govern …" [3].

Table 1 lists some of the common IT security protocols that are generally found within OT infrastructures.

Table 1—Common IT Security Protocols

Common IT Security Protocols	
Policies	An OT system cybersecurity statement of "… beliefs and objectives" [129]
Procedures	"… a clear set of steps and directions for executing a process…" [129]
Passwords	"…these are the main mechanism used to authenticate human users to computer systems" [3].
Data classification	Assigning, managing, and controlling distribution, access, modification rights, etc. of data according to its criticality. At least three levels of data classification are required to include public, private, and confidential.
Disabling non-required services	Disabling or removing operating system services that are not specifically required to operate the OT application.
Disabling non-required external ports	Specifically disabling computer external ports that are not required such as Universal Serial Bus (USB) ports.
Firewalls	A specific system that is configured to allow specific access and deny unauthorized access. Firewalls contain "…logic for checking and blocking of IP messages…" [129]
Demilitarized Zones (DMZ)	A dedicated network that is inserted between two other networks such as a network between the corporate intranet and the OT network. The two networks can access the computers contained within the DMZ but not each other. "A DMZ is an intermediary zone between trusted and untrusted networks, providing monitored and controlled access and data transfer" [7]
Private Internet Protocol Addresses	These are non-routable IP addresses that identify a devices IP address is unique to that network and the routers will never forward traffic from these devices onto the Internet.
Physical security	OT physical infrastructure is located behind physical security barriers such as locked doors and fences that are secure from access by non-authorized personnel.

Table 2 identifies other cybersecurity approaches that are found within the industry but are not as commonly deployed for specific operational purposes.

Table 2—Other Less Commonly Applied Cybersecurity Approaches

Other Less Commonly Applied Cybersecurity Approaches	
Intrusion detection systems (IDS)	"A type of security management for computers and networks. An IDS gathers and analyzes information from various areas within a device or a network to identify possible security breaches, including intrusions and misuse" [7].
Intrusion prevention systems (IPS)	"Supports the ability to receive IDS sensor or scanner data and then apply analytical processes and information to derive conclusions about intrusions, and to execute an appropriate response" [7].
Biometric access control	Application of "…uniquely identifying humans based upon one or more intrinsic physical or behavioral traits" [7].
Access control list	"A list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object" [7].
Antivirus software	Specific software that is designed and configured to identify and prevent malware from operating on the OT computer infrastructure. Antivirus software limitation is that new malware must first be identified and corrective actions developed before it is included in the antivirus application. Zero day exploits, (i.e. an exploit that takes advantage of a previously unknown vulnerability) are not prevented by antivirus software.
Use of Virtual Private Networks (VPNs)	"VPNs comprise a combination of security technologies that allow a set of computers/users to operate across nonsecure, public, shared networks but with the security one might expect on a totally private network…" [129].
Data encryption	The process of converting OT data into unique code that cannot be read without the decryption algorithm or code. At the present time, most remote site data encryption occurs by using a 'bump in the wire' device, which is a special hardware/software device that receives unencrypted data, encrypts it and then sends the data to the destination. A similar device receives the encrypted data, decrypts it and transmits the unencrypted data to the intended receiver.
White listing	A specific application that only allows those applications that have been granted specific authorization to run. Any application that is not specifically allowed to operate is prevented from running.

3.3 Unique Operational Technology Control System Perspectives

Discussing the methodologies, methods, and implications of cybersecurity within the ONG's OT infrastructure brings forward the views of (a) how OT is different from IT, (b) how OT and IT are very similar as they often use the same hardware and telecommunications infrastructures, and (c) how OT and IT convergence "…will deliver…the connectivity and integration needed to address skilled workforce shortages and synchronize supply chains for optimal operation" [114]. In reality, when viewing the industry each of these positions have considerations that drive the current and future state of cybersecurity within the ONG OT infrastructure. These positions also influence industry standards and the regulatory environment as well.

When discussing ONG's OT infrastructure and the application of cybersecurity, what makes OT different or unique from the corporate enterprise or IT side of the corporation? Initially one can view the differences as grounded in the terms of consequences, availability, reliability, and data integrity.

Consequences are the events, results, or outcomes that occur following some sequence of earlier happenings. When an OT system operates as designed, the consequences are as intended—safe and efficient operations. When the OT system fails, for whatever reason, the consequences of the failure can be catastrophic.

It is the potential for extreme negative consequences that makes OT system failures unique when compared to IT system failures. When an OT system fails the consequences can range from an item requiring maintenance to a catastrophic event.

To ensure that the OT system performs as designed, each and every time it is operated, the industry turns to system design criteria of availability, reliability, and data integrity. Availability in an OT environment means "…ensuring the proper operational state for a business to operate…whenever they are needed" [129]. Stated another way, availability is the "…probability that a system is operating successfully when needed. Availability is often expressed as a percentage" [116]. For each organization's operationally high value systems, availability is a paramount need. The system needs to operate successfully every time it is needed, which is typically 24 hours, 7 days a week, 365 days a year.

As indicated, it is mandatory that the OT systems that are monitoring, controlling, and ensuring safe processes always be available to minimize the potential of negative consequences. This criterion is different than the IT system availability requirements where outages impact enterprise operations but generally do not carry the same level, depth and far reaching negative impact of an OT system event. Achieving highly available systems is often seen as utilizing reliable systems that include redundancy of equipment and communication networks.

Another critical part of the OT environment is reliability. A definition of reliability is "…the likelihood that a device will perform its intended function during a specific period of time" [116]. As an example, OT software applications must always work as designed. It is unacceptable for an OT application to stop working or require a reboot in the course of normal operations. When the application comes online, it must correctly perform all functions as designed and continue to do so for the foreseeable future. Full reliability is an imperative.

Availability and reliability are different, but both are essential elements of an OT infrastructure. Unless the system is available and the components reliable, the system will not meet the organization's needs of safely, efficient monitoring, and process control.

The third major differentiator is data integrity. Data integrity means that the data transferred across the OT system are accurate and consistent. This specifically means the data have not been corrupted, inaccurately altered, or modified to reflect something other than reality. From the literature, data integrity means:

> "… ensuring that information displayed by and stored in the system is accurate, up-to-date, of known quality, and confirmed to have come from the correct sources and been processed in the correct manner…" [129]

OT data integrity is essential because "Data integrity attacks (e.g., manipulating sensor or control signals) … through the SCADA network could have severe effects as it misleads operators into making wrong decisions" [134].

Some unique aspects of OT systems, when compared to IT infrastructures, include items such as in Table 3 and those in the following list.

— *System complexity*—Complexity is defined in many ways such as "one whose properties are not fully explained by an understanding of its component parts" [81] or "…the extreme quantity of interactions and of interference between a very large number of units" [99]. The ONG industry OT system design objective is to develop a fully deterministic system. This means that for every event we can say exactly what the result will be. Yet, the OT system includes the human element, many interconnecting parts, various software applications, and failure modes that were never identified or were deemed virtually impossible to happen. Thus, the systems are complex with humans interacting with a network of many distinct devices. The larger the OT system, the more interconnections, and with each increase in the number of interactions, an ever increasing level of complexity occurs.

Ultimately system complexity limits the organization's ability to model and define the system response to various failure modes. As some research points out "… the model and methodologies available for dependency analysis are very limited…" [103]. This unique attribute limits the industry's overall ability to plan a full range of event detection and mitigation efforts.

— *Software patching*—It is not uncommon that OT software applications are not up to date on vendor operating or application system patches. OT system software changes require a much deeper level of testing, validation, and planning. Unlike in enterprise IT, OT operators cannot simply roll out or push updates to OT systems because of these heightened testing and validation requirements.

  If the vendor supplying the operating system software releases a new version or patch, the operator must determine if their OT system vendor has certified that the OT system will continue to work if the new version or patch is applied. Obtaining OT vendor certification often takes time, and in some instances the OT vendor has not certified the new version or patch for compatibility. In this case the ONG company must either continue to use the older operating system, which may have security flaws, or develop an in-house process to validate compatibility.

  Once a decision to upgrade the application is made, deployment of the change requires a methodical, extensively tested, and well supported process. The process may require sending people to remote sites during the upgrade to operate the system in a local or manual mode if remote monitoring and control may not be possible during the upgrade. Clearly patching or upgrading an OT system requires more resources, planning, time, and carries more risk than patching an IT system.

— *Lack of in depth cybersecurity capabilities*—Most technologies deployed today that fall under the OT umbrella do not include minimal cybersecurity capabilities. For example, the majority of remote terminal units, programmable logic controllers, flow computers, etc., either have no password capabilities or use very rudimentary passwords. These systems also fail to provide secure data transfer capabilities such as encryption or antivirus protection.

— *Limited or no personnel located at remote location*—The industry relies on highly available and reliable OT systems to ensure safe and efficient operations. As such, the vast majority of remote locations have no personnel on site. If an event occurs that disables or disrupts the ability to remotely monitor and control a site, it is not uncommon for the operator to shut down the process until someone can travel to that location and restore service.

  Depending on a host of variables, response times can be very long and once on-site the respondent may not have the spare parts or software required to restore the system. Each of these unique events extends the duration that the system may be down and the potential that negative consequences can occur.

— *Long life cycles*—Unlike many IT systems, OT systems have a very long life cycle. Once installed and operational, the systems may operate for ten years or more. During this time, operational changes occur, technology advances by several generations, and the vendor may stop supporting the system as it ages out. Ultimately system support may only be available in-house.

Table 3—Unique Aspects of OT Systems

Unique Aspects of OT Systems	
System complexity	Systems include the interaction of humans, multiplicity of system interconnections, devices, and applications. Complexity increases with "…the extreme quantity of interactions and of interference between a very large number of units" [99].
Software patching	The process of updating installed software. OT system software changes require a much deeper testing, validation, and implementation planning effort than IT systems.
Lack of in depth cybersecurity capabilities	Most OT technologies deployed today do not include minimal cybersecurity capabilities such as passwords, data encryption, etc.
Limited or no personnel located at remote location	Many OT systems are located in remote locations. The majority of the time these sites have no personnel on site.
Long life cycles	Installed OT systems have longer life cycles than IT systems. It is not uncommon for these to be installed for ten years or longer.

OT systems are truly unique. In the ONG sector, each OT system has operational, physical, relational, and environmental differences, influences and requirements that differentiate them from any and all other systems. Although all OT systems share core requirements of providing safe, effective, and efficient monitoring and controlling of the process, no two systems are alike and each implementation is as unique as the process being monitored and controlled.

Consequently, ONG asset owners must develop and maintain in-house expertise with the highest level of knowledge, skills and experience to support these infrastructures. This requires the investment of time and money to:

- find and hire the individual with the right skill set,
- train OT workers,
- provide hands-on experience under the tutelage of experienced mentors,
- keep employees abreast of technology advances and new threats.

Each OT operator has a set of specific OT systems and employees with deep institutional knowledge of those OT systems. These employees, possessing expert knowledge of OT systems, are in the best position to understand and apply industry standards and process that provide the highest levels of safe, effective, and efficient operation of their OT system.

The complexity and unique attributes of the overall ONG OT infrastructure restricts the ability to provide system specific laws and regulations. The best any such effort may achieve is establishing a minimum set of requirements that may not apply to all ONG infrastructures. For the past decade there has been debate around what constitutes critical infrastructure. If we cannot define what constitutes critical infrastructure, how can we design fully-inclusive, detailed, advanced regulatory requirements to address cybersecurity requirements for these very complex OT systems that government does not understand? Such regulation is not practical, expedient, or possible. The best approach is public-private collaboration that uses best practices and industry standards as the basis for an ongoing assessment and remediation process to secure OT systems.

4 Operational Technology in the Oil and Natural Gas Industry

4.1 General

Operational technology, as applied in this paper, refers to the control systems used in the ONG industries. This section provides a detailed discussion on the various technologies that are found within this industry.

4.2 Operational Technologies

4.2.1 General

Operational Technology (OT), in the ONG industries, is a general term which refers to those systems which monitor and control physical processes. This is separate from the Enterprise or company IT systems, which is "… about automating human activity [versus] … providing information instrumentation for machinery" [122]. For this paper, API defines OT as control systems that included a finer delineation of systems as identified in API's refinement of the overarching OT definition and published literature are in alignment as to what distinct processes are grouped under the general OT definition.

Table 4—Operational Technology Systems

Operational Technology Systems
Industrial Control Systems (ICS),
Production Control Systems[1] (PCS),
Supervisory Control and Data Acquisition Systems (SCADA),
Distributed Control Systems (DCS).

The Department of Homeland Security identifies the various types of OT as "Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), etc. [which] generally refers to systems which control, monitor, and manage the nation's critical infrastructures…" [34]. These systems "…gather key information electronically from field locations… [and] are configured to present field data to the controllers, and may include additional historical, trending, reporting, and alarm management information… [Further,] a controller may take direct action… to operate equipment or the controller may alert and defer action to others" [36].

Control systems have been in use for a hundred years. "Around 1912, the Chicago power industry merged a centrally located control room operator, a remote process control system, [and] a telecommunication interface…" [157] to provide remote monitoring and control functions from a central location. Over time, control systems "… evolved into sophisticated technology enablers which allow operation of virtually every type of process control system. They ensure a steady source of reliable electrical power, a steady supply of natural gas to factories and homes, and enhance liquid pipeline control. Many processes now operate at a level of safety, effectiveness, and efficiency never achieved before" [50].

While various approaches to remote monitoring and control expanded from Chicago's rudimentary approach, the Supervisory Control and Data Acquisition term was not used by the pipeline industry until "… late in the 1960s… These early SCADA systems were developed specifically for each companys' needs and in most cases were

[1] API definition of PCS, other sources, such as DHS, identify this as process control systems.

developed by the company. [A broader] …history of SCADA [is] found in an article on 'Telemetry' in Encyclopedia Britannica…" [108].

These early, company specific control systems can be viewed as technology islands within the overall corporate infrastructure. All data flows and communication paths were within the control system itself. During these early days there was no need for near instantaneous data transfer from the control system to the enterprise or business system. These early systems were also islands unto themselves as predominately the computer language used was proprietary to the firm supplying the system. As an island unto itself, there was a minimal cybersecurity threat to these systems.

Over the last decade or so, these automation islands have almost disappeared. In today's automation world the computer's operating systems are often the same as the enterprise computers. Network communications are based on the same telecommunication standards which drive the internet and the control system is directly linked to the enterprise business network. Today's automation systems have a much higher level of cybersecurity risks than systems of yesterday.

Automation systems, or operational technology systems, come in various forms with key differentiating elements. In the following sections, we provide a general overview of what constitutes each system type and what key elements differentiate it from the others.

4.2.2 Industrial Control Systems

The term industrial control systems (ICS) is used in a variety of ways such as:

> "Industrial control system (ICS) is the term used to identify many types of control systems …" [64]
>
> "…supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC)" [104]

The American National Standards Institute (ANSI) expands the NIST definition to include "…remote terminal units (RTUs), intelligent electronic devices … networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. In this context, industrial control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separated or integrated" [4].

As the rest of this section provides expanded views of PCS, SCADA, DCS and specialty systems, this portion of the ICS discussion is limited to what is often referred to in the industry as field systems (FS). "Field systems can be broken down into two categories, each having one or more safety related features: Local Control Systems and Local Safety Systems" [64].

Local control systems may perform isolated functions with no link to a broader structure or they may be systems that perform local monitoring and control and provide minimal data to other systems. Some of the devices that can be included in the local FS category include:

- *Smart Sensors*--These devices contain embedded logic that allows them to monitor and respond to process changes in an autonomous mode. These systems may also communicate with other FS devices and process control systems.

- *Flow Computers*--These devices convert the raw flow meter data into information such as net and gross flow rates, as well as accumulated volumes.

- *Programmable Logic Controller (PLC)*--PLC's are industrial hardened computers that were originally intended to provide the functionality of complex relay logic without all the relays. These devices have advanced to a point that they provide detailed logic, computational, and decision capabilities as either stand-alone installations or as part of PCS, SCADA, and DCS infrastructures.

Figure 1 is a very simplified example of a smart meter installation. In this case the level sensor monitors the tank fluid level. Based on the level the sensor generates a signal to either open or close the inlet valve. The system operates based on local settings without the need of external data exchange.

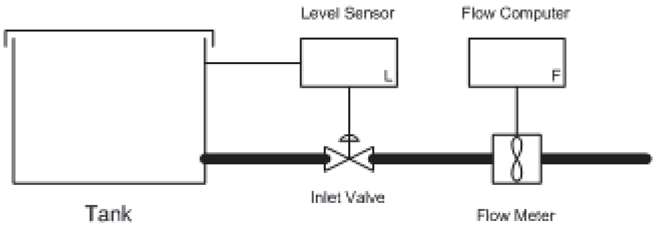


Figure 1—Simplified Smart Transmitter Example

Figure 1 also demonstrates the flow computer interconnection. As shown, the inline flow meter measures the product as it flows through the pipeline. The inline flow meter output is connected to the flow computer, which converts the inline flow meter signal to higher level information such as net and gross flow rates and accumulated volumes. As a stand-alone system these devices have minimal cybersecurity risk.

Figure 2 shows a simplified PLC sketch. In this example the PLC receives data from the level, temperature, and pressure sensors as well as the flow computer. Based on the programmed PLC logic, the PLC will adjust the inlet valve position. The PLC logic capabilities expand the functions that can be performed locally.

As with the basic smart sensor, the PLC can operate in an autonomous mode without interaction or data exchange to higher level systems.

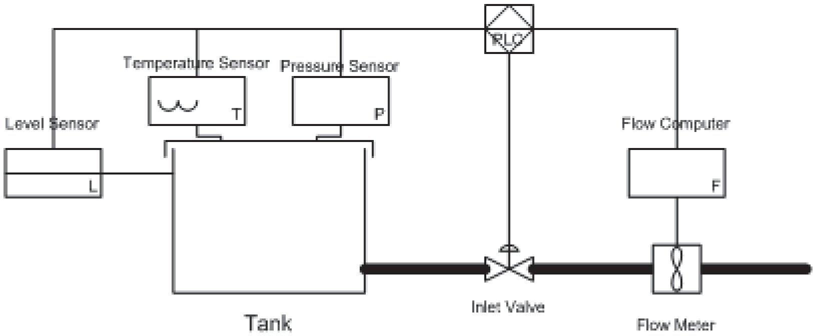


Figure 2—Simplified PLC Example

As a standalone system, the PLC has a lower level of cybersecurity risk. With no external communication interface, modification to the PLC requires someone to physically access it. This reduces the systems overall risk map.

4.2.3 Process Control Systems

Process Control Systems (PCS) are systems that expand the area of monitoring and control beyond the local device or process to include the broader process infrastructure. For this paper and in alignment with published literature PCSs are defined as:

> "... systems which respond to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL >=1" [69].
>
> "Process control refers to the methods that are used to control process variables when manufacturing a product" [111].

Historically "The term automatic process control came into wide use when people learned to adapt automatic regulatory procedures to manufacture products or process material more efficiently. Such procedures are called automatic because no human (manual) intervention is required to regulate them" [70].

A key difference between PCS and distributed controls or supervisory control and data acquisition are the geographic locations where the systems reside. PCS are generally associated with a specific process within a plant, refinery, etc. while distributed controls or supervisory controls typically refer to systems where the various sites are geographically separated.

Figure 3 provides a general view of a type of PCS. In this case the process is to correctly mix two fluids in correct proportions. The process sensor receives the desired process setpoint, which may be set locally or from a remote location. The sensor compares the output of the mixing valve to the desired setpoint. Depending on the results of that comparison the process sensor will signal the inflow control valves to increase or decrease flow.

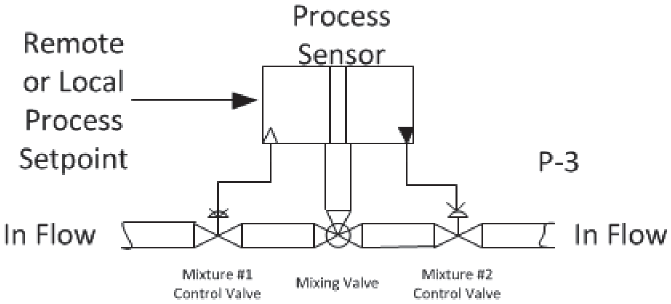


Figure 3—Process Control System Example

With the exception of establishing the desired process setpoint all other actions are automatic.

4.2.4 SCADA Systems

Historically, computer based Supervisory Control and Data Acquisition (SCADA) systems origins can be traced to the 1960s. As an example, Office of the Manager National Communications Systems discusses how "…SCADA systems have evolved since being deployed in the 1960s" [102]. Yet, what is the basic definition and general architecture of a SCADA system?

To answer these questions, a literature review was conducted to identify how SCADA is defined by various standards and governmental organizations. The results of this literature review identify a fairly consistent definition theme across industrial organizations and government entities. The following are representative examples of definitions obtained:

> "A SCADA system is highly distributed. It is specifically designed to address long distance communication challenges… [and] enables the centralized control and data acquisition required for monitoring the remote assets over long-distance…" [64]

> "SCADA systems…are used to monitor critical infrastructure systems and provide early warning of potential disaster situations" [102]
>
> "SCADA (supervisory control and data acquisition) generally refers to industrial control systems: computer systems that monitor and control industrial, infrastructure…" [59]
>
> "SCADA… systems are a type of industrial control system used to collect data and exercise control from a remote location" [108]
>
> "[SCADA], a computer based system in which the Data Acquisition function includes gathering real-time data through a communication network and control functions include controlling field devices" [6]
>
> [SCADA], A combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling" [7]

Leveraging the various definitions and design standards, such as API 1113, functions of a SCADA system include the following.

1. Provide a graphical user interface that allows the controller or operator the ability to graphically see the system information and to initiate field device changes.

2. Monitor remote processes/systems/devices for changes in physical state. These include, but are not limited to, such items as valve positions, motor running state, pump running status, pressures, flow rates, temperatures, circuit breaker status, etc.

3. Control remote devices such as valve control, pump control, changing pressure setpoints, changing relief valve setpoints, etc.

4. Central monitoring and control location is remote from the devices that are being monitored and controlled.

5. A communication infrastructure is required to link the central location to the remote devices.

6. Primary intelligence functions reside at the central location within the master computer.

7. System control through pre-established automated logic functions and user initiated actions.

8. Provide field data and information to enterprise applications.

9. Provide field data and information to specialty systems as described in 2.1.5.

To achieve these functions a SCADA system interconnects many subcomponents which include the following:

- *Human machine interface* (HMI)—This is a software application that presents information and data to the user in a combination of forms such as graphically, numerically, tabular, etc. The application also provides the user the ability to initiate actions, acknowledge events, etc. Literally this is the area where technology and the human meet. API defines HMI as "A computer terminal normally associated with a graphics terminal that allows interaction between people and devices" [7]

- *Master Station*—IEEE describes the "Modern… (SCADA) master stations [as having] both software and hardware in a distributed architecture. The processing power is distributed among various computers and servers that communicate with each other through a real-time dedicated LAN [local area network] in the control center" [59]. Master stations are often co-located with the supervisory control center and the backup supervisory control center in a redundant configuration. The control centers are where the central monitoring and control of the overall process occurs.

— *Telecommunications infrastructure*—This infrastructure provides the electronic link between the central control center and all remote locations. The connectivity can use a wide area network (WAN), dedicated leased data lines, as well as microwave, fiber optic, or satellite based telecommunication systems. SCADA system components are physically separated and required interconnection through some telecommunications infrastructure.

Telecommunication infrastructure is sometimes referred to as a 'process control network.' API defines a process control network as "A network used to transmit instructions and data between control and measurement units and SCADA systems" (1164, June 2009).

— *Remote data terminal units/data concentrators*—Remote site data terminal units/data concentrators come in many forms such as the 'dumb' remote terminal unit (RTUs), programmable logic controllers (PLCs), field data acquisition (FDA) servers, and/or Flow Computers (FC).

RTUs generally provide no local intelligence or logic capabilities. These devices serve the function of monitoring the various field device electrical inputs; such as the binary states of on/off, open/closed, or the voltage or current analog value and on request from the master control center send the field device information back. Often an RTU based SCADA system is called a master/slave system. The central control system is the master while the RTUs are the slave. All logic is performed at the master and the slave responds to the master's commands.

RTUs are "A remote device typically used to gather status, alarms and analog remote readings for transmission to the SCADA system and transfer controls from the SCADA system to a field device" [7].

As SCADA systems matured, remote devices were deployed that started to included intelligence and logic capabilities that replaced basic relay logic functions. These intelligent devices are PLCs. PLCs are capable of providing local decision and logic functions as they contain industrial hardened central processing units (CPUs), memory and a software operating system.

The combination of a CPU, memory, operating system, and application software provides the capability to program the PLC to perform functions beyond just converting the field electrical signal to a communication data stream, which is sent back to the master. One definition of a PLC is "A digital computer used for automation of industrial processes" [7].

Field data acquisition (FDA) unit's primary purpose is to gather all assigned field data into a common device with no human interaction. The acquired data is transmitted to the central control computer either on request or on an exception basis.

Flow computers (FC) are the hardware/software system that implements the required algorithms that convert the flow meter electrical signal to a flow reading, which is usable by the central control computer. The algorithm provides the ability to receive pressure and temperature compensated flow values or non-compensated flow values.

To integrate the various infrastructure subcomponents, a wide variety of configurations have been developed and deployed. The configurations span the range from simple, non-redundant, infrastructures to highly available, fully redundant structures.

As an example, Figure 4 is a simple network view of a non-redundant SCADA system. In this configuration the SCADA Host/Master (Master here forward) computer is collocated with the Operations Control Center (OCC). There is a single computer which connects to the HMI and ancillary devices over a single local area network (LAN). The SCADA Master computer is linked to the field systems over another single telecommunications link.

Finally, the SCADA Master can also be connected to the corporate enterprise through a single demilitarized zone (DMZ) and associated infrastructure. Figure 4's depiction of how the SCADA system interfaces with the corporate enterprise systems is highly dependent on the organization and their unique needs and operating requirements. The depicted DMZ is consistent with API 1164's recommended approach [7].

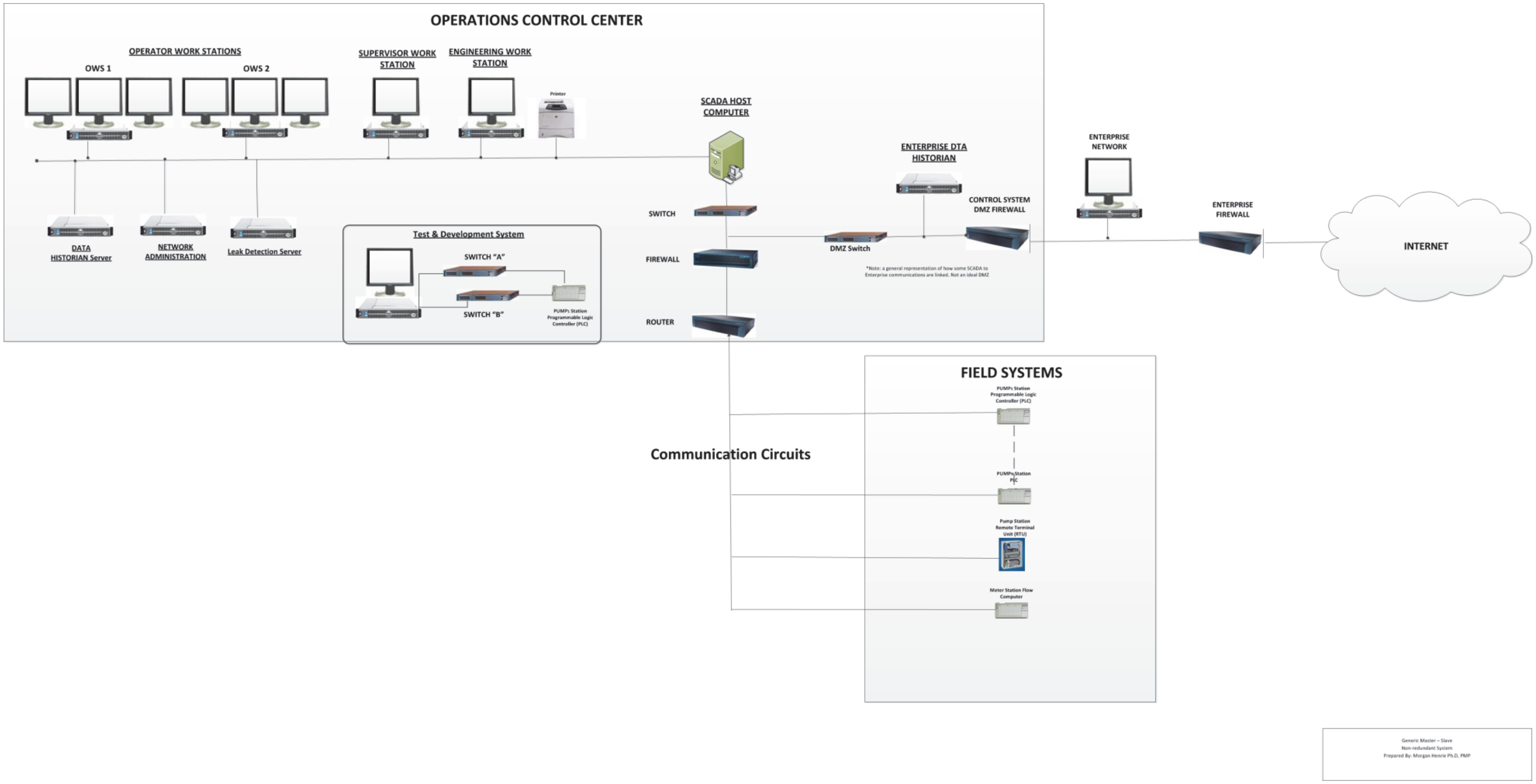

OPERATIONS CONTROL CENTER
OPERATOR WORK STATIONS
OWS 1
OWS 2
SUPERVISOR WORK STATION
ENGINEERING WORK STATION
Printer
SCADA HOST COMPUTER
DATA HISTORIAN Server
NETWORK ADMINISTRATION
Leak Detection Server
Test & Development System
SWITCH "A"
SWITCH "B"
PUMPs Station Programmable Logic Controller (PLC)
SWITCH
FIREWALL
ROUTER
ENTERPRISE DTA HISTORIAN
DMZ Switch
CONTROL SYSTEM DMZ FIREWALL
*Note: a general representation of how some SCADA to Enterprise communications are linked. Not an ideal DMZ
ENTERPRISE NETWORK
ENTERPRISE FIREWALL
INTERNET
Communication Circuits
FIELD SYSTEMS
PUMPs Station Programmable Logic Controller (PLC)
PUMPn Station PLC
Pump Station Remote Terminal Unit (RTU)
Meter Station Flow Computer
Generic Master – Slave
Non-redundant System
Prepared By: Morgan Henrie Ph.D, PMP

Figure 4—Non-Redundant SCADA System

Non-redundant SCADA systems tend to have lower levels of system availability where availability is generally defined "…as the ratio of uptime to total time (uptime + downtime). It is customary to express availability in percentage…" [59].

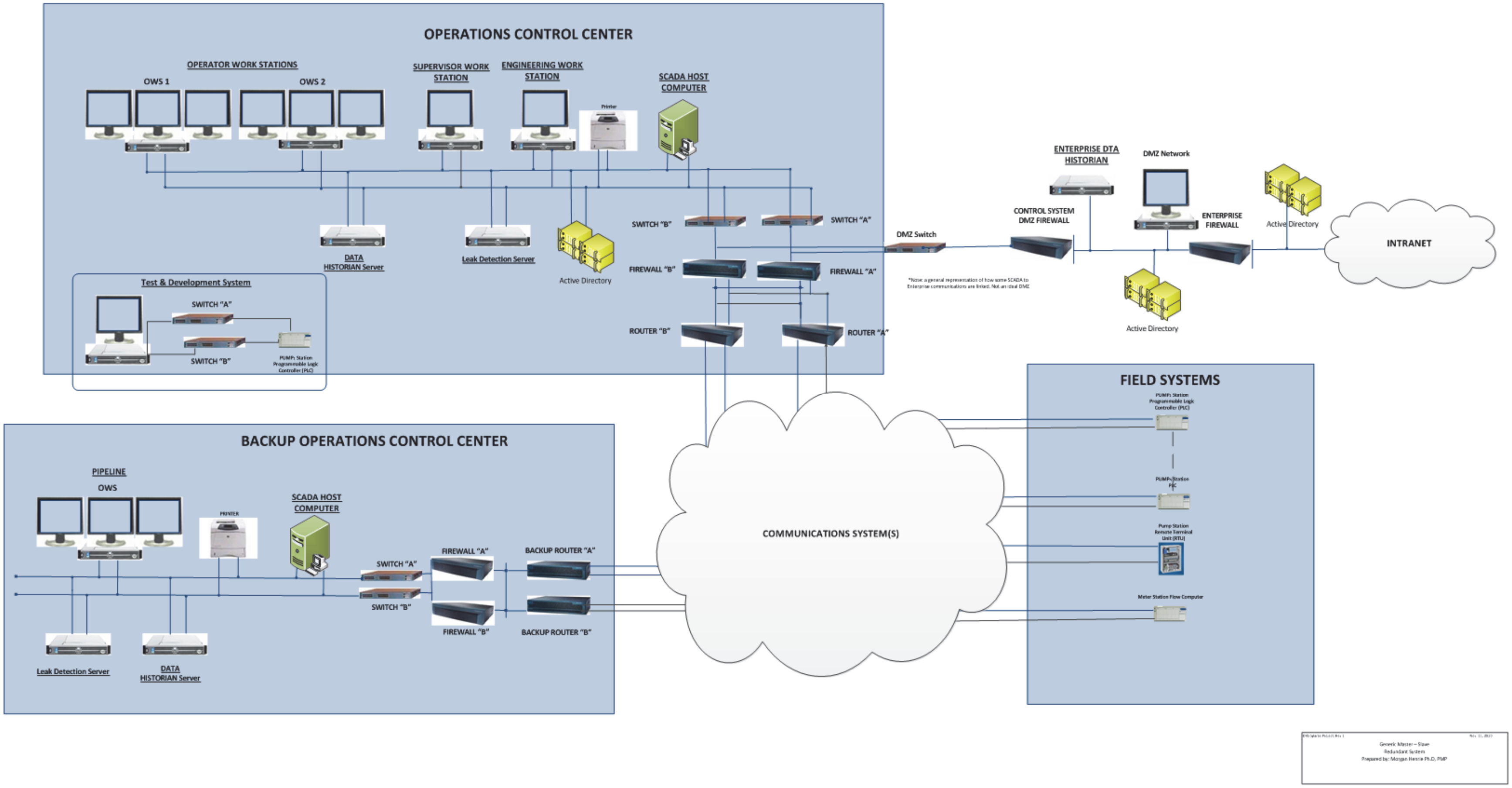
The lower availability percentages occur due to the increased levels of downtime due to system outages of one type or another. In a non-redundant configuration, any key device failure results in downtime. This is not the same in a fully redundant network, which is discussed next.

Figure 5 provides a general view of a redundant SCADA system. In this system there are redundant:

- central control center LANS,
- telecommunication circuits,
- firewalls,
- routers,
- human machine interface (HMI) displays,
- remote field devices,
- redundant operation control centers.

As a redundant infrastructure, the loss of any one device does not result in a system outage. In many cases the infrastructure can experience multiple device interruptions without impacting operations.

In summary, SCADA systems are structures that allow a central control center the ability to monitor and control remote processes. They rely on a central host computer to provide the interface between the user's HMI and all associated field devices.



*Note: a general representation of how some SCADA to Enterprise communications are linked. Not an ideal DMZ

Figure 5—Redundant SCADA System

4.2.5 Distributed Control Systems

On a cursory look, a distributed control system and a supervisory control and data acquisition (SCADA) system appear very similar. Shaw identifies how “Architecturally, a DCS very much resembles a SCADA system…” [129]. They both involve intelligent devices, telecommunication infrastructures, and field devices. Yet, the two systems are distinctly different approaches on how the organization monitors and controls the process be it a pipeline, refinery, etc. This section highlights some historical back ground and what key elements define a distributed control system (DCS).

From a historical review, computer based DCS systems are traced to around 1975 and early 1980s. It was in this era that critical elements that support computer based DCS began to mature. These include digital communications between devices, application of networks within the process control environment, vendors providing commercial off-the-shelf components, various industry standards, and owner/operators adoption of this technique.

The early DCS adoption appears to be within the local plant where networks were established by hardwired interconnections. As the technologies matured DCS systems started to expand beyond the plant floor to providing distributed control over wide area networks that linked remote sites to each other and to the control center. Today, DCSs are found throughout the industry providing distributed control across a range of processes. This expansion is fueled by further maturing of industry, national and international standards, technology advances, vendors responding to the owner/operators’ needs.

Yet, as the application and use of DCSs continue to expand, what defines a DCS since, as the literature identifies DCSs and SCADA systems tend to resemble each other?

To provide an answer to this question, a literature review was conducted to identify how DCSs are defined and what common themes constitutes a DCS. The following definitions provide a general view of how DCSs’ are defined within academic and organizational standards bodies.

> “Distributed Control System… a system consisting of several intelligent devices cooperating for common purpose. Intelligent devices… support processes, which coordinate activities and information exchange via a communication network.” [53]

> “Distributed computer system – A system that involves multiple computers, possibly remote from each other, that each has a role in computation problem or information processing.” [6]

These definitions provide the key to what differentiates DCS from SCADA and the other OT systems. Specifically, a DCS system includes (a) multiple computers, (b) autonomous process monitoring and control at the local site, (c) inter-site automated data exchange, and (d) inter-site coordination of activities. DCS systems also utilizes common OT requirements of a telecommunication infrastructure and human-machine interfaces (HMI).

Figure 6 depicts what DCS system architecture could look like when implemented. As shown, the figure demonstrates how a DCS server/computer is found at all sites, item (a). Often these servers are found in redundant configurations so if one fails the other, redundant local server automatically takes over. This dramatically increases the overall system availability.

An essential element of the DCS infrastructure is each site’s ability to monitor local activities and initiate control functions, item (b). This autonomous capability provides the system with faster response to local activities as well as minimizes the telecommunication interactions and control center work load as well.

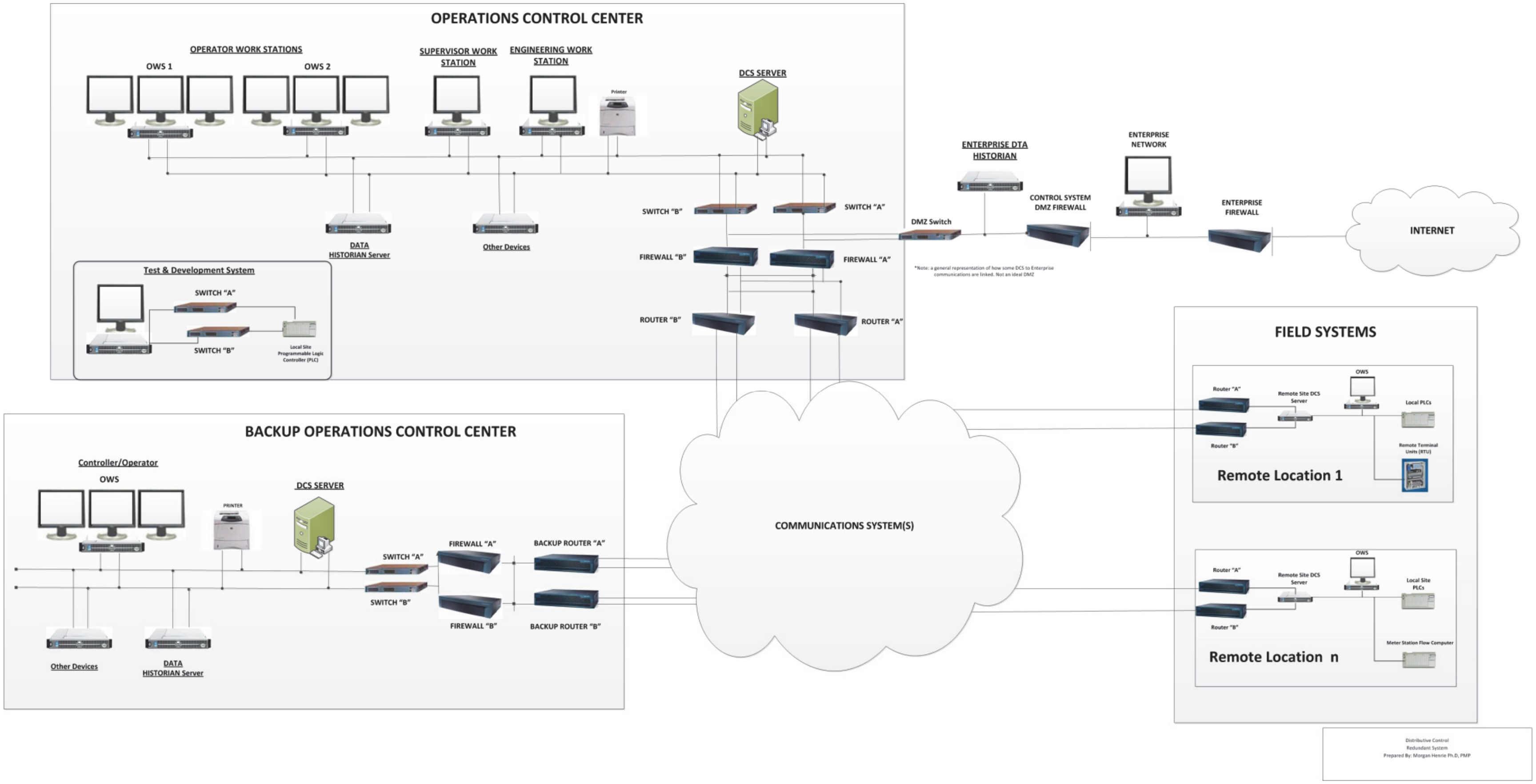


Figure 6—Redundant Distributed Control Diagram – General Architecture

As we see from the National Transportation Safety Board, “Some systems have a distributed control system so that if the main control system fails, remote sites can monitor the whole system” [108].

Another feature of the system is the ability of each location to share information with the other sites without the need of a central data processing center, item (c). This inter-site communication and data sharing extends the overall system’s capability for automatic process control to inter-site coordination and control of the broader system.

As with SCADA systems, the telecommunication infrastructure connects all systems together. To ensure the highest level of system availability requires physical and even technology divergent telecommunication systems. As an example, one network could be on a local telephone system high speed data network while a second path could be a satellite or microwave system.

In summary, DCS system extends the overall control system’s monitoring and control to the remote sites. In this configuration, the remote sites DCS server/computer operates in an autonomous mode for specific established conditions. It also provides data and information to other sites to provide an interconnected infrastructure of intelligent devices. If properly designed and implemented, it provides a very fast, highly available control system.

> “Distributed systems have many advantages over centralized systems. Since the data processing is shared on the network, the various servers require less processing power than in a centralized system. In this way, the cost of computers can be reduced. It is also easier to upgrade or to add servers if additional processing power is required. Another advantage of distributed systems is that the failure of one server does not necessarily affect the whole system.” [59]

4.2.6 Specialty Systems

Speciality systems, such as the Safety Instrument Systems (SIS) or Emergency Shutdown Systems (ESD), fall outside of the previous sections definitions.

> “Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industry.” [58]

By definition a SIS is

> “implementation of one or more safety instrumented functions [which are]…composed of any combination of sensor(s), logic solver(s), and final elements(s).” [69]

SIS systems should be independent of any other OT application. In an ideal SIS implementation, the communications and software structures are independent of OT systems. Therefore, a compromise of other OT systems should not compromise the SIS.

In the literature, SIS and emergency shutdown systems are often used as interchangeable terms such as by ANSI where they state “Other common terms used for emergency shutdown systems include safety instrumented systems…” [5]. For the purpose of this document we take the position that SIS and ESD are the same systems and refer to them collectively as SIS.

Figure 7 is a simplified view of how an SIS may be configured. In this example, various sensors monitor the process. These sensors provide data to the SIS. If the SIS determines that the process is approaching or outside established limits it initiates changes to the control valve designed to return the system to a safe state.

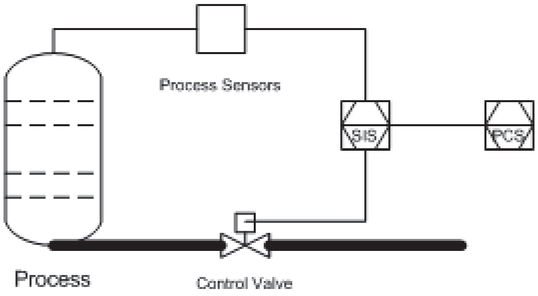


Figure 7—Simplified SIS Example

Figure 7 also shows a communication link between the SIS and a local PCS. The interconnection with other systems, such as PCS, SCADA, or DCS, is one of discussion within the literature. One ESD definition states that the "…emergency shutdown systems (ESD)… run independently from their control systems. The ESD system … [is designed] to return the facility to a safe state in the event of adverse operating conditions" [64]. On the other hand, designs that have the SIS sending the other systems data and information do occur as well.

The SIS cybersecurity risk profile is different if it is implemented as a standalone system or a system with connections to other control system infrastructures. A standalone system's cybersecurity risk is lower than the interconnected infrastructure since to make changes requires someone to physically access the device. Conversely, if the SIS is linked to other networks its cybersecurity risk map increases as it now becomes possible to make SIS application changes remotely.

4.2.7 Enterprise Cybersecurity

The need for enterprise cybersecurity predates OT cybersecurity by many years. The origins for both enterprise and OT cybersecurity are traced to 1949 when "Hungarian scientist John von Neumann (1903 – 1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their 'memory'" [79]. Yet, it isn't until 1979 that "Engineers at Xerox Palo Alto Research Center discover the computer "worm," a short program that scours a network for idle processors. Designed to provide more efficient computer use, the worm is the ancestor of modern worms--destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted" [79]. In a parallel effort, the internet and its inherent lack of security was coming of age.

In 1962, J.C.R Licklider and W. Clark, of MIT, present a paper on "On-Line Man Computer Communications." In 1968, an ARPANET request for quotes is issued to develop host level protocols for communications over ARPANET. By 1971, there are fifteen nodes connected to ARPANET. The first international connection occurs in 1973; while in 1980, ARPANET comes to a complete halt because of an accidently propagated status message virus.

By 1987, there are over 10,000 host computers on the internet. In 1988, an internet worm infected about 6,000 out to the 60,000 host computers [154]. This worm demonstrates how the internet was "… designed for openness and flexibility, not for security" [37]. The parallel activities of internet and virus development, as well as events such as, "Kevin Mitnick [committing] the largest computer-related crime in the U.S. history [which resulted in…a] loss of eighty million dollars in U. S. intellectual property and source code" [29] set the stage for addressing enterprise cybersecurity.

An outcome of these efforts is development of cybersecurity methodologies, methods, and tools; such as the first antivirus software in the 1980s, and cybersecurity standards. The overall enterprise cybersecurity system objective is to ensure that "… systems remain dependable in the face of malice, error, or mischance" [3].

Implications of Enterprise Security on Operational Technology

Enterprise, holistic system-based cybersecurity predates OT cybersecurity methodologies. Enterprise system owners and operators were driven to addressing the issue earlier as they were connected to the internet and their systems were relying on common operating systems and protocols. Conversely OT infrastructures, as discussed earlier, experienced a historical view of inherent security through network isolation, vendor specific protocols, and cultural view of 'why would anyone want to attack a control system?'

As OT infrastructures emerged from their islands of obscurity they evolved into systems that utilized many of the enterprise based operating systems and protocols. The technological convergence of these infrastructures didn't lesson the enterprise risks and vulnerabilities, but it did significantly raise OT's risk quotient as the vulnerability base was dramatically raised. This increase in cyber risk is demonstrated by the number of documented OT cybersecurity incidents in Figure 8.

This figure clearly shows a marked increase in events in just over a decade. This time frame matches with the convergence of enterprise and OT hardware, operating systems, and network protocols.

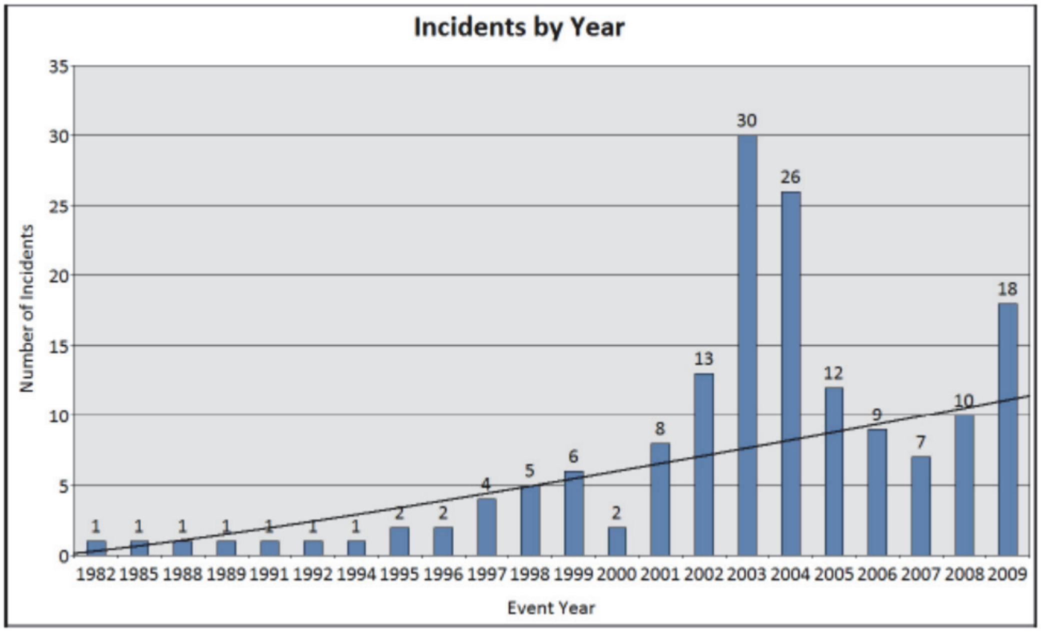


Figure 8—Number of Industrial Cybersecurity Incidents (Tudor & Fabro, 2012)

"These technologies provided features and services such as remote monitoring, remote management, intra-system coordination, inter-system communication and self-orchestration. Unfortunately, critical infrastructure assets are susceptible to a large number of [Information and Communications Technologies] ICT attacks" [39].

As OT cybersecurity needs started to increase, it was consistent to leverage the knowledge, tools, skills, methodologies, and methods that already existed in the enterprise world. A significant driver to early adoption of enterprise practices was the fact that the enterprise systems were already grappling with cyber events and the OT infrastructure, up to this time, had remained largely immune from these threats. As such, enterprise cyber capabilities were more advanced. As an example, the enterprise side of the house started to develop and deploy communities of practice such as the Information Security Forum (1990s) and standards such as IEC 27003 (1995) much earlier than comparable OT systems. The OT organizations didn't release comparable standards, such as the first edition of API 1164 until September 2004 and the American Gas Association (AGA) did not release AGA Report No. 12 series (AGA Report 12) until 2004. AGA Report 12 is intended "… to save

SCADA operators time and effort for recommending a comprehensive system designed specifically to protect SCADA Communications” [1].

Based on the sequence of events and evolution of OT infrastructures it is understandable why the majority of OT cybersecurity oversight and tools have origins within the organizations IT department.

While leveraging these established IT resources does increase the overall OT cybersecurity posture, there is a counter view that just applying an IT approach to a critical infrastructure OT environment is insufficient to achieve optimum OT cybersecurity. As an example, Favion et al. state, “Due to the peculiarities of industrial systems, ICT countermeasures cannot be deployed efficiently in all environments” [39]. Further, an exclusive IT protection system applied to OT infrastructure view is one of “… protection being put into place for SCADA systems… in the form of building a security perimeter… This denotes an outward-looking siege mentality. The problem is that the most dangerous (although admittedly least frequent) threats come from the trusted insiders…” [129].

OT “… cybersecurity must be regarded holistically if real-world security is to be improved” [44]. The holistic approach must take into consideration the operational context and uniqueness of the environment. Based on these foundations the appropriate mixture of IT and OT cybersecurity methodologies, methods, tools, skills and standards can be developed. The view should be a holistic OT contextual view, not a siege mentality. Further research is needed in this area to make the next OT cybersecurity advances.

4.2.8 Operational Technology—Enterprise Interface

As noted previously, early day OT systems were isolated with no direct interface with the organization’s enterprise or business systems. As competition expanded globally and communications become nearly instantaneous an organization’s need for time critical information became essential. This combination of events became the genesis of providing a direct communication connection between OT and enterprise systems.

This linking of OT and enterprise, aka information technology (IT), systems extended the enterprise level cybersecurity risk to the OT infrastructure. As an example, TSA identifies:

> “The control systems used by operators to manage their infrastructure and products are vital to the pipeline’s safe and efficient operation. The growing convergence of information technology (IT) and control systems brings with it increased capabilities, but also increased exposure to cyber attacks against the infrastructure” [41].

As it becomes advantageous, industry has used a variety of methods to link OT and IT systems together. Figure 9 through Figure 13 provide examples of how interconnections can be made.

Figure 10 through Figure 12 are examples within API 1164. These views also show varying levels of cybersecurity risk reductions. Figure 10 is the simplest approach and one that the highest cybersecurity risk. Figure 10 has minimal protection, which is supplied by the internet firewall. In this example there is nothing to restrict or prevent an action on the internet from impacting the control system.

Figure 12 provides a higher level of risk reduction as a demilitarized zone (DMZ) is provided as well as the corporate to internet firewall. The DMZ is a shared location where the enterprise and control system servers can exchange data. The DMZ must be configured to prevent any direct connection from the enterprise to/from the control system.

Figure 13 enhances the cybersecurity risk reduction much higher. Not only does this approach include all of the previous examples positive benefits it also includes different manufacturer firewalls linked in a back to back fashion. Installing firewalls in this configuration requires any hacker to have a much higher skill set and knowledge base if they are to be successful in hacking different manufacturer firewalls. This configuration also provides for redundant firewalls and communication networks.

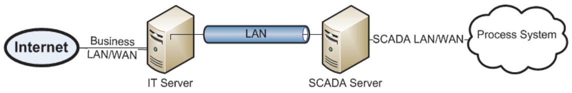


Figure 9—Simple OT to IT Connection

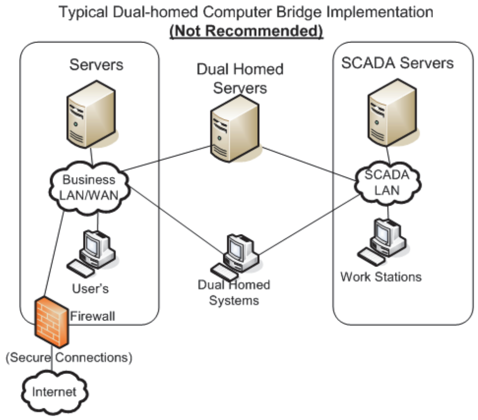


Figure 10—Typical Dual-homed Computer (API 1164)

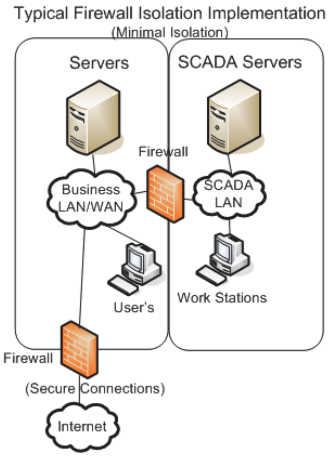


Figure 11—Typical Demilitarized Zone (DMZ) Implementation (API 1164)

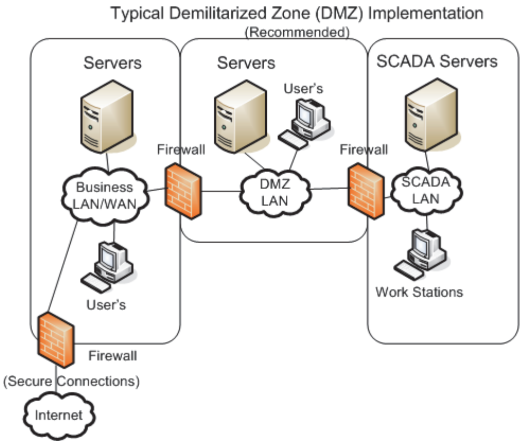


Figure 12—Firewall Implementation (API 1164)

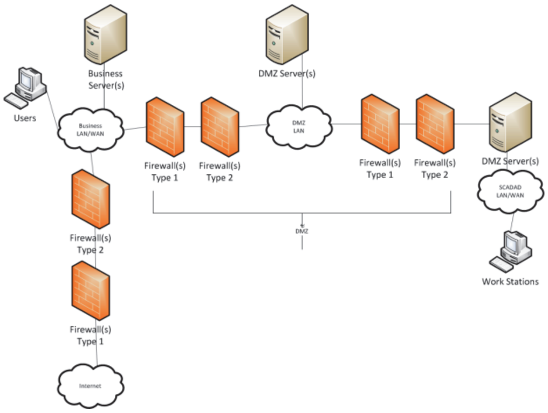


Figure 13—Redundant Demilitarized Zone (DMZ)

4.3 Current State of Operational Technology Security

4.3.1 General

This section provides a summary view of the current state of operational technology security within the ONG industry. It is important to note that all ONG sectors use various combinations of all technology types. Organizations and vendors work together to specify architectures that benefit operations and efficiency. Asset owners vary in their usage of systems based on individual needs.

The data, information, and findings identified here are derived from industry workshops the investigators have lead over the past 5 years, industry surveys, interviews and various literature sources.

The industry continues to advance its focus on OT cybersecurity. The revision of API 1164 [7] and the release of INGAA's control system cybersecurity guideline [64] are just two examples of how the industry continues to focus on these issues.

A study conducted in 2010 (see Annex A) by the Center for Strategic and International Studies called "In the Dark: Crucial Industries Confront Cyberattacks" states that 80% of 200 "IT" executives at utilities, oil, gas, and water companies responded that they had experienced large scale denial of service attacks [35]. This study is cited countlessly in articles on cybersecurity for critical infrastructure, and is often referred to as definitive, illustrating the lack of critical infrastructure survey data. The study, however, includes international respondents.

4.3.2 Variance within Sub-Industries

Cybersecurity challenges facing ONG sub-industries discussed briefly above share more commonalities than variances. Each of these sub-industries shares:

- requirement to monitor the process,
- requirement to obtain data for organizational needs,
- requirement to control the process using OT,
- "IT is now heavily involved in the operations…" [73],
- remote monitoring and control requirements,
- telecommunication requirements,
- need to have 100% availability,
- need for data integrity,
- need for confidentiality.

In looking across the ONG sub-industries it is clear that overall the challenges appear to be consistent where a set of universal issues and concerns exist. Within the industry it is clear that "Understanding this particular vulnerability [OT cybersecurity] and what it means requires some background on how process control systems have developed and evolve. Addressing the security of those systems is a very small community of government, industry, and academic entities whose work is but a small niche in the rapidly growing area of information security" [73]. While ONG industry specific knowledge base is expanding there exists a limited population of individuals who understand the operational, technology, and risk context of ONG industry's OT cybersecurity.

Variance among the sub-industries illustrates the challenge of implementing cybersecurity and the need for different and flexible solutions. The complexity of systems, technology implementation, criticality of product and consumer, all factor in to the risk equation (discussed in Section 3). Mitigating these risks require different approaches to cybersecurity to ensure operational continuity.

4.3.3 Offshore Platforms

Offshore Platforms are complex ‘man made’ islands that support exploration and production. Offshore ONG exploration and productions is classified as activities that occur upstream of oil refineries, gas sale pipeline transfer points, and transportation pipelines. In general, this industry sub-group explores, develops, and extracts petroleum products from offshore areas. To safely, efficiently, and effectively fulfill the upstream requirement involves OT where operation’s personnel monitor and control the overall process.

“Offshore means beyond the line of ordinary low water along that portion of the coast of the United States that is in direct contact with the open seas and beyond the line marking the seaward limit of inland waters” [22].

Offshore platform uniqueness involves remote locations, access means, and challenges associated with transporting the produced petroleum to the oil refineries or gas sale pipeline transfer points. To this ONG sub-industry group, everything is remote and operational requirements are very unique. As an example, how the offshore platform operations respond to a hurricane is different than how an onshore transportation pipeline would respond. In each situation the organization has different methods, policies, and processes in place to ensure workers safety, production facility integrity, and protection of the environment.

From a cybersecurity perspective, the delays in data flows due to isolated and periodic communications to shore, complicates the ability for situational awareness. Likewise, there is little physical access control to core systems once on the platform. Therefore layered security must be employed that includes data security, human-system interaction, and processing a variety of inputs for situational awareness. Emphasis on physical and personnel security adds to overall cybersecurity.

4.3.4 Onshore Exploration and Production (E&P)

Onshore exploration and production (Onshore E&P) is classified as onshore activities that occur upstream of oil refineries, gas sale pipeline transfer points, and transportation pipelines. In general, this industry sub-group explores, develops, and extracts petroleum products from onshore areas. To safely, efficiently, and effectively fulfill the upstream requirement involves OT where operation’s personnel monitor and control the overall process.

The digital oil field is fast becoming a technologically advanced, common theme in the ONG industry. As systems become interconnected for optimization and remote access, the role of cybersecurity will increase. Remote monitoring of drilling sites and wells is a new and rapidly advancing area in onshore E&P. The geographic disparity and often unmanned operations is a perfect application for advanced technology to facilitate operations. As trends indicated, and like other aspects of the industry, cybersecurity is expected to increase in this area.

As API’s Events & Training web site identifies “Most studies show that 80% of industry training requirements overlap by 80%” [68]. While no direct industry based operational technology comparison was identified experience indicates that a similar or higher overlap exists across the various ONG sub-industries use of OT and cybersecurity concerns. As but one example of support for the direct observation Karen Boman identifies that “U.S. oil and gas companies have become more vulnerable to cyberattacks as information technology (IT) is now heavily used in energy production, processing and distribution operations…” [13].

Onshore E&P focused organizations are collaboratively working to enhance the industry segment cybersecurity posture. As an example the Special Meritorious Awards for Engineering Innovation is soliciting proposals for its 2013 contest specific to systems integration cybersecurity [65].

4.3.5 Pipelines

ONG pipelines sub-industry group involves a diverse set of pipeline types as defined and described in 49 *Code of Federal Regulations* (*CFR*) Part 195. Organizations which own, operate, and maintain ONG pipelines are part of the midstream sector classification. The general physical boundaries of this sub-industry start at the production and gathering system termination and ends at the refinery or selling and distribution facilities.

Pipelines involve long distances and traverse virtually every conceivable environment. The physical infrastructure is located above ground, below ground and below bodies of water. All pipelines require at least one initial pump station or compressing facility which provides the work that moves the raw product from the pipeline inlet to the ultimate termination. Frequently; depending on hydraulic factors (e.g. geographical constraints, distances, etc.), pipelines require more than one pump station or compressor station along its length and ends at the refinery, distribution facility or terminal.

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

Pipeline threat vectors are also unique as:

- the physical infrastructure covers long distances,
- virtually no physical means to monitor the entire system on a 24×7×365 basis exists,
- third party access to the infrastructure is common,
- wireless telecommunications is very common, and
- physical infrastructure frequently transverses unique geographic areas.

Pipelines, as a midstream classified activity, will impact both upstream and downstream activities if the pipeline system is shutdown. The potential for wide spread cascading negative impacts due to a pipeline incident increases this sub-industry overall risk factor.

Cybersecurity of pipeline operations is particularly critical given the inability to physically secure or man miles of pipe. Data integrity ensures situational awareness and facilitates seamless, optimal operations. Advanced OT in pipelines often includes significant cybersecurity.

4.3.6 Oil Refineries

The ONG sub-industry group of oil refineries is classified as part of the downstream sector. Overall, the downstream sector term refers to the functions which occur at the conclusion of production and gathering systems which are included in the offshore and onshore E&P as well as the midstream pipelines.

Refineries are a unique ONG sub-industry in that system monitoring and process control generally occurs from a local, versus remote, location. All operations are usually contained within a restricted physical area. As such, the need for long distance telecommunication infrastructures is usually not required and access to the various process areas does not require personnel to travel long distances. From a descriptive perspective refinery OT systems tend to be PCS, PLC, and SIS rather than SCADA or long distance computer/server based DCSs. The local process telecommunication requirements also tends to be owned, operated, and maintained by the refinery rather than telecommunications obtained from a third party supplier such as the local telephone company or satellite telecommunication supplier.

Refineries receive the crude oil from the distribution pipelines and transfer the produced commodities to the selling and distributed by over the road tankers, railroad tankers, and distribution pipelines.

Cybersecurity in refineries can be easier to manage given the defined boundary and ease of situational awareness in a contained area. However, refineries make attractive targets and face physical security challenges with rail movement, lack of controlled airspace, and geographic location.

5 Risk Management Techniques

Although the science of risk and risk management has existed for centuries, in the ONG industry risk was typically considered in safety science, loss of product or downtime, or risks of noncompliance. Increased interconnectedness in recent decades has elevated the inclusion of cyber risk management into the ONG industry operations. The expansion and inclusion of cyber risk management is demonstrated as TSA's *Pipeline Security Guidelines* with "The intent of … [bringing] a risk-based approach of security measures throughout the pipeline industry," [141]. It is also an approach that many in the critical infrastructure realm agree with as "We and everyone else think that risk-based approach to cybersecurity is the right way to go' said Miles Keogh, NARUC Director of Grants and Research" [97]

Historically, cyber risks were difficult to identify and mitigate, given the rapidly evolving threat technology. Like most risk managers, the natural inclination in assessing risk begins with quantification and metrics. "A metric is a standard of measurement. The goal... is to quantify data to facilitate insight … [and] good metrics lead to good decision and bad metrics lead to bad decisions" [14]. Standard metrics also provide the industry the ability to evaluate how their systems compare with others.

Establishing definitive, quantifiable metrics is an ideal state and one that has received extensive research [10, 14]. However the cybersecurity research shows diametrically opposed views. On the one hand, there is a great deal of research which disproves the existence of valid technical metrics [140] and "Cybersecurity is a quality that has long resisted – and continues to resist-precise numerical classifications" [44]. On the other end of the spectrum, there is research that provides identification of specific metrics, the assessment method and process to use in establishing control system specific metrics [146].

While research and analysis on OT cybersecurity metrics continues to be an active effort, as demonstrated by ISA99 Committee efforts [71], at this point in time the information identifies that an asset owner simply cannot quantitatively state that they are 75% secure against cyber threats. Instead, the industry must view cyber risks within the standard risk equation, Equation (1). The standard risk equation reduces this problem into elements that an asset owner can define and identify based on their own set of operations and OT architecture.

Operations are critical to the continuity of business. This continuity is a motivating factor, along with safety, in mitigating risks. Elements of risk must be defined and considered in terms of business continuity.

$$Risk(f) = (T)Threat \times (V)Vulnerability \times C(Consequence) \tag{1}$$

A threat implies that an individual or group has the ability and access to carry out a process that creates damage to, or exploits a system for a specific gain. Vulnerability is a weakness that exists in a system, network, application, or process that can be exploited by a threat to create an adverse effect. A consequence is the resulting loss, damage, or impact resulting from a threat successfully exploiting vulnerability. The results of a successful exploit can have physical, economic, environmental, and human consequences [92]. It is important to recognize that vulnerability is the only element of risk controllable by the ONG industry. Without the ability to eliminate the threat, an asset owner can characterize and identify potential threats, but ultimately must live with the existence of a threat. Reducing or eliminating vulnerabilities, and thereby minimizing potential consequences, is the best option for mitigating overall risk.

Many asset owners assemble a team within the organization or hire consultants to assist in the risk management process. Locating and assessing vulnerabilities in both the technology and operational processes is critical to mitigating the overall risk. In the past decade assets owners have shifted from simple penetration testing to identify technical risks to more comprehensive assessments that include policy and design reviews, as well as organizational communications. Embarking on this process, asset owners often pose the following common questions.

1. How secure is my architecture?
2. Am I compliant with industry standards?
3. How does my security compare to my competitors'?

Answering these questions requires analysis for each organization. Regardless of the approach, building an understanding of how each vulnerability leads to a consequence, one can then develop a business case for applying security. In previous industry workshops, asset owners shared common overall operational goals. These include [88]:

- financial stability,
- production and movement of product,
- safety,
- security,
- reliability,
- environmental compliance,
- preparedness.

Basic steps of a risk assessment process are outlined below. These steps are necessary to collect and analyze operational characteristics, and to identify potential consequences [89].

1. Threat Assessment

   Who or what can cause damage?

   Why would they want to do damage?

   What are the tools or perspectives necessary to do damage?

2. Vulnerability Analysis

   Where are the weak spots?

3. Consequence Definition

   What are the immediate effects?

4. Business Impacts Conclusions

   What are the damages?

5. Mitigation

   What fixes are necessary?

6. Life-cycle Application

   What are the long term prevention options?

Asset owners have numerous options to conduct these steps, which are discussed later in this section. In all cases, however, identifying and analyzing vulnerabilities is critical to applying the most useful mitigations. Vulnerabilities can be technical, operational, physical, or organizational in nature and can be categorized into the following classes [87]:

- system data handling;
- security administration;
- architecture and design;
- platforms, operating systems, and applications;
- networks and communications;
- incident response and handling.

Successful exploitation of a vulnerability leads to a host of technical effects. For example [90]:

- access control and authorization compromised;
- ability to escalate privileges;
- ability to hijack traffic, capture data;
- possible control of systems, applications, or network;
- installation opportunities;
- information gathering;
- ability to traverse the entire network;
- data theft.

Identifying technical effects can lead to understanding potential impacts. These are categorized in Table 6 [87].

Table 5—Potential Consequences and Impacts

Technical Consequence	Effect	Impact
Access/Read/Alter Data	– Theft or alteration of corporate/industry data – Theft or alteration of critical operations data used for future attack – Theft of personnel data – Divulge corporate trading partner info – Billing and purchasing data changed	– Economic (i.e. loss of trading partner, market instability, downtime) – National critical infrastructure (i.e. weaknesses in operations may be exploited, downtime, unavailability) – Quality of life (i.e. identify theft, negative publicity for corporation and industry) – Safety issues – Physical impacts to equipment
Gain Control of SCADA Systems	– Full operation of control systems – Can alter, stop, or destroy equipment and operations	
Denial of Service	– Halt operations on process control, business systems, or telecommunications	
Access Systems as Jump-points	– Use systems as part of a large scale, coordinated attack	
Physical Access to SCADA Systems	– Can physically damage systems – Access as a trusted insider if electronic access controls are not in place	
Introduction of a Virus/Worm	– Can slow or halt operations	

Asset owners may choose to conduct a comprehensive risk assessment or a compartmentalized assessment. This is often dependent on the security culture within the organization and integration of security into the corporate values. It is more common for assets owners to approach cybersecurity in smaller, compartmentalized assessments with defined objectives. This is typically the case when an assessment is prompted by a specific incident. Approaching risks in this manner is often more cost effective and results are established quickly with actionable findings. This methodology can make security more approachable and a less daunting task than attempting to assess all organizational OT in a single assessment. Likewise, different levels of acceptable risk and operational boundaries exist within a single organization. A one-size-fits-all mitigation set cannot be applied against technically and geographically disparate architectures.

Many approaches can be combined or extrapolated based on an organization’s primary objectives and the structure of their operations. It is common for an asset owner to choose one or more of the following methods to assess security [89]:

- compartmentalized assessments,
- compliance assessments,
- paper reviews,
- design assessments,
- hands-on testing and analysis,
- red teaming,
- threat assessments,

- specific vulnerability testing,
- statistical approaches,
- modeling and simulation.

Compartmentalized assessments are common when a defined technical or operational objective is known. These assessments target one aspect or function within operations and evaluate a specific capability or element, and an individual policy or procedure. Asset owners often begin with this approach to develop a precise finding, but realize it provides only a small piece of an organization's entire security posture. While some compartmentalized assessments seek to define the damage that could be created by a specific threat--such as an insider or outsider--it is the identification of risks that can be controlled or mitigated that is of most value to an asset owner.

One of the most valuable and common approaches selected is the ranking of critical assets. This is often a complicated equation that includes consideration of physical and logical assets, value of product, cost of downtime, cost of potential safety events, and public confidence. A ranked list of critical assets is of highly valuable to an organization and can become a map for applying security and mitigations at the most valuable locations.

In the ONG industry, compliance assessments are often the basis for establishing minimum standards within the organization. Organizations select industry and/or government guidelines and recommended practices which are used to conduct assessments. Additional protections are then added to the most critical asset locations within the organization. Sub-industries within the ONG industry typically select guidelines most applicable to their operations. This may include digital oil field operations, pipelines, or refining. Likewise, the product being produced or transported, and the geographic location of the assets may also be factors in selecting certain guidelines.

Certifications, like the Wurldtech Achilles Certification, are available to the ONG industry, though not as common as individual compliance assessments against specific guidelines. Large numbers of certifications or compliance software applications are not part of the ONG industry compared to other industries.

It should also be noted that compliance does not equal security. Compliance merely states than an architecture or process meets a minimum standard or recommendation. Changing technologies make these minimum standards moving targets. Compliance is a step toward security, but the best applied security is inherent to the process or system. The vast differences between complex architectures and operational surfaces within the ONG industry create a spectrum of best practices which more attractive to many asset owners.

Flexibility in these options also affords asset owners the option to defend against emerging threats. Meeting minimal compliance without an organizational-specific understanding of risk can leave an asset owner unprepared for a rapidly evolving threat landscape. As this landscape grows, asset owners must have flexibility in managing risk to account for increased target visibility within the ONG industry, broader attack surfaces and increased connectivity, integration of IT software in control environments without security testing, and growth in cloud activity and outsourcing. A flexible approach that facilitates identification and mitigation of the most critical risks lends itself to better protective mechanisms integrated within the life cycle in a cost effective way.

6 Technical Expertise

6.1 General

Science and technology expertise within the ONG industry is significant. The high-tech aspects of daily operations require advanced knowledge of operational processes and the application of control technology is critical to the success in energy production, refining, and transportation.

6.2 Oil and Natural Gas Industry

The ONG industry retains significant operational expertise within their workforce. This includes control system design and operation, controller functionality, and decision science required to make substantial operational choices to achieve optimal performance of energy production, refining and delivery. The standalone nature of early control systems created a clear division between network/IT and OT functions. Increased interconnectedness and the standardization of control systems on common operating platforms have resulted in a merging of these functions. Individual companies handle this merge differently. For example, some companies rely heavily on the enterprise/IT part of the organization to provide backbone communications and support to the OT functions. Others create OT departments that confer with enterprise/IT to achieve a common goal. From a security perspective, many of the more successful implementations leverage collaboration among several groups within an organization, including OT/SCADA controls, physical security, enterprise/IT, auditors, and management. This includes a clear mapping of risk mitigation to meet corporate values and strong intra-organizational communication.

Given the evolution of systems, cyber security is often an add-on requirement for control system manager, SCADA managers, and technicians. In very rare instances, dedicated OT security staff exist in the organization, the primary responsibility for these positions is the protection of control system assets and the continuity of operations. The growing interest in establishing these positions may be an indication that organizations recognize the importance of maintaining security to achieve operational continuity.

Unlike other scientific areas, implementation of OT may vary greatly depending on a multitude of organizational factors. Blanketed approaches and standard implementations can be difficult to achieve without considering these factors and details. Because of this, achieving security in realistic operational settings requires subject matter expertise that is often only resident within the industry itself, or gained through many years of OT experience.

6.3 Government

In consideration of technical expertise within the Federal Government, DHS is an optimum source to start with. “To build its own cybersecurity expertise, the Homeland Security Department should bring in details from the National Security Agency … [as] cybersecurity experts are in high demand in the private sector and difficult for DHS to hire…” [119]. It is also reported that “… none of the PSD [TSA’s Pipeline Security Division] staff have the specialized computer system expertise needed to support more extensive cybersecurity activities…” [113].

These two examples highlight some of the overall challenges and issues associated with a key element of DHS Cybersecurity Mission of “Providing technical expertise to the private sector and critical infrastructure and key resources (CIKR) owners and operators … to bolster their cybersecurity preparedness …” [48]. Further, as the Department of Defense accurately portrays “The demand for new cyber personnel is high, commensurate with the severity of cyber threats” [31]. Therefore, the Federal Government’s challenges include competing with private industry for a limited set of resources and lack of resources with the in depth skill set and knowledge base for an extremely diverse technological infrastructure. Even private industry faces these same challenges, but it begins from a position of having personnel with the relevant skills, knowledge, background, and expertise that are unique to their organizations and operating environments. The Federal Government does not have these same core competencies within their agencies.

However, the government has a history of engaging academia and civil servants to form advisory bodies that recommend guidelines and requirements for the ONG industry. The difficulty in this approach is a lack of awareness or exposure by these advisors to the rapidly changing OT environment. There can be a clear disconnect between operational process realities and the suggested best practices of the government, which can result in frustration among the industry. Successful examples of advisory bodies and forums always employ clear collaboration with industry and recognize the input and expertise of industry subject matter experts.

6.4 Collaboration and Partnerships

Government and private cybersecurity collaboration and partnership is not a recent topic or recently identified need. In 2009, *The President's National Security Telecommunications Advisory Committee* issued a report that "…outlines the United States' need to develop a joint, integrated public-private …capability" [106]. In 2011, the 112th Congressional Hearing on infrastructure protection identified the "Homeland Security Presidential Directive 7, [which]… outlines our National policy for Federal departments and agencies to partner with private sector… [and] the public-private partnership remains a key part of the Nation's efforts to secure and protect its critical cyber-reliant infrastructures" [48]. In 2012, the literature identifies how "…TSA believes that … it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well." [113]. Further, "the thing that regulators need to do is partner up with their utilities and ask good questions about what their cybersecurity investments mean …" [97].

A number of collaborative efforts have been conducted over the past decade[2]. A consensus of the various sources identified in this research effort can be summarize as "Collaboration is key – no single organization can respond effectively" [46]to ensure the breadth and depth of ONG cybersecurity is adequately addressed.

Collaborative efforts which have gained significant industry participation are considered more successful as they often facilitate the conveyance of threat information to industry and facilitate intra-industry and government communication. Likewise, the release of findings from technological research programs, such as those that assess the application of secure technologies in the operational environment, is considered to be more effective.

> "A coordinated and collaborative approach is needed.
>
> While some agencies strive to coordinate cybersecurity research and development efforts within their organization, when viewed across all the government agencies the chance of duplication, omission, and contradicting directions is all too likely. A national research agenda is urgently needed, with problems prioritized, innovative approaches encouraged and tracked, and a pipeline of short, medium, and long-term projects created." [151]

The sections 6.4.1 through 6.4.5 highlight several collaborative efforts and outcomes that have been achieved.

6.4.1 I3P and ESCSWG

Not only has the need for collaboration and partnership been clearly identified, there are several examples where this approach has been successfully leveraged. The Institute for Information Infrastructure Protection (I3P) and the Energy Sector Control System Working Group (ESCSWG) are just two examples of successful public-private collaboration.

[2] The authors of this paper have served in technical leadership roles, as advisory board members, researchers, and/or report authors on the I3P, ESCSWG, LOGIIC, and ICSJWG efforts.

I3P was formed in 2002 with the focus of bringing "… together researchers, government officials, and industry representatives to address cybersecurity challenges affecting the nation's critical infrastructures" [56]. This collaborative effort has produced a number of research reports, articles, risk characterization approaches and models [56].

The Energy Sector Control Systems Working Group (ESCSWG) "… is a unique public-private partnership initially formed in 2007 to help guide implementation of the priorities identified in the industry-led Roadmap to Secure Control Systems in the Energy Sector" [38]. A major outcome of this partnership is the Roadmap which "…provides a platform for pursuing innovative and practical activities that will improve the cybersecurity of our nation's energy infrastructure" [38].

6.4.2 LOGIIC

Formed in 2004, the Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) program is an ongoing collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate [148]. LOGIIC facilitates "cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems" and maintains "impartiality, the independence of the participants, and vendor neutrality" [148]. A LOGIIC consortium was formally established as collaboration between DHS, the Automation Federation, and five major oil and gas companies [148]. Research includes the evaluation of technologies, methods, and security mechanisms for OT environments, with a goal to affect change towards the development and applications of more secure technologies in OT. Information products and overarching research findings are published upon completion of each LOGIIC project and directed towards the entire ONG industry and vendor community.

6.4.3 HSIN

The Homeland Security Information Network (HSIN) was created after HSPD-7 in the early 2000s, and is defined as "a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission" [147]. Although the program was defined as a method to "securely share" information within a Community of Interest, it was met with reluctance by industry who was wary to share proprietary security information. Members are vetted through an application process, and the program website describes HSIN capabilities that include "secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing" [147]. Perhaps because of its early formation, HSIN has not been well-utilized by industry and was quickly overshadowed by other collaborative programs. In March and April 2009, HSIN was hacked twice [8], contributing to industry's reluctance to participate.

6.4.4 ICS-CERT and ICSJWG

As part of the DHS Control Systems Security Program (CSSP), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides control system security capabilities in collaboration with U.S. Cyber Emergency Response Team (U.S.-CERT) [144]. The ICS-CERT is a resource for the ONG industry as well as other infrastructure sectors. The ICS-CERT performs the following tasks [144]:

- "respond to and analyze control systems related incidents;
- conduct vulnerability and malware analysis;
- provide onsite support for incident response and forensic analysis;
- provide situational awareness in the form of actionable intelligence;

- coordinate the responsible disclosure of vulnerabilities/mitigations; and
- share and coordinate vulnerability information and threat analysis through information products and alerts."

Although recommended practices, secure design guidance, and assessment services are provided to industry, the alert and advisory reporting capability is perhaps the most valuable service. Feedback from industry consistently identifies the need for useful threat information. The alerts and advisory reports provide technical information to industry that assists industry in their prevention and incident response programs.

The Industrial Control Systems Joint Working Group (ICSJWG), was formed under the DHS CSSP to foster collaboration and information sharing. The ICSJWG is a "coordinating body" that "provides a vehicle for communicating and partnering across all Critical Infrastructure and Key Resources Sectors (CIKR) between federal agencies and departments, as well as private asset owners/operators of industrial control systems" [143]. The stated objective of the ICSJWG is "to continue and enhance the collaborative efforts of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems" [143]. The ICSJWG has gained significant participation by industry. It maintains five technical subgroups, conducts conferences, and produces information products such as the Cross Sector Roadmap.

6.4.5 FBI Infragard

The Federal Bureau of Investigation (FBI) established the InfraGard program in 1996. Infragard is an information sharing and analysis effort and a partnership with the FBI, businesses, academic institutions, state and local law enforcement agencies, and other participants "dedicated to sharing information and intelligence to prevent hostile acts against the United States" [63]. "InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters" [63]. Many ONG industry members participate in Infragard, which considers physical and cyber security, and criminal activities that pertain to infrastructure.

7 Recommendations

7.1 General

The findings from this research project lead to overarching conclusions and recommendations for approaches by industry and government. These recommendations are not technical; rather they address roles in response to a changing threat landscape, technological advancements, and evolving regulatory environment. These recommendations consider the industry's position as it relates to the topic of cybersecurity as a whole.

7.2 ONG Industry

As the industry moves forward with projects, optimization, and implementation of advanced technologies, several steps related to cybersecurity can be taken to be well positioned for changes ahead. These steps can be taken at the organizational level or through industry forums such as API. In either case, the industry should anticipate an increased federal role in cybersecurity of critical infrastructure to include involvement in incidents and potential data reporting requirements.

Individual Responsibility—On an individual basis, it is recommended that asset owners continue to employ cybersecurity that secures operations while facilitating business continuity and optimization. As the industry recognizes, secure technology mitigates the risk of an incident, potential downtime, and various consequences.

Continued preventative measures, ongoing risk mitigation, and maintenance of existing security programs, are key aspects of maintaining the standard of secure operations that the industry has established.

Path Forward as a Unified Industry—As the industry has illustrated in the past through the development of numerous cybersecurity standards and guidelines, tackling the implementation of highly technical concepts in a process control environment can be easier to handle as a group. It is recommended that the industry, through collaborative efforts and industry forums, map the effect of pending legislation and regulation, and mobilize a unified response. A unified approach to this technical topic may increase awareness of the complexities of OT.

One approach forward is to apply the framework used by forums such as Energy Nation. This approach outlines the key motivators for energy security and the promotion of domestic ONG resources. These same motivators apply to cybersecurity that facilitates and enhances operational processes to handle those resources. Resulting actions such as reducing barriers, providing access, and government-industry collaboration, are discussed in the federal approach later in this section.

Public Awareness—Robust public awareness programs exist regarding industry safety and public interaction with pipelines and utilities. Several past media campaigns outlined the role of industry in renewable investments, education, and community development. However, no awareness programs for the role of ONG in securing the infrastructure through technology presently exist. The public is unaware of the coordinated efforts of the industry to establish standards and guidelines, and the existing technical security controls in place to ensure continuity of operations and protection of assets. It is recommended that the industry develop an education and outreach effort that promotes the awareness of ongoing efforts of the ONG industry and their role in critical infrastructure stability and security. This effort should showcase the numerous ongoing efforts among the industry, collaboration between industry and government, and the technology advancements applied in ONG without mandates or regulation. The ONG industry clearly sees value in security and has implemented cybersecurity controls that promote stability of the national infrastructure. Significant advancements have been made in developing advanced cyber controls for operational environments, many at the request of ONG asset owners. An awareness campaign could promote the technical advancements, ongoing projects, and industry-wide efforts to ensure security.

7.3 Federal Government

Historically, the most successful role of the federal government in technology is facilitating solutions that promote continuity of operations through collaborative efforts with the industry.

Reducing Barriers—The federal government role should include reducing barriers and preventing new barriers such as regulation. Promoting cybersecurity through technology facilitates a secure infrastructure while promoting US investment. Advancing technology rather than establishing minimum standards, fosters innovation and inherent security solutions. Using competition within the US high-tech markets to solve security issues and create advanced technology for OT environments, secures national infrastructure and contributes to the economy.

Providing Access—Providing access to key resources such as actionable threat information and information resources is a key to successful, industry-wide cybersecurity. This is true in preventing and recovering from incidents, particularly incidents with potential cascading impacts across the critical infrastructure. Focusing on and supporting resources that are proven and working, like the US-CERT, is of utmost importance.

Likewise, facilitating access to new projects rather than extending the process, like permitting, is important. Setting regulations at a level not readily attainable in existing technology, processes, and information flows will reduce access to new projects and efforts.

Facilitating Domestic Projects—Promoting US solutions and facilitating new projects are important to prevent projects from moving overseas. It is extremely easy to move information and computing capabilities, as well as investments, overseas where cybersecurity regulation may not apply.

Over the past decade, the cyber-threat landscape for the ONG industry has evolved from virtually non-existent to a reality of daily operations. The industry has adapted and responded to these threats by implementing security controls through technology and industry standards. The industry continues to employ advanced technologies while mitigating risk and continuing secure operations.

Annex A
(informative)

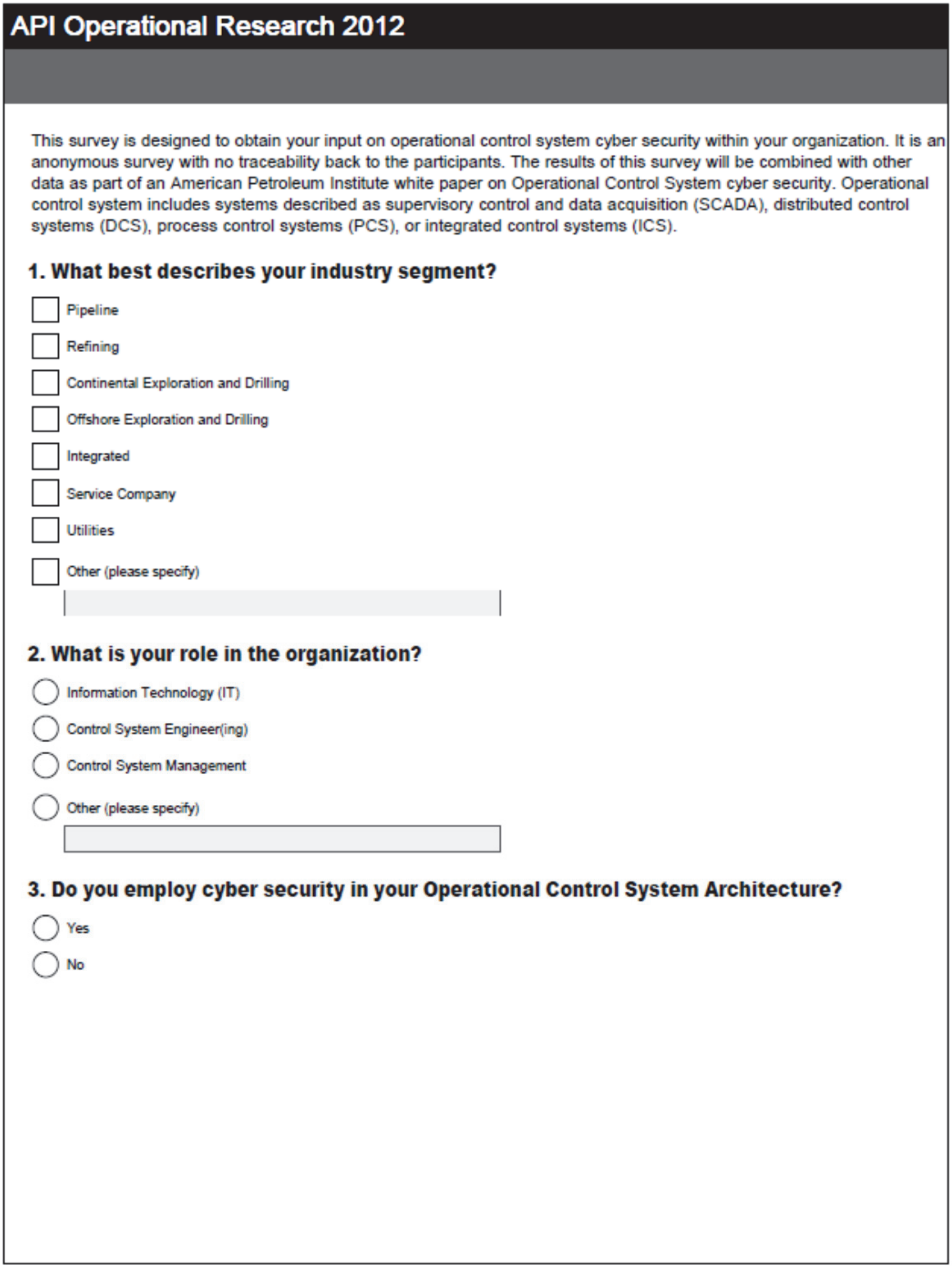
Industry Survey

A.1 General

A study conducted in 2010 by the Center for Strategic and International Studies called “In the Dark: Crucial Industries Confront Cyberattacks” states that 80% of 200 “IT” executives at utilities, oil, gas, and water companies responded that they had experienced large scale denial of service attacks [35]. This study is cited countlessly in articles on cybersecurity for critical infrastructure, and is often referred to as definitive, illustrating the lack of critical infrastructure survey data. The study, however, includes international respondents.

To obtain a focused and current view of the ONG industry views on cybersecurity, an on-line API survey was conducted between September 31 and October 24, 2012 and repeated at the November 12th, 7th Annual API Cybersecurity Conference Operational Technology Workshop. Between the two surveys populations a total of 39 usable survey results were obtained. The following section highlights the survey findings. Note, all percentages have been rounded to the next whole number.

The following pages contain images of the Survey, followed by the results and a summary of the findings.



API Operational Research 2012

This survey is designed to obtain your input on operational control system cyber security within your organization. It is an anonymous survey with no traceability back to the participants. The results of this survey will be combined with other data as part of an American Petroleum Institute white paper on Operational Control System cyber security. Operational control system includes systems described as supervisory control and data acquisition (SCADA), distributed control systems (DCS), process control systems (PCS), or integrated control systems (ICS).

1. What best describes your industry segment?

□ Pipeline

□ Refining

□ Continental Exploration and Drilling

□ Offshore Exploration and Drilling

□ Integrated

□ Service Company

□ Utilities

□ Other (please specify)

2. What is your role in the organization?

○ Information Technology (IT)

○ Control System Engineer(ing)

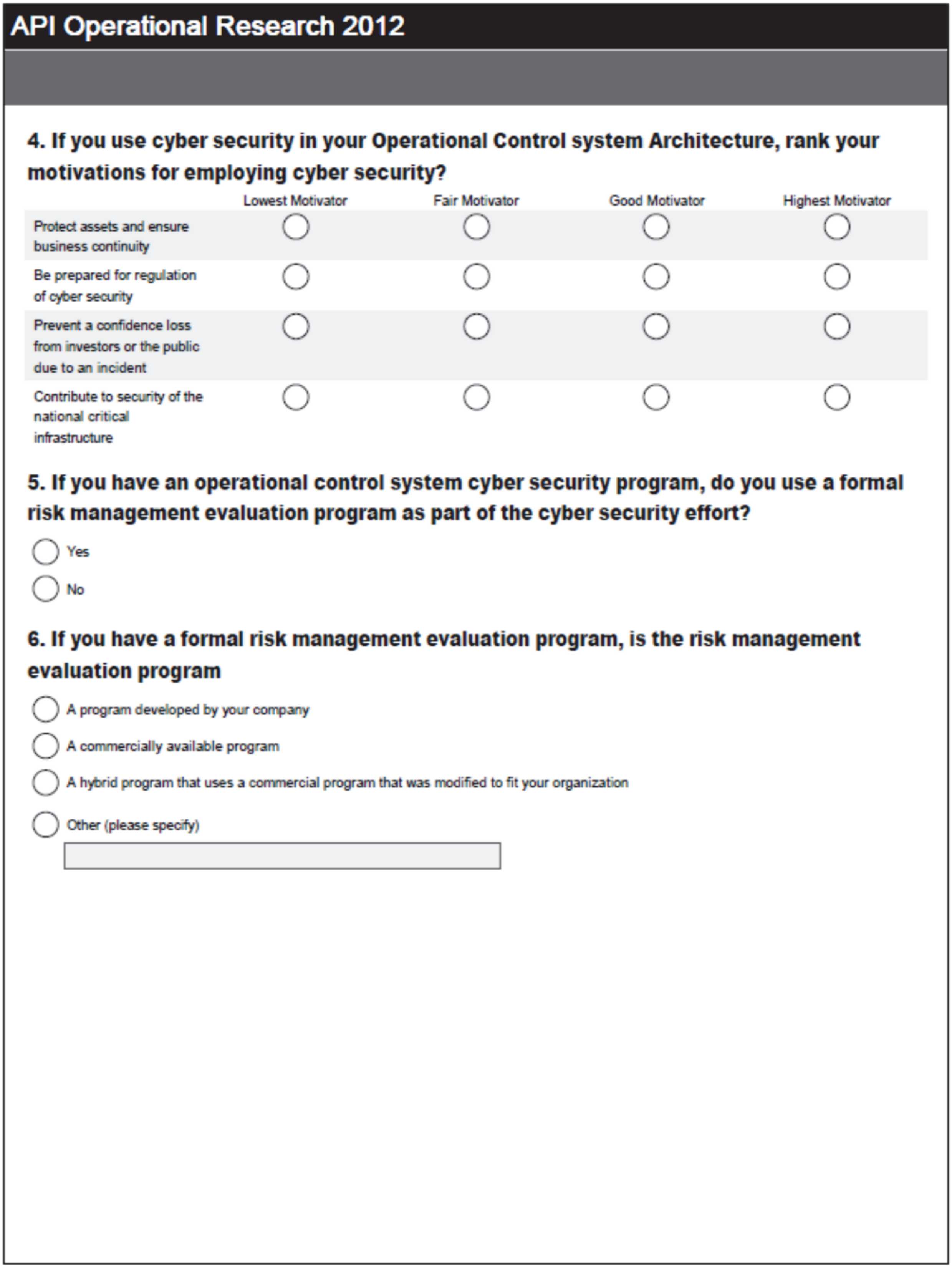
○ Control System Management

○ Other (please specify)

3. Do you employ cyber security in your Operational Control System Architecture?

○ Yes

○ No



API Operational Research 2012

4. If you use cyber security in your Operational Control system Architecture, rank your motivations for employing cyber security?

	Lowest Motivator	Fair Motivator	Good Motivator	Highest Motivator
Protect assets and ensure business continuity	○	○	○	○
Be prepared for regulation of cyber security	○	○	○	○
Prevent a confidence loss from investors or the public due to an incident	○	○	○	○
Contribute to security of the national critical infrastructure	○	○	○	○

5. If you have an operational control system cyber security program, do you use a formal risk management evaluation program as part of the cyber security effort?

○ Yes

○ No

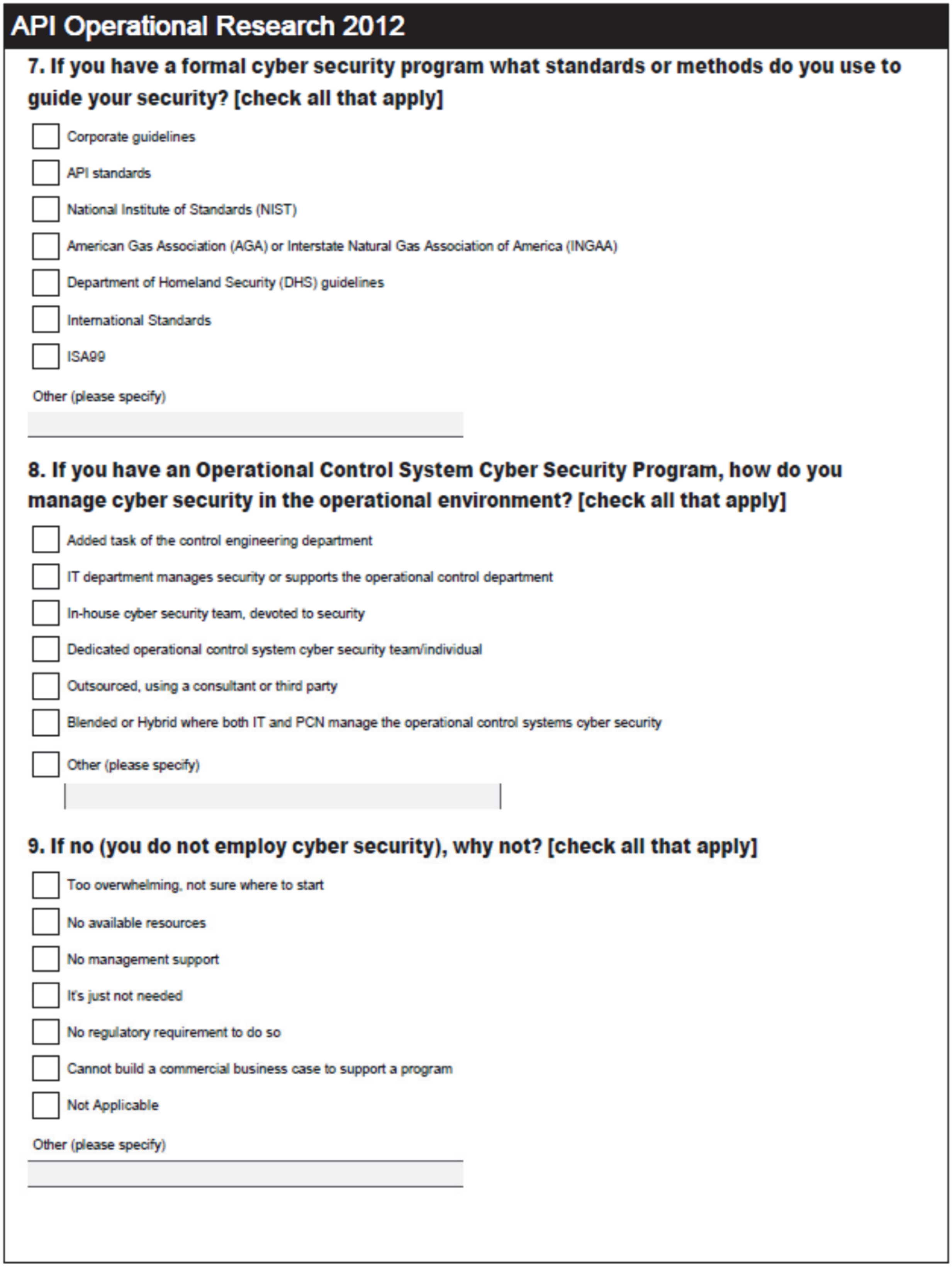
6. If you have a formal risk management evaluation program, is the risk management evaluation program

○ A program developed by your company

○ A commercially available program

○ A hybrid program that uses a commercial program that was modified to fit your organization

○ Other (please specify)



API Operational Research 2012

7. If you have a formal cyber security program what standards or methods do you use to guide your security? [check all that apply]

□ Corporate guidelines

□ API standards

□ National Institute of Standards (NIST)

□ American Gas Association (AGA) or Interstate Natural Gas Association of America (INGAA)

□ Department of Homeland Security (DHS) guidelines

□ International Standards

□ ISA99

Other (please specify)

8. If you have an Operational Control System Cyber Security Program, how do you manage cyber security in the operational environment? [check all that apply]

□ Added task of the control engineering department

□ IT department manages security or supports the operational control department

□ In-house cyber security team, devoted to security

□ Dedicated operational control system cyber security team/individual

□ Outsourced, using a consultant or third party

□ Blended or Hybrid where both IT and PCN manage the operational control systems cyber security

□ Other (please specify)

9. If no (you do not employ cyber security), why not? [check all that apply]

□ Too overwhelming, not sure where to start

□ No available resources

□ No management support

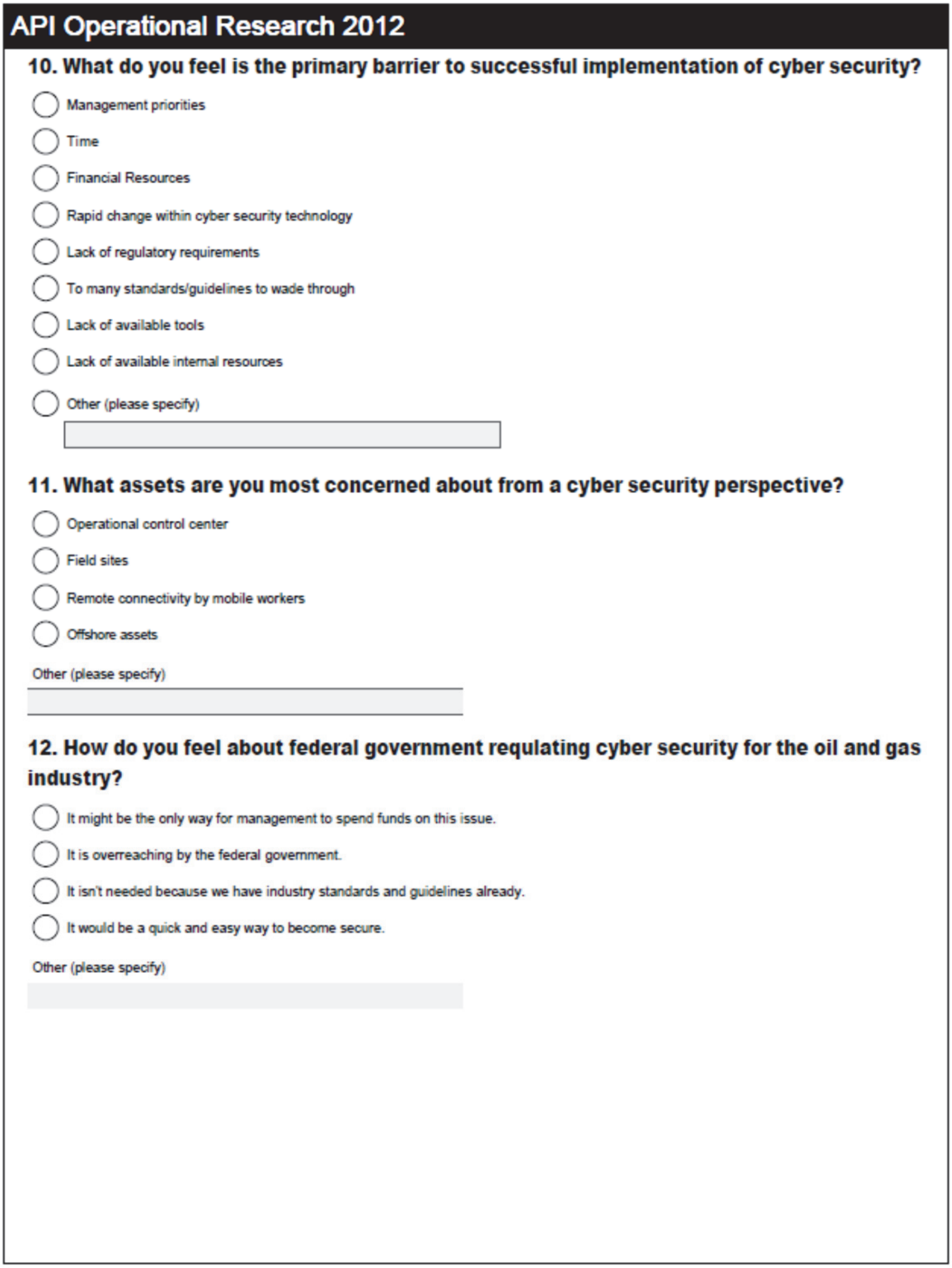
□ It's just not needed

□ No regulatory requirement to do so

□ Cannot build a commercial business case to support a program

□ Not Applicable

Other (please specify)



API Operational Research 2012

10. What do you feel is the primary barrier to successful implementation of cyber security?

○ Management priorities

○ Time

○ Financial Resources

○ Rapid change within cyber security technology

○ Lack of regulatory requirements

○ To many standards/guidelines to wade through

○ Lack of available tools

○ Lack of available internal resources

○ Other (please specify)

11. What assets are you most concerned about from a cyber security perspective?

○ Operational control center

○ Field sites

○ Remote connectivity by mobile workers

○ Offshore assets

Other (please specify)

12. How do you feel about federal government requlating cyber security for the oil and gas industry?

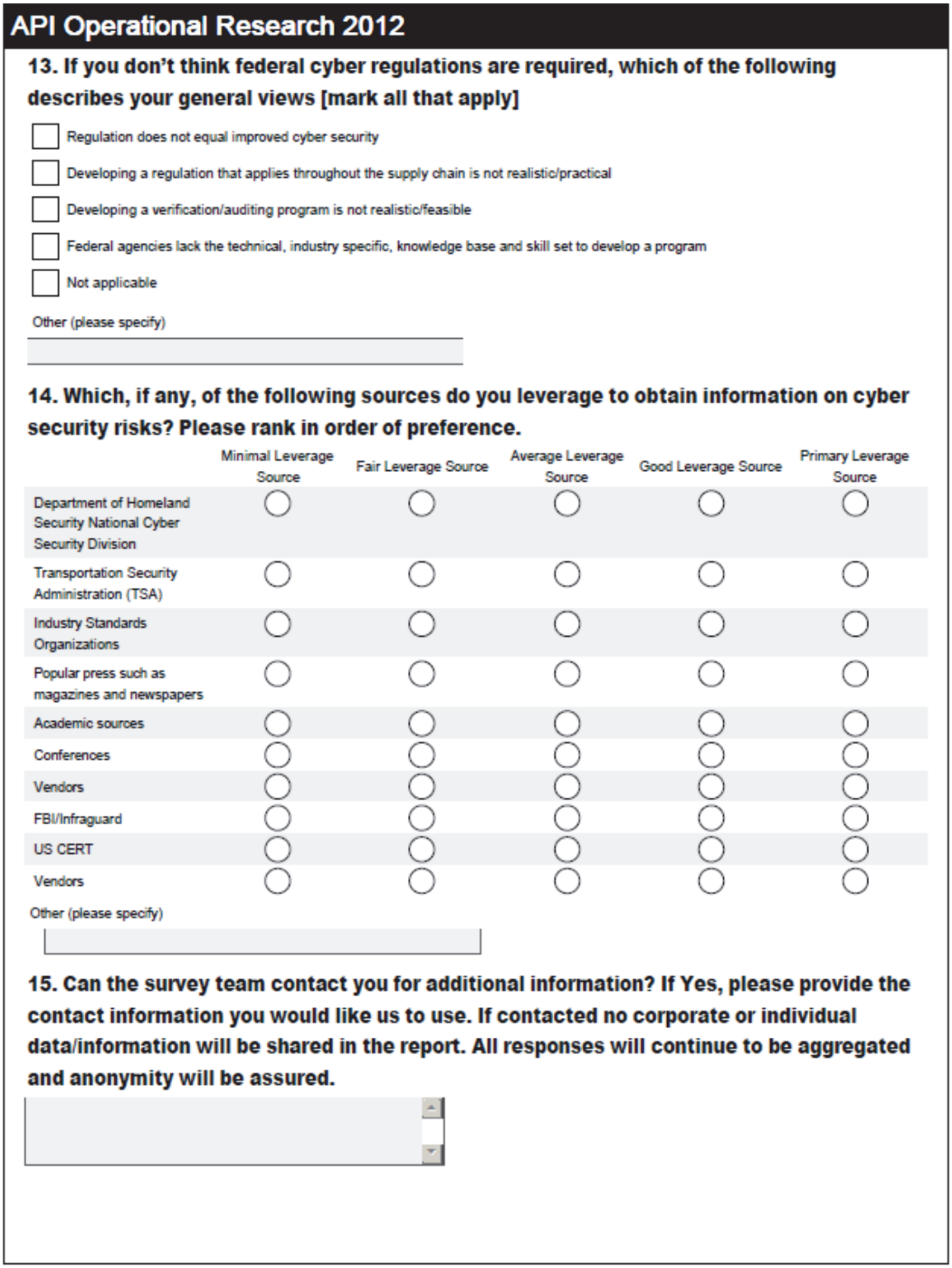
○ It might be the only way for management to spend funds on this issue.

○ It is overreaching by the federal government.

○ It isn't needed because we have industry standards and guidelines already.

○ It would be a quick and easy way to become secure.

Other (please specify)



API Operational Research 2012

13. If you don't think federal cyber regulations are required, which of the following describes your general views [mark all that apply]

□ Regulation does not equal improved cyber security

□ Developing a regulation that applies throughout the supply chain is not realistic/practical

□ Developing a verification/auditing program is not realistic/feasible

□ Federal agencies lack the technical, industry specific, knowledge base and skill set to develop a program

□ Not applicable

Other (please specify)

14. Which, if any, of the following sources do you leverage to obtain information on cyber security risks? Please rank in order of preference.

	Minimal Leverage Source	Fair Leverage Source	Average Leverage Source	Good Leverage Source	Primary Leverage Source
Department of Homeland Security National Cyber Security Division	○	○	○	○	○
Transportation Security Administration (TSA)	○	○	○	○	○
Industry Standards Organizations	○	○	○	○	○
Popular press such as magazines and newspapers	○	○	○	○	○
Academic sources	○	○	○	○	○
Conferences	○	○	○	○	○
Vendors	○	○	○	○	○
FBI/Infraguard	○	○	○	○	○
US CERT	○	○	○	○	○
Vendors	○	○	○	○	○

Other (please specify)

15. Can the survey team contact you for additional information? If Yes, please provide the contact information you would like us to use. If contacted no corporate or individual data/information will be shared in the report. All responses will continue to be aggregated and anonymity will be assured.

A.2 Survey Results

The survey objective was to identify current OT cybersecurity practices, areas and sources where the industry obtains cybersecurity support/input to their programs, the application and use of risk analysis as applied to cybersecurity program, as well as industry views on potential cybersecurity regulation.

Figure A.1 identifies the survey respondents' industry segments. With the exception of two participants, the majority identified that their organization included multiple industry segments. The most commonly identified industry segments include Continental Exploration and Drilling, Offshore Exploration and Drilling, and Pipelines. These three segments account for 65% of the respondents. The smallest industry segmented represented was the utility sector with 2% of the responses. In general, a diverse portion of the industry was represented by these participants as every portion of the industry was represented.

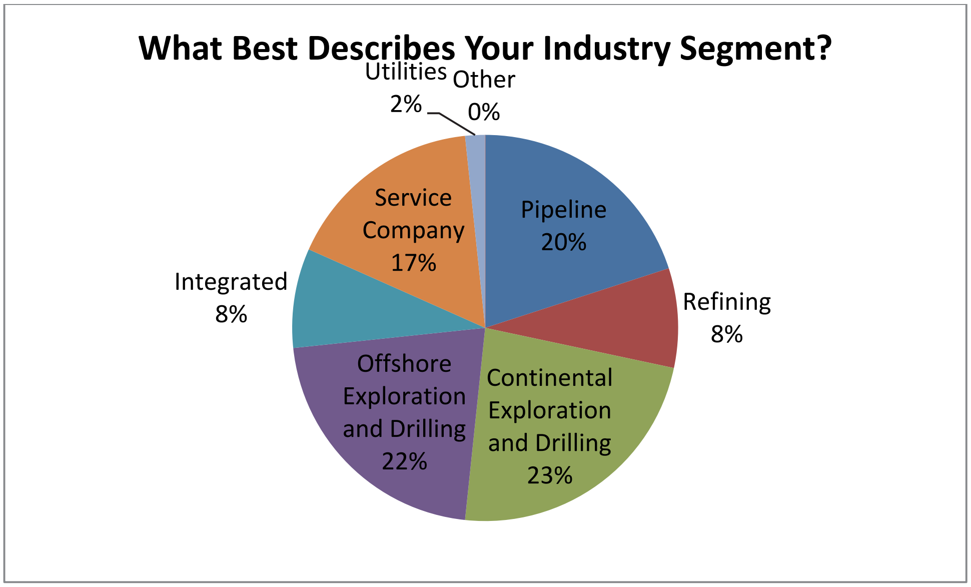


Figure A.1—Survey Response Industry Segment

The survey specifically requested that the respondents identify which part of the organization they work within based on the options of (a) Information Technology, (b) Control System Engineer(ing), (c) Control System Management, or (d) other. Figure A.2 shows 85% of the respondents who answered this question identified themselves as working in the Information Technology (IT) portion of their organization. Of the remaining responses there were two respondents each in the (b) Control System Engineer(ing), (c) Control System Management, or (d) other. One of the 'other' respondents identified themselves as a SCADA cybersecurity person, and the other respondent said they were in the Security Compliance group. This question clearly identifies that the IT organization has a major influence and control over OT cybersecurity.

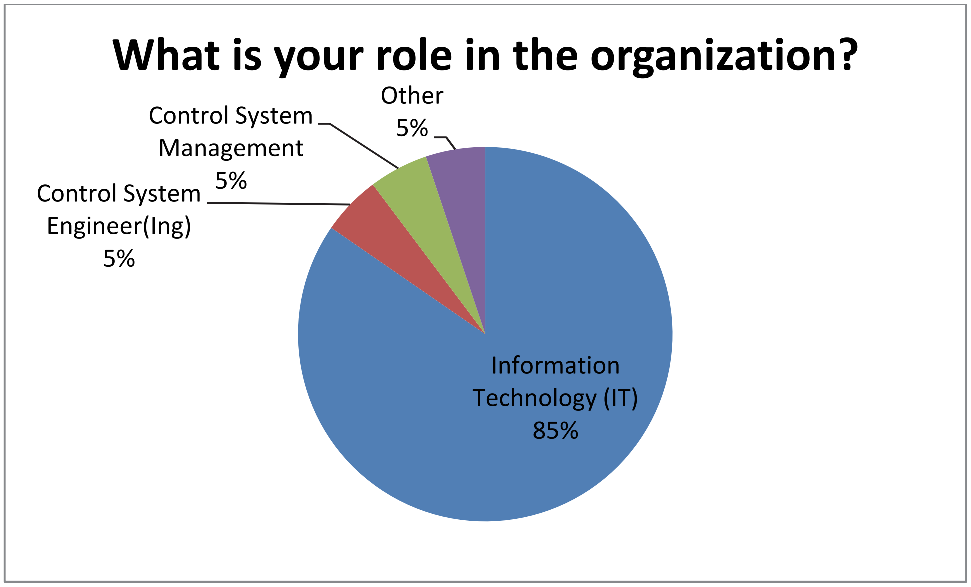


Figure A.2—Respondent Organization Location

The third survey question asked the respondent if their organization "…employ cybersecurity in your Operation Control System Architecture…" The responses identified that 82% did while 18% did not. The remainder of the survey questions responses was gathered from the 82% of the participants who employ cybersecurity.

Question 4 identified the motivator for employing cybersecurity in the OT infrastructure. Figure A.3 identifies that the highest motivator is to "protect assets and ensure business continuity with 85% of the respondents. All respondents identified that the need to protect assets and ensure business continuity was either the highest or a good motivator.

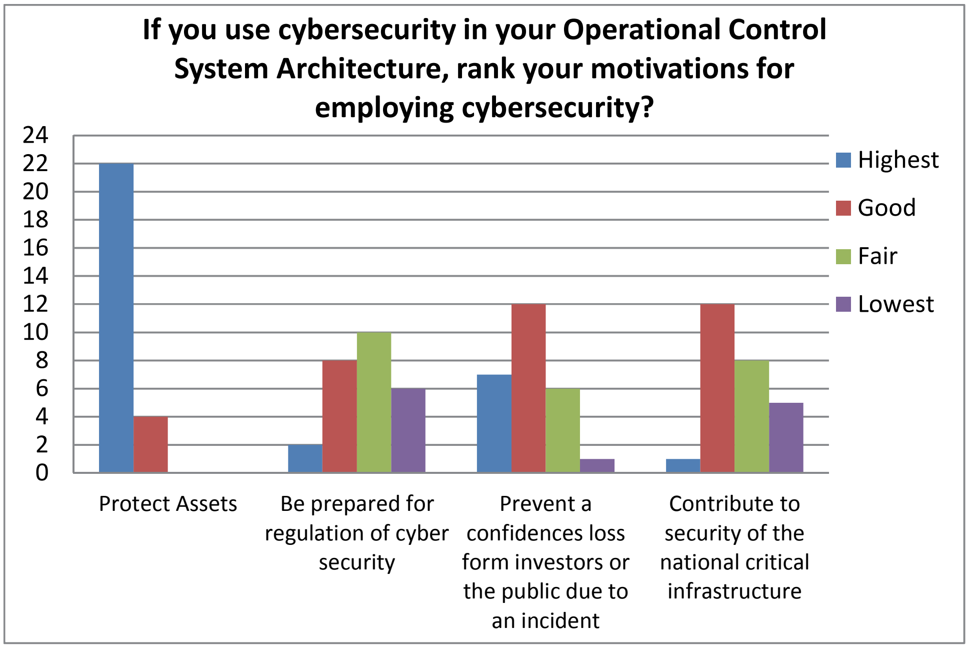


Figure A.3—Motivation for Applying Cybersecurity

Overall, the lowest motivator category was to "Be prepared for regulation of cybersecurity." Between the "Lowest" and "Fair" selections 62% of respondents selected these categories. The next lowest motivator is

"Contribute to the security of national critical infrastructure." Only one of the respondents' selected this as their highest motivator while 46% indicated it was a "Good" motivator, 31% said it was a "Fair" motivator and 19% identified this as the "Lowest" motivator.

Question 5 asked the participants if they use a "…formal risk management program…" as part of their cybersecurity program. Just over two-thirds of the responses said yes, 70%, while the remaining 30% said no.

Of the 70% who use a formal risk management program, it was an even split between programs that are developed internal to the organization and all other approaches. Of the three remaining methods, the prevalent approach was "A hybrid program that uses a commercial program that was modified to fit your organization." Using a "Commercially available program" method was identified by two respondents, while the remaining two respondents identified the use of an 'informal' program.

Based on the survey responses a very limited set of firms, 9%, of the firms rely on commercially available risk management evaluation programs. The remaining 91% rely on systems that are customized for their organization.

Question 7 provides a range of standards or methods that can be used to guide development of the corporate security program. The question asked the participants to select all which they leveraged. As shown in Figure A.4 "Corporate guidelines" are leveraged the most with 24% of the respondents selecting this category. The next two most frequently selected sources are "National Institute of Standards and Technology (NIST)" and "Department of Homeland Security (DHS) guidelines," which were selected by 19%, each, of the survey participants. "API standards" were selected by 16% of the individuals.

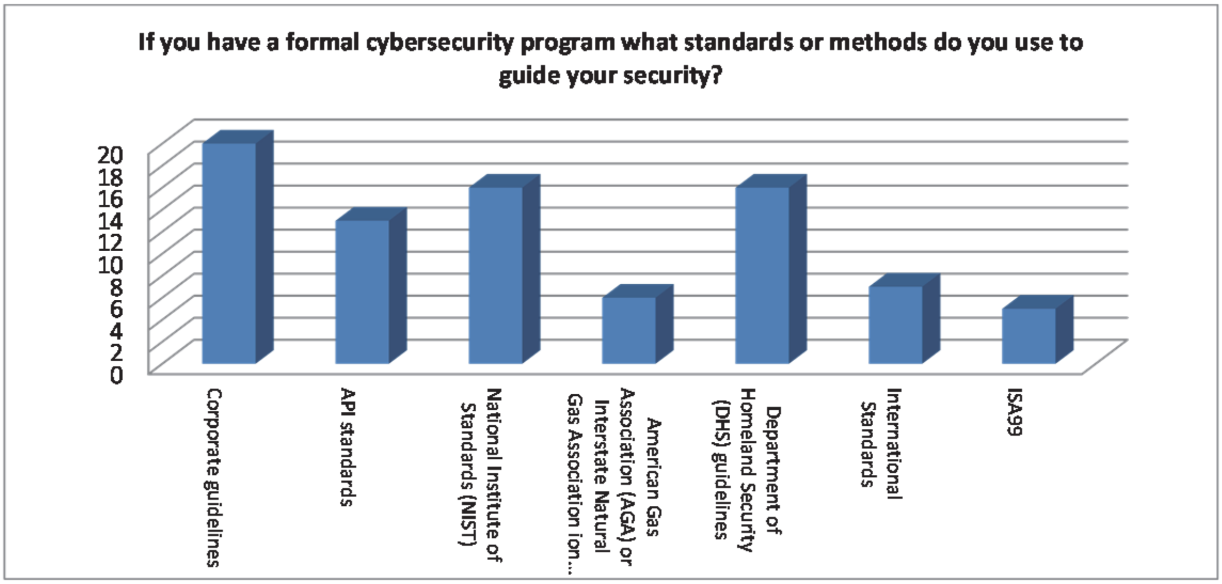


Figure A.4—Guiding Methods

"International Standards" were identified by 8%, while "The American Gas Association (AGA) or Interstate Natural Gas Association of America (INGAA) guidelines" were used by 7% of respondents. ISA 99 received 6% of the selections.

All respondents identified that they used more than one guiding method. All whom selected "Corporate Guidelines" selected at least one other method, which included "API standards" [11 out of the 20 times], "National Institute of Standards (NIST)" [11 out of the 20 times], and "Department of Homeland Security (DHS) guidelines [8 out of the 20 times]. The key factor is that the organizations leverage more than one guiding method.

In Question 8 the focus was on how the cybersecurity program is managed in the organization. Figure A.5 identifies that of these participants, 30% use a blended approach where both IT and OT manage the operational controls system cybersecurity. The next most frequent organizational management approach is pure IT department with 27%. The third most frequent approach is use of In-house cyber security teams with 25%.

The least common organizational management approaches included “Dedicated operational control system cyber security team/individual” 9%, “Added task of the control engineering department” 7%, and Outsourced 2% [1].

It is notable that combining the “Blended” and “IT department” methods account for 57% of the organizational approaches. This majority approach matches with the overall view that the IT organization is significantly involved in OT cybersecurity for most organizations.

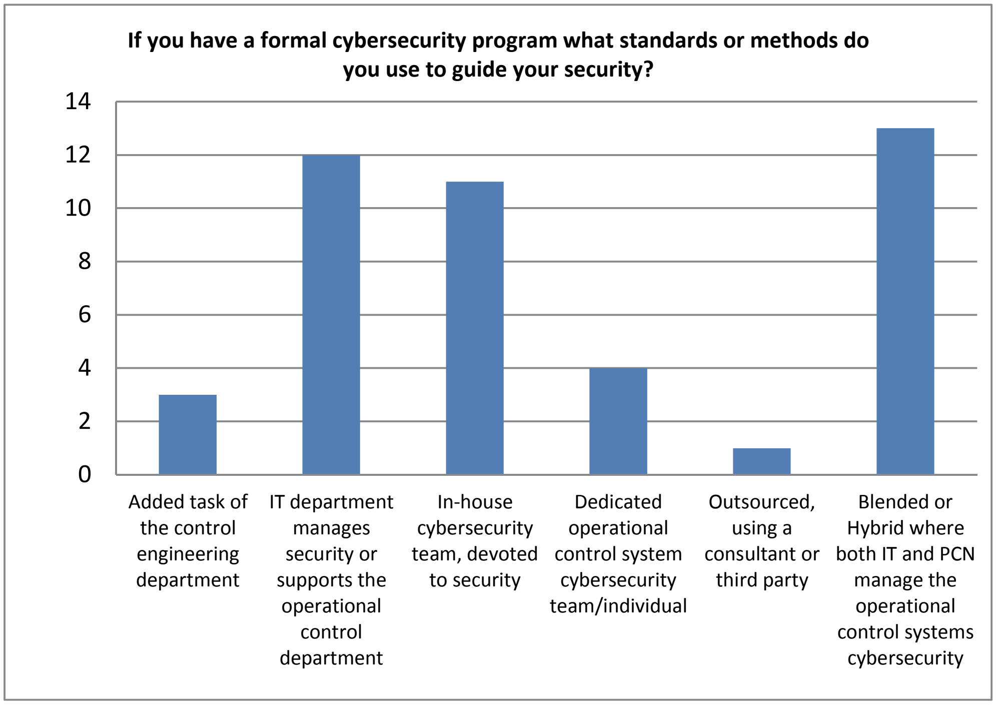


Figure A.5—How Cybersecurity Program Managed

Question 9 had no responses as everyone who reached this portion of the survey had identified that they were using cybersecurity.

Question 10 focused on what barriers appeared to be preventing the successful cybersecurity implementation within the organization. Figure A.6 identifies “Management priorities” and “Time” as the top two barriers; 33% and 21% respectively. The respondents were equally split between “Lack of available internal resources” and “Financial resources”, 17%, as the next level of barriers. The last selected category, “Too many standards/guidelines to wade through,” was selected by 12% of the survey participants.

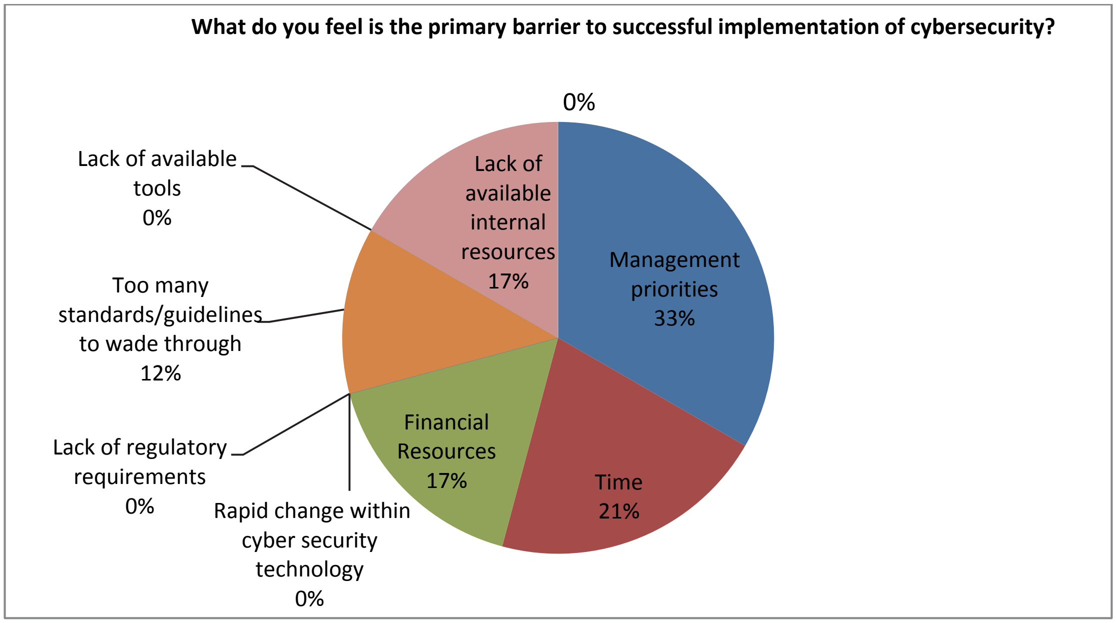


Figure A.6—Barriers to Successful Implementation

In question 11, the intent was to identify which assets the industry was most concerned with. As shown in Figure A.7, the responses identified the operational control center as the asset with the highest level of concern with 46% selecting this category. Field sites were next on the list with 39% concerned. Remote connectivity was selected 12% of the time, while offshore assets were identified 4%.

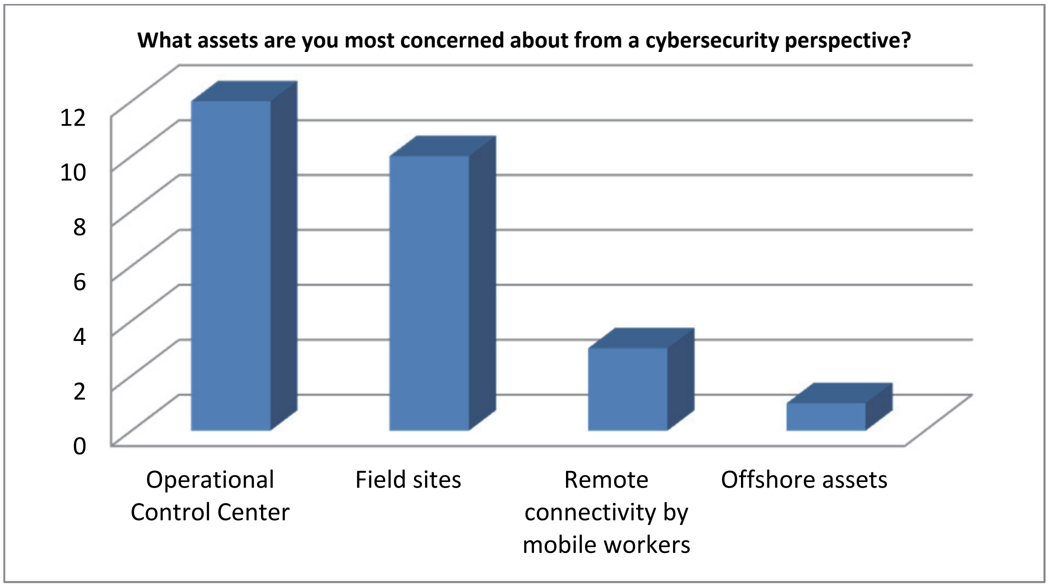


Figure A.7—What assets are you most concerned with?

Questions 12 and 13 focused on the industry view of federal regulation for the ONG industry. Question 12 specifically looked at the industry's view of federal regulations. As identified in Figure A.8, the highest number of responses, 48% identified that "It isn't needed because we have industry standards and guidelines already" while 29% said it was "overreaching by the federal government." The remaining 24% respondents identified that it "might be the only way for management to spend funds on this issue."

Combining the top two categories identifies that the respondents to this survey do not view federal regulation as a positive thing, 76%.

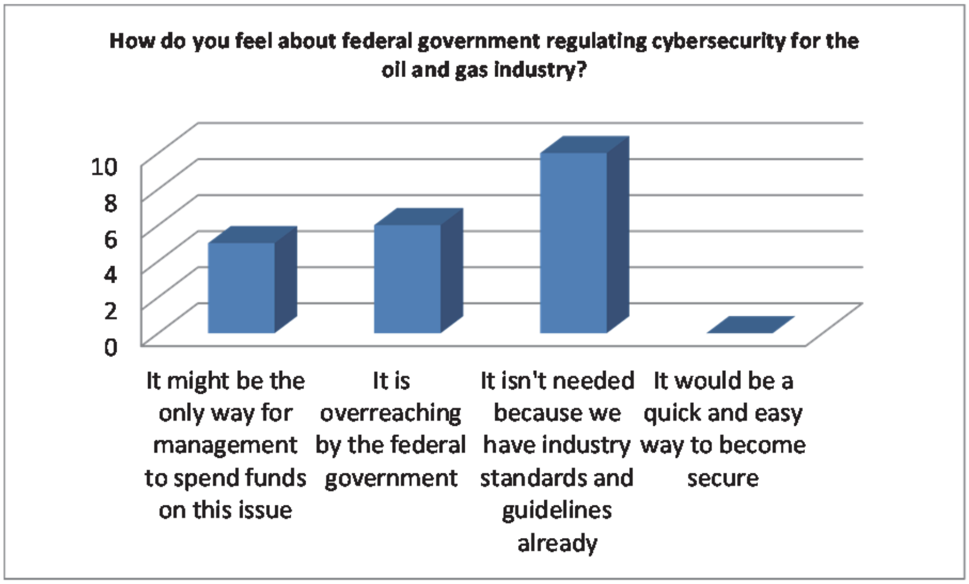


Figure A.8—Industry View on Federal Regulation

Question 13 looked at what might be the underlying reasons why the industry does not have a positive view of federal regulations on cybersecurity. As shown in Figure A.9, overwhelmingly, 42% clearly disassociate regulation and improved cybersecurity. The industry also holds the view that there is a lack of technical, industry-specific knowledge within the federal government, 27%, and developing regulation that applies throughout the supply chain is not realistic or practical, 24%.

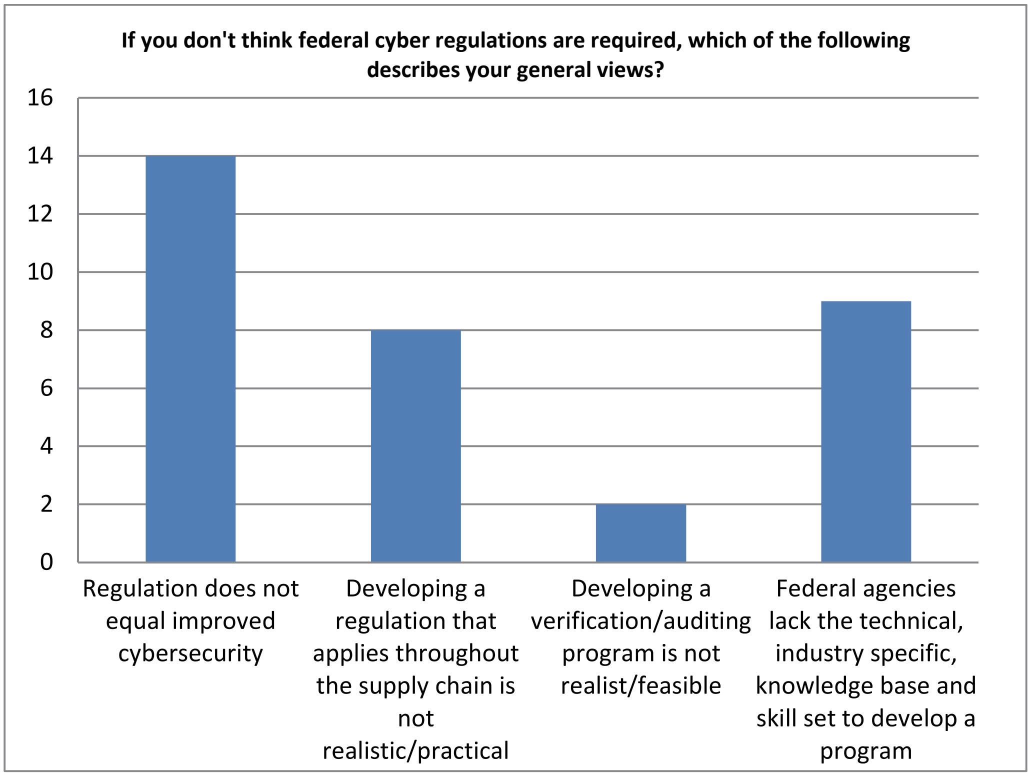


Figure A.9—Why is Federal Regulation Not Required

The final question, Question 14, identifies where the industry is obtaining its information on cyber risks. In this question, participants could select multiple sources. As shown in Figure A.10, the industry's information source most often used is industry standards. Of the respondents 49% identify that they find U.S. CERT as either their primary or a good source of cybersecurity information. This is followed by the Industry Standards where 41% of respondents identify that this is either their primary or a good source of information. The industry identifies the least used sources as academic sources, popular press and conferences. No respondent identified these as their primary source of information. Rather the respondents identify that these sources are general average or below.

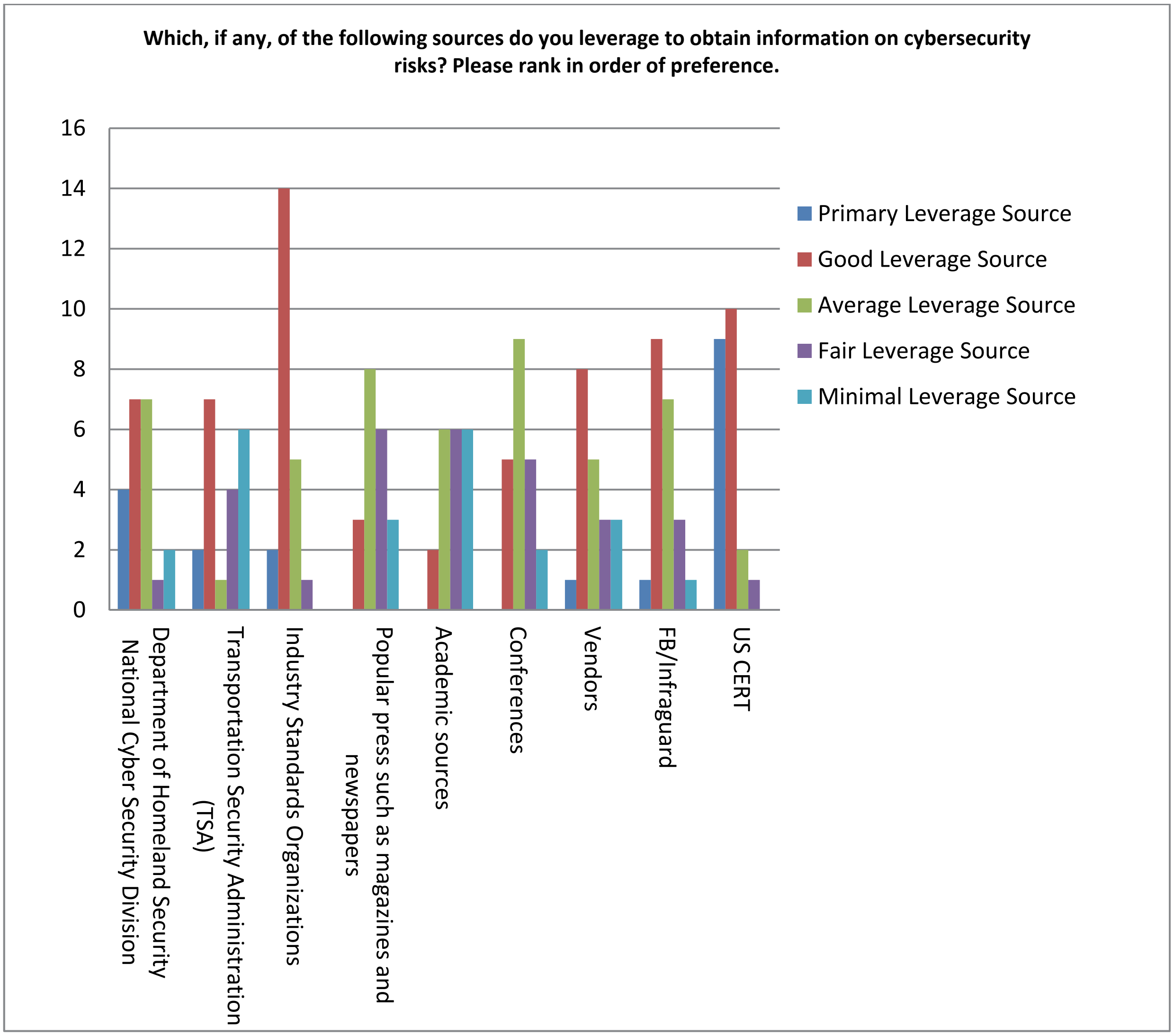


Figure A.10—Risk Information Sources

A.3 Summary of Findings

A.3.1 General

Conclusions from the research, survey data, and analysis of findings can be categorized into several areas listed below. In total, these findings are useful in describing the status of security in OT environments within the ONG industry.

A.3.2 Present State of Security

Over the past decade, asset owners have shown a significant interest in applying security to their OT systems. The realization that continuity of operations depends on the security of OT systems is generally shared among the industry. Security objectives, such as safety and public perception, must map to the values of the asset owner, in order to justify the resources required to apply security. Asset owners agree that security is important and provides long-term benefits, but like many operational continuity aspects, it must be set forth as part of the organizational culture and supported across the company.

Many asset owners suggest that Stuxnet, Duqu, Shamoon, and other similar events, enhance the case for security and keep awareness fresh within the organization. A lack of documented threats or incidents can make security an afterthought. Likewise, a constant cyber-doom warning without a realistic occurrence often invalidates the need for security among those in the organizations that allocate resources and do not understand the techniques behind potential attacks.

Asset owners can leverage a number of resources to meet security objectives. Typically, an asset owner develops a security program that maps to their OT environment and needs. They may develop the program in-house or obtain assistance from third parties or consultants. A number of common motivations typically prompt development of such a program. These may be responses to incidents, an OT system upgrade, a new business continuity plan, and so forth. When developing a security program, asset owners presently have the option of designing a program that is highly specific to their operational needs. They may choose a set of guidelines or standards to leverage. These may be government generated, such as the TSA guidelines discussed in this paper, or they may be industry authored, such as API or AGA standards. The spectrum of choices allows industry to select a best-fit for their operational space and typically considers many factors such as geographic location of the system, criticality of the system, consumers served, etc.

In addition to written guidance, asset owners have options for building the programs to include assessments and audits, policy and procedure development, and incident response capabilities. A wealth of information regarding assessment science, options, and components has been developed by both government and industry forums to assist with this process. Some asset owners choose to delegate this responsibility to in-house audit teams, whereas others opt to hire outside consultants to perform zero-knowledge or outsider threat testing.

Presently, written and human resources exist in both the government and private sector to assist with all phases of design and implementation of a security program. Asset owners benefit from the availability of these resources and the ability to tailor their own program with the most effective security solutions. These may include threat analyses, system design specifications, assessments and penetration tests, incident response and recovery planning and physical and personnel security policies.

In the early 2000's, collaborative government-industry efforts sought to provide awareness of potential security threats, and asset owners worked to determine potential consequences and available protective mechanisms for the OT environment. In the past decade, this has evolved to an increased understanding of operational impacts and is perpetuated by the need to remain competitive. Many asset owners seek to meet or exceed their competitor's security efforts, with a desire to not be lagging in this technical space.

Collaborative efforts that provide useful technical findings, best practices, threat information and that facilitate sector communications have been identified as most useful. To date, these have provided the most valuable information for asset owners as they define their own tailored security programs. It is likely that motivation to maintain security and mitigate risk will continue. What remains to be seen is the large-scale effect of legislation and regulation on the implementation of security and the approach towards compliance. Several conclusions may be inferred and are discussed in the regulation section (A.3.4).

A.3.3 Technical Findings

Within the area of technical findings, this research has identified:

- Supporting evidence that OT system cyber-attacks are increasing.

- Advanced skill set cyber-attacks will continue to occur.

- Vendor cybersecurity research and product enhancement will only be driven by industry willingness to pay the increased costs. There is no financial benefit to a vendor to advance their products' cybersecurity capabilities if the industry is not willing to pay additional costs to obtain them.

- Vendor cybersecurity advances appear to be driven by IT requirements, not OT needs.

- OT cybersecurity is predominantly driven by IT methodologies, methods, skills, and tools. This fails to adequately take into account the uniqueness and operational context of the OT infrastructure.

- OT cybersecurity with an IT centric approach appears to be an outward looking method which fails to adequately take into account the insider threat. Detailed research is required to enhance OT cybersecurity methodologies, methods, and tools which are specific to the OT environment.

- There are many types of IT cybersecurity certifications. A few examples include "ISC's Certified Secure Software Lifecycle Professional (CSSLP) ... GIAC Secure Software Programmer - Java (GSS-JAVA) ... Certified Information Systems Auditor (CISA) ... Certified Information Systems Security Professional (CISSP) ... Certified Wireless Security Professional (CWSP)..." (Prince, 2010) (Gupta, 2012). A corresponding set of in-depth OT related cybersecurity certifications does not exist.

In summary, OT cyber-attacks are forecasted to increase. The increased threat level increases overall organizational risk. OT security has leveraged IT cybersecurity approaches, yet these approaches are not universally applicable to the operational and environmental context of the OT infrastructure. There is a lack of OT operational and environmental context cybersecurity systems and industry approved certifications. Vendors are asking the industry if they are willing to support advanced cybersecurity capabilities by paying the extra costs to acquire it.

A.3.4 Regulation

Over the past decade, the approach to identifying and implementing best security practices was offered by collaborative projects that provided guidance, methodologies, and research findings. Since the suggestion of the Cybersecurity Act in early 2012, a number of relevant legislative pieces were drafted. The challenges of regulating a highly technical topic were compounded by the specific identification of critical infrastructure in this legislation. The difficulty of applying technical security requirements in very specific, custom, OT environments is well understood by industry. Other complications include protections for information sharing governing agencies, identified "incentives", and "voluntary" participation leads to a vagueness that proves worrisome to the industry.

At the most basic levels, the idea of regulating complex technology is one that has been debated for many years. Complex information technologies are not well understood by many, yet their standardization and increased availability have allowed for topics such as cybersecurity to become more realistic to the public. OT systems are still not commonly understood. In fact, the general public only minimally understands the existence of control systems in the critical infrastructure space. Although industry, government, and the public agree that critical infrastructure stability and OT security is decidedly important, the mechanism to provide this security is really the point of debate. Regulation often creates a lowest common denominator of compliance. Even the

Executive Order suggests a “minimum” standard. This level of mediocrity does not promote advanced security techniques or a level of customization that may provide the most effective risk mitigations in complex environments. Because OT environments can be significantly different, drafting a broadly applicable regulation often removes the ability to make technically detailed policies that are the best protections.

There is a realization among the industry that regulation is likely to occur in the near future. The ramifications of such legislation remain to be seen, but many can conclude that impacts to the industry will occur. Aside from the questionable use of regulation to achieve the most effective security in OT environments, other aspects of regulation are a concern to the industry. These include:

- *Expertise and the Structure of Regulation*—The regulatory language, technical expertise available in the authorship, and compliance assessments may be conducted by industry agencies with little exposure or awareness to operational environments. Operational consequences may not be well understood by those outside the industry. Without a clear definition of exactly what will be mandated or “voluntary”, a path forward for implementing these regulations is unknown.

- *Orders to Cease Operations*—All operational incidents require forensic analysis and review. A lack of clarity over the government’s role in response to both an incident or lack of compliance during an audit raises concerns about the ability to issue orders to cease operations. Cyber incidents often contain false positives and data that require analysis. As is done with emissions, leak detection, and other regulations, the ability to shut down operations based on non-compliance or a perceived incident, impacts both the asset owner as well as the consumer.

- *Wall of Shame*—Unfortunately many regulatory programs in place use success metrics that include the percentage of industry fined or cited. Promotion of these metrics, as well as publishing details of asset owner operations and potential incidents, misses the original intention of securing OT in the critical infrastructure.

- *Financial Impacts*—The financial impacts of potential regulations can be identified in two areas. The compliance area that requires an investment of resources to change existing designs and controls to meet cybersecurity requirements, and the potential levied fine area to deal with issues of non-compliance.

A.3.5 Media

OT and OT security is a complex technical topic that is rarely conveyed in the media with scientific validity. The media often portrays technical topics, particularly cybersecurity, in a doomsday scenario directed toward gaining headline attention. Although this is not new, the ONG industry also faces an approach by the media that mischaracterizes both OT capabilities as well as the motivations to employ security. The ONG industry is often portrayed as ill-prepared, motivated by profit, and unsympathetic to the need to secure critical infrastructure. This is perhaps a perpetuation of the stigma associated with environmental impacts and the ONG industry, and the perceived lack of concern for natural resources.

The industry does face a new challenge. Atypical of the past, the media is presently used to promote the ideology of the Administration. Promotion of the Administration’s doomsday scenarios, need for regulation, and the general idea that the ONG is motivated solely by profit, result in an uphill climb for the industry to change the present perception. Facing not just negative public perception, but legislation and an Executive Order, the industry must increase awareness of the significant efforts they have made in the OT cyber security area.

A coordinated media campaign may be a solution to raising the public awareness of the significant efforts of the ONG industry underway to protect OT assets and to contribute to the security of the national critical infrastructure. Asset owners have engaged in technical collaboration and advanced research projects, drafted best practices, and developed comprehensive OT security programs at their organizations. These remain unknown by the public as there is an absence of press on ONG cyber security efforts and a lack of positive press on the ONG industry's preparedness.

A.3.6 Industry Impacts

The research identified two major impacts on the industry at this time. First, based on interviews and conference proceedings, the C-level lacks a comprehensive awareness of OT logical and technical topics. They tend to be more aware of enterprise cybersecurity issues and needs. This may be a result of their daily interaction with enterprise systems which they generally do not have for OT systems.

The second major observation is that organizations have either stopped or significantly slowed the amount of funds being allocated to OT cybersecurity. The curtailing of funds coincided with the announcement of pending regulations. The organizations appear to be hesitant to fund infrastructure changes that may not align with pending regulations. The research also indicates that some organizations may only be willing to fund OT cybersecurity system changes to meet minimum regulatory requirements. The regulations will establish the minimum spending bar.

Bibliography

General Bibliography

[1] AGA. (2004). *Cryptographic Protection of SCADA Communications; Part 1: Background, Policies and Test Plan.* American Gas Association.

[2] Agency, U. E. (2012, October 18). *US Environmental Protection Agency*. Retrieved from http://www.epa.gov/compliance/resources/cases/civil/caa/oil/

[3] Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems.* Canada: John Wiley & Sons, Inc.

[4] ANSI. (October 29,2007). *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models.* American National Standard, ANSI/ISA-99.00.01-2007.

[5] ANSI-1. (March 28, 2001). *Identification of Emergency Shutdwon Systems and Controls That ARe Critical to Maintaining Safety in Process INdustries.* American National Standard ANSI/ISA 91.00.01.

[6] API-1. (June 2012). *Developing a Pipeline Supervisory Control Center: API Recommended Practice 1113.* American Petroleum Institute.

[7] API-2. (June 2009). *Pipeline SCADA Security Standard, API Standard 1164 Second Edition.* American Pertroleum Institute.

[8] Bain, B. (2009, May 13). *Information-sharing platform hacked*. Retrieved from Federal Computer Week: http://fcw.com/Articles/2009/05/13/Web-DHS-HSIN-intrusion-hack.aspx

[9] Beauchesne, A. M. (2012, 10 18). *More Regulation Isn't the Answer*. Retrieved from New York Times - Room for Debate: http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/more-regulation-isnt-the-answer

[10] Black, P. E., Scarfone, K., & Souppaya, M. (2008, July 22). *Cyber Security Metrics and Measures.* Retrieved from xlinux.nist.gov: http://xlinux.nist.gov/~black/Papers/cyberSecurityMetrics2007proof.pdf

[11] Blakeman, B. B. (2012, 2). *PolicyMic.* Retrieved from http://www.policymic.com/debates/4652

[12] Blue, R. (2011, 4 27). "The Fiscal Impact of the Offshore Drilling Moratorium", Brief Analysis No. 743. *National Center for Policy Analysis*. Blue, Rob. "The Fiscal Impact of the Offshore Drilling Moratorium". Brief Analysis No. 743. National Center for Policy Analysis. April 27, 2011.

[13] Boman, K. (2012, October 29). *Middle East Attacks Highlight Cybersecurity Trheat for O&G Industry*. Retrieved from Rigzone: http://www.rigzone.com/news/oil_gas/a/121596/Middle_East_Attacks_Highlight_Cybersecurity_Threat_for_OG_Industry

[14] Boyer, W., & McQueen, M. (2012, October 29). *Ideal Based Cyber Security Technical Metrics for Control Systems.* Retrieved from www.if.uidaho.edu: http://www.if.uidaho.edu/~amm/faculty/Ideal%20Based%20Cyber%20Security%20Technical%20Metrics%20for%20Control%20Systems.pdf

[15] Bradley, T. (2010). *PCWorld*. Retrieved from http://pcworld.about.net/od/securit1/Critical-Infrastructure-under.htm

[16] Brennan, J. O. (2012, 4 15). *Washington Post.* Retrieved from http://www.washingtonpost.com: http://www.washingtonpost.com/opinions/time-to-protect-against-dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html

[17] Brown, K. A. (June 2006). *“A Brief History of Critical Infrastructure.* Spectrum Publishing Group, Inc. Retrieved from Brown, Kathi Ann, “A Brief History of Critical Infrastructure,” Spectrum Publishing Group, Inc, June 2006.

[18] Brumfield, C. (2012, 12 3). *New Cybersecurity Executive Order is Business-Friendly, Far Less Regulatory*. Retrieved from DigitalCrazyTown: http://www.digitalcrazytown.com/2012/12/new-cybersecurity-executive-order-is.html

[19] Bucci, S. (2012). *Heritage.org*. Retrieved from http://blog.heritage.org/2012/06/01/stuxnet-revelation-continues-obama-administration-trend-of-classified-leaks/

[20] Bumiller, E. (2012, 10 12). *NY Times.* Retrieved from http//www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0

[21] Cekuta, R. F. (2012, 2 6). *US State Department*. Retrieved from http://www.state.gov/e/enr/rls/rem/2012/183875.htm

[22] CFR195. (n.d.). Code of Federal Regulation 195. *Transportation of Hazardous Liquids by Pipeline*. United States of America.

[23] Chambliss, S. (2012, 6 28). *Press Release*. Retrieved from The Cedartown Standard: http://cedartownstd.com/view/full_story/19127211/article-Senators-renew-push-to-strengthen-cyber-security?instance=home_news_lead_story

[24] Clancy, M. (2012, August 1). First: Define critical infrastructure. *First: Define critical infrastructure*. SC Magazine.

[25] Clayton, M. (2012, 5 17). *Cybersecurity: How US utilities passed up chance to protect their networks* . Retrieved from Christian Science Monitor: http://www.csmonitor.com/USA/2012/0517/Cybersecurity-How-US-utilities-passed-up-chance-to-protect-their-networks

[26] Clinton, L. (2012, 10 22). *Exaggeration Unfairly Shifts Responsibility*. Retrieved from New York Times - Room for Debate: http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/exaggerating-threats-shifts-responsibility-to-busines

[27] Cole, P. (2012, 10 22). *Chemical Facility Security News*. Retrieved from http://chemical-facility-security-news.blogspot.com/feeds/posts/default

[28] Cox, R., & Martinez, J. (2012, 8 2). *The Hill*. Retrieved from http://thehill.com/blogs/hillicon-valley/technology/241851-cybersecurity-act-fails-to-advance-in-senate

[29] Daya, B. (2012, November 20). *http://web.mit.edu/~bdaya/www/Network%20Security.pdf.* Retrieved from http://web.mit.edu: http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[30] DD. (2012, September 20). *The Daily Dot*. Retrieved from The Daily Dot: http://www.dailydot.com/news/cybersecurity-executive-order-obama-close

[31] Defense, D. o. (2011). *Departmetn of Defense Strategy for Operating in Cyberspace.* Washington: Department of Defense.

[32] Dekker, M. (1997, November 20). *http://www.cert.org/encyc_article/tocencyc.html#History.* Retrieved from http://www.cert.org/: http://www.cert.org/encyc_article/tocencyc.html#History

[33] Dempsey, M., & Brown, K. (2012, 4 26). *Senate Press Release*. Retrieved from http://epw.senate.gov/public/index.cfm?FuseAction=Minority.PressReleases&ContentRecord_id=ef0e7a3f-802a-23ad-4255-2211799f6cf5

[34] DHS-1. (September 2009). *Department of Homeland Security: Cyber Security Procurement Language for Control Systems.* Department of Homeland Security, Control System Security Program, National Cyber Security Division.

[35] Disaster Resource Guide. (2012). *Disaster Resouce Guide's Continuity e-Guide*. Retrieved from http://www.disaster-resource.com/index.php?option=com_content&view=article&Itemid=1230&id=921:e-guide-landing-pages-template&catid=76:

[36] DOT-1. (n.d.). *Pipeline Safety: Control Room Management/Human Factors,".* Department of Transportation, Pipeline and Hazardous Material Safety Administration, 49 CFR Parts 192 and 195.

[37] Engleman, E. (2012, 8 8). *Bloomberg.* Retrieved from http://www.bloomberg.com/l: http://www.bloomberg.com/news/2012-08-08/obama-considering-executive-branch-action-on-cybersecurity-plan.html

[38] ESCSWG. (2012, Ocober 18). *ieRoadmap*. Retrieved from www.controlsystemroadmap.net: https://www.controlsystemsroadmap.net/AboutUs/Pages/Working-Group.aspx

[39] Favino, I. N., Maesera, M., Guglielmi, M., Carcano, A., & Trombetta, a. A. (2010). Distributed Intrustion Detection System for SCADA Prototcols. In T. Moore, & S. Shenoi, *Critical Infrastrucutre Protection IV* (pp. 95 - 112). Springer.

[40] FoxNews. (2012, October 21). *FoxNews*. Retrieved from http://www.foxnews.com/politics/2012/10/21/inhofe-epa-punting-regs-until-after-election-that-pell-doom-for-jobs-economy/

[41] Gedalyahu, T. B. (2012, 10 21). *Israel National News.* Retrieved from http://www.israelnationalnews.com: http://www.israelnationalnews.com/News/News.aspx/161161

[42] Gillespie, S. (2013, February 17). *Safety Instrumented Systems*. Retrieved from http://www.idc-online.com/technical_references/pdfs/instrumentation/safety_instrumented_systems.pdf: http://www.idc-online.com/technical_references/pdfs/instrumentation/safety_instrumented_systems.pdf

[43] Goins, C. (2011, 3 21). *CNSNews*. Retrieved from http://cnsnews.com/news/article/19000-jobs-worth-11-billion-wages-lost-nationally-offshore-drilling-moratorium-imposed

[44] Goodman, S. E., & Lin, H. S. (2007). *Toward a Safer and More Secure Cyberspace.* Washington, DC: National Research Council and National Academy of Engineering.

[45] Greenburg, K. J. (2012, 10 22). *Juan Cole.* Retrieved from http://www.juancole.com: http://www.juancole.com/2012/10/big-brother-is-looking-for-a-cyber-attack-pretext-to-crack-down-greenberg.html

[46] Guenther, B., & Brammer, R. F. (June 2012). Advanced Cyber Security Center. *25th IEE Computer Security Foundations.* Cambridge: http://csf2012.seas.harvard.edu/.

[47] Gupta, U. (2012, December 2). *Top 5 Certifications for 2012*. Retrieved from Bank infor Security: http://www.bankinfosecurity.com/top-5-certifications-for-2012-a-4291/op-1

[48] Hearing. (2012). *Hearing Before The Subcommittee on Cybersecurity, Infrastrcuture Protection, and Security Technologies.* Washington: Committe on Homeland Security.

[49] Henrie, M., & Carpenter, P. (2006). Process Control Cyber-Security: A Case-Study with Design Proposals. *2006 IEEE/IAS Industrial & Commercial PowerSystems TEchncial Conference.* Detroit, MI: IEEE.

[50] Henrie, M., & Liddell, P. (2008, March 1). Quantifying Cyber Security Risk. *Control Engeering*.

[51] Herb, J. (2012). *The Hill*. Retrieved from http://thehill.com/blogs/defcon-hill/policy-and-strategy/230985-senate-dems-blast-leaks-about-iranian-cyberattacks

[52] History, C. (2012, October 18). *Texaco refinery, Port Arthur, Texas*. Retrieved from www.computerhistory.org: http://www.computerhistory.org/revolution/real-time-computing/6/130/543

[53] Holecko, P. (June 2008). Overview of Distributed Control Systems Fomalisms. *Advances in Electrical and Electronic Engineering*, 253-256.

[54] HR 624. (2013, 2 14). *HR 624*. Retrieved from THOMAS Locator: http://thomas.loc.gov

[55] I3P. (2012, October 18). *Institute for Information Infrastructure Protection*. Retrieved from www.thei2p.org: http://www.thei3p.org/about/index.html

[56] I3P. (2012). *Process Control Systems (PCS) Project Publications*. Retrieved from The I3P: http://www.thei3p.org/publications/project_detail.html?3

[57] ICS CERT. (2012). *ICS-ALERT-12-269-01P—GLEG AGORA SCADA+ EXPLOIT PACK .* US Department of Homeland Security.

[58] IEC-1. (2003). *Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1 .* International Electrotechnical Commission, IEC61511-2.

[59] IEEE-1. (2012, October 20). *IEEE Technology Navigator*. Retrieved from IEEE: http://technav.ieee.org/tag/1489/scada

[60] Impellizzeri, P. (2012, June 21). *Bluegrass Institute*. Retrieved from http://www.bipps.org/epas-most-devastating-edict-stands-kentucky-to-pay-the-cost/

[61] Impellizzeri, P. (2012, June 22). *Bluegrass Institute*. Retrieved from http://www.bipps.org/750-layoffs-follow-the-epas-most-devastating-new-regulation/

[62] Industry, O. (2012). ONG Industry Members. (A. McIntyre, Interviewer)

[63] Infragard. (2012). *About Infragard*. Retrieved from Infragard: http://www.infragard.net/about.php?mn=1&sm=1-0

[64] INGAA. (2011). *Control Systems Cyber Security Guidelines for the Natual Gas Pipeline Industry.* Interstate Natural Gas Association of America.

[65] Innovation, M. A. (2012, December 24). *Measure Your Technology Against the World's Best*. Retrieved from Special Meritorious Awards for Engineering Innovation: http://www.epmag.com/mea/mea.process.php

[66] Inserra, D. (2013, 2 12). *Cybersecurity Executive Order Is a Mistake Every Way You Look at It*. Retrieved from The Foundry: http://blog.heritage.org/2013/02/12/cybersecurity-executive-order-is-a-mistake-every-way-you-look-at-it/

[67] Institute for Energy Research. (2012). *Presidential Debate Fact Check.* Retrieved from http://www.instituteforenergyresearch.org/wp-content/uploads/2012/10/Obama-Romney-Debate-on-energy.pdf

[68] Institute, A. P. (2012, December 24). *E & P ONshore Safety*. Retrieved from Events & Training: http://www.api.org/events-and-training/api-worksafe/e-and-p-onshore-safety.aspx

[69] ISA-1. (2002). *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 1: Introduction.* Instrument Society of American, ISA-TRA84.00.02.2002 – Part .

[70] ISA-2. (2012, October 14). *Measurement and Control Basics,"* . Retrieved from www.isa.org: http://www.isa.org/Template.cfm?Section=Books3&template=Ecommerce/FileDisplay.cfm&ProductID=8879&file=ACFF375.pdf

[71] ISA-3. (October 14, 2012). *Security for industrial automation and control systems; System Cybersecurity Conformance Metrics Draft 5, Edit 7.* Research Triangle Park: International Society of Autmoation .

[72] Jackson, W. (2011, 3 17). Retrieved from http://defensesystems.com/articles/2011/03/17/critical-infrastructure-vulnerable-to-attack.aspx

[73] James A. Baker III Institute for Public Policy of Rice University. (2012, September). *Cybersecurity Issues and Policy Options for the U. S. Energy Industry*. Retrieved from http://www.bakerinstitute.org/publications/IT-pub-PolicyReport53.pdf

[74] Joe St Sauver, P. (2004, December 7). *SCADA Security and Critical Infrastruture.* Retrieved from www.sans.org/.../security-critical-infrastructure-scada-systems_1644

[75] Kaspersky. (2012). *Kaspersky Lab*. Retrieved from http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected

[76] Kelly, S. (2012, 7 4). *CNN.* Retrieved from http://security.blogs.cnn.com/: http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/?iref=allsearch

[77] Kirk, J. (2011, 3 26). *TechWorld*. Retrieved from http://www.techworld.com.au/article/381042/russian_security_team_upgrade_scada_exploit_tool/

[78] Koenig, D. (2012). *TheProphetic Years.* Retrieved from http://www.thepropheticyears.com/comments/imminent_danger_7_cyber_attack.htm

[79] Krebs, B. (2003, February 14). A Short History of Computer Viruses and Attacks. Washington , District Of Columbia, United States of American.

[80] Lawson, S. (2012, 10 16). *Forbes.* Retrieved from http://www.forbes.com/: http://www.forbes.com/sites/seanlawson/2012/10/16/of-cyber-doom-dots-and-distractions/

[81] Lewin, R. (1999). *Complexity: Life at the Edge of Chaos.* Chicago: The Unversity of Chicago Press.

[82] Liu, A. (2011). *FoxNews*. Retrieved from http://www.foxnews.com/tech/2011/03/22/major-industries-vulnerable-cyber-attack/#ixzz291zearZW

[83] Lukasik, S. J. (1998, January). "Review and Analysis of the Report of the Presidents' Commission of Critical Infrastructure Protection,. *"Review and Analysis of the Report of the Presidents' Commission of Critical Infrastructure Protection,*. Center For International Security And Cooperation, Stanford University.

[84] Lyngsby, C. (2012, 11 12). *Threat of 'Spectacular' Cyberattack Looms: Official*. Retrieved from CNBC: http://www.cnbc.com/id/49853917

[85] Masnick, M. (2012, 9 14). *TechDirt*. Retrieved from http://www.techdirt.com/articles/20120914/19280020390/leaked-heres-white-houses-draft-cybersecurity-executive-order.shtml

[86] McCain, J., Hutchison, K., & Chambliss, S. (2012, 9 13). *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10000872396390444017504577647131630683076.html

[87] McIntyre, A. (2007). Cyber Security for Process Control Systems. *API Pipeline Conference.* Albuquerque: American Petroleum Institute.

[88] McIntyre, A. (2009, November). Final Institute Report Refines, Forecasts Cyber-Security Issues. *Oil & Gas Journal*.

[89] McIntyre, A. (2010). Emerging Risk Assessment Options. *API Pipeline Conference & Cybernetics Symposium.* New Orleans: American Petroleum Institute.

[90] McIntyre, A., & Stamp, J. (2008). I3P Security Forum: Connecting the Business and Process Control System Networks. *API IT Security Conference.* Houston: American Petroleum Institute.

[91] McIntyre, A., Becker, B., & Halbgewachs, R. (2007, September). *Security Metrics for Process Control Systems.* Retrieved from energy.gov: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/18-Security_Metrics_for_CS.pdf

[92] McIntyre, A., Cook, B., Stamp, J., & Lanzone, A. (2006, October). Workshop Identifies Threats to Process Control Systems. *Oil & Gas Journal*.

[93] McQueen, M., Boyer, W., McBride, S., Farrar, M., & Tudor, Z. (2008, January). *Measurable Control System Security Through Ideal Driven Technical Metrics.* Retrieved from www.inl.gov: Idaho National Laboratory Report to the Department of Homeland Security, INL/EXT-06- 12016, Cyber Security Metrics, December 2006.

[94] Melvin, J. (2012, 8 1). *Chicago Tribune*. Retrieved from http://articles.chicagotribune.com/2012-08-01/business/sns-rt-usa-securitycyberl2e8j1jan-20120801_1_cybersecurity-bill-senate-version-general-keith-alexander

[95] Miller, K. (2012, 10 12). Retrieved from http://www.securityinfowatch.com/news/10813806/senators-opposed-to-cybersecurity-executive-order

[96] Miller, K. (2012, 10 12). *Security Info Watch*. Retrieved from http://www.securityinfowatch.com/news/10813806/senators-opposed-to-cybersecurity-executive-order

[97] Mitchell, T. (2013, August 15). *Risk of smart grid security breaches higher than ever*. Retrieved from www.fiercesmartgrid.com: http://www.fiercesmartgrid.com/story/risk-smart-grid-security-breaches-higher-ever/2012-08-15?page=0,0

[98] Morgan, C. (2012, 10 19). *StorageCraft.* Retrieved from http://www.storagecraft.com: http://www.storagecraft.com/blog/america-danger-cyber-attack/

[99] Morin, E. (2008). *On Complexity.* Dreskill, New Jersey: Hampton Press, Inc.

[100] Moscaritiolo, a. (2010). Retrieved from http://www.scmagazine.com/critical-infrastructure-lacking-cyber-supply-chain-security/article/191735/

[101] NBCNews. (2012). *Son of Stuxnet Virus Could be Used to Attack Critical Computers Worldwide*. Retrieved from http://redtape.nbcnews.com/_news/2011/10/18/8384786-son-of-stuxnet-virus-could-be-used-to-attack-critical-computers-worldwide?lite

[102] NCS. (October 2004). *Technical Information Bulleting 04-1, Supervisory Control and Data Acquisiton (SCADA) Systems.* Office of the Manager National Communications Systems.

[103] Nieuwenhuijs, A., Luijf, E., & Klaver, M. (2008). Modeling Dependecies in Critical Infrastructure. In M. P. Shenoi, *Critical Infrastructure Protection II* (pp. 205-214). New York, New York: Springer.

[104] NIST. (2011). *Buide to INdustrial Control Systems (ICS) Security.* National Institute of Standards and Technology, U. S. Department of Commerce, Special Publication 800-82.

[105] Nobvosti, & Guneeu. (2012, 6 6). *RT.* Retrieved from http://rt.com/news/kaspersky-fears-cyber-pandemic-170

[106] NSTAC. (May 21, 2009). *Cybersecurity Collaboration Report; Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detectioon, Prevention, Mitigation, and Response Capability.* President's National Security Telecommunications Advisory Committee.

[107] NTSB. (2005). *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines.* National Transportation Safety Bureau, PB2005-917005, Notationa 7505A.

[108] NTSB-1. (2005). *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines; Safety Study,NTSB/SS-05/02 .* National Transportation Safety Board, PB2005-917005, Notation 7505A.

[109] Obama, B. (2012, 7 20). *US Embassy*. Retrieved from http://translations.state.gov/st/english/article/2012/07/201207209392.html?CP.rss=true#axzz2A4ghh42X

[110] Office of the Press Secretary. (2013, 2 12). *PRESIDENTIAL POLICY DIRECTIVE/PPD-21*. Retrieved from Federation of American Scientists: http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf

[111] PAC. (2006). *Instrumentation & Control; Process Control fundamentals*. Retrieved from PAControl: www.pacontrol.com

[112] Palmer, B. (2012, 4 27). *Slate.* Retrieved from http://www.slate.com/: http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html

[113] Parfomak, P. W. (August 16, 2012). *Pipeline Cybersecurity: Federal Policy.* Congressional Research Service 7-5700, R4260.

[114] Parker, K. (2010, February 26). *Automation/IT convergence vision meets cyber-security reality*. Retrieved from www.epmag.com: http://www.epmag.com/Production-Field-Development/Automation-IT-convergence-vision-meets-cyber-security-reality_54960

[115] Peterson, J. (2012, 2 20). *Daily Caller*. Retrieved from http://dailycaller.com/2012/02/20/mccain-promises-gop-alternative-to-super-regulator-cybersecurity-bill/

[116] Pietrzyk, A., Root, B., & Gruhn, P. (2012, October 19). *Designing a Control System for High Availability.* Retrieved from www.isa.org: www.isa.org/FileStore/Intech/WhitePaper/High%20Availability.doc

[117] Prince, B. (2010, March 10). *Top IT Security Certifications That Will Get You a Raise*. Retrieved from eWeek: http://www.eweek.com/c/a/Security/Top-IT-Security-Certifications-That-Will-Get-You-a-Raise-233791/

[118] Rashid, F. (2012, 11 18). *Cybersecurity Bill Stalls Again, Executive Order Coming Soon?* Retrieved from PC Magazine: http://securitywatch.pcmag.com/none/305133-cybersecurity-bill-stalls-again-executive-order-coming-soon

[119] Rausnitz, Z. (2012, September 21). *Baker: DHS should borrow cyber experts from NSA*. Retrieved from http://www.fiercehomelandsecurity.com: http://www.fiercehomelandsecurity.com/story/baker-dhs-should-borrow-cyber-experts-nsa/2012-09-21

[120] Ryan, M. (2012, 6 19). *BizJournals*. Retrieved from www.bizjournals.com: http://www.bizjournals.com/houston/morning_call/2012/06/atp-sues-us-government-for-deepwater.html

[121] Sanger, D. (2012). *NYTimes*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&ref=todayspaper

[122] Santos, J., & Popkin, J. (2012, October 22). *IT/OT Convergence and Implications*. Retrieved from www.gartner.com: http://www.gartner.com/DisplayDocument?doc_cd=200630&ref=g_noreg ID: G00206362

[123] Schwartz, M. J. (2013, 2 14). *CISPA Cybersecurity Bill, Reborn: 6 Key Facts*. Retrieved from InformationWeek Security: http://www.informationweek.com/security/cybercrime/cispa-cybersecurity-bill-reborn-6-key-fa/240148600

[124] Senate 2102. (2012). *THOMAS*. Retrieved from Library of Congress: http://thomas.loc.gov/home/thomas.php

[125] Senate 2105. (2012). *THOMAS*. Retrieved from Library of Congress: http://thomas.loc.gov/home/thomas.php

[126] Senate 2151. (2012). *THOMAS*. Retrieved from Library of Congress: http://thomas.loc.gov/home/thomas.php

[127] Senate 3342. (2012). *THOMAS*. Retrieved from Library of Congress: http://thomas.loc.gov/home/thomas.php

[128] Senate 3414. (2012). *THOMAS*. Retrieved from Library of Congress: http://thomas.loc.gov

[129] Shaw, W. T. (2006). *Cybersecurity for SCADA Systems.* Penwell.

[130] Sider, A., Clark, K., & Singh, F. (2012, August 7). *Chevron Refinery Fire Out: Markets Brace for Impcat*. Retrieved from Walstreet Journal: http://online.wsj.com/article/SB10000872396390443792604577575100790843414.html

[131] Silverstein, & Sahimi. (2012). *The Guardian*. Retrieved from http://www.guardian.co.uk/commentisfree/2012/jun/08/obama-virus-wars-mutually-assurred-cyberdestruction

[132] Smith. (2012). *NetworkWorld*. Retrieved from http://www.networkworld.com/community/blog/cyber-sabatoge-feds-investigate-who-leaked-stuxnet-cyberattack-iran

[133] Solar, I. I. (2012, January 5). *Chevron loses $18bn appeal for environmental damage in Ecuador*. Retrieved from In the Media: http://digitaljournal.com/article/317330

[134] Sridhar, S. (25-29 July 2010). Data integrity attacks and their impacts on SCADA control systems. *Power and Energy Society General Meeting, 2010 IEEE* (pp. 1-6). IEEXplore.

[135] Stevens, N. (2012, 6 28). *RedState*. Retrieved from http://www.redstate.com/neil_stevens/2012/07/28/tech-at-night-republicans-to-try-to-fix-lieberman-collins-cybersecurity-bill/

[136] Symantec. (2012, 8 16). *Shamoon*. Retrieved from http://www.symantec.com/connect/blogs/shamoon-attacks

[137] Symantec. (2012). *Stuxnet Dossier*. Retrieved from www.symantec.com: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[138] Symantec. (2012). *W32.Duqu*. Retrieved from http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

[139] Symantec. (2012). *W32.Stuxnet*. Retrieved from http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

[140] Torgerson, M. (2007). Security Metrics. *International Command and Control Research and Technology Symposia (ICCRTS).* Newport, RI: The Command and Control Center Research Program.

[141] TSA. (2010). *Pipeline Security Guidelines.* Transportation Security Administation.

[142] Tudor, Z., & Fabro, m. (2012). What Went Wrong? A Study of Actual Industrial Cyber Security Incidents. *ISCJWG 20120 Spring Conference.* SRI International.

[143] US CERT. (2012). *Control Systems Cyber Security Program (CSSP) Industrial Control Systems Joint Working Group (ICSJWG)*. Retrieved from US CERT: http://www.us-cert.gov/control_systems/icsjwg/

[144] US CERT. (2012). *Control Systems Security Program (CSSP) Industrial Control Systems Cyber Emergency Response Team*. Retrieved from US CERT: http://www.us-cert.gov/control_systems/ics-cert/

[145] US CERT/ ICS CERT. (2012). *Joint Security Awareness Report- JSAR-12-243-01.* US Department of Homeland Security.

[146] US Department of Homeland Security. (2009, June). *Primer Control Systems Cyber Security Framework and Technical Metrics.* Retrieved from www.us-cert.gov: http://www.us-cert.gov/control_systems/pdf/Metrics_primer_v9_7-13-09_FINAL.pdf

[147] US Department of Homeland Security. (2012). *Homeland Security Information Network*. Retrieved from US Department of Homeland Security: http://www.dhs.gov/homeland-security-information-network

[148] US Department of Homeland Security. (2012). *LOGIIC – Linking the Oil and Gas Industry to Improve Cyber Security*. Retrieved from DHS Science and Technology Directorate: http://www.cyber.st.dhs.gov/logiic/

[149] White House Press Secretary. (2013, 2 12). *Executive Order -- Improving Critical Infrastructure Cybersecurity*. Retrieved from White House: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[150] Williams, M. (2012, 10 12). *ComputerWorld.* Retrieved from http://www.computerworld.com/: http://www.computerworld.com/s/article/9232317/Future_cyber_attacks_could_rival_9_11_cripple_US_warns_Panetta

[151] Wyborne, M. N., Austin, M. F., & Palmer, C. C. (2009). *National ICyber Security: Research and Development Challenges.* Hanover: Institute for Information Infrastructure Protection.

[152] York, F. (2011, November 18). *EPA Abuse*. Retrieved from http://epaabuse.com/2978/editorials/senators-try-4th-time-to-get-response-from-epa/

[153] Yost, P. (2012). *The Times-Picayune*. Retrieved from http://www.nola.com/politics/index.ssf/2012/06/us_attorney_general_eric_holde_1.html

[154] Zakon, R. H. (2012, November 20). *Hobbes' Internet Timeline 10.2.* Retrieved from http://www.zakon.org/robert: http://www.zakon.org/robert/internet/timeline/

[155] Zetter, K. (2012). *Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers*. Retrieved from http://www.wired.com/threatlevel/2012/05/flame

[156] Zetter, K. (2012). *Wired*. Retrieved from http://www.wired.com/threatlevel/2012/06/stuxnet-leak-investigation/

[157] Zubairi, J. A., & Mahboob, A. (2012). *Cyber Security Standards, Practices and Industrial Applications; Systems and Methodologies.* Information Science Reference, ISBN 978-1-60960-851-4.

Cybersecurity Standards/Guides Listing

[158] American Gas Association, *Cryptographic Protection for SCADA Communications General Recommendations*, 12, March 2006

[159] American National Standards/International Standards Organization, *Security Technologies for Manufacturing and Control Systems*, TR99.00.01-2007, Third edition, November 2007

[160] American National Standards/International Standards Organization, Report, *Integrating Electronic Security into the Manufacturing and Control Systems Environment*, TR99.00.02-2009, Second edition, 2009

[161] American Petroleum Institute, Standard 1164, *Pipeline SCADA Security*, Second edition, June 2009

[162] American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, Third edition, April 2005

[163] Department of Homeland Security, Guideline, *Catalog of Control Systems Security: Recommendations for Standards Developers*, First edition, September 2009

[164] Department of Homeland Security, *Department of Homeland Security: Cybersecurity Procurement Language for Control Systems*, First edition, September 2009

[165] International Organization for Standardization, *Information Technology – Code of practice for information security management*, ISO/IEC-17799:2005, First edition, June 2005

[166] International Organization for Standardization, *Information Technology – Code of practice for Security techniques – Information security management systems - Requirements*, ISO/IEC-27001, Third edition, July 2007

[167] Interstate Natural Gas Association of America, *Control Systems Cybersecurity for the Natural Gas Pipeline Industry*, First edition, January 2011

[168] National Institute of Standards and Technology, *System Protection Profile for Industrial Control Systems*, First edition, May 2004

[169] National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, 800-82, June 2011

[170] Transportation Security Administration, *Pipeline Security Guidelines*, First edition, December 2012

[171] U.S. General Accounting Office (GAO), *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, First edition, March 2004

[172] UK National Centre for the Protection of National Infrastructure, *Good Practice Guide on Firewall Deployment for SCADA and Process Control Network*, First edition, February 2005

Federal Cybersecurity Regulations/Guidelines

These document are an expansion of an original source obtained from “Cybersecurity Standards, Practices and Industrial Applications; Systems and Methodologies,” Editors: Junaid Ahmend Zubairi & Athar Mahboob, Page 207-208

[173] *President’s Commission on Critical Infrastructure Protection (PCCIP) Formed*, 1996. PCCIP charter [is] to designate critical infrastructures, to assess their vulnerabilities, etc.

[174] *Critical Foundations: Protecting America’s Infrastructure, President’s Commission on Critical Infrastructure Protection (PCCIP)*, 1997, Report. Report on infrastructure vulnerabilities, etc.

[175] *Presidential Decision Directive/NSC – 63,* White House, 1998, Policy. Initiates development of a National Infrastructure Assurance Plan, requires all Federal department and agency to develop a plan for protecting its own critical infrastructure. Appoints a Lead Agency senior officer for each Critical Infrastructure as that Sector's Liaison Official

[176] *Aviation and Transportation Security Act (P.L. 107-71),* 107th Congress, *2001*, Public Law. Established the Transportation Security Administration (TSA), within DOT and authorized TSA "…to issue, rescind, and revise such regulations as are necessary to carry out its functions

[177] *Homeland Security Act of 2002 (P.L. 107-296),* 107th Congress, 2002, Public Law. Created the Department of Homeland Security (DHS) and transferred TSA under DHS

[178] *National Strategy to Secure Cyberspace*, DHS, 2003, Report. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.

[179] H*omeland Security Presidential Directive-7, Presidential Directive*, 2003, Policy. Directs DHS, in coordination with other sector-specific agencies, for identification of and prioritizing for protection of critical infrastructure and to prepare a national plan to protect the infrastructure to include coordination and participation with the private sector. Replaces PDD-63.

[180] *Critical Infrastructure Protection: Challenges and Efforts to secure Control Systems*, General Accounting Office (GAO): GAO – 04-354, 2004, Advisory. Recommends DHS develop and implement a strategy to coordinate efforts to meet challenges associated with security control systems and current efforts for both the federal and private sector

[181] *National Infrastructure Protection Plan*, DHS, 2006, Plan. Provides the overarching planning process and structure for security partnerships and federal/private sector response to protect critical infrastructure.

[182] *Commission Act of 2007* (P.L. 110-53), 2007. Directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate.

[183] *Sector Specific Plans, SSA*, 2007, Plan. All Sector Specific Agencies (SSAs) in coordination with SCCs were directed to complete plans within the NIPP partnership framework by 2006. These provide high level assessment, goals, and objectives for infrastructure protection.

[184] *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO – 07-1036, 2007 , Advisory. Recommends DHS develop a coordination strategy for public and private sectors and process for improving information sharing

[185] *Toward a Safer and More Secure Cyberspace*, NRC, 2007, Advisory. The National Research Council (NRC) conducted a study on research priorities for security cyberspace. Control systems issues were included in their scope.

[186] NSPD-54/HSPD-23, Presidential Directive, 2008, Policy. Mandatory intrusion detection requirements for federal facilities.

[187] *Pipeline Security Guidelines*, TSA, 2011, Guideline.

[188] CIP PPD, Proposed Presidential Directive, 2012, Proposal. White House Proposal

[189] *Cybersecurity Act of 2012*, 2012, Proposal. 112th Congress

AMERICAN PETROLEUM INSTITUTE

1220 L Street, NW
Washington, DC 20005-4070
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

Phone Orders:	1-800-854-7179	(Toll-free in the U.S. and Canada)
	303-397-7956	(Local and International)
Fax Orders:	303-397-2740	

Information about API publications, programs and services is available on the web at www.api.org.