Idaho State University

ISA GLOBAL CYBERSECURITY ALLIANCE

INL Idaho National Laboratory

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

CURRICULUM GUIDANCE: Industrial Cybersecurity Knowledge

April 2024

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

Acknowledgments

This document is the culmination of a years-long collaborative effort among the Idaho National Laboratory, the US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER), Idaho State University, 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.

Special recognition is due to Glenn Merrell of Freelance Consulting, Carl Schuett of QED Secure, Heidi Cooke of ISA, and Sami ElMurr of Hunter Strategy who selflessly volunteered to help analyze the survey results.

Appreciation is due to the following interns from the Idaho National Laboratory who helped author entries in the Process Equipment Category: 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.

Idaho State University is an NSA-designated Center of Academic Excellence in Cyber Defense.

Executive Summary

The Challenge

As the wave of digitization subsumes industrial automation smart devices and networks proliferate both taking advantage of and helping to form complex global supply chains; threats multiply, requiring adequate preparation of professionals who can securely design, build, operate, maintain, and dismantle critical cyber-physical systems, and defend such systems from cyber events and incidents throughout that life cycle.

Historically, professionals who work within industrial automation environments receive vastly different formal education, report up different chains of command, and are subject to different performance incentives than those who secure information systems, creating a sharp cultural and knowledge gap separating disciplines that are now washing together [1].

This document, "Industrial Cybersecurity Knowledge" is intended to provide course authors, instructors, education administrators, and students with a clear description of what "industrial" cybersecurity includes that distinguishes it from traditional cybersecurity programs. As such, it serves as an informative – though not necessarily definitive – glossary.

The document is organized around the analogy of a building with three components: 1) an environment, 2) a foundation, and 3) a superstructure:

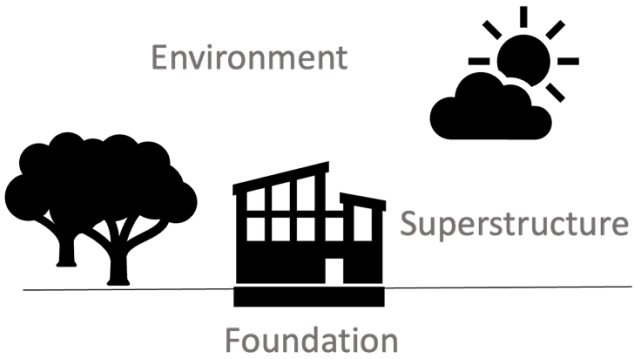


Figure 1: Industrial Cybersecurity Knowledge Model

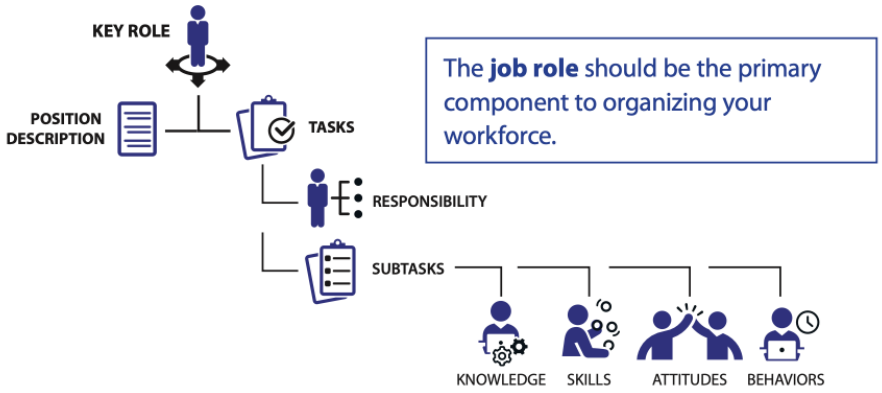
- The *Industrial Operations Environment* describes the contexts (business, geopolitical, professional, and industry) within which industrial control systems and industrial cybersecurity exist.
- The *Industrial Control Systems Foundation* describes the elements (instrumentation & control, process equipment, industrial networking & communication, and process safety & reliability) that compose an industrial control system.
- The *Industrial Cybersecurity Superstructure* describes the elements (guidance & regulation, common weaknesses, events & incidents, and defensive techniques) that most immediately and intuitively pertain to assuring an industrial control system.

Each component is organized into categories, topics, and subtopics to reach a level of reasonable granularity -- up to six levels deep.

The document makes extensive use of cross-referenced hyperlinks to facilitate navigation. Capitalized terms with a description can be clicked to move to that entry. A link at the bottom of each page returns the reader to the table of contents.

Workforce Description and Development Model

To properly use the document, it is important to recognize that knowledge is only one part of a comprehensive workforce description and development model such as the one shown below:



Knowledge provides a baseline that applies across a variety of archetype roles, including engineers, technicians, analysts, managers, and researchers. As such, it provides an indispensable component of an education or training program; but it must be complemented with educational content covering skills, attitudes, and behaviors aligned to tasks and team relationships for selected job roles.

The document aims to guide and foster curricula development rather than require specific learning objectives. Identified stakeholder needs, which are subject to certain variability, should be the driving force behind each covered topic, learning activity, module, course, and program of study.

What This Document Does Not Include

It is important to recognize that the document approaches the challenge from the perspective of "what is missing from traditional cybersecurity curricula?" As a result, the document does not cover all the knowledge that must be included within an industrial cybersecurity curriculum – just those parts that which make industrial cybersecurity different. For example, host and server operating systems and networking fundamentals should be taught, but are not specifically listed in this document. They are outside the document's defined scope.

While some topic names are identical to those found in traditional cybersecurity contexts, this document describes the unique or special considerations of those topics for industrial and operational technology (OT) environments.

As the field of industrial cybersecurity evolves, this document will require periodic updates, and the reader should be aware of this constraint.

Why the Document Was Created

A review of cybersecurity workforce development literature and cybersecurity curricular guidance documents from leading English language sources found 1) A lack of "industrial" or "OT" specific cybersecurity guidance; 2) No clear description of what is meant by "industrial" or "OT" cybersecurity; 3) No documentation describing what methodology was used to create the guidance [2].

The "Curricular Guidance: Industrial Cybersecurity Knowledge" document presents the results of a collaborative multi-year research effort conducted by Idaho State University (ISU), Idaho National Laboratory (INL), and the International Society of Automation (ISA) to address those needs.

Details about the methodology used to create this document can be found on the ISAGCA website (.zip file will download automatically).

References

[1] Sean McBride, Corey Schou, and Jill Slay "Curricular Guidance to Bridge the IT–OT Cybersecurity Gap" in "A Practical Guide on Security and Privacy in Cyber-Physical Systems" (2023). https://doi.org/10.1142/9789811273551_0007

[2] "Building and Industrial Cybersecurity Workforce: A Managers' Guide" (2021). Idaho National Laboratory and Idaho State University. https://inl.gov/content/uploads/2023/07/ICS_Workforce-ManagersGuide2021.pdf

[3] Ida Ngambeki, Sean McBride, and Jill Slay "Knowledge Gaps in Curricular Guidance for ICS Security" (2022). Journal of the Colloquium for Information Systems Security Education. https://doi.org/10.53735/cisse.v9i1.149

Table of Contents

Industrial Operations Environment

"Industrial operations" are generally considered to be the large-scale production of goods – extending from the extraction of natural resources to the creation of consumable products. "Industrial operations ecosystem" refers to the various contexts or stakeholder perspectives involved in industrial operations. These include: Business Context, Geopolitical Context, Professional Context, and Industry Context.

Business Context

"Business context" represents 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 but are not limited to Production Operations, IT vs OT, Organizational Roles, Supply Chain, Supply & Demand, Capital Budget & Expense, Cost Center vs Profit Center, Human Capital, Business Continuity, Regulation, Business Risk.

Production Operations

Production operations refers to the physical work of making the product or producing the good. Businesses sometimes call this the "production arm" or "operations arm" of the organization. It includes the production Facilities, processes, Equipment, Industrial Control Systems, and personnel who physically make the product. This differs from other organizational functions such as strategy, marketing, sales, human resources, or even engineering.

IT vs OT

IT means "information technology" and refers to the computers and network equipment that process data. OT means "operational technology" and refers to the computers and network equipment, along with the instrumentation and control systems, that support not just data, but the physical, real world being controlled via automated means. The term "OT" is often used synonymously or near synonymously with "Industrial Control Systems (ICS)," "industrial automation," and "process control systems," terms which pre-date "OT." In strict interpretation, "OT" encompasses non-industrial cyber-physical systems and processes, and therefore may be a preferable term in some circumstances.

In the late 1990s and early 2000s businesses began connecting IT networks with operational technology, precipitating significant challenges between the organizational divisions that operate these technologies. It is important to recognize that IT and OT professionals have disparate educational preparation, reporting chains, and performance priorities. Organizations that successfully manage cybersecurity risk will intentionally address the disparity between the two groups.

Organizational Roles

"Organizational roles" refers to the types of organizations that deal with industrial control systems. These are Vendors, Integrators, Owner/Operators, and Maintenance Providers. The industrial cybersecurity Guidance found in ISA/IEC 62443 calls these "principal roles."

Industrial Control Systems Vendor

An ICS vendor manufactures and markets industrial control systems software and/or hardware solutions. While there are thousands of firms serving this market, leading vendors include but are not limited to Rockwell Automation, Yokogawa, Emerson Process Management, Honeywell Process Solutions, Siemens Industrial Automation, Schneider Electric, and Mitsubishi Electric Automation.

Industrial Control Systems Integrator

An ICS integrator deploys and integrates the Control System Components within the controlled process. This is a common function among engineering firms.

Industrial Control Systems Owner/Operator

An ICS owner/operator is the business or organization that owns or operates the production process and associated equipment.

Industrial Control Systems Maintenance Provider

An ICS maintenance provider specializes in maintaining an Industrial Process and its associated control system. 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 but are not limited to Black & Veatch and Veolia.

Supply Chain

Supply chain refers to the process whereby product outputs are themselves inputs into additional products. Many market goods are the combination of dozens or even hundreds of previously manufactured products. Complex global supply chains are essential to operating even the smallest businesses. Products with 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 as it does to physical manufactured goods.

Supply & Demand

Supply and demand are core business and economic concepts that describe how markets operate. Supply means the quantity of a good or service that is available, and demand means 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. Industrial operations that automate mass production processes and keep them running will maximize profits.

Capital Budget & Expense

The term “capital budget and expense” describes 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 ideally contributes to revenue generation (making money). This category is generally distinct from ongoing operations and maintenance budget and expense categories.

Cost Center vs Profit Center

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

Human Capital

Human capital refers to the employees of an organization. Competitive businesses and organizations recognize that competent employees drive success, and thus 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 cyber attacks. Successful businesses plan to address key elements of these potentialities before they occur, thus ensuring business continuity.

Regulation

Regulation is the legal and procedural framework that punishes organizations (usually by fine) for failure to meet minimum acceptable 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 think about events that could harm the business, such as its finances, reputation, employees, the public, and the environment. Managers then think about ways to reduce, transfer, or accept the risk. Conversations about Process Safety & Reliability and cybersecurity often focus on loss reduction.

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 – which are a significant source of wealth. Components within the geopolitical context include, but are not limited to: Natural Resources, National Borders, Technological Development, Conflicts, Military, State-Owned Enterprises, Demographics, State Security Sources, Capabilities, and Geopolitical Risk.

Natural Resources

Natural resources include the biological and geological components on earth from which products useful to humanity are derived. Examples include, but are not limited to 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 boarders 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

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 to maximize output for given inputs within a nation-state. Modern manufacturing processes are the result of technological development. Countries with greater technological development may outcompete countries of 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 to businesses, communities, and governments. Critical infrastructures are frequently designed, built, operated, and maintained by private/non-government organizations. Hence, while governments have great interest in preserving these infrastructures, they may only have a supporting role in their protection. Some governments classify critical infrastructure in terms of Industry Sectors – or groupings of similar functions. While this is useful for administrative purposes, infrastructure sectors are highly dependent on one another.

Conflicts

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

Military

Military refers to the organized armed forces of a nation-state. Militaries both rely on and operate a variety of critical industrial control systems. Militaries may also designate units to plan and attack critical facilities and processes using a variety of techniques, including cyber attacks.

State-Owned Enterprises

State-owned enterprises are for-profit businesses that are heavily influenced, if not entirely controlled by a nation-state. National governments around the world use businesses to achieve their interests and policies in 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) in case of Conflicts.

Demographics

Demographics describe the general characteristics of individuals, including citizens and non-citizens, 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 to maintain 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 action (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 nation-state conflict, the term "capabilities" refers to the people, procedures, and tools that a Military or State Security Service can bring to bear against another country. This may include deception, cyber attack, sabotage, or direct military action against

identified targets. Understanding the capabilities possessed by a nation-state is an important input to a clear understanding of risk.

Geopolitical risk

Geopolitical risk is the estimation of the causes, timing, and consequences of adverse events in foreign countries, including conflicts among nation-states. Customer 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 describes the viewpoint of the individuals involved in industrial operations. It consists of Professional Roles & Responsibilities and Workplace Safety.

Professional Roles & Responsibilities

Archetype professional roles involved in industrial operations include but are not limited to: Engineer, Technician, Process Operator, Control Room Operator, Shift Supervisor, Plant Manager, and the Chief Operating Officer. Each of these roles requires specialized knowledge to perform key tasks. Ethics and Operational Security are significant concerns for every role.

Engineer

An engineer is a professional who designs and specifies products, processes, and systems of many types. Engineers make calculations based on requirements, create drawings, and specify bills of material. With a focus on Design, engineers are less involved in the Operation and Maintenance of the systems they design. Most engineers receive formal preparation in a four-year engineering degree. Engineers frequently specialize in a field, such as chemical, mechanical, civil, or electrical. 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. Some organizations only allow engineers to program the control system, including the Operator Interfaces (both local and supervisory) and Controllers (PLCs), while others allow Technicians to do so.

Technician

A technician is a professional with specialized knowledge of and ability to use an engineering technology. Within an industrial operations environment, “instrument technician” and “maintenance technician” are common job titles. Instrument technicians specialize in selecting, configuring, calibrating, and deploying Sensors, Transmitters, and Controllers of various types. 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. Some organizations allow technicians to program Controllers.

Process Operator

A process operator is a professional who helps run 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 formalized professional preparation, but rather gain significant knowledge regarding the process they operate via 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 human machine interface. Becoming a control room operator frequently requires years of experience as a process operator. Some Industry Sectors require control room operators to obtain specialized training and certification.

Shift Supervisor

Many industrial operations run continuously for longer than a typical working day – with many running 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 represents a particularly critical or potentially vulnerable moment because a new team is stepping into an existing or emergent situation they may not fully understand.

Plant Manager

The plant manager is accountable for what happens with the plant. All plant employees ultimately report to the plant manager. The plant manager is frequently evaluated on their ability to maximize the productivity and efficiency of the plant – that is, to achieve expected product quality with high production and low costs. Plant managers are very knowledgeable about all aspects of a plant. They interface between the technical professionals making the plant run, and business management. Plant managers frequently have formalized preparation in business management. The plant manager reports to the Chief Operating Officer.

Chief Operating Officer

The chief operating officer (COO) is responsible for the day-to-day operations of a company. For an industrial enterprise, this may include responsibility for many 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 formalized preparation in business management and years of experience in various aspects of an industry. The Chief Operating Officer reports to the chief executive officer (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 in an industrial organization. Specialized knowledge and access possessed by every employee could put the lives of coworkers, the health of consumers, and the viability of the business at risk.

Operational Security (OPSEC)

Operational security refers to 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 but are not limited to circumspection about sharing potentially valuable details, marking and locking up valuable information, wearing identity badges, confronting questionable behavior, and reporting suspicious activities.

Workplace Safety

Workplace safety is an essential element of the professional context of industrial operations. Personnel who enter industrial facilities require familiarity with various elements 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 concerns -- 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, Lock-Out Tag-Out, Safe Work Procedures, Safety Regulations, and Workplace Safety Communications.

Electrical Safety

Electric current above 50 milliamps is dangerous to human health. Electricity above 100 milliamps can be fatal. Anyone working around electricity – and especially within an industrial environment, such as in an open Control Enclosure – should be aware of basic electrical safety, including Lock-Out Tag-Out procedures.

Lock-Out Tag-Out

Lock-out tag-out refers to disconnecting electrical service (power) from equipment that is under maintenance or repair. A Physical lock with a safety tag is attached to the 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, non-melting fabrics, a harness, and more. While many industrial organizations provide 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 beforehand. 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. 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 refer to 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). The regulations cover 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 weather, 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 but are not limited to 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 types is useful in understanding the consequences of a disturbance.

Continuous Processes

Continuous processes are those that occur without interruption in which the product is not accounted 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 provides a memorable example. 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, but the DHS groupings are not the only reasonable way to discuss industry sectors. It may be helpful to recognize that sectors may have alternate/related names, often have high interdependencies, and that the line between industries is not always clear. Common industry sector groupings include but are not limited to: Electric Power, Oil & Natural Gas, Petrochemical, Food & Pharmaceutical, Mining & Metals, Manufacturing, Pulp & Paper, Water & 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 – the production of electricity at generating plants such as hydroelectric dams; transmission – moving electricity from the generating plants that produce it through long distance corridors of low gauge wire to the general vicinity of its consumers; and distribution – spreading out reasonable voltages of electricity from distribution substations to industrial, commercial, and residential electricity consumers.

Oil & Natural Gas Sector

The oil and natural gas industry consists of identifying oil (petroleum) and natural gas deposits buried beneath the earth, exploiting those deposits (called "upstream operations"), converting them into consumable products ("midstream"), and delivering those products to end users ("downstream"). Oil is liquid, and is generally moved by Pumps, while natural gas is in a gaseous state, and is generally moved by Compressors. Oil products include gasoline, diesel fuel, and jet fuel critical to the Transportation industry. In 2023, natural gas is the fuel source for nearly 40% of commercially generated electricity in the United States.

Petrochemical Sector

The petrochemical industry uses midstream Oil & Natural Gas operations (such as oil refining) to create chemicals that support a multitude of manufacturing processes, including but not limited to plastics, synthetic fibers, and adhesives.

Food & Pharmaceutical Sector

The food and pharmaceutical industry provides products that are consumed by humans and animals to keep them alive and healthy. This industry entails plant science, farming, animal science, livestock, and medicines. Agriculture is often described as the basis of society and civilization because without food sources, humans cannot live, much less organize themselves to accomplish greater objectives.

Mining & Metals Sector

The mining and metals industry identifies valuable elements and compounds contained within the crust of the earth, 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. Manufacturing is often considered "discrete" manufacturing – meaning products that can be exactly counted. This can range from apple pies to zip ties, and from baseball bats to yellow yarn.

Pulp & Paper Sector

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

Water & Wastewater Sector

The water and wastewater industry provides the basic human need of consumable fluid that composes 60% of the adult human body. Waterworks serve the consumption and sanitary needs (cleaning and flushing) for population centers small and large. In some locations and jurisdictions, the industry protects the environment through treatment processes of 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 forces of nature, security from spying or attack, physical organization, and 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 deals with the movement of 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 with a purpose. Facilities often house industrial equipment and processes but are considered separately from those processes. Facilities may also be mobile, such as trains, ships, and aircraft. Important topics within facilities include but are not limited to Facility Type, Facility Planning & Design, Facility Location, and Facility-Wide Services.

Facility Type

Each facility can be described by the industry it supports and the processes that occur therein. 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 on facility (and process) design.

Facility Planning & 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

Facility 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 of a facility 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 but are not limited to 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 the those involved in the industrial process.

Electric Power

The facility-wide service of electric power refers to the power supply supporting the entire facility. This normally includes step-down transformers outside the building. It may include a battery system as a temporary backup power source, or an onsite Generator in case offsite power fails. It includes the electrical wiring and outlets of various voltages.

Heating, Ventilation & Air Conditioning

Heating, Ventilation & 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 equally 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 detection of human presence. Some light sources are more energy efficient than others. Light can influence employee health and productivity. Adequate light plays a key role in safety and security.

Fire Protection

Fire protection is an integral concern for commercial and industrial facilities, which must conform to 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 firestops, alarms, automatic, and manual systems. They can be configured to communicate with local fire fighters.

Physical Security

Physical security systems control entrance (ingress) to and exit (egress) from facilities and within facility areas, including to lock or unlock doors and turnstiles. These systems can

dissuade and delay unauthorized individuals and provide useful records about credentials presented, dates, times, and locations.

Engineering Documentation

Engineering documentation refers to details useful to Design, Build, Operate, and Maintain an industrial facility and its components. Such documentation includes but is not limited to Facility Drawings, Process Flow Diagrams, Piping & Instrumentation Diagrams, Loop Diagrams, Wiring Diagrams, Product Specifications, 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 and require specialized knowledge and practice to fully interpret.

Process Flow Diagrams

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

Piping & 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, as designated by a loop number. Details include the wiring that extends from Sensors/Transmitters (field instruments) through terminals and to the Controller and its associated signal type, along with the calibration associated with each input and output.

Wiring Diagrams

Wiring diagrams are a graphical depiction of the terminals (electrical connection points) of electrical devices/equipment and wires that connect them together 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 contrasts with 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 product vendor's or distributor's web site.

User Manuals

User manuals provide detailed, step-by-step guidance on how to install, connect to, control, communicate with, manage, and maintain a product. Manuals often provide images, tips, warnings, and references to other useful resources. Manuals are much longer than Product Specifications, and can be found on the Vendor's Web site.

Industrial Lifecycles

The term "Industrial lifecycles" refers to the stages of existence for industrial Facilities, Processes, Control Systems, and the products produced thereby. The idea that a company or organization is responsible for a facility, process, product, or system from idea 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 stages can include Design, Specify & Procure, Build, Operate & 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 often incorporate products which themselves are outputs from other Lifecycles.

Specify & 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 exact characteristics of an input are important. Procurement is often a business task which involves ensuring a sound understanding of the specified good, obtaining samples, testing samples, negotiating price, and placing an order. Once trusted relationships are in place, the procurement process is often simple and highly automated.

Build

The build phase of the Lifecycle follows Specify & Procure and involves creating or assembling the physical elements of the facility, process, or system. The build phase is often much shorter than the Operate & Maintain Phase. 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 techniques and configuration merit special attention from cybersecurity practitioners.

Operate & Maintain

Operate and maintain refers to the phase in which the process or facility are operational – they are carrying out their intended mission. Operate and maintain is typically the longest phase and can last decades. Large industrial facilities may operate 24 hours a day and seven days a week because they are turning a profit for the company. Some failures and breakdowns can be addressed with minimal impact to 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 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 no longer supported by their original manufacturer.

Dismantle

Dismantle is the Lifecycle phase in which the facility or process is permanently shut down and disassembled. Some consumer products last only a short time, meaning that the Industrial Process lasts less than one year. When an industrial facility is closed, dismantling can also last a long time and be 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 Preventative Maintenance and 2) Change Management.

Change Management

Change management refers to a formal process of maximizing plant and process reliability through proposal, approval, testing, full implementation, documenting, and monitoring of changes to a facility or system. Key concepts for change management include but are not limited to: System Model/Inventory, Device Configurations, Software & Hardware, Recalls, Errata, Release Notes, Software Bill 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. Information available within the model may include but is not limited to facility, location, process, Engineering Documentation, network information (such as IP address), and name and contact information of responsible individuals. Keeping the model accurate and up to date maintains continuity among the "as designed," "as built," and "as exists" versions of a Facility, system, or process. Because an integrated system model intends to hold all current information about the system, it represents 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 but are not limited to the placement of jumpers on pins within a Transmitter, the Scaling of a 4-20mA signal, and whether logging is enabled. Device configurations should be kept under Change Management and be included in an Integrated System Model.

Software & Hardware

Software represents the code or logic that determines how a system operates. 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 needs addressed. The term recall most frequently applies to a physical product, where "advisory," "patch," or "update" frequently apply to 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. Errata 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 errata. Recognizing the applicability of an errata may result in a change to the process or system.

Release Notes

Each time a Vendor releases a patch or a new version of software or a computer-based product, they 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). Review of 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 that 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 allow an Asset Owner to recognize relationships and relevant vulnerabilities that would otherwise remain obscure. Armed 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 case the primary data or software are 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 restore a system to known-good state in short order.

Change Records

Change records describe what changes were made to a system, by whom, and when. They are the essential element 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

The "Foundational Industrial Control Systems Knowledge" section describes the core Industrial Control Systems (ICS) terminology required for an individual's professional success within the field of industrial cybersecurity. Categories include: Instrumentation & Control, Process Equipment, Industrial Networking & Communications, and Process Safety & Reliability.

Instrumentation & Control

Instrumentation and control represent a category of foundational Industrial Control Systems knowledge. The category includes but is not limited to Industrial Control Systems, Control Theory, Control System Components, Programming & Control Logic, Alarm Management, and Control System Software.

Industrial Control Systems

Industrial Control Systems (ICS) refer to the field of study and practice that deals with using technology to automate and control a wide 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.

Control Theory

Control theory refers to the conceptual underpinnings of Process Control. Key control theory terms and concepts include but are not limited to Control Loop, Set Points, Process Variables, Control Variables, Primary Control Elements, Final Control Devices, E Feedback, Open & Closed Loop, Process Dynamics, Error, Control Algorithms, Control Strategy, Loop Tuning, Simulation & Modeling, and Deadband & 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 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 degrees Fahrenheit during the day and 68 degrees Fahrenheit at night.

Process Variables

Process variables are the current actual measurement of the physical characteristics of a system. Common process variables include but are not limited to Temperature, Pressure, Level, and Flow. If the current temperature in a home is 82 degrees Fahrenheit, the process variable is 82 degrees.

Control Variables

A control variable is the measurement of the physical condition 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 degrees, and the process variable (actual temperature) is 82 degrees, 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, or rate.

Primary Control Elements

The primary control element refers to 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 is the single pole, double throw relay that allows electricity to energize the air conditioner. In many other processes, the final control device regulates a rate – for example a valve positioner that governs the rate at which liquid flows through a Pipe.

Feedback

Feedback refers to continual input into the decision-making component of a control system (often a Controller), which results in dynamic behavior of a Final Control Device. For example, In the case of a residential air conditioning system, the feedback is the continual measurement of the temperature. Once the temperature reaches the Set Point, the Controller sends the signal to turn the air conditioner “off.”

Open & Closed Loop

An open loop control system relies on human input to make an adjustment (manipulate the Final Control Device). For example, in an open loop system, once a Tank has reached its “full” mark, a human closes a manually operated gate Valves to prevent the entry of additional fluid. A closed loop control system on the other hand requires no human intervention to make an adjustment. For example, a float switch indicates that a tank is “full,” and the Controller sends a signal for the Motor to close the associated Valve. Closed loop systems have increased the efficiency and safety of Production Operations by minimizing the numbers of humans required to operate a Facility. Determining what loops should be open or closed is a Design consideration with significant Safety and Reliability implications.

Process Dynamics

Process dynamics refer to the way an Industrial Process changes over time given differing inputs and external loads/context. Reduced to practice, process dynamics are the mathematical model that describe 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, and allows a Controller to implement a Control Algorithm.

Control Algorithms

Control algorithms describe the mathematics that determine what action 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.

Proportional means that the final control device should be actuated by the same amount (proportionally) as the deviation (also known as the error) between the process variable and the set point: if there is a 5% deviation (a 5% error), the Valve should be moved by 5%.

Integral means that 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 of actuation should be updated by how well proportional control worked the last time it was used.

Derivative means the Final Control Element should be actuated in anticipation of the future effects of the actuation – fully accounting for the current rate of change of the error.

When a controller can implement all three of these algorithms together, it is known as a PID controller (which is not to be confused with P&ID - Piping and Instrumentation Diagram).

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 but are not limited to feedforward control, ratio control, and cascade control.

Feedforward control 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 itself. For example, rather than control the amount of water in a continuous Boiler based on the current level of water, a feedforward strategy would control the flow of steam out of the boiler by considering water level within the boiler as a source of disturbance in steam flow. Feedforward is often implemented alongside PID control.

Ratio control aims to maintain optimal performance by seeking a set point that is a ratio between process variables, rather than two individual values that might otherwise compete with one another.

Cascade control uses the output of one controller as the input into another controller – essentially forming a nested loop.

Loop Tuning

Loop tuning describes actions 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 error between the set point and Process Variable, ultimately influencing the efficiency of a process over time.

Simulation & Modeling

Process and control system simulation and modeling techniques provide insight for: Control System Vendors seeking to develop new products or product features, Engineers seeking to optimize a process before or after deployment, Owners & Operators to train Process Operators (including control room operators). Simulation and modeling software can incorporate principles of physics, chemistry, and mathematics 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 facilitates safety, security, and reliability decisions.

Deadband & Dead Time

Deadband 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. Deadband 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 deadband range of 4 degrees built into a residential air conditioning system. That is to say that given a Set Point of 72 degrees Fahrenheit, the air conditioner will not turn on until the temperature reaches 74 degrees and will not shut off until the temperature reaches 70 degrees. No control action will occur within this 4-degree deadband.

Control System Components

Control system components are the devices and interfaces that make up a control system. They include but are not limited to Control Rooms, Control Centers, Control Panels, Control Enclosures, Sensors & Transmitters, Controllers, Operator Interfaces, Engineering Computers, Application Servers, and Motor Controllers.

Control Centers

A control center may bring together control information for multiple facilities – 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 describes a room wherein Operators supervise 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 control system Vendors.

Control Panels

Frequently found in a Control Room, a control panel generally describes the console or display from which a Process Operator or Control Room Operator observes and interacts with an Industrial Processes. A control panel may be physical or digital, or a combination of each.

Control Enclosures

A control enclosure is a cabinet that frequently contains a DC power supply to provide electricity to electronic Control System Components, a Controller (such as a PLC), input and output modules, terminal blocks, wiring, and a network switch. Panel-based HMIs are sometimes mounted to the front of a control enclosure. Components within the enclosure are often mounted on DIN rail. Workplace Safety procedures should govern when and how to open each enclosure. Because enclosures provide physical access to key control system components, they may be subject to physical access control.

Operator Interfaces

Operator interfaces are the technologies designed for human operators to interact with a controlled process in real-time. Interfaces represent the controlled process as representative icons and graphics. Operator interfaces are often 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 a normally a large monitor/screen or set of monitors located within a Control Room 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 from the plant floor. The software allows 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. The Application Server is often located in a

server room or data center. This client-server architecture allows control room operators to work remotely if desired. Because of their ability to interact with the controlled process, supervisory interfaces are high value targets to would-be attackers. Numerous Control Systems Vendors provide supervisory interface software. These include but are not limited to Siemens, Rockwell Automation, Schneider Electric, and ABB, each with a different market focus and geographical orientation.

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 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 inform HMI design.

Engineering Computers

Engineering computers refers to a variety of computers that are used by Engineers or Technicians within an industrial environment. These include but are not limited to Engineering Workstations, Technician Laptops, Contractor Computers, Tablets, Process Analyzers, and Calibrators & Configurators. These computers incorporate hardware that suits their deployment and use (such as hardened form factors).

Engineering Workstations

The computer that Engineers use to design and support the Industrial Control System for a process or group of processes is commonly known as an engineering workstation. The workstation normally runs on Microsoft Windows, and includes 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 plant. The workstation will have access to every aspect of the process control network, making it both a valuable asset and attack target.

Technician Laptops

A technician laptop may include similar software as the Engineering Workstation, but in a more portable 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.

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.

Tablets

Tablets are handheld computers that serve essentially a mixed function between a Technician 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 composition of gasses or liquids. Output of these analyzers aids in adjusting process characteristics to enhance process efficiency and product quality. Process analyzers are particularly common in chemical, Petrochemical or Pharmaceutical processes. Common process analyzer vendors include but are not limited to ThermoFisher Scientific and Yokogawa.

Calibrators & Configurators

Calibrators and configurators are handheld devices that allow Technicians to perform Calibration, configuration, and testing of 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 but are not limited to Fluke, Emerson, and Endress+Hauser.

Application Servers

Application servers describe the services available to hosts on a Process Control Network or from the process control network to the Corporate Network. These can include but are not limited to Process Data Historians, Supervisory Interfaces, Manufacturing Execution Systems, and Enterprise Resource Planning.

Process Data Historians

Process Data Historians maintain a history (a database) of Process Variables, Set Points, and Control Variables together 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 a possible pivot point for attackers moving from the corporate network onto the process control network. Manipulation of data within a historian may impair the ability to conduct an accurate analysis and thus lead to poor decisions of various types. 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 but are limited to Aveva (formerly OSIsoft), Canary Labs, and Aspen Technology.

Manufacturing Execution Systems (MES)

A manufacturing execution system is a software package dedicated to linking business systems, such as Enterprise Resource Planning systems to production operations, including the 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 MES can include: laboratory information management, warehouse management, and maintenance management. Because they provide critical information about, and linkages to production operations, manufacturing execution systems are high value targets for would-be attackers. Typical MES vendors include but are not limited to SAP, Dassault Systems, Siemens, and Rockwell Automation.

Enterprise Resource Planning (ERP)

Enterprise resource planning software integrates 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 can link closely to Manufacturing Execution Systems, and therefore into Industrial Control Systems, making them high value targets to would be attackers. Typical ERP vendors include but are not limited to Oracle (Netsuite) and SAP (S4/HANA).

Controllers

Controllers are specialized electrical devices that monitor for inputs (such as Process Variable) and drive outputs (such as 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 but are not limited to: Relays, Controller Hardware, Input/Output, Controller Memory, Tags, Program Scan, Programming Key Switch, Programmable Logic Controller (PLC), Distributed Control Systems (DCS), 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 logic gates for increasingly complex cases. Early automation systems relied on complex arrangements of such relays. 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 immunity from cyber attacks.

Controller Hardware

"Controller hardware" refers to the physical components of a Controller. These devices are engineered to withstand temperatures, vibrations, and other conditions that may exist in an industrial environment. A typical Programmable Logic Controller (PLC) requires DC power to operate. 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 (IO) modules. The modules connect to one another such that information from the IO modules makes it to and from the CPU module. 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 a microprocessor, integrated circuits for performing common tasks, non-volatile memory, and volatile memory. Many controller form factors have interfaces for inserting memory cards that hold a program. Some have battery backups for retaining values within volatile memory in case of power loss. Most form factors have a Programming Key Switch.

Input/Output

Input and output, also known as "IO" and "I/O," carry input electrical signals (that represent the Process Variables) from the Sensors/Transmitters to the CPU module, and output electrical signals (Control Variables) from the CPU module to the Actuators. IO modules vary by the type of signal required by the transmitter or actuator. Each IO module may have terminals to support one or more connections. When programming the CPU module, it is necessary to accurately identify which physical terminal corresponds to what transmitter or actuator. Misassignment can cause devastating impacts.

Controller Memory

Controller memory may be non-volatile for storing firmware and program files, and volatile for storing a loaded program and process data. 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, etc., 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 is extremely useful to Technicians and Engineers programming both controllers and Operator Interfaces as it allows for quick recognition of what is being calculated, considered, measured, or controlled. An example Tag name would be TC204_SP, which may indicate temperature control loop 204 Set Point. Tag designation could also include a data type, a scope (what 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 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 real 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 on the front of a programmable Controller which allows a user to select among 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 programmed. “Program” tends to mean that the controller does not execute new logic while it is being programmed. “Remote” tends to mean that the key switch can be virtually moved between “run” or “program” within 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 commonly left in “remote” mode for the sake of convenience. This is a significant 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 (PLC) is the common name and acronym for general purpose programmable Controllers that receive Input Signals (such as 4-20mA or 1-5V), 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, among others.

Distributed Control Systems (DCS)

DCS refers to turnkey automation systems that incorporate Controller hardware and Supervisory software in a single system from a single vendor. DCSs are commonly found in the Petrochemical Sector. Leading vendors include Honeywell Process Solutions, Emerson Automation Solutions, and Yokogawa Electric, among others.

Remote Terminal Units (RTUs)

RTU is the name used in certain industry sectors (including but not limited to Electric Power, Oil & Natural Gas, and Mining & Metals) for a programmable Controller that aggregates control at remote locations. Leading vendors include ABB, GE Grid Solutions, Siemens Energy, and Schneider Electric, among others.

Intelligent Electrical Devices (IEDs)

"IED" describes a programmable Controller applied to equipment in the Electric Power Sector, such as Transformers and Circuit Breakers, and are used to make control decisions based on characteristics such as voltage and frequency. IEDs may be connected to RTUs or operate independently thereof. Leading vendors include ABB, GE Grid Solutions, Siemens Energy, and Schneider Electric, among others.

Protective Relays

A protective relay is a special type of IED intended to open a Circuit Breaker, shutting off the flow of electricity, when dangerous conditions are detected as part of an electric transmission or electric distribution system.

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.

Soft PLCs

"Soft PLC" generally refers to a traditional, general-purpose computer being 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 but are not limited to Motor Starters, Adjustable Speed Drives, Motor Protection, Motor Control Centers, and Smart Motor Controllers.

Motor Starters

Motor starters are a class of electrical device that protects Electric Motors by limiting inrush current to short durations during motor startup. 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 to 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 allows 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 a motor-driven Industrial Processes and the energy efficiency of the motor. Adjustable speed drives are also known as variable frequency drives (VFDs), adjustable frequency drives (AFDs), and AC drives. ASDs can be mounted on a wall or within a Control Enclosure. Using vendor-provided software, a user can input the parameters of the controlled motor, and then set speed, acceleration and deceleration, skip frequencies, and overload limits. Typical vendors include but are not limited to Siemens, Rockwell Automation, Danfoss, and Yaskawa. Manipulation of ASD programming can have significant impacts.

Motor Protection

Motor protection refers to techniques and mechanisms to safeguard an electrical motor from electrical, thermal, or mechanical faults resulting from overcurrent, undercurrent, over and under voltage, 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 control, protection, and distribution to the various motors within the facility. MCCs placed within protective Enclosures, and can be located in their own building, in their own room, or along a wall close to the equipment they control.

Smart Motor Controllers

A smart motor controller incorporates a variety of functionality, such as Motor Protection, remote monitoring and control, and communications interface into a single motor control device.

Sensors & Transmitters

Sensors and transmitters measure and communicate, respectively, the physical characteristics of a process. These measurements are known as the Process Variable. Important terms related to sensors and transmitters include but are not limited to Sensors, Transmitters, Units of

Measure, Transduction, Principles of Operation, Temperature, Pressure, Level, Flow, Calibration & Configuration , Scaling, Transmitter Failure Mode, Transmitter Security, Meters, and Smart Instrumentation. Sensors and transmitters are sometimes referred to as “field instruments.”

Sensors

A sensor is the element that reduces the physical characteristic of a process to a measured value, such as Temperature, Pressure, Level, or Flow (though many other types of sensors exist). It is important to recognize that a sensor identifies the value by applying the Principles of Operation.

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. While sensors and transmitters are often tightly integrated, it is important to recognize that they are technically different elements with different purposes. Some transmitters are “indicating transmitters” – meaning that the value being transmitted (and its associated signal) can be directly read by a human viewing a display on the transmitter. Transmitters have various levels of functionality and programmability. Accurate readings from and predictable behavior of transmitters are essential to safe, reliable, and effective process control. Leading transmitter vendors include but are not limited to Endress + Houser, Emerson Rosemount, and Honeywell.

Units of Measure

A unit of measure is a standard for communicating an amount. For example, Temperature may be communicated 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’s 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 refers to the conversion of one type of physical force 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 a transducer at the bottom of a reservoir. An I-to-P transducer (notice the different order of the terms) could be used in an a Pneumatically Actuated Valve Positioner to implement the specified Control Variable.

Principles of Operation

The “principle of operation” describes 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 magnetic flow meter. Specific details of the process being controlled determine the appropriate principle of operation to apply.

Temperature

Temperature refers to the hotness or coldness of an object or substance. Examples of Industrial Processes that rely on temperature measurement include but are not limited to Boiler operations for commercial or residential heating, and steam production for electricity generation. Common temperature sensor types include resistance temperature detector (RTD), thermistor, and thermocouple. Common units of measure for temperature include Kelvins, degrees Fahrenheit, and degrees Celsius.

Pressure

Pressure refers to the force that one object exerts against another. Examples Industrial Processes that rely on pressure measurement include but are not limited to Compressor operations for natural gas transmission, and distillation columns for oil refining. Numerous pressure measurement devices and technologies exist, including but not limited to strain gauges and piezoelectric and capacitive models. Common units of measure for pressure include Pascal, pounds per square inch (PSI), atmosphere, bar, and inches of mercury.

Level

Level refers to the fullness or emptiness of a reservoir, container, or vessel. Examples of Industrial Processes that rely on level include but are not limited to pumped storage electricity generation, and aeration lagoon operations for wastewater treatment. Common level measurement devices include ultrasonic, guided wave radar, capacitance, and level switches. Common units of measure for level include feet or meters. Additional meaning is obtained when expressing level as a percent of full.

Flow

Flow refers to the quantity and velocity of liquid or gas through an area, both a Pipe and an open channel. Examples of Industrial Processes that rely on flow measurement include but are not limited to pasteurization, and petroleum pipelines. Common flow measurement devices include but are not limited to vortex shedding, sonar, Coriolis, and magnetic. Common units of measure for flow can be volumetric (such as cubic feet per second, cubic meters per second, and liters per second), or mass (such as pounds per minute, or tons per hour). Because flow of gasses can vary by temperature and pressure, specialized “flow computers” can be used to calculate flow and transmission values.

Calibration & Configuration

Calibration is the process of attuning a Sensor/transmitter to a verified quantity/measurement within a specified error tolerance. Calibration involves identifying the range of the sensor, connecting the sensor to the test equipment (such as documenting Calibrator), and testing the desired range of the sensor (this is the “as found” test). If the output does not match, 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). Documentation of this process, called the “calibration certificate” is stored electronically in the maintenance management system. Calibration frequency depends on criticality of the measurement to the controlled

process, and guidance from the instrument vendor. Depending on the application, uncalibrated Sensors/Transmitters (field instruments) or intentionally mis-calibrated field instruments can have devastating Impacts.

Configuration refers to a variety of settings within a transmitter that match the process context. Some settings, such as selecting signal output (current vs voltage), are accomplished with a handheld Configurator. Others settings, such as Transmitter Failure Mode and Transmitter Security are done via the placement of physical jumper pins within the Transmitter housing.

Scaling

Scaling means setting the Sensors/Transmitters (field instrument) output to correspond with a desired Signal, such as a 0-5 Volts (V) or 4-20 milliamps (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 degrees Fahrenheit (lowest expected temperature) to 212 degrees Fahrenheit (highest expected temperature). The transmitter would be scaled to send a 4mA signal to a Controller at 72 degrees, and a 20mA signal at 212 degrees. Temperatures below 72 or above 212 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 20mA), or a low signal (such as below 4mA). The Controller software can recognize that this signal means the transmitter value cannot be trusted. The failure mode (high or low) is set by an Instrument Technician by the placement of 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

Some Transmitters can be set to disallow configuration changes. Transmitter security is often set via the placement of a physical jumper within the transmitter housing.

Meters

A meter measures a quantity delivered over a period or periods of time. In general, a meter differs from a Transmitter in that its output is not used for an immediate control decision. It may be used instead 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 allowing both customers and providers to easily read the meter, and remote disconnect (in the case of electricity meters) allowing the electricity provider to turn off power to the customer. Smart meters can save costs by simplifying meter-

reading, and by altering consumer behavior which results from making electric usage information immediately available to them.

Smart Instrumentation

In addition to transmitting Sensor values to a Controller, smart instruments/Transmitters allow retrieval of additional diagnostic information about control system components to which they are connected. A common example would be HART interface that allows instrument Technicians to easily retrieve or change Calibration and Configuration.

Programming & Control Logic

The behavior of programmable Controllers can be defined by Technicians or Engineers who program them by using specialized software on Engineering Workstations or Technician Laptops. This programming transferred (downloaded) to the controller is commonly known as "control logic." Topics for controller programming include but are not limited to IEC 61131-3, Ladder Diagram, Function Block Diagram, Structured Text, Sequential Function Chart, and Controller Code Quality.

IEC 61131-3

IEC 61131-3 is the leading international standard that describes "the syntax and semantics of 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 describes a Sequential Function Chart that structures programs and function blocks.

Ladder Diagram

A Ladder Diagram is the most common programming language for programmable Controllers. It is primarily a visual language consisting of two vertical rails, and a series of rungs that resemble a ladder. The ladder is read from left to right and from top to bottom. The code 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. On the right, at the end of a rung, are the "coils" or outputs, representing Relays, Motor Starters, or other outputs.

Function Block Diagram

A function block diagram is a popular programming language for programmable Controllers. The diagram represents the functions as blocks within the diagram. For example, a block can be a logic "AND" block or a "Timer delay" block. 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. Function blocks are commonly used by Distributed Control Systems (DCSs).

Structured Text

Structured text is a textual base programming language similar in format to computer programming languages such as BASIC, C, or Python. Structured text is the most portable of the three IEC 61131-3 languages, meaning that structured text is most likely to execute on any PLC platform that complies with the IEC 61131-3 standard.

Sequential Function Chart

A sequential function chart graphically describes 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. SFC is an important tool for organizing and managing system states.

Controller Code Quality

Controller code quality describes the characteristics of user-generated Controller code that make it desirable, valuable, and lasting. Examples of such characteristics include but are not limited to maintainability, portability, reliability, reusability, testability, security, and safety. Controller code quality standards can be found in documents such as the "PLC Open Coding Guidelines" and the "Top 20 Secure PLC Coding Practices."

Alarm Management

Alarm management describes the processes of identifying, defining, creating, monitoring, responding to, and maintaining alarms for an Industrial Control System. Key topics include but are not limited to Alarms, Alarm Management Lifecycle, Consequence Severity, Alarm Prioritization, Alarm States, Alarm Performance, and Safety Alarms. ISA18 Committee deals with alarm management. ANSI/ISA-18.2-2016 is an international standard for alarm management in Process Control.

Alarms

Alarms are pre-determined warnings and alerts to a human Process Operator about a condition that's 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 colors, and 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 refers to the sequential 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 appropriate considerations and

responses should be fully documented and made available for later reference 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, plant and equipment, production loss, 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 human Process Operator or Control Room Operator where to best put their attention in the moment. Prioritization can be based on a combination of Consequence Severity and acceptable response time. Prioritization can be achieved via placement of popups on the screen, colors of alarms, and types of sounds.

Alarm States

Alarm states refer to the process of balancing the process state (normal or abnormal), alarm state (active or inactive), and acknowledgment state (acknowledges or unacknowledged). In addition, Alarms may be permanently or temporarily removed from service (suppressed).

Alarm Performance

Alarm performance describes the process of assessing the transitions between Alarm States over time, together with supervisory actions taken as the result of an Alarms. Such analysis can allow 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 refers to the code used to operate an Industrial Process, this can include 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. Leading vendors for such software include but are not limited to 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 describes the physical components used to perform work within an Industrial Operations environment. Such a variety of equipment exists that it is difficult to identity and describe them all.

Industrial cybersecurity professionals should have a basic understanding of how relevant equipment operates, the effects of its manipulation and its Failure Modes. Such understanding may draw on concepts of physics, chemistry, metallurgy, and thermodynamics for example. Some equipment is specific to certain Industry Sectors, and other equipment is deployed across many sectors.

Common equipment includes, but is not limited to Actuators, Electric Motors, Pumps, Compressors, Valves, Piping, Conveyors, Tanks & Vessels, Electric Power Equipment, Process Heating & Cooling, Process Chemistry, Turbines, Robotics, Motion Control, Vision Systems, Air Handling Equipment, Filters & Scrubbers, Engines, Ingress & 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 application of the actuator, 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 fluid is introduced by the pump, and a pressure regulator that limits pressure by allowing fluid to

escape to the reservoir. Examples of hydraulic systems include but are not limited to 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 but are not limited to AC induction motors, DC motors, stepper motors, piezoelectric motors, and electrostatic motors. The type of motor chosen should match the requirements of the application, 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 the rotation of 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 of 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 requiring movement of liquid: Water & Wastewater, and Oil & 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. Performance of the pump can be determined by examining the pump performance curve that describes 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 for placement within/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, 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 gasses from one location to another through a Tube or Pipe. Compressors are used in any industry requiring movement of gasses: Oil & Natural Gas and Petrochemical are prime examples. Compressors should be chosen based on process requirements, such as: compression ratio, power requirements, speed, and efficiency. Performance of the compressor can be determined by examining the compressor performance curve that describes compressor efficiency given the application details.

It is important to recognize that compressors may be used to provide 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 both take in and 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, other process equipment, harm to people and environmental damage.

Valves

Vales allow or disallow the flow of material (liquids, gasses, and solid particles) through a tube or chute, providing a critical process control function in nearly every Industry Sector. Common types of valves include but are not limited to rotary, linear, ball, butterfly, plug, globe, gate, needle, solenoid, coaxial, and angle seat. Valve type is specified by 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 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 of 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 & Natural Gas, Petrochemical, Water & 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 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—allowing for increased energy efficiency and finer-tuned movement. Applications of conveyors 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, failure or stoppage of a conveyor can halt operations.

Tanks & 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 & Natural Gas, Petrochemical, Pharmaceuticals, and more.

Tank Shape

The shape of a tank or vessel describes its physical form or configuration. A tank or vessel's shape is designed based upon several factors such as the type of material being stored, the desired capacity, space limitations, and operational considerations – such as desired flow. Some common shapes of tanks and vessels are rectangular, cylindrical, spherical, and conical.

Tank Materials

Materials refers to the substances or compounds of which tanks and vessels are constructed. These materials are chosen based upon their interaction with tank contents, and environmental

conditions such as resistance to pressure, temperature, and corrosion. Common materials that for tanks and vessels include steel, carbon steel, stainless steel, aluminum, and other alloys.

Electric Power System Equipment

Electric power system equipment refers to 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 but is not limited to Generators, Conductors, Insulators, Bushings & 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, which 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 created by combustion.

Components of electromagnetic generators include rotor, stator, windings or magnets, and the armature. Generator design determines whether an electric power system uses DC – direct current, or AC – alternating current. 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. Overloaded power lines may sag until they contact vegetation or the ground, producing a fault and igniting fires.

Insulators, Bushings & Arrestors

Insulators, bushings, and arrestors 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 normally cover short distances of conductor (from half a meter to 10 meters), such as entry points to transformers. Arrestors 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 arrestors are commonly made of porcelain and filled with insulation. Their failure can destroy electrical equipment, interrupt the supply of electricity, and harm individuals present when the failure occurs.

Transformers

Within the Electric Power System, alternating current (AC) transformers receive electricity at one voltage and provide an output at another voltage. Transformers consist of two sets of windings: copper wire wound repeatedly on two sides of a ferromagnetic core. If the input side (primary winding) has a greater number of windings than the output side (secondary winding), it is a step-up transformer, as the voltage entering the transformer is lower than the voltage exiting it. If the input side has fewer windings, it is a step-down transformer, as the voltage entering the transformer is greater than the voltage exiting it. Step-up transformers are commonly used for electricity transmission. Step-down transformers are commonly used to change electricity from transmission voltages to distribution voltages, and from distribution voltage 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 located within 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 gasses. Transformers that experience voltages that exceed their rating can fail and even explode.

Switchgear

Switchgear are Electric Power Systems Equipment, that makes and breaks connections between electrical circuits, helping regulate, protect, and isolate electric systems. Examples of switchgear include but are not limited to 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 a loaded spring) to interrupt an electrical circuit; 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, hydraulic, or pneumatic device, as well as a manual operating principle such as 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 vacuum interrupter. After breaker operation, 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 offsite power system failure. Technological advancements in energy storage technology (such as Lithium-ion batteries) are altering the energy landscape by: increasing demand for power generation, enhancing the usefulness of renewable energy, and creating a more flexible grid. These batteries are often managed by their own control systems. Disruption of these systems could prevent a facility or process from functioning as intended – especially in case of offsite power failure.

Capacitors

Capacitors allow for the accumulation of electric charge that can later be released. They consist of two conductors (often metallic plates) separated by either air or a dielectric material, which 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 converts 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. Malfunction of a turbine or its components can have a devastating impact on the controlled process.

Process Heating & Cooling

Process heating and cooling describes the mechanisms to provide or remove heat to an Industrial Process. Process heating and cooling is common in nearly all Industry Sectors. Its equipment includes but is not limited to Boilers, Heaters, Heat Exchangers, Furnaces, Distillation Columns, Refrigerators & 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 non-pressurized environments. If the tubes contain the fire, it is a fire-tube boiler, if the tubes contain the 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 are 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 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 heats close by one another – 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 pre-heat milk on its way from the refrigerator to the pasteurizer (which heats milk to kill bacteria), and to pre-cool 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. Temperatures in these furnaces can reach thousands of degrees Fahrenheit. Combustion furnaces include burners where fuel is constantly emitted, 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 & Metals, Petrochemical, and Manufacturing. For example, in metal production, a blast furnace dumps ores in the top, and blasts hot air from the 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 component parts by changing the liquid to steam (boiling). The steam is then condensed to back to a liquid form. In a distillation column, the liquids with highest boiling points are removed from the bottom of the column, closest to the heat source/Furnace, and the liquids with 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, 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 & Pharmaceutical industry sector, and in the Petrochemical industry sector. For example, distilled water 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 & 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, which 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 Food & Pharmaceutical and Transportation industries because they keep consumables from spoiling. Malfunctions of refrigerators and freezers can damage products and human health.

Industrial Chillers

An industrial chiller is used to remove heat from buildings, machines, processes, and products, which require intensive cooling. Examples include but are not limited to metal finishing, injection molding, and printing. Chillers work on the same basic principle as refrigerators but 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

Process chemistry refers to the chemical reactions and processes that form an integral part of industrial operations across industry sectors including Petrochemical, Water & Wastewater, Pharmaceutical, and Manufacturing. Process chemistry equipment commonly includes Crackers and Reactors. The volatile of 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 which 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 – used for non-continuous applications, and continuous stirred tank reactors – where mixing occurs at a constant rate.

Robotics

Robotics refers to automated, non-living, 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.

Robotics are used in a variety of industrial settings. For example, automotive manufacturing uses robotic arms to place and secure parts within 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. Malfunctions of robots 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 refers to 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 accurately recognize its position and speed. 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 factories of various types. Important concepts for motor control include but are not limited to Axis, Motion Type, and Acceleration & 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 & Deceleration

Acceleration and deceleration refer, respectively, to the increasing or decreasing speed of a motor. Accelerating and decelerating a motor cause stress could damage or destroy the motor and related components.

Vision Systems

Vision systems rely on visible light to inform process control decisions. An imager (or photo-eye) – which consists of a lens and a photoelectric Sensors – 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 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 but is not limited to: 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 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. Failure of air handling equipment can disrupt sensitive processes and damage products.

Filters & 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 gasses include paper, polyester, fiberglass, nylon mesh, activated carbon, and ultraviolet light. Filters for liquids can work by forcing liquid through a membrane, through activated carbon, reverse osmosis, or ultraviolet irradiation. While commonly used across many industries, Water and Buildings sectors easily come to mind for their use of filters to clean water and air for human use.

Scrubbers remove or nullify dangerous and unwanted particles from gasses by forcing the gasses through scrubber solutions (which may be gas or liquid). The solutions function by adsorbing (in some cases reacting with) the contaminants. 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 gasses (at the top of smokestacks). Submarines use scrubbers to remove carbon dioxide from the air – keeping the air safe to breathe.

Filters and scrubbers can fail when their components (such as fans, sprayers, and Pumps) fail. Impacts of failures 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 mechanical energy. Steam engines burn fuel to boil water, then trap steam to harness its force. Turbines rely on 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 describes how effectively an engine converts energy (such as fuel or electricity) into mechanical work. Torque refers to the rotational force an engine can produce. Emissions are the pollutants, like carbon dioxide (CO2) or nitrogen oxides (NOx) that leave a combustion engine.

Ingress/Egress Equipment

Ingress and Egress Equipment refers to devices and systems that allow or deny physical entry (ingress) and exit (egress) of 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 series of gates – are doors which open or close when certain conditions are met. A lock may be applied to or within a gate to physically prevent the gate 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, human frustration, and eventually delay the operations that occur within a facility.

Safety Equipment

Safety equipment refers to 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. Programmability of these devices (such as connecting them to a Controller) may allow an adversary 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 consist of a spring-loaded mechanism allows the release of fluid or gas at a specified pressure.

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 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 actuate by either physical contact with an object, or the absence of an object in a designated area. Actuation of 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 and placed on or next to a patient's body to provide diagnostic, treatment, life-support, and reseach 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 but are not limited to heart monitors, blood sugar monitors, and blood oxygen level monitors for diagnosis; CPAP 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 increasingly incorporate network connectivity, facilitating, configuration, control, and communication.

Skid-Mounted Systems

A skid-mounted system is an Industrial Process system all packaged together 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 have opened innovative models such as Machine-As-A-Service.

Machine-As-A-Service

Machine-As-A-Service refers to the business model where rather than owning a machine or Skid, a company or organization pay an ongoing fee for using the skid. This allows both the skid user and the skid owner to predict costs/revenues. While contract details may vary, the skid owner – who is the expert on the skid, is likely to provide maintenance for the skid (by sending their own Technician). While reliance on Machine-As-A-Service 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 simultaneously attack many MAAS customers.

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 deployment of increasingly smarter equipment.

Industrial Networking & Communications

Industrial networking and communications refer to the transmission of data among devices used within an industrial environment and between the Process Control Network and the

Corporate Network. Key topics include but are not limited to Network Architecture & Integration, Data Management, Network Equipment, Signals & Protocols, and Wireless Communications.

Network Architecture & Integration

Network architecture refers to the physical design and layout of a network, including the placement of various nodes and Network Equipment. Network integration refers to incorporating nodes and functionalities into the network. Key topics for network architecture & integration include but are not limited to: 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 an Process Control Network within the context of an entire enterprise. Common terms related to reference architectures include but are not limited to Purdue Enterprise Reference Architecture, Converged Plantwide Ethernet, Levels, Zones, Cells, and Conduits.

Purdue Enterprise Reference Architecture (PERA)

The PERA, first published in 1992, defined hierarchical model for describing the relationship between manufacturing operations and business functions supported by computers and networking technologies. The model relies on the concepts 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 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, Level 0 includes physical devices such as Sensors and Actuators; Level 1 includes local programmable Controllers, Level 2 includes 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 Enterprise Resource Planning (ERP) systems.

Process Control Network

"Process control network" (PCN), also called the "industrial network," "industrial control network," or "industrial control systems network," describes the network of Control System Components used to directly support control of the Industrial Process. Assets within the process control network are often managed by Operations personnel. The term is commonly used to contrast with the Corporate Network.

Corporate Network

"Corporate network" describes the network of computers used to directly support business operations. These are the servers, workstations, laptops, phones, printers, etc., 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 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 – normally dedicated to a specific process or part of a process. For example, there may be a zone for refining operations and another zone for tank farm management. The concept of a zone helps identify what network-connected resources need to talk to 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 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 among Cells within a Zone, and among 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 refers to 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 represents a Common Weakness in Industrial Control Systems.

Cloud Services

Cloud services is a reliance on computing hardware and software that resides in an off-site data center. Cloud services may be hosted internally (by the organization itself) or by and external vendor. Examples of cloud services relevant to Production Operations include but are not limited to 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 product offerings.

Edge Computing

Edge computing refers to a principal reliance on processing and storage closer to network nodes rather than to 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 is ascertaining weaknesses and potential consequences of cybersecurity events.

Machine-to-Machine

Machine to machine (M2M) refers to communications that coordinate directly among computers (in some cases cyber-physical machines) rather than in a centralized client-server architecture. Examples include but are not limited to communications between programmable Controllers, communications between automobiles, and communications between electric meters and in-home energy consuming devices.

Bring-Your-Own-Network (BYON)

Bring-your-own-network 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 OnStar 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

Within an industrial operations environment, data management deals with the creation, processing, storage, and use of data – primarily relative to an Industrial Process. Topics include but are not limited to 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 made. Within an Production Operations environment, Data includes the representation of Set Points, Process Variables, Control Variables, and other process-oriented quantities and concepts.

Data Source

Data source refers to the place data is created or the place from which it is sent. Process data often originates at the Sensor/Transmitter. A Set Point change or Forced Control Variable 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 were created. They often generate new data based on analysis of process data.

Data Path

Data path refers to 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, sent to the Controller, to the local HMI, and to the Supervisory control application, to an Engineering Workstation and to the Historian. Data path is a factor in determining the Impact of a Cybersecurity Event.

Data Storage (Process Data Historians)

Data storage refers to the physical location that data is kept and the software (database) that organizes and controls access to the data. Such software systems are commonly called “process data historians” because they keep a history of Process Variables, Set Points, and Control Variables together with other data relative to production and maintenance.

Data Use

“Data use” describes the decisions the data informs or the actions it determines. Within an Industrial Control System, data use includes but is not limited to Process Control, Supervisory Control, Process Analytics, Manufacturing Execution Systems, and Predictive Maintenance

Systems. The way data is used places requirements on its timeliness. Data use is a factor in determining the Impact of a Cybersecurity Event.

Process Control

Process control refers to the execution of decisions that keep an Industrial Process performing its intended function. In general, routine control decisions are made, and actions are taken, by an automated Controller – such as a PLC.

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 execution of temporary, one-time, control decisions. In some industries, such as Electric Power, and Water & 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

Manufacturing Execution Systems (MES) interface with and extend beyond Process Control, and into supply chain management and accounting applications. For example, a manufacturing execution system may monitor the quantity of ingredients remaining in a hopper for immediate use, the rate of use of those ingredients, and the quantity 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 refers to routers, switches, converters, access points, extenders, taps, 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 but are not limited to Industrially Hardened Network Equipment, Protocol Converters, and Leading Vendors.

Industrially Hardened Network Equipment

"Industrially hardened" refers to the characteristics of the equipment that enable its functionality 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 but are not limited to Rockwell Automation (Stratix), Cisco (IE Series), Siemens (Scalance, RuggedCom), and Belden (Hirschmann), and Moxa.

Signals & Protocols

Signals and protocols describe the ways that network nodes/end points assign meaning to electrical conditions over a physical media to communicate with one another. Within an Production Operations environment, common signals and protocols include but are not limited to 4-20mA, 0-5V, HART, Foundation Fieldbus, Profibus & Profinet, Modbus, EtherNet/IP, DNP3, IEC 61850, BACnet, MC Protocol, Controller Area Network (CAN), Open Platform Communications (OPC), and Message Queueing Telemetry Transport (MQTT).

4-20mA

A 4-20 mA signal refers to the current sent over a wire between the Transmitter and the Controller. These continuous analog signals are normally set by an instrument Technician such that a 4mA signal represents the lowest scaled value, and a 20mA signal represents the highest scaled value. Values that are above or below the determined scale will not be specifically recognized. 4-20mA is commonly used to transmit values related to Temperature, Pressure, Level, and Flow. The first 4 volts can be used to power the circuit. 4-20mA has low susceptibility to noise and can handle longer distances without loss of signal. 4-20mA stands in contrast to common Ethernet cable communications in that Ethernet cable uses voltage differential to communicate a digital (1 or 0) message.

0-5V

A 0-5V signal refers to 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 such that a 0V signal represents the lowest scaled value, and a 5V signal represents the highest scaled value. Values that are above or below the determined scale will not be specifically recognized. 0-10V, 1-5V, or 2-10V may also be used. Compared with 4-20mA 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 allows a digital signal to exist on top of a continuous analog current (4-20mA) 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 HART standards are maintained by the FieldComm Group.

Foundation Fieldbus (FF)

Foundation Fieldbus is a 2-wire voltage-based digital data transmission scheme originally envisioned as an open, standards-based replacement for 4-20mA signals (operating) between the Transmitter and the Controller. Two differing implementations of Foundation Fieldbus exist: H1 and HSE (high speed Ethernet), which require different interfaces and physical media. The HSE implementation commonly operates over port 1600. The FF standards are overseen by the FieldComm Group.

Profibus & Profinet

Profibus and Profinet are communications protocols used primarily with Siemens programmable Controllers. Profibus is a serial protocol deployed in a master-servant relationship where the controller is the master and the IO devices are servants – normally between the Transmitter and the controller, as well as between programmable controllers. Profinet extends a similar concept to Ethernet networks rather than serial communications, used among Level 1 devices, and from Level 1 to Level 2. Profibus and Profinet standards are overseen by PROFIBUS and PROFINET International.

Modbus

Modbus is a digital communication protocol used by a wide variety of programmable Controllers. The protocol is deployed in a master-servant relationship – 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, operating 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 the protocol. The protocol maps the Common Industrial Protocol (CIP) to Ethernet. The protocol 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 ODVA (Open DeviceNet Vendor Association).

DNP3

Distributed Network Protocol 3 (DNP3) is a digital communication protocol used primarily by programmable Controllers in the Electric and Water & Wastewater sectors. In the electric sector, the protocol is commonly used for substation automation, communicating among RTUs and IEDs. DNP3 normally operates on port 20000. The protocol is overseen by the DNP User Group.

IEC 61850

International Electrotechnical Commission (IEC) 61850 is a suite of digital communication protocols used primarily by Intelligent Electronic Devices in the Electric sector, including for utility automation, between substations, and between substations and control centers. IEC 61850 is normally operates over ports 102 and 10200.

BACnet

Building Automation and Control Network (BACnet) is a digital 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 serial or Ethernet cable. BACnet c is commonly used among Controllers, Engineering Workstations and Supervisory Interfaces. It normally operates on port 47808.

MC Protocol

Mitsubishi Communication (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 among Controllers and normally operates over port 5002.

Controller Area Network (CAN)

Controller Area Network is 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. It is formallly specified in the ISO 11898 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. OPC UA commonly uses port 4840. The OPC standards are overseen by the OPC Foundation.

Message Queueing Telemetry Transport (MQTT)

MQTT is a transportation protocol designed for use by the internet of things (IoT). In particular, the protocol seeks to provide 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. MQTT also offers quality of service levels that can be selected based on need for confirmation of receipt. MQTT commonly uses port 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 but are not limited to Licensed Spectrum, Global Positioning Systems (GPS), Wireless HART, ISA-100.11a, ZigBee, and Software Defined Radio.

Licensed Spectrum

Licensed spectrum describes the permission granted within a regulatory Jurisdiction to exclusively use certain radio frequency ranges. Within the United States, licenses are overseen by the Federal Communications Commission (FCC). Licenses 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, but not limited to, pump stations in the Water & Wastewater Sector or Oil & Natural Gas Sector, Compressor stations in the Oil & 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. These unlicensed bands are commonly known as ISM (industrial, scientific, and medical). They include 5.8Ghz, 2.4 GHz, and sub-GHz bands. Industrial Control Systems and internet of things wireless devices frequently operate in these spectra. It may be difficult to detect and stop intentional and malicious interference with radio communications within these ranges.

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)

Global positioning systems track the geolocation of an electronic device via communications with/from earth-orbiting satellites. These signals enable the accurate and safe operation of automobiles, trains, airplanes, ships, and in some cases, the electric grid (synchrophasors).

Wireless HART

Wireless HART describes 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 Internet of things environments with 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 SDR provides opportunities for improving the robustness and reliability of wireless networks, and for attacking them. Leading providers of SDR solutions include but are not limited to Ettus Research, National Instruments, Lime Microsystems, and HackRF.

Process Safety & Reliability

Process Safety and Reliability is one of the most important concerns in Production Operations, and clearly differentiates industrial cybersecurity from traditional cybersecurity. Terms and concepts for this category include but are not limited to Safety Risk, Functional Safety, Process States, Maintenance Strategies, Control Overrides/Forcing, Process & Product Safety Communications, and Electric Sector Reliability.

Safety Risk

Safety risk describes the potential and possibility of physical harm (including death) to humans (employees and the public) resulting from Industrial Operations. Safety risk can be viewed from

two sometimes conflicting perspectives: the human right to a reasonably safe work environment; and, economic consequences to a business associated with safety events. Key concepts related to safety risk include but are not limited to 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 but are not limited to 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

Numerous and nuanced relationships that exist among 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 a 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 but are not limited to 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 but are not limited to 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 cyber attacks), 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 before-hand 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 nuance.

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 hazard. 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 the assessment.

HAZOP

HAZOP is short for hazard and operability study. This Process Hazards Assessment 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

Failure Mode Effect Analysis (FMEA) is a structured analytical technique for safety, reliability, and quality of a design, function, or process. The analysis seeks to identify Failure Modes – which are essentially causes of failure, and associated "effects" – which 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 & Safety, Plant & Equipment, the Environment, the Business, and Society. Impact analysis informs the determination of a Safety Level/Category for a given Industrial Process. Cybersecurity risk analysis often overlooks these types of impacts.

Human Health

Impacts to human health describe 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 & Safety

Impacts to product quality and safety describe how an event damages the product being produced. In a Manufacturing environment, a reduction in 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 & Equipment

Damage to plant and equipment describes the impacts to 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 burnout, or a Boiler to explode. Full consideration of impacts to plant and equipment can include both replacement cost and lead times.

Environmental Consequences

Impacts of an adverse event include near and long-term effects on the flora and fauna of a region. Environmental effects are influenced by location and elevation of Process Equipment within a facility. For example, location and elevation of a holding Tank or reservoir relative to what is beneath it will influence the results of an overflow or leak.

Business Consequences

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

Societal Consequences

Societal consequences refer to 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 refers to 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 consequence 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 but are not limited to Functional Safety Standards, Safety Instrumented Functions & 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 but are not limited to ANSI/ISA-61511 series/ IEC 61511 series (process industries), ISO 26262 (automotive), EN 50128 (rail transportation), IEC 62304 (medical devices), and IEC 60880 (Nuclear). The confluence of software, safety, and cybersecurity is a complex and evolving area for which standards continue to evolve.

Safety Instrumented Functions & 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 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)

Safety integrity levels (SILs) represent a level of assurance that a Safety Instrumented Function & 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 SIL3 may have redundant input circuits, redundant processors, and redundant output circuits – together 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 Safety Controller by a certification body, confirming that the safety controller conforms to standards for deployment in a certain Safety Integrity Level. Common testing/validation laboratories for safety controllers include but are not limited to 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 a Functional Safety System, which is focused on the Industrial Process itself. 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: "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 to quickly understand and communicate the existing physical conditions. This understanding allows 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 but are not limited to Redundancy, Spares, Maintenance Outages, Predictive Maintenance, and Preventative 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) than 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 in an unused state. Effective use of the spares strategy requires prediction of 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 to add security 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 addressing them. In theory, a temporary intentional outage has lower costs than recovering from a surprise failure. Many vendors provide predictive maintenance software solutions. These include but are not limited to IBM, Microsoft, Honeywell, and GE.

Preventative Maintenance

Preventative maintenance is based on the premise that intervention of an anticipated need is less costly than a repair after failure. While it may be superior to a "wait to fail" strategy, preventative maintenance can result in conducting less-required maintenance, while missing some failures (vs. Predictive Maintenance).

Control Overrides/Forcing

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. In certain circumstances, one controller must take precedence over another controller. Control overrides may be useful to an attacker trying to cause a specific physical effect.

Process & Product Safety Communications

The term "process and product safety communications" describes a variety of safety-related communications relative 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 appropriate, 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 that would be caused by physical destruction of equipment and possible physical harm to employees or the public. Important concepts and terminology for electric system reliability includes but is not limited to 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 describes 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, which requires specialized communication among 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 (volage) 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 occurs when an 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 uses or users from the system – such as by temporarily turning off power to a specified geography or turning off specified air conditioners.

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 reductions to the primary mover – such as providing less fuel to a combustion engine, or adding a resistive load.

Inter-Area Flows

An "inter-area flow" refers to the movement of electricity across service areas of disparate utilities. Coordination among 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 in 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 the electric system may be temporary (transient) in nature – such as a tree or an animal causing a ground fault by contacting electrical equipment. Automatic reclosing attempts to re-establish the flow of electricity in case the fault has cleared – such as the tree is no longer touching the line. Automatic reclosers draw the breaker contacts back together without the need for direct human interaction. Automatic reclosers may be programmed to attempt a 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 composes the grid. SPS actions may affect generating assets (as opposed to Underfrequency or Undervoltage load shedding). Important terms related to special protection systems include but are not limited to SPS Database, and SPS Performance.

SPS Database

The SPS database is a repository of information about the conditions that would trigger a significant reduction (shut down) 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 among necessary power companies and the North American Electric Reliability Corporation (NERC).

SPS Performance

SPS performance refers to a description when the SPS was invoked and 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, "Industrial Cybersecurity Knowledge," describes core terminology associated with industrial cybersecurity. It expresses the relevance of each term, and provides basic nuance for the application of terms within the context of Production Operations and Industrial Control System environments – as opposed to traditional Corporate Networks. Categories include: Guidance & Regulations, Common Weaknesses, Industrial Cybersecurity Events & Incidents, and Defensive Techniques.

Guidance & Regulations

The "Guidance and Regulations" category includes Frameworks & Paradigms, Guidance & Standards, Regulations, Groups & Associations that cover the policy background to industrial cybersecurity.

Frameworks & Paradigms

Frameworks and paradigms are the overarching principles and concepts that guide thinking about industrial cybersecurity. These include, but are not limited to: Critical Function Assurance, Seven Ideals, SRP (Safety, Reliability, Productivity), Five Ds (Deter, Detect, Deny, Delay, Defend), 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 provision of electric power and clean drinking water. Within an aviation context it could include providing thrust and landing gear deployment. To assure means to make sure or certain. Hence, critical function assurance deals with the process of making sure the delivery and performance of the critical function.

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

Seven Ideals

The seven ideals model describe a memorable technique for thinking about Industrial Cybersecurity within an adversarial context. The ideals are: 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. Productivity – the ability to maximize desired output. These characteristics stand in contrast to the confidentiality, integrity, and availability (CIA) triad with which cybersecurity personnel are usually familiar.

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. The five Ds are: Deter – to dissuade an adversary from choosing the organization as a target; Detect – to identify attack attempts; Deny – to provide a challenging first line of defense; Delay – to slow an adversary's progress; 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 & Standards

Guidance & standards refer to the documents intended to direct the development and deployment of 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 & 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 & standards bodies, whose mission is focused on multiple countries; or, national guidance & standards bodies, whose mission is focused on a single country.

International General Industrial Cybersecurity Guidance & Standards Bodies

International guidance and standards bodies for industrial cybersecurity include but are not limited to: International Society of Automation (ISA), International Electrotechnical Commission (IEC), European Network & Information Security Agency (ENISA).

International Society of Automation (ISA)

ISA is a global professional society whose members work in the Industrial Automation Profession. Over 15,000 ISA members participate in the society, with over 100 geographic sections in 33 countries.

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 standard, developed by the ISA99 Committee, is published by ISA as the ANSI/ISA-62443 and published by International Electrotechnical Commission (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 (TR-84), "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 84.00.09-2017, "Cybersecurity Related to the Functional Safety Lifecycle"

ISA-TR84.00.09 addresses integration of 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 advise the general practice of industrial cybersecurity. It has published the IEC 62645 to advise cybersecurity within the electrical and control systems within the nuclear sector.

ISA/IEC 62443 "Industrial Automation and Control Systems Security"

The ISA/IEC 62443 series of standards developed by the International Society of Automation is the leading international consensus-based standard for industrial cybersecurity. Its guiding concepts include: principal control systems roles, 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 International Electrotechnical Commission, describes the application of the ISO 27001 general cybersecurity guidance to Industrial Control Systems used in nuclear power plants.

European Network & Information Security Agency (ENISA)

ENISA is an agency of the European Union (EU) dedicated to promote high levels of cybersecurity across the EU member states. Its initiatives inform the creation of 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 & Standards Bodies

National guidance and standards bodies for industrial cybersecurity are available in at least the following countries: 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 but are not limited to: US National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA). Bodies providing sector-specific guidance and standards for the United States include but are not limited to: Department of Energy.

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 required for application to 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"

NIST SP 800-82 provides guidance on securing Industrial Control Systems – which revision 3 of the document calls "operational technology (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)

DHS is a US federal agency broadly charged with maintaining security within the United States. The agency has primarily 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, DHS has provided resources for Industrial Control Systems security primarily though 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 vulnerabilities.

Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies

Guidance and standards bodies may focus on advising a particular industry or sector. Some of these are national in scope, and others 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 sectors with guidance will change over time, sectors with recognized industrial cybersecurity guidance include, but are not limited to: Transportation, Electric Power, Oil & Natural Gas, Water & Wastewater, Food & 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 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 automotive industry is ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering.

ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering

The ISO/SAE 21434:2021 document, created and promoted by SAE International, that 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. The ISO published ISO 27001 to address cybersecurity in general, and jointly with the International Electrotechnical Commission, published ISO/IEC 27019:2017 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"

The ISO/IEC 27019:2017 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)

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 develop 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 Strategy for Cyber-Informed Engineering.

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 assets, OT assets, and information assets. The guidance consists of 300 cybersecurity practices divided into 10 domains. The way a firm 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 & Natural Gas industries. The organization is composed of some 600 North American corporations who have collaborated to develop over 800 standards, including American Petroleum Institute Standard 1164 "Pipeline Control Systems Cybersecurity."

American Petroleum Institute Standard 1164 "Pipeline Control Systems Cybersecurity"

The API 1164 document describes the 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, 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 "Water Sector Cybersecurity Risk Management Guidance."

"Water Sector Cybersecurity Risk Management Guidance"

This guidance document provided by the American Water Works Association (AWWA) provides water utilities several approaches to quickly improve their cybersecurity posture: it lists 100 prioritized cybersecurity controls across 14 categories; it incorporates a set of questions designed to help water utilities easily recognize areas for improvement; and, it 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" represents 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 non-binding guidance issued by the FDA affirms that cybersecurity is part of Device Safety and the Quality System Regulations. It points device manufacturers to the guidance provided by the National Institute of Standards and Technology (NIST) and the International Society of Automation (ISA), and 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 non-compliance. This topic consists of: Jurisdictions, Regulatory Bodies, Regulation Documents, Audits & Enforcement.

Jurisdictions

A jurisdiction is a 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 but are not limited to 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 – 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 holds the authority.

Governments with Industrial Cybersecurity Regulations

Governments create rules that organize society. Countries have differing processes for creating laws, assigning regulatory authority, and enforcing regulations. Governments that have laws

addressing Industrial Control Systems cybersecurity include but are not limited to the United States and the European Union.

United States Industrial Cybersecurity Regulations

Regulatory bodies in the US include but are not limited to: North American Electric Reliability Corporation (NERC), Nuclear Regulatory Commission (NRC), 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 collaborating to ensure the reliability of the electric system. The US Federal Energy Regulatory Commission (FERC) assigned NERC authority to create and enforce reliability standards. Its regulations relative 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 describing cybersecurity controls that must be applied by owners and operators of the US bulk electric system. Compliance with the standards is assessed by auditors from NERC regional entities. Fines for non-compliance can reach one million dollars 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 and 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 Regulation (CFR) 73.54 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 establish a cybersecurity plan that includes incident response activities.

NRC Regulatory Guide 5.71 "Cybersecurity Programs for Nuclear Facilities"

NRC Regulatory Guide 5.71 describes an approach that NRC staff finds acceptable to complying with 10 CFR 73.54. The Guide offers additional guidance 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 United States Department of Homeland Security charged with the safety of interstate transportation, including aviation, rail, vehicle, and pipeline transportation,

including to enforce 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

TSA Security Directive 1580-21-01A requires all freight railroad carriers and TSA-designated freight railroads within the United States to designate a Cybersecurity Coordinator, report cybersecurity incidents to the Critical Infrastructure and Security Agency, develop a cybersecurity incident response plan, and conduct a cybersecurity vulnerability assessment and report the results to the TSA. Violations can result in civil sanctions of up to about $13,000.

TSA Security Directive 1582-21-01A

TSA Security Directive 1582-21-01A requires all passenger railroad carriers and rail transit systems within the United States to designate a Cybersecurity Coordinator, report cybersecurity incidents to the Critical Infrastructure and Security Agency, develop a cybersecurity incident response plan, and conduct a cybersecurity vulnerability assessment and report the results to the TSA. Violations can result in civil sanctions of up to about $13,000.

Security Directive Pipeline-2021-02C

This directive requires all owners and operators of a hazardous liquid and natural gas pipeline 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 relative to industrial cybersecurity were incorporated into the National Defense Authorization Act of 2022.

National Defense Authorization Act (NDAA) of 2022 (Sections 1541 & 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 Critical Infrastructure and Security Agency (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 from time-to-time, orders 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, Executive Order 13920 Securing the United States Bulk-Power System (revoked). Additional orders with broad impact on industrial cybersecurity may be issued in the future.

Order 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 National Institute of Standards and Technology 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 application of the framework. It required the Department of Homeland Security (DHS) to identify critical infrastructure where a cybersecurity incident could have devastating regional or national effects, and to notify owners and operators of identified infrastructure.

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience

PPD 21 is a companion document to EO 13636 issued in 2013 by President Obama. It directs the Department of Homeland Security to align federal efforts for coordination with critical infrastructure owners and operators, with a focus on information sharing.

Executive Order 13920: Securing the United States Bulk-Power System (revoked)

Based on the premise that foreign adversaries are increasingly creating and exploiting vulnerabilities in the US bulk power system (generally considered “the electric grid”), EO 13920, issued by President Trump in May 2020, intended to prohibit acquisitions of 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 European Union (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 for expertise to support cybersecurity preparedness and cooperation among member states. The act emphasizes ENISA’s role in helping 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 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

Regulation documents describe requirements to which a regulated entity will be held by Audits & Enforcement. 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 & Enforcement

These concepts describe the process by which a Regulatory Body or its agents check whether the regulated entity complies with mandatory requirements. Consequences for noncompliance may include fines.

Industrial Cybersecurity Groups & Associations

Groups and associations consist of efforts to promote industrial cybersecurity that are primarily forums for collaboration – often among individual professionals. These include but are not limited to: International Society of Automation (ISA), Information sharing and analysis centers (ISACs), and Professional Conferences.

Information Sharing and Analysis Centers (ISACs)

ISACs are non-profit 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 among participants on Web sites, 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, a 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 include, but are not limited to 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 but are not limited to Managerial Weaknesses, System & Host Weaknesses, Network Weaknesses, and Instrumentation & Control Weaknesses. Many of these weaknesses result from the different priorities perspectives, priorities, and training in IT vs OT personnel and systems.

Managerial Weaknesses

Managerial weaknesses affecting industrial cybersecurity originate at a leadership and governance level within an organization. Weaknesses within this category include but are not limited to: Lack of Sponsorship & Resources, Inadequate Consideration of ICS Cybersecurity Risk, Lack of Stakeholder Alignment, Lack of Cybersecurity Awareness & Training, No ICS Cybersecurity Program, No ICS Security Policies, Contingency Plans Lack ICS Focus.

Lack of Sponsorship & Resources

Sponsorship and resources refer 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 the risk, and is committed to address 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 & Training

Awareness and training efforts are pivotal to altering attitudes and behaviors relative to cybersecurity. While many organizations offer annual or semi-annual 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 critical Industrial Control 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. ISA/IEC 62443 recommends elements of a high-quality ICS cybersecurity program.

No ICS Security Policies

Policy is an indispensable element of an industrial cybersecurity program. Cybersecurity policies for industrial operations professionals, including but not limited to Engineers, Technicians, Process Operators, and Control Room Operators often do not exist. Policies should clearly describe: the aim of the policy, to whom the policy applies, the practices that must be followed, the manner of enforcement, and the consequences of non-compliance. Individuals to whom the policy applies should be trained in its implementation. Policies should have a process for requesting and documenting exception and be periodic review and improvement.

Contingency Plans Lack 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 both IT and OT systems. Such lack of planning will increase and prolong undesirable impacts.

System & 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 but are not limited to Lack of Authentication Requirements, Lack of Software Integrity Mechanisms, Lack of Physical Access Controls, Lack of Least Privilege, Lack of Software Backups, Lack of 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 asserting one's identity and authority. This is commonly accomplished though passwords and, more commonly with additional factors such as one-time tokens. Within an Industrial Control System environment is it 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 represents a serious concern. In addition, Panel-Based HMIs are almost never configured to require authentication – meaning that anyone with physical access to the 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 findings.

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 only run signed code, thus bypassing an important integrity mechanism. Some Panel-Based HMIs do have the ability to enforce 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" refers to factors that limit individuals from physically accessing (touching) control systems 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 HMIs to be physically accessible to anyone within the facility. Control enclosures are frequently left unlocked without video surveillance or Security Alerts indicating that the enclosure has been opened.

Lack of Least Privilege

Least privilege refers to conferring only the minimum permissions upon a user that a user needs to complete their expected tasks. While some control system software, including Supervisory Interfaces, Process Data Historians, and human machine interface design software includes 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 refers to 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 reliance 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 Software Upgrade Path

Lack of upgrade path refers to the obsolescence of currently operational control systems technology. For instance, new hardware that offers encrypted communications protocols does not offer backward compatibility with older hardware. Worse yet, 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 the design and modification of Industrial Control Systems. Software used to program Controllers and Operator Interfaces is frequently downloaded from vendor Web sites 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. The 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. The operational requirements of industrial environments may restrict the ability to deploy patches in a timely manner. This challenge is amplified by 1) Unrecognized Third-Party Relationships; and 2) Lack of awareness of vulnerabilities and patches.

Unassured Provenance

Unrecognized provenance refers to the general opacity of where and how a product is made and delivered. 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 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 incorporate a cryptographic libary 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

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 indicates 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 work within or interfacing to vendor-provided solutions such as Process Data Historians. Code quality and security development lifecycle practices for such user-generated code are expected to vary widely. However, 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 but is not limited to 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 the extension and application of 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, 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 that physical programming switches could be used to disallow remote programming of Controllers. The result is that for many commonly deployed process control network protocols,

anyone connecting to a controller can reprogram the controller, 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 themselves. The significance of this weaknesses 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, the important question remains of designing valuable alerts, deciding who will receive the alerts, and determining what action to take for each alert.

Poorly Managed Temporary Network Nodes

A temporary network node could take various forms, such as a Technician 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 different organizations altogether (such as to a contractor), making it difficult to assure 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 an 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 administrator.

Unauthorized Wireless Networks

A wireless network can provide 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 & Control Weaknesses

Instrumentation and control weaknesses affects Controllers, Sensors, and Actuators. Its components include but are not limited to Programmable Physical Damage, Poor Controller Coding Practices, 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 Engineers nor 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, in 2016 the controller interoperability organization, PLCopen, published "PLC Code Quality" recommendations. In 2020, a grassroots group 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, manipulation of the sensor/transmitter signal/data provides an opportunity to disrupt the controlled process. Transmitters and their corresponding IO cards on common Controllers do nothing to ensure the integrity of the signal/data. This may allow for supply chain compromise of the transmitters, transmitter calibration/scaling attacks, physical manipulation of the sensors (such as moving the location of 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 & Incidents

An industrial cybersecurity event or incident involves undesirable consequences due at least in part to poor control system design, control system malfunction, or intentional cyber attack, that affected Production Operations. Identifying and analyzing industrial cybersecurity events and incidents provides essential learning experience. This category includes a list of Industrial Cybersecurity Events and Incidents Cases, and a representative list of Analytical Concepts that can be applied thereto.

Industrial Cybersecurity Events & Incidents Cases

This non-exhaustive 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, 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 Department of Homeland Security 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 of 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 with collaboration from other countries, disrupted Iran's nuclear weapons program by attacking Engineering Workstations and programmable logic controllers (PLCs) within 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 USB, 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 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 of the city. The outage was triggered my 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 – 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 affect that 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 nicely 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, among 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 they 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 their cars 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 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. Investigation found that the event was precipitated by a poorly anchored Sensor conduit, relocation of safety sensors, imprudent Controller Programming, and 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, D.C. 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 speed of 49 miles per hour, killing eight people and injuring 80 more. While not an intentional cyberattack, the incident demonstrates the dangers of reliance 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 a 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 were compromised (lost and/or 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 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 & 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, but are not limited to Tactics, Techniques & Procedures (TTPs), Targeting, IT vs OT Vectors & Impacts, and Root Cause Analysis.

Tactics, Techniques & Procedures (TTPs)

Tactics, techniques, and procedures (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 attacks. 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 allows 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 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 protecting operational systems, it is key to recognize that adversaries can operate throughout Lifecycles and Supply Chains.

IT vs OT Vectors & Impacts

Information technology (IT) and Operational Technology (OT) are useful concepts to differentiate between the fundamental purpose 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 Design 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, but are not limited to: Root Causes, Investigations, Internal vs External Causes, Deliberate vs Unintended Effects, and Lessons Learned.

Root Causes

Root causes are the fundamental reasons an event occurred. Within industrial cybersecurity, these are likely to be combination 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 vs 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 vs 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 are the opportunities to avoid similar results in the future. Lessons learned documents and briefings are valuable inputs to developing self-evaluations and rich training scenarios. Organizations would also do well to also develop lessons learned for near-miss events. Lessons learned

provide significant opportunities for interdisciplinary teams from both 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 & Host, and Instrumentation & Control. Security professionals must recognize and consider the strengths and weaknesses of respective classes and techniques. In addition, security professionals should identify and proficiently employ tools that implement defensive techniques.

Managerial Defensive Techniques

Managerial defensive techniques describe key concepts and approaches that guide cybersecurity at an organizational level rather than a technical level. These techniques include but are not limited to: Industrial Cybersecurity Champion, Awareness & Training for ICS-Related Personnel, ICS Security Program, Cybersecurity Risk Management, ICS security Policies, Lifecycle Management, Contingency Plans with ICS Focus, Incident Response Plans with ICS Focus, Security Operations Center for ICS, Managed Security Services, Professional Ethics, Privacy Assurance.

Industrial Cybersecurity Champion

Industrial cybersecurity champion refers an organizational leader who can marshal the resources to seriously 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 & Training For ICS-Related Personnel

Personnel that should receive role-specific training in industrial cybersecurity include, but are not limited to: 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 ISA/IEC 62443 and NIST Special Publication 800-82.

Cybersecurity Risk Management

Simply put, "cybersecurity risk management" describes the balance of what could go wrong with information technologies and operations technologies with what should be done to prevent it from going wrong. Within a Production Operations environment, components of this topic include but are not limited to: Stakeholders, Integrated System Model (Asset Inventory), Adversary Mindset, Threat Intelligence, Vulnerability Intelligence, and Safety vs Security.

Stakeholders

Stakeholders are the groups and individuals that 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 allow the security team to efficiently make accurate decisions. The integrated system model allows the security team to answer questions such as: 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 controller use? Who has access to those controllers? Who is responsible to update the controller firmware? Where is the backup of that controller's logic?

Adversary Mindset

Adversary mindset refers to 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 uncomfortable questioning of assumptions and encourages exploration of "the possible" rather than taking comfort in "the probable." In a Production Operations environment, 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 security posture. For example: a rising trend in cyberattack-for-ransom, escalating geopolitical tensions, mergers involving foreign firms, and 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 relevant list of relevant terms for which 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. 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 refers to the intentional effort to identify known software vulnerabilities that affect the products on which an organization relies. 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.

Safety vs Security

Risk management within industrial environments requires the adaptation of 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 generally consider that security prevents and mitigates the consequences of unauthorized access to information systems. Because industrial automation connects physical processes to information systems, both paradigms must be fully understood and considered.

OT/ICS Security Policies

ICS security policies and procedures are intended to ensure that employee actions keep the system within risk tolerance. ICS security policies should clearly identify to whom the policy applies, provide the rationale for the policy, clearly describe the procedure by which the policy is followed, describe how compliance is monitored, identify consequences of non-compliance, and describe the process for seeking exception to the policy. Examples of ICS security policies could include but are not limited to management of transient devices, contractor/vendor Remote Access, 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; but rather, require special considerations for industrial environments.

Lifecycle Management

Operations Environments are the culmination of numerous Lifecycles, including but not limited to product development, process development, facility development, and software development. Each lifecycle extends from initial idea conception, through include Design, Specify & Procure, Build, Operate & Maintain, Support, and Dismantle. 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" describe security controls applicable when Control Systems Asset Owners or Integrators acquiring 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 removal of network connectivity, implementation of restrictive subnets, deployment of protocol-aware firewall rules, and hardware replacement plans.

Secure Software Development Lifecycle

Secure software development lifecycle includes a group of recommended practices to ensure software quality from initial software design through software end-of-life/end-of-support. The topic applies primarily to those developing ICS software, both at Control Systems Vendors and Control System Operators. ISASecure offers the Secure Software Development Lifecycle Assurance Certification for vendors to demonstrate conformance to recommended development practice.

Secure development practices should also apply to PLC programmers, HMI programmers, SCADA programmers, and Process Data Historians programmers/users. Programmers of 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 OT/ICS Focus

Contingency plans are carefully designed instructions for how an organization will respond to a specific situation before that situation occurs – including who is responsible to take each identified action. Organizations that own or operate Industrial Control Systems should prepare contingency plans that allow them to maintain critical production operations in the face of cybersecurity events. For example, a contingency plan to deal with cyberattack-for-ransom may

include a pre-made decision of 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 control system and network architecture.

Incident Response Plans with 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. ICS focus means that Positive Controllability of the Industrial Process, and human safety are paramount considerations during 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 procedures 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 choose 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 from 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). These security alerts are passed to security personnel within the Security Operations Center for action. It is important that each security alert and corresponding course of action be documented, and that appropriate stakeholders (including both corporate cybersecurity personnel and process operations personnel) be trained in following these courses of action.

Managed Security Services

Many organizations determine to rely on the security expertise of external providers for ongoing detection and various tiers of incident response. These external solutions are known "managed security service." 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.), and how events will be communicated to the appropriate parties (i.e., specified recipients of event detection).

Professional Ethics

Professional ethics refer to a standard of conduct directly relative 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 highest levels of technical competence, trustworthiness, and responsibility at all times, including continuous concern for the security of one's own work and person.

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 but are not limited to 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 but are not limited to: 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 & Observation, Analysis of Security Data, Secure Remote Access, Software Defined Networking, Data Diodes, Wireless Communications Analysis, Deceptive Technologies, and Security-Enhanced ICS Network Communications & Protocols.

Secure Network Architecture

Network architecture refers to 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 IEC 62443 standard, achieves this by overlaying the Purdue Enterprise Reference Architecture 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 activation of Contingency Plans (such as network isolation or 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 creation of and reliance on alternate secure architecture approaches.

Network Boundaries

Network boundaries describe what group or individuals are responsible for what 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 to administer and maintain 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 both the IT and OT networks. 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 is 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 to not worry about managing the security of the process control network. In such cases, a virus that spreads via 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 Process Data Historians, that has IP addresses on both the corporate network and process control network. Alternate approaches to “air gap” include data diodes, dual-firewall DMZ, and intertied airlock.

Management of Ports & 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 opportunity exists for attack. Hence, good practice requires industrial cybersecurity professionals to understand the ports and services that are truly required 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 change a Set Point.

Process Control Network Anomaly Detection

Process Control Networks are typically static in comparison to enterprise networks – devices are not 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, determining what action to take on each alert, and assigning the actions to the appropriate personnel requires the expertise and collaboration of process Engineers, field Technicians, and Process Operators.

Quarantine & Observation

Isolating and testing equipment suspected of malicious behavior is an important defensive technique. Examples of quarantine and observation used in operations environments include but are not limited to: security review as part of site acceptance test, staged/limited roll-out of a new technology, and 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, multi-factor authentication, time-based controls, Process Control Network Firewalls, and the use of carefully monitored jump boxes, can help assure these connections against malicious use.

Software Defined Networking

When thoughtfully used in industrial environments, software defined networks can provide rapid configurability that speeds deployment of 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 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 level 0-1, Wi-Fi at Purdue level 1-2, and cellular, licensed spectrum, and even satellite at Purdue level 2-3 and higher. The advent of Machine-as-a-Service, and Bring-Your-Own-Network (BYON) adds additional complexity to wireless network management. Careful detection and analysis of wireless communication helps ensure clear and accurate transmission and 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 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), release of malware into simulated Process Control Networks, creation, and operation of sock-puppets (such as fake profiles of non-existing 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 & 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 & 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) within an Operations environment. Such techniques include but are not limited to Device Hardening, Device Monitoring, Software/Firmware Updates, Software Integrity Mechanisms, Passwords & Credential Management, Physical Security, and Hardware Reviews.

Device Hardening

Device hardening refers to changing the configuration of a device 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" which disallows attempts to obtain the code from the PLC. Some PLCs offer "code binding" which only allow 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 deployment of a software agent onto the host operating system that monitors various aspects of the host for suspicious or malicious activity. Antivirus software and application whitelisting 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 local Operator Interfaces (e.g., HMIs), Controllers, Configurators, and Transmitters.

Device monitoring solutions such as antivirus 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 latest versions is an important way to remediate known weaknesses within vendor-provided control system software. Control system vendor capability 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 for 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 careful consideration of 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 within 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 both 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 & 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 applies to all users during the system lifecycle, protects the system, minimizes management effort, and prioritizes 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 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), detailed security review of all potentially electronic subsystems may transcend the purchaser's expertise, and thus may require coordination with government resources.

Instrumentation & 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 but are not limited to 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 representation of real-world conditions; 2) Control Logic appropriately considers all relevant process variables; 3) Actuators faithfully implement the dictated control decisions (controller outputs or supervisory commands). Positive control may be achieved by Sensor/Transmitter Integrity Assurance Mechanisms, Controller Security, and diverse Principles of Operation.

Cyber-Informed Engineering (CIE)

Cyber-Informed Engineering is an approach for incorporating cybersecurity concepts within engineering education and practice. While retrofitting existing systems is within 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 cyber attacks.

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 to: 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, 5) 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 refers to adopting an adversarial mindset and 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 cyber-attack against an Industrial Control System.

Special Consideration of Safety Functions

Safety Instrumented Functions & Systems intend to protect the physical welfare of facility personnel and the public at large. As such, they represent a high value target, and merit special cybersecurity consideration.

Cyber-Physical Fail-Safes

A cyber-physical fail-safe is an engineered mitigation that prevents a physical impact or consequence that otherwise would result from a cyberattack. Examples of cyber-physical fail-safes include but are not limited to 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 but are not limited to: 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

Changing the Control Logic for the Industrial Process provides an opportunity for an adversary to cause significant (physical) consequences. 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 review of 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 consequence; 4) to determine whether the control logic is intentionally malicious. Inspection should check 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 cyber attacks. These practices include, but are not limited to: Control Data Validation, Centralize Operational Logic in the Controller (vs HMI), Allocate Controller Memory 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) historic values. Values outside of set limits should not allow manipulation of output. Control data validation topics include but are not limited to 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 from 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) checking whether a value provided by a Controller Data Source is reasonable before acting on that value. One technique for 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 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) checking 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.

Centralize Operational Logic in The Controller (vs 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.

Allocate Controller Memory by Function

The individual programming the Controller may choose to designate specific memory areas (*e.g.*, blocks of register addresses) to specific 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 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 entry on Industrial network firewalls).

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 highest concern (see entry for Secure controller programing for additional discussion of validating write commands). It is

important to note that proper implementation of these firewall/network monitoring 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 what function.

Controller Self-Diagnostics

This topic refers to reliance on 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 but is not limited to: Configuration Change Monitoring, Controller Performance Monitoring, Controller Error Monitoring, and Controller Alerts.

Controller Configuration Change Monitoring

Some Controller models allow for controller configuration changes to be used as tags. These tags can be used in the controller logic, displayed on the HMI, or passed elsewhere. This functionality should be turned on because configuration changes may indicate malicious activity.

Controller Performance Monitoring

Controllers may allow for controller data such as CPU usage, CPU temperature, CPU shutdown and CPU restart, to be available to users. Unexpected events or deviations from 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 for error logging and reporting. For example, mathematical errors such as divide by zero, counter overflow, and negative counter can be logged and reported as a potential indicator 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 to the Security Operations Center for OT/ICS as a 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 but are not limited to: Prevent Simultaneous Assertion of Exclusive System States, Define a Safe Process Restart State, Enable Conservative Control, Make Appropriate Stakeholders Aware of the Process State, and Trap Manipulation of Process State Variable.

Prevent 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 enforces the exclusivity. This lack of enforcement may enable attacks to achieve physical consequences. Where possible, Cyber-Physical Fail-safes should prevent simultaneous assertion of exclusive system states. Where not possible, Control Logic should intentionally disallow such violations of state.

Define Safe Process Start State

The Controller should check Process State on each start-up (including for 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 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 Process State is an intentional component of control system safety design that ensures 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.

Trap Manipulation of Process State Variable

Attackers may attempt to cause damage or to distract operators by manipulating the Process State variable) to cause a false alarm or to suppress a legitimate Alarm. Control Logic can be written to detect such manipulation by monitoring the process state variable itself, 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 comparison of Process

Variables and Set Points to historic or reasonable ranges. The result of such analysis (a Security Alert) is detective rather than preventative 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 but are not limited to the presence of hardware and software implants, intentional miscalibration, re-scaling, and man-in-the middle attacks against communications. The deployment of single pair ethernet may expand the available attack surface for sensors/transmitters. Specific mechanisms to assure sensor/transmitter integrity include but are not limited to: Emanations Monitoring of Transmitters, Independent Sensing & Transmission, 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 fingerprinting” can trigger a Security Alert to appropriate stakeholders when anomalies are detected.

Independent Sensing/Transmission & Backhaul

Independent sensing/transmission and backhaul refers to the use of multiple and diverse Sensors/Transmitters and communication channels (backhaul) for important Process Variables. Data from the multiple sensors/transmitters may be sent to the Controller or to a Process Data Historian or security information and event management (SIEM) tool. The use of independent communications channels may also help resist network-based attacks. Significant discrepancies between the values provided by both 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, as this technique could cause questioning of which reading were more accurate. Analog and non-networked digital readouts may be particularly useful as a ground truth independent sensor given their resistance to cyberattack.