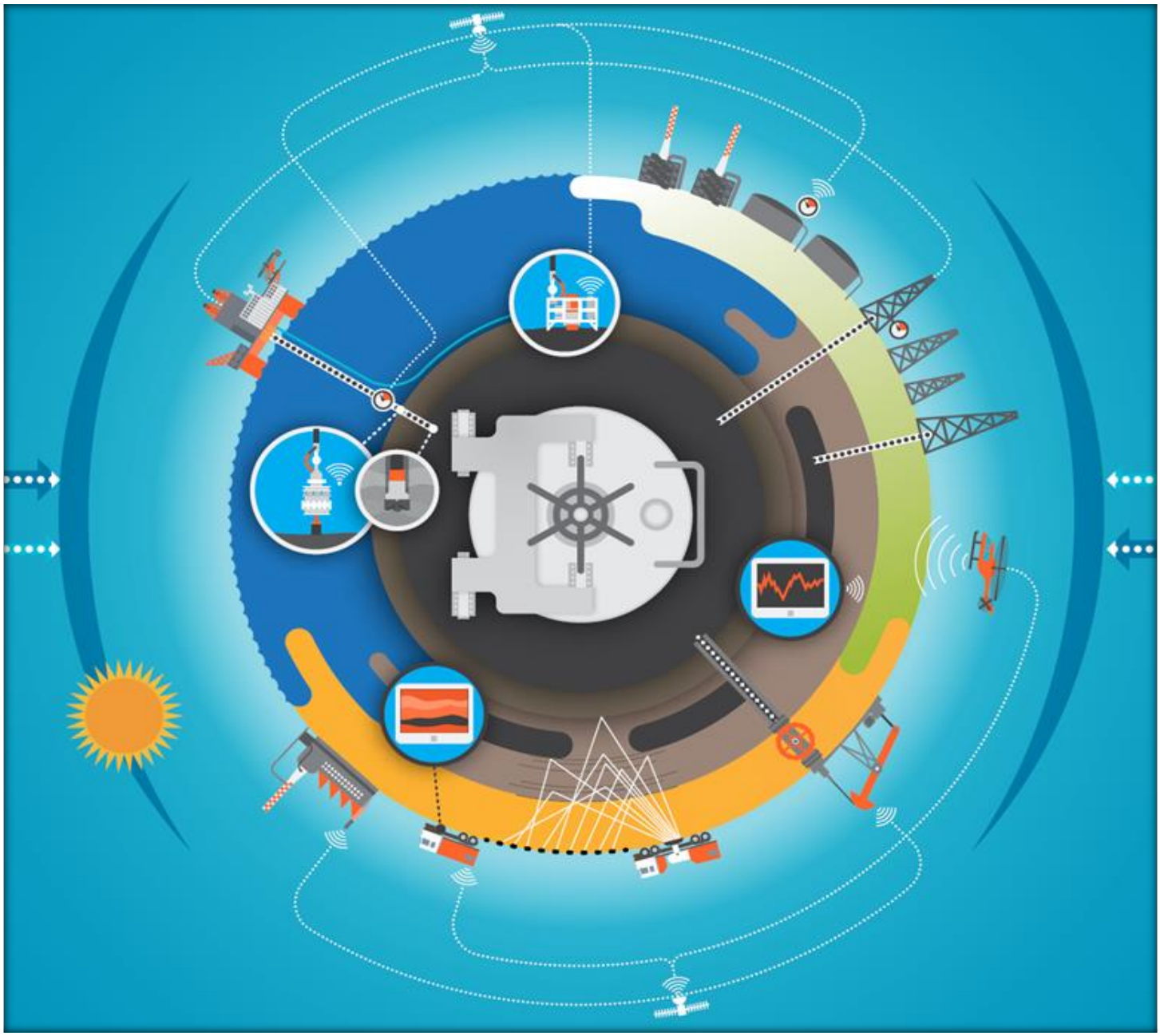
Protecting *Cybersecurity and Resiliency* of *U.S. Critical Infrastructure* - Energy, Oil & Gas



Research Published – Dec 15th, 2018

Best practices for Cybersecurity of top-priority infrastructure across USA

A research report & whitepaper by

Anil Lamba, (Ph.D. Cyber Security, CISA, CDPPM)

Author

Anil Lamba is an industry speaker, researcher and an experienced professional with impressive industry credentials and proven success in spearheading Strategic Initiatives, IT Security Advisory & Risk Mgmt. Projects, Complex Information Security Audits & Governance Initiatives, Regulatory & Industry standard assessments, Large-scale IT Infrastructure projects across industry verticals.*

He has led various complex information security audits viz. Cybersecurity Assessments (NIST & FFIEC), IAM & Data Privacy Audits, PCI-DSS & ITGC Assessments, ISO27001 & Secure SDLC Audits, Enterprise Data Warehouse (Data Lake & Grid) Audits, Third-Party Risk Assessments, Cloud Security Audits, ITIL Implementation Assessment, BCP & DR Audits and Mobile Security audits. He is well versed in using top Vulnerability Management & Pen-Testing tools such as BurpSuite, MetaSploit, NmAp, Nessus, OpenVAS, WebInspect, Rest C. and PostMan.

Industry Credentials*: *Ph.D. Cyber Security, M.B.A. – Strategic Project Management, CISA ®, CISSP, CDCP, CPD, CFE, PMP, Amazon Web Services (AWS) Certified Architect, AZURE Certified, Prince2, ITIL Expert, ISO 27001 Lead Auditor, MCSE, 6σ Sigma Green Belt, CEH and CCNA.*

Research Report 

This research report & whitepaper establishes the foundation for the critical need of ***"Establishing Best practices of Cybersecurity and Resiliency for protecting nation's most critical infrastructure, viz. Energy, Oil & Gas".***

This report documents the current Cybersecurity gaps across Energy, Oil & Gas sector systems spread throughout US, highlights required security enhancements and recommendations to foster Cyber Security & Resiliency of our Nation's Critical Infrastructure.

I analyzed several previous research papers, studied the overall Cybersecurity posture of nation's critical infrastructure, made assessments on the information security aspects of these systems to identify gaps and come up with specific recommendations for the prevention and management of the top risks to ensure an impact-less and resilient environment.

My research concluded in November and this whitepaper was distributed in December 2018. It was shared in a major conference and over 1900 copies distributed in less than a quarter viz. 300+ CIO/ CISO, 1600+ Information Security officials and 50+ Energy Sector professionals. As a Ph.D. in Cybersecurity, Infrastructure Security is my passion and I will continue to give my applied knowledge contributions for all critical areas of our country (USA).

General Disclaimer

This research report & whitepaper was prepared by Anil Lamba for informational purposes only. The term "best practices" is used to reference practices which the authors currently believe to be generally accepted and recommended practices. Further, author do not make any express or implied warranty or representation concerning the information contained in this presentation, or as to merchantability or fitness for a particular purpose or function.

The intended audience for this guide includes Cybersecurity & information security professionals, and others that are interested in a detailed overview & comment on the highlights of Cybersecurity for the utility industry (Energy, Oil & Gas). It assumes a reasonable level of general network architecture and administration as well as basic understanding of the major components of Energy, Oil & Gas utility information and operations technology.

The guide is not meant to be comprehensive or to be used as the foundation for a robust and complete Cybersecurity program. Anil reserves the right to make changes to this research paper without further notice to anyone.

Credits

This whitepaper has been prepared following a review of the relevant literature, as well as various interviews with experts and professionals in the areas of energy and Cybersecurity in United States & Europe. I would like to thank all those who agreed to be interviewed for their support and the information they provided on this sensitive subject. Since the individuals who agreed to be interviewed have asked to remain anonymous, the information that derives from these interviews, and which was used to prepare this policy paper, has not been attributed.

Copyright

Published & Printed in the United States of America. Published, 2018; Distributed, 2019.

Document Number: CRTCLSECEOGCYPR6

Executive Summary

Protecting America's energy systems from cyber-attacks and other risks is a top national priority.

This Cybersecurity Research report identifies collaborative actions to reduce cyber risks in the U.S. energy sector. This research identifies the goals, objectives, and activities that can be pursued to reduce the risk of energy disruptions due to cyber incidents.

Reliable energy and power is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food and agriculture, emergency services, and more.

Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. As nation-states and criminals increasingly target energy networks, the Federal Government must help reduce cyber risks that could trigger a large-scale or prolonged energy disruption.

A multi-pronged approach to Cybersecurity preparedness is required. System operators must have the capacity to operate, maintain, and recover a system that will never be fully protected from cyber-attacks. Relevant issues that need to be addressed include cloud security, machine-to-machine information sharing, advanced Cybersecurity technologies, outcome-based regulation to avoid prolonged outages and increase system resilience, and international approaches to Cybersecurity.

Executive Order 13800 (EO 13800)

In 2017, President Trump issued Executive Order (E.O.) 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" because ***the risks of cyber threats to critical infrastructure are perceived as a national security imperative.***

E.O. 13800 called for an assessment of a prolonged electric power outage resulting from a cyberattack, and an evaluation of the "readiness and gaps in the United States' ability to manage and mitigate consequences of a cyber incident against the electric subsector." The cyber supply chain and public-private Cybersecurity information sharing were listed among a number of major Cybersecurity potential vulnerabilities.

The growing anxiety among United States policy-makers, and the American energy sector in particular, about cyberattacks on the nation's energy infrastructure was vividly underscored recently in a front page article in The Wall Street Journal headlined, 'U.S. Officials Push New Penalties for Hackers of Electrical Grid.

Widespread connection of Distributed Energy Resources (e.g. demand response, generation including from wind and solar, energy storage, and energy control devices) will increase digital complexity and attack surfaces, and therefore require more intensive Cybersecurity protection.

- Robust regulatory standards for Cybersecurity and privacy are needed for all components of an interconnected electricity network.
- To keep pace with rapidly evolving Cybersecurity threats against large and complex electric power systems, electric utilities, vendors, law enforcement authorities, and governments should share current cyber threat information and solutions quickly and effectively.

Abstract

With rare exceptions, energy & utilities (Oil & Gas) do an excellent job of managing traditional types of risks facing their operations. However, cyber security is the one category of risk that remains stubbornly opaque and resistant to attempts to manage, monitor, and measure. Determining the likelihood and severity of cyber security risks, as well as the efficacy of approaches to mitigate them, continues to be a challenge.

Cyber security for energy and utilities organizations

Cyber security is one of the most important policy and technology topics an organization must address. Critical infrastructure for energy and utilities is vital to personal safety, economic growth and national defense. There is growing interest in the topic from senior utility executives, regulators and customers around the world. But there are also legitimate concerns about ensuring that adequate resources and focus are directed to the task of securing critical infrastructure.

1. A Power Sector in Transition

The increasing digitalization of the power sector through the deployment of Information and communications technologies (ICTs) is also embodied in the rollout of advanced metering infrastructure and other network sensing infrastructure in the U.S. In the U.S., roughly 59 million smart meters have been deployed, covering over 40% of metered sites (EIA, 2016).

The widespread connection of solar, wind, demand-response, and other distributed energy resources with two-way digital controls increases cyber vulnerabilities and requires more widespread and intensive Cybersecurity protection. Utilities throughout the world are therefore focusing on resilience and preparation to contain and minimize the consequences of cyber incidents.

The increasingly widespread collection and, in certain markets, dissemination of energy production and consumption data is already causing privacy concerns and raising questions over who should own and manage this data.

A modern functioning society requires highly reliable electricity. Electric utilities are vulnerable to cyber and physical attack and will be more so in the next decade as utility systems have more digital and complex controls, and the same digital interconnectedness that increases efficiencies, increase risks. Connection of Distributed Energy Resources (**DERs**) will increase cyber vulnerabilities.

Protecting a nation's electricity grid from widespread cyber or physical attack or electromagnetic pulses are important national security issues, and require wise risk-based analysis and planning by electric utilities. Utilities throughout the world need resilience and contingency planning, to contain and minimize the consequences of cyber and physical incidents.

2. Envisioning a Future with Distributed Energy Resources: Cybersecurity, Resilience, and Privacy

Cybersecurity threats to the distribution system can be expected to challenge the industry for many decades. Throughout the world, utilities and non-utilities that interact with the grid need resilient systems and must be prepared to contain and minimize the consequences of cyber incidents.

Because an increasing quantity of private and corporate information will be gathered and stored by utilities and their affiliated companies, utilities of the future will need to address privacy challenges. Increased use of internet-connected devices in homes, offices, and industrial facilities will exacerbate these challenges, especially since many of these devices store their data in the cloud.

In a National Cybersecurity Summit, DHS Secretary Kirstjen M Nielsen said, ***'I believe that cyber threats collectively now exceed the danger of physical attacks against us'.***

3. The 'largest interconnected machine' in the world

To put the American threat into larger context, the US electricity grid, which has been referred to as the 'largest interconnected machine' in the world, consists of 'more than 7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of miles of low-voltage distribution lines.

In June, the President's National Infrastructure Advisory Council, which includes many energy sector leaders, said, ***'The US needs to prepare for a "catastrophic power outage"*** possibly caused by a cyberattack. 'Given the interconnected nature of critical systems and networks, new broad-scale approaches are needed to adequately prepare for, and respond to, and recover from catastrophic disasters that can create significant power outages with severe cascading impacts to multiple critical sectors.

4. The crippling of Ukrainian utilities

US electric utilities are not the only ones to have been targeted by cyber attackers. According to reporting in The Wall Street Journal, ***'Cyber hackers working for Russia crippled three Ukrainian utilities on Dec. 23, 2015, plunging hundreds of thousands of civilians into the darkness on a chilly winter's eve'.***

FERC, the independent regulator that supervises the North American Electric Reliability Corporation (NERC), has also become increasingly concerned about cyber threats. FERC has ordered NERC to expand cyber threat incident reporting by transmission operators and owners of power plants.

In this regard, former FERC Commissioner "Suedeen Kelly" has said the mandatory reporting of cyber incidents 'is an important step forward.

However, NERC and FERC rules apply only to large companies, *not small ones that have also been of interest to hackers.*

5. Security and compliance challenges

Whether assessing the threat of equipment failure or the potential for employee injuries, energy and utilities organizations have long been accustomed to managing operational risk. Now, as the transition to advanced communication, control and computing technologies accelerates, a new kind of operational risk is emerging. Now a days, more dynamic and integrated electricity production and delivery systems along with advanced metering infrastructure. Sensitive operations and personal data are now moving over common or integrated communications infrastructure, flowing in multiple directions within a dense, multi-nodal system.

By definition, a smart grid has more access points and multiple networked systems. As this positive transformation of operations continues, there is an impact on cyber security— a marked increase in the risks of cyber breaches.

Regulations covering data privacy and information security protections are becoming the norm around the world. Therefore, policy-making bodies have developed an increased interest in what energy & utilities are doing to meet the following challenges:

- Integrating information technology (IT) and operational technology (OT) networks due to grid modernization and other business initiatives
- Exposing both IT/OT networks to the Internet—either directly or indirectly, whether intended or not
- Mitigating threats to IT and OT systems from the widespread use of mobile devices, social media and easily portable USB drives, and lack of governance for the use of these tools in critical environments
- Eliminating internal threats posed by disgruntled employees and human error by authorized technicians
- Countering recent OT threat events, such as the emergence of Stuxnet, Flam and their variants on E&U programmable logic controllers (PLCs) and other control system equipment

There are increased expectations for the reporting of compliance with security and privacy directives. Scrutiny by federal agencies such as the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the Department of Energy (DOE) is likely to expand. Future versions of the NERCCIP standards promise to expand the scope and depth of utility compliance requirements.

6. Growing Concern

Most Americans probably don't give a lot of thought to critical infrastructure, even though it's something they rely on every day. The industry sectors that encompass the nation's critical infrastructure cover virtually every aspect of people's lives, including power generation, oil, gas, and manufacturing — to name a few.

In the digital era of the 21st century, securing the networks, systems and data in these sectors is of vital importance. But as the numerous compromises of the past few years have shown, a lot of work needs to be done to protect critical infrastructure organizations against increasingly sophisticated and targeted attacks.

Executives and boards of directors at many critical infrastructure organizations struggle to understand and address the risks they face. At the same time, they must deal with a complex security ecosystem that includes vendors, business partners, government and industry regulatory bodies, customers, and other entities.

There is a growing consensus among many of these corporate leaders that little can be done to block intrusions except to stand by and keep an eye out for them. But this reactive approach invites potential disaster.

Preventative, proactive, and robust Cybersecurity protects critical infrastructure organizations across multiple sectors. By extension, it also protects their employees, customers, business partners, and others.

This research report & whitepaper offers best practices that can help IT and security executives at these organizations deliver the protection they need.

7. What Is Critical Infrastructure and Why Is It So Vital?

Critical Infrastructure represents a national security vulnerability that is not within the direct purview of the U.S. government. ***Any cyberattack against an organization that provides critical infrastructure products or services presents a potentially significant risk to the American public.***

Rather than being a simple subject of data security, public safety issues are at stake. The people who lead the organizations in these industries have a keen understanding of the need for safety to protect employees, and in many cases, customers, as well as the people residing near their facilities.

Depending on the organizations involved in an attack, and the extent of the attack, there could be significant national security implications.

According to the U.S. Department of Homeland Security (DHS), the nation's critical infrastructure ***"provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health.*** We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family."

In all, ***the DHS considers 16 sectors to be part of the critical infrastructure.*** These include, but are not limited to, chemicals, communications, defense, emergency services, ***energy***, food and agriculture, government, healthcare, manufacturing, and transportation.

The incapacitation or destruction of systems and networks operated by organizations in these industries could have a debilitating and potentially monumental impact on other business or government agency Cybersecurity systems, economic security, national public health or safety, or any combination thereof, according to DHS.

For example, if the power grid for part or all of the country were to be shut down for a substantial period, that would affect hundreds of millions of individuals as well as businesses and other organizations throughout the world.

In December 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The disruption was due to a third party's illegal entry into and attack against its computer and SCADA systems. ***The outages caused about 225,000 customers across various areas to lose power.***

The power grid breach provides a real-world example of how critical infrastructure attacks can cause large-scale disruption, and illustrates how similar incidents could happen elsewhere without adequate protection in place.

8. Outdated Defenses and a Complex Ecosystem

Despite the urgent need for strong security measures at critical infrastructure organizations, many continue to struggle to protect their systems and data against attacks. In a lot of cases, business and technology leaders don't thoroughly grasp the seriousness of the threats they face and all the ways in which these threats might target their systems and networks.

Many critical infrastructure organizations still rely solely on traditional security offerings such as signature-based anti-malware products and firewalls, thinking that those solutions will provide an adequate defense.

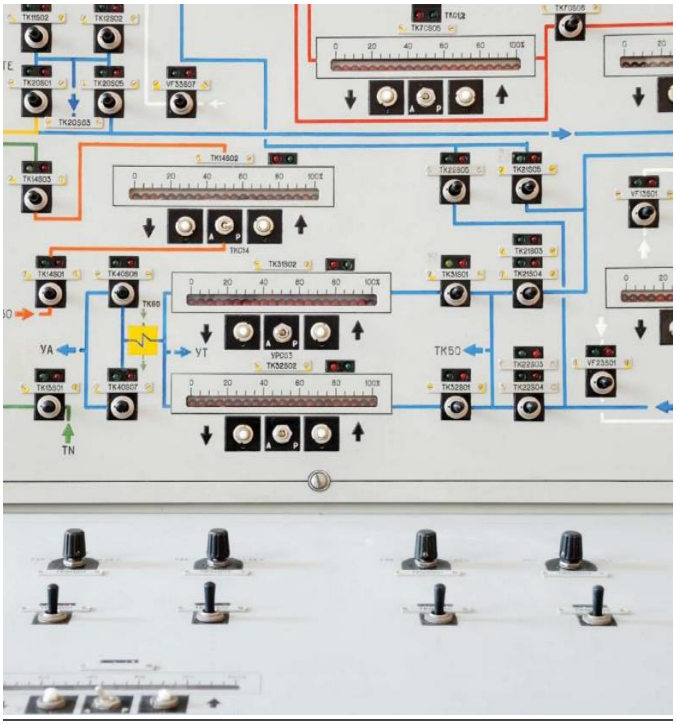
The threat environment today is far more insidious and sophisticated than in the past. Many of the attackers are intelligent, state-sponsored individuals who are dedicated to learning about the inherent weaknesses in a particular organization's defenses. Once they learn this, they determine the best way to take advantage of the weaknesses.

Today's malware, which is a component of most attacks against critical infrastructure systems, is far more sophisticated and can be customized to bypass the defenses an organization has in place.

At the same time organizations in this sector struggle to address threats with outdated technologies, they operate in highly complex business environments that can have a further negative impact on security.

The typical ecosystem of a critical infrastructure organization includes employees, customers, business partners, product and service vendors, consultants, third-party service providers, outsourcing providers, and government regulatory agencies.

Each can present potential security risks and vulnerabilities or impact the security program in some way.



Organizations also must deal with the challenge of having their operational technology (OT) connected to their IT networks and systems, putting both at risk of attacks that were not previously possible.

9. Key Challenges of Cybersecurity & relevant recommendations

1. *Cybersecurity Preparedness –*

- Increasing sophistication and frequency of cyber threats on a growing attack surface. The network environment has grown with the increased deployment of new digital devices (e.g. the internet of things (IOT)) that are located outside the physical boundary the department. These devices potentially introduce a greater variety of cyber-attack vectors.
  - ✓ Monitoring capabilities of the critical data streams and communications pathways in networks must be bolstered to identify and ultimately disrupt emerging cyber-attacks.
- Meeting stringent privacy and security requirements while exchanging data - Real-time threat monitoring and analysis often requires exchanging sensitive data from operating environments, triggering privacy and liability concerns.
  - ✓ Real-time threat monitoring requires technical products and assessments that meet the requirements of systems and ensure protection of sensitive data.
- Effective assessments require specialized expertise - Effective assessment of Cybersecurity risks and capabilities requires consistent, industry-accepted tools and best practices.
  - ✓ Departmental Element sites, particularly smaller sites may lack the skills and resources on staff to conduct assessments and prioritize mitigations without tools and resources.
- Information sharing requires processes in place prior to the threat - Vital information concerning high-level Cybersecurity threats and risks is often classified. This makes it difficult to distribute the information widely if partners lack clearances and if information sharing processes are not in place prior to an event or threat.
  - ✓ More efficient processes are needed to identify and prioritize private-industry partners who have a “need to know” and grant them appropriate security clearances.

2. *Incident Response and Recovery –*

- Coordinating roles among many diverse stakeholders - Federal support of Cybersecurity and incident response cuts across multiple government agencies and disciplines, from intelligence, to law enforcement, to emergency response.
  - ✓ National leadership is needed to avoid issues such as conflicting roles and responsibilities and activities that are redundant or poorly aligned.
- Developing flexible, adaptable procedures - Cyber threats evolve quickly, and government hierarchies may not be well-suited for a rapid reprioritization of activities.

- ✓ Continuous coordination across the Federal Government is required to unify national efforts and limit the strain on the private sector of partnering with multiple departments and agencies.

- Coordinating geographically dispersed and diverse functional resources - Unlike many physical events, cyber events may affect infrastructure across a wide geographic area, and the consequences of an incident may be different for each affected system.
- ✓ Cyber incident response also may require a different set of resources, personnel, and skills than traditional energy disruptions. Some of these skills may not be included in traditional incident response procedures and training and may not be frequently tested.

3. *Resilient Systems –*

- New solutions must support the business case - Develop Cybersecurity tools and technologies that are economical, cost effective, and support operations, effectively making the system easier and less expensive to operate.

- Diverse legacy and modern devices - Cybersecurity solutions must integrate with existing systems that often contain a mix of new and legacy devices, a mix of platforms and vendors, and devices with different levels of computational and communications resources available to support Cybersecurity measures.

- Solutions from diverse vendors and third-party providers must interoperate - New tools and technologies must be built to common standards to allow devices from different vendors to connect and operate without issue.
- ✓ Interoperable Cybersecurity solutions require common standards development.

- Securing devices sourced from a global supply chain - Departmental Elements must ensure the integrity of the system hardware, firmware, and software components as they traverse the supply chain.

- Anticipating security in the future grid - Designing future systems with built-in cyber resilience requires anticipating future cyber threat scenarios and protection requirements.

- Meeting the growing demand for Cybersecurity professionals - To manage and defend increasingly complex and sophisticated cyber systems, universities must build the nation's Cybersecurity workforce.
- ✓ The current workforce increasingly faces heavy workloads, a shortage of critical skills, and constantly evolving expertise needs.

Smart Grid's Cyber Security

"Types of Attacks, their Impact and Proposed Countermeasures"

1. Introduction

Smart grid uses the power of information technology to intelligently deliver energy to customers by using a two-way communication, and wisely meet the environmental requirements by facilitating the integration of green technologies.

Although smart grid addresses several problems of the traditional grid, it faces a number of security challenges. Because communication has been incorporated into the electrical power with its inherent weaknesses, it has exposed the system to numerous risks.

Any interruptions in power generation could disturb smart grid stability and could potentially have large socio-economic impacts.

In addition, as valuable data are exchanged among smart grid systems, theft or alteration of this data could violate consumer privacy. Because of these weaknesses, smart grid has become the primary target of attackers, which attracted the attention of government, industry, and academia.

Several research papers have discussed these problems. However, most of them classified attacks based on confidentiality, integrity, and availability, and they excluded attacks which compromise other security criteria such as accountability.

In addition, the existed security countermeasures focus on countering some specific attacks or protecting some specific components, but there is no global approach which combines these solutions to secure the entire system.

The purpose of this paper is to review the security requirements and investigate in depth a number of important cyber-attacks in smart grid to diagnose the potential vulnerabilities along with their impact.

In addition, we proposed a cyber security strategy as a solution to address breaches, counter attacks, and deploy appropriate countermeasures. Finally, some future research directions are shared.

Index Terms— *Smart grid, cyber-attacks, vulnerabilities, confidentiality, availability, integrity, accountability, IDS, cryptography, network security.*

2. Smart Grid Overview

- **Smart grid's features**

The main benefits expected from the smart grid are increasing grid resilience and improving environmental performance. Resilience indicates the capability of a given entity to resist unexpected events and recover quickly thereafter.

Smart grid promises to provide flexibility and reliability by enabling additional dispersed power supply, facilitating the integration of new resources into the grid, and enabling corrective capabilities when failures occur.

Moreover, smart grid systems are expected to enable electric vehicles, reducing energy used by customers and reducing energy losses within the grid.

- **Smart grid's conceptual model**

According to the national institute of standard and technology (NIST), a smart grid is composed of seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and operations, each of which include both actors and applications.

Actors are programs, devices, and systems whereas applications are tasks performed by a one actor or more in each domain. Fig. 1 shows the conceptual model of smart grid and the interaction of actors from different domains via a secure channel.

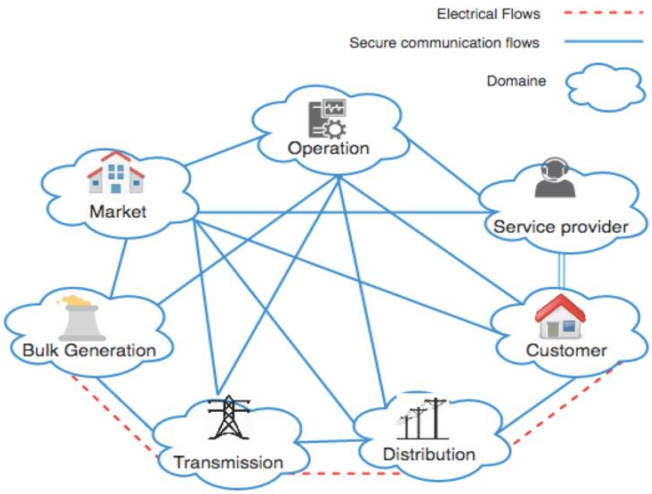


Fig. 1. Smart grid's conceptual model based on NIST.

- **Smart grid's systems**

Smart grid is composed of several distributed and heterogeneous applications, including advanced metering infrastructure (AMI), automation substation, demand response, supervisory control and data acquisition (SCADA), electrical vehicle (EV), and home energy management (HEM).

In this section we will discuss three critical and vulnerable applications in the smart grid: ***AMI, SCADA, and automation substation.***

Advanced metering infrastructure (AMI) is responsible for collecting, measuring and analyzing energy, water and gas usage. It allows two-way communication from the user to the utility. It is composed of three components: smart meter, AMI headend, and the communication network.

Smart meters are digital meters, consisting of microprocessors and a local memory, and they are responsible first for monitoring and collecting power usage of home appliances, and also for transmitting data in real time to the AMI headend in the utility side.

An AMI headend is an AMI server consists of meter data management system (MDMS). The communication between the smart meters, the home appliances, and the AMI headend is defined through several communication protocols such as Z-wave and ZigBee.

Supervisory control and data acquisition (SCADA) is a system that measures, monitors and controls electrical power grid. It is typically used for large-scale environments.

It consists of three elements: the remote terminal unit (RTU), master terminal unit (MTU), and human–machine interface (HMI).

- RTU is a device composed of three components: first one used for data acquisition, second one responsible for executing instructions coming for the MTU, and a third one designed for the communication.
- MTU is a device responsible for controlling the RTU.
- The HMI is a graphic interface for the SCADA system operator. The communication within SCADA system is based on many industrial protocol including distributed network protocol v3.0 (DNP3) and IEC 61850.

The Automation Substation is a key element in the power grid network. It performs several functions including receiving power from generating facility, regulating distribution, and limiting power surge. It contains devices that regulate and distributes electrical energy such as a remote terminal unit (RTU), global positioning system (GPS), human–machine interface (HMI), and intelligent electronic devices (IEDs).

The substation sends operation data to the SCADA for controlling the power system. Many operations are automated within the substation in order to increase the reliability of the power grid. The communication between the automation substation and other devices in transmission and distribution is defined by the standard IEC 61850.

- **Smart grid's network protocols**

Distributed and heterogeneous applications in smart grid require different communication protocols. ***Fig. 2*** illustrates the smart grid network architecture and the protocol used within each network. In the home area network (HAN), home appliances uses ZigBee and Z-wave protocols.

In the neighborhood area network (NAN), devices are usually connected via IEEE 802.11, IEEE 802.15.4, or IEEE 802.16 standards. In the wide area network (WAN) and in supervisory control and data acquisition (SCADA) applications, several industrial protocols are used specially distributed networking protocol 3.0 (DNP3) and modicon communication bus (ModBus). Within substation automation, protocol IEC 61850 is used.

In this section we will discuss two widely used yet vulnerable protocols in smart grid: ***Modbus and DNP3.***

- Modicon communication bus (ModBus) is a 7 layer protocol of the model OSI; it was designed in 1979 to enable the process controller to communicate in real-time with computers.

  In a SCADA system, ModBus is a master-slave protocol responsible for exchanging instruction between one master, remote terminal unit (RTU) or master terminal unit (MTU), and several slave devices, such as sensors, drivers, and PLCs.

  On one hand, Modbus is widely used in industrial architecture, because of its relative ease of use by communicating raw data without restriction of authentication, encryption, or any excessive overhead.

  One the other hand, these features make it vulnerable and easily exploitable.

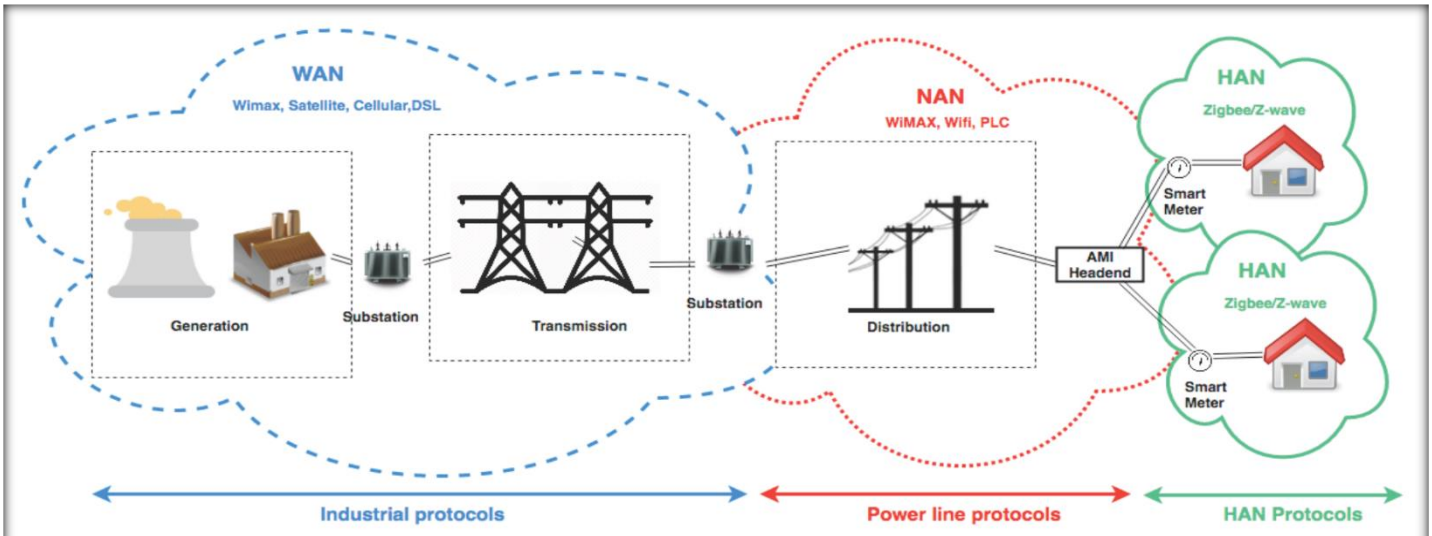


Fig. 2. Illustration of smart grid network architecture

- **Distributed network protocol v3.0 (DNP3)** is another widely used communication protocol for critical infrastructure, more specifically in the electricity industry. It was initiated in 1990 as a serial protocol to manage communication between "Master stations" and slave stations called "outstations'.

  In electrical stations, DNP3 was used for connecting master stations, such as RTUs, with outstations, such as intelligent electrical devices (IEDs). In 1998, DNP3 was extended to work over IP network through encapsulation of TCP or UDP packets.

  DNP3 uses several standardized data formats and support timed-stamped (time-synchronized) data, making the data transmission reliable and efficient.

  At first DNP3 did not provide any security mechanism such as encryption or authentication, but this problem was fixed with the secure version of DNP3 called DNP3 secure.

3. Security Requirements of Smart Grid

The National Institute of Standards and Technology (NIST) has defined three criteria required to maintain security of information in the smart grid and keep it protected, specifically confidentiality, integrity, and availability. According to, accountability is another important security criterion. The description of each criterion is given below.

A. Confidentiality

In general, confidentiality preserves authorized restrictions on information access and disclosure. In other words, the confidentiality criterion requires protecting both personal privacy and proprietary information from being accessed or disclosed by unauthorized entities, individuals, or processes. Once an unauthorized disclosure of information occurs, confidentiality is lost.

For instance, information such as control of a meter, metering usage, and billing information that is sent between a customer and various entities must be confidential and protected; otherwise the customer's information could be manipulated, modified, or used for other malicious purposes.

B. Availability

Availability is defined as ensuring timely and reliable access to and use of information. It is considered the most important security criterion in smart grid because the loss of availability means disruption of access to information in a smart grid.

For example, loss of availability can disturb the operation of the control system by blocking the information's flow through the network, and therefore denying the network's availability to control the system's operators.

C. Integrity

Integrity in smart grid means protecting against improper modification or destruction of the information. A loss of integrity is an unauthorized alteration, modification, or destruction of data in undetected manner.

For example, power injection is a malicious attack launched by an adversary who intelligently modifies the measurements and relays them from the power injection meters and power flow to the state estimator. Both nonrepudiation and authenticity of information are required to maintain the integrity. Nonrepudiation means that individuals, entity or organization, are unable to perform a particular action and then deny it later; authenticity is the fact that data is originated from a legitimate source.

D. Accountability

Accountability means ensuring tractability of the system and that every action performed by a person, device, or even a public authority is recordable so that no one can deny his/her action. This recordable information can be presented as an evidence within a court of law in order to determine the attacker.

An example of an accountability problem would be the monthly electricity bills of customers. Generally smart meters could determine the cost of electricity in real-time or day-to-day. However, if these meters are under attack this information is no longer reliable because they have been altered. As a result, the customer will have two different electric bills, one from the smart meter and the other from the utility.

4. Security Attacks and Countermeasures in Smart Grid

- **Smart grid attacks**

In general and as shown in Fig. 3, there are four steps used by malicious hackers to attack and get control over a system, namely reconnaissance, scanning, exploitation, and maintain access.

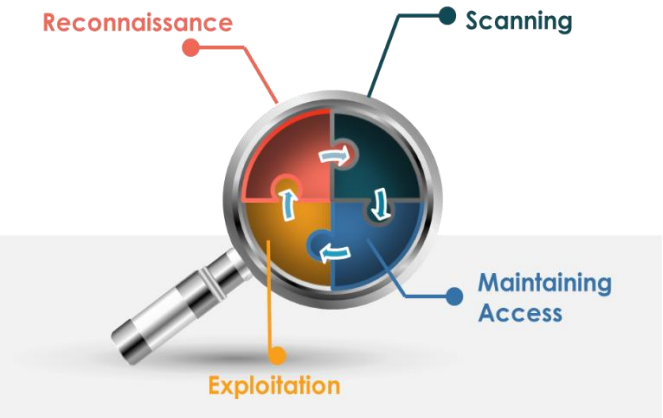


Fig. 3. Attacking cycle followed by hackers to get control over a system.

- During the first step, reconnaissance, the attacker gathers and collects information about its target.
- In the second step, scanning, the attacker tries to identify the system's vulnerabilities. These activities aim to identify the opened ports and to discover the service running on each port along with its weaknesses.
- During the exploitation step, he/she tries to compromise and get a full control of the target.
- Once the attacker has an administrative access on the target, he/she proceeds to the final step which is, maintaining the access.

This step is achieved by installing a stealthy and undetectable program; thus he/she can get back easily to the target system later.

In smart grid, the same steps are followed by attackers to compromise the security's criteria. During each step, they use different techniques to compromise a particular system in the grid. Thus, attacks can be classified based on these steps.

1) Reconnaissance

The first phase, reconnaissance, includes the attacks: social engineering and traffic analysis. Social engineering (SE), relies on social skills and human interaction rather than technical skills. An attacker uses communication and persuasion to win the trust of a legitimate user and get credential and confidential information such as passwords or PIN number to log on into a particular system.

For examples, phishing and password pilfering attack are famous techniques used in SE. The traffic analysis attack is used to listen to the traffic and analyze it in order to determine the devices and the hosts connected to the network along with their IP addresses. Social engineering and traffic analysis compromise mainly the confidentiality of the information.

2) Scanning

Scanning attack is the next step used to discover all the devices and the hosts alive on the network. There are four types of scans: IPs, ports, services, and vulnerabilities. Generally, an attacker starts with an IPs scan to identify all the hosts connected in the network along with their IP addresses. Next, he or she goes deeper by scanning the ports in order to determine which port is open. This scan is executed on each discovered host on the network. The attacker then moves on to the service scan in order to find out the service or system running behind each opened port. For instance, if the port 102 is detected open on a particular system, the hacker could infer that this system is a substation automation control or messaging.

If the port 4713 is open, the target system is a Phasor Measurement Unit (PMU). The final step, vulnerabilities scan, aims to identify the weaknesses and vulnerabilities related to each service on the target machine to exploit it afterward.

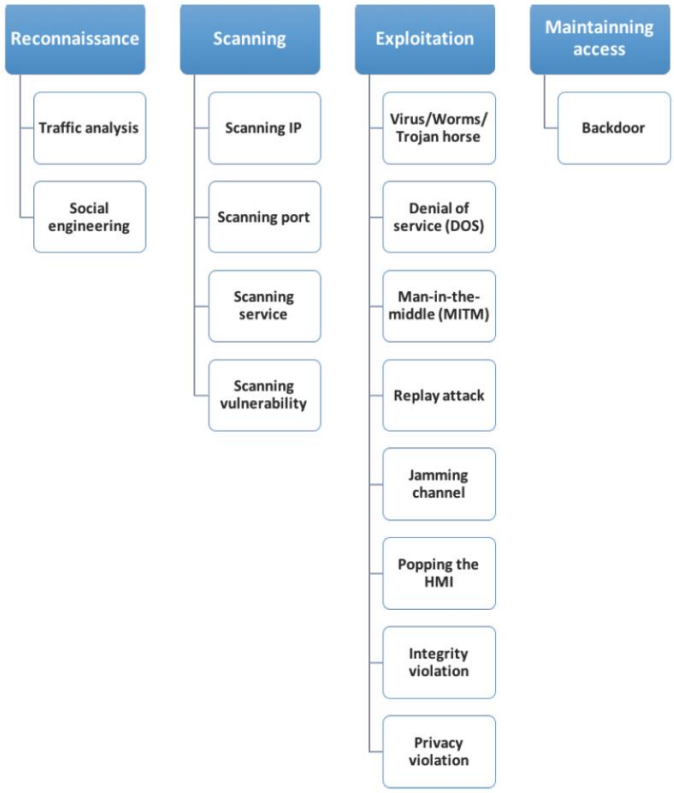


Fig. 4. Types of attacks across various steps

Modbus and DNP3 are two industrial protocols vulnerable to scanning attacks. Given that Modbus/TCP was designed for communication rather than security purpose, it can be compromised by an attack called Modbus network scanning.

This attack consists of sending a benign message to all devices connected in the network to gather information about these devices. Modscan is a SCADA Modbus network scanner designed to detect open Modbus/TCP and identify device slave IDs along with their IP addresses.

It is recommended to scan the DNP3 protocol and discover hosts, specifically, the slaves, their DNP3 addresses, and their corresponding master. As one can see, these attacks target mainly the confidentiality of the smart grid.

3) Exploitation

The third step, exploitation, includes malicious activities that attempt to exploit the smart grid component's vulnerabilities and get the control over it.

These activities include viruses, worms, Trojan horses, denial of service (DOS) attacks, man-in-the-middle (MITM) attacks, replay attacks, jamming channels, popping the human machine interface (HMI), integrity violations, and privacy violations.

Here is a brief about all 16 types of attacks on smart grid –

1. **A virus is a program** used to infect a specific device or a system in smart grid. A worm is self-replicating program. It uses the network to spread, to copy itself, and to infect other devices and systems. A Trojan horse is a program that appears to perform a legitimate task on the target system. However, it runs a malicious code in the background. An attacker uses this type of malware to upload a virus or worm on the target system.

2. **In denial of service (DOS) attacks**, several methods are used, particularly SYN attacks, buffer overflow, teardrop attacks, and smurf attacks, puppet attack, time-delay-switch (TDS), and time synchronization attack (TSA). A SYN attack exploits the three-way handshake (SYN, SYN-ACK, ACK) used to establish a TCP session. The attacker floods a target system with connection requests without responding to the replays, forcing the system to crash. The Modbus/TCP protocol is vulnerable to these attacks since it operates over TCP.

3. **In buffer overflow attack**, the attacker sends a huge amount of data to a specific system, thereby exhausting its resources. For example, the ping-of-death is considered as a buffer overflow attack as it exploits the internet control message protocol (ICMP) by sending more that 65K octets of data. It then makes the system crash.

4. **In a teardrop attack**, an attacker alters and modifies the length and the fragmentation offset fields in sequential IP packets. Once the target system receives these packets, it crashes because the instructions on how the fragments are offset within these packets are contradictory.

5. **In smurf attack**, the attacker targets not only a specific system, but it can saturate and congest the traffic of an entire network. It consists of three elements: the source site, the bounce site, and the target site. For source site, the adversary sends a spoofed packet to the broadcast address of the bounce site.
   These packets contain the IP address of the target system. Once the bounce site receives the forged packets, it broadcasts them to all hosts connected to the network and then causes these hosts to replay, saturating the target system.

6. **In puppet attack** targets the advanced metering infrastructure (AMI) network by exploiting a vulnerability in dynamic source routing (DSR) protocol and then exhausting the communication network bandwidth. Due to this attack, the packet delivery drops between 10% and 20%.

7. **The time-delay-switch (TDS) attack** consists of introducing a delay in control system creating instability in the smart grid system.

8. **The time synchronization (TSA) attack** targets mainly the timing information in smart grid. Because power grid operations such as fault detection and event location estimation depend highly on precise time information, and also most of the measurement devices in smart grid are equipped with global positioning system (GPS), attack such as TSA, which spoof the GPS information, could have a high impact on the system.
   DOS represents a significant threat to the smart grid system because communication

and control messages in such a system are time critical, and a delay of few seconds could compromise the system availability.

9. **The man-in-the-middle (MITM) attack** is performed when an attacker inserts itself between two legitimate devices and listens, performs an injection, or intercepts the traffic between them. The attacker is connected to both devices and relays the traffic between them. These legitimate devices appear to communicate directly when in fact they are communicating via a third-device.

10. **Intercept/alter attack** is another type MITM attack. It attempts to intercept, alter, and modify data either transmitted across the network or stored in a particular device. For example, in order to intercept a private communication in advanced metering infrastructure (AMI), an attacker uses electromagnetic/radio-frequency interception attack.
Eavesdropping attack is also another MITM attack's type, where the attacker intercepts private communications between two legitimate devices. All these MITM attacks attempt to compromise the confidentiality, the integrity, and the accountability.

11. **In replay attack**, as the industrial control traffic is transmitted in plain text, an attacker could maliciously capture packets, inject a specific packet, and replay them to the legitimate destinations, compromising then the communication's integrity. Intelligent electronic device (IED), which is a device designed for controlling and communicating with the SCADA system, could be targeted by replay attacks so that false measurements are injected in a specific register.

    Replay attack could also be used to alter the behavior the programmable logic controllers (PLC). In AMI, where an authentication scheme is used between smart meters, a replay attack involves a malicious host to intercept authentication packets sent from smart meter and re-sending them at a later point in time, expecting to authenticate and gain unauthorized entry into the network.

12. **In the jamming channel attack**, an adversary exploits the shared nature of the wireless network and sends a random or continuous flow of packets in order to keep the channel busy and then prevents legitimate devices from communicating and exchanging data. Due to its time-critical nature, smart grid requires a highly available network to meet the quality of service requirements and such an attack can severely degrade its performance.

13. **Popping the HMI is an attack** that exploits a known device's vulnerability, especially device's software or OS vulnerabilities, and then installs a remote shell, allowing the attacker to connect remotely to the server from his computer to get unauthorized access in order to monitor and control the compromised system. SCADA systems, substations, or any system running an operation system with a console interface is considered as a potential target of this attack.

14. **In the masquerade attack**, a malicious person may pretend to be a legitimate user in order to gain access to a system or gain greater privileges to perform unauthorized actions. This attack could tamper with the programmable communicating thermostat (PCT) which is used to reduce electric power at a residential site. It compromises the availability, integrity, confidentiality, and accountability of the system.

15. **Integrity violation attacks** aim to violate the integrity and/or the accountability of the smart grid by altering intentionally or unintentionally the data stored in a given device in the network. For instance, a customer could perform this attack to alter the smart meter data in order to reduce his electricity bill.

16. **Privacy violation attack** aims to violate privacy by collecting private information about customers. For example, as smart meters collect electricity usage many times per hour, information about the user electricity's consumption could be obtained. Thus, if a meter does not show electricity usage for a period of time, that commonly indicates that the house is empty. This information could then be used to conduct a physical attack like burglary.

4) Maintaining access

In the final step, maintaining access, the attacker uses a special type of attack to gain permanent access to the target, especially backdoors, viruses, and Trojan horses. A backdoor is an undetectable program, stealthy installed on the target to get back later easily and quickly.

If the attacker succeeds in embedding a backdoor into the servers of the control center of the SCADA, he or she can launch several attacks against the system which can cause a severe impact on the power system.

In IT network, security's parameters are classified based on their importance in the following order: confidentiality, integrity, accountability, and availability. Whereas in smart grid, they are classified: availability, integrity, accountability, and confidentiality.

Thus, we can say that attacks which compromise the availability of the smart grid systems have a high severity, while those targeting confidentiality have a low severity. In addition to the level of severity, each attack has a level of likelihood to be performed.

For instance, attacks such as Stuxnet and Duqu, has a high severity because they are able to vandalize the industrial control system and bypass all the security boundaries; but, they are complex and sophisticated. So, these viruses have high severity, but their likelihood to be performed is low. Another example is the HMI popping attack.

It has a high severity and it does not require advanced networking skills or significant experience in security and industrial control system to perform it.

Since the devices' vulnerabilities documentation are publicly available, a hacker or the so-called script-kiddies may simply use open source tools such as MetaSploit and Meterpreter to launch such an attack. Therefore, this attack has high severity and it is very likely to be performed.

Table II shows a summary of the cyber-attacks in smart grid based upon the four steps: reconnaissance, scanning, exploitation, and maintaining access.

		Severity of the Attack		
		Low	Medium	High
Likelihood of the attack to be performed	High	- Traffic analysis - Privacy violation		- Virus, worms, Trojanhorse - DOS - Backdoor
	Medium	- Social engineering - Scanning	- MITM - Replay attack	- Jamming channel - Masquerade attack - Integrity violation
	Low			- Popping the HMI

Table II shows the likelihood of each attack to be performed and its associated level of severity.

Smart grid countermeasures

A number of attack detection and countermeasure techniques are proposed in the literature to counter cyber-attacks. Security solutions today contribute to the smart grid's security however, they are insufficient to face sophisticated and blended attacks. We believe that security cannot be achieved through one specific solution, but by deploying several techniques incorporated into a global strategy.

In this section, and as ***Fig. 5*** shows, we propose a cyber security strategy composed of three phases: pre-attack, under attack, and post-attack. As follows, and for each phase, relevant published solutions in terms of security protocols, security technology, cryptography, and other cyber-attack countermeasures are described.

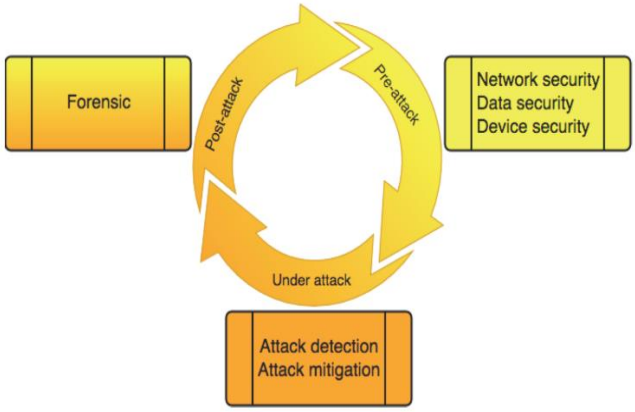


Fig. 5. Cyber security strategy for smart grid

1) Pre-attack

During this first phase, pre-attack, various published solutions are recommended to enhance the smart grid's security and to be prepared for any potential attack. Security countermeasures commonly fall into three categories, namely network security, cryptography, and device security.

We will discuss technologies and secure protocols such as IDS, SIEM, DLP and secure DNP3 for the network security. Encryption, authentication, and key management for the data security. Finally, Host IDS, compliance checks, and diversity technique for the device security.

a) Network security

The network is the backbone of a smart grid. So, network security plays a significant role in securing the entire system. Using firewalls supplemented with other monitoring and inspection technologies is recommended to secure the smart grid network. A firewall is intended to allow or deny network connections based on specific rules and policies. But an unknown or an advanced attack technique can easily bypass many firewall techniques. ***Therefore***, firewalls should be associated with other security technologies such as intrusion detection system (IDS), security information and event management systems (SIEM), and network data loss prevention (DLP).

This secured version named secure DNP3 added a secure layer for encryption and authentication between the TCP/IP and application layer. *Using such a protocol,* ***several attacks*** *can be avoided,* for example, authentication mechanism can protect against MITM attack, whereas encryption decreases eavesdropping and replay attacks.

Network DLP is a system responsible for preventing the loss or the theft of the data across the network. In addition to these security systems, secure network protocols such as IPsec, transport layer security (TLS), secure sockets layer (SSL), Secure DNP3 can also be used to enhance security in the network.

b) Cryptography for data security

Encryption mechanisms aim to ensure data's confidentiality, integrity, and nonrepudiation. There are two types of key encryptions: symmetric and asymmetric. In symmetric key encryption, or single-key encryption, one key is used to encrypt and to decrypt data.

The most used algorithms employing symmetric encryption are advanced encryption standard (AES) and data encryption standard (DES). Asymmetric key encryption, on the other hand, uses two keys to encrypt and decrypt data: private key and public key.

Both symmetric and asymmetric key encryption can be used, and the selection depends on several factors, including data criticality, time constraints, and computational resources.

Authentication is defined as the act of verifying that an object's identity is valid, such as the use of a password. Multicast authentication is a particular type of authentication and its applications are widely used in smart grid.

The proposed three methods to achieve authentication for multicast applications: secret-info asymmetry, time asymmetry, and hybrid asymmetry.

Key management is a crucial approach for encryption and authentication. Public key management (PKI), or shared secret key management, can be used to ensure authenticity for communication across networks.

Due to the distributed nature of smart grid, some specific requirements should be considered to design a cryptography key management, for which several basic yet relevant requirements of the key management scheme, particularly efficiency, evolve-ability, scalability, and secure management.

In addition, several key management frameworks have been proposed specifically for the power system: single-key, key establishment scheme for SCADA systems (SKE), key management architecture for SCADA systems (SKMA), advanced key management architecture for SCADA systems (ASKMA), ASKMA+, and scalable method of cryptographic key management (SMOCK) to name a few.

The choice of a framework relies on different criteria, including scalability, computational resource capability, and support for multicast.

c) Device security

Device protection is the third crucial element in the supply chain of smart grid security. In several security technologies have been recommended, particularly, host IDS, anti-virus, and host data loss

prevention (DLP) along with an automated security compliance check.

Such a tool performs a check against all smart grid components to verify that each device's configuration is up to date, especially the device's firmware and the current configuration file. As the smart grid components are highly connected and a weakness in one component can expose the entire system to risk, a compliance check is a crucial tool.

d) Defense-in-Depth

Defense-in-depth is the concept of layering multiple security features within the network such that the system is no longer attractive to would be attackers. Network operators must deploy intrusion detection systems, intrusion prevention systems, and DMZs, on control networks and use protection mechanisms such as moving target defense, protected (enclaved) computing, obfuscation, and other defense-in-depth techniques (e.g. cryptography, privilege zones, etc.).

Based on the DHS defense-in-depth recommended practice, the five key countermeasures for networks are:

1. Identify, minimize, and secure all network connections.
2. Harden the network and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
3. Continually monitor and assess the security of systems, networks, and interconnections.
4. Implement a risk-based defense-in-depth approach to secure systems and networks.
5. Manage the human element—clearly identify requirements for networks; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide PV network security training for all operators and administrators.

These countermeasures should be incorporated at the device and network levels to secure the communications system.

e) Additional Best Practices and Strategies

These best practice technologies, processes, and operational protective strategies can reduce the risks to the distribution grid.

With appropriate application, the risk of a major service outage resulting from a breach within the distribution grid can be minimized, if not eliminated, by following established best- practices and protocols.

The following suggested best practices and strategies can be taken to reduce risks:

- *Changing default passwords.* Standard protection solutions offered today on workstations and servers need to be extended to distributed energy devices. Device manufacturers should employ a technology that requires changing default passwords when a device is first connected. This requirement could also be integrated into existing standard processes, such as generator interconnection or permitting. A significant share of successful cyber incursions occur through unchanged factory default passwords.

- *Maintenance of passwords.* In addition to changing default passwords, it is important to remove access to existing or old passwords for users who should no longer have access. Often, employees and service providers will save passwords for future access. These passwords can be compromised, depending on how they are stored, and they can also be used by the bearer for unauthorized access.

- *Updating malware and software protection.* All parties must accept that they have a responsibility to ensure software patches and malware protection are kept up-to-date on all devices, regardless of regulatory mandate. Requirements such as these could be integrated into UL 1741 listing requirements.

- *Encrypting messages.* Encryption solutions with minimal resource requirement and high protection should be chosen. When utilizing encryption, the latest NIST standards should be followed. Endpoint devices should not share secret and/or private keys.

- *Firmware protective measures.* At the device level, firmware should be signed by the device manufacturer and it should not be possible for unsigned firmware to be loaded into the device.

- *Isolation.* Network segmentation with distinct security enclaves and enabling groups of devices to interact by securely sharing a certificate, such that the DER resource can communicate to other devices on the premise.

- *External interface protection limitations.* Interfaces should be disabled at the operating system level and not available for use unless specifically activated. Applications or operating systems (OS) that run on the device should have the ability to be securely updated or patched as needed.

- *Penetration testing.* Comprehensive penetration testing should also be done prior to release and periodically thereafter to validate that no vulnerabilities have been introduced.

- *Customer data protection.* Platforms should incorporate strict requirements to address issues ranging from secure transfer and storage of customer information to authentication protocols when interacting with devices and utility systems.

  Only essential information should be collected by platforms (i.e., name, email, address, time zone, Wi-Fi name (SSID), device IP address). Personally Identifiable Information and device-related information should be stored on a hardened and encrypted server with multiple layers of security control.

- *Third-party cloud security.* Cloud vendors utilized by these platform providers should be fully compliant with applicable security standards and undergo periodic Statement on Standards for Attestation Engagements (SSAE) auditing.

- *Incorporating* such communication protocols and end-to-end encryption for server storage and data access prevents the device or the network itself from being exploited by packet sniffing, IP spoofing, and Man-in-the-Middle attacks.

- *Reliable operations.* Network redundancy methods should be employed for data storage, distributed across multiple servers, to ensure 24/7 availability of data. All data changes should be logged into an audit trail, by capturing the user, date and time of the change, and the application that was used (e.g., web or mobile). Databases used must be backed up using a method that was designed for high availability.

- *User security measures.* Energy platforms must utilize role-based access controls in accessing application functions and data access within the software platform, log all events for reporting purposes, and require multi-factor authentication for all users.

These recommendations must be balanced against the high cost of Cybersecurity attacks. Cybersecurity practices for advanced and intelligent distribution grids should be developed and deployed in a manner that enables, rather than constrains, innovation and advancement in energy technology.

2) Under attack

This step is divided into two tasks: attack detection and attack mitigation. Several approaches and technologies can be used during each task, to detect the malicious activity, and then deploy the appropriate countermeasures.

During the attack detection, all the deployed security technologies are recommended, including SIEMS, DLP, and IDS. But, some of these solutions have a number of limitations and need improvements, particularly IDS as it has high rate of false positives.

The IEC61850 IDS was capable of detecting many attacks such as a DOS attack, a password cracking attack, and an ARP packet sniffer attack. The combination of two classifiers SVM and AIS have produced satisfactory results in terms of detection malicious traffic.

Once the attack are detected, mitigation can be executed using the following methods. In pushback method, the router is configured to block all the traffic coming from the attacker's IP address.

In the reconfiguration method, the network topology is changed to isolate the attacker. For jamming attacks, anti-jamming schemes such as frequency hopping spectrum spread (FHSS) and direct sequence spectrum spread (DSSS) are advised to mitigate attacks.

3) Post-attack

When an attack is not detected, such as in the case of Stuxnet, the post-attack period is an important step.
First, it is critical to identify the entity involved in the attack. Then, the IDS signature, anti-virus database and security policies must be kept up to date by learning from attacks and to protect the smart grid against future similar attacks.

Forensic analysis is the primary technique used during the post-attack. Smart grid forensic studies

collect, analyze, and intercept digital data in order to identify the entity involved in the event.

They are also useful to determine and address cyber and physical vulnerabilities of the smart grid in order to anticipate potential attacks.

In addition, forensic analysis in smart grid plays an important role in the investigation of cyber-crimes such as hacking, viruses, digital espionage, cyber terrorism, manipulating the operation of the smart grid, violating the consumer's privacy, and stealing valuable information including intellectual property and state secrets.

Fig. 4 below illustrates the category of attacks during each step, compromised smart grid's application or protocol, compromised security's parameter and possible countermeasures.

Attacking Cycle Step	Attack Category (Attack Example)	Compromised smart grid's application /protocol	Compromised Security's Parameter	Possible Countermeasures
Reconnaissance	Traffic analysis Social engineering (Phishing, Password pilfering)	Modbus protocol, DNP3 protocol	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK), TLS, SSL, Encryption, Authentication
Scanning	Scanning IP, Port, Service, Vulnerabilities (Modbus network scanning, DNP3 network scanning)	Modbus protocol, DNP3 protocol	Availability	IDS, SIEM, Automated security compliance checks
Exploitation	Virus, worms, Trojan horse (Stuxnet, Duqu)	SCADA PMU, Control device, SCADA	Confidentiality Integrity Availability Accountability	DLP , IDS , SIEM, Antivirus , Diversity , technique
	Denial of service (DOS) (Puppet attack, TDS, TSA)	AMI Instability of smart grid systems, PMU, smart grid equipment's GPS	Availability	SIEM, IDS, flow entropy, signal strength, sensing time measurement, transmission failure count, pushback, reconfiguration methods
	Man-in-themiddle (MITM) (Eavesdropping attack , Intercept/ alter)	HMI, PLC SCADA DNP3, SCADA AMI	Confidentiality Integrity	Secure DNP3, PKI (SKMA, SMOCK) [7], TLS, SSL, encryption, authentication
	Replay Attack	Authentication scheme in AMI	Confidentiality Integrity	Secure DNP3, TLS, SSL, encryption, authentication[1] PKI (SKMA, SMOCK) [7],
	Jamming Attack (MAS-SJ)	PMU CRN in WSGN	Availability	JADE, anti-jamming (FHSS, DSSS)
	Popping the HM1	SCADA, EMS, Substations	Confidentiality Integrity Availability Accountability	DLP, IDS , SIEM , Antivirus, automated security compliance checks
	Masquerade attack	PLC	Confidentiality Integrity Availability Accountability	DLP, IDS, Secure DNP3, SIEM, TLS, SSL, encryption, authentication, PKI (SKMA, SMOCK)
	Integrity violation (FDI)	Smart meter, RTU EMS, SCADA, AMI	Confidentiality Integrity Availability Accountability	DLP, IDS ,SIEM, Secure DNP3, TLS, SSL, encryption, authentication, PKI (SKMA, SMOCK)
	Privacy Voilation	Demand Response program, Smart meters.	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK)[7], TLS, SSL, encryption, authentication
Maintaining access	Backdoor	SCADA	Confidentiality Integrity Availability Accountability	IDS, SIEM,Anti-virus , Diversity technique

Fig. 4: *Cyber Attacks in Smart Gird, Their Impacts and Countermeasures*

5. Challenges and Future Direction

In heterogeneous systems such as smart grid, different devices coexist and communicate through various network protocols. This heterogeneity represents a great challenge and a potential threat for the smart grid security.

The communication between devices requires aggregation of data and translation between protocols.

However, this aggregation can enable accidental breaches and vulnerabilities simply because a feature in one protocol could not be translated properly into another.

Furthermore, ***the majority of industrial network protocols used in smart grid such as, DNP3, ICCP, Modbus, and Profibus were designed for connectivity but not for security purposes.***

Thus, these protocols not only cannot ensure a secure communication channel, but they may also be used as an attack surface.

Though there are some secure version of many industrial protocols, such as secure DNP3. However, the problem with this new version is its incompatibility with legacy installations.

In addition to network protocols, operating systems and physical equipment in smart grid may be vulnerable and expose the system to a wide variety of attacks.

I believe that smart grid cyber-attacks may be mitigated more effectively by combining several security mechanisms through a cyber security strategy.

Such a strategy have several benefits, including, addressing the system's vulnerabilities, detecting a number of cyber-attacks, deploying the appropriate countermeasures, and identifying the involved entity.

6. Conclusion

Smart grid is a system composed of distributed and heterogeneous components to intelligently deliver the electricity and easily integrate the renewable technologies. However, this critical system suffers from a number of security weaknesses.

In this study, a comprehensive overview of Cybersecurity in smart grid and investigate in depth the main cyber-attacks threating its infrastructure, its network protocols, and its applications is provided.

In addition, ***I have proposed a strategy composed of possible countermeasures designed to address potential components' vulnerabilities, detect malicious activities, enhance communication security in the network***, and protect the customer's privacy.

Cybersecurity Challenges, Mitigations and Best Practices for *U.S. Oil & Gas Industry*

Case Study – 2
Oil & Gas Sector Cyber-Security

A research report on efficiently applying guided recommendations for fast changing utilities' eco-system

Cybersecurity for the Oil & Gas Industry

1. Introduction

This report underscores the modern world's dependence on oil and illustrates why the industry's security is critical to the security of every nation. From military aggression to cyber threats, the oil and gas sector is a high-profile target for adversaries' intent on disrupting production, intercepting sensitive data, and crippling national and global economies.

Past attacks against this industry have proved the value of risk management and risk-based security policies for stakeholders. As a critical infrastructure, the oil and gas industry faces additional risks beyond those in many organizations. In addition to the intellectual property that any company must protect in its corporate Risk Management Framework, threats to the oil and gas infrastructure also put at risk the physical wellbeing of people and the environment as well as the national security.

In addition to the traditional physical and operational risks faced by the industry, the oil and gas sector also is susceptible to the escalating risk of cyber-attacks that threaten other companies, organizations and government agencies worldwide.

Regardless of the numbers, two common trends in Cybersecurity are clear:

- Cyber-attacks continue to increase
- The attacks are becoming more destructive and the impact of the attacks is increasing

2. Current State of Cybersecurity

According to a study by Frost & Sullivan, *"Global Oil and Gas Infrastructure Security Market Assessment,"* ***the total oil and gas infrastructure security market is predicted to increase from $18 billion dollars a year in 2011 to $31 billion dollars by 2021.***

Despite this spending, the ABI Research study describes the process Control Networks (PCN) in many oil and gas companies as "poorly protected against cyber threats… at best, they are secured with IT solutions which are ill-adapted to legacy control systems such as PCN."

The increase in the number of cyberattacks combined with the increasing costs of a breach ramp up the risks for oil and gas companies, especially the risks from complex, highly targeted attacks against the industry's high-profile, high-value infrastructure and intellectual property.

"Attackers run the gamut from unsophisticated script kiddies through hacktivists and cybercriminals to terrorists and state-sponsored hackers, each with their own skillsets, toolkits and motives."

---

3. The Threats to OIL & GAS

The challenges created by the integration of IT and OT for any organization are further exacerbated in the oil and gas industry by two major issues.

1. First there is greater integration in the value chain than in many other industries. The oil sector is an ecosystem composed of upstream, midstream and downstream companies and organizations engaged in different aspects of the business, which complicates the security landscape. This environment includes independent oil companies, state-owned oil companies, smaller companies that focus on only certain streams, and armies of service providers and other third parties.

2. This integration provides a ripe environment for security gaps and multiple points of entry. The integration of these organizations can create ripple effects when a disruption such as a spill, an attack, or a sociopolitical event occurs.

3. Secondly there are newer technologies coming into the industry at a rapid pace. Adding to the complexities of a highly -integrated industry already dealing with integrated IT and OT systems are the new technologies on the horizon that could further complicate the job of

the CIO and CISO responsible for ensuring the security of the enterprise.

Digital oil fields connected to cloud platforms running big data analytics, the use of drones in upstream oil and gas to run surveys or monitor for environmental issues, and third-party companies hosting 3D modeling for well and field planning are a few of the new technologies entering the industry that could create additional vulnerabilities.

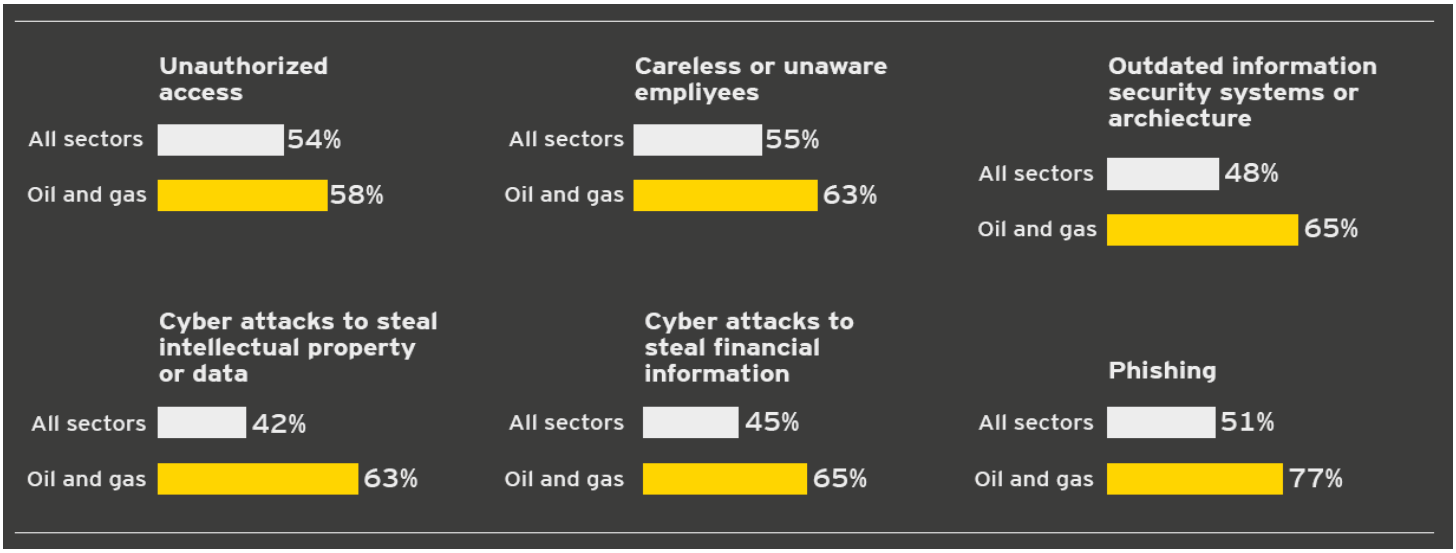


Fig. 2: Cyber threats faced by oil and gas sector as compared to all industrial sectors

4. Which threats and vulnerabilities have most increased your risk exposure over the last 12 months?

The oil and gas infrastructure is geographically dispersed and it includes remote stations and legacy operational technology with differing capabilities that is being integrated into the IT infrastructure. These factors combine to create a large attack surface for critical assets where continuous operation is required. Defending this environment requires extending Cybersecurity to the entire enterprise.

Companies need to create comprehensive security policies, plan for the training to implement them, audit to ensure that the policies are being complied with, and monitor systems to detect changes in near real time. The nature of OT systems, with their emphasis on reliability and stability, means that some risks will remain in place, and policies need to address the mitigation and management of these risks based on their likelihood and their potential impact.

5. Solutions for Securing the Oil and Gas Infrastructure

"Regardless of the organization's level of awareness and maturity, assistance is available to help improve Cybersecurity status."

It is required to chart a roadmap to full implementation of the technology, processes and practice needed to achieve the appropriate levels of security for oil and gas.

Companies have different needs and are at different levels in the maturity of their security programs, and so will have different paths to their desired end state.

Unfortunately, awareness of the critical nature of Cybersecurity often is lacking in the industry, particularly regarding Operational Technology systems, which can include industrial and process control systems (ICS and PCS), Distribution Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems.

Spending on OT system security too often is viewed as a cost rather than an investment.

Safety budgets used to be seen this way in the oil and gas industry, but that has changed. Companies now realize that being safe is good business as well as a regulatory requirement. Recognition of the need for security in operational technology systems is now rapidly growing through the industry and is catching up to the acceptance of safety in industrial systems.

Stuxnet is perhaps the best-known attack against an industrial control system, but German officials in 2014 confirmed that a cyberattack did massive damage to an unnamed steel mill. Key services, such as electricity, water, food processing, and transport, as well as oil and gas and refining, depend on OT systems to operate safely and reliably. If these services fail the impact on society can be rapid, with risks to both public safety and economies. A risk to an OT is a risk to the business itself, impacting safety, the environment, financial wellbeing, reputations, and contractual or regulatory requirements.

Integrated IT and OT security is a new trend in the oil and gas industry, although there are varying levels of awareness and implementation. Some organizations have little or no awareness of or interest in the issue, while some are aware of the need but are unsure how to proceed. Some are addressing security but are not as advanced as they believe, and others have misplaced confidence in IT perimeter defenses that cannot adequately protect OT systems.

Regardless of the organization's level of awareness and maturity, assistance is available to help improve Cybersecurity status.

6. Steps for Addressing Security

Here is the orderly set of steps that can be used to help apply proposed recommendations to help accelerate the specific cyber security objectives.

- **Raise awareness and achieve stakeholder buy-in:** This is not necessary for everyone; some companies are keenly aware of the need for securing process control systems. But more often some education on the issue is required, especially to include all stakeholders, to attain the strategic direction and funding in the context of the day-to-day operations.
  - Events such as the Stuxnet attack discovered in 2010, Project Shine, a global scanning project in 2012 and 2013 to discover Internet accessible ICS and PCS systems, together with the recently recognized cyberattacks in Turkey and Germany, have helped to bring the security issue to light. But the threat is far broader than a few high profile incidents at high value targets.
  - Any organization can be a victim, and for every major breach that makes headlines, there are many other less well-known minor incidents and even more near misses. To fully understand security needs, executives should be aware of the full spectrum of incidents and threats that they face.

- **Situational review:** The next step is a high-level review of the organization's current level of security. This often can be done quickly, producing an overview of the company's security posture. In most cases the findings show that there still needs to be more focus on the basics of security.
  - Companies need to begin with core activities including having security policies and plans in place, having an up-to-date inventory of control systems, identifying critical systems, identifying the risks to these systems, assessing the level of impact of an incident compromising each system, and providing security training for personnel.

  - When the review is completed, priorities can be established for the organization's immediate, mid-term and long-term goals with a recommended roadmap of options to achieve those goals.

  - Change can be difficult in any organization, and the most significant factor in the time it takes to achieve long-term goals often is the organization's ability to absorb and adapt to

changes rather than its ability to make them.

- **Detailed assessment:** Once priorities have been established, a more in -depth look at the security situation can be done to help get proper policies into place and assess compliance with them. This can include a survey of the infrastructure, the security controls and procedures being used, an assessment of vulnerabilities and the impact of their exploitation.
  - This assessment can identify the gaps between the organization's present state of security and the desired end state, and allow for planning on how to address those gaps. Not all gaps in security plans can be eliminated. In PCN especially, some older systems cannot be upgraded; they would need to be replaced in order to bring them into full security compliance. More than likely, replacement will be impractical and the risks associated with the system will have to be accepted.
  - Accepting risk does not mean ignoring it, however. Attention must be paid to residual risk according to its severity, controls put in place to mitigate it and reduce the likelihood of an exploit, and response plans created to deal quickly with an exploit.

- **Implementation:** With priorities and gaps identified, technology can be put into place along with the people and processes that will be responsible for security. Security training is an organization-wide effort that should include not only security officials, but all employees so that they know their roles and responsibilities in ensuring the security of the organization's systems
  - Automation is a key factor in effective security, speeding responses and freeing humans from routine manual tasks to focus on more critical analysis. But there are practical limits to the degree and types of automation that are practical in the control system environment. Although Intrusion Detections Systems can be valuable, for instance, Intrusion Prevention Systems are rarely if ever used in industrial and process control because the need to keep processes operating trumps the efficiency of an automated response to a detected intrusion.

- **Continual monitoring and maintenance:** Once the desired end-state for an organization is achieved, it must be maintained. This can involve ongoing monitoring of the security of the systems, controls, and processes as well as on-site maintenance to ensure that configuration remains within intended parameters.

7. Digitization magnifies the challenges

Apart from the upstream industry's "critical infra-structure" status, a complex ecosystem of computation, networking, and physical operational processes spread around the world makes the industry highly vulnerable to cyber-attacks; in other words, the industry has a large attack surface and many attacks (see figure 1).

A large O&G company, for instance: uses half a million processors just for oil and gas reservoir simulation; generates, transmits, and stores petabytes of sensitive and competitive field data; and operates and shares thousands of drilling and production control systems spread across geographies, fields, vendors, service providers, and partners.

What adds to this vulnerability is contrasting priori-ties of companies' operation technology and information technology departments. Operation systems close to drilling and well site operations such as sensors and programmable logic controllers are intended to perform tasks with 24X7 availability as their primary attribute, followed by integrity and confidentiality.

In contrast, IT systems such as enterprise resource planning have a reverse priority order of confidentiality, integrity, and availability. This clash of objectives—safety versus security—plays out in drilling and production control rooms where engineers fear that stringent IT security measures could introduce unacceptable latency into time-critical control systems, impacting decision making and operational response.

The technical set-up of ICS also carries inherent security challenges.

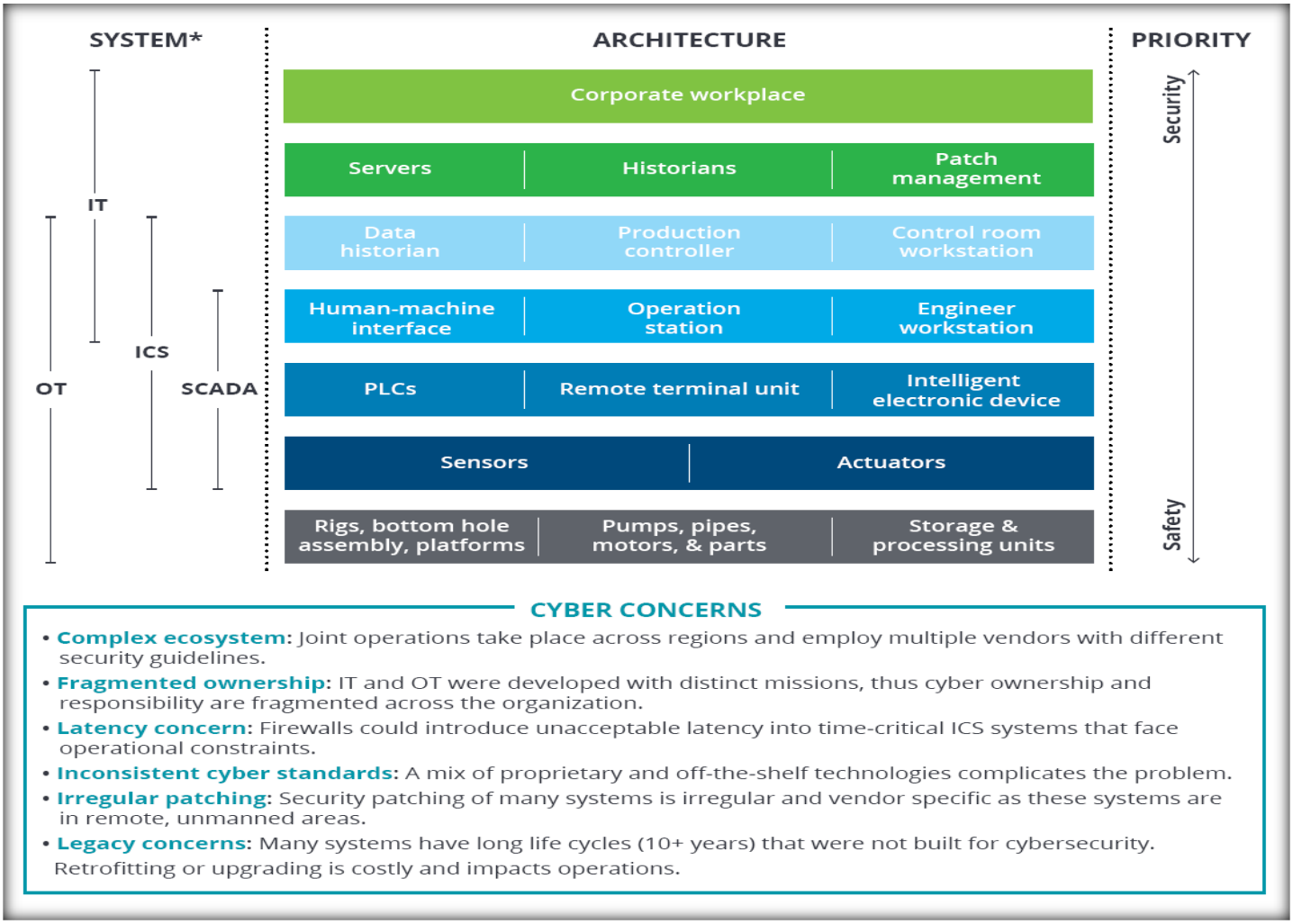


Fig. 1. Typical IT/OT architecture and cyber concerns of an O&G company

Growing digitization and interconnectedness of operations have heightened cyber risks further. Connected technology, in the embryonic form of digital oil fields or smart fields, has opened up an altogether new landscape of attack vectors for hackers by connecting upstream operations in real time.

Further, intelligent instrumentation at a field level have taken cyber risks into the front line of upstream operations. *For example*, a malicious hacker could slow down the oil extraction process by varying the motor speed and thermal capacity of an integrated sucker rod pump (the "front line" of the oil production process) by altering speed commands sent from internal optimization controllers.

With connected technology's adoption and penetration getting ahead of current Cybersecurity practices, it is not just the new IoT-generated information and value that is at risk. The future opportunity cost—including the safety of personnel and impact on the environment—is at stake.

8. Importance of intelligence against cyber-threat and integration in the oil and gas industry

Early warning and detection of breaches are essential for being in a state of readiness, indicating that the emphasis of Cybersecurity has changed to threat intelligence.

Organizations may not be able to control when information security incidents occur, but they can control how they respond to them expanding detection capabilities is a good place to start.

A well-functioning security operations center (SOC) can form the heart of effective detection.

By leveraging industry-leading practices and adopting strategies that are flexible and scalable, oil and gas organizations will be better equipped to deal with incoming (sometimes unforeseen) challenges to their security infrastructure.

9. Additional Measures oil and gas organizations can take

Oil and gas organizations have the broad experience necessary to manage and support complex operations linked by large-scale networks and with many points of ingress and egress. They should apply this experience to securing these environments by:

- Implementing security monitoring capabilities
- Enhancing response plans
- Working more closely with public sector security bodies and security partners
- Leveraging the strong health and safety culture that already exists to instill a true security culture

Technical measures to achieve the above would include but are not limited to:

- Segregate corporate and ICS networks to reduce island-hopping attacks
- Reduce and protect privileged users to detect and prevent lateral movement
- Employ application whitelisting and file integrity monitoring to prevent execution by malicious codes
- Reduce the attack surface by limiting workstation-to-workstation communication
- Deploy robust network IPS (Intrusion Protection services), application-layer firewalls, forward proxies, and breach detection with sandboxing or other dynamic traffic and code analyzes
- Use and monitor host and network logging
- Implement pass-the-hash mitigations
- Deploy anti-malware reputation services to augment traditional, signature-based anti-virus services
- Run host intrusion-prevention systems
- Quickly shield and patch known operating system and software vulnerabilities.

10. Growing importance of predictive analytics and Big Data by oil and gas companies to tackle cyber attacks

Predictive analytics have the power to proactively help businesses identify security threats before they can do any damage. Instead of only focusing on the "infection stage" of an attack, enterprises can detect future incidents and maximize prevention. The hacker bots use complex analytics and big data to sniff out vulnerabilities before an attack.

In the future, organizations can hybridize their security efforts with bots and humans: bots can search the system for irregularities while humans focus on patching, fortifying and protecting the system.

Predictive analytics and hacker bots work using self-learning analytics and detection techniques to monitor network activity and report real-time data. This enables an enterprise to identify threats without needing to know the attack's exact signature — thereby filling the current gap in coverage that is powerless against the modern point-and-click exploits with unique attack signatures. Predictive analytics can immediately detect irregularities in traffic flow and data, sounding the alarm for a security threat before the attack occurs.

Coupling machine learning with predictive analytics will enable Cybersecurity to shed its current cumbersome blacklist strategy and detect impending threats. AI techniques can improve their overall security performance and provide better protection from an increasing number of sophisticated cyber threats. AI combined with human insight has proven overall success in this sphere. Thus, socially responsible use of AI techniques will be essential to further mitigate related risks and concerns.

11. Conclusion

Both increasing IT/OT integration imposed by raising business requirements in the oil and gas industry and cutting-edge security capabilities sourced in different delivery models (capital expenditure (CAPEX), as-a-Service)) result in developing a very wide and complex environment to protect.

A focused program that combines traditional security tools, automation techniques, cyber security standards and best practices, threat intelligence, and human analysis is essential for oil and gas companies to maintain an appropriate risk-based security posture.

References:

1. Utility of the Future Study: Cybersecurity, W. Draffin.
2. Digitization and cyber disruption in oil and gas, Ciepiela.
3. Best practices for cyber security in the electric power sector, IBM.
4. Definitive Guide to Cybersecurity for the Oil & Gas Industry, Jasn Holcom.
5. Proactive steps Builds a Stronger Security Posture, Cilance.
6. Photovoltaic Cybersecurity, Jay Jason.
7. Smart Grid's Cybersecurity, Z. Elrabetl, H. Elghazil, N. Kaboch.

CISO level thought -

"The only answer is to change, at a fundamental level, the way companies operate. It starts with expanding the mission of enterprise security, from the tech staff and their machines to every person within the company, and everyone who does business with it … In the end, success hinges upon creating a strong and persistent awareness: a risk-aware culture … It represents a new way of thinking, one in which a pragmatic approach to security informs every decision and procedure at every level of the company. This must recast the way people handle information, from the "C-suite" to summer interns."