Idaho State University

ISA GLOBAL CYBERSECURITY ALLIANCE

Idaho National Laboratory

U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response

OT Security Knowledge Framework: A Guide For Educators and Students

Second Edition 2025

CURRICULAR GUIDANCE

isu.edu | isagca.org | inl.gov | energy.gov

OT Security Knowledge Framework: A Guide for Educators and Students

Sean McBride, “OT Security Knowledge Framework: A Guide for Educators and Students”

Idaho National Laboratory

United States Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response

Idaho State University

International Society of Automation Global Cybersecurity Alliance

Version 1.1, December 2025

For the best user experience, download the document and review it with Adobe Acrobat or Adobe Reader to be able to navigate to a linked term and return to the text containing the link. After clicking on a linked term, indicated in blue text, and reviewing the explanation, you can return to the section containing the link by pressing the Alt and back arrow keys.

Acknowledgments

This document is the culmination of a multi-year collaborative effort among the Idaho National Laboratory (INL); the US Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER); Idaho State University, a National Security Agency-designated Center of Academic Excellence in Cyber Defense; and the International Society of Automation Global Cybersecurity Alliance (ISAGCA) under the supervision of Dr. Sean McBride.

The work would not have been possible without the time of nearly 100 anonymous survey respondents who contributed an average of 45 minutes each. We appreciate their time and participation in this project.

Special recognition goes out to Glenn A. Merrell, ISA Certified Automation Professional (CAP), of Freelance Consulting/Industrial Control Systems Security, for his careful, expert technical review.

Thank you to Liegh Elrod, ISA Book Publishing Manager for her editorial review of the publication.

We would also like to recognize Carl Schuett of QED Secure, Heidi Cooke of ISAGCA and Sami ElMurr of Hunter Strategy, who selflessly volunteered to help analyze the extensive survey results from which the list of terms was derived.

Thank you to Jill Slay and Corey Schou for the counsel they provided in the early stages of research that culminated in this document.

We appreciate the contributions from the following interns from the INL who helped author entries in the Process Equipment section: Jana Richens, Cade Williams, Jack Hall, Thomas Wood, Robert McLendon, Evan Singer, Zachary Dalton, Brian Schumitz, Daniel Gurvich, Remy Stolworthy, Ashley Michelich and Levi Farber.

Special thanks to Rob Smith, Eleanor Taylor, Ralph Ley and Dr. Shane Stailey of the INL for their unflagging support of the project.

Thank you to ISA99 WG15 for taking this document under change control. Please report any errors or concerns about this document to the ISA Working Group 15 cochair, Sean McBride, SeanMcBride@isu.edu.

Copyright

Introduction

This document provides educators and students with a description and taxonomy of 531 terms and concepts that an operational technology (OT) security professional needs to know *that are not provided in traditional cybersecurity programs*.

It was created in response to the recognition that our increasingly digitized world requires a new class of professionals who can work effectively in engineering, information technology (IT) and cybersecurity domains to securely design, build, operate, maintain, dismantle and defend cyber-physical systems.

By providing this framework of required knowledge, the organizations from industry, government and academia who sponsored this document intend to help establish a basis for formally developing OT security training and education programs.

Those programs must include elements that are addressed by other efforts, such as targeted work roles and tasks, program-level objectives, course sequences, course-level objectives, learning activities and evidence-based assessment methodologies.

To help readers think comprehensively about the terms and concepts included, the guide is organized around the analogy of a building with three components: 1) an environment, 2) a foundation and 3) a superstructure, as seen in Figure 1.

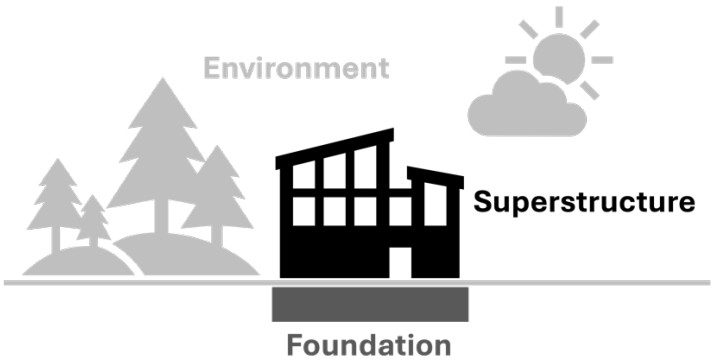

Figure 1: Industrial Cybersecurity Knowledge Model

- The *Industrial Operations Environment* section of this guide describes the contexts (business, geopolitical, professional and industry) within which industrial control systems and industrial cybersecurity exist.
- The *Industrial Control Systems Foundation* section of this guide describes the elements (instrumentation and control, process equipment, industrial networking and communication, and process safety and reliability) that must be secured.

- The *Industrial Cybersecurity Superstructure* section of this guide describes the elements (guidance and regulation, common weaknesses, events and incidents, and defensive techniques) that most immediately come to mind for industrial cybersecurity.

Within each organizational component, the terms and concepts are further divided into categories, topics and subtopics up to six levels deep. In addition, the document makes extensive use of cross-referenced hyperlinks to facilitate navigation. Linked terms, indicated in blue text, can be clicked to move to that entry. A link at the bottom of each page returns the reader to the Table of Contents.

Details about the methodology used to create this document can be found in the academic paper "What Does An OT Security Professional Need To Know?," included as Appendix A. Users may also wish to review a webinar on this paper (watch the recording; view the slides) or download the supporting data and analysis.

Table of Contents

Industrial Operations Environment

"Industrial operations" are generally considered to be the processes involved in the automated or large-scale production of goods, extending from extracting natural resources to creating consumable products. The industrial operations environment consists of the various contexts or stakeholder perspectives involved in industrial operations, including business, geopolitical, professional and industry contexts.

Business Context

The "business context" is the perspective of the organization engaged in industrial operations. This can range from a global enterprise, such as an energy company with subsidiaries organized in scores of countries, to a small municipality that operates a water provisioning system. Relevant key terms from the perspective of a business/organization include production operations, IT versus OT, organizational roles, supply chain, supply and demand, capital budget and expense, cost center versus profit center, human capital, business continuity, regulation and business risk.

Production Operations

The term "production operations" refers to the physical work of making a product or producing a good. Businesses sometimes call this the "production arm" or "operations arm" of the organization. It includes the production facilities, processes, equipment, industrial control systems, policies and procedures, and professionals who physically manufacture the product. This differs from other organizational functions such as strategy, marketing, sales, human resources or even engineering.

IT Versus OT

"IT" stands for "information technology" and refers to the computers and network equipment that process data.

"OT" stands for "operational technology" and refers to the instrumentation and control systems, along with the supporting computers and network equipment, that manipulate not just data but elements of the physical, real world.

"OT" is often used synonymously, or near synonymously, with "industrial control systems" (ICSs), "industrial automation" and "process control systems," terms that predate "OT." In strict interpretation, "OT" also encompasses nonindustrial cyber-physical systems and processes, and therefore, may be a preferable term in some circumstances.

Connecting IT networks with OT began practically at the moment the first programmable logic controllers (PLCs) added a data port to enable data acquisition, precipitating significant challenges between the organizational divisions that operate these technologies. It is important to recognize that IT and OT professionals have disparate educational and disciplinary preparation, reporting chains and performance priorities. Organizations that successfully manage cybersecurity risk will intentionally address the disparities between the two groups.

Organizational Roles

"Organizational roles" refers to the types of organizations that deal with ICSs. These are vendors, integrators, owner/operators and maintenance providers. The industrial cybersecurity guidance found in the ISA/IEC 62443 standards refers to these as "principal roles."

ICS Vendor

An ICS vendor manufactures and markets industrial control systems software and/or hardware solutions. This organizational role may include a dedicated or independent product distribution network. While there are thousands of firms serving this market, leading vendors include Rockwell Automation, Yokogawa, Emerson Process Management, Honeywell Process Solutions, Siemens Industrial Automation, Schneider Electric, Yaskawa, GE, Kuka and Mitsubishi Electric Automation, each with strengths across different functions, industries and geographies.

ICS Integrator

An ICS integrator deploys and integrates the control system components within the controlled process as defined in a contract, typically in a design specification. This is a common function among engineering firms.

ICS Owner/Operator

An ICS owner/operator is a business or organization that owns or operates the production process and associated equipment. An asset owner may contract the asset operation to an operator service provider.

ICS Maintenance Provider

An ICS maintenance provider specializes in maintaining industrial processes and their associated equipment and control systems. Some ICS owner/operators perform this function, while some outsource it to firms that specialize in maintenance. Common maintenance tasks include adding lubricants, changing filters and replacing failed process equipment or control system components. Prominent ICS maintenance providers in the United States include Black & Veatch and Veolia.

Supply Chain

The supply chain is a network that obtains and provides raw materials and components to be manufactured into final products, many of which are combinations of dozens or even hundreds of previously manufactured products. Complex global supply chains are essential to operating even the smallest businesses. Products with a dominant market share at certain steps in the supply chain can exert seemingly inordinate influence on the reliability and security of final products. This concept applies equally to software and physical manufactured goods.

Supply and Demand

Supply and demand are core business and economic concepts that describe how markets operate. “Supply” refers to the quantity of a good or service that is available, and “demand” refers to the quantity of a good or service desired by consumers. Successful businesses aim to produce the greatest share of demanded quantity and quality at the lowest cost of production. Organizations that automate their mass production processes and keep them running will maximize profits.

Capital Budget and Expense

The term “capital budget and expense” refers to the funds set aside (budget) and used (expense) to buy physical equipment (generally not software) to be used in business operations. Capital can include debt or equity, and it ideally contributes to revenue generation (making money). Capital budget and expense is generally distinct from the ongoing operations and maintenance budget and expense categories.

Profit Center Versus Cost Center

“Profit center” and “cost center” are accounting terms that describe whether managers view a department as a source of revenue (a profit center) or a necessary expense (a cost center). This is a pivotal distinction because business managers are generally more willing to use resources if they can clearly see a return (profit) on those resources. Industrial automation falls clearly within the profit center of a manufacturing operation. IT and cybersecurity are more likely to fall within the cost center of a manufacturing operation.

Cost-Benefit Analysis

Cost-benefit analysis is a comparison of the costs and benefits (including time, energy, expertise and money) of an investment. The concept applies in numerous contexts but is particularly applicable to technology specification and procurement. When considered across the total lifetime of an investment, cost-benefit analysis is sometimes referred to as the “total cost of ownership.”

Human Capital

"Human capital" refers to the employee assets of an organization. Competitive businesses and organizations recognize that competent employees drive success; therefore, they spend time ensuring that employees are adequately trained to perform their required tasks and are rewarded for high performance. Within production operations, this training includes careful consideration of safety and security elements.

Business Continuity

During its existence, a business or organization may face a variety of challenges, including geopolitical unrest, loss of key employees, mistakes, lawsuits, natural disasters and cyberattacks. Successful enterprises plan to address key elements of these events before they occur, thus ensuring business continuity.

Regulation

Regulation is the legal and procedural framework that punishes organizations (usually through fines) for failing to meet minimum acceptable standards of behavior. Regulations may be set by law or by delegated authority. Many aspects of a business, including financial dealings, safety and cybersecurity, may be subject to regulation.

Business Risk

Business risk is the way that business managers think about the things that could go wrong for their business. The common approach is to consider events that could harm the business, such as its finances, reputation and employees, as well as the public and the environment. Managers then consider whether and how to reduce, transfer or accept the risk. Conversations about process safety and reliability, and cybersecurity often focus on loss reduction as opposed to the expected return on investment (ROI).

Geopolitical Context

The "geopolitical context" is the relationships that exist between global political powers (i.e., nation-states) that compete or cooperate with one another for control over scarce resources that are a significant source of wealth. Components within the geopolitical context include natural resources, national borders, technological development, conflicts, military capabilities, state-owned enterprises, demographics, state security services, capabilities and geopolitical risk.

Natural Resources

Natural resources include the biological and geological components of the Earth from which products useful to humanity are derived. Examples include minerals, metals, plants, and oil and natural gas deposits. Natural resources are found in key geographic locations throughout the Earth. Nation-states organize themselves to obtain natural resources.

National Borders

National borders are the agreed-upon physical limits of control between one nation-state and another. Natural resources exist within national borders. Nation-states may seek access to natural resources within another nation-state's borders through cooperation or coercion.

Technological Development

Within the geopolitical context, "technological development" refers to the specialization of tools and techniques that a nation-state can use to achieve its objectives. It is the cumulative, long-term result of ingenuity and capital investment aimed at maximizing output for a given set of inputs within a nation-state. Modern manufacturing processes are the result of technological development fostered in the private and government sectors. Countries with greater technological development may outcompete countries with lesser technological development. In general, nation-states with greater technological development are more susceptible to cyber events and incidents than those with lesser technological development.

Critical Infrastructure

Critical infrastructures are the systems and resources on which modern societies and economies are built, such as electricity, communications and water systems. The loss or impairment of these resources would have devastating effects on businesses, communities and governments. Critical infrastructures may be designed, built, operated and maintained by private/non-government and/or government organizations. As a result, some nation-states play a direct role in defending their infrastructures, while others may offer only indirect support. Some governments classify critical infrastructure by industry sectors or groupings of similar functions. While this is useful for administrative purposes, infrastructure sectors are highly interdependent.

Conflicts

Nation-states may disagree about access to resources or rightful reward structures, or they may simply want the upper hand. Conflicts occur when nation-states seek to impede the progress or damage the infrastructure capabilities of one another, prompting them to employ physical violence, economic sanctions, harsh words, diplomatic rebuffs and covert actions.

Military Capabilities

The term “military capabilities” refers to the organized armed forces of a nation-state. Militaries rely on and operate a variety of critical ICSs. They may also designate units to plan and launch attacks against essential facilities and processes using a variety of techniques, including cyberattacks.

State-Owned Enterprises

State-owned enterprises are for-profit businesses that are heavily influenced or entirely controlled by a nation-state. National governments around the world use businesses to achieve their interests and policies to varying degrees. The emergence of world-leading, state-owned enterprises with high levels of specialized technological development as pillars of global supply chains causes other countries to fear interest-preserving action (such as sabotage) when conflicts arise.

Demographics

Demographics are the general characteristics of individuals, including citizens and noncitizens, residing within the boundaries of a nation-state. Demographics can include age, religion, education level, ethnicity, population density and geographic dispersion, among others. Demographics are important factors in explaining and predicting attitudes and behavior, which can in turn be central to understanding (including causing and responding to) conflicts.

State Security Services

State security services are government agencies tasked with maintaining political order within and outside the country’s physical boundaries among its citizens and in relation to citizens of other countries. Some security services may characterize their mission in terms of political ideals (such as “a rule-based international order”), others in terms of preserving the status of a country’s current rulers. State security services frequently engage in intelligence gathering (spycraft) and in planning and carrying out covert actions (government-sponsored actions for which the government does not claim credit). Actions against critical infrastructure systems of other nation-states are well within the scope of state security services.

Capabilities

Within the context of a nation-state conflict, the term “capabilities” refers to the people, procedures, technologies and tools that a military or state security service can bring to bear for both defensive and offensive security measures. The capabilities—which may include deception, cyberattacks and counterattacks, sabotage or other direct military action against identified targets—are important to consider when evaluating the risks posed by a nation-state.

Geopolitical Risk

Geopolitical risk is the estimation of the causes, timing and consequences of adverse events involving foreign countries, including conflicts between nation-states. Consumer markets in foreign countries, reliance on foreign suppliers and complex global supply chains are factors that influence exposure to geopolitical risk. Some insurance policies exclude losses resulting from geopolitical events, such as war, from coverage.

Professional Context

Professional context is the viewpoint of the individuals involved in industrial operations. It consists of professional roles and responsibilities, as well as workplace safety.

Professional Roles and Responsibilities

Archetype professional roles involved in industrial operations include engineers, technicians, process operators, control room operators, shift supervisors and plant managers. These roles may be filled by employees or contractors, and each requires specialized knowledge and awareness to perform key tasks securely. The management C-suite, including the chief executive officer (CEO), the chief operating officer (COO), the chief information officer (CIO) and the chief information security officer (CISO), is responsible for appropriately setting priorities and allocating resources. Ethics and operational security are significant concerns for every role.

Engineer

An engineer is a professional who applies specialized knowledge to design and specify many types of products, processes and systems. Engineers make calculations based on requirements, create drawings and develop bills of material. With a focus on design, engineers are less involved in the day-to-day operation and maintenance of the systems they design; however, they must be cognizant of the effects of their work at each stage of the lifecycle. Most engineers receive formal preparation in a four-year engineering degree program. Engineers frequently specialize in a specific field, such as chemical, mechanical, civil or electrical engineering. They may obtain an engineering license by meeting requirements that include passing an exam. In the United States, the National Council of Examiners for Engineering and Surveying (NCEES) offers a Control Systems Engineering exam. In many parts of the world, regulating authorities classify engineers based on their training and/or third-party professional certifications. Some organizations only allow engineers or other certified professionals to program the control system, including the operator interfaces (both local and supervisory) and controllers (PLCs). In contrast, others allow trained technicians to perform this task. In engineering projects, it is common for engineers to report to a lead or chief engineer. In some organizational hierarchies, a chief engineering officer (CEngO) may oversee all engineering efforts to ensure quality, efficiency and innovation.

Technician

A technician is a professional with specialized knowledge of and the ability to use an engineering technology. Within an industrial operations environment, “instrument technician,” “engineering technician” and “maintenance technician” are common job titles. Instrument technicians specialize in selecting, configuring, calibrating and deploying various types of sensors, transmitters and controllers. Many technicians receive formal preparation in a two-year, hands-on engineering technology degree. Some choose to demonstrate their competence by obtaining a professional certification, such as ISA Certified Control System Technician (CCST). Some organizations allow trained technicians to program controllers.

Process Operator

A process operator is a trained professional responsible for operating an industrial process, such as a manufacturing line. In many cases, process operators may be considered factory floor workers. Process operators generally do not require formal academic preparation; instead, they gain significant knowledge about the process they operate through on-the-job training and experience.

Control Room Operator

A control room operator is a specialized process operator who, instead of working on the factory floor, works in a control room where they exercise supervisory control over the industrial process by watching and interacting with a supervisory interface. Becoming a control room operator frequently requires years of experience and training as a process operator. Some industry sectors require control room operators to obtain highly specialized training and industry-specific certification.

Shift Supervisor

Many industrial operations run continuously for longer than a typical working day—some run 24 hours a day. This requires work to be divided into shifts. A shift supervisor oversees what happens within the industrial environment—especially to the industrial process and on the plant floor—during their duty period. Technicians, process operators and control room operators all report to the shift supervisor. The shift supervisor reports to the plant manager. It is important to recognize that shift changeover can be a particularly critical or potentially vulnerable moment, as a new team may be stepping into an existing or emergent situation that they may not fully understand.

Plant Manager

Plant managers are responsible for plant operations, and all plant employees ultimately report to them. Plant managers are frequently evaluated on their ability to maximize plant productivity and efficiency, achieving expected product quality with high production and low costs. They are knowledgeable about all aspects of a plant, and they interface between the technical professionals

who make the plant run and the business management. Plant managers frequently have formal training in business management. The plant manager reports to the chief operating officer.

Chief Executive Officer (CEO)

The CEO is the individual ultimately responsible for the operation of a company or organization. The CEO is the public face of a company and, generally speaking, is chosen by and reports to a company's board of directors.

Chief Information Officer (CIO)

The CIO directs and oversees all of the information infrastructure that supports company operations. This includes information technology-related personnel, hardware (such as computers and networks) and the software that facilitates productivity and information flows. In some cases, the CIO may also be responsible for software development activities. The CIO normally reports to the chief executive officer.

Chief Information Security Officer (CISO)

The CISO is ultimately responsible for ensuring business systems remain trustworthy and reliable. The CISO sets the security strategy and directs the security architecture development. The CISO normally reports to the CIO. Historically, the CISO has focused primarily on information systems (IT assets) rather than industrial control systems (OT assets).

Chief Operating Officer (COO)

The COO is responsible for a company's day-to-day operations. For an industrial enterprise, this may include responsibility for multiple plants/industrial facilities, meaning that many Plant Managers report to them. COOs are less knowledgeable about the specifics of any given plant, but very knowledgeable about the business environment in which the company operates, including its business model, customers, competitors, regulations and general risk environment. COOs frequently have formal training in business management and years of experience in various aspects of an industry. The COO reports to the CEO.

Ethics

Ethics are the guiding principles of responsibility to other human beings and the planet. They are an important component of every job role within an industrial organization. The specialized knowledge and access possessed by every employee could put the lives and reputations of coworkers, the health of consumers and the public, and the viability of the business at risk.

Operational Security (OPSEC)

"Operational security" refers to the basic precautions that every employee should take to protect the organization and its mission from would-be threats, including malicious insiders, competitor

companies, activists and other countries. These precautions include exercising caution when sharing potentially valuable details, marking and securing valuable information, wearing identity badges, confronting questionable behavior and reporting suspicious activities.

Policies and Procedures

Within the context of industrial operations, policies refer to documents that explain how decisions should be made. Policies often include a title, a reference number, a statement of objective, job titles affected by the policy, descriptions of allowable and unallowable activities, descriptions of enforcement mechanisms and the consequences of nonadherence. Policies affecting industrial operations may cover topics such as health and safety, acceptable use of company equipment and waste minimization.

Procedures are the steps workers are to follow to ensure desirable outcomes, including those specified in policies. Within the industrial operations context, technical professionals, including engineers, technicians and process operators, often follow standard operating procedures and safety protocols that describe the steps for performing the work in detail. Policies and procedures are usually gathered in operating manuals and handbooks. Employees should know where to find policies and procedures, and be appropriately trained in following them.

Workplace Safety

Workplace safety is an essential element of the professional context of industrial operations. Personnel who enter industrial facilities must be familiar with various aspects of workplace safety preparation, depending on their roles and responsibilities. Workplace safety practices can vary from employer to employer and location to location. This curricular guidance document emphasizes electrical safety because cybersecurity personnel are most likely to be exposed to electrical safety hazards—especially when accessing control enclosures. Other workplace safety topics could include chemical safety, pressurized equipment safety (hydraulic and pneumatic) and process equipment safety. Other key workplace safety concepts include personal protective equipment, lockout/tagout, safe work procedures, safety regulations and workplace safety communications.

Electrical Safety

Electric current above 50 mA (milliamps) is dangerous to human health. Electric current above 100 mA can be fatal. Anyone working around electricity—especially in an industrial environment, such as an open control enclosure—should be aware of basic electrical safety, including lockout/tagout procedures.

Lockout/Tagout

“Lockout/tagout” refers to disconnecting electrical service (power) or any stored energy from equipment that is under maintenance or repair. A physical lock with a safety tag is attached to any

energy connection/disconnection point to notify all parties that they should not restore power because doing so could injure or kill a worker.

Personal Protective Equipment

"Personal protective equipment" (PPE) refers to safety equipment used by workers in a variety of industrial settings. This can include eye protection, hearing protection, protective footwear, a bump hat, nonmelting fabrics, a harness and more. While many industrial organizations provide industry-specific, facility-specific and role-specific training to employees, all individuals, including IT, networking and cybersecurity personnel, who enter the operations area of an industrial facility should be proactive and vigilant about the proper use of PPE.

Safe Work Procedures

Work procedures describe how work is to be performed within an industrial environment. Every procedure should include provisions for performing the work safely. These procedures are developed by conducting a safety risk assessment. Each party participating in the work should fully understand their role and how to perform their work safely before work begins. Work that is performed on a regular basis may already have a well-documented safe work procedure in place, along with regular training. Following safe work procedures can affect the lives of coworkers and other stakeholders, not just the individuals who perform the work.

Safety Regulations

Safety regulations are the rules that organizations must follow to keep their workers safe. In the United States, this includes regulations produced by the Occupational Safety and Health Administration (OSHA) and other relevant agencies. The regulations cover safe working practice topics, such as exposure to harmful substances, fire protection, fall protection and exposure to infectious diseases.

Workplace Safety Communications

It is essential to effectively communicate safety information to employees and contractors within industrial environments. These communications must be clear, timely and relevant. They must reflect the evolving environment, including the weather, the quantity of expected personnel present and the nature of the work being performed. Workers must be trained to understand safety communications quickly and correctly, and to take appropriate action. Workplace safety communication systems include sirens, visual beacons and public address systems. Digital workplace safety communication systems face risks, including false communications and intentionally suppressed communications.

Industry Context

"Industry context" refers to the type of work being accomplished. Topics include industrial processes, industry sectors, facilities, engineering documentation and industrial lifecycles.

Industrial Processes

An industrial process is a series of steps that leads to the large-scale production of a good. Created by process engineers, industrial processes rely on industrial control systems to control process equipment within an industrial facility. Industrial processes can be categorized by the way that a product moves through each step. These categories include continuous, discrete and batch. It may be useful to consider "continuous" and "discrete" as opposite ends of a spectrum, rather than mutually exclusive categories. Recognizing the process category is useful in understanding the consequences of a disturbance.

Continuous Processes

Continuous processes are those that occur without interruption and in which the product is not accounted for in individual units produced. Key examples include wastewater treatment and electricity generation.

Discrete Processes

Discrete processes are those that repeatedly create individual units. Discrete processes account for most consumer goods manufacturing, from golf balls to silverware.

Batch Processes

Batch processes conceptualize the process in terms of "at a time" production capacities. Baking cookies is a simple and familiar example of a batch process. The ingredients are mixed and processed as a "batch." The same process equipment could be used to make a batch of chocolate chip cookies today and a batch of oatmeal raisin cookies tomorrow.

Industry Sectors

Industry sectors represent groupings of similar work processes and products. Within the United States, the Department of Homeland Security (DHS) recognizes 16 "critical infrastructure" sectors; however, the US DHS groupings are not the only reasonable way to discuss industry sectors. In the European Union, the critical infrastructure sectors are organized by areas providing essential services. It may be helpful to recognize that sectors may have alternate or related names, that there are often high interdependencies and that the line between industries is not always clear. Common industry sector groupings include electric power, oil and natural gas, petrochemical, food and pharmaceutical,

mining and metals, manufacturing, pulp and paper, water and wastewater, buildings, transportation and nuclear.

Electric Power Sector

Since the discovery of electricity in the 1820s, electrical power has achieved ubiquitous adoption in developed societies, with all facets of life (including other industry sectors) depending on its continuous, reliable delivery. The electric power industry can be divided into three main verticals: generation, producing electricity at generating plants such as hydroelectric dams; transmission, moving electricity from the generating plants through long-distance corridors of low-gauge wire to the general vicinity of its consumers; and distribution, spreading reasonable voltages of electricity from distribution substations to industrial, commercial and residential electricity consumers.

Oil and Natural Gas Sector

The oil and natural gas industry identifies oil (petroleum) and natural gas deposits buried beneath the Earth, extracts those deposits ("upstream operations"), converts them into consumable products ("midstream") and delivers the products to end users ("downstream"). Oil is a liquid that is generally moved by pumps, while natural gas is in a gaseous state and is usually moved by compressors. Oil products include gasoline, diesel fuel and jet fuel that are critical to the transportation industry. In 2023, natural gas was the fuel source for nearly 40% of commercially generated electricity in the United States.

Petrochemical Sector

The petrochemical industry uses midstream oil and natural gas operations (such as oil refining) to create chemicals that support a multitude of manufacturing processes, including plastics, synthetic fibers and adhesives.

Food and Pharmaceutical Sector

The food and pharmaceutical industry provides products that humans and animals consume to remain alive and healthy. This industry entails plant science, farming, animal science, livestock and medicine. Agriculture is often described as the basis of society and civilization because humans cannot survive without food sources, let alone organize to achieve greater objectives.

Mining and Metals Sector

The mining and metals industry identifies valuable elements and compounds contained within the Earth's crust, extracts these resources, and processes them into an astounding array of primary and secondary goods. For example, this industry takes iron ore from the ground and produces steel rebar and I-beams for constructing buildings, sheets of aluminum for making automotive bodies, ferrous cores for large power transformers and cast iron for Dutch ovens (and other products).

Manufacturing Sector

"Manufacturing" refers to industrial operations that make all classes of products. It is often referred to as "discrete" manufacturing, which produces products that can be counted. Items in this category range from apple pies to zip ties and from baseball bats to yellow yarn.

Pulp and Paper Sector

The pulp and paper industry utilizes a variety of plant-based inputs, such as trees, to produce high quantities of consumer goods, including toilet paper, printing paper and cardboard.

Water and Wastewater Sector

The water and wastewater industry fulfills the basic human need for consumable fluid that composes 60% of the adult human body. Waterworks serve the consumption and sanitary needs (including cleaning and flushing) for small and large population centers. In some locations and jurisdictions, the industry protects the environment through treatment processes, such as coagulation, flocculation, sedimentation, filtration and disinfection, before returning the water to the natural environment.

Buildings Sector

Buildings—in some cases known as "the built environment"—provide protection from the forces of nature, security from spying or attack and physical organization, as well as centralized access to supporting services such as electric power and running water. Buildings can incorporate a variety of automated services, including energy management, heating, ventilation, air conditioning, locks and lighting.

Transportation Sector

The transportation industry manages moving people and goods from one location to another via maritime shipping, ground vehicles (including automobiles and trains), pipelines and airplanes.

Nuclear Sector

The nuclear industry specializes in materials, equipment and processes related to energy-emitting subatomic particles, including nuclear power plants and their supply chains. The discovery and development of nuclear energy in the 1930s and 1940s altered the global balance of power through the creation of the nuclear bomb that precipitated the end of World War II. The promise of inexpensive energy through nuclear fission led to the buildout of nuclear power plants in various countries in the post-war period. The radioactivity of nuclear fuel in its various lifecycle stages remains a challenge to the continued adoption of nuclear energy worldwide.

Facilities

Facilities are buildings (or areas) designed for specific purposes. Facilities frequently house industrial equipment and processes, but are often considered to be separate from those processes. Facilities may also be mobile, such as trains, ships and aircraft. Important topics within facilities include facility type, facility planning and design, facility location and facility-wide services.

Facility Type

Each facility is characterized by the industry it supports and the processes that take place within it. For example, facilities in the electric industry can include generating stations, switchyards and substations. Facilities in the natural gas industry can include natural gas fields, storage areas, compressor stations and town gates. Some firms specialize in designing facilities, others in building them and others in maintaining them. Firms may operate similar facilities in various locations, choosing to standardize a facility (and process) design.

Facility Planning and Design

Facility design involves reducing the concept of a facility to firm details. It may require site surveys, impact assessments, public hearings, and permits and approvals. Outputs include engineering documentation and project plans. Facility planning and design can require years before the first shovel is turned. This phase may provide crucial information and access to forward-thinking adversaries.

Facility Location

A facility's location is a strategic decision that considers expertise available in the local economy, access to natural resources, distance from major population centers, access to transportation and other important factors. The location is an important factor for determining risk to the environment (the impacts of a spill or release), from the environment (what natural disasters are most common in the area?) and from would-be adversaries (what geographical advantages or disadvantages would an adversary have to view, approach or attack the facility?).

Facility-Wide Services

Facilities contain industrial processes and equipment. They provide the infrastructure on which those industrial processes rely. Examples of facility-wide services include electric power; heating, ventilation and air conditioning (HVAC); compressed air; lighting and physical security. Technicians and maintenance personnel assigned to the facility may have a separate organizational structure from those involved in the industrial process.

Electric Power

The facility-wide electric power service is the power supply that supports the entire facility. This normally includes step-down transformers outside the building, and it may include a battery system or an on-site generator as a temporary backup power source in case off-site power fails. The electric power service also includes the electrical wiring and outlets for various voltages.

Heating, Ventilation and Air Conditioning

Heating, ventilation and air conditioning, commonly referred to as HVAC, provides key environmental controls within a facility. Different portions of a facility may require different internal environmental controls. Without these controls, it may not be ideal or even possible for the process to operate or for workers to remain within a facility.

Compressed Air

For some process equipment, compressed air is as necessary as electric power or HVAC. This may be provided by a large, centralized compressor that supports multiple processes or process lines, with regulators ensuring that the pressure in any process meets the operating range.

Lighting

Lighting is a key facility-wide service that enables round-the-clock industrial operations. Energy management systems may be configured to turn lights on or off based on detecting human presence. Some light sources are more energy efficient than others. Light can influence employee health and productivity, and adequate lighting plays a key role in ensuring safety and security.

Fire Protection

Fire protection is an integral concern for commercial and industrial facilities that must comply with the requirements of the authoritative jurisdiction. The details of the facility and process being controlled influence the type of fire that could occur and the appropriate protection and/or suppression approach to deploy. Fire protection systems can include fire-stops, alarms, and automatic and manual systems. They can be configured to communicate with local firefighters.

Physical Security

Physical security systems control entrance (ingress) to and exit (egress) from facilities and within facility areas, including locking or unlocking doors and turnstiles. These systems can deter and delay unauthorized individuals and provide useful records about the credentials presented, dates, times and locations.

Engineering Documentation

“Engineering documentation” refers to the detailed information required to design, build, operate and maintain an industrial facility and its components. Such documentation includes facility drawings,

process flow diagrams, piping and instrumentation diagrams, loop diagrams, wiring diagrams, product specifications and user manuals. In addition to their primary use, the details in such documentation may be of great value to competitors and/or adversaries alike.

Facility Drawings

Facility drawings, such as blueprints, prepared by engineers, specify the physical aspects of the facility, including its precise physical location, shape, dimensions and materials. Drawings for industrial facilities can be hundreds of pages long and require specialized knowledge and practice to interpret fully.

Process Flow Diagrams

Process flow diagrams are graphical depictions of the steps or stages in an industrial process, showing how inputs are transformed into processed outputs. The diagrams use arrows to indicate the process direction and order.

Piping and Instrumentation Diagrams

Piping and instrumentation diagrams, commonly known as P&IDs, use symbols standardized by the International Society of Automation to represent the process equipment and control system components used in an industrial process. The diagram is similar to the process flow diagram but provides additional detail about the organization, location and function of controllers and transmitters. P&IDs include graphical detail about multiple control loops.

Loop Diagrams

Loop diagrams provide important details about each control loop, which is designated by a loop number. Details include the wiring that extends from sensors/transmitters (field instruments) through terminals to the controller, as well as the signal type and calibration associated with each input and output.

Wiring Diagrams

Wiring diagrams are graphical depictions of the terminals (electrical connection points) of electrical devices and equipment, as well as the wires that connect them in an electrical circuit or circuits.

Product Specifications

Product specifications describe the key characteristics of a product and may include images of various aspects of the product, dimensions, wiring diagrams and safety ratings. Specifications, colloquially known as “spec sheets,” are frequently used by engineering and technology professionals to select a product that meets their requirements. A product specification differs from a user manual, which helps a professional who already has a product understand how to use or interact with it. Specifications can be located on a product vendor’s or distributor’s website.

User Manuals

User manuals provide detailed, step-by-step guidance on how to install, connect, control, communicate with, manage and maintain a product. Manuals often provide images, tips, warnings and references to other useful resources. A manual is much longer than a product specification and can be found on the vendor's website.

Industrial Lifecycles

The term "Industrial lifecycles" refers to the stages of existence for industrial facilities, processes, control systems and the products produced. The idea that a company or organization is responsible for a facility, process, product or system from its initial conception through end-of-life is a powerful analytical tool with special application to cybersecurity. Lifecycle activities are often carried out as projects. Lifecycle stages might look slightly different for an industrial control system asset owner than for a vendor, but the stages for both generally include design, specify and procure, build, operate and maintain, support and dismantle. Key concepts within a lifecycle also include asset management and change management.

Design

In the design stage, a facility, product, process or service is reduced from an abstract idea to an increasingly realistic representation through a series of plans, drawings and models. The design phase can take years. For consumer goods, designs themselves are often modified on a regular basis (such as annually) to create new and improved versions. Designs frequently incorporate products that are outputs from other lifecycles.

Specify and Procure

As a lifecycle phase, "specify and procure" refers to deciding which material inputs will be incorporated into the final product, facility, process or system and then obtaining them. Specifying is often an engineering task, where the exact characteristics of an input are important. Procurement is often a business task that involves ensuring a sound understanding of the specified good, obtaining and testing samples, negotiating the price and placing an order. Once trusted relationships are in place, the procurement process is often streamlined and automated.

Build

The build phase of the lifecycle follows the specify and procure phase and involves creating or assembling the physical elements of the facility, process or system. The build phase is often much shorter than the operate and maintain phase that follows it. Building a facility, process or system is frequently handled by contractors rather than by the firm that owns and operates it. Within the build phase, initial deployment and configuration merit special attention from cybersecurity practitioners.

Operate and Maintain

In the operate and maintain phase, the process or facility is operational; it is carrying out its intended mission. The operating and maintaining phase is typically the longest and can last for decades. Large industrial facilities often operate 24 hours a day, 7 days a week because they are turning a profit for the company. Some failures and breakdowns can be addressed with minimal impact on plant productivity. Other issues accrue until a scheduled "turnaround" or maintenance outage window.

Support

Support is a lifecycle phase that applies primarily to product vendors. This involves answering customer questions and addressing errors in hardware or software that a customer has purchased and is currently using. Many vendors offer online product support forums where customers pose questions and provide answers, often to one another. Some asset owners purchase support contracts that include a minimum level of service or a number of support hours from the vendor. When a vendor designates a product as "end-of-life," it no longer supports that product. Some industrial firms specialize in supporting end-of-life products that are no longer supported by their original manufacturers.

Dismantle

Dismantle is the lifecycle phase in which the facility or process is permanently shut down and disassembled. Some consumer products have a short lifespan, meaning that the industrial process lasts less than one year. When an industrial facility is closed, dismantling can take a long time and is often carried out by outside contractors.

Asset Management

"Asset management" refers to 1) maintaining an accurate record of an organization's assets and 2) using that record for a variety of planning and operations purposes. An organization's assets can be organized into categories and subcategories such as facilities, processes and components. Two prominent examples of asset management are 1) predictive and preventive maintenance and 2) change management.

Change Management

"Change management" is the formal process of maximizing plant and process reliability through proposing, approving, testing, fully implementing, documenting and monitoring changes to a facility or system. Key concepts for change management include system models, inventory, device configurations, software and hardware, recalls, errata, release notes, software bills of materials, backups and change records.

Integrated System Model/Inventory

An integrated system model is the central software interface to support safety, reliability and security decisions, including change management, for a system or set of systems. Information available within the model may include details about facilities, locations, processes, engineering documentation, network information (such as IP addresses) and the names and contact information of responsible individuals. Keeping the model accurate and up to date ensures continuity among the "as designed," "as built" and "as exists" versions of a facility, system or process. Because an integrated system model may contain all current information about the system, it is a high-value target for potential attackers.

Device Configurations

Device configurations describe the settings—hardware and software—of any equipment used in an industrial facility or process. Examples could include the placement of jumpers on pins within a transmitter, the scaling of a 4–20 mA signal and whether logging is enabled. Device configurations should be kept under change management and be included in an integrated system model.

Software and Hardware

Software is the code or logic that determines how a system operates. The term "hardware" can refer to the physical aspects of a computerized system or the actual process equipment. Both software and hardware should be kept under change management. Entries for software and hardware in the integrated system model could include relevant images and other helpful documentation.

Recalls

A product vendor may issue a recall when a product has a known flaw that must be addressed. The term "recall" most frequently applies to a physical product, whereas the terms "advisory," "patch" and "update" are commonly associated with a software product. One important use of an integrated system model is to help an asset owner identify deployed hardware and software for which the vendor has issued a recall. Recognizing the applicability of a recall may result in a change to the process or system.

Errata

Errata is a statement released by a product vendor that formally recognizes an error in documentation or performance after a product has been released for use. The error may or may not warrant a recall. One important use of an integrated system model is to help an asset owner identify deployed hardware and software for which the vendor has issued an errata statement or list. Recognizing the applicability of an error may result in a change to the process or system.

Release Notes

When a vendor releases a patch, a new version of software or a computer-based product, they may provide "release notes," a text document/file that describes the changes made. In many cases, the

changes enhance the quality and functionality of the product. Careful reading of release notes may identify the presence of security weaknesses in prior versions (even when the vendor has made no other public vulnerability disclosure). Reviewing release notes may help an asset owner determine whether to deploy a patch or update.

Software Bill of Materials

A software bill of materials describes the components of a software product much as a bill of materials describes the subassemblies and components that compose a physical product, such as a refrigerator. Modern software products may integrate open-source and other commercially licensed code. Knowing the software bill of materials can enable an asset owner to recognize relationships and relevant vulnerabilities that would otherwise remain obscure. Prepared with this knowledge, an asset owner can determine when a change (such as a firewall rule or a software update) may be advised.

Backups

A backup is a saved copy of data or software. Its purpose is to facilitate system restoration in the event that the primary data or software is damaged or destroyed. As a change management mechanism, a backup can help roll back a problematic change. As a reliability and security mechanism, a backup can help quickly restore a system to a known good state.

Change Records

Change records are documents that describe the changes made to a system, including who made them and when. They are the essential elements of a change management regime. Some change records may be automatically generated (such as security logs), while others are manual entries.

Industrial Control Systems Foundation

This section describes the core industrial control system (ICS) terminology required for an individual's professional success in securing control system components, control system functions and society-supporting infrastructures provided by control systems. Categories include instrumentation and control, process equipment, industrial networking and communications, and process safety and reliability.

Instrumentation and Control

The term "instrumentation and control" represents a category of foundational ICS knowledge. As it is not uncommon for electric power to be considered as part of instrumentation and control, control systems professionals sometimes refer to it as electrical instrumentation and control systems (EI&CS). The category includes industrial control systems, control theory, control system components, programming and control logic, alarm management and control system software.

Industrial Control Systems (ICSs)

ICSs encompass a wide brushstroke of study and practice that applies technology to automate and control a range of industrial processes (such as electric generation, oil extraction and wastewater treatment) as a central component of production operations and facilities management. The terms "industrial control systems," "industrial automation," "process control" and "operational technology" (OT) are often used synonymously. The preferred term may vary across time, industry sector and geography.

Control Theory

"Control theory" refers to the conceptual underpinnings of process control. Key control theory terms and concepts include control loop, set points, process variables, control variables, primary control elements, final control devices, feedback, open and closed loops, process dynamics, error, control algorithms, control strategy, loop tuning, simulation and modeling, dead band and dead time.

Control Loop

A control loop is the fundamental concept of control theory. Its purpose is to regulate an industrial process. The word "loop" represents the circular relationship that exists between a set point and a process variable through the manipulation of a final control device.

Set Points

A set point is the desired physical condition of an industrial process at a certain point in time. For example, the set point for a residential dwelling could be 72°F during the day and 68°F at night.

Process Variables

Process variables are the current actual measurements of the physical characteristics of a system. Common process variable types include temperature, pressure, level and flow. For example, in a residential cooling system, if the current temperature in a home is 82°F, the process variable is 82°F.

Control Variables

A control variable is the output of the device that directly influences the process variables. For example, if the set point of a temperature control system for a residential dwelling is 72°F and the process variable (actual temperature) is 82°F, the control variable for the air conditioner should be "on." In addition to values such as "on" or "off," a control variable may also be a position, speed, rate or any one or a combination of many other physical properties.

Primary Control Elements

The primary control element is the device that measures the process variable. In common language, this can be considered a sensor. For example, in the case of residential air conditioning, the primary control element is the sensor within the thermostat. Sensors for temperature, pressure, level and flow can rely on various principles of operation to obtain their measurements.

Final Control Devices

A final control device physically implements a change based on a comparison between the process variable and the set point. In simple terms, the final control device is the actuator. In a temperature control system within a residential dwelling, the final control device could be the relay that allows electricity to energize the air conditioner. In many other processes, the final control device regulates a rate, such as a valve positioner that governs the rate at which liquid flows through a pipe. Final control devices are also known as finite elements.

Feedback

The term "feedback" refers to the continual or periodic input into the decision-making component of a control system (often a controller) that results in the manipulation of the dynamic behavior of a final control device. For example, in the case of a residential cooling (air conditioning) system, the feedback is provided by the continual measurement of the temperature and its comparison with the set point. Once the temperature reaches the set point, the controller sends the signal to turn the air conditioner compressor "off" or vary the speed of the compressor and associated fans and motors.

Open and Closed-Loop

Control systems are often characterized as either open or closed-loop. An open-loop control system relies primarily on human input to make adjustments (such as manipulating the final control device). For example, in an open-loop system, once a human operator observes that a tank has reached its "full" mark, the operator closes a manually operated valve to prevent additional fluid from entering.

An open-loop system can achieve a minor degree of automation by deploying a simple timer. For example, a timer is set to turn off the inflow to the tank 15 minutes after the inflow began.

A closed-loop control system, on the other hand, requires no human intervention to make an adjustment because a sensor verifies the desired state or process value. For example, a float switch sensor indicates that a tank is "full," and the controller sends a signal for the motor to adjust the associated valve or vary the speed of or turn off a feed pump. Closed-loop systems have increased the reliability, efficiency and safety of production operations by minimizing the number of humans required to operate a facility. Determining which control actions should be taken in response to sensor inputs is a design consideration with significant safety and reliability implications.

Process Dynamics

"Process dynamics" refers to the way an industrial process changes over time, given differing inputs and external loads/context. Reduced to a discipline, process dynamics is the mathematical model that describes how a process operates and is controlled.

Error

The error is the difference between the set point and the process variable. The error value is a key component of feedback, enabling a controller to implement a control algorithm. In the example of a residential cooling system, the error is the difference between the current temperature (82°F) and the set point (72°F), which is 10°F. Error can also be expressed as a percentage of the set point. In this case (10 / 72 = 13.8%).

Control Algorithms

Control algorithms describe the mathematics that determine what actions a controller instructs final control devices to take to align the set point and the process variable. Key control algorithms are proportional, integral and derivative. These are commonly referred to collectively as PID control.

- **Proportional Control**
  The final control device should be actuated by the same amount, either directly proportional or inversely proportional, as the deviation between the process variable and the set point (also known as the error). For example, if there is a 5% deviation (a 5% error), the valve should be moved by 5%.
- **Integral Control**

The final control device should be actuated to account for historical residual differences between the process variable and the set point. Expressed simply, integral means the amount that actuation should be updated based on how well proportional control worked the last time it was used.

- **Derivative Control**
  The final control device should be actuated in anticipation of the future effects of the actuation and fully accounting for the current rate of change of the error.

A controller that can implement all three of these algorithms is known as a PID controller (which is not to be confused with P&ID, a piping and instrumentation diagram).

The concept of PID control is directly founded in physics and calculus, having many mechanical variations dating to the seventeenth century. The first standardized PID algorithm for automation and control systems was developed by the Instrumentation Society of America (now known as the International Society of Automation) and is called the ISA PID equation.

Control Strategy

In many industrial processes, complex and interdependent relationships exist among set points, process variables and control variables *in different loops*, requiring a process engineer to select and apply a control strategy. Control strategies can include feedforward control, ratio control and cascade control and result in an engineered functional design of the control system.

- **Feedforward Control**
  This strategy aims to implement an understanding of how a particular process works (a process model) to control the disturbance (source of error) rather than the error. For example, rather than controlling the amount of water in a continuous boiler based on the current water level, a feedforward strategy would control the flow of steam out of the boiler by considering the water level within the boiler as a source of disturbance in steam flow. Feedforward is often implemented alongside PID control.
- **Ratio Control**
  This strategy aims to maintain optimal performance by seeking a set point that is a designed mathematical ratio between process variables, rather than using two individual values that might otherwise compete with one another.
- **Cascade Control**
  This strategy uses the output of one controller as the input to another controller, essentially forming a nested loop. A cascading loop is applied when different control process values need to be derived and controlled for other parts of the control system. This enables controlling the process in the fastest and most efficient manner.

Loop Tuning

Loop tuning is the action taken to optimize the action the controller takes in response to a set point change. Some controllers support self-tuning; others require manual tuning. Specialized software can aid in the tuning process. Loop tuning will affect the amount and duration of the error between the set point and process variable, ultimately influencing the efficiency of a process over time.

Simulation and Modeling

Process and control system simulation and modeling techniques provide insights that help control systems professionals identify and meet the reliability, repeatability, availability and safety requirements of control system functions. Control system vendors use simulation and modeling to develop new products or product features. Engineers use simulation and modeling to optimize a process before or after deployment. Owners and operators use simulation and modeling to train process operators (including control room operators).

Simulation and modeling software can incorporate physics, chemistry and mathematics principles that provide realistic system behavior and operator experience. Simulations may also include details about computers and networks. Virtual reality can provide an immersive and realistic visual experience. Simulation and modeling services are often referred to as “virtual plant” or “digital twin” technologies.

An accurate, up-to-date, integrated system model helps industrial cybersecurity professionals make timely decisions that balance the expectations and requirements for reliability, repeatability, availability and safety, and cybersecurity. For example, an accurate integrated model can help a professional recognize which assets are affected by a newly disclosed cybersecurity vulnerability, where those assets are located, who has access to those assets, and whether and when the asset should be patched.

Dead Band and Dead Time

“Dead band” refers to the range of process variables for which no control action is taken. This results in a period of time (dead time) in which no control action is taken. Dead band may be intentionally built into the controller to minimize the costs associated with frequent oscillations between system states, such as wear on equipment from continuously turning equipment on and off. For example, one might find a dead band range of 4 degrees built into a residential air conditioning system. That is to say that given a set point of 72°F, the air conditioner will not turn on until the temperature reaches 74°F and will not shut off until the temperature reaches 70°F. No control action will occur within this 4-degree dead band. It is also common for control system engineers to use the term “hysteresis” to describe dead band and dead time.

Control System Components

Control system components are the devices and interfaces that make up a control system. They include control rooms, control centers, control panels, control enclosures, sensors and transmitters, controllers, operator interfaces, engineering computers, application servers and motor controllers.

Control Centers

A control center may contain control information for multiple facilities; it is a hierarchical layer above a control room. For example, operators in a natural gas control center in Texas may be able to view and interact with industrial processes at dozens of compressor stations throughout the United States.

Control Rooms

A control room is a room where operators supervise the control of all the industrial processes within a facility. The room includes control panels and large displays designed for rapid assimilation of key information. Computerized operator workstations allow operators to interact remotely with a process if necessary. Telephones and radios facilitate communication with process operators or technicians on the plant floor, with the engineering team and with control system vendors.

Control Panels

Frequently found in a control room, a control panel is the console or display from which a process operator or control room operator observes and interacts with an industrial process. A control panel may be physical or digital, or a combination of both. Control panels typically contain various purposefully designed and configured components.

Control Enclosures

A control enclosure is a cabinet typically constructed of metal, plastic or fiberglass that provides physical environmental protection for the components inside. Enclosures frequently contain power supplies for control system components, controllers, input and output modules, terminal blocks, wiring and a network switch. Panel-based human-machine interfaces (HMIs) are often mounted to the front of a control enclosure to facilitate local control by a process operator.

Components within the enclosure are often mounted on a DIN rail and/or back panel. Workplace safety regulations and industry procedures govern when and how to open each enclosure. In contrast, regulatory codes govern the arrangement and separation of various components and power within a control enclosure. Because enclosures provide physical access to key control system components, they may be subject to physical access control measures.

Operator Interfaces

Operator interfaces are the technologies designed for human operators to interact with a controlled process in real time. Those range from simple pushbuttons, switches and lights arranged on a panel

or enclosure to complex computer graphics depicting the entire architecture of a process. Interfaces display the controlled process and status as representative icons and graphics, often in real time. Operator interfaces are usually called human-machine interfaces (HMIs). Two basic types are the supervisory interface (SCADA HMI) and the panel-based/skid-mounted interface (HMI).

Supervisory Interface (SCADA HMI)

A supervisory interface is commonly known as a "SCADA interface," where SCADA stands for supervisory control and data acquisition. Beyond the physical interface, SCADA is a control philosophy developed by ISA to combine the theories of automated supervisory control with the previous approaches for data acquisition. SCADA may be deployed as a large monitor/screen or a set of monitors located within a control room and/or control center that displays information and graphics about the industrial processes that are occurring within a facility or facilities. Supervisory interfaces may also incorporate real-time video feeds to and from the plant floor. The software enables the control room operators to remotely "reach in" and control (start, stop and alter) the process manually if necessary. Supervisory interfaces are often web browsers within a Microsoft Windows operating system pointed at an application server, though other operating systems are used. The application server is usually located in a server room or data center. This client-server architecture enables control room operators to work remotely if desired. Numerous control systems vendors provide SCADA software. Because of their ability to interact with the controlled process, supervisory interfaces are high-value targets to would-be attackers.

Panel-Based/Skid-Mounted Interface (HMI)

A panel-based/skid-mounted interface is normally a small screen mounted near the process that is being controlled, sometimes on the front of a control enclosure. The panel-based HMI is networked to the programmable controller and displays process information for that specific process. Process operators can use the interfaces to start, stop or adjust the process. Panel-based HMIs commonly run on an embedded version of Microsoft Windows.

Human-Machine Interface (HMI) Design

Because HMIs are used by local process operators and control room process operators to start, stop and adjust a process, ease of use is an important consideration. Engineers or technicians who design HMI screens must consider the size, placement and color of the icons, graphics, text and buttons for an optimal user experience under dynamic conditions, including emergency situations. The International Society of Automation offers the ANSI/ISA-101.01-2015 standard and ISA-TR101.02-2019 technical report to assist with HMI design.

Engineering Computers

Engineering computers are a variety of computers used by engineers or technicians in an industrial environment. These include engineering workstations, technician laptops, contractor computers,

tablets, process analyzers, calibrators and configurators. These computers incorporate hardware that suits their deployment and use (such as industrially hardened form factors).

Engineering Workstations

The computers engineers who design and support the industrial control system for a process or group of processes are commonly known as engineering workstations. The workstation frequently operates on a Microsoft Windows operating system and typically includes a range of software to program controllers, design supervisory interfaces, and design and program panel-based HMIs. The workstation may be continuously connected to the process control network and reside in office space within the facility. The workstation will have access to every aspect of the process control network, making it a valuable asset that needs protection from compromise.

Technician Laptops

A technician's laptop may include software that is similar to that on the engineering workstation, but in a more portable hardware form. Technicians may carry the laptop with them between industrial processes and potentially between facilities. The laptop may be used to update controller firmware or make programming adjustments to controllers. As such, it is likely to include various versions of controller programming software, compatible versions of controller firmware and, potentially, PLC program files, along with other useful software. These valuable assets require protection from compromise.

Contractor Computers

Contractor computers are substantially similar to engineering workstations and technician laptops, but are normally brought on-site or connected remotely to the process control network by contractors who have specialized expertise in a certain aspect of the industrial process or technology. Control systems integrators and vendors are common types of contractors whose computers may attach to the control network. Because these devices are not managed by the control system owner/operator, they may present an additional or unknown risk that asset owners must fully consider.

Tablets

Tablets are handheld computers that serve a mixed function between a technician's laptop and an operator interface, often connecting to the process control network via Wi-Fi.

Process Analyzers

A process analyzer is a type of sensor/transmitter (field instrument) that helps identify the physical properties and chemical compositions of gases or liquids. The analyzer output aids in adjusting process characteristics to enhance process efficiency and product quality. Process analyzers are

particularly common in chemical, petrochemical and pharmaceutical processes. A wide variety of instrument manufacturers provide process analyzers.

Calibrators and Configurators

Calibrators and configurators are handheld devices that enable technicians to calibrate, configure and test transmitters and actuators, often using the HART digital communication protocol. Many of these devices support wireless connectivity to a plant network for immediate storage and retrieval of calibration and configuration information. Common calibrator and configurator vendors include Fluke, Emerson and Endress+Hauser. Due to their transient use by engineers and technicians, these oft-forgotten devices must be specifically included in cybersecurity policies and procedures.

Application Servers

Application servers provide information services to hosts on a process control network or the corporate network. These can include process data historians, supervisory interfaces, manufacturing execution systems and enterprise resource planning. The network placement of these servers depends on network architecture and security requirements. In a large organization, application servers may process business-critical information for global operations. These high-value assets require protection from compromise.

Process Data Historians

Process data historians maintain a history (a database) of process variables, set points and control variables with other data relative to operations and maintenance. Data from process historians is commonly useful for a variety of industrial operations and business purposes. As such, replicating a historian from the process control network into the corporate network can create a redundant source of data while protecting the storage location. It is also common to find dual-homed historian servers (accessible from both the process network and the corporate network). Because of this connectivity, process data historians are often identified as possible pivot points for attackers moving from the corporate network onto the process control network. Manipulating data within a historian may impair the ability to conduct an accurate analysis and lead to poor decisions. Unavailability or permanent loss of data within a historian may significantly impair business operations or result in regulatory consequences. Common process data historian vendors include Aveva (formerly OSIsoft), Canary Labs and Aspen Technology.

Manufacturing Execution Systems (MES)

An MES is a software package dedicated to linking business systems, such as enterprise resource planning systems, to production operations, including industrial control systems. Typical functions or modules of an MES include work order management, scheduling, production monitoring, quality management, inventory management, traceability and performance dashboards. Other systems and terminology related to the MES can include “laboratory information management,” “warehouse

management" and "maintenance management." Because they provide critical information about and linkages to production operations, MES are high-value targets for would-be attackers. Typical MES vendors include SAP, Dassault Systèmes, Siemens and Rockwell Automation.

Enterprise Resource Planning (ERP)

ERP software integrates the management of core business functions across an enterprise. Common ERP components and modules include customer relationship management, sales, procurement, production, distribution, accounting, human resources, asset management and business intelligence. ERP systems not only contain sensitive company information but they can also link closely to manufacturing execution systems and, therefore, to industrial control systems, making them high-value targets to would-be attackers. Typical ERP vendors include Oracle (NetSuite) and SAP (S4/HANA).

Controllers

Controllers are specialized electrical devices that monitor for inputs (such as a process variable) and drive outputs (such as a control variable) accordingly. The invention of the programmable logic controller in the late 1960s revolutionized manufacturing by replacing both workers and individual control relay schemes. Significant topics related to controllers include relays, controller hardware, input/output, controller memory, tags, program scans, programming key switches, programmable logic controllers (PLCs), distributed control systems (DCSs), remote terminal units (RTUs), intelligence electrical devices (IEDs), protective relays, safety controllers and soft PLCs.

Relays

Relays are simple electromechanical devices that change electrical connections (circuits) based on the presence or absence of an electric current that energizes or de-energizes a magnet. Relays can be arranged to form fixed logic control scenarios. Early automation systems relied on such relays and could only be modified through rewiring between the relays or repiping air or fluids between various relay-controlled actuators. While microprocessor-based programmable controllers have replaced electromechanical relays in many cases, relays are still actively and appropriately used in modern industrial control systems. Because electromechanical relays are not programmable, they offer a degree of immunity from cyberattacks, but are susceptible to malicious, intentional physical damage and strong, induced electromagnetic pulses that may be difficult to detect or monitor.

Controller Hardware

"Controller hardware" refers to the physical components that comprise a controller. These devices are engineered to withstand temperatures, vibrations, pressures, dust, moisture and many other conditions that may exist in an industrial environment. A typical PLC may rely on an AC (alternating current) or DC (direct current) power supply. The form factor normally includes a processor module (commonly called a CPU module), a network module (which may also be integrated into the CPU) and various input and output (I/O) modules. Depending on the manufacturer and design architecture,

PLCs may separate functions, such as safety, logic control, input and output communications, and network communications, into separate internal CPUs to increase reliability and the availability features necessary in a control system. The modules connect to one another such that information from the I/O modules is buffered and made available to the CPU modules and other PLC functions.

The CPU can be programmed from an engineering computer over the network (if it has a network card) or via a serial connection (such as USB). The CPU module contains various configurations of microprocessors and circuits for performing common tasks using nonvolatile and volatile memory. Many controller form factors have external interfaces (such as SD or MicroSD) for inserting memory cards that store current versions of the control functions program or retain critical process values necessary for starting a process. Some have battery backups for retaining values within volatile memory in case of power loss. Most form factors have a programming key switch. PLC designs have, since circa 1990, implemented various security schemes into their designs and recommended architectures. However, deploying available security features ultimately depends on the willingness of the end user to 1) include security within the control system's functional specification and 2) bear the increased expense associated with the enhanced security features.

Input/Output

Input and output, also known as "I/O" and "IO," carry input electrical and/or physical signals (that represent process variables, such as temperature, pressure, level, flow, etc.) from the sensors/transmitters to the CPU module and output signals (control variables) from the CPU module to the actuators and/or indicators. I/O modules vary by the type of signal supported by the transmitter or actuator. Electrical I/O modules will have terminals to support one or more connections. Some I/O modules support wireless connectivity. Remote I/O adapter modules may be used to connect physically distant sensors and actuators to the PLC. When programming the CPU module, it is necessary to accurately identify which physical terminal corresponds to each transmitter or actuator, as misassignment can cause devastating impacts.

Controller Memory

Controller memory may be nonvolatile for storing firmware and program files and volatile for storing a loaded program and process data. Many PLC configurations rely on a battery backup to help ensure that volatile memory is preserved. Each programmable controller vendor has its own way of structuring controller memory. Common concepts include program memory, data memory, data types and tags. Program memory stores the user-generated controller program. Data memory stores the values corresponding to inputs and outputs representing the current state of the controlled process. Data types describe whether the values are Booleans, integers, floating points and so on, and tags help programmers refer to specific locations within data memory.

Tags

A tag is a human-readable reference to a location within controller memory. This concept (familiar in many programming languages) enables technicians and engineers to program controllers and operator interfaces to quickly recognize what is being calculated, considered, measured or controlled. An example tag name would be TC204_SP, which may indicate the temperature control loop 204 set point. Tag designation could also include a data type, a scope (which programs with a controller could use the tag) and an access level (such as read/write). Clear and well-documented tag naming conventions can be essential in helping others understand a controller program or operator interface program.

Program Scan

"Program scan" refers to the order in which a programmable controller handles its tasks. The three primary components of a program scan are update inputs, execute the program and update outputs. In addition, controllers must also manage communications (such as from other controllers, operator interfaces or engineering computers) and run diagnostics. It is important to recognize that there is a very deliberate order of operations to be maintained within the context of a dynamic (potentially high-speed) physical environment and that overwhelming a controller or disrupting its timing can have significant real-world consequences.

Programming Key Switch

The programming key switch is a physical switch (toggle switch) on the front of a programmable controller that enables a user to select programming modes. While nuances exist among vendors about the functionality of each position, common switch locations include "run," "program" and "remote." "Run" tends to mean that the controller cannot be changed or programmed through any remote connection. "Program" tends to mean that the controller will accept new programming, but does not execute new logic while it is being programmed. "Remote" tends to mean that the key switch can be moved virtually between "run" and "program" with remotely connected software. The programming key switch can perform an important safety and security function by requiring physical access to the controller before it can be programmed. Some key switches include removable keys; others are merely switches that cannot be separated from the device. Even removable keys are commonly left in the controllers, and switches are widely left turned to "remote" mode for the sake of convenience. The programming key switch can be a significant safety and security control, given that many commonly implemented process control network protocols do not support authentication services such as passwords. An alert should be provided to operations, engineering and security teams each time the switch position changes (especially to "remote").

Programmable Logic Controllers (PLCs)

"Programmable logic controller" is the common name, and "PLC" is the common abbreviation, for general-purpose, programmable controllers that receive input signals (such as 4–20 mA or 1–5 V),

process the data from that signal and make control decisions, which they send to actuators for implementation. PLCs commonly use real-time operating systems such as VxWorks. Leading PLC vendors include Rockwell Automation, Siemens Process Automation, Schneider Electric and Mitsubishi Electric Automation.

Distributed Control Systems (DCSs)

DCSs are turnkey automation systems that incorporate controller hardware and supervisory software into a single system from a single vendor, typically distributed across a large industrial site. DCSs are commonly found in the petrochemical sector. Leading vendors include Honeywell Process Solutions, Emerson Automation Solutions and Yokogawa Electric.

Remote Terminal Units (RTUs)

RTU is the term used in certain industry sectors (including electric power, oil and natural gas, and mining and metals) for a programmable controller that aggregates control at remote locations. Leading RTU vendors include ABB, GE Grid Solutions, Siemens Energy and Schneider Electric.

Intelligent Electrical Devices (IEDs)

An IED is a programmable controller applied to equipment in the electric power sector, such as transformers and circuit breakers, and used to make control decisions based on characteristics such as voltage and frequency. IEDs may be connected to RTUs or operate independently. Leading IED vendors include ABB, GE Grid Solutions, Siemens Energy and Schneider Electric.

Protective Relays

A protective relay is a special type of IED programmed to open a circuit breaker, shutting off the flow of electricity, when dangerous conditions are detected in an electric transmission or electric distribution system. Protective relays may have hardware and functional characteristics that are similar to a PLC, but they are intended to regulate electrical processes.

Safety Controllers

A safety controller is designed for industrial processes and environments where loss of human life is a paramount concern. While safety controllers perform the same basic functions as a standard programmable controller, they conform to international standards for fault diagnosis and fault tolerance by implementing diagnostic and redundant circuits within the controller's internal hardware. Safety controllers may be designed, built and tested to meet industry-specific or application-specific requirements, such as a burner management safety controller.

Soft PLCs

"Soft PLC" generally refers to a traditional, general-purpose computer (that relies on a Windows or Linux operating system) that is used to perform PLC-like tasks. Soft PLCs take advantage of existing

mass supply chains, are generally less expensive and can be programmed with standard text-based programming languages.

Motor Controllers

Motor controllers refer to the controller technologies specifically applied to electric motors. These include motor starters, adjustable speed drives, motor protection and smart motor controllers. Motor controllers are frequently located within motor control centers (MCCs).

Motor Starters

Motor starters are electrical devices that protect electric motors by limiting inrush current to short durations during motor start-up. Starters can also be set to disconnect a motor when a predetermined load (demand) on the motor is exceeded. Motor starters are commonly deployed for generators and conveyor systems. A programmable controller may close a circuit to a motor starter, which then softly starts the motor. The absence of a motor starter may represent a cyber-exploitable condition that could quickly damage a motor by repeatedly starting and stopping it.

Adjustable Speed Drives (ASDs)

Many electric motors have just two positions: on or off, full speed or no speed. An ASD enables an electric motor to operate at different speeds by altering the characteristics of the voltage and frequency supplied to the motor, greatly increasing the precision of motor-driven industrial processes and the energy efficiency of the motor. ASDs are also known as variable frequency drives (VFDs), adjustable frequency drives (AFDs), variable speed drives (VSDs) and AC drives. ASDs can be mounted on a wall, within a control enclosure or within an MCC. Using vendor-provided software, a user can input the parameters of the controlled motor and then set the speed, acceleration and deceleration, skip frequencies and overload limits. Typical vendors include Siemens, Rockwell Automation, Danfoss and Yaskawa. ASDs are valuable assets that require protection because manipulating the programming can have significant impacts.

Motor Protection

Motor protection consists of the techniques and mechanisms to safeguard an electrical motor from electrical, thermal or mechanical faults resulting from vibration, overcurrent, undercurrent, overvoltage, undervoltage and phase failure conditions. Protection devices include overload relays, circuit breakers, fuses and temperature sensors.

Motor Control Center (MCC)

Industrial facilities and processes that rely heavily on electric motors often aggregate motor control equipment within an MCC. An MCC receives incoming electricity and centralizes the control, protection and distribution of medium to high voltage electricity to the various motors within the facility. MCCs are placed within protective enclosures and can be located in their own building, in their

own room or along a wall, typically close to the equipment they control to minimize expensive cabling and line loss.

Smart Motor Controllers

A smart motor controller incorporates a variety of functionalities, such as motor protection, soft start, torque control, preprogrammed speed profiles, remote monitoring and control, and communications interfaces into a single motor control device.

Sensors and Transmitters

Sensors and transmitters measure and communicate, respectively, the physical characteristics of a process. These measurements are known as the process variables. Important terms related to sensors and transmitters include sensors, transmitters, engineering units, transduction, principles of operation, temperature, pressure, level, flow, calibration and configuration, scaling, transmitter failure mode, transmitter security, meters and smart instrumentation. Sensors and transmitters are sometimes referred to as "field instruments." Sensors and transmitters may also be used in motion control.

Sensors

A sensor is the element that presents the physical characteristic of a process as a measured value (process variable), such as temperature, pressure, level, flow, specific gravity, density or weight (though many other types of sensors exist). It is important to recognize that a sensor identifies the value by applying the principles of operation. Relying on a variety of physical techniques and specially designed electronic circuits, the sensor typically provides its value to a transmitter.

Transmitters

A transmitter takes the measured value provided by the sensor and communicates it to the system (such as to a controller) using a signal, typically using purpose-designed electronic components. In addition to communicating with the system, some transmitters, called "indicating transmitters," include a display to enable a human to read the value and the associated signal being transmitted. While sensors and transmitters are often tightly integrated, it is important to recognize that they are technically different elements with different purposes. Transmitters have various levels of functionality and programmability. Process engineers will specify the range (high and low engineering units handled) and resolution (degree of precision/significant digits) required from a sensor/transmitter in a particular application. Transmitters are frequently tested and calibrated before deployment. Some industrial processes require periodic testing during operation. Accurate readings from and predictable behavior of transmitters are essential to safe, reliable and effective process control. Leading transmitter vendors include Endress + Hauser, Emerson Rosemount and Honeywell.

Engineering Units

An engineering unit of measure is a standard for communicating an amount. For example, temperature may be expressed in degrees Fahrenheit or in degrees Celsius. The International System of Units (SI) applies special prefixes (such as deci-, centi-, kilo- and mega-) to describe the unit size. Ensuring consistency of measurement units throughout a system is essential to safe, reliable and effective process control, and to human understanding of the scale of operations and the scale of event impacts.

Transduction

Transduction is converting a physical characteristic to an electrical signal. For example, a P-to-I transducer changes pressure (P) to electrical current (I) and could be used to measure fill level by placing it at the bottom of a reservoir. An I-to-P transducer (notice the different order of the terms) could be used in a pneumatically actuated valve positioner to implement the specified control variable.

Principles of Operation

The "principle of operation" is how the sensor obtains its measurement. Various techniques exist for measuring process variables. For example, flow could be measured by a vortex shedding meter or by a magnetic flow meter. Specific details of the process being controlled determine the appropriate principle of operation to apply, that is, the type of sensor to use. The type of sensor chosen can have a significant influence on the reliability of the controlled process.

Temperature

"Temperature" refers to the hotness or coldness of an object or substance expressed in a desired unit of temperature measurement (engineering unit). Examples of industrial processes that rely on temperature measurement include boiler operations for commercial or residential heating and steam production for electricity generation. Common temperature sensor types include resistance temperature detectors (RTDs), thermistors and thermocouples (TCs). Common engineering units for temperature include Kelvins, degrees Fahrenheit and degrees Celsius.

Pressure

Pressure is the force that one object exerts against another. Examples of industrial processes that rely on pressure measurement include compressor operations for natural gas transmission and distillation columns for oil refining. Pressure is also applied in level sensing and various flow measurement instruments utilizing differential pressure theory. Numerous pressure measurement devices and technologies exist, including strain gauges and piezoelectric and capacitive models. Common engineering units for pressure include Pascal, pounds per square inch (psi), atmosphere, bar and displaced inches of water or mercury.

Level

"Level" refers to the relative fullness or emptiness of a reservoir, container or vessel. Examples of industrial processes that rely on level include pumped storage electricity generation and aeration pond/lagoon operations for water/wastewater treatment. Common level measurement devices include ultrasonic, guided wave radar, capacitance, level switches and displacement instruments. Common engineering units for level include feet or meters. Additional meaning is obtained when expressing level as a percentage of full.

Flow

Flow is the quantity and velocity of liquid or gas through an area, a pipe or an open channel. Examples of industrial processes that rely on liquid flow measurement include pasteurization and petroleum pipelines. An example application of gas flow measurement is burner management in combustion processes. Common flow measurement devices include vortex shedding, sonar, Coriolis, differential pressure, level through a calibrated area, Doppler and magnetic. Common engineering units for flow can be volumetric (such as cubic feet per second, cubic meters per second and gallons per minute) or mass (such as pounds per minute or tons per hour). Because liquid and gas flows can vary by specific gravity, temperature and pressure, specialized "flow computers" can be used to calculate flow and transmission values.

Calibration and Configuration

Calibration is the process of attuning a sensor/transmitter to a verified quantity/measurement within a specified error tolerance. Calibration may occur at initial deployment and periodically as required by the specific application. Calibration enables correcting or compensating for the linear or nonlinear behavior of a sensor based on its elemental design and principle of operation.

Calibration involves identifying the full range of the sensor, connecting the sensor to the test equipment (such as a documenting calibrator) and testing the desired range of the sensor (this is the "as found" test). If the output does not match the expected value, the range setting of the sensor/transmitter would be adjusted, and the test would run again until the output matched the expected value (this is the "as left" test). The process documentation, called the "calibration certificate," is stored electronically in the maintenance management system. Calibration frequency depends on the criticality of the measurement to the controlled process and guidance from the instrument vendor.

The term "configuration" refers to a variety of settings within a transmitter that match the process context. Some settings, such as selecting signal output (current versus voltage), are accomplished with a handheld configurator. Other settings, such as transmitter failure mode and transmitter security, are configured by placing physical jumper pins in the appropriate positions within the transmitter housing.

Because the integrity of a control system is in the accuracy of its sensors, their calibration and configuration must be designed, configured, verified, tested and monitored.

Scaling

Scaling is setting the sensors/transmitters (field instrument) output to correspond with a desired signal, such as a 0–5 V or 4–20 mA. Scaling is an arbitrary range that may be recommended by the process engineer and set by the instrumentation technician. For example, a process could monitor for process variable temperatures ranging from 72°F (lowest expected temperature) to 212°F (highest expected temperature). The transmitter would be scaled to send a 4 mA signal to a controller at 72°F and a 20 mA signal at 212°F. Temperatures below 72°F or above 212°F would be outside of the perceptible range to the controller. Scale is set both in the transmitter and in the controller software. Inaccurate scaling can have devastating impacts.

Transmitter Failure Mode

Some transmitters can detect failures via self-diagnostic routines. Such transmitters may be set to send a high signal (such as above 20 mA) or a low signal (such as below 4 mA). The controller software can recognize that this signal means the transmitter value cannot be trusted. An instrument technician sets the failure mode (high or low) by installing physical jumper pins when deploying the transmitter. The instrument technician should choose the failure mode (high or low) that ensures the safety of the system. Making this decision requires the technician to understand the relationship between the process variable coming from the transmitter and the control variable set by the controller.

Transmitter Security

Transmitters may offer a variety of security features. Some can be set to disallow configuration changes by installing a physical jumper in the transmitter housing. Others allow monitoring and controlling all modifications through software security features.

Gauges and Indicators

A gauge or an indicator displays the current status of a process or process variable. Gauges are frequently analog sensors (without electricity or electronics) that show a value, for example, a Bourdon tube pressure gauge with a needle pointing to a pressure value. Gauges can be placed within process equipment to enable technicians or operators to obtain accurate readings on the spot. These gauges may sometimes be called “indicators.” Importantly, because they lack electronic parts, these gauges are immune to direct cybersecurity attack.

The term “indicator” is also used to refer to a visual notice that a process is operating (or not). These indicators can be lights affixed to control panels or control enclosures. When used in this sense, indicators are controller outputs.

Finally, the term “indicator” can refer to a digital display/LCD contained within the transmitter housing. Such transmitters are called “indicating transmitters.” This display (sometimes called a “readout”) serves the same function as a gauge, but is more susceptible to cyberattack.

Meters

A meter measures a quantity delivered over a period or periods of time. In general, a meter is a human-readable display device. A meter differs from a transmitter in that its output is not used for an immediate, automated control decision. For example, an operator may observe a meter and then perform an action. A technician may use a purpose-built meter to decide when to perform maintenance or calibration. A meter designed with recording features may be used to track total usage or for billing purposes. Common examples include electricity meters and water meters. Newer meters incorporate additional functionality, such as wireless communication interfaces that enable customers and providers to read the meter easily and remote disconnect (in the case of electricity meters), which enables the electricity provider to turn off power to the customer. Smart meters can save costs by simplifying meter reading and by altering consumer behavior by making electric usage information immediately available to them.

Smart Instrumentation

In addition to transmitting sensor values to a controller, smart instruments/transmitters enable the retrieval of additional diagnostic information about the control system components they are connected to. Smart instruments may be configured for a wide range of functions and process signals, perform automatic calibration to a known set of parameters, perform automatic corrections for various sensor problems (such as noise) and be configured to perform a range of signal stabilizations, such as averaging over time. A common example would be a HART interface that enables instrument technicians to easily retrieve or change calibration and configuration.

Programming and Control Logic

The behavior of programmable controllers is typically defined by technicians or engineers who program them using specialized software on engineering workstations or technician laptops. The programming that is transferred to the controller is commonly known as “control logic” or the “application program.” The transfer process is commonly termed “download” because it is described from the PLC’s point of view. The program defines what the control system does and how individual I/O are treated. Languages and techniques related to controller programming include IEC 61131-3, Ladder Diagram, Function Block Diagram, Structured Text, Sequential Function Chart and controller code quality. Each PLC vendor processes PLC programs slightly differently, so it is important for programmers to have detailed knowledge and training on any particular vendor’s development software. When choosing a PLC programming language, the technician or engineer would do well to consider the capabilities of the personnel who will be maintaining and modifying the system in the

future. The language chosen should make it as easy as possible for them to troubleshoot and make future modifications.

IEC 61131-3

International Electrotechnical Commission (IEC) IEC 61131-3 is the leading international standard that describes “the syntax and semantics of a unified suite of programming languages” for programmable controllers. Version 3 of the standard specifies three programming languages: Ladder Diagram, Function Block Diagram and Structured Text. It also defines a Sequential Function Chart that structures programs and function blocks. It should be recognized that multiple languages can be used within a single program. IEC 61131-3 also provides common approaches for program structure, data handling, tag configurations and nomenclature that are applicable to many types of equipment.

Ladder Diagram

Ladder Diagram is the most common programming language for programmable controllers. It was developed from pre-PLC technology called “relay logic,” which was represented on an electrical schematic showing various devices such as pushbuttons, relays, indicators, contactors and motors. Ladder Diagram is primarily a visual language consisting of two vertical rails and a series of rungs that resemble a ladder. The ladder rung is read from left to right and from top to bottom. The software development environment allows a user to drag and drop elements onto each rung. On the left, “contacts” or inputs represent the conditions that result in a determined output. An example would be a push button or contactor. On the right, at the end of a rung, are the “coils” or outputs, representing relays, motor starters or other outputs.

Function Block Diagram

Function Block Diagram is a popular programming language for programmable controllers. Functions are represented as blocks within the diagram. Function blocks typically contain predefined structured programming that has been standardized and optimized for the controller by its vendor. Function blocks can be typical reusable functions in a PLC (such as a logic “AND” block or a “Timer Delay” block), or they can be custom programming that an equipment provider designs specifically for their own equipment. In the latter case, the equipment provider may lock access so the function cannot be altered. Some PLC manufacturers call function blocks “add-on instructions” (AOIs).

Each block may have one or more inputs and one or more outputs. An output from one block can be an input to another block. The diagram is read top to bottom and left to right. Function block is similar to flow-based programming techniques used in other languages such as Scratch, Node-RED and LabVIEW. DCSs commonly use function blocks.

Structured Text

Structured Text is a text-based programming language similar in format to computer programming languages such as BASIC, C or Python. Structured Text can be much more efficient than Ladder Diagram, as it requires fewer lines to accomplish an objective. Structured Text may be more challenging for engineers and technicians to troubleshoot and modify if they have been trained only in Ladder Diagram and Function Block.

Sequential Function Chart

A Sequential Function Chart graphically illustrates the ordered steps or actions a system takes. This approach allows each of the languages specified in IEC 61131-3 to be used to determine when a step is completed and when the next step begins. Sequential Function Chart is an important tool for organizing and managing system states. It is best applied for repetitive complex steps. In some PLCs, it is called “drum sequencers” as a carryover from when a mechanical rotating cylinder had pins, cams or holes in paper tape to turn on or off various outputs by triggering a connected switch or sensor.

Controller Code Quality

The controller code quality is the characteristics of user-generated controller code that make it desirable, valuable and lasting. Examples of such characteristics include maintainability, portability, reliability, reusability, testability, security and safety. Controller code quality guidance can be found in documents such as the “PLCopen Coding Guidelines” (https://www.plcopen.org/downloads/), the “Top 20 Secure PLC Coding Practices” (https://plc-security.com/) and IEC 61131-3.

Alarm Management

Alarm management is the process of identifying, defining, creating, monitoring, responding to and maintaining alarms for an industrial control system. It is critical that alarm management adhere to standards so as not to overwhelm an operator and prioritize critical alarms to ensure they are addressed in order of importance. Key topics include alarms, alarm management lifecycle, consequence severity, alarm prioritization, alarm states, alarm performance and safety alarms. The ISA18 Committee deals with alarm management. ANSI/ISA-18.2-2016 is an international standard for alarm management in process control.

Alarms

Alarms are predetermined warnings and alerts to a human process operator about a condition relevant to a controlled process or system—frequently, a safety-related condition. Alarms are predicated on the assumptions that process control equipment is not capable of detecting and controlling every possible condition affecting the process and that human attention can provide an optimized decision for some cases. Within industrial control systems, alarms are warning sounds, significant lighting and colors, and concise written messages that appear to a human via an operator

interface, especially a supervisory interface. A maliciously generated false alarm or an inappropriately suppressed alarm can have significant safety consequences.

Alarm Management Lifecycle

The alarm management lifecycle is the sequence of steps through which all alarms may pass: identification, rationalization, design, implementation, operation and maintenance. It is important to recognize that poorly designed alarms and alarm maintenance practices can detract from the alarm's intended purpose of focusing operator attention on making good decisions in a timely way. Each alarm, including its associated considerations and responses, should be fully recorded, and the documents should be made available later for analysis and improvement, and to help train operators.

Consequence Severity

"Consequence severity" refers to assigning an alarm to a severity category, such as low, medium and high. This assignment can be made by considering potential impacts to employees, the public, the environment, the plant and equipment, and production and quality loss, among others. Consequence severity is a significant input into an alarm prioritization strategy.

Alarm Prioritization

Alarm prioritization is a strategy for telling a process operator or control room operator where to focus their attention. Prioritization can be based on a combination of consequence severity and acceptable response time. Prioritization can be achieved via pop-up placement on the screen, alarm colors and types of sounds.

Alarm States

The term "alarm states" refers to the process of balancing the process state (normal or abnormal), alarm state (active or inactive) and acknowledgment state (acknowledged or unacknowledged). In addition, alarms may be permanently or temporarily removed from service (suppressed).

Alarm Performance

Alarm performance is determined by assessing the transitions between alarm states over time with the supervisory actions taken as a result of each alarm. Such analysis can enable engineers to tune alarm prioritization strategies or to improve the process and its control parameters.

Safety Alarms

For high-consequence process states, engineers may design and designate certain alarms as "safety alarms." Such alarms may be subject to specialized documentation, testing, training and suppression management.

Control System Software

Control system software is the code used to design the control system functions and operate an industrial process. This includes various software types (firmware, software and user-generated control logic) used to program controllers, configure transmitters and actuators, store historical data, provide supervisory interfaces and provide interfaces on panel-based HMIs. Because of its central role throughout the control system lifecycle, detailed knowledge of control system software is necessary to secure the control system functions from compromise. Leading vendors for such software include Siemens Automation, Rockwell Automation, Emerson Process Solutions, Honeywell Process Solutions, Mitsubishi Electric Automation, Yokogawa Industrial Automation, AVEVA, Schneider Electric, ABB and GE Intelligent Platforms.

Process Equipment

Process equipment is the physical components used to perform work within an industrial operations environment. Such a variety of equipment exists that it is difficult to identify and describe them all.

In order to design security measures to protect control system equipment functions from compromise, industrial cybersecurity professionals should have a sound understanding of how relevant equipment operates, the effects of its manipulation and its failure modes. For example, such understanding may draw on concepts of physics, chemistry, metallurgy and thermodynamics. Some equipment is specific to certain industry sectors, and other equipment is deployed across many sectors.

Common equipment includes actuators, electric motors, pumps, compressors, valves, piping, conveyors, tanks and vessels, electric power equipment, process heating and cooling equipment, process chemistry equipment, turbines, robotics, motion control equipment, vision systems, air handling equipment, filters and scrubbers, engines, ingress and egress equipment, safety equipment, medical machines, skid-mounted systems and smart devices/equipment.

Some process equipment incorporates other process equipment. For example, because pumps frequently have integrated motors, the subtopics listed under “Electric Motors” and “Motor Controllers“ also generally apply.

Actuators

Actuators provide action or movement within an industrial process. Within a control loop, actuation is often the process output determined by the controllers. Most actuators rely on mechanical, electrical/motor-controlled, hydraulic or pneumatic energy to operate; sometimes, these energy sources work in tandem to complete the desired movement. Depending on the actuator application, untimely actuation can have devastating effects.

Mechanical Actuators

Mechanical actuators achieve movement by converting one kind of motion to another. Spring-operated valves and centrifugal switches are examples of mechanical actuators.

Motor-Controlled Actuators

Motor-controlled actuators rely on electricity to create rotational force. Motor-operated valves, pumps and driveshafts are common examples.

Hydraulic Actuators

Hydraulic actuators rely on the properties of enclosed liquids to achieve motion. Relatively small movements pressing on hydraulic oil can exert large forces. Hydraulic systems include a reservoir to hold hydraulic oil for potential use, a pump to force fluid into the system, a valve that holds the liquid in place, an actuator (cylinder) that moves the load when the pump introduces the fluid and a pressure regulator that limits pressure by allowing fluid to escape to the reservoir. Examples of hydraulic systems include backhoes and airplane landing gear.

Pneumatic Actuators

A pneumatic actuator relies on compressed air to achieve motion. Pneumatic actuation has the advantage of requiring limited maintenance. While pressurized air can allow small movements to exert large forces, the inefficiency of maintaining air compression limits the usefulness of pneumatics for moving massive objects. In industrial automation, pneumatic actuators are frequently used to control and position valves via a piston or diaphragm.

Electric Motors

Electric motors are used to convert electrical energy to mechanical energy (motion) for process equipment across virtually all industry sectors. They are plugged into an electric power system and provide motion for work. Examples include running a conveyor belt, positioning a valve and turning a pump. Types of electric motors include AC induction motors, DC motors, stepper motors, piezoelectric motors and electrostatic motors. The type of motor chosen should match the application requirements, including current, voltage, torque (rotational force) and velocity.

Motors typically include a housing or frame, which encloses and protects the internal components; iron cores and copper windings, which create a magnetic field when power is applied; a stator, which remains stationary; a rotor, which rotates when voltage is applied; a shaft, which spins with the rotor, connecting the motor to its task; and bearings, which facilitate rotating the shaft and rotor within the housing. Motors can be small enough to fit inside a cell phone and large enough to have their own room inside a large industrial facility. Motors are frequently engaged and controlled by specialized motor controllers.

Pumps

A pump is a device (frequently an electromechanical device connected to a motor) that moves liquids from one location to another, typically through a tube or pipe. Pumps are used in any industry or application that requires moving liquid: water and wastewater, and oil and natural gas are prime examples. Pumps should be chosen based on process requirements such as fluid type, required flow rate, required pressure, viscosity, specific gravity and temperature. A pump's performance can be evaluated by examining the pump performance curve, which illustrates pump efficiency given the application details.

Pumps can be classified into two main categories: positive displacement and dynamic. A positive displacement pump takes in and discharges a specific amount of fluid for each rotation/stroke. A dynamic pump relies on rotating impeller blades to both take in and discharge the fluid. Pumps designed to be placed within or under the liquid are known as submersible pumps or "sumps."

Operating or not operating a pump at the wrong time or operating it at the wrong speed can cause significant damage to the pump and other process equipment (such as a water hammer), harm to people and environmental damage.

Compressors

A compressor is a device (frequently an electromechanical device connected to a motor) that moves gases from one location to another through a tube or pipe. Compressors are used in any industry that requires moving gases: oil, natural gas and petrochemicals are prime examples. Compressors should be chosen based on process requirements, such as compression ratio, power requirements, speed and efficiency. A compressor's performance can be evaluated by analyzing the compressor performance curve, which illustrates pump efficiency based on application details.

It is important to recognize that compressors may be used to provide an air supply for pneumatic process control, such as to operate pneumatic valve positioners. In such cases, loss of compressed air would shut down any process relying on pneumatically actuated valves.

Compressors can be classified into two main categories: positive displacement and dynamic. A positive displacement compressor takes in, traps and discharges a specific amount of gas for each rotation/stroke. A dynamic compressor relies on rotating impeller blades to take in and to discharge the gas.

Operating or not operating a compressor at the wrong time or operating it at the wrong speed can cause significant damage to the compressor and other process equipment, harm to people and environmental damage.

Valves

Valves allow or disallow the flow of material (liquids, gases and solid particles) through a tube or chute, providing a critical process control function in nearly every industry sector. Common types of valves include rotary, linear, ball, butterfly, plug, globe, gate, needle, solenoid, coaxial and angle seat. Valve type is specified by the desired size, precision, pressure limits, temperature limits, frequency of actuation, type of actuation and type of valve function (cut off, throttle, check, relief). Valves are also specified as normally open, normally closed, fail-open and fail-closed, depending on the details of the process being controlled.

Valves are typically composed of a body, the solid frame to which the other parts are connected; a bonnet, which rises above the opening in the body; and the valve trim. "Valve trim" generally refers to the parts that directly facilitate opening and closing the valve without leakage. Trim can include the glands, spacers, packing, guides, bushings, gaskets and springs, along with the stem, plug and seats. The stem moves up and down, the plug blocks flow and the seat is the point of contact between the plug and the body. Valves are subject to wear against process forces, including pressure, cavitation and erosion, which can cause the valve to leak or malfunction. Depending on the application, valve failures (including failure to operate, unnecessary operation or physical failure) can have catastrophic consequences for process operation and human safety.

Piping

Piping consists of interconnected tubes that transport fluids, gases and other materials in oil and natural gas, petrochemical, water and wastewater, building and other industries. Piping can be made of various types of metal and plastic to withstand internal and external pressures and temperatures as the process may require. Couplings, such as elbows, tees, valves and flanges, join pipes together. Elbows change the direction of pipelines and their contents, normally at 90-degree angles. Tees create branches. Valves control the flow rate, direction or pressure of pipeline contents. Flanges, or protruded rims, provide strong connections between pipes or other process equipment.

Conveyors

Conveyors continually move materials from one location to another. The two most common conveyors are belt conveyors and roller conveyors. Belt conveyors are constructed with belts and pulleys; the belts are wide strips of material wrapped from a motor on one end to one or more pulleys and back again, providing a flat moving surface. In comparison, roller conveyors consist of a series of rotating cylinders ("rollers") mounted within a frame that guide materials to a destination. Rollers may spin freely, "coasting" on gravity and inertia; or they may rely on a motor, which allows for increased energy efficiency and finer-tuned movement. Conveyor applications include moving materials within a production line, sorting materials to different locations, and raising and lowering

materials within transit. Because many facilities rely on a single line of conveyors to move products, conveyor failure or stoppage can halt operations.

Tanks and Vessels

Tanks and vessels are physical containers or enclosures used in industrial processes to store, transport or process various solid, liquid and gaseous substances. Tanks and vessels are designed and constructed using specific materials and certain shapes to meet the needs of the process and contents. Tanks and vessels are crucial in industries such as oil and natural gas, petrochemical, pharmaceuticals and more.

Tank Shape

The shape of a tank or vessel is based on several factors, such as the type of material being stored, the desired capacity, space limitations and operational considerations, such as the desired flow. Some common shapes of tanks and vessels are rectangular, cylindrical, spherical and conical.

Tank Materials

Materials are the substances or compounds used in constructing tanks and vessels. These materials are chosen based on their interaction with tank contents and environmental conditions, such as resistance to pressure, temperature and corrosion. Common materials for tanks and vessels include steel, carbon steel, stainless steel, aluminum and other alloys.

Electric Power System Equipment

Electric power system equipment consists of a range of electromechanical or electrochemical systems that provide electromotive force (electric power) for a variety of applications across every industry sector. This category includes generators, conductors, insulators, bushings and arrestors, transformers, switchgear, batteries and capacitors. These devices are commonly classified by high, medium and low voltages.

Generators

Generators are the heart of electric power systems, providing energy for residential, commercial and industrial users. Generators induce an electric current that can be harnessed to supply power to electronic devices. These can be classified into three types: electromagnetic, which rely on a rotating magnetic field to induce current in wires; photovoltaic, which convert light energy to electric energy; and electrochemical, which convert chemical energy to electric energy with the help of fuel (such as hydrogen). Electromagnetic generators, which provide most of the power for the world's electric grids today, are further classified by the force that rotates the magnetic field. This force is known as the primary mover: water, wind, steam, hot gas or direct combustion. Steam may be created by combustion or nuclear fission that boils water, and heated gas is produced by combustion.

Components of electromagnetic generators include rotors, stators, windings or magnets and armatures. Generator design determines whether an electric power system uses DC or AC. Generators may also incorporate electronic components to help regulate output characteristics such as voltage and waveform according to specific requirements or preferences. It should be noted that large electromagnetic generators often require an independent power source to provide excitation that produces the magnetic field.

Generator failure can have enormous downstream consequences due to heavy reliance on electric energy. Electric power grids are frequently designed to continue operation in case a power source (generator) fails.

Conductors

Conductors carry electricity from one location to another. Within electric power systems, conductors are commonly seen as large aluminum or copper cables mounted on pylons or power poles, though they may also be buried. Within substations, solid aluminum, copper or brass busbars perform this function. Conductors are specified to meet anticipated voltages. Overloaded conductors can cause physical damage. For example, overloaded electric power lines may sag until they contact vegetation or the ground, producing a fault and igniting fires.

Insulators, Bushings and Arresters

Insulators, bushings and arresters stop the flow of electricity from one location to another (via a direct path or arcing). Insulators are commonly applied to keep power lines at appropriate distances from one another and from their supporting structures. Bushings keep electric energy within a conductor for short distances from half a meter to 10 meters) where potential for leakage is high, such as entry points to transformers. Arresters provide a safe path for high voltage electricity (such as that caused by a lightning strike) to dissipate before it can damage electrical power system equipment. Insulators, bushings and arresters are commonly made of porcelain and filled with insulation. Their failure can destroy electrical equipment, interrupt the electricity supply and harm individuals present when the failure occurs.

Transformers

Within the electric power system, AC transformers receive electricity at one voltage and provide an output at another voltage. A transformer consists of two sets of copper windings: one around the input side of the ferromagnetic core, and one around the output side of the same core. If the input side has fewer windings, it is a step-up transformer, as the voltage entering the transformer is lower than the voltage exiting it. Step-up transformers are commonly used for electricity transmission and can be found where generated electricity enters the transmission grid. If the input side (primary winding) has a greater number of windings than the output side (secondary winding), it is a step-down transformer; the voltage entering the transformer is higher than the voltage exiting it. Step-down

transformers are commonly used to change electricity from transmission voltages to distribution voltages and from distribution voltages to industrial, commercial or residential uses. Step-down transformers are commonly located on cement pads or on pole tops on or near customer premises. The windings and core are inside a shell that is insulated by gas, paper or mineral oil. Transformers may be instrumented to disconnect from the power system in the presence of high-temperature, high-pressure or dissolved gases. Transformers that experience voltages that exceed their rating can fail and even explode.

Switchgear

"Switchgear" refers to electric power systems equipment that makes and breaks connections between electrical circuits, which helps to regulate, protect and isolate electric systems. Examples of switchgear include switches, circuit breakers, protective relays and fuses. Switches may open and close to connect different conductor pathways; isolation switches disconnect electrical equipment within a substation for maintenance; circuit breakers use stored energy (such as a loaded spring) to interrupt an electrical circuit; and fuses burn out to interrupt the circuit.

Circuit Breakers

A circuit breaker is an electromechanical device that breaks (or opens) an electrical circuit to interrupt the flow of power. One of the primary purposes of circuit breakers is to interrupt a power system before conditions cause physical damage. Breakers include an automatic actuating mechanism, such as a magnet, spring, motor or a hydraulic or pneumatic device, as well as a manual operating principle, such as a crank or lever. A signal to open the breaker results in breaker actuation (forcing the contacts to separate). As this may result in arcing electricity between the separated contacts, the breaker quenches the arc by air separation, air blast, SF6 gas or a vacuum interrupter. After a breaker activates, the operating mechanism is restored/recharged for subsequent operations. Circuit breakers can fail due to exposure to currents or voltage beyond their ratings, control system failures and physical damage. These failures can result in explosions that damage equipment and cause power outages.

Batteries

A battery is an energy storage device. The term is often used to denote electrochemical devices that operate on the principle of reduction and oxidation, whereby electrons are stored during charging and made available for use during discharge. Batteries are specified by amp-hour and output voltage. In industrial facilities of all types, battery banks provide backup power for short-term use (before local backup generators engage) in case of power system failure. Technological advancements in energy storage technology (such as Lithium-ion batteries) are altering the energy landscape by increasing the demand for power generation, enhancing the usefulness of renewable energy and creating a more flexible grid. Batteries are often managed by their own control systems. Disrupting these systems

could prevent a facility or process from functioning as intended—especially in the case of off-site power failure.

Capacitors

Capacitors accumulate electric charges that will be released as needed. They consist of two conductors (often metallic plates), separated by either air or a dielectric material, that hold opposite charges. Due to the attraction between opposite charges, a significant charge imbalance can be established and maintained on each plate. Capacitor banks are commonly used with electrical systems to provide temporary energy storage and power conditioning. Capacitors can fail (even explode) due to exposure to currents or voltages beyond their ratings.

Turbines

The curved blades of a turbine harness the energy of moving water, steam, gas and wind, and convert it into rotational force. When attached to a generator, a turbine can create electrical energy (electricity) in addition to mechanical energy. Water and wind turbines are popular generators of renewable energy. Steam turbines rely on a boiler to convert water to steam, which can then turn the blades. Steam turbines are deployed in coal-fired and nuclear power plants. Gas turbines draw air in, compress and heat it, ignite it and exhaust it over the turbine blades. Gas turbines are commonly found in airplane jet engines and natural gas power plants. The malfunction of a turbine or its components can have a devastating impact on the controlled process.

Process Heating and Cooling

Process heating and cooling systems provide heat to or remove it from an industrial process. Process heating and cooling systems are common in nearly all industry sectors. Their equipment includes boilers, heaters, heat exchangers, furnaces, distillation columns, refrigerators and freezers, industrial chillers and cooling towers.

Boilers

Boilers create hot liquid or steam from a feed supply of liquid. They generally consist of thick steel walls and tubes. Because boilers are sealed and pressurized, they can maintain water and steam at lower temperatures than in nonpressurized environments. If the tubes contain fire, it is a fire-tube boiler; if the tubes contain liquid, it is a liquid-tube boiler. Boilers are built to run on specific fuels, frequently natural gas. Two primary uses of boilers are to create heat for facilities and to create power for performing work. When used for facility heating, the hot water or steam is sent through pipes and radiators to provide warmth. When used for power, steam is discharged onto a turbine that drives mechanical work or generates electricity. A breach of the sealed boiler or a low water level within the boiler can cause catastrophic steam explosions.

Heaters

Heaters are used to warm air or other materials within a given environment. Electric heaters typically rely on electrical resistance to produce heat. The heat produced may be moved with a fan (forced air) or without a fan (radiant).

Heat Exchangers

A heat exchanger is a mechanical device used to transfer heat from one substance to another. This is often accomplished by passing two liquids of different temperatures close to one another but separated by thin plates or a series of metal tubes. Heat exchangers are used in a wide variety of industry sectors. In the food sector, heat exchangers are used to preheat milk on its way from the refrigerator to the pasteurizer (which heats milk to kill bacteria) and to precool pasteurized milk heading in the opposite direction. Failure of a pump moving liquid through a heat exchanger can have significant consequences for the product, process or environment.

Furnaces

A furnace is a structure in which heat is produced. Common industrial furnace types include oil combustion, natural gas combustion and electric arc. Furnace temperatures can reach thousands of degrees Fahrenheit. Combustion furnaces include burners that constantly emit fuel, igniters that light the emitted fuel, flame detection sensors that prevent the buildup of fuel, blowers that move or remove the heated air or other particles (such as soot) and valves that control the supply of fuel. Arc furnaces rely on electrodes through which electric current is applied, turning surrounding gas to plasma as electricity flows between the electrodes. Additional fuel and oxygen injectors help produce optimum heat, facilitating the melting or burning of contents, such as metals, within the arc furnace. Furnaces are used in a variety of industry sectors, including mining and metals, petrochemical and manufacturing. For example, in metal production, a blast furnace dumps ore in the top and blasts hot air from beneath, melting the ore so it can be removed from the bottom. Buildup of unignited fuel and oxygen within furnaces can have explosive consequences.

Distillation Columns

A distillation column separates liquids into various components by changing the liquid to steam (boiling). The steam is then condensed back to a liquid form. In a distillation column, the liquids with the highest boiling points are removed from the bottom of the column, closest to the heat source/furnace, and the liquids with the lowest boiling points are removed from the top of the column, further from the heat source. Components typically include a vertical shell that can be a hundred feet high or more, trays and plates that aid in separation and take-off, a reboiler that heats or reheats the feedstock, a condenser to return the fractioned products to a liquid state and a reflux drum that captures some liquid to feed back into the column. Distillation columns are used notably in the food and pharmaceutical and the petrochemical industry sectors. For example, water distillation

purifies the water by leaving behind contaminants that have different boiling points. Within a petrochemical facility, distillation is an initial step, as it breaks crude oil into naphtha, light oils and heavy oils, each with its own boiling point.

Refrigerators and Freezers

Refrigerators and freezers remove heat from materials and processes through a continuous cycle of changing a refrigerant from a high-pressure and high-temperature gas into a cool liquid and back again. This cycle is motivated by an electric-powered compressor. When within the refrigerator or freezer enclosure, the refrigerant is a cold liquid that absorbs heat from the contents (such as food). When outside the refrigerator or freezer enclosure, the refrigerant radiates heat to the environment. Refrigerators and freezers are commonly used in the food and pharmaceutical and the transportation industries to keep consumables from spoiling. Malfunctions of refrigerators and freezers can damage products and affect human health.

Industrial Chillers

An industrial chiller is used to remove heat from buildings, machines, processes and products that require intensive cooling. Examples include metal finishing, injection molding and printing. Chillers work on the same basic principle as refrigerators, but they are designed for industrial applications because they cool a separate stream of heat transfer fluid rather than only the air within a refrigerator unit. Types of industrial chillers include water-cooled, air-cooled, vapor compressor, vapor absorption and centrifugal. Failure of a chiller (including its components) may damage the process or product.

Cooling Towers

A cooling tower is a vertical structure used to cool water that is heated as part of an industrial process. Cooling towers generally spray the hot water from near the top of the tower downward onto a suspended fill medium over which the water flows. Ambient air is blown or allowed to blow from beneath the suspended fill, towards the top of the tower, cooling the water as the air passes upwards. The cooled water drips into a reservoir beneath the tower, from which it may be recirculated into the process. Cooling towers are icons of nuclear power plants, though they are also common in the petrochemical sector. Failure to sufficiently cool water may lead to process shutdown or significant damage to the product, process equipment, people and the environment.

Process Chemistry

The term “process chemistry” refers to the chemical reactions and processes that form an integral part of industrial operations across industry sectors, including petrochemical, water and wastewater, pharmaceutical and manufacturing. Process chemistry equipment commonly includes crackers and reactors. The volatile nature of many chemical reactions presents special safety hazards.

Crackers

Crackers perform controlled fragmentation or decomposition of complex molecular structures into simpler and more valuable compounds by using chemical reactions involving temperature, pressure and catalysts. For example, in the petrochemical industry, crackers convert distilled products such as heavy oils into lighter and more useful products, which eventually become gasoline, diesel, jet fuel and chemical feedstocks that are essential for a wide range of industries.

Reactors

A reactor is a specialized vessel/tank designed to facilitate chemical reactions with precision and control. Reactors play a fundamental role in the synthesis, transformation or conversion of chemicals at an industrial scale. Reactor forms and designs are tailored to the specific requirements of the chemical process at hand. Typical reactor types include batch reactors for noncontinuous applications and continuous stirred tank reactors where mixing occurs at a constant rate.

Robotics

"Robotics" refers to automated, nonliving, mobile or semi-mobile machines that autonomously interact with the physical world. Robot components are essentially similar to industrial control systems, including sensors, actuators, microprocessors and a variety of task/process equipment. Robots may be preferable to human workers because they perform tasks with exactness and consistency, and can diminish risks to human health by performing dangerous tasks or tasks in hazardous environments.

Robotics are used in a variety of industrial settings. For example, automotive manufacturing uses robotic arms to place and secure multiple parts in each car. Warehouse robots transport parts or products from one location to another. Some robots work in isolation from humans—separated by cages—to prevent harm. Other robots—called cobots—can work closely with humans without harming them. Robot malfunctions and programming mistakes within robots can damage products and harm people. Robots can be built and programmed for destructive purposes as well. As robot capabilities advance, ethical and policy questions will continue to arise.

Motion Control

Motion control is the process of manipulating the location and position of a machine to conduct work or make a product, involving special motors known as servos, steppers and encoders. A servo (short for servomotor) relies on electronics to create a closed-loop feedback mechanism to recognize its position and speed accurately. A stepper motor uses teeth and shifting magnetic fields to gain precise control over the rotational position of the motor, without a feedback mechanism. An encoder is an electromechanical device mounted on a motor that tracks the position and velocity of the shaft, providing closed-loop feedback. Motion control is common in various types of factories. Important

concepts for motor control include axis, motion type and acceleration and deceleration. Abuse of motor control can have devastating and dangerous physical consequences.

Axis

"Axis" refers to the direction in which the motion is being controlled. Axes are also known as "degrees of freedom," of which there are six: up-down, back-forward, left-right, pitch, yaw and roll. A motor operating a conveyor has one axis: forward and backward. A milling machine, which forms shapes by cutting away material, may have all six axes.

Motion Types

Motors and a variety of gears can be used to create several types of motion, such as linear (straight line), rotational (rotating), oscillation (wavelike) and reciprocating (back and forth).

Acceleration and Deceleration

The terms "acceleration" and "deceleration" refer, respectively, to increasing and decreasing the speed of a motor. Accelerating and decelerating a motor causes stress that could damage or destroy the motor and related components.

Vision Systems

Vision systems rely on visible light to inform process control decisions. An imager consists of a lens and a photoelectric sensor, which converts light (photons) to electrical signals and passes them to software to process the image. Vision system outputs can include inspection results, alarm signals, control signals and reports. For example, in a potato processing facility, a vision system may identify potato chips with undesirable color as they move down a conveyor belt and trigger their removal from the stream. Vision systems are commonly found in manufacturing and vary in complexity depending on the task/process requirements.

Air Handling Equipment

Air handling equipment aids in cooling, heating, circulating and humidifying air in buildings and industrial processes. This equipment includes fans that diffuse air through an open area by means of rotating motorized blades; blowers that concentrate and force airflow in a specific direction (including as dryers) using motorized impeller blades; humidifiers that increase water content (humidity) in the air by a wetted element, evaporative pan, water spray or steam release; mixers that combine airflow from different sources; ductwork that encloses and directs airflow; and dampers that open and close to regulate airflow to certain locations. Air handling equipment is commonly used in HVAC systems for human comfort in residential, commercial and industrial buildings. Air handling equipment also plays an important role in process-specific applications such as wine cellars, paper production and printing,

and computer facilities. Air handling equipment failure can disrupt sensitive processes and damage products.

Filters and Scrubbers

Filters and scrubbers separate unwanted materials and particles (commonly known as contaminants) from a stream of gas or liquid. Contaminants may include dust, volatile organic compounds, mold, bacteria and viruses. The "filter medium" refers to the substance that performs the separation. Filters are specified based on particle size, effectiveness and flow rate. Air filters can work on the principles of diffusion, interception, inertial impact and electrostatic attraction. Common filter media for gases include paper, polyester, fiberglass, nylon mesh, activated carbon and ultraviolet light. Filters for liquids can work by forcing liquid through a bag, membrane, media (such as sand or activated carbon) or ultraviolet irradiation. While commonly used across many industries, the water and buildings sectors easily come to mind for their use of filters to clean water and air.

Scrubbers remove or nullify dangerous and unwanted particles from gases by forcing the gases through scrubber solutions (which may be gas or liquid). The solutions function by adsorbing (in some cases reacting with) the contaminants. The scrubber solutions used depend on the contaminant being scrubbed. Scrubbers are often oriented vertically so that the rising contaminated gas passes upwards through porous fill material and scrubber solution, which is sprayed from the top. After passing by/through one another, the cleaner gas exits the top of the scrubber, and the now-contaminated scrubber solution is collected at the base. Scrubbers are found in a variety of industrial processes. They commonly remove pollutants from exhaust gases (at the top of smokestacks). Submarines use scrubbers to remove carbon dioxide from the air to keep the air safe to breathe.

Filters and scrubbers can fail when their components (such as fans, sprayers and pumps) stop working. The impacts of malfunctions vary by the process, depending on what happens next to the stream of liquid or gas. Environmental damage is a clear impact of many failures. Regulated industries may also face fines.

Engines

Engines are mechanical devices that convert various forms of energy into mechanical work. Engines provide power for a wide variety of industries. Common engine types include internal combustion engines, electric motors, steam engines and gas turbines. In common usage, the term "engine" refers to internal combustion engines (such as those used in gasoline- or diesel-powered automobiles) that burn fuel to turn a drive shaft. In contrast, electric motors use magnetic fields to convert electrical energy into mechanical energy. Steam engines burn fuel to boil water, then trap the steam to harness its force. Turbines rely on the pressures of moving or expanding gas against curved blades to produce work. Engine performance is measured by factors including power output, efficiency, torque and emissions. Power output, measured in watts, indicates the amount of work an engine can produce

within a given timeframe. Efficiency is how effectively an engine converts energy (such as fuel or electricity) into mechanical work. Torque is the rotational force an engine can produce. Emissions are the pollutants, like carbon dioxide (CO_2) or nitrogen oxides (NOx), produced by a combustion engine.

Ingress/Egress Equipment

Ingress and egress equipment are devices and systems that allow or deny physical entry (ingress) and exit (egress) to individuals or materials to a facility or location. The physical space leading to an entry/exit point is known as a pathway. A gate, or a series of gates, is a door that opens or closes when certain conditions are met. A lock may be applied to or within a gate to prevent it from opening. Ingress/egress equipment is generally considered to be part of the facility and may be managed by building automation and building security systems. Airports and government facilities make heavy use of ingress/egress equipment. Halting ingress or egress can result in long lines and frustration, and eventually delay the operations that occur within a facility.

Safety Equipment

Safety equipment consists of the specialized devices and systems designed to ensure the safety of personnel, protect equipment and prevent accidents or hazardous situations in industrial operations environments. Safety equipment includes a variety of devices such as safety valves, safety switches and limit switches. In cases where these devices are programmable (such as being connected to a controller), an adversary may be able to bypass their intended safety function.

Safety Valves

Safety valves are mechanical devices designed to prevent equipment failure or explosions due to excessive pressure. These devices typically allow the valve to release fluid or gas when the internal pressure exceeds the resistance of a spring.

Safety Switches

Safety switches are electromechanical devices designed to interrupt the power supply or control circuit in the presence of unsafe conditions. Safety switches may activate on the detection of excessive temperature or pressure, the presence of hazardous liquids or gases, or the activation of an emergency stop button. Safety switches are commonly used in machinery, conveyor systems, robotics and other applications.

Limit Switches

Limit switches are electromechanical devices that detect the presence or position of an object within a specified range of motion. The switches are actuated by either physical contact with an object or the absence of an object in a designated area. Actuating a safety limit switch can trigger a remedial control action, such as a process shutdown.

Medical Machines

Medical machines provide medical services and support to patients and health care professionals. They may be implanted within a patient or placed on or next to a patient's body for diagnostic, treatment, life-support and research purposes. Because failure and/or abuse of this equipment within a demanding medical environment could endanger the lives and health of patients and health care professionals, the equipment must often meet a higher standard of manufacture than consumer-grade devices. Examples of medical machines include heart monitors, blood sugar monitors and blood oxygen level monitors for diagnosis; CPAP (continuous positive airway pressure) machines and surgical robots for treatment; heart-lung machines for life-support; and hematology analyzers and clinical centrifuges for research purposes. Each type of medical machine has its own principles of operation, often incorporating sensors, transmitters and actuators. These devices often incorporate network connectivity to facilitate configuration, control and communication.

Skid-Mounted Systems

A skid-mounted system is an industrial process system packaged on a single frame, or "skid." Skids are convenient because they are modular, portable and can be purchased from a single supplier (who has already integrated the process equipment and process control equipment). A common skid-mounted system is a palletizer that stacks goods and wraps pallets of products for shipment. While reliance on a skid may be convenient, skid owners must be diligent about ensuring its safety and security, especially if it plays an integral role in industrial operations. Skids paved the way for innovative models such as Machine-as-a-Service.

Machine-as-a-Service

Machine-as-a-Service (MAAS) is the business model where a company or organization pays an ongoing fee for using a skid, rather than owning it. This enables both the skid user and the skid owner to predict costs/revenues. While contract details may vary, the skid owner, the expert on the skid, is likely to provide maintenance services for the skid (by sending their own technician). While reliance on MAAS may be convenient, process owners must be diligent about ensuring the safety and security of the entire process, including the MAAS. If an adversary were to access the MAAS servers, they may be able to attack many MAAS customers simultaneously.

Smart Devices/Equipment

Smart devices incorporate industrial control system elements within a piece of process equipment. For example, a smart engine may record how many times it was started, and a smart pump might record its use by time of day. The miniaturization and inexpensive availability of reliable sensors and network equipment drive the deployment of increasingly smarter equipment.

Industrial Networking and Communications

The term “industrial networking and communications” refers to transmitting data between devices used within an industrial environment and between the process control network and the corporate network. Key topics include network architecture and integration, data management, network equipment, signals and protocols, and wireless communications.

Network Architecture and Integration

Network architecture is the physical design and layout of a network, including the placement of various nodes and network equipment. Network integration is the process of incorporating nodes and functionalities into the network. Key topics for network architecture and integration include reference architectures, enterprise systems, remote access, third-party systems, cloud services, edge computing, machine-to-machine and Bring-Your-Own-Network.

Reference Architectures

Reference architectures provide a common model and language for describing the components of a process control network within the context of an entire enterprise. Common terms related to reference architectures include Purdue Enterprise Reference Architecture, converged plantwide Ethernet, levels, zones, cells and conduits.

Purdue Enterprise Reference Architecture (PERA)

The PERA, first published in 1992, defined a hierarchical model for describing the relationship between manufacturing operations and business functions supported by computers and networking technologies. The model relies on the concept of four levels. The concept of levels was later incorporated into and adapted by the International Society of Automation ISA95 Enterprise-Control System Integration Committee and the Rockwell Automation converged plantwide Ethernet publications. Though not originally intended as a security architecture, the ISA99 Industrial Automation and Control Systems Security Committee adopted a similar “levels” approach. The growth of vendor-provided cloud services and Bring-Your-Own-Network (BYON) solutions challenges the usefulness of the PERA model.

Converged Plantwide Ethernet

Converged Plantwide Ethernet (CPwE) is the Cisco-Rockwell Automation guidance for creating a robust communication network linking industrial operations to the enterprise network. The documents include design and implementation guides that cover topics such as Common Industrial Protocol (CIP) security, cell/zone security, time distribution, redundancy, process control network firewalls and others.

Levels

Levels are a core concept of the Purdue Enterprise Reference Architecture and other architecture models. While the concept can vary somewhat among organizations presenting the concept, in general, Level 0 includes physical devices such as sensors and actuators; Level 1 includes local programmable controllers; Level 2 contains panel-based operator interfaces; Level 3 includes supervisory interfaces, application servers and engineering workstations; Level 3.5 is a demilitarized zone (DMZ) separating the process control network from the corporate network; and Level 4 is the corporate network, including ERP systems.

Process Control Network

A "process control network" (PCN), also called the "industrial network," "industrial control network" or "industrial control systems network," is the network of control system components used to directly support controlling the industrial process. Assets within the process control network are often managed by operations personnel. The term is commonly used to contrast with the term "corporate network."

Corporate Network

The term "corporate network" describes the network of computers used to support business operations directly. These are the servers, workstations, laptops, phones, printers, and other devices that one normally associates with a corporate/office environment. Assets within the corporate network are managed by the information technology (IT) department. The term "corporate network" is often used to contrast with the term "process control network."

Zones

From the perspective of a reference network architecture for process control networks, a zone is a specific area within an industrial facility that is normally dedicated to a particular process or part of a process. For example, there may be one zone for refining operations and another zone for tank farm management. The concept of a zone helps identify which network-connected resources need to communicate with one another on a regular basis. Dividing a network into zones aids in designing, implementing and maintaining a secure and robust process control network.

Cells

From the perspective of a reference network architecture for process control networks, a cell is a specific area within a zone. For example, a catalytic cracker may form a cell within the refinery operations zone, or a single chemical tank may form a cell within a tank farm operations zone. Dividing a zone into cells aids in designing, implementing and maintaining a secure and robust process control network.

Conduits

From the perspective of a reference network architecture for process control networks, a conduit provides connectivity between cells within a zone and between zones within a network. The concept of conduits helps networking professionals to define expected network traffic, which, in turn, aids in designing, implementing and maintaining a secure and robust process control network.

Enterprise Systems

The term "enterprise systems" can be used to refer to 1) systems or assets related to the entire organization and its mission, including both traditional corporate network assets and process control network assets or 2) systems or assets that do not include industrial control systems. Its meaning can normally be deduced by examining the context of its use. Enterprise systems that commonly span both traditional corporate networks and process control networks include enterprise resource planning and manufacturing execution systems.

Remote Access

Employees and support personnel frequently require access to industrial control system networks from distant locations, over networks not controlled by the asset owner organization. Poorly controlled network access can be a significant vulnerability. Strategies for secure remote access can help address this weakness.

Third-Party Systems

Third-party systems are the software and hardware solutions within a network that were produced by an organization other than the seller and purchaser. These normally become part of an operational industrial control system through a vendor's supply chain. They could also be introduced by a control system integrator. Unrecognized third-party relationships are common weaknesses in industrial control systems.

Cloud Services

Cloud services are computing hardware and software that reside in an off-site data center. Cloud services may be hosted internally (by the organization) or by an external vendor. Examples of cloud services relevant to production operations include converged data management, manufacturing execution systems, analytics and predictive maintenance. Cloud services are commonly believed to reduce computer/server maintenance costs, provide access to a greater breadth of data and open new information-based services/product offerings.

Edge Computing

"Edge computing" refers to relying on processing and storage closer to network nodes rather than data centers. Edge computing is particularly useful when latency and bandwidth costs are key

concerns. For example, sensors used for predictive maintenance may connect to a server within the plant rather than to a cloud-based server. The locus of decision-making (edge or cloud) is an important factor in ascertaining weaknesses and potential consequences of cybersecurity events.

Machine-to-Machine (M2M)

"Machine-to-machine" refers to communications that coordinate directly between computers (in some cases, cyber-physical machines) rather than in a centralized client-server architecture. Examples include communications between programmable controllers, communications between automobiles and communications between electric meters and in-home energy-consuming devices.

Bring-Your-Own-Network (BYON)

BYON refers to resources, assets and machines that come with their own network connectivity. A memorable example is the cloud connectivity of a modern automobile, such as via satellite or cellular networks. The owner does not need to configure the network; it is simply part of the integrated package. Machine-as-a-Service models, such as a palletizing skid, may rely on BYON to communicate diagnostic information to the skid vendor.

Data Management

Data management encompasses the creation, processing, storage and use of data, primarily relative to an industrial process. Topics include data, data source, data path, data storage and data use.

Data

Data are the logical representation (in bits and bytes) that, within a proper context, allow timely decisions to be made. Within an environment, data include the representation of set points, process variables, control variables and other process-oriented quantities and concepts.

Data Source

The data source refers to the place data are created or the place from which it is sent. Process data often originates at the sensor/transmitter. Set point changes or forced control variables typically have their origin in an operator interface, engineering workstation or technician laptop. Control systems often generate metadata to describe when and where process data was created. They often generate new data based on the analysis of process data.

Data Path

The data path is the course that data follows, from its place of creation through network equipment to the multiple places where it is used. In an industrial control system, data may be created at the transmitter and sent to the controller, to the local HMI, to the supervisory control application, to an

engineering workstation and to the historian. The data path is a factor in determining the impact of a cybersecurity event.

Data Storage (Process Data Historians)

Data storage is the physical location where data are kept and the software (database) that organizes and controls access to the data. Such software systems are commonly called "process data historians" because they house a history of process variables, set points and control variables together with other data relative to production and maintenance.

Data Use

The term "data use" describes the decisions the data informs or the actions it determines. Within an industrial control system, data use includes process control, supervisory control, process analytics, manufacturing execution systems and predictive maintenance systems. The way data are used places requirements on its timeliness. Data use is also a factor in determining the impact of a cybersecurity event.

Process Control

"Process control" refers to executing decisions that keep an industrial process performing its intended function. In general, routine control decisions are made, and an automated controller, such as a PLC, takes action.

Supervisory Control

Situations may arise in which an automated controller is not capable of perceiving enough context to make an accurate control decision. In such cases, a supervisory control system gathers and presents data to a human, such as a control room operator, and facilitates executing temporary (potentially one-time) control decisions. In some industries, such as electric power and water and wastewater, software that facilitates such human-centric decisions is known as supervisory control and data acquisition (SCADA) software.

Process Analytics

Analytics systems process a wide variety of process data to facilitate tactical, longer-term decisions on how to run a process more efficiently or effectively.

Manufacturing Execution Systems (MES)

An MES interfaces with and extends beyond process control into supply chain management and accounting applications. For example, an MES may monitor the quantity of ingredients remaining in a hopper for immediate use, the rate of use of those ingredients and the amount of ingredients held in storage. The MES could then automatically place an order with the ingredient supplier.

Predictive Maintenance Systems

A predictive maintenance system relies on sensors, such as vibration sensors, thermal imaging and diffused gas analysis, to identify areas that require maintenance before the component fails, thus limiting the costs that would result from an unanticipated failure. Information from predictive maintenance systems will be used by plant managers, technicians and engineers who work to keep the plant and process operating.

Network Equipment

Network equipment consists of the routers, switches, converters, access points, extenders, taps and firewalls that enable control system components (such as controllers and engineering workstations) to communicate. Within a production operations environment, important concepts not normally covered by a traditional networking curriculum include industrially hardened network equipment, protocol converters and leading vendors.

Industrially Hardened Network Equipment

"Industrially hardened" refers to the characteristics of the equipment that enable it to function in physically harsh environments, which may include exposure to extreme temperatures, electric shock, vibration, dust, moisture and corrosive substances. Industrially hardened devices may feature special materials, coatings, seals, mountings, dampers, reinforcements, filters and connectors.

Protocol Converters

Within industrial environments, a protocol converter, sometimes called a "gateway," acts as a "technology bridge," changing one communications protocol to another. For example, small hardware devices change serial communications (such as Modbus RTU) to IP communications (such as Modbus TCP). Software solutions, such as OPC gateways, make information from a variety of common industrial protocols (such as Modbus TCP or DNP3) available to other computers (such as supervisory control interfaces, process data historians and engineering computers) on the network.

Leading Network Equipment Vendors

Leading vendors of networking equipment for process control networks include Rockwell Automation (Stratix), Cisco (IE Series), Siemens (Scalance, RuggedCom), Belden (Hirschmann) and Moxa.

Signals and Protocols

Signals and protocols describe the ways that network nodes/endpoints assign meaning to electrical conditions over a physical medium to communicate with one another. Within a production operations environment, common signals and protocols include 4–20 mA, 0–5 V, HART, FOUNDATION Fieldbus, PROFIBUS and PROFINET, Modbus, EtherNet/IP, DNP3, IEC 61850, BACnet, MC protocol, Controller

Area Network (CAN), Open Platform Communications (OPC) and Message Queueing Telemetry Transport (MQTT).

4–20 mA

A 4–20 mA signal is the current sent over a wire between the transmitter and the controller. These continuous analog signals are normally set by an instrument technician who specifies a 4 mA signal as the lowest scaled value and a 20 mA signal as the highest scaled value. Values that are above or below the determined scale will not be specifically recognized. 4–20 mA is commonly used to transmit values related to temperature, pressure, level and flow. Compared with a 0–5 V signal, 4–20 mA has low susceptibility to noise and can handle longer distances without loss of signal. 4–20 mA stands in contrast to common Ethernet cable communications in that Ethernet cable uses voltage differential to communicate a digital (1 or 0) message.

0–5 V

A 0–5 V signal is the voltage sent over a wire between the transmitter and the controller (Levels 0 and 1 in the Purdue Enterprise Reference Architecture). These analog signals are normally set by an instrument technician who specifies a 0 V signal as the lowest scaled value and a 5 V signal as the highest scaled value. Values that are above or below the determined scale will not be specifically recognized. 0–10 V, 1–5 V or 2–10 V may also be used. Compared to a 4–20 mA signal, a voltage-based signal is more susceptible to noise/interference, requires a third wire to provide power to the instrument and is susceptible to voltage drops over long distances.

Highway Addressable Remote Transducer (HART)

HART is a communications protocol commonly found in industrial environments that enables a digital signal to exist on top of a continuous analog current (4–20 mA) between the transmitter and the controller. This allows HART-enabled instruments (transmitters and actuators) to provide additional information (such as device identification, configuration, diagnostics and maintenance information) back to the controller, potentially for use in predictive maintenance applications. The FieldComm Group maintains the HART standards.

FOUNDATION Fieldbus (FF)

FOUNDATION Fieldbus is a two-wire, voltage-based digital data transmission scheme originally envisioned as an open, standards-based replacement for 4–20 mA signals (operating) between the transmitter and the controller. Two differing implementations of FOUNDATION Fieldbus exist, H1 (which does not rely on TCP/IP) and HSE (high-speed Ethernet), which require different interfaces and physical media. The HSE implementation commonly operates over port 1600. The FieldComm Group oversees the FOUNDATION Fieldbus standards.

PROFIBUS and PROFINET

PROFIBUS and PROFINET are communications protocols used primarily with Siemens programmable controllers. PROFIBUS is a serial protocol deployed in a host-client where the controller is the client and the I/O devices are hosts, normally between the transmitter and the controller and between programmable controllers. PROFINET extends a similar concept to Ethernet networks, rather than using serial communications between Level 1 devices and from Level 1 to Level 2. PROFIBUS and PROFINET International oversee PROFIBUS and PROFINET standards.

Modbus

Modbus is a digital communication protocol used by a wide variety of programmable controllers. The protocol is deployed in a client-server relationship that is normally between the transmitter and the controller, among programmable controllers and between controllers and panel-based HMIs. Modbus has also been adapted to Ethernet networks, in which case it typically operates on port 502.

EtherNet/IP

EtherNet/IP is a digital communication protocol used primarily by programmable controllers from Rockwell Automation, though other vendors also support it. The protocol maps the Common Industrial Protocol (CIP) to Ethernet, commonly operates between controllers (panel-based HMIs and engineering workstations) and normally operates on ports 44818 and 2222. The EtherNet/IP protocol is overseen by the Open DeviceNet Vendor Association (ODVA).

Distributed Network Protocol 3 (DNP3)

DNP3 is a digital communication protocol used primarily by programmable controllers in the electric and water and wastewater sectors. In the electric industry, the protocol is commonly used for substation automation and communicating between RTUs and IEDs. DNP3 normally operates on port 20000. The DNP User Group oversees the protocol.

IEC 61850

International Electrotechnical Commission (IEC) 61850 is a suite of digital communication protocols used primarily by intelligent electronic devices in the electric sector for utility automation, where it facilitates communications between substations and between substations and control centers. IEC 61850 normally operates over ports 102 and 10200.

Building Automation and Control Network (BACnet)

BACnet is a data communication protocol used in buildings to control heating, ventilation and air conditioning (HVAC); lights; fire alarms and suppression; and other equipment. The protocol can run over a serial or Ethernet cable. BACnet is commonly used on controllers, engineering workstations

and supervisory interfaces. It normally operates on port 47808. The protocol is specified in ANSI/ASHRAE 135-2020.

Mitsubishi Communication (MC) Protocol

MC protocol is the digital communication protocol used predominantly by industrial automation products from Mitsubishi Automation, a leading industrial control systems vendor serving the Asia Pacific region. MC Protocol is commonly used among controllers and normally operates over port 5002.

Controller Area Network (CAN)

CAN is a digital protocol used primarily to control automobiles. It is also commonly found in electric generators and medical equipment, among a variety of other applications. The protocol operates in a bus topology and is formally specified in the ISO 11898-1:2024 standard.

Open Platform Communications (OPC)

OPC is a standardized way for industrial automation equipment, such as programmable controllers, to exchange process-related information with traditional computers. OPC is commonly used to make information from a variety of common industrial protocols (such as Modbus TCP or DNP3) available to other computers (such as supervisory control systems, process data historians and engineering computers) on the network. OPC Classic was historically based on Microsoft remote procedure call (RPC) technology. OPC UA was designed to reduce dependency on Microsoft technologies and enhance security, and it commonly uses port 4840. The OPC Foundation oversees the OPC standards.

Message Queueing Telemetry Transport (MQTT)

MQTT is a network transportation protocol designed for use by the internet of things (IoT). In particular, the protocol provides reliable communications in conditions of high latency or low bandwidth. MQTT implements a publish-broker-subscribe model that eliminates the need for a direct connection between a server and client. It also offers quality of service levels that can be selected based on the need for confirming the receipt of data. MQTT commonly uses ports 1883 and 8883. The MQTT standard is maintained by OASIS Open.

Wireless Communications

Wireless communications (also known as radio communications) play an important role in operations environments, especially for communication with remote sites and facilities. Important concepts for wireless communications within operations environments include licensed spectrum, global positioning systems (GPSs), Wireless HART, ISA-100.11a, ZigBee and software-defined radio.

Licensed Spectrum

A “licensed spectrum” is the permission granted by a regulatory jurisdiction to use certain radio frequency ranges exclusively. Within the United States, licenses are overseen by the Federal Communications Commission (FCC) and are leased to users. Interference within the licensed spectrum can be reported and license rights enforced. Licensed bands may be employed for communications with remote facilities such as pump stations in the water and wastewater sector or oil and natural gas sector, compressor stations in the oil and natural gas sector, and electric power substations in the electric power sector.

Some bands are not licensed, meaning that anyone in a particular area is free to use that frequency with limited legal recourse for interference. Therefore, it may be difficult to detect and stop intentional and malicious interference with radio communications within these ranges. These unlicensed bands are commonly known as ISM (industrial, scientific and medical). They include 5.8 GHz, 2.4 GHz and sub-GHz bands. Industrial control systems and IoT wireless devices frequently operate in these spectra.

Some devices in these ranges are known to accept communications without authenticating the sender or gateway. Many devices that do support authentication schemes require the device to authenticate to the network, but do not require the network to authenticate to the device, leaving some industrial control systems open to abuse with significant consequences.

Global Positioning Systems (GPS)

GPSs track the geolocation of an electronic device via communications with/from Earth-orbiting satellites. These signals enable automobiles, trains, airplanes, ships and, in some cases, the electric grid (synchrophasors) to operate accurately and safely.

Wireless HART

Wireless HART is a standard for communicating between field devices (sensors and actuators) and programmable controllers. Wireless HART uses a mesh topology and operates with the 2.4 GHz ISM band, with a purported range of several hundred meters. Use of Wireless HART transmission can alleviate the costs of purchasing, installing and maintaining wired connections, while maintaining access to the same type and formats of data available via wired HART.

ISA-100.11a

ISA-100.11a is a low-power radio communication standard developed by the International Society of Automation that is designed for production operations environments. It uses a mesh topology and operates in the 2.4 GHz ISM band, with a purported range of up to several hundred meters. ISA-100.11a can alleviate the costs of purchasing, installing and maintaining wired connections.

ZigBee

ZigBee is a low-power wireless radio communication standard designed for IoT environments, which has good adoption in building automation for residential and industrial contexts. It can use various topologies (such as star and mesh) and operates in the 2.4 GHz, 900 MHz and 868 MHz bands. It has a purported range of tens of meters, which is shorter than WirelessHART and ISA-100.11a. Within the electric power sector, ZigBee radios may provide a bridge point between a utility-operated smart meter network and a consumer-operated home network.

Software-Defined Radio

A software-defined radio (SDR) replaces dedicated radio hardware with software-configurable components, allowing SDR users to communicate with radios throughout the electromagnetic spectrum. The versatility and relatively inexpensive nature of SDRs provide opportunities for improving the robustness and reliability of wireless networks and for attacking them. Leading providers of SDR solutions include Ettus Research, National Instruments, Lime Microsystems and HackRF.

Process Safety and Reliability

Process safety and reliability are two of the most important concerns in production operations. They clearly differentiate industrial cybersecurity from traditional cybersecurity. Terms and concepts for this category include safety risk, functional safety, process states, maintenance strategies, control overrides/forcing, process and product safety communications, and electric sector reliability.

Safety Risk

A safety risk is the potential and possibility of physical harm (including death) to employees and the public resulting from industrial operations. Safety risk can be viewed from two sometimes conflicting perspectives: 1) the right to a reasonably safe work environment and 2) economic consequences to a business associated with safety events. Key concepts related to safety risk include causes, process hazards assessment, impact analysis and layers of protection.

Causes of Safety Risk

Causes of safety risk and safety events are many and varied. Key concepts in understanding causes include maintenance failure, complexity, intentional events and counterfeits.

Maintenance Failure

Process equipment experiences wear and tear due to a combination of the materials used in the equipment and environmental conditions. Failure to adequately maintain process equipment over

time against rust, vibration, expansion and contraction, and other countervailing forces can result in damage ranging from basic to catastrophic.

Complexity

Complexity—the numerous and nuanced relationships that exist between humans, machines and the environment within an industrial facility—can cloud perceptions of cause-and-effect, allowing a safety incident to occur.

Intentional Events

Intentional safety events occur when a human being, such as a disgruntled employee or motivated adversary, purposefully harms or kills another by abusing the industrial process or access thereto. "Sabotage" is a closely related term. Safety analysis within industrial environments has not typically considered intentional events.

Counterfeits

A counterfeit is an unofficial or unauthorized version of a good or service intended to appear like the official, authorized good or service. Counterfeits of many types pose a safety risk to operations environments mainly because they represent lower quality/functionality. Examples of counterfeited products include programmable controllers, software, electronic components, computer chips and safety documentation/certification, such as functional safety certifications.

Process Hazards Assessment (PHA)

"Process hazards assessment" is the term that encompasses formalized approaches to identify, describe and deal with dangers that arise within an operations environment. Significant concepts related to process hazards assessment include checklist, what-if, HAZOP and failure mode effect analysis. It is important to note that process hazards assessments have historically not included issues related to complexity, intentional events (including cyberattacks) and counterfeits.

Checklist

A checklist approach to a process hazards assessment requires the individual or team performing the assessment to ask a series of prompts or questions to discover whether a hazard may exist. Ideally, prompts are formulated so that a "yes" or "no" answer consistently indicates that a hazard does or does not exist. Checklists are valuable because they can be generated beforehand by teams familiar with the process, its potential hazards and the ways that incidents have occurred previously. Conversely, because checklists are intended for blanket application, they may miss situation-specific nuances.

What-If

Within the context of a process hazards assessment, what-if analysis seeks to produce critical thinking about how a hazard might occur and what might be done to address the potential risk. Because what-if analysis is essentially a structured brainstorming exercise, the success of this approach depends substantially on the expertise and sincerity of those conducting and participating in the assessment.

Hazard and Operability Study (HAZOP)

A HAZOP is a type of process hazards assessment that involves identifying system nodes/elements (often by examining engineering documentation) and considering deviations from expected operating parameters within each node. Guidewords for considering deviations may include “no,” “too high,” “too low,” “too fast,” “too slow,” “reverse” and “simultaneous.” This technique strikes a balance between the structure of a checklist and the less-structured what-if analysis. The potentially arbitrary identification of system nodes/elements may lead the team conducting the analysis to miss important relationships between nodes.

Failure Mode Effect Analysis (FMEA)

FMEA is a structured analytical technique for safety, reliability and quality of a design, function or process. The analysis seeks to identify failure modes, essentially the causes of failure and the associated effects that are the outcomes of those failures. Ideally, the analysis gives rise to actions that can reduce the possibility, likelihood or effects of identified failures. Various organizations have created standards and guidelines for conducting FMEA. One potential weakness of the FMEA is that it normally considers that only one failure mode can occur at a time.

Impact Analysis

Impact analysis (also known as effect analysis) seeks to identify and describe the outcomes of an undesirable event. Within the context of industrial automation, impacts may involve chains of events that ultimately damage human health, product quality and safety, the plant and equipment, the environment, the business and society. Impact analysis forms the basis for determining a safety level/category for a given industrial process. Traditional cybersecurity risk analysis often overlooks these types of impacts.

Human Health

The impact on human health is a description of damage to humans resulting from an event/incident. This can include short-term health effects, long-term health effects and deaths. Health effects are particularly applicable in radiological, chemical and explosive environments.

Product Quality and Safety

The impact on product quality and safety is a description of how an event damages the product being produced. In a manufacturing environment, a reduction in the quality of a component may cause

failure in the end product. In a pharmaceutical environment, incorrect amounts of ingredients could alter the effect of the drug on its consumer.

Plant and Equipment

Damage to plant and equipment is a description of the impacts on the physical components of an industrial process. An event could cause a coupling to shear, a robotic arm to crash into a conveyor, a pump to burn out or a boiler to explode. The full consideration of impacts to the plant and equipment should include the downtime and replacement costs.

Environmental Consequences

The impacts of an adverse event include the near- and long-term effects on the flora and fauna of a region. Environmental effects are influenced by the location and elevation of process equipment within a facility. For example, the location and elevation of a holding tank or reservoir in relation to what is beneath it will influence the results of an overflow or leak.

Business Consequences

Business consequences are the influences an event has on a company, agency or organization. These can include impacts to the confidence of consumers and partners, devaluation of brand/goodwill, and the ability of the organization to access capital markets, as well as the costs of engaging in legal or regulatory proceedings, leadership turnover and fines.

Societal Consequences

“Societal consequences” refers to the impacts of the event on society in general. These are generally considered “downstream” or “second order” effects and can include unavailability of goods, supply chain disruption, loss of shareholder wealth, long-term consequences of environmental impacts and new regulations.

Safety Levels/Categories

A safety level/category indicates the degree of safety required for equipment deployed within an operational context. In general, the higher the potential consequence of an event/incident or the more dangerous the situation, the higher the required level of safety.

Layers of Protection

“Layers of protection” refers to the concept that successive safety controls reduce the likelihood or impact of an adverse safety event or incident. Conceptually, each layer of protection helps mitigate the failure or ineffective operation of each previous layer. For example, an alarm or operator intervention may provide a first layer, then a safety instrumented function/system may take over if the operator does not catch the situation. Ideally, an engineered safeguard, such as a rupture disc, limits the consequences in case the safety system (safety instrumented function) does not fully

operate. A physical protection, such as thick walls and a thin roof, would direct the force of an explosion upward rather than outward. Finally, city emergency services would arrive to put out fires and offer medical treatment. Designing and operating each layer of protection requires specialized expertise.

Functional Safety

Functional safety is the field of study and practice that intends to protect humans from failures of engineered industrial processes and process equipment. The most effective approaches to functional safety seek to integrate safety at each phase of the process lifecycle. Key concepts related to functional safety include functional safety standards, safety instrumented functions and systems, failure modes, safety integrity levels, functional safety certifications, life safety systems and adequacy.

Functional Safety Standards

Many industries have developed standardized approaches to ensuring the safety of products and processes. Core to these is IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. Related standards include ANSI/ISA-61511 series/IEC 61511 series (process industries), ISO 26262 (automotive), EN 50128 (rail transportation, developed by CENELEC), IEC 62304 (medical devices) and IEC 60880 (nuclear). The confluence of software, safety and cybersecurity is a complex area for which standards continue to evolve.

Safety Instrumented Functions and Systems

A safety instrumented function relies on instrumentation and a programmable controller to detect and respond appropriately to a potentially dangerous situation. A safety instrumented system (SIS) typically addresses multiple functions. Safety instrumented functions and systems may be more consistent, reliable and effective than humans in certain safety-related conditions because of their accuracy and speed. For example, a sensor may detect a rapidly rising pressure and signal the safety controller to quench the input of natural gas into a boiler more quickly than a human could interpret and react to the evolving situation.

Failure Modes

Failure modes are essentially the ways a process or a component fails—the causes of failure. Over time, certain process components may fail due to similar causes, resulting in the concept of “common failure modes.” Failures may also be statistically modeled to produce “failure rates.” Such rates can be expressed as ratios (such as defective parts per thousand), average times (such as mean time between failures [MTBF]) or average uses (expected number of operations). These figures are useful in devising maintenance strategies. It is important for industrial cybersecurity practitioners to understand the failure modes of the processes and equipment with which they work.

Safety Integrity Levels (SILs)

SILs represent a level of assurance that a safety instrumented function and system will perform properly. This is normally interpreted as meeting a specific threshold of probabilistic failure combined with how many times per year the safety function is intended to operate. The IEC 61508 standard describes four levels, where SIL 4 has the lowest probability of failure. For example, a safety controller selected for use in an environment requiring SIL 3 may have redundant input circuits, redundant processors and redundant output circuits combined with diagnostic circuits to continue operations and alert the user (technician) in case of component failure.

Functional Safety Certifications

"Functional safety certifications" refer to certificates awarded to a safety controller by a certification body, confirming that the safety controller conforms to standards for deployment in a certain SIL. Common testing/validation laboratories for safety controllers include Exida and TUV SUD.

Life Safety Systems

A life safety system intends to preserve the lives of those present in case of adverse events, such as fire, earthquake, gas leak or loss of electricity. These stand in contrast to functional safety systems, which are focused on the industrial process. Life safety systems are clearly high-value targets for adversaries seeking to maximize certain consequences.

Adequacy

"Adequacy" refers to the effort to determine whether all specified safeguards reduce the risk of individual and combined events and impacts to an acceptable level. In many cases, this is a mathematical or quasi-mathematical analysis based on overall financial impact and frequency of occurrence. In a simplified form, adequacy leads one to ask something like this: "Is my company willing to accept a loss of $1M once every 10 years?" This analysis helps guide investments in safeguards.

Process States

A "process state" is a set of physical conditions in which an industrial process may exist. For example, in an "off" state, a pump may be off and a valve may be closed. In an "on" state, a pump may be on and a valve may be open. States can include more complicated/longer lists of conditions. Process state awareness helps engineers, technicians and control room operators understand and communicate the existing physical conditions quickly. This understanding enables them to create specialized safety alarms and security alerts and to follow safe work procedures.

Maintenance Strategies

Maintenance strategies are techniques to ensure plant operations continue in the face of engineering limitations (inevitable component failures). Strategies include redundancy, spares, maintenance outages, predictive maintenance and preventive maintenance. Production operations may employ these strategies simultaneously.

Redundancy

Redundancy is the simultaneous deployment of components, such that if one fails, the "extra" component immediately takes over performing the function. One weakness with a redundancy strategy is that the cause of failure that affects one component may quickly affect its replacement. Redundancy may be used in conjunction with diversity, meaning the redundant component has a core difference (such as a different principle of operation for a sensor) from the original.

Spares

A spare is an unused component available for deployment in case another component fails. A spares strategy differs from redundancy in that the extra component remains unused. Effective use of the spares strategy requires predicting which components are likely to fail and maintaining enough spares on hand.

Maintenance Outages

A maintenance outage is a period of planned operational downtime—when the plant and its processes are not running—in order to repair, replace and upgrade components. This period is also known as a maintenance "turnaround window." These are moments of intense activity as technicians and contractors make improvements before returning the plant to its operational state. Every moment the plant is not working represents lost revenue. Maintenance outages can also be useful in adding safety and cybersecurity measures, such as deploying software updates or network security enhancements.

Predictive Maintenance

Predictive maintenance relies on instrumentation (such as vibration sensors and ultraviolet cameras) to anticipate what failures are likely to occur soon and intentionally address them. In theory, a temporary intentional outage has lower costs than recovering from a surprise failure. Many vendors provide predictive maintenance software solutions.

Preventive Maintenance

Preventive maintenance is based on the premise that intervention for an anticipated need is less costly than a repair after failure. While it may be superior to a "wait to fail" strategy, preventive

maintenance (versus predictive maintenance) can result in conducting less-required maintenance while missing some failures.

Control Overrides/Forcing

The term "control overrides/forcing" refers to writing a specific input value to a controller that differs from the actual process variable, or writing an output (control variable) when the input value does not require it. This is particularly useful during tests of control system functionality. Control overrides may be used by an attacker trying to cause a specific physical effect.

Process and Product Safety Communications

The term "process and product safety communications" covers a variety of safety-related communications related to a specific process or product. One example would be a safety recall for a skid-mounted process system. Such communications must be carefully crafted to help the intended audience clearly understand and make appropriate decisions, such as to discontinue use or perform maintenance. These communications should use proper, recognized distribution channels to ensure prompt recognition and action.

Electric Sector Reliability

System reliability in the electric power sector is governed by the idea that an intentional short-duration loss of electric power is preferable to a long-duration loss caused by the physical destruction of equipment and possible physical harm to employees or the public. Important concepts and terminology for electric system reliability include reliability operating limits, undervoltage, overvoltage, underfrequency, overfrequency, inter-area flows, control circuits, automatic reclosing and special protection systems (SPS)/remedial action schemes.

Reliability Operating Limits

Reliability operating limits are the criteria within which the system is intended to function. These can include facility and equipment ratings for current, voltage, frequency and heat. Interconnected systems are subject to special interconnection reliability operating limits that require specialized communication between interconnected parties (such as adjacent electric utilities).

Undervoltage

Undervoltage is a condition in which an electric system does not deliver enough electromotive force (voltage) for electric equipment to operate properly. This is commonly called a "brownout." While damaging, undervoltage typically has less immediate destructive potential than overvoltage.

Overvoltage

Overvoltage is a condition in which an electric system delivers more than the required amount of electromotive force (voltage) than the electric equipment requires. This can be immediately destructive to electrical equipment. A lightning strike is an example of a temporary overvoltage condition.

Underfrequency

Underfrequency is a condition that occurs when unanticipated load (use of electricity) is added to the system, causing the generator to slow. To maintain the reliability of the system (as measured by frequency), a load shedding scheme may remove certain electricity users or uses from the system. This could be achieved by temporarily turning off power to a specified geography or by turning off certain types of electricity use (customer air conditioners on a hot summer day).

Overfrequency

Overfrequency occurs when an unanticipated load (use of electricity) is removed from the system, causing a generator to speed up. To maintain the reliability of the system (as measured by frequency), the generator must be slowed. This can be accomplished by modifying input, such as providing less fuel to a combustion engine or by adding a resistive load.

Inter-Area Flows

“Inter-area flow” refers to the movement of electricity across service areas of disparate utilities. Coordinating utilities can require careful communication about supply and load. The further apart (geographically) the generation resources are, the more difficult it can be to synchronize systems, potentially causing oscillation among groups of generators, threatening grid stability.

Control Circuits

Within the context of the electric grid, a control circuit helps ensure that the amount of electricity generated matches the amount of load or demand at each moment. These can include automatic generation control, load frequency control and grid protection. In certain circumstances, a control circuit may send a signal to disconnect the load from the source or to trip the source (generator) offline.

Automatic Reclosing

Faults in an electric system may be temporary (transient) in nature, such as a tree or an animal causing a ground fault by contacting electrical equipment. In such cases, an automatic recloser can detect and rectify the issue without requiring human intervention. A recloser is an electric switch that monitors the electrical line for overcurrent caused by faults. When a fault occurs, the recloser interrupts power by opening the breaker contacts. The recloser continues to monitor the line and is

programmed to attempt to close the breaker contacts multiple times to reestablish the flow of electricity in case the fault clears, such as when the tree is no longer touching the line. Automatic reclosers can be programmed to attempt to operate a certain number of times and to wait a specified time period before trying again.

Special Protection System/Remedial Action Schemes

A special protection system (SPS), also known as a remedial action scheme (RAS), is a series of programmed actions taken by control circuits to stabilize the grid and prevent catastrophic damage to the equipment that comprises the grid. SPS actions may affect generating assets (as opposed to underfrequency or undervoltage load shedding). Important terms related to special protection systems include "SPS database" and "SPS performance."

SPS Database

The SPS database is a repository of information about the conditions that would trigger a significant reduction (shutdown) of grid operations. Because of their implicit knowledge of the most dangerous conditions on the grid, SPS databases may represent sensitive information. They are shared between necessary electric power companies and the North American Electric Reliability Corporation (NERC).

SPS Performance

SPS performance is a description of when the SPS was invoked and how well it worked. Information about performance may include the amount of time the SPS has existed, how many times it has operated, how many times it has failed, how many times it has operated incorrectly and how many times it has operated unnecessarily.

Industrial Cybersecurity Superstructure

This section describes core terminology associated with industrial cybersecurity. It expresses the relevance of each term and provides a basic nuance for applying terms within the context of production operations and industrial control system environments, as opposed to traditional corporate networks. Categories include guidance and regulations, common weaknesses, industrial cybersecurity events and incidents, and defensive techniques.

Guidance and Regulations

This category includes frameworks and paradigms, guidance and standards, regulations, and groups and associations that cover the policy background to industrial cybersecurity.

Frameworks and Paradigms

Frameworks and paradigms are the overarching principles and concepts that guide thinking about industrial cybersecurity. These include critical function assurance, the Seven Ideals, SRP (Safety, Reliability, Productivity), the Five Ds (Deter, Detect, Deny, Delay, Defend) and SAIC (Safety, Availability, Integrity, Confidentiality).

Critical Function Assurance

A critical function is an indispensable or key action or event. For example, within the context of modern societies, critical functions could include providing electric power and clean drinking water. Within an aviation context, it could involve providing thrust and landing gear deployment. To “assure” means to make sure or certain. Hence, critical function assurance is the process of making sure the critical function is delivered and performs as intended.

It is important to recognize that critical function assurance includes employing technology, processes and people across the domains of physical world engineering, information technology (IT) systems and cybersecurity. One method of conducting critical function assurance is Consequence-driven Cyber-informed Engineering (CCE).

Seven Ideals

The seven ideals model is a memorable technique for thinking about industrial cybersecurity within an adversarial context. The ideals are as follows:

1. The security group knows the current system perfectly.
2. The attack group knows nothing about the system.
3. The system is inaccessible to the attack group.
4. The system has no vulnerabilities.

5. The security group detects attacks instantly.
6. The security group restores system trust immediately.
7. The system cannot cause damage.

These ideals are ordered such that if each successive ideal is not met, the following ideal provides additional assurance. Under this model, the ultimate backstop (ideal 7) consists of cyber-physical fail-safes.

SRP (Safety, Reliability, Productivity)

The SRP framework emphasizes system characteristics that resonate with engineering and production operations personnel: safety, the ability to protect humans from physical harm; reliability, the ability to keep the process running given the physical demands of the operating environment; and productivity, the ability to maximize the desired output. These characteristics stand in contrast to the confidentiality, integrity and availability (CIA) triad that cybersecurity personnel are usually familiar with.

Five Ds (Deter, Detect, Deny, Delay, Defend)

The Five Ds provide a defensive mindset rooted in physical security. The model applies well to industrial cybersecurity because industrial control systems can represent high-value targets to well-resourced and co-adaptive adversaries. These are the Five Ds:

1. Deter – To dissuade an adversary from choosing the organization as a target
2. Detect – To identify attack attempts
3. Deny – To provide a challenging first line of defense
4. Delay – To slow an adversary's progress
5. Defend – To directly confront an adversary to force an attack to stop

SAIC (Safety, Availability, Integrity, Confidentiality)

The SAIC framework expresses desired control system characteristics in order of importance. It extends the CIA triad to emphasize the primacy of safety, which is the preservation of human life and health. It points out that in traditional cybersecurity literature, safety exists only as a characteristic derived from the other three. It also explains that in an industrial control system, confidentiality is of the least concern.

Guidance and Standards

Guidance and standards refer to the documents intended to direct developing and deploying industrial cybersecurity and to the bodies (groups) that create those documents. Industrial cybersecurity guidance and standards may be general or sector-specific. Some standards bodies provide both general and sector-specific guidance and standards.

General Industrial Cybersecurity Guidance and Standards Bodies

Within the context of industrial cybersecurity, a guidance and standards body is a group that creates and promotes cybersecurity advice pertinent to organizations that deal with industrial control systems, regardless of sector or industry. General guidance and standards bodies can be considered international guidance and standards bodies, whose mission is focused on multiple countries, or national guidance and standards bodies, whose mission is focused on a single country.

International General Industrial Cybersecurity Guidance and Standards Bodies

International guidance and standards bodies for industrial cybersecurity include the International Society of Automation (ISA), the International Electrotechnical Commission (IEC) and the European Network and Information Security Agency (ENISA).

International Society of Automation (ISA)

ISA is a global professional society whose members work in the industrial automation profession. Over 17,600 ISA members participate in the society, with over 103 geographic sections in 33 countries (according to the ISA 2024 Annual Report).

ISA's mission includes providing guidance and standards in the field of industrial automation and control systems across all industry sectors. ISA drives several efforts dedicated to enhancing the cybersecurity of industrial control systems, including the ISA Global Cybersecurity Alliance and ISASecure, a conformity assessment scheme for OT cybersecurity.

ISA's industrial cybersecurity standards, developed by the ISA99 Committee, are published by ISA as the ISA-62443 series and published by the IEC as the IEC 62443 series. To represent this relationship, the documents are often referred to as ISA/IEC 62443. ISA has also developed Technical Report 84 (TR84)*, Cybersecurity Related to the Functional Safety Lifecycle*.

- **ISASecure**

  ISASecure is a membership-driven effort to certify industrial control systems devices and the organizations that manufacture them as conforming to security requirements set forth in the ISA/IEC 62443 series of cybersecurity standards for industrial automation and control systems.

- **ISA Technical Report 84.00.09-2024, *Cybersecurity Related to the Functional Safety Lifecycle***

  ISA-TR84.00.09 addresses integrating the key elements of the safety lifecycle with the cybersecurity lifecycle for industrial automation and control systems.

International Electrotechnical Commission (IEC)

The IEC is an international standards body headquartered in Switzerland that prepares and publishes standards dealing with electricity and electronics-related fields across a broad variety of focus areas. In coordination with ISA, IEC publishes the IEC 62443 series to provide advice on the general practice

of industrial cybersecurity. It has published IEC 62645 to provide cybersecurity guidance for the electrical and control systems in the nuclear sector.

- **ISA/IEC 62443, *Industrial Automation and Control Systems Security***

  The ISA/IEC 62443 series of documents developed by ISA and the IEC is the leading international consensus-based standard for industrial cybersecurity. Its guiding concepts include principal control systems roles, the industrial control system lifecycle, security architecture and security levels.

- **IEC 62645 Ed. 2.0 b: 2019, *Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements***

  The IEC 62645 document, promoted by the IEC, describes the application of the ISO 27001 general cybersecurity guidance to industrial control systems used in nuclear power plants.

European Network and Information Security Agency (ENISA)

ENISA is an agency of the European Union (EU) dedicated to promoting high levels of cybersecurity across the EU member states. Its initiatives foster cooperation in creating guidance and policy. ENISA has addressed the topic of industrial cybersecurity in the past through documents such as *Protecting Industrial Control Systems: Recommendations for Europe and Member States*, and *Good Practice Guide for CERTs in the Area of Industrial Control Systems*.

National General Industrial Cybersecurity Guidance and Standards Bodies

The following national guidance and standards bodies for industrial cybersecurity are located in the United States of America.

United States Industrial Cybersecurity Guidance and Standards Bodies

The United States government has been a global leader in producing industrial cybersecurity standards and guidance. Bodies providing general standards and guidance for the United States include the US National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). The Department of Energy is an example of one of the bodies that provides sector-specific guidance and standards for the United States.

- **US National Institute of Standards and Technology (NIST)**

  NIST is an agency of the United States Department of Commerce charged with coordinating the development of technology and standards that promote common understanding and interoperability in many fields. NIST has developed dozens of cybersecurity guidance and standards documents that must be followed for systems owned by the United States government. These documents are also useful to private industry regardless of an

organization's home nation. Special Publication 800-82, *Guide to Operational Technology Security*, specifically applies to industrial cybersecurity.

  - ***NIST SP 800-82, Guide to Operational Technology Security***
    This publication provides guidance on securing industrial control systems; revision 3 of the document refers to "operational technology" as "OT." The document introduces OT systems, describes the development of a security program and discusses risk management, security architecture and the application of security controls within OT environments.

- **US Department of Homeland Security (DHS)**

  The DHS is a US federal agency broadly charged with maintaining security within the United States. The agency primarily has a supportive role for cybersecurity issues, offering a variety of services to other agencies and US-based businesses and organizations, ranging from professional training to incident response. Since 2018, the DHS has provided resources for industrial control systems security primarily through the Cybersecurity and Infrastructure Security Agency (CISA).

- **US Cybersecurity and Infrastructure Security Agency (CISA)**

  CISA is a civilian-led agency that oversees federal efforts related to cybersecurity, infrastructure security, emergency communications and risk management. Industrial control systems are a focus area within CISA's cybersecurity mission. CISA coordinates disclosures of ICS-related software vulnerabilities.

Sector-Specific Industrial Cybersecurity Guidance and Standards Bodies

Guidance and standards bodies may focus on advising a particular industry or sector. Some of these are national in scope, others are international. Some sector-specific bodies have well-developed guidance; others are just beginning to create guidance. Some sectors have no sector-specific industrial cybersecurity guidance at all. While the list of industries with guidance will change over time, sectors with recognized industrial cybersecurity guidance include transportation, electric power, oil and natural gas, water and wastewater, and food and pharmaceutical. Sector-specific industrial cybersecurity guidance and standards bodies may be national or international in scope.

SAE International

SAE International is an association of engineers and technical experts serving the transportation sector, including the aerospace and automotive industries, throughout the world. The body promotes professional development, knowledge sharing and the creation of guidance and standards. The body's cybersecurity standard for the automotive industry is ISO/SAE 21434:2021, *Road Vehicles – Cybersecurity Engineering*.

- **ISO/SAE 21434:2021, *Road Vehicles – Cybersecurity Engineering***

  This document, created and promoted by SAE International, describes risk management and vulnerability management practices that should be applied to vehicle electric and electronic systems throughout the vehicle life cycle.

International Organization for Standardization (ISO)

ISO is an international body composed of member standards bodies from throughout the world. It has over 800 committees and subcommittees that have developed more than 24,000 standards since the organization's formation in 1945. ISO published ISO 27001 to address cybersecurity in general and published ISO/IEC 27019:2017 jointly with the IEC to guide information security controls in the energy utility industry.

- **ISO/IEC 27019:2017, *Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry***

  This document applies the terminology and risk management structure described in the ISO 27001 and 27002 standards to industrial control systems used in the energy utility industry.

US Department of Energy (DOE)

The DOE is an agency of the United States government dedicated to maintaining the country's energy security. The DOE has been involved in industrial cybersecurity since a least 2005 via its involvement in the National SCADA Test Bed. Through its various divisions, the organization has funded numerous research and development projects for industrial cybersecurity and published resulting documentation and guidance. Among the most significant documents are the DOE's Cybersecurity Capability Maturity Model (C2M2) and the *National Cyber-Informed Engineering Strategy*.

- **Cybersecurity Capability Maturity Model (C2M2)**

  The C2M2 guides firms operating industrial control systems to consistently evaluate the maturity of their cybersecurity efforts relative to IT, OT and information assets. The guidance consists of 300 cybersecurity practices divided into 10 domains. The way an organization applies the practices indicates a maturity level for each domain, ranging from 0 (practices are not performed) to 3 (practices are advanced and well-managed).

American Petroleum Institute (API)

API is a trade association formed in 1919 whose current mission is to promote safety and influence US policy across all aspects of the oil and natural gas industries. The organization is composed of approximately 600 North American corporations that have collaborated to develop over 800 standards, including American Petroleum Institute Standard 1164, *Pipeline Control Systems Cybersecurity.*

- **API Standard 1164, *Pipeline Control Systems Cybersecurity***

  This document describes API's recommendation for pipeline operators to develop and maintain a robust, risk-based cybersecurity program consistent with requirements from the US Transportation Security Agency and guidance from the National Institute of Standards and Technology and the ISA/IEC 62443 series.

American Water Works Association (AWWA)

Founded in 1881, AWWA is a membership-based society composed of 4,300 utilities and roughly 50,000 individuals collaborating to advance knowledge, educate the public and conduct research related to water systems and water resources within the United States. The group has developed more than 190 standards. Its primary guidance for industrial cybersecurity is the *Water Sector Cybersecurity Risk Management Guidance*.

- ***Water Sector Cybersecurity Risk Management Guidance***

  This document, provided by the AWWA, describes several approaches for water utilities to implement to improve their cybersecurity posture quickly. It lists 100 prioritized cybersecurity controls across 14 categories, incorporates a set of questions to help utilities easily recognize areas for improvement, and provides a list of potential improvement projects.

US Food and Drug Administration (FDA)

The FDA is an agency of the US Department of Health and Human Services with regulatory authority to ensure public health relative to the nation's food supply, pharmaceuticals, medical devices and radiation-emitting products. The FDA has issued guidance regarding software included in medical devices since the late 1990s. *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff* presents the FDA's latest thinking on the topic (2023).

- ***Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff***

  This nonbinding guidance issued by the FDA affirms that cybersecurity is part of device safety and quality system regulations. It points device manufacturers to the advice provided by the National Institute of Standards and Technology and the International Society of Automation, and it includes specific guidance on security risk management, security architecture and cybersecurity transparency. The last of these requires product labeling to provide device users with cybersecurity information, including a software bill of materials.

Regulations

Industrial cybersecurity regulations differ from guidance and standards in that they intend to be mandatory and carry imposed consequences, such as fines, for noncompliance. This topic consists of jurisdictions, regulatory bodies, regulation documents, audits and enforcement.

Jurisdictions

A jurisdiction is the scope of enforcement for a regulatory body or regulation. This scope can consist of a geographic context (such as within a country's borders) and/or industry context (such as within a specific industry sector). Elements of a jurisdiction include governments, regulatory processes and authorities.

Regulatory Processes

Regulatory processes can describe the way that regulations are created and the way those regulations are ultimately enforced. Laws and regulations may affect some industry sectors and not others.

Authorities

"Authorities" refers to permission granted to an agency or regulatory body to create and enforce regulations. Such permissions are usually given in a law. It is common for a law to describe what the authority is, but not how that authority is to be exercised, which may be developed by the organization that has been given the authority.

Governments with Industrial Cybersecurity Regulations

Governments create rules that organize society. Countries have differing processes for making laws, assigning regulatory authority and enforcing regulations. Governments that have laws addressing industrial control systems cybersecurity include the United States and the European Union.

United States Industrial Cybersecurity Regulations

Regulatory bodies in the United States include the North American Electric Reliability Corporation (NERC), Nuclear Regulatory Commission (NRC) and Transportation Security Agency (TSA). In addition, the president of the United States has issued relevant Executive Orders.

- **North American Electric Reliability Corporation (NERC)**

  NERC is an industry body consisting of owners and operators of electric power systems in the United States and Canada that collaborates to ensure the reliability of the electric system. The US Federal Energy Regulatory Commission (FERC) assigned NERC the authority to create and enforce reliability standards. Its regulations relating to the cybersecurity of the electric grid are known as the Critical Infrastructure Protection (CIP) standards.

- **NERC Critical Infrastructure Protection (CIP)**
  NERC CIP is a set of 12 regulatory standards that describe cybersecurity controls that owners and operators of the US bulk electric system must apply. Compliance with the standards is assessed by auditors from NERC regional entities. Fines for noncompliance can reach $1M per violation per day.

- **US Nuclear Regulatory Commission (NRC)**

  The NRC is the US government agency charged with preserving public and environmental health and safety relative to nuclear energy. The NRC has published 10 CFR 73.54 and NRC Regulatory Guide 5.71 to regulate cybersecurity in the nuclear industry.

  - **10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks***
    This section of the Code of Federal Regulations (CFR) requires licensed operators of nuclear power plants to submit a cybersecurity plan that covers digital equipment used for safety functions, security functions, emergency preparedness functions and support systems to the NRC for review and approval. Operators must identify assets that need protection and establish a cybersecurity program as a component of a physical protection program. They must also develop a cybersecurity plan that includes incident response activities.
  - **NRC Regulatory Guide 5.71, *Cybersecurity Programs for Nuclear Facilities***
    This guide describes an approach that NRC staff finds acceptable for complying with 10 CFR 73.54. It offers additional advice for developing a cybersecurity plan, refers to other national and international guidance, and provides a template for creating a cybersecurity plan.

- **US Transportation Security Agency (TSA)**

  The TSA is an agency of the US DHS charged with overseeing the safety of interstate transportation, including aviation, rail, vehicle and pipeline transportation, and enforcing security-related regulations and requirements. The TSA has released cybersecurity directives for rail transportation (passenger and freight) and pipelines.

  - **TSA Security Directive 1580-21-01A**
    This directive requires all freight railroad carriers and TSA-designated freight railroads within the United States to designate a cybersecurity coordinator, report cybersecurity incidents to the CISA, develop a cybersecurity incident response plan and report the results of a cybersecurity vulnerability assessment to the TSA. Violations can result in civil sanctions of up to $13,000.
  - **TSA Security Directive 1582-21-01A**
    This directive requires all passenger railroad carriers and rail transit systems within the United States to designate a cybersecurity coordinator, report cybersecurity incidents to

the CISA, develop a cybersecurity incident response plan and report the results of a cybersecurity vulnerability assessment to the TSA. Violations can result in civil sanctions of up to $13,000.

  - **Security Directive Pipeline-2021-02C**
    This directive requires all owners and operators of hazardous liquid and natural gas pipelines and TSA-notified liquefied natural gas facilities to establish a TSA-approved cybersecurity implementation plan, develop and maintain an up-to-date cybersecurity incident response plan and establish a cybersecurity assessment program. The directive includes a list of cybersecurity measures the affected organizations must incorporate. Violations can result in civil sanctions of up to about $15,000.

- **US Laws**

  The legislative process in the United States generally requires proposed laws (bills) to be passed by both houses of Congress and signed by the US president. Numerous proposals have dealt directly with industrial cybersecurity, but relatively few have been signed into law. Clauses related to industrial cybersecurity were incorporated into the National Defense Authorization Act of 2022.

  - **National Defense Authorization Act (NDAA) of 2022 (Sections 1541 and 1548)**
    The NDAA is a series of laws authorizing the annual budget and expenditures for the US Department of Defense. Section 1541 of the 2022 law requires the CISA to maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. Section 1548 of the 2022 law authorizes CISA's CyberSentry program to establish strategic relationships with owners and operators of industrial control systems that support national critical functions in order to provide continuous monitoring and detection of cybersecurity risks.

- **Executive/Presidential Orders**

  In his capacity as chief executive of the United States, the president can order executive branch agencies to take specific actions. Several orders (made by various presidents) have addressed the cybersecurity of critical infrastructure. These include "Executive Order 13636: Improving Critical Infrastructure Cybersecurity," "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" and "Executive Order 13920 Securing the United States Bulk-Power System" (suspended). Additional orders with a broad impact on industrial cybersecurity may be issued in the future.

  - **`Executive Order No. 13636: Improving Critical Infrastructure Cybersecurity"**
    This order, issued under President Obama in 2013, attempted to create a unified approach to critical infrastructure cybersecurity within the United States. It required the US NIST to create a baseline framework to reduce risk to critical infrastructure, including standards,

methodologies, procedures and technological approaches. It ordered agencies responsible for regulating the security of critical infrastructure to determine whether they had clear authority to require the application of the framework. It required the DHS to identify critical infrastructure where a cybersecurity incident could have devastating regional or national effects and to notify owners and operators of the identified infrastructure.

- **‘Presidential Policy Directive 21: Critical Infrastructure Security and Resilience“**
  PPD 21 is a companion document to Executive Order No. 13636, issued in 2013 by President Obama. It directed the DHS to align federal efforts for coordination with critical infrastructure owners and operators, with a focus on information sharing.
- **‘Executive Order No. 13920: Securing the United States Bulk-Power System“ (suspended)**
  Based on the premise that foreign adversaries are increasingly creating and exploiting vulnerabilities in the US bulk-power system (generally considered “the electric grid”), Executive Order No. 13920, issued by President Trump in May 2020, was intended to prohibit acquiring equipment used in the bulk-power system from companies or individuals subject to the direction of a foreign adversary. The order charged the Secretary of Energy to oversee its implementation. The order was suspended in January 2021 by President Biden.

European Union Industrial Cybersecurity Regulations

The EU is a political body composed of representatives from its various member countries. The EU uses a consultative process when developing legislation. The EU Parliament approved a Cybersecurity Act in 2013, which it updated in 2019 as Regulation (EU) 2019/881.

- **Regulation (EU) 2019/881 (EU Cybersecurity Act)**

  This act charges the European Network and Information Security Agency (ENISA) to serve as an independent center of expertise to support cybersecurity preparedness and cooperation among member states. The act emphasizes ENISA’s role in helping to establish, maintain and promote a European cybersecurity certification framework. Introductory clause (65) of the Act emphasizes the importance of cybersecurity certification for a variety of cyber-physical systems, including industrial automation control systems, but it does not create or constitute a regulatory regime per se.

Regulatory Bodies

A regulatory body is a group that creates and enforces regulations.

Regulation Documents

Regulatory documents outline the requirements that regulated entities must meet and the enforcement actions that will be taken if an audit determines that they are not met. Codes, such as

national or international fire protection codes, electrical codes and building codes, are influential regulation documents because jurisdictions may require compliance with their provisions, which are updated periodically. Such provisions may include cybersecurity or industrial cybersecurity practices.

Audits and Enforcement

These concepts describe the process a regulatory body or its agents follow to check whether the regulated entity complies with mandatory requirements. Consequences for noncompliance may include fines.

Industrial Cybersecurity Groups and Associations

Industrial cybersecurity groups and associations consist of collaborative efforts to promote industrial cybersecurity. These include the International Society of Automation (ISA), information sharing and analysis centers (ISACs), and professional conferences.

Information Sharing and Analysis Centers (ISACs)

ISACs are typically nonprofit groups created for the purpose of sharing security information, including between the government and private industry. These groups develop their own rules and procedures, with various levels of formality and sponsorship. Information may be shared between participants on websites, through automated feeds, during monthly calls and in periodic gatherings. The quality of the information shared can vary greatly. ISACs are commonly organized by industry sector within a country. In the United States, the National Council of ISACs lists 25 member ISACs.

Professional Conferences

Numerous professional conferences throughout the world are dedicated to the topic of cybersecurity for industries that rely heavily on industrial control systems. These provide an opportunity for participants to learn and develop professional relationships. Prominent examples of such conferences include S4, Dragos DISC, SANS ICS Security Summit and the ICS Cybersecurity Conference.

Common Weaknesses

“Common weaknesses” refers to vulnerabilities frequently found in industrial control system environments. Classes of such weaknesses may include managerial weaknesses, system and host weaknesses, network weaknesses, and instrumentation and control weaknesses.

Managerial Weaknesses

Managerial weaknesses affecting industrial cybersecurity originate at a leadership and governance level within an organization. These include lack of sponsorship and resources, inadequate consideration of ICS cybersecurity risk, lack of stakeholder alignment, lack of cybersecurity awareness

and training, no ICS cybersecurity program, no ICS security policies and contingency plans that lack an ICS focus.

Lack of Sponsorship and Resources

This topic refers to the attention and commitment of an organization's executives to industrial cybersecurity. Without intentional and prolonged executive leadership, it is not likely that an organization can implement the structural, cultural and administrative changes required.

Inadequate Consideration of ICS Cybersecurity Risk

The complex and interdisciplinary nature of systems engineering and the growing interdependencies between modern information systems and industrial control systems have resulted in compartmentalized and inaccurate consideration of ICS cybersecurity risks. This is commonly characterized by 1) risk models that do not consider the ease with which adversaries might carry out intentional attacks (*possibility* rather than *probability*) and 2) the erroneous assumption that "someone must have already been assigned to think about that."

Lack of Stakeholder Alignment

Even if an executive team has recognized an industrial control system cybersecurity risk and is committed to addressing it, identifying and convincing all the right people, including managers and employees across various organizational functions, to feel concern, establish new relationships and dedicate their energy to make lasting changes presents a significant challenge.

Lack of Cybersecurity Awareness and Training

Awareness and training efforts are pivotal to altering attitudes and behaviors relative to industrial control systems cybersecurity. While many organizations offer annual or semiannual general cybersecurity awareness training for all their employees, this training is seldom customized to the roles and responsibilities of those who design, implement, operate, maintain and support such systems.

No ICS Cybersecurity Program

Once the need for industrial cybersecurity has been recognized, a plan for sustained effort and continuous improvement should be put in place. Industrial cybersecurity differs significantly from information systems security and requires additional, specialized considerations. The ISA/IEC 62443 series of documents recommends elements of a high-quality ICS cybersecurity program.

No ICS Security Policies

A policy is an indispensable element of an industrial cybersecurity program. Cybersecurity policies for industrial operations professionals, including engineers, technicians, process operators and control room operators, often do not exist. Each policy should clearly describe the aim of the policy, who the

policy applies to, the practices that must be followed, the manner of enforcement and the consequences of noncompliance. Individuals who will be impacted by a policy should receive training on how to implement it. Each policy should have a process for requesting and documenting exceptions and be subject to periodic review and improvement.

Contingency Plans Lack an ICS Focus

Many organizations have contingency plans in place for various aspects of their operations, including incident response plans for network and facility disruptions. However, these plans may not adequately consider cyber incidents that simultaneously affect IT and OT systems. Such a lack of planning will increase and prolong undesirable impacts.

System and Host Weaknesses

"System and host weaknesses" refers to a class of weaknesses affecting the computers—such as supervisory interfaces, engineering workstations, HMIs, technician laptops and controllers—used to design, build, operate and maintain industrial control systems. Weaknesses in the system and host category include lack of authentication requirements, lack of software integrity mechanisms, lack of physical access controls, lack of least privilege, lack of software backups, lack of a software upgrade path, uncontrolled file transfer, unpatched software, unassured provenance, unrecognized third-party relationships and poor programming practice.

Lack of Authentication Requirements

Authentication is the process of proving one's identity and authority. This is commonly accomplished through passwords and additional factors such as one-time tokens. Within an industrial control system environment, it is not uncommon to find no required authentication. Controllers (e.g., PLCs) built before the 2020s almost never support authentication; rather, they simply accept commands to change set points or modify control logic. Combined with indefensible network architectures, this presents a serious concern. In addition, panel-based HMIs are almost never configured to require authentication, meaning that anyone with physical access to the panel-based HMI could disrupt the industrial process. It should be recognized that 1) proper password management, such as defining permission levels, assigning unique passwords to each user, requiring certain password complexity and removing users from the system as necessary, can require significant planning and effort within a production operations environment and 2) that requiring an operator to enter a password (that could be forgotten or must be looked up) when action is immediately required on the plant floor may not be an acceptable constraint. As a result, a lack of authentication requirements, shared credentials, default credentials and vendor backdoors are common security concerns.

Lack of Software Integrity Mechanisms

"Software integrity" refers to the ability to detect changes to software. This is normally accomplished through hash checking and code signing. Controller firmware and control system software, including engineering software from leading vendors, is normally signed. However, control systems engineers and integrators may not verify the hashes or set their computers to run only signed code, thus bypassing an important integrity mechanism. Some panel-based HMIs have the ability to enforce the integrity of the HMI program, but this ability is seldom used. Nearly all controllers do not support code signing of user-generated code (e.g., control logic). That is to say that a controller may accept and run any logic it is told to run without recording or reporting when its logic has changed.

Lack of Physical Access Controls

Physical access controls are factors that limit individuals from physically accessing (touching) control system equipment. While some industrial facilities do have strong physical safety and access control mechanisms, such as guards and gates, it is common for control equipment, such as transmitters and panel-based HMIs, to be physically accessible to anyone in the facility. Control enclosures are frequently left unlocked without video surveillance or security alerts to indicate that the enclosure has been opened.

Lack of Least Privilege

"Least privilege" refers to granting users only the essential permissions they need to complete their expected tasks. While some control system software, including supervisory interfaces, process data historians and human-machine interface design software, contains provisions for least privilege implementations (such as role-based access control or granular permissions control), these capabilities are frequently left unconfigured.

Lack of Software Backups

Backups are intentional and up-to-date copies of software that can be used to quickly restore a system to a trusted or known good state. Code for controllers and HMIs is not often subject to standardized and managed backup policies and procedures. This can be complicated by relying on contracted system integrators or process integrators, or a small (single-person) process operations team whose focus is to get the process running rather than to restore a system after a cybersecurity event.

Lack of a Software Upgrade Path

"Lack of an upgrade path" refers to the obsolescence of currently operational control systems technology. For instance, new hardware that offers encrypted communications protocols is not backward compatible with older hardware. Another example occurs when a vendor declares a product as "end-of-life" even though the product is still used to provide critical services such as

reliable electricity to an important region of the country. If vulnerabilities are discovered in these products, owners cannot merely upgrade the software.

Uncontrolled File Transfer

File transfer plays a prominent role in designing and modifying industrial control systems. Software used to program controllers and operator interfaces is frequently downloaded from vendor websites onto engineering computers. User-generated software files, including control logic and HMI designs, must be transferred to the controller and HMI, respectively, at initial commissioning and to facilitate process changes. This transfer may occur via memory cards, USB connections or network connections. Engineering professionals (who may be contractors) are normally given wide latitude and trust to transfer files appropriately, without additional checks.

Unpatched Software

Once an industrial process has been commissioned, the goal is to keep the process running without interruption. This requirement may restrict the ability to deploy security patches and software updates in a timely manner. The challenge of unpatched software is amplified by 1) unrecognized third-party relationships and 2) a lack of awareness of vulnerabilities and patches.

Unassured Provenance

"Unassured provenance" refers to the general opacity of where and how a product is made and delivered to the customer. This results in the inability of the end owner, the industrial control system owner/operator in this case, to require accountability throughout the supply chain. Unassured provenance differs from unrecognized third-party relationships in that it views the supply chain as a network of influence rather than a chain of discrete companies. Specifically, it may consider elements such as product packaging, the delivery mechanism between suppliers, locations of manufacturing facilities, controlling interests in companies and individual employees involved.

Unrecognized Third-Party Relationships

Complex supplier relationships for industrial control systems hardware and software obfuscates security concerns and inhibits mitigatory action. For example, firmware for a commonly deployed controller may rely on a real-time operating system designed by another vendor. In turn, that vendor may have incorporated an open-source web server. The same firmware may also include a cryptographic library from a separate vendor. These issues extend to design flaws in software development kits provided by leading suppliers and even to hardware design flaws. As a result, the organization that owns or operates the control system may be ignorant of and exposed to significant (and documented-yet-unrecognized) security concerns.

Poor Programming Practice

The programming of industrial control systems can generally be divided into two categories: supplier-provided software (such as controller firmware) and user-generated software (such as control logic). While one may expect that suppliers with larger and longer-lasting software development businesses would have more mature software development practices, continual vulnerability disclosures from leading vendors indicate this is not always the case. Some vendors invest time and attention to identify vulnerabilities and eradicate them from their code base; others conduct no self-review and essentially ignore disclosures from external sources.

On the user-generated side, some asset owners/operators employ code development teams to focus on OT applications. Some of these organizations write code from scratch. Some modify the vendor code or create interfaces to the vendor-provided solutions, such as process data historians. Code quality and security development lifecycle practices for such user-generated code can vary widely. Errors in this software are likely to be limited to the scope of that company, facility or controlled process.

For information specific to controllers and local human-machine interfaces (HMIs), please consult the entry for "Poor Controller Programming Practices."

Network Weaknesses

This class of weaknesses affects communications between network nodes. It includes indefensible network architectures, insecure process control network protocols, unmonitored networks, poorly managed temporary network nodes, poorly controlled network access and unauthorized wireless networks.

Indefensible Network Architectures

A drive for cost savings and improved decision-making has led to extending and applying network services throughout industrial environments. Because industrial operations professionals and IT/networking professionals have historically not understood one another's perspectives, many process control networks were never designed to resist cyberattack. Indefensible architectures may be characterized by reliance on unmanaged network switches, unconfigured or poorly configured managed network switches, physical ports left enabled, limited use of VLANs (virtual local networks), limited use of firewalls and poorly configured firewalls.

Insecure Process Control Network Protocols

Many network communication protocols specifically intended for industrial applications were designed without support for authentication services, that is, without support for logins and maintenance of authenticated sessions. This was due in part to the assumptions that process control networks would not be connected to corporate networks, encryption services would dangerously slow

network communications and consume valuable processor resources, and physical programming switches could be used to disallow remotely programming controllers. The result is that many commonly deployed process control network protocols allow anyone who connects to a controller to reprogram it, replay previously captured traffic and change set points.

This weakness cannot simply be patched. It requires a redesign of 1) controller hardware (more capable processors), 2) controller firmware (new capabilities) and 3) the network protocols. The significance of this weakness should not be ignored. Several leading vendors have introduced new products to address this weakness, but the installed base of legacy products and lack of compatibility between new and old products ensure this weakness will exist for many years.

Unmonitored Networks

Many process control networks are not monitored for anomalous or malicious behavior. When monitoring capabilities are deployed and configured, several important questions must be addressed: How should the alerts be designed? Who will receive the alerts? And what actions should be taken for each alert?

Poorly Managed Temporary Network Nodes

A temporary network node could take various forms, such as a technician's laptop, a remotely connected computer or a handheld device such as a tablet, phone or configurator. These devices may belong to different divisions within an organization or other organizations altogether (such as a contractor), making it difficult to ensure the device is appropriately managed from a security perspective.

Poorly Controlled Network Access

Policies, practices and technologies for admitting, managing and removing nodes to or from a process control network are often poorly defined and may be difficult to enforce. Securely enabling and disabling remote access for remote employees and contractors is of special concern. Poorly controlled network access may result from a lack of expertise or attention by those performing the role of network administration.

Unauthorized Wireless Networks

A wireless network can provide the convenience of remote access and enhanced productivity. It is not uncommon for industrial operations professionals to set up their own remote access points to facilitate remote work. These connections increase the risk of a cybersecurity incident because they provide unmanaged access paths to the network. In addition, adversaries may seek to bring their own network access to industrial processes by embedding cellular or satellite gateways into the supply chain.

Instrumentation and Control Weaknesses

Instrumentation and control weaknesses affect controllers, sensors and actuators. Examples include programmable physical damage, poor controller coding practices and lack of sensor integrity mechanisms.

Programmable Physical Damage

By abusing the way the physical process is designed, programmed and controlled, an attacker may damage equipment, cause defects in products, injure human life and harm the environment. Programmable physical damage is the single most important distinguishing characteristic of industrial cybersecurity from typical cybersecurity.

Poor Controller Programming Practices

In general, neither the engineers nor the technicians tasked to program controllers and human-machine interfaces (HMIs) have been trained in practices that ensure their code is both safe to deploy and difficult to abuse. To help address this deficiency, controller interoperability organization PLCopen published *PLC Code Quality* recommendations in 2016, and in 2020, plc-security.org published the *Top 20 PLC Secure Coding Practices*.

In addition, policies and procedures for designing, deploying, maintaining and updating control logic (covering topics such as code review, code testing, version control, backups, coordination with control room operators, key switch positioning and field accessibility of controllers) seldom exist.

Lack of Sensor/Transmitter Integrity Mechanisms

The output of sensors and transmitters provides input to the controller. Logic in the controller determines what process control actions are taken. Therefore, manipulating the sensor/transmitter signal/data provides an opportunity to disrupt the controlled process. Transmitters and their corresponding I/O cards on common controllers do nothing to ensure the integrity of the signal/data. This may allow for compromises along the supply chain, transmitter calibration/scaling attacks, physical manipulation of the sensors (such as relocating a sensor to change the meaning of its output) and physical man-in-the-middle attacks against the signal wires. As transmitter capabilities continue to evolve, the attack surface for these devices will increase, but so will opportunities to ensure sensor/transmitter signal integrity.

Industrial Cybersecurity Events and Incidents

An industrial cybersecurity event or incident involves undesirable consequences due, at least in part, to poor control system design, control system malfunctions, malicious or unintentional actions, or intentional cyberattacks that affect production operations. Monitoring, detecting, identifying and analyzing industrial cybersecurity events and incidents provides an essential learning experience. This

category includes a list of industrial cybersecurity events and incident cases, and a representative list of analytical concepts that can be applied to them.

Industrial Cybersecurity Event and Incident Cases

This inexhaustive list includes both intentional cyberattacks and non-attack, cyber-physical events across a variety of industries, geographies and impacts: DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, NotPetya, Norsk Hydro ransomware, Oldsmar, Colonial Pipeline, Jeep/Chrysler demonstration attacks, Tam Sauk Hydroelectric Station, DC Metro Red Line and San Bruno.

DHS Aurora

Aurora is the code name given to the first widely recognized public demonstration of a cyberattack that could cause a physical consequence. In an experiment sponsored by the US DHS and carried out at the Idaho National Laboratory in 2007, researchers used a cyberattack to destroy a diesel generator connected to the electric grid.

The cyberattack instructed a protective relay (a device intended to prevent physical damage to grid equipment) to open and close the generator's connection (circuit breaker) to the grid when the generator was out of sync with the electric polarity of the grid. This has been described as analogous to forcing an automobile transmission into reverse while the automobile is traveling forward at 100 kilometers/hour.

Stuxnet

Stuxnet is the first widely recognized and well-documented cyberattack that caused physical damage. The action, allegedly carried out in 2009 by the United States government in collaboration with other countries, disrupted Iran's nuclear weapons program by attacking engineering workstations and PLCs in a uranium enrichment facility in Natanz, Iran. The cyberattack required sophisticated knowledge of the Natanz facility, which must have included engineering diagrams and control logic files. In addition, the Stuxnet code exploited several previously unknown vulnerabilities in Microsoft Windows (spread via USBs), kept a list of infected computers, would only execute its ultimate payload against a precise target and included a self-destruct date.

Ukraine 2015

A coordinated cyberattack allegedly from Russian sources simultaneously struck three regional electricity distribution companies in western Ukraine, shutting off electricity for more than 200,000 people for several hours in December 2015. Attackers gained interactive access to dispatcher workstations and opened circuit breakers by clicking icons on the screen. Attackers then pushed malicious firmware to communication devices and wiped the boot records from dozens of computers to ensure the electric system could not be restored quickly. This is the first publicly recognized power outage due to a cyberattack.

Ukraine 2016

In December 2016, a cyberattack hit a transmission substation in Kyiv, Ukraine, causing a temporary power outage to roughly 200,000 inhabitants in the city. The outage was triggered by malicious software designed to send commands over network communications protocols commonly used for substation automation. Analysts believe that this attack, like the 2015 Ukraine power outage, was intended as a demonstration of Russian capability and dominance over Ukraine.

Triton

Triton is the name given to an attack framework that triggered a safety shutdown of the Petro Rabigh oil refinery in Saudi Arabia. Attackers gained access to the refinery's safety system through lateral connections to the public internet and a controller programming key switch left in the "remote" position. The attack framework incorporated details of a communication protocol used specifically with Triconex safety controllers, which is indicative of significant adversary commitment to manipulate safety systems. Analysis indicates that the intruders inadvertently triggered several shutdowns, which ultimately led to their discovery.

Norsk Hydro Ransomware

Norsk Hydro, headquartered in Norway with facilities in some 50 countries, is one of the world's largest aluminum-producing companies. In 2019, a Hydro employee opened a malicious email that released the Lockergoga ransomware across Hydro networks, ultimately stopping production at 170 plants. Hydro refused to pay the ransom, decided to be open about the attack and turned to its trusted suppliers to help them rebuild their network from backups. The incident demonstrates the effect an attack on a corporate network can have on production operations, shows the importance of falling back to more manual operations if necessary and highlights the importance of maintaining backups. The incident contrasts with the ransomware incident affecting Colonial Pipeline.

NotPetya

NotPetya is a name given to a false ransomware that initially targeted Ukrainian businesses in 2017 and quickly spread across unpatched Windows computers throughout the world. Though NotPetya did not intentionally target cyber-physical systems, it caused significant real-world consequences, including a global disruption of shipping operations at Maersk and numerous other examples. The event highlights the consequences of complex global supply chains, conflicted relationships between companies and the countries where they are headquartered, and reckless behavior by state-nexus threat actors.

Oldsmar

Oldsmar is a 15,000-person municipality in suburban Tampa, Florida. In February 2021, an unknown adversary accessed the city's poorly protected water provisioning system over the TeamViewer

application and increased the set point for lye (used to sanitize water for public consumption) to dangerous levels. A conscientious employee at the treatment facility noticed the change and took steps to limit public impact. Officials claimed that additional pH-level monitoring equipment would have detected the danger before citizens could be harmed. The incident highlights the challenge of securing low-budget water systems, the value of appropriate operator awareness and the importance of holistic system engineering.

Colonial Pipeline

Colonial Pipeline may be the United States' most significant gasoline pipeline, transporting 3 million barrels of fuel per day between Texas refineries and New York. In May 2021, a computer on Colonial's corporate network became infected with ransomware. The company decided to pay a $4.5 million ransom and to intentionally shut down the pipeline while it investigated the extent of the breach and took appropriate remedial actions. The US Federal Motor Carrier Safety Administration declared a regional state of emergency. The pipeline was shut down for five days. While not a cyberattack intentionally targeting industrial control systems, the event highlights a close linkage between IT and OT networks and demonstrates the scope of potential consequences.

Jeep/Chrysler Demonstration Attacks

In 2015, noted cybersecurity researchers Chris Valasek and Charlie Miller shared the results of their investigation into automobile cybersecurity. Focusing on newer (as of 2015) Jeep and Chrysler models, the pair found bugs that allowed them to connect remotely to the car and interact with its transmission and braking systems. Chrysler issued a recall to update the software for affected cars, but this required owners to take them to the dealership. The demonstration attacks illustrate that appealing features of digital connectivity have significant downsides. It shows the necessity of robust security testing rather than merely trusting vendor efforts. It also highlights the options that vendors have for responding to disclosure of security concerns.

Tam Sauk Hydroelectric Station

Tam Sauk is a pumped storage hydroelectric facility located on a Missouri mountaintop. In 2005, the parapet wall collapsed, releasing 4,300 acre-feet of water that scoured a 281-acre path through a Missouri State Park below. The investigation found that the event was precipitated by a poorly anchored sensor conduit, relocation of safety sensors, imprudent controller programming and the lack of a safety spillway. While this incident was not the result of a cyberattack, it demonstrates the importance of appropriate risk management during system design, the dangers of relying on programmable controls for safety systems and the importance of accurate sensor readings.

DC Metro Red Line

The DC Metro is the railway/subway system that serves the Washington, DC metropolitan area. In June 2009, an incorrectly installed trackside sensor allowed a train operating in automated mode to

collide with a train stopped on the track ahead at a speed of 49 miles per hour, killing 8 people and injuring 80 more. While not an intentional cyberattack, the incident demonstrates the dangers of relying on automated systems for critical functions such as human transportation.

San Bruno

San Bruno, a city 10 miles south of San Francisco, California, was the site of a natural gas pipeline explosion in 2010. The incident was precipitated by the replacement of an uninterruptible power supply (UPS) at a pipeline terminal (interconnection point between pipelines). When technicians completed a temporary changeover to the new UPSes, pressure readings became inaccurate, allowing a series of monitoring and regulating valves to open, effectively increasing the downstream pipeline pressure. This, in turn, burst a faulty weld in the 30-inch pipeline directly beneath a residential neighborhood. The resulting explosion destroyed or damaged 108 homes, killed 8 people and injured 58. Flames from the pipeline soared hundreds of feet into the air for an hour before the valves controlling the flow of natural gas to the local area could be manually shut. While not an intentional cyberattack, the incident highlights the significance of accurate diagrams, careful maintenance, clear communication and the potential for disastrous consequences caused by compromised transmitter signals.

Analytical Concepts for Events and Incidents

"Analytical concepts for events and incidents" refers to guiding ideas and vocabulary for understanding and communicating about industrial cybersecurity events and incidents. These concepts include tactics, techniques and procedures (TTPs), targeting, IT versus OT vectors and impacts, and root cause analysis.

Tactics, Techniques and Procedures (TTPs)

TTPs describe ways an adversary approaches its task of planning and carrying out an attack. It begins with how the adversary thinks about the attack and extends to when, where and how the adversary carries out an attack. TTPs are generally patterns that emerge as the result of technological constraints (such as software used), human creativity (such as discovering novel approaches) and organizational realities (such as reporting structures and budgetary constraints). Conceptually, recognizing a TTP enables defenders to take steps that mitigate entire classes of attacks. From an industrial cybersecurity perspective, it is useful to recognize the TTPs that can be leveraged to cause physical impacts. Efforts such as MITRE ATT&CK and ATT&CK for ICS attempt to describe and document known TTPs.

Targeting

"Targeting" refers to structured efforts to plan attacks well in advance of carrying them out. Broadly speaking, a target can be any asset that can be exploited to cause an intended effect. A target can be

an individual, a piece of information or a system. A target can also be an end goal or a means of achieving another goal. Targeting is often an intelligence function carried out by an interdisciplinary team tasked to provide options to a commanding officer. A cyberattack against a significant objective, such as critical infrastructure industrial control systems, may benefit from years of accumulated targeting until the moment is chosen to set an operation in motion. Some efforts by countries to infiltrate critical infrastructure industrial control systems are accurately described as "targeting," "prepositioning" and "intelligence preparation of the battlespace" rather than actual "attacks." While defenders often consider themselves as protectors of operational systems, it is important to recognize that adversaries can operate throughout lifecycles and supply chains.

IT Versus OT Vectors and Impacts

The terms "information technology" (IT) and "operational technology" (OT) are used to differentiate between the fundamental purposes of the underlying technologies. Simply put, IT controls information, OT controls physical operations. A "vector" is an attack pathway, and an "impact" is the outcome of an attack. Defenders should keep in mind that in some attacks that have affected OT systems, adversaries have not actually touched OT systems (Colonial Pipeline and NotPetya are notable examples). Defenders should also recognize that nearly all publicly documented attacks affecting industrial control systems have followed an IT attack vector to reach the OT network (Oldsmar and Triton/Petro Rabigh are notable examples).

Root Cause Analysis

Root cause analysis intends to identify the primary and contributing causes of an event or incident. While establishing root causes can be a complex and painstaking process, it enables defenders to think critically about their susceptibility to a similar event. The designs of the industrial process, control system and process control network can play a role in both preventing and causing events and incidents. It is important to note that the outcomes of root cause analysis may affect legal liability and insurance coverage. Topics in this category include root causes, investigations, internal versus external causes, deliberate versus unintended effects and lessons learned.

Root Causes

A root cause is the fundamental reason an event occurred. Within industrial cybersecurity, these are likely to be combinations of cybersecurity weaknesses and physical system design/engineering.

Investigations

Adequate root cause analysis of industrial cybersecurity events and incidents—that is, one that accurately identifies root causes—requires formal investigation carried out by trained investigators who gather evidence using field techniques, scientific instruments, interviews and available records. In

the United States, bodies such as the National Transportation Safety Board and the National Chemical Safety Board provide government-sponsored investigations in certain industries and cases.

Internal Versus External Causes

One of the most significant items addressed in a root cause analysis is whether the event was the result of actions within a company's direct control (internal) or not (external). This issue is particularly challenging when dealing with complex supply chains, long lifecycles and intentional adversaries.

Deliberate Versus Unintended Effects

Root cause analysis may attempt to discover the degree to which the event was deliberate, reasonably foreseeable or unforeseeable by the initiating party. The conclusion to this question helps determine the severity of a response (punishment) against the perpetrator.

Lessons Learned

One of the most valuable results of any investigation and root cause analysis is the opportunity to avoid similar results in the future. Lessons learned documents and briefings are useful inputs to developing self-evaluations and rich training scenarios. Organizations would also do well to develop lessons learned for near-miss events. Lessons learned provide significant opportunities for interdisciplinary teams from IT and OT organizations to identify ways they can work together to avoid similar situations in the future.

Defensive Techniques

The "defensive techniques" category includes four classes of mitigations that defenders can apply to industrial environments: managerial, network, system and host, and instrumentation and control. Security professionals must recognize and consider the strengths and weaknesses of respective classes and techniques. In addition, they should identify and proficiently employ tools that implement defensive techniques.

Managerial Defensive Techniques

Managerial defensive techniques are key concepts and approaches that guide cybersecurity at an organizational level rather than a technical level. These techniques include an industrial cybersecurity champion, awareness and training for ICS-related personnel, ICS security programs, cybersecurity risk management, ICS security policies, lifecycle management, contingency plans with an ICS focus, incident response plans with an ICS focus, a security operations center for ICS, managed security services, professional ethics and privacy assurance.

Industrial Cybersecurity Champion

The term “industrial cybersecurity champion” refers to an organizational leader who can marshal the resources to address the industrial cybersecurity challenge. It may be a member of the executive leadership team, such as the chief information officer (CIO). This champion may name another individual with industrial cybersecurity expertise and leadership experience to take responsibility for industrial cybersecurity across the entire enterprise.

Awareness and Training For ICS-Related Personnel

Personnel who should receive role-specific training in industrial cybersecurity include plant managers, shift supervisors, electrical engineers, product engineers, process engineers, design engineers, specifying engineers, field technicians, instrumentation technicians, electrical technicians, control room operators and process operators. In larger organizations, such role-specific training should be intentionally managed.

OT/ICS Security Program

An organization’s ICS security program represents its intentional and managed effort to maintain and improve the security posture of its production operations environment. This is not equivalent to simply stating that existing cybersecurity programs and guidance for the corporate network also apply to industrial control systems and the process control network. Consensus guidance for developing an ICS security program can be found in the ISA/IEC 62443 series and NIST Special Publication 800-82.

Cybersecurity Risk Management

Simply put, “cybersecurity risk management” describes the process of balancing the possible damages from IT or OT attacks and failures with the costs of limiting those damages. Within a production operations environment, components of this topic include stakeholders, an integrated system model (asset inventory), an adversary mindset, threat intelligence, vulnerability intelligence and safety versus security.

Stakeholders

Stakeholders are the groups and individuals who will suffer loss in the case of an event or incident. Stakeholders can include the company as an entity, shareholders, employees, suppliers, customers, the region and the country.

Integrated System Model (Asset Inventory)

The foundation to any security effort is an accurate and up-to-date understanding of what one is trying to protect. Some have referred to this as an “asset inventory,” but “integrated system model” is a more compelling and useful term. The system model provides information about process equipment, control system components, computers, networks, configuration details, responsible

parties and relationships that enable the security team to make accurate decisions efficiently. The integrated system model enables the security team to answer questions such as these: How many of a specific type of controller do we have? Where are those controllers located? How important are those controllers to our operations? What firmware version do those controllers use? Who has access to those controllers? Who is responsible for updating the controller firmware? Where is the backup of the logic for those controllers?

Adversary Mindset

Having an adversary mindset is the ability to consider a system from an attacker's point of view. This indispensable security behavior can be learned but is seldom taught. It requires the uncomfortable questioning of assumptions and encourages exploring "the possible" rather than taking comfort in "the probable." In a production operations environment, the adversary mindset must cover elements such as insider threats, supply chain compromise and hardware implants that could achieve real-world, physical consequences.

Threat Intelligence

"Threat intelligence" refers to considering the effect that the evolving, external threat environment may have on the organization's security posture. For example, a rising trend in cyberattack-for-ransom, escalating geopolitical tensions, mergers involving foreign firms and the release of attack tools that focus on control-system-specific protocols may all alter risk. Organizations should assign analysts to monitor the threat environment for relevant changes and recommend appropriate countermeasures. The integrated system model provides a list of relevant terms to monitor. Appropriately organized threat intelligence can form part of an early warning system.

Vulnerability Intelligence

Security researchers constantly identify new vulnerabilities affecting products used in production operations environments. The researchers choose which of these vulnerabilities to disclose and to whom. These discoveries and disclosures, along with associated attack tools, change the risk an organization faces. Some industrial control system vendors share information about vulnerabilities that affect their products and issue software patches to address the vulnerabilities, and some do not. Vulnerability intelligence is an organization's intentional effort to identify known software vulnerabilities in the software it uses. Organizations may monitor a variety of sources, such as security conferences, mail lists and vulnerability databases, to identify newly disclosed vulnerabilities. Organizations use vulnerability intelligence to decide what system components to patch and when to patch them, or what alternate compensating controls to deploy.

Safety Versus Security

Risk management within industrial environments requires adapting two prevailing risk paradigms: safety and security. Engineering professionals working within the context of industrial automation

generally consider that safety protects humans from the effects of physical equipment failures and basic human errors. IT professionals' perspective is that security prevents and mitigates the consequences of unauthorized access to information systems. Because industrial automation connects physical processes to information systems, those developing effective risk management must fully understand and consider both paradigms.

OT/ICS Security Policies

ICS security policies and procedures are intended to ensure that employee actions keep the system within risk tolerance. These policies should clearly identify who the policy applies to, provide the rationale for the policy, clearly describe the procedure for following the policy, explain how compliance is monitored, identify the consequences of noncompliance and describe the process for seeking an exception to the policy. Examples of ICS security policies could include the management of transient devices, contractor/vendor remote access, the process for obtaining software from web-based resources, ICS vulnerability identification, ICS patch identification, ICS patch deployment, acceptable use of social media by engineers and technicians, control logic assurance and control logic backup. These policies cannot simply be copied from similarly named IT security policies; rather, they require special considerations for industrial environments.

Lifecycle Management

Operations environments are the culmination of numerous lifecycles, including product development, process development, facility development and software development. Each lifecycle extends from the initial idea conception through the design, specify and procure, build, operate and maintain, support and dismantle phases. While it is natural to focus primarily on the operate and maintain stages, industrial cybersecurity requires careful observation and documentation at each stage of the lifecycle. Particular attention must be paid to asset management, change management, procurement techniques, security management of legacy devices and the secure software development lifecycle.

Procurement Techniques

Procurement techniques are the applicable security controls applied when control systems asset owners or integrators acquire industrial automation and communication technologies (that is, during the procurement lifecycle phase). While secure procurement techniques themselves may be substantially similar to those used for IT enterprise environments (such as requirements generation, questionnaires, secure development practices, vendor audits and authorized channels), organizations may not have deeply considered security as part of the procurement process for industrial control systems. ISASecure ISA/IEC 62443 Conformance Certifications (https://isasecure.org/) are notable efforts to simplify aspects of secure procurement specifically for industrial environments.

Security Management of Legacy Devices

Legacy devices are devices (such as controllers, HMIs and other equipment) whose hardware may lack the capacity to implement security functionality and/or may no longer be actively supported by the vendor. It is important that security teams positively identify which currently used devices meet this description and adopt techniques that mitigate associated vulnerabilities. Such techniques could include removing network connectivity, implementing restrictive subnets, deploying protocol-aware firewall rules and developing hardware replacement plans.

Secure Software Development Lifecycle

The secure software development lifecycle is a group of recommended practices to ensure software quality from the initial software design through software end-of-life/end-of-support. The topic applies primarily to those developing ICS software, both control systems vendors and control system operators. ISASecure offers the Secure Software Development Lifecycle Assurance Certification for vendors to demonstrate conformance to recommended development practices.

Secure development practices should also apply to PLC programmers, HMI programmers, SCADA programmers and process data historian programmers/users. Those programming these systems may not have had training in software development practices and may not be part of a formalized code development organization with established practices. Topics of code quality, code management, input validation and integrity mechanisms are of special concern.

Contingency Plans with an OT/ICS Focus

Contingency plans are carefully designed instructions for how an organization will respond to a specific situation, including who is responsible for taking each identified action. Organizations that own or operate industrial control systems should prepare contingency plans that enable them to maintain critical production operations in the face of cybersecurity events. For example, a contingency plan to deal with a cyberattack-for-ransom may include a premade decision on whether to pay the ransom, whether to engage law enforcement, whether to tell the public, which systems to isolate from other networks and which processes to operate in a purely manual mode. Successful contingency plans require complete awareness of the control system and network architecture.

Incident Response Plans with an OT/ICS Focus

Incident response plans provide general guidance for responding to a cybersecurity incident. This includes points of contact, communication procedures (including alternate band communications) and guidance regarding preparation, detection, analysis, containment, eradication and recovery. Having an ICS focus means that positive controllability of the industrial process and human safety are paramount considerations during the design of the incident response plan.

Security Operations Center (SOC) for OT/ICS

Security operations involve continuous security team actions in response to ongoing and evolving threats and incidents. The OT/ICS SOC receives incoming security information and internally generated OT/ICS security alerts and assigns them to analysts for action/remediation. Security operations for production operations environments require specialized expertise and experience, as well as tailored procedures. For example, a process may only offer one opportunity per year to upgrade vulnerable controller firmware during a maintenance outage. Some organizations choose to add specialized ICS security operations personnel to the enterprise-wide SOC, while others prefer to create an ICS-specific SOC.

Security Alerts for OT/ICS

Security alerts are formalized technical communications often generated automatically from devices/network hosts (such as engineering computers, operator interfaces and controllers) and network devices (such as process control network anomaly detection) or as the result of combined analysis (such as analysis of process data for security purposes). It is important that each security alert and corresponding course of action be documented and that appropriate stakeholders (including corporate cybersecurity personnel and process operations personnel) be trained in following these courses of action.

Managed Security Services

Many organizations rely on the security expertise of external providers for ongoing detection and various tiers of incident response. These external solutions are known as “managed security services.” While reliance on external expertise may be a reasonable approach, ICS asset owners should consider how the technical capabilities of the network security sensors (i.e., what ICS-specific protocols are covered and to what depth), the types of events that will be identified (e.g., new IP addresses, set point changes, control logic updates, etc.), how events will be communicated to the appropriate parties (i.e., specified recipients of event detection), what actions will be taken and who will take those actions.

Professional Ethics

“Professional ethics” refers to a standard of conduct directly related to one’s work, including tasks performed and relationships with an employer organization, customers and the public. Because societies depend on the reliable operation of industrial processes, industrial cybersecurity professionals must recognize and appreciate that their privileged access to critical systems and details requires the highest levels of technical competence, trustworthiness and responsibility at all times, including continuous concern for their own security and the security of their work.

Privacy Assurance

Privacy assurance addresses the potential that information gathered by a system could be divulged to other systems. While this topic is often covered in a traditional cybersecurity course or program of study, it should not be overlooked for production operations environments when the system can gather information about its users. Examples of such systems include smart meters and automobiles.

Network Defensive Techniques

Network defensive techniques are those safeguards that apply primarily to data in transit and the systems (network devices) that handle data transit. Topics in this category include secure network architecture, network boundaries, network segmentation, physical separation (air gap), management of ports and services, process control network firewalls, process control network anomaly detection, quarantine and observation, analysis of security data, secure remote access, software-defined networking, data diodes, wireless communications analysis, deceptive technologies and security-enhanced ICS network communications and protocols.

Secure Network Architecture

Network architecture is the physical and logical layout of a network. An intentional approach to developing a secure network architecture increases network performance and manageability while diminishing the effects of successful attacks. The secure network architecture advanced in the IEC 62443 standard achieves this by overlaying the Purdue Enterprise Reference Architecture (PERA) levels with zones and conduits. These concepts aid in appropriate network segmentation and placement of security technologies. A well-planned network architecture enables efficient actions during contingency plan activation (such as network isolation or the switch to manual-only operations). The advent of a cloud-connected industrial internet of things (IIoT), Machine-as-a-Service and Bring-Your-Own-Network (BYON), among other changes, necessitates creating and relying on alternate (non-PERA) secure architecture approaches.

Network Boundaries

Network boundaries describe which group or individuals are responsible for specific network assets. Establishing formalized network boundaries—particularly between IT and OT—is key to a securely managed network infrastructure. Several approaches exist. One is to have a key demarcation point, such as a firewall, separating the enterprise IT from the OT network, where each group is solely responsible for administering and maintaining the devices on their side of the demarcation. Another is to have the IT group administer and maintain all the network equipment, but not the hosts on the OT network. A third is to have the IT group administer all the network equipment and all the traditional hosts, but not the HMIs and PLCs on the OT network. Open conversations, trust, respect for expertise and acceptance of differing points of view are key to effectively determining network boundaries.

Network Segmentation

"Network segmentation" refers to partitioning networks into manageable chunks. This increases network efficiency and security. Segmentation is achieved by reviewing the network topology and security architecture, ensuring the use of adequate managed switches, configuring appropriate VLANs and supporting network services, and deploying appropriately configured firewalls.

Physical Separation (Air Gap)

An air gap is an absence of network connectivity between two networks, theoretically meaning that the corporate network cannot talk to the process control network. Under this paradigm, any sharing of data across the gap is accomplished with removable media, such as a USB flash drive. While the concept of an air gap is compelling, it has often been cited as a reason not to worry about managing the security of the process control network. In such cases, a virus that spreads via a USB drive may face few if any constraints once it is on the OT network. In addition, experience has shown that individuals claiming that an air gap exists are often ignorant of the actual connectivity. One common example is a dual-homed host, such as a process data historian, that has IP addresses on both the corporate network and process control network. Alternate approaches to "air gap" include data diodes, a dual-firewall DMZ and an intertied airlock.

Management of Ports and Services

The term "ports and services" refers to the network services and corresponding TCP/UDP ports utilized by those services. Conventional wisdom holds that the more ports and services that are available on a network, the more opportunities exists for an attack. Hence, good practice requires industrial cybersecurity professionals to understand the ports and services that are truly necessary for process operation and control, while disallowing all others. A simple example may be the decision to block access to a web server on a PLC that provides only simplified diagnostic information. Many engineers and technicians have never considered the process control network from this point of view.

Process Control Network Firewalls

Some network security tools and devices can examine packets for specific aspects of ICS network protocols. One example is Modbus function codes: a firewall capable of parsing the Modbus protocol could disallow Modbus write commands (recognized by function code) unless they came from the local HMI or the SCADA HMI (recognized by address). In this way, other devices on the network would not be allowed to take actions, such as changing a set point.

Process Control Network Anomaly Detection

Process control networks are typically static in comparison to enterprise networks, where devices are constantly being added and removed. This more static nature can increase the ease and effectiveness of establishing a baseline and then recognizing deviations from the baseline. Taking advantage of this

opportunity may require network configuration and deployment of baselining tools. Creating appropriate alerts for deviations/anomalies, determining what action to take on each alert and assigning the actions to the proper personnel requires the expertise and collaboration of process engineers, field technicians and process operators.

Quarantine and Observation

Isolating and testing equipment suspected of malicious behavior is an important defensive technique. Examples of quarantine and observation used in operations environments include security review as part of a site acceptance test, the staged/limited roll-out of a new technology and the isolation of a potentially misbehaving component as part of a troubleshooting process.

Analysis of Security Data with Process Control Data

Process control data, such as data already being collected by a process historian for analyzing and improving a process, can be used to identify potentially malicious behavior. For example, deviations of set points or process variables from normal ranges can be used to trigger additional investigation and incident response.

Secure Remote Access

Industrial control systems are frequently configured to allow remote access to specialized employees, contractors and vendors. Such access can improve process efficiency, provide timely troubleshooting and decrease costs and travel time. Careful policies and intentional technology choices, such as VPNs (virtual private networks), multifactor authentication, time-based controls, process control network firewalls and the use of carefully monitored jump boxes, can help protect these connections against malicious use.

Software-Defined Networking

When thoughtfully used in industrial environments, software-defined networks can provide rapid configurability that speeds deploying network-available services and stymies adversarial reconnaissance. However, the complexity of such solutions may exceed the expertise normally available to operate the process control network infrastructure.

Data Diodes

A data diode is a device that physically enforces one-way (unidirectional) network communication. Diodes accomplish this by using light (rather than electricity) as a one-way communication mechanism. To deal with TCP protocols, the diode solution spoofs back the expected response to the source address. Process control networks may use these devices to allow communications out of the process control network (to the corporate network), but not into the ICS network. An advantage of these devices is that one-way communication is physically ensured. In comparison, a stateful firewall may fail, become overwhelmed or be disabled. Stateful firewalls may also be vulnerable to attacks

from properly established connections. Data diodes may be used in any communications network, but they have been specifically marketed for use in production operations environments.

Wireless Communications Analysis

Wireless communications are increasingly common in production operations environments. These can range from low-power wireless networks, such as Wireless HART at Purdue Levels 0 and 1; Wi-Fi at Purdue Levels 1 and 2; and cellular, licensed spectrum and even satellite at Purdue Levels 2 and 3 and higher. The advent of Machine-as-a-Service and BYON adds additional complexity to wireless network management. Careful detection and analysis of wireless communication helps ensure clear and accurate transmission and the absence of malicious networks and nodes.

Deceptive Technologies

Deceiving would-be adversaries is a well-known and documented defensive technique. The drawback is that convincing deception schemes can require a significant investment of time and resources. Because some industrial environments represent high-payoff targets, these techniques may justify the effort. Approaches include

- honeypots/nets,
- selective direction to honeynets (such as based on country of origin),
- the release of malware into simulated process control networks,
- the creation and operation of sock-puppets (such as fake profiles of nonexisting control engineers and technicians on social media) to see who tries to contact them and
- the intentional release of inaccurate details about the control system/network.

Security-Enhanced ICS Network Communications and Protocols

Since about 2020, control system vendors (and some visionary open-source developers) have offered process control network communications protocols with security capabilities, such as user authentication and encryption. This development addresses a major vulnerability in industrial environments. However, the unavoidable lack of backward compatibility means that the security benefits of these tools will not be fully realized for many years.

System and Host Defensive Techniques

The system and host category of defensive techniques deals with solutions deployed on or pertaining to individual devices/network hosts (such as engineering computers, operator interfaces and controllers) in an operations environment. Such techniques include device hardening, device monitoring, software/firmware updates, software integrity mechanisms, passwords and credential management, physical security and hardware reviews.

Device Hardening

"Device hardening" refers to changing the device configuration to make it more challenging for an adversary to abuse. Hardening can involve disabling unnecessary ports and services, implementing appropriate group policy settings (for Windows-based devices), disabling/removing unnecessary physical ports and setting passwords. While these approaches clearly apply to laptops and workstations found in operations environments, they may also apply to controllers and panel-based HMIs, depending on the make and model. Some controllers offer "code protection" that disallows attempts to obtain the code from the PLC. Some PLCs offer "code binding," which only allows the code to run when associated with a specific PLC or memory card. Intelligent transmitters may have security switches or jumpers that can be set to prevent configuration changes. Transmitters may also be set to require passwords for configuration changes.

Device Monitoring

Device monitoring, also known as "endpoint protection," normally involves deploying a software agent onto the host operating system that monitors various aspects of the host for suspicious or malicious activity. Antivirus software and application allowlisting are common device monitoring solutions. Device monitoring solutions apply more readily to traditional computers used in industrial environments, such as application servers, supervisory interfaces, engineering workstations and technician laptops, than they do to panel-based operator interfaces (e.g., HMIs), controllers, configurators and transmitters.

Device monitoring solutions such as antivirus software could have a potentially negative impact on computers within a process control network if they consume too many resources (CPU time). Asset owners should check with their control systems vendor to know what device monitoring solutions have been tested and approved for use.

Software/Firmware Updates

Updating software and firmware to the latest versions is an important way to remediate known weaknesses within vendor-provided control system software. The capability of control system vendors to appropriately receive vulnerability disclosures, validate researcher findings, create an update for all affected products and communicate with customers/users varies greatly.

Control system asset owners should assign someone to monitor software updates affecting all control system-related products they use, keeping in mind that release notes may or may not clearly describe the security implications of an update.

The need to continually operate an industrial process may require carefully considering which updates should be deployed and when to deploy them. While control system vendors should carefully test each update prior to release, asset owners may also wish to test an update prior to full-scale

deployment. Some industrial processes/facilities undergo regular maintenance downtime, which may provide an ideal opportunity to deploy updates.

Formalized and managed processes for software/firmware updates should be clearly included in an organization's change management policies.

Software Integrity Mechanisms

Software integrity mechanisms prevent unauthorized changes to software and log attempts to make such changes. These mechanisms can provide technology enforcement of change management policies. Software integrity solutions have historically applied to application servers, supervisory interfaces, engineering workstations and technician laptops rather than controllers. Some panel-based HMIs provide built-in integrity check mechanisms.

For controllers, it is important to ensure the integrity of the firmware (provided by the vendor) and the control logic (provided by the controller programmer). Various solutions have been proposed and created to detect changes, some by relying on network traffic, some on file comparisons and some on PLC functionality.

Passwords and Credential Management

Passwords are the most used authentication mechanism and, despite significant constraints for their use in operations environments, can provide an important layer of protection. Control system vendors, integrators, asset owners and maintenance firms should adopt authentication strategies that apply to all users during the system lifecycle, protect the system, minimize management effort and prioritize productivity.

Physical Security

Physical security aims to limit hands-on, in-person access to industrial control systems components. While physical security must be considered at each stage of the lifecycle, operational control systems must be sure to consider remote facilities/locations, communications media (including cable runs) and control enclosures. Solutions are available to aid in physically disabling unused physical communication ports.

Hardware Reviews

Hardware reviews, including hardware reverse engineering, may detect supply chain compromise and the presence of unspecified functionality. For example, a hardware review could reveal hidden control functionality within important infrastructure, such as large power transformers, that a nation-state adversary could use to its advantage in the case of future conflict. While purchasers of engineered systems have historically required factory acceptance testing (FAT) and site acceptance testing (SAT) to determine whether a system conforms to engineering specifications (including performance), a

detailed security review of all electronic subsystems may transcend the purchaser's expertise and, thus, may require coordination with government resources.

Instrumentation and Control Defensive Techniques

Instrumentation and control defensive techniques deal primarily with the assets at Levels 0 and 1 of the Purdue Enterprise Reference Architecture, that is, process equipment, sensors, transmitters, actuators and controllers. Instrumentation and control defensive techniques include positive control; cyber-informed engineering; consequence-driven, cyber-informed engineering; process hazards-based approaches; consequence red-teaming; special consideration of safety functions; cyber-physical fail-safes; controller security; analysis of process data for security and sensor/transmitter integrity assurance.

Positive Control

"Positive control" refers to the assurance that 1) sensor readings/process variables used for both automated control and supervisory decision-making provide accurate and timely representations of real-world conditions, 2) control logic appropriately considers all relevant process variables and 3) actuators faithfully implement the dictated control decisions (controller outputs or supervisory commands). Sensor/transmitter integrity assurance mechanisms, controller security and diverse principles of operation may be used to achieve positive control.

Cyber-Informed Engineering (CIE)

Cyber-informed engineering is an approach for applying engineering concepts to address cybersecurity concerns and applying cybersecurity concepts within engineering functions. While retrofitting existing systems is within its scope, the focus is on the original design of the process and its controls. Hence, technicians and engineers must consider both the physics of the process and the possibility of intentional cyberattacks.

Consequence-Driven Cyber-Informed Engineering (CCE)

Consequence-driven Cyber-informed Engineering is a specific implementation of cyber-informed engineering. It provides a repeatable methodology to help system owners and operators of high-value national security targets identify high-priority critical functions, describe the steps an adversary might take to accomplish its objectives against those functions, understand adversary capability to target and attack those functions, identify cyber-physical fail-safes and establish early warning systems.

Process Hazards-Based Approaches

Process hazards analysis is a long-standing technique to identify potential failures of controlled processes. This analysis relies on a model of the system (such as piping and instrument diagrams) and

expert input to identify and mitigate process hazards. Process hazards-based approaches extend this process to include cybersecurity events.

Consequence Red-Teaming

Red-teaming is adopting an adversarial mindset and applying adversarial techniques. Consequence red-teaming involves considering (using a variety of structured and semi-structured approaches) the consequences that an adversary would hope to intentionally achieve by a cyberattack against an industrial control system.

Special Consideration of Safety Functions

Safety instrumented functions and systems are intended to protect the physical welfare of facility personnel and the public at large. As such, safety functions and systems represent high-value targets and merit special cybersecurity consideration.

Cyber-Physical Fail-Safes (Engineered Controls)

A cyber-physical fail-safe is an engineered mitigation that prevents a physical impact or consequence that would otherwise result from a cyberattack. Examples of cyber-physical fail-safes include centrifugal switches, buckling pins and mechanically operated pressure relief valves.

Controller Security

“Controller security” refers to a collection of practices intended to increase the security of the controller and its programming. These include a programming key switch, controller hardening, controller logic change monitoring, controller logic inspection, secure controller programming, controller self-diagnostics and process state awareness.

Controller Hardening

“Controller hardening” refers to altering the configuration options on the controller in a way that minimizes the attack surface. Examples include disabling unused ports and services and enabling security settings, such as secure protocol versions, where technologically feasible.

Controller Logic Change Monitoring

Because an adversary could cause significant (physical) consequences by changing the control logic of an industrial process, the security group should receive a notification each time logic is pushed to the controller. A copy of the entire control logic project file from the engineering workstation should be maintained for backup and inspection (including comparison).

Controller Logic Inspection

This topic involves reviewing control logic 1) to determine whether the logic follows recommended programming practices, 2) for errors that could result in unintentional consequences, 3) for ways in

which the logic could be abused to cause physical consequences and 4) to determine whether the control logic is intentionally malicious. The inspection should include checking assumptions and initial values.

Secure Controller Programming

A variety of controller programming practices make it more likely that the program will operate as intended and resist cyberattacks. These practices include

- control data validation,
- operational logic centralized in the controller (versus HMI) and
- controller memory allocated by function.

Control Data Validation

This topic refers to the practice of comparing data sent to the controller from various data sources with 1) reasonable values and 2) historical values. Values outside the set limits should not allow output manipulation. Control data validation topics include controller data sources, comparison with reasonable values and comparison with historic values.

- **Controller Data Sources**

  Data that influences how an industrial process behaves may come from a variety of sources, such as a sensor/transmitter, another controller, a local HMI, a supervisory interface, an engineering computer, another device on the network or an internal memory transfer. An adversary with a presence at any of these locations could attack the industrial process by sending manipulated/dangerous data, such as process variables, set points, or counter and timer values.

- **Comparison with Reasonable Values**

  "Comparison with reasonable values" refers to the technique of a controller (e.g., PLC) determining whether a value provided by a controller data source is reasonable before acting on that value. One method for determining reasonability is to identify the physically possible engineering limits. If a value exceeds those limits (such as a negative value on a counter), the PLC should not take control action based on the value. Instead, the controller may enter a conservative control state and/or generate an OT/ICS security alert.

- **Comparison with Historic Values**

  This topic refers to the technique of a controller (e.g., PLC) determining whether a value provided by a control data source is within historical norms before acting on that value. This requires the controller to keep a historical record of values received. If a value exceeds those limits, the PLC does not take control action on the value. Instead, the controller may enter a conservative control state and/or generate an OT/ICS security alert.

Operational Logic Centralized in the Controller (Versus HMI)

Because the controller ultimately makes control decisions, centralizing data processing for control use within the controller—as opposed to the HMI—ensures accuracy and efficiency while also reducing the attack surface. For the same reasons, the controller must ultimately enforce control data validation even if acceptable input ranges are also specified on the HMI.

Controller Memory Allocated by Function

The individual programming the controller may designate specific memory areas (e.g., blocks of register addresses) to particular functions, such as reading, writing, validating writes and performing calculations. This practice enhances memory organization and allows firewalls/network monitoring devices to discern the intent of a write command with greater granularity. Rules of this type are possible because ICS network protocols, such as Modbus, include a field that specifies which memory address is being accessed (see the "Process Control Network Firewalls" entry).

These enhanced firewall/network monitoring rules could be used to discern when an asset normally expected to write to controller memory (such as a SCADA HMI or engineering workstation) attempts to modify the memory area used to validate write commands. Unauthorized changes to validation techniques would be of greatest concern (see the "Secure Controller Programming" entry for additional discussion on validating write commands). It is important to note that properly implementing these firewall/network monitoring rules would require the individual who programs the controller to help the individual writing the firewall/IDS rule to understand which memory areas are allocated to each function.

Controller Self-Diagnostics

This topic refers to relying on the functionality built into the controller (e.g., PLC) to alert appropriate parties, such as process operators, technicians, engineers and security analysts, of suspicious conditions within the controller. This functionality includes configuration change monitoring, controller performance monitoring, controller error monitoring and controller alerts.

Controller Configuration Change Monitoring

Some controller models allow controller configuration changes to be used as tags. These tags can be used in the controller logic, displayed on the HMI or passed elsewhere. Where possible, this functionality should be employed to draw attention to potentially malicious activity.

Controller Performance Monitoring

Controllers may allow controller data, such as CPU usage, CPU temperature, CPU shutdown and CPU restart, to be available to users. Unexpected events or deviations from the baseline may indicate malicious activity on the controller. This performance data can be monitored at the local HMI or sent elsewhere for monitoring and alerting.

Controller Error Monitoring

Functionality built into the controller may allow error logging and reporting. For example, mathematical errors, such as divide by zero, counter overflow and negative counter, can be logged and reported as potential indicators of malicious activity.

Controller Alerts

Controller configuration changes, performance, errors and unexpected conditions can be communicated to the pertinent stakeholders through the local operator interface (HMI), supervisory control interface (via alarms), process data historians and the security operations center for OT/ICS as an OT/ICS security alert.

Process State Awareness

Programmable controllers may track process states (lists of simultaneous physical conditions) via Boolean (on-off, true-or-false) values. Tracking the process state enables several safety and cybersecurity risk management techniques, which include preventing simultaneous assertion of exclusive system states, defining a safe process restart state, enabling conservative control, making appropriate stakeholders aware of the process state and trapping the manipulation of process state variables.

Prevention of Simultaneous Assertion of Exclusive Process States

Certain process system states should never occur at the same time. For example, a control valve should not be entirely closed while the pump that moves liquid through the valve is on, as this may lead to damaged components or destroy the pump. The same principle also applies to near-simultaneous state changes, such as rapidly toggling a system on and off. The fact that two states were never intended to occur simultaneously or near simultaneously does not mean that the controller necessarily enforces the exclusivity. This lack of enforcement may enable attacks to achieve physical consequences. Where possible, cyber-physical fail-safes should prevent simultaneously asserting exclusive system states. Where this is not possible, control logic should intentionally disallow these state violations.

Define Safe Process Start State

The controller should check the process state on each start-up (including each controller restart) to ensure that control actions do not cause a safety concern. Such a check will require the process engineer and control logic programmer to carefully consider possible states during the design of the process control system. The check may slow the process start or restart procedure.

Conservative Control

Conservative control is a reliability and safety approach intended to force a controlled process that is operating in a potentially dangerous or “under attack” state into safer operations. This may include

stepping back from engineering limits, operating for reduced output, increasing cycle times and relying on analog and manual controls rather than digital controls.

User Awareness of Process State

User awareness of the process state is an intentional component of control system safety design. It ensures that technicians, process operators, control room operators, engineers and plant managers can 1) clearly recognize a dangerous process state (via alarms and alerts) and 2) recognize their responsibilities for a given state.

Manipulation of Process State Variable Trapping

Attackers may attempt to cause damage or to distract operators by manipulating the process state variable to cause a false alarm or suppress a legitimate alarm. Control logic can be written to detect such manipulation by monitoring the process state variable in addition to the list of conditions. This trap would send a security alert when triggered. It must be recognized, however, that the trap could be bypassed if an attacker removes it by loading new control logic.

Analysis of Process Data for Security Purposes (Historian/SIEM)

"Analysis of process data for security purposes" refers to analyzing process data for anomalous, potentially malicious behavior. This analysis occurs within a process data historian or security information and event management (SIEM) tool and may involve comparing process variables and set points to historic or reasonable ranges. The result of such analysis (a security alert) is detective rather than preventive in nature.

Sensor/Transmitter Integrity Assurance Mechanisms

Because sensor/transmitter values drive the output commands made by the controllers, ensuring their accuracy and integrity is a key element of industrial cybersecurity. Attacks against sensors/transmitters could include the presence of hardware and software implants, intentional miscalibration, rescaling and man-in-the-middle attacks against communications. The use of increasingly capable/intelligent electronics is expanding the available attack surface for sensors/transmitters. Specific mechanisms to assure sensor/transmitter integrity include emanations monitoring of transmitters, independent sensing/transmission and backhaul, and analysis of process data for security purposes (historian/SIEM).

Emanations Monitoring of Transmitters

Because transmitter values determine controller output, transmitters may represent high-value targets to certain adversaries. Transmitter behavior may be baselined by deploying radio devices to monitor their electromagnetic emanations. This technique, commonly called "RF (radio frequency) fingerprinting," can trigger a security alert to appropriate stakeholders when anomalies are detected.

Independent Sensing/Transmission and Backhaul

Independent sensing/transmission and backhaul is the use of multiple and diverse sensors/transmitters and communication channels (backhaul) for important process variables. Data from the various sensors/transmitters may be sent to the controller, a process data historian or a SIEM tool. Using independent communications channels may also help resist network-based attacks. Significant discrepancies between the values provided by multiple sensors will trigger a security alert. When designing independent sensing and backhaul, it is important to fully consider and document procedures for responding to alerts and for determining which readings are the most accurate. Analog and non-networked digital readouts may be particularly useful as ground truth, independent sensors, given their resistance to cyberattack.

Further Information

The dates and editions for standards and other references in this chapter are current as of publication. The reader is encouraged to check for later revisions or editions.

American Petroleum Institute

Standard 1164, *Pipeline Control Systems Cybersecurity*

American Water Works Association (AWWA)

Water Sector Cybersecurity Risk Management Guidance

Cisco-Rockwell Automation

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

European Committee for Electrotechnical Standardization (CENELEC)

EN 50128:2011, *Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems*

European Union (EU)

Good Practice Guide for CERTs in the Area of Industrial Control Systems

Protecting Industrial Control Systems: Recommendations for Europe and Member States

International Electrotechnical Commission (IEC)

IEC 60880:2006, *Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions*

IEC 61131-3:2025, *Programmable Controllers – Part 3: Programming Languages*

IEC 61508:2010 CMV, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

IEC 61511 Series, *Functional Safety – Safety Instrumented Systems for the Process Industry Sector*

IEC 61850 Series, *Communication Networks and Systems for Power Utility Automation*

IEC 62304:2006+AMD1:2015 CSV, *Medical Device Software – Software Life Cycle Processes*

IEC 62443 Series, *Industrial Communication Networks – Network and System Security*

IEC 62645 Ed. 2.0 b:2019, *Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements*

International Organization for Standardization (ISO)

ISO 11898-1:2015, *Road Vehicles – Controller Area Network (CAN)*

ISO 26262-6:2018, *Road Vehicles – Functional Safety – Part 6: Product Development at the Software Level*

ISO/IEC 27001:2022, *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*

ISO/IEC 27002:2022, *Information Security, Cybersecurity and Privacy Protection – Information Security Controls*

ISO/IEC 27019:2017, *Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry*

ISO/SAE 21434:2021, *Road Vehicles – Cybersecurity Engineering*

International Society of Automation

ANSI/ISA-101.01-2015, *Human Machine Interfaces for Process Automation Systems*

ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*

ANSI/ISA-61511 Series, *Functional Safety*

ISA-TR84.00.09-2024, *Cybersecurity Related to the Functional Safety Lifecycle*

ISA/IEC 62443 Series, *Security for Industrial Automation and Control Systems*

ISA-100.11a, *Wireless Systems for Industrial Automation: Process Control and Related Applications*

ISA-TR101.02-2019, *HMI Usability and Performance*

North American Electric Reliability Corporation

Critical Infrastructure Protection (CIP) standards

PLCopen

PLC Code Quality

US Government

“Executive Order No. 13636: Improving Critical Infrastructure Cybersecurity"

“Executive Order No. 13920: Securing the United States Bulk-Power System” (suspended)

“Presidential Policy Directive 21: Critical Infrastructure Security and Resilience”

US National Institute of Standards and Technology

NIST Special Publication 800-82, *Guide to Operational Technology Security*

US Nuclear Regulatory Commission (NRC)

10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks*

NRC Regulatory Guide 5.71, *Cybersecurity Programs for Nuclear Facilities*

Appendix A

BEST PAPER AWARD

What Does An OT Security Professional Need To Know?

Sean McBride
Informatics Research Institute
Idaho State University
Sean.McBride@isu.edu
0000-0002-4234-7358

Glenn Merrell
Freelance Consulting
Controls@FreelanceConsulting.com
0009-0003-3794-1728

Abstract—Industrial Cybersecurity is an emerging interdisciplinary field of study and practice. This paper presents the results of research and collaboration to create a data-supported and consensus-based curricular guidance document describing the knowledge needed of professionals in the field.

Keywords—*control system security, curriculum development*

I. INTRODUCTION

Industrial cybersecurity is an emerging interdisciplinary field, composed primarily of industrial automation and cybersecurity, but including elements of many other fields. It is the result of the global trend of technology advancement and digitization, wherein computers increasingly interact with and influence the physical world.

Since about the early 2000s, industrial cybersecurity has been shaped by 1) the discovery and disclosure of software vulnerabilities affecting industrial control systems, 2) unintentional safety events precipitated by flawed control systems design or maintenance, and 3) intentional cyberattacks motivated by enthusiasts, criminals, and geopolitical actors [1-3].

The trend of increasing automated control of the physical world creates a national and global security imperative to ensure these intelligent systems do not cause physical damage (or disaster) through either accident or intentional abuse.

This paper presents the results of a collaboration among government (U.S. Department of Energy Office of Cybersecurity, Energy Security and Emergency Response, and the Idaho National Laboratory), academia (Idaho State University), and industry (the International Society of Automation) to establish an appropriate educational foundation for creating a new class of engineering and technology professional – capable of moving seamlessly among previously disparate domains.

The paper is organized in typical academic fashion including a review of relevant literature, discussion of research method, presentation of results, and proposal of future work.

II. LITERATURE REVIEW

For this effort, the researchers were particularly interested in existing official guidance for creating cybersecurity professionals – with a focus on industrial automation and operational technology.

The researchers began by reviewing education and training guidance from nine organizations, including Accreditation Board of Engineering and Technology (ABET) [4], European Union Agency for Network and Information Security (ENISA) [5] , Global Information Assurance Certification (GIAC) [6], International Society of Automation (ISA) & Department of Labor [7], Task Force on Cybersecurity Education [8], National Institute of Standards and Technology [9], National Security Agency [10], Pacific Northwest National Laboratory [11], the Singapore Cyber Security Agency [12], and INL [13].

As the researchers examined the documents, they created a list of criteria that one would expect from a truly foundational curricular guidance document. The researchers then compared the criteria across the existing documents. A more-detailed treatment of the criteria can be found at [14]. The results of the comparison are summarized in Table I, where Y means yes, P means partial, N means no, and U means unknown.

TABLE I. Comparison of Curricular Guidance Efforts

Criteria	Curricular Guidance Efforts/Documents										Total Ys
	ABET	**ENISA**	**GIAC**	**ISA**	**JTF**	**NIST**	**NSA**	**PNNL**	**SF**	**INL**	
1. Addresses Industrial cybersecurity	N	Y	Y	Y	N	N	Y	Y	Y	Y	8
2. Clearly differentiates industrial	N	P	P	Y	N	N	P	N	N	Y	2
3. Consensus-based	Y	Y	Y	U	Y	N	N	Y	U	N	5
4. Qualified participants	Y	Y	Y	U	Y	U	U	Y	U	U	6
5. Publicly available	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	11
6. Includes knowledge	P	Y	Y	Y	Y	Y	Y	Y	Y	N	8
7. Justifies knowledge	N	N	N	N	N	N	N	N	N	N	0
8. Evidence of empirical validation	N	N	N	N	N	N	N	N	N	P	0
TOTAL Ys	3/8	5/8	5/8	4/8	4/8	2/8	3/8	5/8	3/8	3/8	

Perhaps the most important finding is that all the documents exhibited two complete deficiencies: 1) None of the documents "justified knowledge". That is, none of them provided a reason each term was included – its relevance to the field. 2) None of them provided "evidence of empirical validation". That is, none of them provided a detailed description of how their guidance was created, or the qualifications of their creators/contributors. They provided results, but only limited discussion of methods, and no raw data or data analysis.

In conclusion, a review of literature found a concerning lack of appropriately detailed and validated guidance among the bodies expected to advise the formal preparation of professionals to secure critical cyber-physical systems.

III. METHODOLOGY

Starting in Jan 2019, authors of [14-15] used the nominal group technique to engage a group of 14 professionals from the Idaho National Laboratory in creating an initial list of knowledge topics that would not normally be covered in a traditional cybersecurity course or program of study. The nominal group technique encourages broad perspectives by relying on anonymous, written responses rather than potentially political and emotional implications of verbal discussion/debate. The 14 professionals came from a variety of educational and professional backgrounds, totaling 31 years in industrial cybersecurity, 32 years in non-industrial cybersecurity, and 88 years in industrial operations.

The results of that work, ultimately published as "Industrial Cybersecurity Workforce Development: A Manager's Guide" by the Idaho National Laboratory [16], included two lists – one dealing with "industrial knowledge" and another dealing with "industrial cybersecurity". "Control systems knowledge" consisted of 45 items distributed across five categories. "Industrial cybersecurity knowledge" included 33 items spread across four categories.

As the researchers reviewed those lists, they recognized that while comprehensive curricular guidance would require program level learning objectives, course objectives, course sequence, schedule of topics, proposed learning activities, and evidence-based assessment methodologies, *knowledge* would be the most essential and straightforward component of consensus-based curricular guidance.

Recognizing that input from just 14 professionals was not sufficient to claim a consensus, the researchers determined to use the combined list from [16] as a strawman about which to elicit further expert insight.

Between November 2021 and March 2022, and with the assistance of the International Society of Automation (ISA) Global Cybersecurity Alliance (which advertised via an email to its members), the researchers administered a survey to professionals with interest and/or experience in industrial cybersecurity.

The survey included 363 possible inputs (some inputs were only displayed if the respondent answered in a certain way) divided into three sections:

1) Respondent Background – 19 possible inputs
2) Foundational Industrial Control Systems Knowledge – 205 possible inputs
3) Industrial Cybersecurity Knowledge – 139 possible inputs

As seen in Table II, the survey had 170 total respondents, 96 of which (56%) answered at least one question in survey Section 2. This group of "Contributors" spent an average of 49 minutes on the survey.

TABLE II. Respondents

Respondents	Number
Total	170
Contributors (answered at least one question in Section II)	96
Section II Finishers	70
Section III Finishers	65
Writers (provided textual input)	58

IV. RESULTS AND ANALYSIS

A. Analysis of Respondent Background

The survey asked up to 32 questions (depending on responses) to ascertain the education background, professional certifications, and professional experience of respondents.

Of the 96 Contributors, most had bachelor's degrees; engineering disciplines, including in control systems, accounted for 34 degrees, while computer science and cybersecurity accounted for 20 (see Tables III and IV). Of the 29 contributor respondents who had a Professional Engineer (PE) license, 23 reported a specialization in control systems (see Tables V and VI).

Contributor respondents claimed industry experience across a variety of industry sectors – predominantly in petrochemical and electric power (see Table VII) – and reported 1,085 cumulative years working for control system asset owners and control system integrators (see Table VIII). This experience was complemented by a cumulative total of 959 years working in cybersecurity, with more than ¾ of this time dedicated to control systems rather than IT (see Table IX). More than half of the contributor respondents held a professional cybersecurity certification, and one third held a certification specialized in industrial cybersecurity (See Tables X and XI).

TABLE III. Contributor Degree Levels

Highest Degree	Count
Bachelor	47
Master	33
Associate	6
Doctorate	6
High School Diploma/GED	4
Total	**96**

TABLE IV. Respondents by Degree Groupings

Degree Group	Count of Degree Grouping	Percent
Electrical Engineering	14	14.58%
Control Systems	10	10.42%
Cybersecurity	10	10.42%
Other Engineering	10	10.42%
Computer Science	10	10.42%
Electronics	9	9.38%
Business	6	6.25%
Information Systems	5	5.21%
Unspecified	5	5.21%
High School	4	4.17%
Mechanical Engineering	4	4.17%
Arts/Science	3	3.13%
Security Studies	3	3.13%
Information Technology	2	2.08%
Education	1	1.04%
Total	**96**	**100.00%**

TABLE V. Respondent Licensure

Licensed Professional Engineer?	Count
No	67
Yes	29
Total	**96**

TABLE VI. Respondent Licensure Specialty

PE Specialty (multiple allowed)	Count	Percent
Control Systems	23	79.31%
Electrical	10	34.48%
Industrial	6	20.69%
Other	5	17.24%
Mechanical	4	13.79%
Chemical	3	10.34%
Civil	1	3.45%

TABLE VII. Respondent Industry Focus

Industry (multiple allowed)	Total	Percent
Aerospace	15	16%
Power	42	44%
Chemical & Petroleum	48	50%
Mining & Metals	21	22%
Construction & Design	30	31%
Food & Pharmaceuticals	25	26%
Water & Wastewater	25	26%
Manufacturing	29	30%

TABLE VIII. Respondent Organizational Roles

Organizational Role	Cumulative Years
Asset Owner	543
ICS Integration Provider	532
ICS Supplier	200
ICS Maintenance Service Provider	161

TABLE IX. Respondent Cybersecurity Certifications

Cybersecurity Experience Category	Count
Control Systems	55
IT	41
Total	**595**

TABLE X. Respondent Cybersecurity Certifications

Cybersecurity Certification	Count
With	55
Without	41

TABLE XI. Respondent Industrial Cybersecurity Certifications

Industrial Cybersecurity Certification	Count
With	34
Without	62

The key take-away from the analysis of respondent background is that the survey reached an appropriately qualified group of professionals to address the important topic of industrial cybersecurity.

B. Analysis of Responses Relative to Strawman

Sections 2 and 3 of the survey, dealing with foundational control system knowledge and industrial cybersecurity knowledge, respectively, asked respondents to rank each category and topic provided in the strawman for relevance, and then choose whether to: keep as-is, change name, or remove entirely. If respondents chose “change name” or “remove entirely” they were prompted to make an alternate suggestion or justify their desire to remove the category or

topic in writing. All response data and associated analysis can be found at [16].

1) Analysis of Responses to Survey Section 2 – Foundational Control Systems Knowledge

a) Relevance

Respondents were asked to rank each term on a scale of 1 (irrelevant) to 10 (extremely relevant) for the field of industrial cybersecurity. Table XII shows the Kendall's Tau sub b correlation for "Years in Industrial Automation / Control Systems" with each category within the strawman.

TABLE XII. Correlation Among Categories and Respondent Experience in Industrial Automation

Term	KTb	Sig	N
Industrial operations ecosystem	*0.169	0.036	87
Instrumentation and control	0.106	0.197	87
Equipment under control	0.131	0.103	87
Industrial communications	-0.111	0.184	87
Safety	*0.196	0.019	87

This data shows that those with more experience in industrial automation tend to think that Safety and broad knowledge of the Industrial operations ecosystem are, respectively, more relevant than those with less experience. Correlations for both of these categories meet a p-value of .05 for statistical significance.

The researchers also ran the Kendall's Tau sub b correlation analysis using "Years in cybersecurity" as the comparative variable – as seen in Table XIII.

TABLE XIII. Correlation Among Categories and Respondent Experience in Cybersecurity

Term	KTb	Sig	N
Industrial operations ecosystem	*0.227	0.005	87
Instrumentation and control	0.141	0.091	87
Equipment under control	*0.188	0.020	87
Industrial communications	0.058	0.492	87
Safety	0.137	0.107	87

Those with most experience in cybersecurity considered the Industrial operations ecosystem and Equipment under control as highly relevant. Both of these categories meet a p-value of .05 for statistical significance.

When comparing the two correlation analyses, the most salient findings are that 1) those with more experience in industrial automation or more experience in cybersecurity tend to emphasize the relevance of the industrial operations ecosystem; and 2) those with more experience in industrial automation emphasize the relevance of safety

b) Keep, Change, or Remove

It is clear from a review of survey results that the respondents generally agreed with the foundational control systems categories and topics provided in the strawman. Table XIV shows the responses for "keep as is", "change", and "remove topic" for each category and topic.

TABLE XIV. Respondent Choice Among Keep, Change, Remove by Topic

Cat.	Topic	Count	Keep as-is	Change title	Remove
Instrumentation and Control		93	94%	5%	1%
	Programmable control devices	71	99%	1%	0%
	Control system software	71	99%	1%	0%
	Alarms	71	97%	3%	0%
	Operator interfaces	71	97%	3%	0%
	Control paradigms	71	96%	4%	0%
	Data acquisition	71	96%	3%	1%
	Supervisory control	71	96%	1%	3%
	Programming methods	70	96%	4%	0%
	Process variables	71	94%	1%	4%
	Process data historian	71	94%	1%	4%
	Sensing elements	71	93%	7%	0%
	Control devices	71	93%	6%	1%
	Engineering laptop/workstation	71	92%	6%	3%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Industrial Communications		93	90%	8%	2%
	Industrial Communication Protocols	70	99%	1%	0%
	Reference Architectures	70	97%	1%	1%
	Transmitter Signals	70	94%	1%	4%
	Fieldbuses	63	95%	0%	5%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Safety		93	86%	10%	4%
	Safety Instrumented Functions	68	97%	1%	1%
	Electrical Safety	68	97%	0%	3%
	Safety/Hazards Assessment	68	96%	0%	4%
	Common Failure Modes for Equipment Under Control	68	96%	1%	3%
	Safe Work Procedures	68	93%	1%	6%
	Lock-out Tag-out	68	91%	1%	7%
	Personal Protective Equipment	68	90%	0%	10%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Valves	70	96%	3%	1%
	Motors	70	94%	3%	3%
	Pumps	70	94%	3%	3%
	Variable frequency drives	70	93%	3%	4%
	Generators	69	94%	1%	4%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Relays	70	91%	7%	1%
	Breakers	70	91%	3%	6%
	Transformers	69	91%	1%	7%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Valves	70	96%	3%	1%
	Motors	70	94%	3%	3%
	Pumps	70	94%	3%	3%
	Variable frequency drives	70	93%	3%	4%
	Generators	69	94%	1%	4%
	Relays	70	91%	7%	1%
	Breakers	70	91%	3%	6%
	Transformers	69	91%	1%	7%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Industrial Operations Ecosystem		92	82%	16%	2%
	Industry Sectors	77	97%	3%	0%
	Professional Roles and Responsibilities	77	96%	4%	0%
	Organizational Roles	77	96%	0%	4%
	Process Types	78	95%	3%	3%
	Industrial Lifecycles	77	96%	3%	1%
	Facilities	77	95%	5%	0%
	Engineering Diagrams	76	93%	5%	1%

Over 90% of respondents chose "keep as is" for all but three items: Industrial operations ecosystem (82%), Equipment under control (85%) and Safety (86%).

Notwithstanding this general indication of acceptability, the researchers wanted to consider each suggestion for improvement on its own merits. Seventy-six respondents provided a total 342 suggestions for improvement. As some responses included multiple parts, this gave an atomized quantity of 461 responses.

One respondent offered 47 suggestions. Forty-five respondents offered just one or two suggestions. In addition, four responses from the Industrial Cybersecurity Knowledge Section were moved into the Foundational Industrial Control Systems Knowledge Section, for a grand total of 465.

Of the 465 responses provided, 278 (60%) were incorporated into the guidance. A summary of the final dispositions into the mutually exclusive dispositions appears in Table XV.

TABLE XV. Final Dispositions of Respondents Input by Category

Final disposition	**Count**
Directly accepted	91
Indirectly accepted	158
Note made in guidance document	29
Referred to cybersecurity section	53
Insufficient detail provided	53
No change	81
Total	**465**

c) Survey Responses for Which No Change Was Made

Table XVI shows that the 81 suggestions for which no change was made were place in four explanatory categories:

TABLE XVI. Categories Within Disposition "No Change Made"

Category for "No change"	**Count**
Already included	7
Just commentary	6
Out of scope	22
Otherwise not persuasive	46
Total	**81**

The most common suggestion for which no change was made dealt with networking technologies. While such suggestions were generally out of scope (because the scope was limited to topics not covered in a traditional IT, computer science, or cybersecurity program), these suggestions highlight the importance of including traditional networking topics to adequately prepare industrial cybersecurity professionals in other forms of curricular guidance (such as a model curriculum).

Ultimately, the researchers chose to not change the term that received the highest score (16%) for "change title": Industrial Operations Ecosystem. To address the expressed concerns, the researchers chose to add four subcategories: Business Context, Geopolitical Context, Professional Context, and Industry Context.

d) Description of Changes to Survey Section 2

The most significant changes resulting from the review of each written response were: 1) alterations to category titles; and 2) the addition of subcategories and subtopics.

Changes to category titles are shown in the Table XVII

TABLE XVII. Strawman Categories VS. Final Categories

Strawman Categories	**Final Categories**
Industrial Operations Ecosystem	Industrial Operations Ecosystem
Instrumentation and Control	Instrumentation & Control
Equipment Under Control	Process Equipment
Industrial Communications	Industrial Networking & Communications
Safety	Process Safety & Reliability

2) Analysis of Responses to Survey Section 3 – Industrial Cybersecurity Knowledge

a) Relevance

Respondents were asked to rank each term on a scale of 1 (irrelevant) to 10 (extremely relevant) for the field of industrial cybersecurity. Table XVIII shows the Kendall Tau sub b (KTb) correlation coefficients for "Years in Industrial Automation / Control Systems" with each category in the strawman.

TABLE XVIII. Correlation Among Terms and Respondent Experience in Industrial Automation

Strawman Category	**KTb**	**Sig**	**N**
Regulation and guidance	0.172	0.073	65
Common weaknesses	0.025	0.797	65

Strawman Category	KTb	Sig	N
Events and incidents	0.152	0.114	65
Defensive technologies and approaches	0.169	0.091	65

This correlation analysis indicates weak positive correlation between experience in industrial automation and category titles, but this correlation is not statistically significant.

The researchers also ran the correlation analysis using "Years in cybersecurity" as the independent variable – as seen in Table XIX below.

TABLE XIX. Correlation Among Terms and Respondent Experience in Cybersecurity

Strawman Category	KTb	Sig	N
Regulation and guidance	0.099	0.291	68
Common weaknesses	0.148	0.119	68
Events and incidents	0.157	0.095	68
Defensive technologies and approaches	0.008	0.938	68

This correlation analysis shows weak positive correlations between respondent years in cybersecurity and each of the category titles. None of these correlations was statistically significant.

b) Keep, Change, or Remove

It is clear from a review of survey results that the respondents generally agreed with the industrial cybersecurity categories and topics provided in the strawman. Table XX shows the responses for "keep as is", "change", and "remove topic" for each category and topic.

TABLE XX. Response for Count, Keep As-is, Change Title, Remove for Section 3 – Industrial Cybersecurity Knowledge

Cat.	Topic	Count	Keep as-is	Change title	Remove
Regulation and Guidance		68	99%	1%	0%
	ISA/IEC 624432	67	97%	3%	0%
	Presidential Orders	67	91%	1%	7%
	NIST SP 800-82r2	67	97%	3%	0%
	NERC CIP	67	97%	3%	0%
	EU Cybersecurity Act	67	96%	1%	3%
Common Weaknesses		68	96%	4%	0%
	Indefensible Network Architectures	65	100%	0%	0%
	Unauthenticated Protocols	66	97%	3%	0%
	Unpatched Systems	66	100%	0%	0%
	Lack of Training	64	94%	5%	2%
	Transient Devices	66	95%	5%	0%
	Third Party Access	66	95%	5%	0%
	Supply Chain	65	92%	5%	3%
Events and Incidents		68	97%	3%	0%
	DHS Aurora	64	95%	3%	2%
	Stuxnet	64	95%	3%	2%
	Ukraine 2015	64	95%	3%	2%
	Ukraine 2016	64	95%	3%	2%
	Triton	64	95%	3%	2%
	Taum Sauk Dam	64	95%	3%	2%
	DC Metro Red line	64	95%	3%	2%
	San Bruno	64	95%	3%	2%
	Colonial Pipeline	64	95%	3%	2%
Defensive Technologies and Approaches		68	97%	3%	0%
	Industrial Network Firewalls	65	98%	2%	0%
	Data Diodes	65	94%	2%	5%
	Process Data Analysis	65	95%	3%	2%

Cat.	Topic	Count	Keep as-is	Change title	Remove
	ICS Network Monitoring	65	100%	0%	0%
	Cyber informed engineering	64	100%	0%	0%
	Process hazards assessment based	64	98%	0%	2%
	Cyber-physical failsafes	64	95%	0%	5%
	Awareness and Training for ICS personnel	64	100%	0%	0%

Over 90% of respondents chose "keep as is" for all items. Notwithstanding this general indication of acceptability, the researchers wanted to consider each suggestion for improvement on its own merits.

Fifty respondents provided a total 154 responses. As 58 responses included multiple parts, this gave an atomized quantity of 213 responses. In addition, 53 responses from the Industrial Control System Knowledge Section were moved into the Industrial Cybersecurity Knowledge Section, bringing the total to 266 responses. One respondent offered 29 suggestions. Thirty-three respondents offered just one or two suggestions.

Of the 266 atomized responses provided, 192 (72%) were incorporated into the guidance. A summary of the final dispositions into the mutually exclusive categories is shown in Table XXI.

TABLE XXI. Final Disposition of Suggestions Provided in Survey Section 3 – Industrial Control Systems Knowledge by Category

Final disposition	**Count**
Directly accepted	59
Indirectly accepted	106
Note made in guidance document	28
Final disposition	**Count**
Insufficient detail provided	8
No change	61
Referred to foundational ICS knowledge section	4
Total	**266**

c) Survey Responses for Which No Change Was Made

The 54 suggestions for which no change was made were classified into the four categories displayed in Table XXII.

TABLE XXII. Counts of Responses for Which No Change was Made

Category for "No change"	**Count**
Already included	17
Just commentary	2
Out of scope	13
Otherwise not persuasive	22
Total	**54**

d) Description of Changes to Survey Section 3

The most significant change was the addition of subtopics to provide improved order and organization. In addition, the researchers compared the list of Common Weaknesses to the list of Defensive Techniques to ensure reasonable alignment. The guidance grew from 33 total items in the strawman to 129 items based on respondent suggestions. When incorporating the changes suggested, the researchers added an additional 76 items, bringing the total to 205. These changes enhance the utility of the guidance by providing increased clarity and specificity.

A comparison between the strawman and the final list of categories and topics can be found at [17].

C. Creation of Category and Topic Descriptions

Once the list of categories and topics had been identified, the researchers set out to define and describe each of the key terms in a way that highlighted its importance to industrial cybersecurity. The researchers produced the 122-page "Curricular Guidance: Industrial Cybersecurity Knowledge" document [18].

The document is intended to provide authors, instructors, education administrators, and students with a foundational point of reference for knowledge items common in the field of industrial/OT cybersecurity. As such, it serves as an informative – though not necessarily definitive – hierarchical glossary.

The document is organized in two main sections: Foundational Industrial Control Systems Knowledge, and Industrial Cybersecurity Knowledge. Each section is further decomposed into categories, topics, and subtopics to reach a level of reasonable granularity.

While some topic names are identical to those found in traditional cybersecurity contexts, it describes the unique or

special considerations of those topics for operations environments.

The document makes extensive use of cross-referenced hyperlinks to facilitate navigation. A link at the bottom of each page quickly takes the reader back to the table of contents to navigate within the hierarchical structure.

V. CONCLUSIONS, LIMITATIONS, AND FUTURE WORK

A. Conclusions

This work set out to address two key deficiencies among existing curricular guidance for industrial cybersecurity: a) lack of a clear description of what was meant by the term "OT" or "industrial" cybersecurity; and b) lack of description of how the guidance was created.

To accomplish these objectives researchers implemented a multi-stage research methodology that 1) ensured broad participation from qualified professionals by recording respondent background, 2) administered the survey to a reasonably sized group, 3) performed a statistical analysis of respondents' perception of relevance, 4) considered every written suggestion for improvement, 5) incorporated nearly 2/3 of suggestions for improvement, 6) made the raw data and analysis freely available, and 7) crafted descriptions of each term to differentiate "industrial" or "OT" cybersecurity from traditional cybersecurity.

B. Limitations

The work presented herein is subject to limitations of both methodology and results.

1) Methodology Limitations

From a methodological point of view, it is possible that 65 survey finishers are not sufficient to claim consensus. The term "consensus" implies a group capable of raising meaningful objections has expressed satisfaction with the result. While the methodology employed showed that a vast majority of respondents (between 82% and 100%) chose "keep as is" for each term in the strawman, and the researchers incorporated each suggestion they considered possible, the researchers did not circle back to the survey respondents with the resulting guidance for another round of review.

To deal with these methodological limitations, the researchers suggest the creation of a web-based input form whereby interested individuals could provide ongoing suggestions for improvement, and that those suggestions receive consideration when the knowledge-based curricular guidance is updated from time to time.

In addition, during review of respondent comments, the researchers realized it was necessary to add some 292 unrequested topics, representing more than half (292 of 560) of the final term count. These additions were not subject to the same level of review as the initial strawman. However, a review of the actual dispositions shows that these terms clearly fall under/within the strawman categories or respondent-provided suggestions, and are consistent with the stated purposes of this research because they clearly describe what is meant by "OT" or "industrial" cybersecurity.

It should also be recognized that while the methodology did achieve its stated objective of clearly describing "OT" and "industrial" cybersecurity, it did not explore the question of what would be an optimal level of depth. Coverage may be too deep in some cases and not deep enough in others.

2) Results Limitations

From a content point of view, it is apparent that as the field of industrial cybersecurity evolves, the knowledge document will require periodic updates to address new developments. This is a struggle faced by any curricular guidance. Second, because the knowledge document intended to cover knowledge that is different from traditional cybersecurity, additional work will need to describe required knowledge that is the same as traditional cybersecurity. Finally, because the field is by nature interdisciplinary, topics such as industry sectors, process equipment, and communications protocols will require some discretion for appropriate implementation by instructors.

C. Future Work

From the perspective of the researchers, this work should be followed-up with the development of a model curriculum (or curricula). Such a curriculum should describe one way the knowledge described in this work can guide the development of engineering (engineers) or engineering technology professionals (technicians) who design, build, operate, maintain, dismantle, and defend operational technology environments.

A model curriculum should include IT, networking, and computer science topics not covered in the knowledge document. It should describe program level learning objectives, course objectives, course sequence, schedule of topics, proposed learning activities, and advance evidence-based assessment methodologies. Ideally learning activities would incorporate cognitive and behavioral instructional modalities that reflect both descriptive (what is currently done) and prescriptive (what should be done) practices.

REFERENCES

[1] Miller, A., Erickson, K. (2004). Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity. https://apps.dtic.mil/sti/tr/pdf/ADA447337.pdf, accessed August 2024.

[2] National Transportation Safety Board, Pipeline Accident Report Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire San Bruno, California September 9, 2010. https://www.ntsb.gov/investigations/accidentreports/reports/par1101.pdf, accessed August 2024.

[3] Falliere, N., O Muchu, L, Chien, E. "W32.Stuxnet Dossier". https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en, accessed August 2024.

[4] ABET. "Criteria for Accrediting Computing Programs , 2023-2024". (no date). https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/, accessed September 2024.

[5] European Union Agency for Network and Information Security, (2014). "Certification of Cyber Security skills of ICS/SCADA professionals". https://www.enisa.europa.eu/sites/default/files/publications/Certification%20Schemes%20at%20European%20level%20for%20Cyber%20Security%20Skills%20of%20ICS%20SCADA.pdf, accessed April 2025.

[6] Harp D., Gregory-Brown B. (2016.) The GICSP: A Keystone Certification. https://www.sans.org/reading-room/whitepapers/training/gicsp-keystone-certification-37232, accessed September 2024.

[7] Department of Labour (2009). Automation Industry Competency Model V. 4. (updated 2018). https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=automation, accessed September 2024.

[8] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E., Kaza, S., Levy, Y., Parrish, A. (2017). Cybersecurity Curricula 2017:Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, accessed September 2024.

[9] Peterson, R., Santos, D., Smith, M., Wetzel, K., Witte, G. (2020) "Workforce Framework for Cybersecurity (NICE Framework)". Accessed September 2024.

[10] Information Assurance Directorate (2020). "2020 Knowledge Units". https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf, accessed September 2024.

[11] O'Niel, L., Conway, T., Tobey, D., Grietzer, F., Dalton, A., Pusey, P. (2015). SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioral Interview Guidelines by Job Roles. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24140.pdf, retrieved September 2024.

[12] Cybersecurity Agency of Singapore "Operational Technology (OT) Cybersecurity Competency Framework" (2021). https://www.csa.gov.sg/resources/publications/operational-technology-cybersecurity-competency-framework--otccf-, accessed April 2025.

[13] Lampe, B., et al. Idaho National Laboratory "Cyber Informed Engineering (CIE) Curriculum Guide" https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_141694.pdf, accessed January 2025.

[14] McBride, S. (2021) Foundations of Industrial Cybersecurity Education and Training. https://opal.latrobe.edu.au/articles/thesis/Foundations_of_Industrial_Cybersecurity_Education_and_Training/19119443?file=33966695, accessed August 2024.

[15] S. McBride, C. Schou, J. Slay (2023). "Curricular Guidance to Bridge the IT-OT Cybersecurity Gap" in "Practical Guide to Security and Privacy in Cyber-Physical Systems" edited by P. Sharma and S. Goel. https://doi.org/10.1142/9789811273551_0007

[16] S. McBride (2020). "Building an Industrial Cybersecurity Workforce: A Manager's Guide". https://inl.gov/content/uploads/2023/07/ICS_Workforce-ManagersGuide2021.pdf, accessed April 2025

[17] "Supporting Docs" zip file. https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/Supporting%20docs.zip, accessed August 2024.

[18] McBride, S. (2024). "Curricular Guidance: Industrial Cybersecurity Guidance", https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/Industrial%20Cybersecurity%20Knowledge%20FINAL.pdf, accessed September 2024.