Dispositions of Survey Responses

This document describes the final dispositions taken for each of the suggestions made by survey respondents.

The document is organized into three sections, one for “Methodology”, one for “Foundational Control Systems Knowledge”, and one for “Industrial Cybersecurity Knowledge”. These last two align to sections two and three of the survey.

Methodology

This list became a strawman about which to elicit further expert insight. Between January and March 2022, ISU, INL and the International Society of Automation (ISA) I administered a survey to 175 respondents with interest and experience in industrial cybersecurity. The survey asked respondents to share their thoughts about the strawman categories and topics to form the basis for curricular guidance. The survey included three sections: 1) Respondent background, 2) Industrial control system knowledge, and 3) Industrial cybersecurity knowledge.

The survey asked respondents to rank each category and topic for relevance, and then choose whether to keep as is, change name, or remove entirely. If respondents chose change name or remove entirely, they were prompted to make an alternate suggestion or justify their desire to remove the category or topic.

For such responses, a review committee representing academia, industry, and government considered each suggestion and made final dispositions into one of five categories:

- “Directly accepted” means that the suggestion was incorporated as-is or very nearly as-is.

- “Indirectly accepted” means that the core element of the suggestion was incorporated, but with minor changes, such as using an alternate term, or adding the suggestion as a subtopic in another category.

- “Note” means that the suggestion would help curricular designers and/or instructors clarify and interpret the guidance.

- “Insufficient detail provided” means that a respondent indicated that they would like a change, but then did not describe the change they would like to have. We have treated these differently than “no change” because it is possible that changes made in response to other input also addressed the unstated reason for the response.

- “No change” means no action was taken on the respondent’s input.

Dispositions of “No change” were further placed into one of four categories: Already included, Just commentary, Out of scope, Otherwise not persuasive.

- “Already included” means that the suggestion was already covered within the strawman.

- “Just commentary” means that the response did not include an actionable suggestion.

- “Out of scope” means that the suggestion went beyond the intended scope of the request for input. This commonly occurred when input dealt with content that would normally be covered in a traditional cybersecurity course or program.

- “Otherwise not persuasive” means that the review committee chose to not include the suggestion, but for reasons outside of the other four.

A detailed record of each suggestion and disposition can be found in the EXCEL FILES.

Foundational Industrial Control Systems Knowledge

This section discusses the dispositions of respondent input for Foundational Industrial Control Systems Knowledge.

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

Category	Topic	Count	Keep as-is	Change title	Remove
Instrumentation and Control		93	94%	5%	1%
	Programmable control devices	71	99%	1%	0%
	Control system software	71	99%	1%	0%
	Alarms	71	97%	3%	0%
	Operator interfaces	71	97%	3%	0%
	Control paradigms	71	96%	4%	0%
	Data acquisition	71	96%	3%	1%
	Supervisory control	71	96%	1%	3%
	Programming methods	70	96%	4%	0%
	Process variables	71	94%	1%	4%
	Process data historian	71	94%	1%	4%
	Sensing elements	71	93%	7%	0%
	Control devices	71	93%	6%	1%
	Engineering laptop/workstation	71	92%	6%	3%
Industrial Communications		93	90%	8%	2%
	Industrial Communication Protocols	70	99%	1%	0%
	Reference Architectures	70	97%	1%	1%
	Transmitter Signals	70	94%	1%	4%
	Fieldbuses	63	95%	0%	5%
Safety		93	86%	10%	4%
	Safety Instrumented Functions	68	97%	1%	1%
	Electrical Safety	68	97%	0%	3%
	Safety/Hazards Assessment	68	96%	0%	4%
	Common Failure Modes for Equipment Under Control	68	96%	1%	3%
	Safe Work Procedures	68	93%	1%	6%
	Lock-out Tag-out	68	91%	1%	7%

	Personal Protective Equipment	68	90%	0%	10%
Equipment Under Control		93	85%	11%	4%
	Valves	70	96%	3%	1%
	Motors	70	94%	3%	3%
	Pumps	70	94%	3%	3%
	Variable frequency drives	70	93%	3%	4%
	Generators	69	94%	1%	4%
	Relays	70	91%	7%	1%
	Breakers	70	91%	3%	6%
	Transformers	69	91%	1%	7%
Industrial Operations Ecosystem		92	82%	16%	2%
	Industry Sectors	77	97%	3%	0%
	Professional Roles and Responsibilities	77	96%	4%	0%
	Organizational Roles	77	96%	0%	4%
	Process Types	78	95%	3%	3%
	Industrial Lifecycles	77	96%	3%	1%
	Facilities	77	95%	5%	0%
	Engineering Diagrams	76	93%	5%	1%

Over 90% of respondents chose “keep as is” for all but three items: Industrial operations ecosystem (82%), Equipment under control (85%) and Safety (86%).

Notwithstanding this general indication of acceptability, the expert committee wanted to consider each suggestion for improvement on its own merits. Seventy-six respondents provided a total 342 suggestions. As some responses included multiple parts, this gave an atomized quantity of 461 responses. One respondent offered 47 suggestions. Forty-five respondents offered just one or two suggestions. In addition, four responses from the Industrial Cybersecurity Knowledge Section were moved into the Foundational Industrial Control Systems Knowledge Section, bringing the total to 465 responses.

Overall, of the 465 responses provided, 278 (60%) were incorporated into the guidance. A summary of the final dispositions into the mutually exclusive dispositions is shown below.

Final disposition	**Count**
Directly accepted	91
Indirectly accepted	158
Note made in guidance document	29
Referred to cybersecurity section	53

Insufficient detail provided	53
No change	81
Total	**465**

Survey responses for which no change was made

The 81 suggestions for which no changes were made were classified into the following four categories:

Category for "No change"	**Count**
Already included	7
Just commentary	6
Out of scope	22
Otherwise not persuasive	46
Total	**81**

The most common suggestion for which no change was made, dealt with networking technologies. While such suggestions were generally out of scope (because the scope was limited to topics not covered in a traditional IT, computer science, or cybersecurity program), these suggestions highlight the importance of including traditional networking topics to adequately prepare industrial cybersecurity professionals. It is also important to recognize that networking topics are not normally covered in the educational pathways of engineers and technicians. Industrial cybersecurity professionals should also be taught select IT, networking, and computer science topics. These topics are to be included in the Industrial Cybersecurity Model Curricula, but not in the Industrial Cybersecurity Curricular Guidance – Knowledge document.

Description of changes to Foundational Industrial Control Systems Knowledge Section

The most significant changes were: 1) alterations to category titles; and 2) the addition of subtopics. The guidance grew from 45 total items in the strawman to 139 items based on respondent suggestions. When incorporating the changes suggested, the review committee added an additional 216 items, bringing the total to 355. These changes enhance the utility of the guidance by providing increased clarity and specificity.

The strawman presented in the survey and the updated guidance are provided below. The updated guidance shows changes that resulted from survey responses in red, and additions by the expert review committee in blue.

Several items appear in the list more than once. This emphasizes the importance of the repeated topics within several contexts.

Strawman Proposal – as Presented in Survey

Industrial Operations Ecosystem
Industry sectors, Professional roles and responsibilities in industrial environments, Organizational roles, Facilities, Engineering diagrams, Process types, Industrial life-cycles

Instrumentation and Control
Sensing elements, Control devices, Programmable control devices, Control paradigms, Programming methods, Process variables, Data acquisition, Supervisory control, Alarms, Engineering laptops/workstations, Process data historians, Operator interfaces, Control system software

Equipment Under Control
Motors, Pumps, Valves, Relays, Generators, Transformers, Breakers, Variable Frequency Drives

Industrial Communications
Reference architectures, Industrial communications protocols, Transmitter signals, Fieldbuses

Safety
Electrical safety, Personal protective equipment, Safety/Hazards assessment, Safety Instrumented Functions, Lock-out tag-out, Safe work procedures, Common failure modes

Resulting Guidance with Changes Shown

Changes made as result of survey responses appear in red. Additions made by committee appear in blue.

Industrial Operations Ecosystem

Business Context, Geopolitical Context, Professional Context, Industry Context

Business Context: Production Operations, IT vs OT, Organizational Roles, Supply Chain, Supply & Demand, Capital Budget & Expense, Cost Center vs Profit Center, Cost-Benefit Analysis, Human Capital, Business Continuity, Regulation, Business Risk

Organizational roles: Industrial Control Systems Vendor, Industrial Control Systems Integrator, Industrial Control Systems Owner/Operator, Industrial Control Systems Maintenance Provider

Geopolitical Context: Natural Resources, National Boarders, Technological Development, Critical Infrastructure, Conflicts, Military, State-Owned Enterprises, Demographics, State Security Services, Capabilities, Geopolitical Risk

Professional Context: Professional Roles & Responsibilities, Workplace Safety

Professional Roles and Responsibilities: Engineer, Technician, Process Operator, Control Room Operator, Shift Supervisor, Plant Manager, Chief Operating Officer, Ethics, Operational Security (OPSEC)

Workplace Safety: Electrical Safety, Personal Protective Equipment, Lock-Out Tag-Out, Safe Work Procedures, Safety Regulations, Workplace Safety Communications

Industry Context: Industrial Processes, Industry Sectors, Facilities, Engineering ~~diagrams~~ Documentation, Industrial Lifecycles

Industrial Processes: Continuous, Discrete, Batch

Industry Sectors: Electric Power, Oil & Natural Gas, Petrochemical, Food & Pharmaceutical, Mining & Metals, Manufacturing, Pulp & Paper, Water & Wastewater, Buildings, Transportation, Nuclear

Facilities: Facility Type, Facility Planning & Design, Facility Location, Facility-Wide Services

Facility-Wide Services: Electric Power, Heating Ventilation & Air Conditioning, Compressed Air, Lighting, Fire Protection, Physical Security

Engineering Documentation: Facility Drawings, Process Flow Diagrams, Piping & Instrumentation Diagrams, Loop Diagrams, Wiring Diagrams, Product Specifications, User Manuals

Industrial Lifecycles: Design, Specify & Procure, Build, Operate & Maintain, Support, Dismantle, Asset Management, Change Management

Change Management: Integrated System Model/Inventory, Device Configurations, Software & Hardware, Recalls, Errata, Release Notes, Software Bill of Materials, Backups, Change Records

Instrumentation ~~and~~& Control

Industrial Control Systems, Control Theory ~~paradigms~~, Control System Components, ~~Sensing elements, Control devices, Programmable control devices,~~ Programming & Control Logic ~~methods~~, ~~Data acquisition, Supervisory control,~~ Alarm Management, Control System Software

Control Theory: Control Loop, Set Points, Process Variables, Control Variables, Primary Control Elements, Final Control Devices, Feedback, Open & Closed Loop, Process Dynamics, Process Dynamics, Error, Control Algorithms, Control Strategy, Loop Tuning, Simulation & Modeling, Deadband & Dead Time

Control System Components: Control Centers, Control Rooms, Control Panels, Control Enclosures, Operator Interfaces, Engineering ~~laptops/workstations~~ Computers, ~~Process data historians~~ Application Servers, ~~Variable frequency drives~~ Controllers, Motor Controllers, Sensors & Transmitters

Operator Interfaces: Supervisor Interface (SCADA HMI), Panel-Based/Skid-Mounted Interface (HMI), Human-Machine Interface Design

Engineering Computers: Engineering Workstations, Technician Laptops, Contractor Computers, Tablets, Process Analyzers, Calibrators & Configurators

Application Servers: Process Data Historians, Manufacturing Execution Systems (MES), Enterprise Resource Planning (ERP)

Controllers: Relays, Controller Hardware, Input/Output, Memory, Tags, Program Scan, Programming Key Switch, Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), Remote Terminal Units (RTUs), Intelligent Electrical Devices (IEDs), Protective Relays, Safety Controllers, Soft PLCs

Motor Controllers: Motor Starters, Adjustable Speed Drives, Motor Protection, Motor Control Center, Smart Motor Controllers

Sensors & Transmitters: Sensors, Transmitters, Units of Measure, Transduction, Principles of Operation, Temperature, Pressure, Level, Flow, Calibration, Scaling, Transmitter Failure Mode, Transmitter Security, Meters, Smart Instrumentation

Programming & Control Logic: IEC 61131-3, Ladder Diagram, Function Block Diagram, Structured Text, Instruction List, Sequential Function Chart, Controller Code Quality (

Alarm Management: Alarms, Alarm Management Lifecycle, Consequence Severity, Alarm Prioritization, Alarm States, Alarm Performance, Safety Alarms

~~**Equipment Under Control**~~

Process Equipment (1 red)

Actuators, Electric Motors, Pumps, Compressors, Valves, Piping, Conveyors, Tanks & Vessels, Electric Power System Equipment, Turbines, Process Heating & Cooling, Process Chemistry, ~~Relays, Generators, Transformers, Switchgear, Breakers, Variable Frequency Drives~~, Robotics, Motion Control, Vision Systems, Air Handling Equipment, Filters & Scrubbers, Engines, Ingress/Egress Equipment, Safety Equipment, Medical Machines, Skid-Mounted Systems, Smart Devices/Equipment

Actuators: Mechanical Actuators, Motor-Controlled Actuators, Hydraulic Actuators, Pneumatic Actuators

Tanks & Vessels: Tank Shape, Tank Materials

Electric Power Equipment: Generators, Conductors, Insulators, Bushings & Arrestors, Transformers, Switchgear, Batteries, Capacitors

Process Heating & Cooling: Boilers, Heaters, Heat Exchangers, Furnaces, Distillation Columns, Refrigerators & Freezers, Industrial Chillers, Cooling Towers

Process Chemistry: Crackers, Reactors

Motion control: Axis, Motion Types, Acceleration & Deceleration

Safety Equipment: Safety Valves, Safety Switches, Limit Switches

Skid-Mounted Systems: Machine-As-A-Service

Industrial Networking & Communications

Network Architecture & Integration, Data Management, Network Equipment, ~~Industrial communications Network protocols, Transmitter signals, Fieldbuses~~ Signals & Protocols, Wireless Communications

Network Architecture & Integration: Reference Architectures, Enterprise Systems, Remote Access, Third Party Systems, Cloud Services, Edge Computing, Machine-to-Machine, Bring-Your-Own-Network

Reference Architectures: Purdue Enterprise Reference Architecture, Converged Plantwide Ethernet, Levels, Zones, Cells, Conduits

Levels: Process Control Network, Corporate Network

Data Management: Data, Data Source, Data Path, Data Storage (Process Data Historians), Data Use

Data use: Process Control, Supervisory Control, Process Analytics, Manufacturing Execution Systems, Predictive Maintenance Systems

Network Equipment: Industrially Hardened Network Equipment, Protocol Converters, Leading Network Equipment Vendors

Signals & Protocols: 4-20mA, 0-5V, Highway Addressable Remote Transducer (HART), Foundation Fieldbus, Profibus & Profinet, Modbus, EtherNet/IP, DNP3, IEC 61850, BACnet, MC Protocol, Controller Area Network (CAN), Open Platform Communications (OPC), Message Queueing Telemetry Transport (MQTT)

Wireless Communications: Licensed Spectrum, Global Positioning Systems (GPS), Wireless HART, ISA 100.11, ZigBee, Software Defined Radio

~~Safety~~ Process Safety & Reliability

~~Electrical safety, Personal protective equipment,~~ ~~Safety/Hazards~~ Safety Risk, Functional Safety, Process State, ~~Lock-out tag-out, Safe work procedures,~~ ~~Common~~ Maintenance Strategies, Control Overrides/Forcing, Process & Product Safety Communications, Sector-Specific Approaches

Safety Risk: Causes of Safety Risk, Process Hazards Assessment, Impact Analysis, Layers of Protection

Causes: Maintenance Failure, Complexity, Intentional Events, Counterfeits

Process Hazards Assessment: Checklist, What-If, HAZOP, Failure Mode Effect Analysis

Impact Analysis: Human Health, Product Quality & Safety, Environmental Consequences, Plant & Equipment, Business Consequences, Societal Consequences, Safety Levels/Categories

Functional Safety: Functional Safety Standards, Safety Instrumented Functions & Systems, Failure Modes, Safety Integrity Levels, Functional Safety Certifications, Life Safety Systems, Adequacy

Failure Modes: Failures, Failure Rates, Impacts

Maintenance Strategies: Redundancy, Spares, Maintenance Outages, Predictive Maintenance, Preventative Maintenance

Sector-Specific Approaches: Electric Sector Reliability

Electric Sector Reliability: Reliability Operating Limits, Undervoltage, Overvoltage, Underfrequency, Overfrequency, Inter-Area Flows, Control Circuits, Automatic Reclosing, Special Protection Systems (SPS)/Remedial Action Schemes

Special Protection Systems (SPS)/Remedial Action Schemes: SPS Database, SPS Performance

Industrial Cybersecurity Knowledge

This section discusses the dispositions of respondent input for Industrial Cybersecurity Knowledge.

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

Category	Topic	Count	Keep as-is	Change title	Remove
Regulation and Guidance		68	99%	1%	0%
	ISA/IEC 624432	67	97%	3%	0%
	Presidential Orders	67	91%	1%	7%
	NIST SP 800-82r2	67	97%	3%	0%
	NERC CIP	67	97%	3%	0%
	EU Cybersecurity Act	67	96%	1%	3%
Common Weaknesses		68	96%	4%	0%
	Indefensible Network Architectures	65	100%	0%	0%
	Unauthenticated Protocols	66	97%	3%	0%
	Unpatched Systems	66	100%	0%	0%
	Lack of Training	64	94%	5%	2%
	Transient Devices	66	95%	5%	0%
	Third Party Access	66	95%	5%	0%
	Supply Chain	65	92%	5%	3%
Events and Incidents		68	97%	3%	0%
	DHS Aurora	64	95%	3%	2%
	Stuxnet	64	95%	3%	2%
	Ukraine 2015	64	95%	3%	2%
	Ukraine 2016	64	95%	3%	2%
	Triton	64	95%	3%	2%
	Taum Sauk Dam	64	95%	3%	2%
	DC Metro Red line	64	95%	3%	2%
	San Bruno	64	95%	3%	2%
	Colonial Pipeline	64	95%	3%	2%
Defensive Technologies and Approaches		68	97%	3%	0%
	Industrial Network Firewalls	65	98%	2%	0%

	Data Diodes	65	94%	2%	5%
	Process Data Analysis	65	95%	3%	2%
	ICS Network Monitoring	65	100%	0%	0%
	Cyber informed engineering	64	100%	0%	0%
	Process hazards assessment based	64	98%	0%	2%
	Cyber-physical failsafes	64	95%	0%	5%
	Awareness and Training for ICS personnel	64	100%	0%	0%

Over 90% of respondents chose “keep as is” for all items. Notwithstanding this general indication of acceptability, the expert committee wanted to consider each suggestion for improvement on its own merits.

Fifty respondents provided a total 154 responses for improvement. As 58 responses included multiple parts, this gave an atomized quantity of 213 responses. In addition, 53 responses from the Industrial Control System Knowledge Section were moved into the Industrial Cybersecurity Knowledge Section, bringing the total to 266 responses. One respondent offered 29 suggestions. Thirty-three respondents offered just one or two suggestions.

Overall, of the 266 atomized responses provided, 192 (72%) were incorporated into the guidance. A summary of the final dispositions into the mutually exclusive categories is shown below.

Final disposition	**Count**
Directly accepted	59
Indirectly accepted	106
Note made in guidance document	28
Insufficient detail provided	8
No change	61
Referred to foundational ICS knowledge section	4
Total	**266**

Survey responses for which no change was made

The 54 suggestions for which no changes were made were classified into the following four categories:

Category for “No change”	**Count**
Already included	17
Just commentary	2
Out of scope	13
Otherwise not persuasive	22
Total	**54**

Description of changes to Industrial Cybersecurity Knowledge Section

The most significant change was the addition of subtopics to provide improved order via reasonable categories and subcategories. In addition, the committee compared the list of Common weaknesses to the list of Defensive techniques to ensure reasonable alignment. The guidance grew from 33 total items in the strawman to 129 items based on respondent suggestions. When incorporating the changes suggested, the review committee added an additional 76 items, bringing the total to 205. These changes enhance the utility of the guidance by providing increased clarity and specificity.

The strawman presented in the survey and the updated guidance are provided below. The updated guidance shows changes that resulted from survey responses in red, and additions by the review committee in blue.

Strawman – as presented in the survey as Section III (33 total items)

Regulations and Guidance
IEC 62443, Presidential orders, NIST SP 800-82R2, NERC CIP, EU Cybersecurity Act

Common Weaknesses
Indefensible network architectures, Unauthenticated protocols, Unpatched systems, Lack of training, Transient devices, Third-party devices and software, Supply chain

Events and Incidents
DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, Tam Sauk Dam, DC Metro Red Line, San Bruno, Colonial Pipeline

Defensive Technologies and Approaches
Industrial network firewalls, Data diodes, Process data analysis, ICS network monitoring, Cyber informed engineering, Process hazards-based approaches, Cyber-physical fail-safes, Awareness and training for ICS-related personnel

Resulting Guidance with Changes Shown

Changes made as result of survey responses appear in red. Additions made by committee appear in blue.

Guidance & Regulations

Frameworks & Paradigms, General Industrial Cybersecurity Guidance & Standards, Regulations, Industrial Cybersecurity Groups & Associations (4 red)

- *Frameworks & Paradigms*: Critical Function Assurance, Seven Ideals, SRP (Safety, Reliability, Productivity), Five Ds (Deter, Detect, Deny, Delay, Defend), SAIC (Safety, Availability, Integrity, Confidentiality) (5 blue)

- *Guidance & Standards*: General Industrial Cybersecurity Guidance & Standards Bodies, Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies (1 blue, 1 red)

  - *General Industrial Cybersecurity Guidance & Standards Bodies*: International General Industrial Cybersecurity Guidance & Standards Bodies, National General Industrial Cybersecurity Guidance & Standards Bodies (2 blue)

    - *International General Industrial Cybersecurity Guidance & Standards Bodies*: International Society of Automation (ISA), International Electrotechnical Commission (IEC), European Network & Information Security Agency (ENISA) (1 blue)

      - *International Society of Automation*: ISASecure, ISA-Technical Report 84.00.09-2017 “Cybersecurity Related to the Functional Safety Lifecycle” (1 blue, 1 red)

      - *International Electrotechnical Commission (IEC)*: IEC 62443 “Industrial Automation and Control Systems Security”

    - *National General Industrial Cybersecurity Guidance & Standards Bodies*: United States General Industrial Cybersecurity Guidance & Standards Bodies (1 blue)

      - *United States Industrial Cybersecurity Guidance & Standards Bodies*: U.S. National Institute of Standards and Technology (NIST), U.S. Department of Homeland Security (DHS), U.S. Cyber and Infrastructure Security Agency (CISA) (2 blue)

        - *U.S. National Institute of Standards and Technology*: NIST SP 800-82 “Guide to Operational Technology Security”

Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, Transportation, Electric Power, Nuclear, Oil & Natural Gas, Water & Wastewater, Food & Pharmaceutical

Subtopics for *Transportation:* International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies.

International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: SAE International (1 blue)

International: ISO/SAE 21434:2021 Road vehicles — Cybersecurity Engineering (1 blue)

Electric Power: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Guidance & Standards Bodies

International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: International Standards Organization (ISO) (1 red)

International Standards Organization: ISO/IEC 27019:2017 "Information technology — Security techniques — Information security controls for the energy utility industry" (1 red)

National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: U.S. Department of Energy (DOE) (1 blue)

U.S. DOE: Cybersecurity Capability Maturity Model (C2M2) (1 blue)

Nuclear: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies

Subtopics for International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: International Electrotechnical Commission (IEC)

Subtopics for International Electrotechnical Commission (IEC): IEC 62645 Ed. 2.0 b: 2019 “Nuclear Power Plants - Instrumentation, Control and Electrical Power Systems - Cybersecurity Requirements” (1 blue)

Oil & Natural Gas: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies

International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: American Petroleum Institute (API) (1 blue)

Subtopics for *American Petroleum Institute*: American Petroleum Institute Standard 1164 “Pipeline Control Systems Cybersecurity” (1 blue)

Water & Wastewater: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Guidance & Standards Bodies

National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: American Water Works Association (AWWA) (1 blue)

American Water Works Association (AWWA): “Water Sector Cybersecurity Risk Management Guidance” (1 blue)

Food & Pharmaceutical: International Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies, National Sector-Specific Guidance & Standards Bodies

National Sector-Specific Industrial Cybersecurity Guidance & Standards Bodies: U.S. Food and Drug Administration (FDA) (1 blue)

U.S. FDA: “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” (1 blue)

Regulations: Jurisdictions, Regulatory bodies, Regulation Documents, Audits & Enforcement (4 red)

Jurisdictions: Regulatory Processes, Authorities, Governments with Industrial Cybersecurity Regulations, Governments with Industrial Cybersecurity Regulations (3 blue)

Governments with Industrial Cybersecurity Regulations: United States Industrial Cybersecurity Regulations, European Union Industrial Cybersecurity Regulations (2 blue)

United States Industrial Cybersecurity Regulations: North American Electric Reliability Corporation (NERC), Nuclear Regulatory Commission (NRC), Transportation Security Agency (TSA), U.S. Laws, Executive/Presidential orders (4 blue)

NERC: NERC Critical Infrastructure Protection (CIP)

U.S. NRC: 10 CFR 73.54 "Protection of digital computer and communication systems and networks", NRC Regulatory Guide 5.71 "Cybersecurity Programs for Nuclear Facilities" (2 red)

U.S. TSA: TSA Security Directive 1580-21-01A, TSA Security Directive 1582-21-01A, Security Directive Pipeline-2021-02C (3 blue)

U.S. Laws: S. 1605 National Defense Authorization Act of 2022 (Sections 1541 & 1548) (1 red)

Presidential/Executive Orders*:* 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 (Suspended) (3 blue)

European Union Industrial Cybersecurity Regulations: Regulation (EU) 2019/881 (EU Cybersecurity Act) (1 red)

Groups & Associations: International Society of Automation (ISA), Information sharing and analysis centers (ISACs), Professional Conferences (1 blue, 1 red))

Common Weaknesses

Managerial Weaknesses, System & Host Weaknesses, Network Weaknesses, Instrumentation & Control Weaknesses (4 red)

Managerial Weaknesses: 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 (3 blue, 3 red)

System & Host Weaknesses: 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 ~~Systems~~ Software, Unassured Provenance, ~~Supply Chain~~ Unrecognized Third-Party Relationships, Poor Programming Practice (10 red)

Network Weaknesses: Indefensible Network Architectures, ~~Unauthenticated~~ Insecure Process Control Network Protocols, Unmonitored Networks, ~~Transient Devices~~ Poorly Managed Temporary Network Nodes, ~~Third-Party Devices and Software~~ Poorly Controlled Network Access, Unauthorized Wireless Networks (1 blue, 4 red)

Instrumentation & Control Weaknesses: Programmable Physical Damage, Poor Controller Coding Practices, Lack of Sensor/Transmitter Integrity Mechanisms (3 red)

Industrial Cybersecurity Events ~~and~~ & Incidents

Events & Incidents Cases, Analytical Concepts for Events & Incidents (2 blue)

Events & Incidents Cases: DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, Norsk Hydro Ransomware, Notpetya, Oldsmar, Colonial Pipeline, Jeep/Chrysler Demonstration Attacks, Tam Sauk ~~Dam~~ Hydroelectric Station, DC Metro Red Line, San Bruno (3 red)

Analytical Concepts for Events & Incidents: Tactics, Techniques & Procedures, Targeting, IT vs OT Vectors & Impacts, Root Cause Analysis (4 blue)

Root Cause Analysis: Root Causes, Investigations, Internal vs External Causes, Deliberate vs Unintended Effects, Lessons Learned (5 blue)

Defensive ~~Approaches and Technologies~~ Techniques

Managerial Defensive Techniques, Network Defensive Techniques, System & Host Defensive Techniques, Instrumentation & Control Defensive Techniques (4 red)

Managerial Defensive Techniques: Industrial Cybersecurity Champion, Awareness & Training For ICS-Related Personnel, OT/ICS Security Program, Cybersecurity Risk Management, OT/ICS Security Policies, Lifecycle Management, Contingency Plans with OT/ICS Focus, Incident Response Plans with OT/ICS Focus, Security Operations Center for OT/ICS, Security Alerts for OT/ICS, Managed Security Services, Professional Ethics, Privacy Assurance (2 blue, 9 red)

Cybersecurity Risk Management: Stakeholders, Integrated System Model (Asset Inventory), Adversary Mindset, Threat Intelligence, Vulnerability Intelligence, Safety vs Security (6 red)

Lifecycle Management: Procurement Techniques, Security Management of Legacy Devices, Secure Software Development Lifecycle (3 red)

Security Operations Center for OT/ICS: Security Alerts for OT/ICS

Network Defensive Techniques: Secure Network Architecture, Network Boundaries, Network Segmentation, Physical Separation (Air Gap), Management of Ports And Services, ~~Industrial Network~~ Process Control Network Firewalls, Process Control Network Anomaly Detection, Quarantine & Observation, ~~Process Data~~ Analysis of Security Data With Process Control Data, Secure Remote Access, Software Defined Networking, Data Diodes, Wireless Communications Analysis, Deceptive Technologies, Security-Enhanced ICS Network Communications & Protocols (4 blue, 7 red)

System & Host Techniques: Device Hardening, Device Monitoring, Software/Firmware Updates, Software Integrity Mechanisms, Passwords & Credential Management, Physical Security, Hardware Reviews (7 red)

Instrumentation & Control Defensive Techniques: Positive Control, Cyber-Informed Engineering, Consequence-Driven Cyber-Informed Engineering (CCE), Process Hazards-Based Approaches, Consequence Red-Teaming, Special Consideration of Safety Functions, Cyber-Physical Fail-Safes, Controller Security, Analysis of Process Data for Security Purposes (Historian/SIEM), Sensor/Transmitter Integrity Assurance Mechanisms (3 blue, 3 red)

Controller Security: Memory Protection Switch, Controller Hardening, Controller Logic Change Monitoring, Controller Logic Inspection, Secure Controller Programming, Controller Self-Diagnostics, Process State-Awareness (5 blue, 2 red)

Secure Controller Programming: Control Data Validation, Centralize Operational Logic in The Controller (vs HMI), Allocate Controller Memory by Function (3 blue)

Control Data Validation: Controller Data Sources, Comparison with Reasonable Values, Comparison with Historical Values (3 blue)

Controller Self-Diagnostics: Controller Configuration Change Monitoring, Controller Performance Monitoring, Controller Error Monitoring, Controller Alerts (4 blue)

Process State-Awareness: Prevent Simultaneous Assertion of Exclusive Process States, Define Safe Process Start State, Conservative Control, User Awareness of Process State, Trap Manipulation of Process State Alarms (5 blue)

Sensor/Transmitter Integrity Assurance Mechanisms: Emanations Monitoring of Transmitters, Independent Sensing/Transmission & Backhaul (2 blue)