Cyber Resilient Energy Delivery Consortium (CREDC)

Inter-Sector Mapping and Gap Analysis: Energy Delivery System (EDS) Similarities and Differences
October 2017

Work Performed Under Agreement: DE-OE0000780
U.S. Department of Energy
Department of Electricity Delivery & Reliability
Contract Period: 10/01/2015 through 09/30/2020
DOE Project Officer: James Briones, DOE/NETL

RECIPIENT
University of Illinois at Urbana-Champaign
Information Trust Institute (ITI)
1308 W. Main Street
Urbana, Illinois, 61801
DUNS: 041544081

PRINCIPAL INVESTIGATOR
Professor David M. Nicol, Director, ITI
Phone: (217) 244-1925
Fax: (217) 244-1823
dmnicol@illinois.edu

CONTRIBUTING AUTHORS
Alfonso Valdes, University of Illinois at Urbana-Champaign
Wm. Arthur Conklin, University of Houston
Virgil Hammond, Argonne National Laboratory
David Nicol, University of Illinois at Urbana-Champaign
Peter Sauer, University of Illinois at Urbana-Champaign
Shabbir Shamsuddin, Argonne National Laboratory
Paul Skare, Pacific Northwest National Laboratory
Tim Yardley, University of Illinois at Urbana-Champaign

Table of Contents

Executive Summary

Today's energy delivery systems (EDS) consist of the physical infrastructures that carry electric power, petroleum products, and natural gas to all consumers. In June of 2016 the Cyber Resilient Energy Delivery Consortium (CREDC) issued a white paper "Inter-Sector Mapping and Gap Analysis" that explored the operations and interdependencies of these systems, especially the operational similarities. This paper is an adjunct to the original, and examines the key differences in the operations, and the characteristics that create these differences. It also describes industrial control systems as used in the three energy infrastructures and examines functional system and operational characteristics that influence the operations and operating systems of each of the three main EDS. Control systems for each must be designed to support the needs of the system being considered.

The control systems used by each of the three EDS are quite similar, and use many of the same components. SCADA systems are used to control geographically disperse energy infrastructure components (valves, relays, etc.), while DCS are used to control complex processes, usually at a single site such as a refinery or generating station.

Unique characteristics of each system affect the control flexibilities available to the control room personnel. The electric grid has no significant storage capability and must therefore always maintain a close balance between generated supply and consumer demand. This is further complicated by the speed of the process. Because the electric power effectively moves at the speed of light, generation and consumption are virtually instantaneous. Further complicating electrical control is the concept of phase, where the timing with respect to waveforms becomes a concern. Petroleum moves through pipelines at low velocities, and can be diverted into and out of storage tanks to compensate for varying supply and demand. However, because these liquids are incompressible, changes in pipeline supply and demand must be closely managed to avoid dangerous over-pressure conditions. Many petroleum liquids also have temperature concerns, as their viscosity can change with temperature and the effort to control flow is thus affected, making the control logic temperature-dependent. The compressibility of natural gas makes it possible to use the volume within the pipeline as a supply – demand buffer. Petroleum products, whether gas or liquid also have significant risk of fire and/or explosion should control be lost, making positive control a safety necessity.

The paper also looks at certain types of disruptions that might affect an EDS, and how operating personnel might react when such a disruption occurs. It also discusses some of the interdependencies among these infrastructures: for example, dependency on electricity by the gas and oil systems, and dependency of many electric generators on gas or oil as fuel.

The paper also discusses the regulatory environment, as well as the training requirements that have been mandated by the regulatory agencies. Finally, it discusses some significant challenges facing all three energy sectors today, and offers some recommendations for providing greater security in all the energy systems.

Introduction

The modern energy delivery systems (EDS) of today include the physical infrastructure that carries consumable energy, whether it's electrical power, natural gas, or petroleum in any or all of its various forms, to the commercial, industrial, and residential consumers that need these products to function and thrive.

In June of 2016 the Cyber Resilient Energy Delivery Consortium (CREDC) issued a white paper "Inter-Sector Mapping and Gap Analysis" that explored the operations of current energy delivery systems (EDS), especially how those systems are dependent upon cyber-physical actions to manage, operate, monitor, and control energy delivery systems.

An important objective of the report was to explore how these systems operate across the three major sub-sectors of energy: electric power, oil, and natural gas. The report recognized that there are many aspects of EDS that are common for essentially all systems, regardless of the sub-sector (electric power, petroleum, or natural gas). This fact makes analysis of many of the aspects of system operation easier to address, as in most cases the same assumptions apply across all the EDS.

The purpose of this report is to explore the key differences inherent in the operations of the three EDS sub-sector infrastructures. To facilitate this discussion, the report will first explore the system components that are somewhat generic in the energy infrastructures. It will discuss alternatives in control system philosophies and designs, alternatives in communications infrastructures, differences in applications, and why these differences are important. Finally, it will describe which alternatives are favored for each EDS application, and why.

Energy Infrastructure

The electric grid in the United States consists of a system of interconnected power generation, transmission facilities, and distribution facilities. There are thousands of power-generating plants and systems spread across the United States and almost 400,000 miles of electric transmission lines. In contrast, the oil and gas industries include facilities such as oil and gas wells, processing plants, refineries, and pipeline infrastructure to transport raw materials from offshore and onshore production wells through processing plants, refineries, and to consumers. There are approximately 170,000 miles of crude oil and product pipelines, 295,000 miles of gas transmission pipelines, and 1.9 million miles of gas distribution pipelines in the United States, mostly located underground and many crossing multiple states. In general, these energy infrastructures are owned by private industry. The operations of these electric grids, petroleum liquid lines, and gas pipelines are almost always monitored in a control room by controllers using computer-based equipment, such as a SCADA system. A SCADA (Supervisory Control and Data Acquisition) system, collects, records and displays operational information about the electric transmission, or pipeline system, such as voltages, pressures, flow rates, valve positions, and relay information. Some SCADA systems are used by operators to control energy infrastructure components such as transmission and pipe-line equipment, while, in other cases,

operators may dispatch other personnel to operate equipment in the field. These monitoring and control actions, whether via SCADA system commands or direction to field personnel, are a principal means of managing the energy infrastructure operations.

Automated Control Systems or Operational Technology Overview

The successful operation of advanced EDS today is dependent on automated control systems, utilizing computerized components that interact with each other through the use of complex software programs, hardware, and a variety of network communications infrastructure. These include radio, satellite, cellular phone, and Internet, not to mention several other communications mediums.

These automated control systems are referred to as Industrial Control Systems, or ICS. ICS is a general term that encompasses several types of control systems, including SCADA, distributed control system (DCS), and process control system (PCS). Other control system configurations such as programmable logic controller (PLC) and remote terminal unit (RTU) are often found in energy delivery systems, industrial sectors and critical infrastructures.[1] Today, these systems, including the network communication components, are now also called operational technology (OT). Similar to the electric sector, each of these systems in the O&G sector collects data from points throughout the operation, both local and remote, and also communicates control commands from the control center to field equipment within the operation. Each of these ICS types, as well as examples of the components that make up an ICS, are described in the next section of this report.

Control room systems are connected to field networks via a number of strategies. In the case of a power plant or a refinery, the control room connects to the field DCS or Energy Management System (EMS) via a local area networks (LANs) or Plain Old Telephone System (POTS). For geographically distributed systems (transmission and distribution networks in electrical systems as well as oil and gas pipelines) the connection is over a wide area network (WAN), using microwave, common carrier, satellite, POTS, and other means for the physical communication infrastructure. For higher layers in the protocol stack, legacy control protocols are sometimes embedded in Internet protocols (for example, Modbus over TCP). Modern control protocols such as IEC 61850 are designed to work over Internet and Ethernet protocols natively. IEC 61850 is specific to the electric power sector.

DCS in the energy sector are used to control large, complex processes at a single site such as power plants, refineries, processing plants, pumping stations, compressor stations, and liquefied natural gas (LNG) plants. For example, large oil refineries have many thousands of input/output (I/O) devices and employ very large DCS. A typical DCS consists of functionally and/or geographically distributed digital controllers capable of executing from 1 to 256 or more regulatory control loops in one control box. Today's controllers have extensive computational

[1]NIST Special Publication 800-82, Rev. 2, May 2015

capabilities and employ proportional, integral and derivative (PID) control which can generally perform logic and sequential controls.[2] A DCS is comprised of a supervisory layer of control and one to several distributed controllers contained within the same processing plant. The supervisory controller runs on the control server and communicates to its subordinates via a peer-to-peer network. The supervisor sends setpoints to and requests data from the distributed controllers. The distributed controllers control their process actuators based on requests from the supervisor and sensor feedback for process sensors. These controllers typically use a local field bus to communicate with actuators and sensors eliminating the need for point-to-point wiring between the controller and each device. There are several types of controllers used at the distributed control points of a DCS, including machine controllers, programmable logic controllers, process controllers and single loop controllers, depending on the application.[3] Controllers are distributed geographically in various sections of a control area. They are connected to operating and engineering stations that are used for data monitoring, data logging, alarming and controlling purposes via another high-speed communication bus. These communication protocols are of a variety of types, such as Foundation Fieldbus, HART, Profibus, Modbus, etc. DCS provides information to multiple displays for user interface.[4] Quite often, a generation plant will have numerous control systems running, providing primary and secondary control – the DCS (with the governor proving primary control), the SCADA interface (proving inputs for secondary control), and an exciter (or other system designed to stimulate the energy source). What separates DCS from SCADA is where the controlling logic is being deployed. In a DCS system, very little control is done at the central control station and most control is done out at the remote I/O controllers. DCS is typically deployed over a smaller geographic area, but not inside a single building (think oil & gas drilling platform or electrical generation plant). In a SCADA system, the remote I/O controllers have little control over the process. The remote I/O controllers simply acquires data needed to make decisions and passes them along. SCADA systems are typically deployed over a wide geographical area (think pipelines and electric grids), and including the connection of several DCS systems.

SCADA systems used in the O&G sector include combinations of field devices, communications infrastructure, hardware, and software, with all of these integrated into a system that provides for safe and reliable operation of the infrastructure components. Operators of oil and gas production facilities and pipelines, as well as the electric power grid and electric consumer distribution utilities, all use SCADA systems for operational control. In addition, SCADA gathers data used by advanced applications such as an EMS, state estimator, measurement accounting, etc.

---

[2] Genisys undated, "Distributed Control System," available at http://genisys-smart.com/distributed_control_system_01.php

[3] NIST undated, "IT Security for Industrial Control Systems," available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=821684

[4] EL-PRO-CUS undated, "Everything You Need to Know About Distributed Control System," available at https://www.elprocus.com/distributed-control-system-features-and-elements/

The physical connection of the SCADA system to the operating infrastructure (pipeline, electric grid, etc.) is the instrumentation. It is connected to PLCs and RTUs, depending on the type of remote facility. Data then flows from remote devices through the communications network to the SCADA host, also referred to as the SCADA master, Front End Processor (FEP), or master terminal unit (MTU). The term "field device" refers to automation device(s) and intelligent electronic device (s) (IEDs) installed at the remote facility to provide data collection, monitor and control, automation and communication with the SCADA host. Note that PLCs and RTUs manufactured and used by the O&G sector are the same products installed by the electric and other critical infrastructure companies. The key difference between the electric, oil, and gas usage is in the consequences occurring from the disruption of these products, either from cyberattacks or malfunction due to the nature of the energy infrastructure mechanical design, system architecture, operational latency, and use of safety instrumented systems to protect these energy sector operations.

In general O&G operational systems are typically coupled to safety instrumented systems (SIS) that can take over mechanical functions and bring a process to a safe state. Safety conditions addressed are, in order of decreasing priority, risk of death or injury, environmental discharge, damage to equipment, and loss of production. If the SIS takes over, there may be economic loss (loss of production, economic cost of process restart, possible equipment damage), but this is considered preferable by the industry operators to a more serious violation of safety. Although SIS makes use of ICS controls, it does not use the same physical set of controls as does the operational control function. Safety failures tend to be high consequence risks; SIS is used to reduce this risk, so that even if SIS is invoked and an economic loss is incurred, the risk of a higher consequence loss is averted. SIS is designed to automatically bring a system to a safe state without user input; in effect, it acts as a "deadman stick" for the system.

The safety function in the electrical power system is supported firstly by tags and flags, to prevent loss of life scenarios. These allow the operator to designate a device to be disabled from control so that it cannot be energized (while a crew works on it, for example). These functions are built-in to the EMS/DMS/SCADA/AGC systems operating aspects of the grid. In addition, select before operate functionality prevents control actions from diverse locations. Asset protection is provided by protective relays that can disconnect expensive assets rather than damaging them from voltage, current or phase angles being out of the asset's supported range.

In an industrial plant, the DCS and SIS are typically interfaced through a gateway, with each system having its own operator interfaces, engineering workstations, configuration tools, data and event historians, asset management, and network communications. In addition to segregation of control and safety equipment, there is separation of responsibilities between the personnel who manage these assets. The safety engineer is focused on safe operation, whereas the process engineer wants to maximize plant availability and operational profit.

Due to the costs associated with maintaining separate engineering, operation, and maintenance infrastructure for control and safety systems, many companies are now considering a more integrated architecture. Today's advanced digital technology has made it feasible to combine process control and safety instrumented functions within a common automation infrastructure, all while ensuring regulatory compliance. With this approach, plant personnel can view the status of the safety system and its applications, and combine this information with process control functions. The evolution of the Human-Machine Interface (HMI), Man Machine Interface (MMI), or more simply, the User Interface (UI) a term used by some industry allows critical information to be shared between the safety system and controllers and between the safety system and third-party subsystems via a digital bus interface.[5] A further exploration of cybersecurity as it relates to the SIS can be found in ISA-TR84.00.09-2017 Cybersecurity Related to the Functional Security Lifecycle.[6]

Comparing Characteristics of Natural Gas Pipelines, Petroleum Liquid Pipelines, and Electric Transmission operations

It is useful to compare and contrast three energy delivery systems – natural gas pipelines, petroleum liquid pipelines and electric transmission lines – that utilize SCADA control systems for management of their operation. From an outside view, these would appear to be identical in design and operation, but a closer look shows that there are significant differences in the time required to detect and respond to a situation due to the nature of the product they transport and before it becomes a public safety concern.

In general, a controller's job is to control the transport and exit of natural gas, liquids or electricity into the energy delivery system in a safe manner. The time required to move this product is a function of how much energy is expended to move the product. When the amount of product exceeds the capability of a line (pipeline or electric transmission line) there is a possibility of failure of the line. Electric transmission lines will fail due to overheating because the capacity is exceeded. Natural gas and petroleum liquid pipelines can fail if they are significantly over-pressured.

There are differences between gas and petroleum liquid pipeline systems that may help to explain the differences in probability of an incident occurring as a result of a pipeline controller action.

---

[5] ISA 2012, "Integrated DCS and SIS," available at https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2012/april/system-integration-integrated-dcs-and-sis/

[6] ISA-TR84.00.09-2017, "Cybersecurity Related to the Functional Safety Lifecycle," available at https://www.isa.org/store/isa-tr840009-2017,-cybersecurity-related-to-the-functional-safety-lifecycle/56889051

Of the three energy delivery systems studied, natural gas transmission lines permit simple, redundant, decentralized pressure control systems that prevent over-pressuring of the system. These same characteristics allow pipeline controllers sufficient time to recognize and respond to abnormal conditions that may be leading to over-pressure situations.

- ### Petroleum Liquid Pipelines

  Pump stations along the petroleum liquid pipelines provide the energy for increasing the pressure in a liquid pipeline to move the product from the production source to the end markets. Changing the speed and load of the pump at the station has the effect of changing the pressure on the downstream pipeline. Because of the weight of the liquid, changes in elevation of the line also affect pressure within the line. The total pressure will be greatest at the lowest elevations, and least at the highest points. The weight of the moving liquid also creates momentum within the pipe, exerting a significant change in pressure when a valve is closed or there is a change of direction.

  Because petroleum liquid in a pipeline is essentially incompressible, once the line is full any additional product that is added to the pipe without a corresponding offloading of the product in the pipeline will rapidly increase the pressure in the pipeline. This results in virtually instantaneous detectible pressure variances at the site of the variance, such as closing a valve. Viscosity of the product may slow it slightly, but in general, the controller at the central control center can detect pressure variances within the pipe fairly quickly.

  Petroleum liquid pipelines respond very quickly to changes of activity (pump startup, valve closure, etc.). These actions can result in pressure spikes as the system moves from a transient mode to a steady state mode. The weight of the liquid, which can be significant on liquid pipelines with major elevation changes, can compound the effects of the pressure transients. This will, in turn, afford minimal detect and response times (seconds).[7]

  In petroleum liquid operations, the timing of events is very critical. Because pipeline pressures can increase and exceed operating limits quickly, controlling the flow of liquid products is very time-sensitive. In addition, because some operations involve transporting batches of liquid products that should not be mixed (i.e., low-sulfur diesel and most other refined petroleum fuels), the precise timing of 'batch cuts' is critical to operational efficiency. Petroleum liquids, because of stringent environmental as well as public safety concerns, must be contained. Thus, the release volume of liquid is limited by the location and size of the containment provided.[8]

[7] INGAA 2006, "Gas Pipeline Controller Risk Analysis," available at https://www.aga.org/safety/pipeline-safety/transmission-pipelines/control-room-management/white-paper-gas-pipeline

[8] PHMSA 2008, "Human Factors Analysis of Pipeline Monitoring and Control Operations," available at https://primis.phmsa.dot.gov/crm/docs/FinalTechnicalReportNov2008.pdf

Because of viscosity and friction, the pressure in a pipeline is a function of its length. Pumping stations are required along the length of a pipeline, typically every 20-100 miles to bring pressure and flow back to proper levels. These stations require energy to create pressure, making the system dependent upon another energy system. A failure in any one of these systems can cause localized pressure and flow issues, leading to system problems. A local failure resulting in over-pressurization can result in ruptures and system spillage.

- ## Natural Gas Pipelines

  For natural gas, this means production, pipelines and storage need to be sized to meet the greatest potential demand, and deliveries need to move up and down to match changes in consumption. Natural gas has underground and above-ground storage options, as well as line pack. Briefly, line pack involves raising the pressure in a pipeline to pack more molecules into the same space. It's discussed further on in this section. Natural gas flows through a pipeline at velocities averaging 25 mph, depending on the pipeline and the configuration of related facilities, so new supply can take hours or days to reach its destination. That increases the value of market-area storage, which vastly reduces the distance and time needed for gas to reach consumers.[9]

  Compressor stations along the natural gas pipelines provide the energy used to build pressure on a natural gas pipeline to move the gas from the supply sources to the end use markets. Changing the speed and load of the compressors in the stations has the effect of changing the pressure on the downstream pipeline. Because of the compressibility of the gas, as well as the very low density, pressure within the line is essentially unaffected by change in elevation. Although technically present, because of the low density neither weight nor momentum is a significant factor in determining pressure at any point in the line.

  Because natural gas is a compressible fluid, it can sustain large variations of inventory packed into a pre-defined physical space (e.g. pipeline). The volume of natural gas stored in a section of pipeline at Maximum Allowable Operating Pressure (MAOP) is typically 30 to 60 times smaller than the volume of gas at atmospheric pressure, which means that more gas is contained in the line at high pressure than at lower pressures. Hence, when compared to the performance of a pressurized petroleum liquid, the compressibility of the gas provides a buffer that supports increased response times. This buffer volume, which is known as 'line pack' in the natural gas sector is the difference between the maximum volume contained at MAOP and the volume contained when the line pressure is as low as possible and still able to serve all connected loads at their required pressure. Line pack volume is used both as a source of unscheduled supply

[9] FERC 2015, "Energy Primer," available at https://www.ferc.gov/market-oversight/guide/energy-primer.pdf

(achieved by lowering pressure) and as optional storage reserve capacity (achieved by raising pressure).

Because natural gas transmission and distribution pipelines typically operate between pressures of 50% and 100% MAOP, inventory change rates accommodate slow transient response time (several minutes) for pressure increases and decreases. Therefore, the amount of time it takes to detect a sudden change (e.g., pressure drop) in the gas inventory of a pipeline can be significantly longer than the time required to detect a similar pressure change in a petroleum liquid line. Correspondingly, this allows more time (several minutes) for a controller, mechanical and electronic control systems to react and to control excessive pressure transients and volume changes.

In the event of over-pressure, both natural gas and petroleum liquid pipelines have over-pressure protection systems. These systems typically consist of either monitor regulators for gas systems or pressure relief mechanisms for gas and liquid systems. In the case of pressure relief mechanisms, these devices allow excess inventory to escape the pipeline, hence controlling the maximum operating pressure. For natural gas systems, over-pressure protection is typically provided through the use of monitor regulators, and excess natural gas is allowed to release to the atmosphere only through relief valves. The physics and design of natural gas transmission pipelines minimize the probability that a transmission or distribution pipeline controller can cause a reportable incident and allows the controller time to recognize an abnormal event as compared to petroleum liquid pipelines or electric transmission grids.[10]

- ### Electric Transmission Grid Systems

  Generators in the electric power infrastructure are the sources of energy for increasing the voltage and current on an electric transmission and distribution line. Controlling the speed and load of the generator has the effect of changing the voltage and current on the downstream transmission and distribution lines, raising or lowering the system frequency, or increasing or decreasing the interchange or power with your neighbors. It is highly critical to match load with supply, because there is virtually no storage capability in the electric system. Elevation and momentum are not significant factors.

  For electricity, storage is not a factor, although technologies such as batteries and flywheels are being developed. Hydroelectric pumped storage is available in a few locations; this involves pumping water to high reservoirs during times of slack electricity demand, then letting the water flow downhill through electricity-generating turbines when demand for power rises. Generating plants, transmission and distribution lines, substations and other equipment must be sized to meet the maximum amount needed by consumers at any time, in all locations. For all practical purposes, electricity use is

[10] INGAA 2006, "Gas Pipeline Controller Risk Analysis," available at https://www.aga.org/safety/pipeline-safety/transmission-pipelines/control-room-management/white-paper-gas-pipeline

contemporaneous with electricity generation; the power to run a light bulb is produced at the moment of illumination.[11]

The electric transmission industry relies heavily on the use of SCADA systems for energy flow control and monitoring. These systems have extremely short response times. Instead of controlling pressure, they control voltage and reactive power. A good example of the response time of the electric grid is the study of the Eastern U.S. blackout that occurred in 2003. As seen in the 2006 INGAA report (cited), the ripple effect is measured in milliseconds because of the lack of storage capability (no equivalent to the line pack in the natural gas pipeline) in the system. Another key factor in the control of the electric grid system is that there is not significant relief capability (i.e. relief valves) to unload excess energy that is not used. These physical characteristics make the man-to-machine interface in an electric power system the most critical of the three systems.[12]

Table 1 below summarizes the detection time and response time of various energy SCADA systems.

Mode	Signal	Detection Time	Response Time	Control
Electric Transmission	Voltage Reactive Power	Milliseconds	Milliseconds	Breakers Generators
Hazardous Liquid Pipeline	Pressure	Seconds	Seconds	Valves Pumps
Natural Gas Pipeline	Pressure	Minutes	Minutes	Valves Compressors

Table 2 below summarizes the pressure relieving detection time and relief time of energy pipelines.

Mode	Detection Time	Response Time	Exhaust	Transient Effect
Hazardous Liquid Pipeline	Seconds	Minutes	Limited to tanks or ponds	Possible Water Hammer
Natural Gas Pipeline	Minutes	Minutes	Open to atmosphere	

Dealing with Control System Failures

Control system robustness and reliability have come a long way in the last 30 years. The automated control system is now considered to be a vital part of the infrastructure that helps ensure the smooth running of plants, pumping stations, utilities, and processing facilities. However, even the most robust control system will occasionally experience conditions that may

[11] FERC 2015, "Energy Primer," available at https://www.ferc.gov/market-oversight/guide/energy-primer.pdf
[12] INGAA, 2006 – op. cit.

lead to failure of one or more functions of the control system. No technology is perfect, so possible failure types must be identified and strategies developed for the handling of each occurrence of significance. Factors such as how the system is monitored, alarm system capabilities, availability of operators, system uptime requirements, probability of occurrence, possible consequences, and process safety, just to name a few, must always be considered. Strategies for dealing with certain types of failures are discussed here.

- Reaction to the loss of data communications – In the event of the loss of data communications, a natural gas pipeline and other controlled critical natural gas assets will function normally on the last set command sent by the on-duty controller, giving field personnel time to locate the intrusion and to deal with it. This failure could be from a natural phenomenon or a cyber intrusion such as denial-of-service or buffer overrun attacks on the SCADA system. This impact from a loss of SCADA communication to the field devices will still permit the system to operate adequately, albeit less than efficiently, as certain functions such as pressurization are locally controlled. A similar event affecting a petroleum liquids line or an electric power transmission line would need to be treated differently, however. If the critical operating parameters on the system cannot be observed in the control room, a shutdown is almost always required, for both the petroleum and electric infrastructures. Regarding the oil sector, loss of communications will most likely dictate shutdown of the pipeline to maintain the integrity of product mix in the refined products pipeline and for public safety.

- Reaction to operational disruption of the SCADA System – Controllers react to the operational disruption of SCADA in both the oil and natural gas sectors by taking over operation of the facilities, using local operating field personnel. This process is similar to what is done with loss of communication. The mechanical systems, which are hard-wired and/or preset, cannot operate outside of the mechanical range established for their setpoint of the field components. SCADA data irregularities displayed are validated by contacting the SCADA engineers or other relevant field personnel. Such a disruption on an electric system could cause a shutdown. An alternate method for dealing with control system failures is with redundancy. Redundant components such as backup power supplies, multiple processors, dual-trunked communications networks, and backup instrumentation, with automatic fail-over logic, can significantly reduce the loss of control system redundancy. Also, field engineers can usually man substations if the control center has failed.[13]

  In most cases, natural gas delivery facilities into retail service areas (commercial, residential, etc.) have redundant mechanically-operated components (parallel meter

[13] "Control System Failure Survival Strategies", Graham Nasby, Control Engineering, October 2011; http://www.controleng.com/single-article/control-system-failure-survival-strategies/22ffc39ce4336a64a8124bec4f9682b2.html

runs, secondary regulators, e.g.) that mitigate both over- and under-pressure situations. O&G pipeline operations and components are often designed and operated with effective redundant defenses (such as redundant sensors that provide overlapping information regarding system status, automated alarm management that facilitates access to critical information, relief components that minimize the result of over pressurization, and use of safety instrumented systems) that reduce the likelihood that a hazardous situation will result in an actual incident.[14]

- Dependencies/Interdependencies – Operations of both oil and natural gas pipelines depend to a great degree on the availability of electric power. Crude oil and refined petroleum products pipelines can make heavy demands on commercial electricity to drive large motors on pumps and coolers, as well as many smaller motor applications. In addition, electric power operates the SCADA and other ICS equipment needed to manage pipeline control, monitor operations, and collect necessary field component data.

  Natural gas lines for the most part rely on gas-fueled compressors rather than electric-driven ones, but like the petroleum systems, still need electricity for accessory motors, both large and small, and for all the control operations and life support within the offices and shops. However, neither system depends wholly on commercial electric power. Except for the smaller facilities, generator installations are a part of almost every compressor station, and now in many critical pumping stations along the pipelines as well. For offshore production platforms, and for many onshore production sites, onsite generation is the primary (or only) source for meeting daily electricity needs. Loss of power means loss of throughput, which means loss of revenue.

  There are some major exceptions, such as electrically-operated natural gas compressors, petroleum refineries, natural gas processing plants, and petroleum pumping stations. These are all highly dependent on commercial power. Readily available standby electric generation can mitigate the loss of commercial power in some cases for smaller infrastructure components, but may not be sufficient to support larger pumps or electric compressors.

  A backup power supply is also important for maintaining the ICS and SCADA functions during times when commercial power is unavailable. Within limits, both the oil and gas sectors have the capability to control pipeline operations manually and maintain some level of throughput, even when commercial power is off. Largely due to its compressibility, natural gas will continue to flow, keeping the lines full and supplying demand, at least in the short term, even if the SCADA system is not transmitting any

[14] PHMSA 2008, "Human Factors Analysis of Pipeline Monitoring and Control Operations," available at https://primis.phmsa.dot.gov/crm/docs/FinalTechnicalReportNov2008.pdf

data or making any adjustments. However, oil pipeline operations depend on the ability of controllers to see what is happening at all points along the system. If the SCADA system is not functioning, the line must shut down to protect public, personnel, and environment.

Loss of electric power to one or more facilities on either the natural gas or oil infrastructure may be due to a variety of reasons, and is not necessarily due to loss of generation capability or capacity. However, because many commercial power-generating units are fueled by natural gas, loss of that supply, for whatever the reason, will immediately cause the generating unit to shut down. Under some conditions, loss of one generating unit can produce a cascading loss of firm load.

In the United States, over the past decade, the single largest sector of natural gas demand growth has occurred in the area of power generation. As emissions from coal-fired power plants have come under increasing public and environmental scrutiny, and innovative new oil exploration techniques has produced low cost natural gas as a side benefits encouraging more electric utilities and merchant power producers to develop new power plants using natural gas for new baseload and peaking generation. [15] Today, natural gas fuels nearly a third of electricity generation in the United States. The United States has more than 1,000 gigawatts (GW) of total generating capacity. Coal, natural gas and nuclear dominate the power generation market. Natural gas power plants feature three major technologies, each with its distinct set of market advantages and limitations. They are steam boilers, gas turbines and combined cycle generators. In addition, the generating plant may have oil backup, thus depending on the petroleum supply for No. 2 or No. 6 oil. Some of the backup generators may depend on diesel fuel for operating the generator engines.[16]

- Training – The operation of an energy delivery system, whether an oil pipeline, a natural gas pipeline, or an electric grid, is dependent upon the knowledge and expertise of one or two individuals in the control center known as Controllers that are responsible for efficiently and safely maintaining the flow of energy through that system, twenty-four hours per day, and 365 days per year. This is an important and complex responsibility, because an improper action can cause an interruption of service, damage to physical parts of the system, or even potential injury or death.

  The federal agencies responsible for the EDS - the Federal Energy Regulatory Commission (FERC) for the BES and the Pipeline and Hazardous Materials Safety Administration (PHMSA) under the Department of Transportation (DOT) for O&G sector

[15] PNUCC 2012, "Natural Gas-Electricity Primer," available at https://www.columbiagrid.org/client/NaturalGasElectricityPrimer(2012.08.09).pdf
[16] FERC 2015, "Energy Primer," available at https://www.ferc.gov/market-oversight/guide/energy-primer.pdf

facilities controlling all or any part of a pipeline system - have established formal training requirements for Control Room personnel.

Each agency has established its own training requirements (set forth in NERC PER-005.1 for EP control rooms and in 49 CFR 195.446 for O&G control rooms), both of which mandate the creation of system-specific training programs by each operator for each facility for which the operator is responsible, and includes testing and evaluation requirements.

Controllers are usually selected from the pool of employees already familiar with the facility and with the system operations. They frequently spend a considerable period learning the system and the functions of a controller "off-line" before they are assigned any responsibilities as a controller. During that period, they may spend time working on a backup control system, or simulator, to learn how certain actions affect system operations. After perhaps as much as a year, they will start to function as a controller, but their performance will be continuously evaluated for compliance with the regulations.[17,18]

Today computer-based simulator trainers are increasingly viewed by regulators and pipeline operators as essential tools in their evaluation and training process of the controllers to assess their skills in responding to emergency situations. Though Simulator training is not mandated by Regulators, Regulators do expect that the pipeline controllers who are being trained under 49 CFR 195.446 regulatory requirements can perform standard operating tasks such as opening and closing valves and starting and stopping pumps and to handle abnormal operating conditions.[19]

- Regulatory Environment – Oil and Natural Gas Infrastructures are governed by various federal, state, and local regulations. Major agencies involved in the regulation are described as follows:
    - **The Federal Energy Regulatory Commission (FERC) -** is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects.

    - **Department of Transportation (DOT) -** Natural gas pipelines and facilities are governed by DOT Federal CFR Title 49 Part 192 "Transportation of Natural and

[17] "Deciphering 49 CFR 195.446 Control Room Management," Mark Grant, Pipeline and Gas Journal, February 2011 https://pgjonline.com/2011/02/15/deciphering-49-cfr-195-446-control-room-management
[18] NERC Standard PER-003-1 – System Personnel Training; http://www.nerc.com/files/PER-005-1.pdf
[19] Schneider Electric 2013, "Impact of Oil and Gas Pipeline Simulators on Controller Training and Regulatory Compliance," available at http://www2.schneider-electric.com/documents/support/white-papers/oil-and-gas/Oil-pipeline-simulator-training.pdf

other Gas by pipeline- Minimum Federal Safety Standards". This part prescribes minimum safety requirements for pipeline facilities and the transportation of gas, including pipeline facilities and the transportation of gas within the limits of the outer continental shelf as that term is defined in the Outer Continental Shelf Lands Act (43 U.S.C. 1331). DOT has the responsibility and authority to promulgate safety standards, interpret the safety standards, inspect companies' adherence to the standards, and enforce these standards through the Department of Justice.

- **Department of Homeland Security (DHS) -** The "security responsibilities over other modes of transportation that are exercised by the Department of Transportation" was transferred to the Transportation Security Administration (TSA) as part of the Aviation and Transportation Security Act (Public Law 107-71). This places the responsibility for security of Petroleum and Natural gas pipelines under the auspices of TSA and DHS.

- **Office of Pipeline Safety (OPS) -** The Office of Pipeline Safety (OPS) of the DOT is charged with the responsibility to promote safe and environmentally sound operation of natural gas and hazardous liquid pipeline systems. OPS issues and enforces pipeline safety regulations, and provides training and technical assistance to state inspectors and industry.

- **National Transportation Safety Board (NTSB) -** The National Transportation Safety Board is an independent Federal agency charged by Congress with investigating every civil aviation accident in the United States and significant accidents in the other modes of transportation -- railroad, highway, marine and pipeline -- and issuing safety recommendations aimed at preventing future accidents.

- **U.S. Coast Guard -** The Coast Guard is involved in a variety of missions including search and rescue; marine environmental protection, enforcement of laws and treaties; ice-breaking operations for northern inland and coastal waters; drug interdiction; marine safety; and national security. The agency also plays a vital role in response to liquefied natural gas (LNG) transport and emergency response in the navigable waters of the U.S.

- **The Federal Emergency Management Agency (FEMA) –** is responsible for supporting state and local governments in dealing with disasters that require more than local resources can handle. FEMA becomes involved once the President, at the request of a state's governor, has declared a region a disaster

area. FEMA coordinates the activities of federal agencies that can provide services, resources, and personnel to perform necessary functions.

- **Public Utility Commission (PUC) -** In addition to the above regulatory agencies, state public utility commissions have standards and regulations regarding the natural gas infrastructure within each state.

There are similar examples of regulatory disparity in most areas of energy delivery, but this section is not intended as an exhaustive report on the issue. Rather, it's included as an illustration of how both EDS operators and consumers can be affected differently by the varying goals of regulation.

Challenges

The issues discussed in this section are, for the most part, of equal relevance and concern to all three of the major EDS systems – electric power, oil, and gas.

- Myth of security by obscurity – The energy delivery systems are undergoing rapid transformation due to the growing energy demands and increased dependence on operational technologies and open communication technologies. Historically isolated, relatively simple, and proprietary, the energy delivery systems are now becoming more complex and interconnected. Cybersecurity is now identified as a top national security issue due to the risks associated with data, computerized technologies, and Internet connectivity. Claims by the industry that ICSs are isolated from the internet and business functions are no longer reliable. Demand for near-real-time business data from the operation is driving the interconnectedness of the operational technologies with the business systems. Other example of the myth is that cybersecurity incidents will not impact the energy delivery operations. Recent incidents in the Ukraine have demonstrated the vulnerability of the control systems and the impact of disruption of the control systems in the energy sector.[20]

- Interconnectivity of Information Technology (IT) and Operational Technology (OT) systems - IT and OT has had predominantly separate roles within an organization. However, with the emergence of the Industrial Internet and the integration of energy delivery field components with networked sensors and software, the lines between the

[20] IEEE 2011, "Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs," available at https://841cd919-a-62cb3a1a-s-sites.googlegroups.com/site/ludovicpietrecambacedes/publications/files/TPD2010.pdf?attachauth=ANoY7cquoEHmrViO059gm586_DcBbRtUDvD66cWDu9jFxUe6N_lVZ5U4dz2XQup53qVz6_4h848m-wGfY-aQZuvXHY23P6ddoq2rexLQ80sq6MCchtYerUJXsoox5KYCqlffuzsiprTCDZnK1NMD7C1h1M-jde1b2qzoqc6EkIJXRAtcyj37iaKdceH81BtEuzQ3NnExE0-UPRwNeLD3mbz-K95f0qAiztQd8TpSSRX7lWNFP4mWgCJhLcyoT-0QM4-OW8ZQVZ6u&attredirects=0

two technologies are merging. The architecture and security objectives of IT and OT systems are significantly different, leading to issues when they are interconnected without regard to the differences and their purposes. In addition, in recent years the advance of Industrial Internet has started to explode into more OT Internet connectivity, as opposed to the historically closed systems that relied more heavily on physical security to ensure integrity. With this shift from closed to open systems comes an even greater interdependence and overlap between the two systems and a slew of new security concerns. Business is beginning to focus more on greater connectivity and integration in order to achieve smart analytics and control, although more connections and networked devices mean more opportunities for cybersecurity vulnerabilities. These networked systems are presenting new scenarios and risk issues to both systems.[21]

- Proliferation of internet-based commercial over the shelf (COTS) Software - Many control systems in use today were designed for operability and reliability during an era when security received low priority. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and communications technology. Infiltrating these systems often required specific knowledge of individual system architectures and physical access to system components.

  Under the pressures of continuous expansion, deregulation, and increased market competition, the energy sector shifted toward scalable control system architectures. Asset owners and operators gained immediate benefits by extending the connectivity of their control systems. They increasingly adopted commercial off-the-shelf (COTS) technologies that provided the higher levels of interoperability required among today's energy sector constituents. Standard operating systems, such as Windows or UNIX, are increasingly used in central supervisory systems which are now typically connected to remote field devices via private and public communication networks. Common telecommunications technologies, such as the Internet, public-switched telephone networks, and cable or wireless networks are also used. This elevated and open system hardware and software accessibility exposes network assets to potential cyber infiltration and subsequent manipulation of sensitive operations in the energy sector.[22]

- Interoperability - In the oil and gas sector, information produced by the ICS is typically required by a wide variety of applications, including: HMI/SCADA for visualization and

[21] GlobalSign 2016, "IT vs. OT for the Industrial Internet – Two Sides of the Same Coin?" available at https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet/
[22] U.S. Department of Energy 2006, "Roadmap to Secure Control Systems in the Energy Sector," available at https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf

control, Accounting Applications for Custody Transfer, Business Intelligence applications, and many others. The hardware components can range from rod pump controllers, to flow computers and meters to PLCs and DCSs–and will vary depending on whether we are discussing upstream, midstream or downstream operations. In a perfect world, all of this equipment would be standardized and provided by one enduring vendor. However, many oil and gas companies grow through acquisition and inherit sites comprised of disparate equipment–including legacy devices, or those that only speak native protocols. It is simply too expensive to rip out and replace these with equipment the acquirer prefers. Therefore, there is demand for a solution to manage these brownfield sites as if the acquiring company developed them from scratch, and a broader industry need to quickly and effectively integrate both legacy and modern technologies within the SCADA enterprise.[23]

Table 3 provides differences and commonalities of Industrial Control Systems and related impact to the operation for Oil and Natural Gas versus Electric Delivery Systems

Table 3. Energy Systems Attributes (Differences and Commonalities)

Attributes	Electric	Oil	Gas	Comments
Personnel Qualification	Electrical Engineer	Mechanical, Civil, Other disciplines	Mechanical, Civil, Other disciplines	
Physical Dynamics: typical maximum velocity, units of measurement	Energy Moving at the SPEED OF LIGHT (MW- Hour)	Liquid State: 3-6 mph, Barrels per day	Gas State: 20-30 mph Millions of cubic feet per day	
Energy Infrastructure SCADA underlying architecture	Electric Sector SCADA architecture designed around operational requirements. Migrating toward NIST IR 7628 Smart Grid Architecture	Oil Sector SCADA architecture designed around operational requirements and TSA security and API 1164 guidelines.	Gas Sector SCADA architecture designed around operational requirements and TSA security and API 1164 guidelines.	Field update time in minutes for O&G; milliseconds for electric. Various wired and wireless communication media and protocols used.
SCADA Electric, Oil, and Gas	Open loop	Open loop	Open loop	Open-loop means that a human being (Operator) makes the control decisions. Common to electric, oil and gas transmission, electric and Gas distribution

[23] Pipeline & Gas Journal 2013, "Five Key Challenges In The Oil And Gas Industrial Control System," available at https://pgjonline.com/2013/10/22/five-key-challenges-in-the-oil-and-gas-industrial-control-system/

Distributed Control System (DCS)	Closed loop	Closed loop	Closed loop	Closed-loop means that control decisions are made by a pre-defined computer algorithm (power plants, refineries, processing, and liquefied natural gas (LNG) plants, etc.
HMI - Alarming, trending, graphics	Power Models, on/off trends, current flow, voltages, etc.	Pipeline simulation and models – pressure, flows, temperatures, etc.	Pipeline simulation and models - pressure, flows, temperatures, etc.	Interface with special applications. Oil and gas sector recently applying API 1165 (display), and API 1167 (alarm) requirements standards.
Encryption	AES-256-bit encryption	Some application of AGA-12 Encryption standard, AES-256-bit encryption, etc.	Some application of AGA-12 Encryption standard, AES-256-bit encryption, etc.	Use of AES 128 and 256-bit encryption was observed in use by the recipient of the DOE Smart Grid Investment Grant in the electric sector. Encryption is still limited in deployment, especially in legacy installations.
Defense-in-depth	NERC CIP, NIST, and industry best practices applied	NIST, TSA Security Guidelines, API-1164 standards applied. ISA-99/IEC 63443	NIST, TSA Security Guidelines, API-1164 standards applied. ISA-99/IEC 63443	A layered approach (multiple layers of defense) in protecting the energy sector cyber-physical assets from exploits using industry best practices, federal guidelines, and standards.
Authentication/Communication protocols	NERC CIP standard, IEC 62351 suite—Secure Authentication for DNP3 communication	IEC 62351 suite—Secure Authentication for DNP3 communication Modbus	IEC 62351 suite—Secure Authentication for DNP3 communication Modbus	In general the EDS uses both the federal standards, as well as industry developed standards for use in implementing the authentication protocols and access control.
Cybersecurity Regulations	NERC CIP BES (mandatory standard for bulk electric system)	Voluntary Standards	Voluntary Standards	O&G uses American Petroleum Institute (API) 1164, NIST 800-82, NIST 800-53, TSA Security Guidelines, (API) 1164, API – Recommended Practice 780, Risk Assessment Methodology, ⊲ ISA/IEC-62443, Interstate Natural Gas Association of America (INGAA) – Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry, etc.
Time synchronization	Field update requires sub-millisecond accuracy	Field update time in minutes for O&G	Field update time in minutes for O&G	

Protocols	Ethernet, Modbus (TCP/IP, RTU, ASCII), DNP3, IEC 61850, IEC 62351 suite, Object Link and Embedding (OLE), Distributed Component Object Model (DCOM), and Remote Procedure Call (RPC). OLE for Process Control (OPC) as well as proprietary synchronous and asynchronous serial communication protocols.	Ethernet, Modbus (TCP/IP, RTU, ASCII) DNP3, IEC-870-5-101/104, Hart (IP, Wireless, etc.), Foundation Fieldbus, IEC 61158, PROFIBUS (Process Field Bus), Object Link and Embedding (OLE), Distributed Component Object Model (DCOM), and Remote Procedure Call (RPC). OLE for Process Control (OPC)	Ethernet, Modbus (TCP/IP, RTU, ASCII) DNP3, IEC-870-5-101/104, Hart (IP, Wireless, etc.), Foundation Fieldbus, IEC 61158, PROFIBUS (Process Field Bus), Object Link and Embedding (OLE), Distributed Component Object Model (DCOM), and Remote Procedure Call (RPC). OLE for Process Control (OPC)	IEEE 6189 suite—Known as AGA 12 (IEEE 1711). These standards secure SCADA equipment communication protocols. IEC 62351 suite—Secure Authentication for DNP3 communication
Communication	LAN/WAN and leased lines - Licensed and spread spectrum radios - Microwave - Satellite - Cellular networks (GPRS) and CDMA), including POTS	Optical fiber common on pipelines, backed up by VSAT. LAN/WAN and leased lines - Licensed and spread spectrum radios - Microwave - Satellite - Cellular networks (GPRS and CDMA)	Optical fiber common on pipelines, backed up by VSAT. LAN/WAN and leased lines - Licensed and spread spectrum radios - Microwave - Satellite - Cellular networks (GPRS and CDMA)	
Loss of SCADA data communication	Will continue to operate. Degradation to system reliability.	Oil pipeline may potentially shutdown for safety reasons.	Gas pipeline will continue to operate based on last operational field component settings.	

Safety Instrumented Systems (SISs)	Safety function in electrical systems is achieved by protective relays to isolate the fault.	SISs are used in the oil industry to detect the onset of hazardous events and/or to mitigate. Example: Refinery, Processing Plant, Pumping stations, etc.	SISs are used in the gas industry to detect the onset of hazardous events and/or to mitigate. Example Processing Plant, LNG, Compressor Stations, etc.	O&G systems are typically coupled to SISs that can take over and bring a process to a safe state. It is a safety system independent of the process control system.
Dependencies and Interdependences	Natural gas-fired electric power plants are dependent on the natural gas supply. Other non-nuclear generating stations are dependent on coal or oil supplies. Also dependent on communication systems, roads, and water/wastewater systems	Petroleum Infrastructure components are dependent on the electric power for pump stations, refineries, etc. Also dependent on communication systems, roads, and water/wastewater systems	Natural gas infrastructure depends on the electric power for pumps, cooling fans, etc., at compressor facilities and processing plants. The sector is also dependent on the petroleum sector for backup generator oil and other lubricating products. Also dependent on communication systems, roads, and water/wastewater systems	

Summary and Recommendations

We have described a number of commonalities among EDS sectors with respect to cyber resiliency, including similar cyber-physical architectures, operation, technologies, systems and communication protocols that are used across EDS sectors, and vendors that provide equipment to multiple EDS sectors. Other commonalities include common cybersecurity principles: It is a hard problem to provide a cybersecurity solution to a device that can't be physically secured, and unauthenticated communication protocols which are vulnerable if not wrapped in a security solution.

We've also described several differences of how each type of infrastructure operationally performs and its response to abnormal situation. These differences are, in the main, due to

differing physical properties and limitations of each energy product medium, rather than the delivery systems themselves. For example, natural gas is a compressible fluid, while petroleum is incompressible. And both of these can use physical storage to add flexibility, while electric power cannot yet be stored in significant quantities (MWh) and therefore must always maintain and respond to supply – demand balance.

We've also learned that EDS are vulnerable to intrusion from those looking to take over control and either shut down the system or cause physical harm. It's been proven that redundant controls can help to prevent such takeovers, or at least mitigate them to a great degree. Adoption by the operators of a policy favoring redundant controls for all ICS is recommended.

Over the last century or so each system has established an important and sustainable market for what each does best. Natural gas, in particular, was able to significantly increase its market by developing new technology: the concept and demonstration of underground storage. During the 1960's and '70's this allowed natural gas to become the primary fuel source for home heating in the U.S. More recently, new production technology has enabled the O&G sector to produce supplies (both crude oil and natural gas) that were previously unknown or deemed economically non-recoverable. It would also be beneficial to learn about some of the newer drilling and production technologies in use, what is 'unconventional oil and gas production', what are the pluses and minuses relative to renewable energy production, and what is required to get energy to market. In addition there are a number of projects underway in the U.S. and overseas to develop economical large-scale electric storage capability. If they are successful electric power could experience a similar growth.

This paper is not intended to be an in-depth discussion of the EDS subject matter. It's recommended that researchers and those making use of this document also review the material listed in the footnotes and learn the basics of tools and technologies used in the energy sector. In addition, it is important that there is a close collaboration between the researchers and the energy sector participants in identifying and developing cybersecurity tools and practices to protect the Nation' energy delivery system.

Terminology and Acronyms

AMI (advanced metering infrastructure): An integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers, used in electricity and gas.

BES (bulk electric system): For the purposes of this document, any transmission element operated at 100 kV or above

DCS (distributed control system): A form of ICS, in addition to SCADA. NIST SP 800-82 uses DCS in reference to systems that control processes in a local area, such as an industrial plant or a refinery.

EDS (energy delivery system): For the purposes of this document, a system to produce or deliver energy. This includes electricity generation, transmission, and distribution. It also includes oil and gas refining and pipelines.

EMS (energy management system): Systems in electrical substations to manage energy transmission or distribution. They are frequently coupled to substation SCADA and referred to as SCADA-EMS.

ICS (industrial control system): A generic term used to describe a wide range of control system components used in a broad variety of industrial systems, including EDS.

O&G: Oil and gas.

OT (operational technology): A term created to describe the cyber systems and networks used to support operations in an industrial environment. The term was created to differentiate these systems and networks from “traditional” IT networks.

SCADA (supervisory control and data acquisition): A form of ICS. This term is fairly widely used in a number of vertical markets, and may even be used regionally. NIST SP 800-82 uses SCADA to refer to systems that control dispersed assets. It is common, but not strictly correct, to use SCADA to refer to ICS in general.

Setpoint: the desired value in a closed-loop feedback system, as in regulation of temperature or pressure

SIS (safety instrumented system): A set of controls independent from the main process control, which senses that the process is about to enter an unsafe state, and restores the process to a safe state, possibly by safely shutting down the process.

WAM (wide-area measurement system): In power systems, this is a network of PMUs on a regional scale (one or more states).

About CREDC

The Cyber Resilient Energy Delivery Consortium (CREDC) is composed of nine universities and two national laboratories, led by the University of Illinois at Urbana-Champaign, conducting a variety of research activities in support of the cyber security and resiliency of energy delivery systems. Sponsored by the Department of Energy (DOE), CREDC follows from the earlier Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project. CREDC's research scope has expanded to encompass energy delivery systems outside the electric power sector, including oil and gas, as well as the complexities introduced by coupled energy infrastructures. CREDC conducts activities with anticipated deliverable prototype technology in an 18- to 24-month timeframe, as well as longer-term research that anticipates the impact of emerging disruptive technologies, such as big data and cloud environments as well as the Industrial Internet of Things (I2OT). The research is guided by an Industry Advisory Board and is often done in coordination with industry partners to maximize the beneficial impact of CREDC research on the sector.

The consortium includes researchers from Argonne National Laboratory, Arizona State University, Dartmouth College, the Massachusetts Institute of Technology, Oregon State University, the Pacific Northwest National Laboratory, Rutgers University, Tennessee State University, the University of Houston, and Washington State University.

Acknowledgments

This material is based upon work supported by the Department of Energy under Award Number DE-OE000078. The authors wish to acknowledge the assistance of subject matter experts who provided guidance and graciously gave their valuable time in the completion of this paper.

Disclaimer