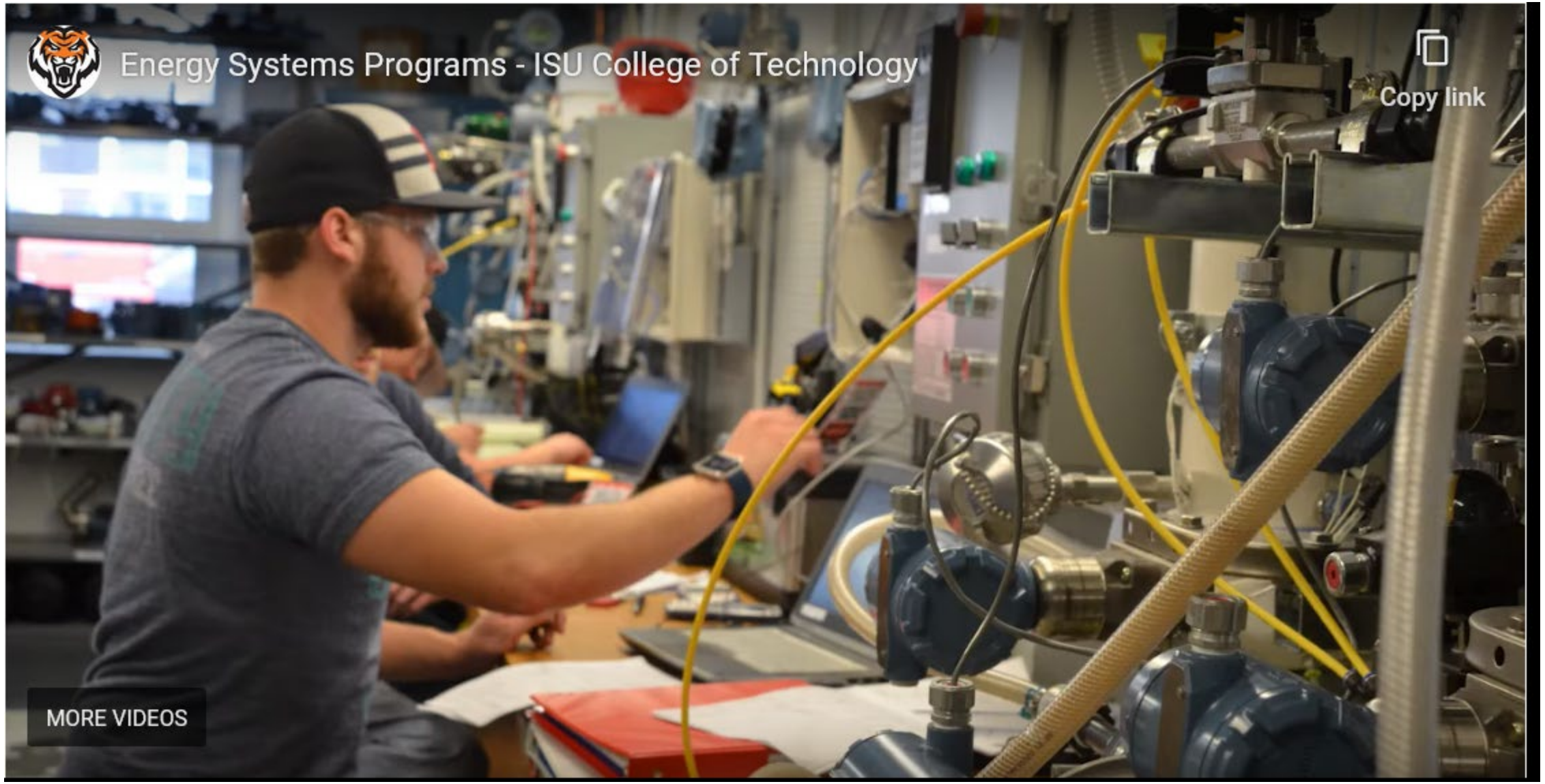
What does an OT Security Professional need to know?

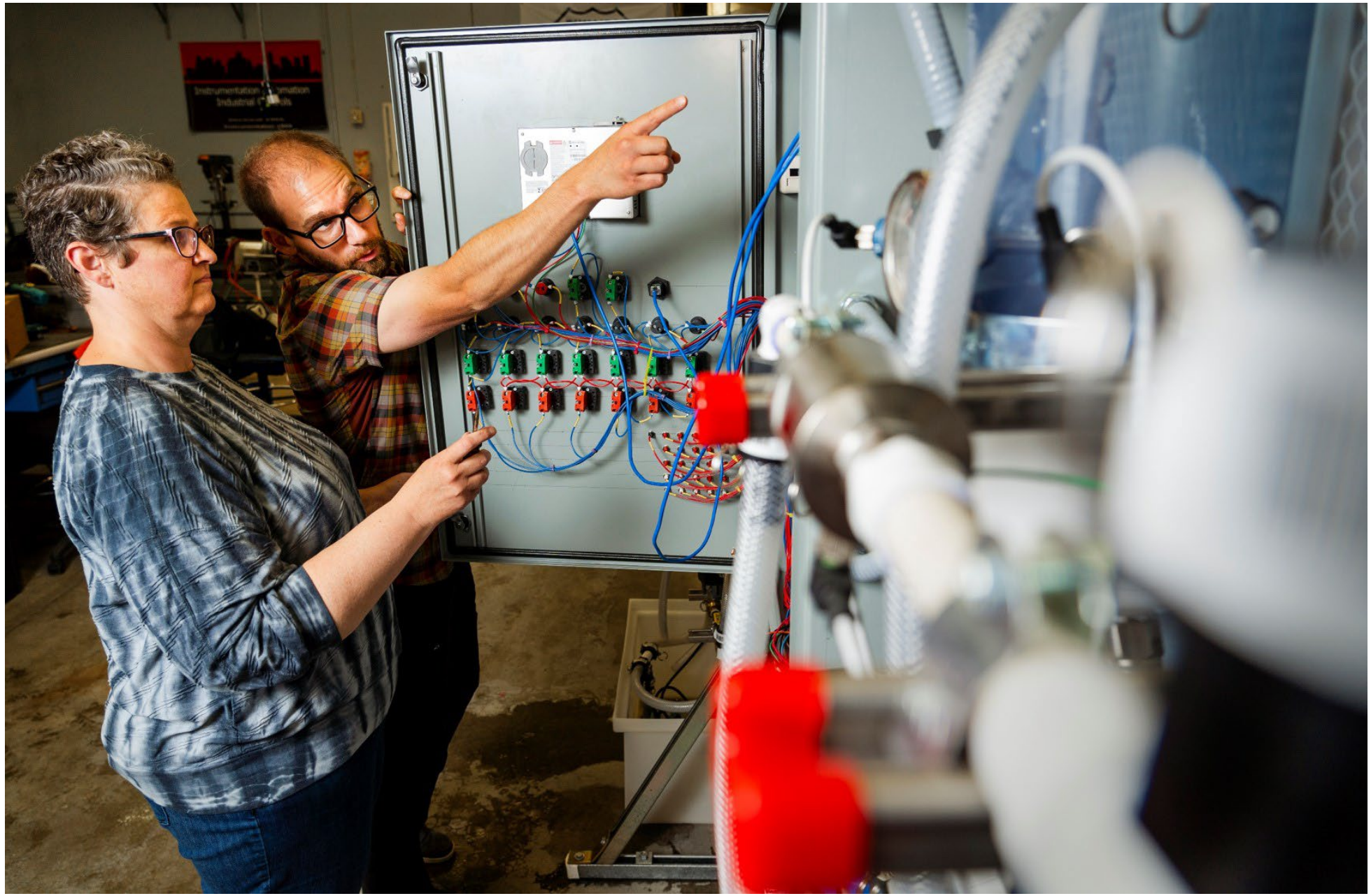
Sean McBride

November 2024

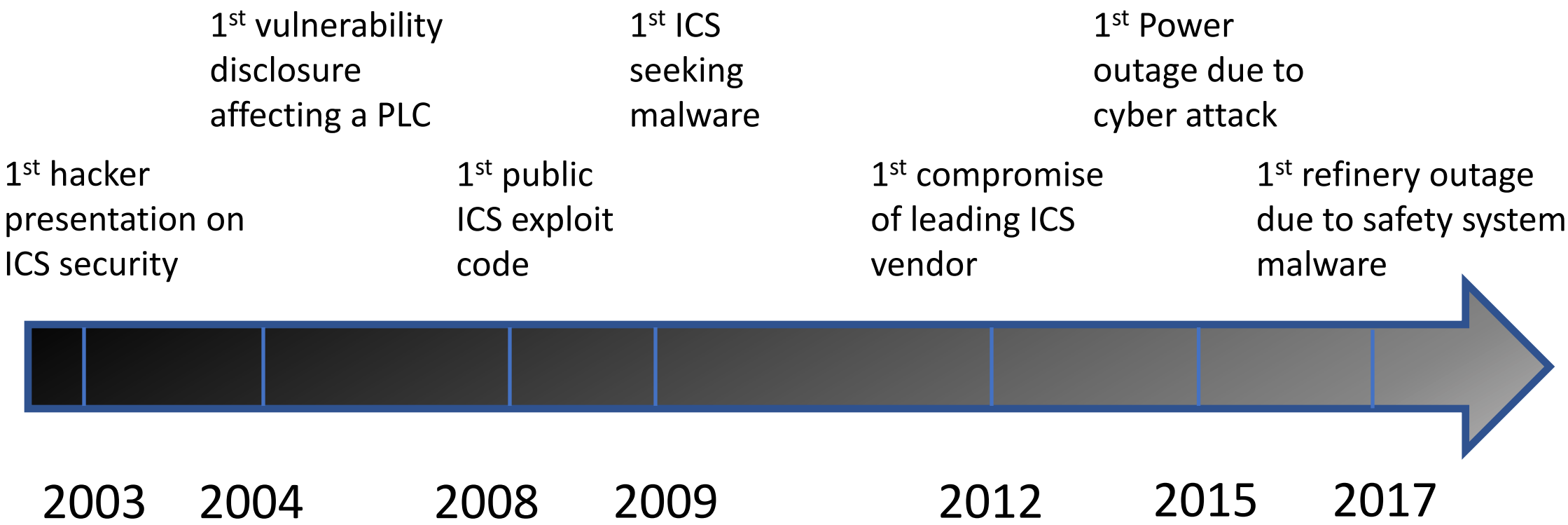
Sean McBride, PHD

- 2006 SFS Graduate Idaho State University (MBA)
- 2006-2009 Idaho National Laboratory
  - Precursor to ICS-CERT
  - On first ICS vulnerability disclosure coordination call
- 2009-2016 Critical Intelligence – iSIGHT – FireEye/Mandiant
  - Worlds first CI/ICS threat intelligence company
  - Top flight customers
  - Acquired by iSIGHT Partners
  - Director of ICS Cybersecurity
- 2017 ISU
  - 2017 Stood up country's first (and to date only) Industrial Cybersecurity degree program
  - 2023 Director of Informatics Research Institute
  - 2023 CAE Designated PoS, 2024 ABET accredited PoS
- 2021 PhD La Trobe University (Jill Slay)
  - Thesis: Foundation of Industrial Cybersecurity Education and Training


Energy Systems Programs - ISU College of Technology
Copy link
MORE VIDEOS



Our moment in time



2003: How Safe is Glass of Water?

Things started to get a little more interesting when semi sober we reconvened to investigate the security surrounding the UKs water management system. The talk was titled "how safe is a glass of water." It was a detailed breakdown of the RF systems that are used by water management authorities in the UK and how these systems can be abused, interfered with and generally messed.

The live demonstration included how to monitor the un-encrypted water management systems and create a denial of service attack. It was also made clear that additional communication channels using dial up connections would kick in automatically in the event of such an attack.

2004: NATO Conference

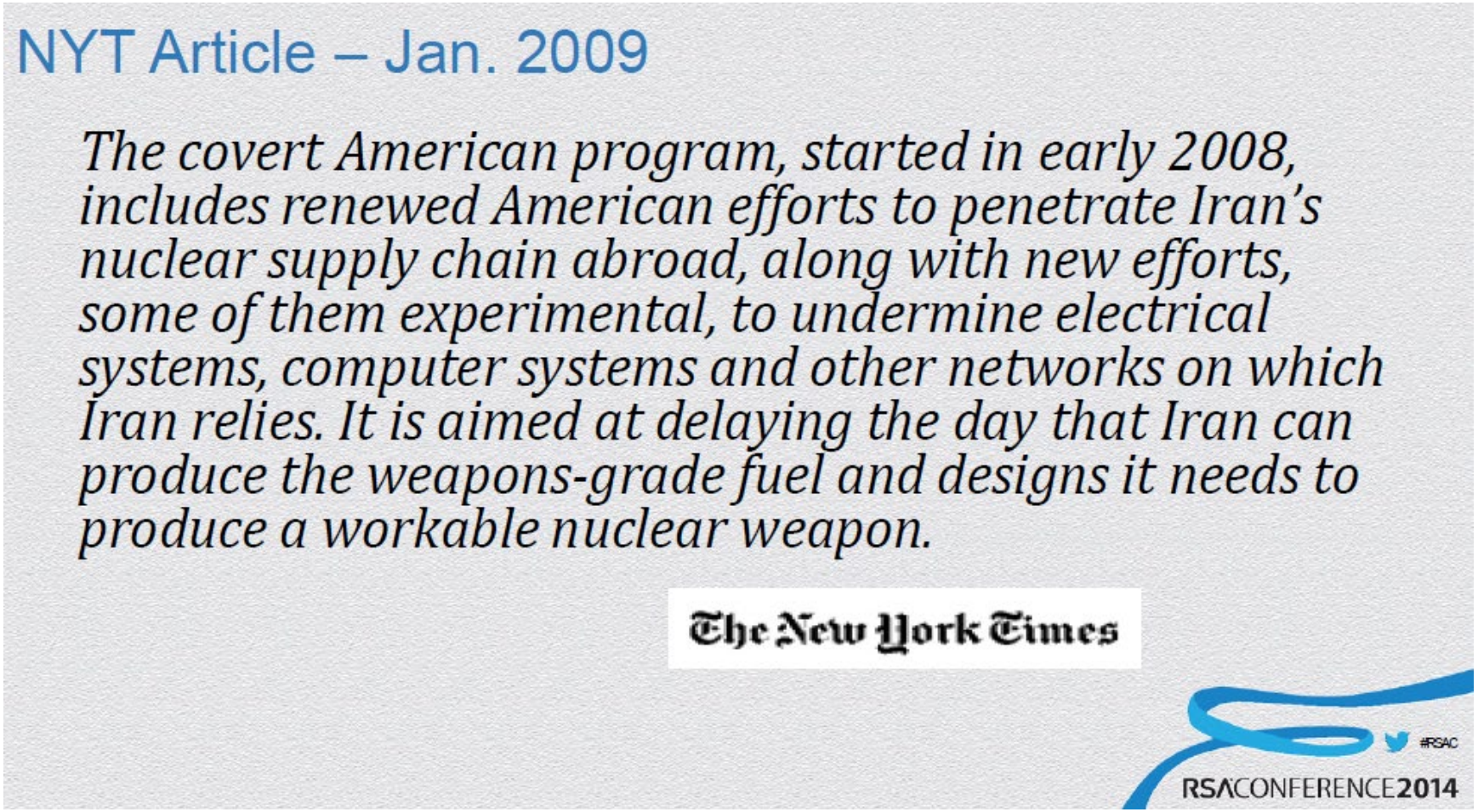
Network Vulnerability Assessment:
A Multi-Layer Approach to Adaptivity

Professor Ann Miller and Professor Kelvin T. Erickson
Department of Electrical and Computer Engineering
University of Missouri – Rolla
Rolla, Missouri 65409-0040
USA

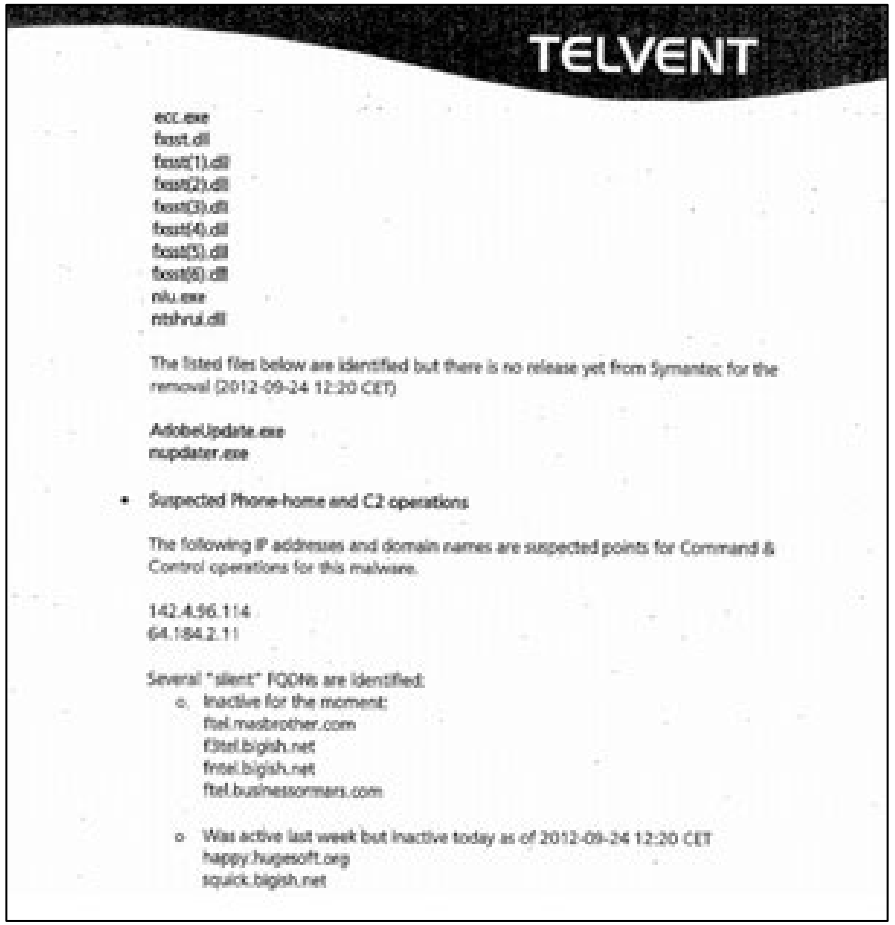
milleran@umr.edu kte@umr.edu

For the ControlLogix ENET module, the response to a DoS attack was different. It gave no response to a small amount of data, but as the amount of data sent to it and the speed of transmission were increased it started responding by sending arbitrary data. This returned data was not decoded

2009: Stuxnet



2012: Pipeline automation firm Telvent Compromised



TELVENT

ecc.exe
fxsst.dll
fxsst(1).dll
fxsst(2).dll
fxsst(3).dll
fxsst(4).dll
fxsst(5).dll
fxsst(6).dll
nlu.exe
ntshrui.dll

The listed files below are identified but there is no release yet from Symantec for the removal (2012-09-24 12:20 CET)

AdobeUpdate.exe
nupdater.exe

- Suspected Phone-home and C2 operations

The following IP addresses and domain names are suspected points for Command & Control operations for this malware.

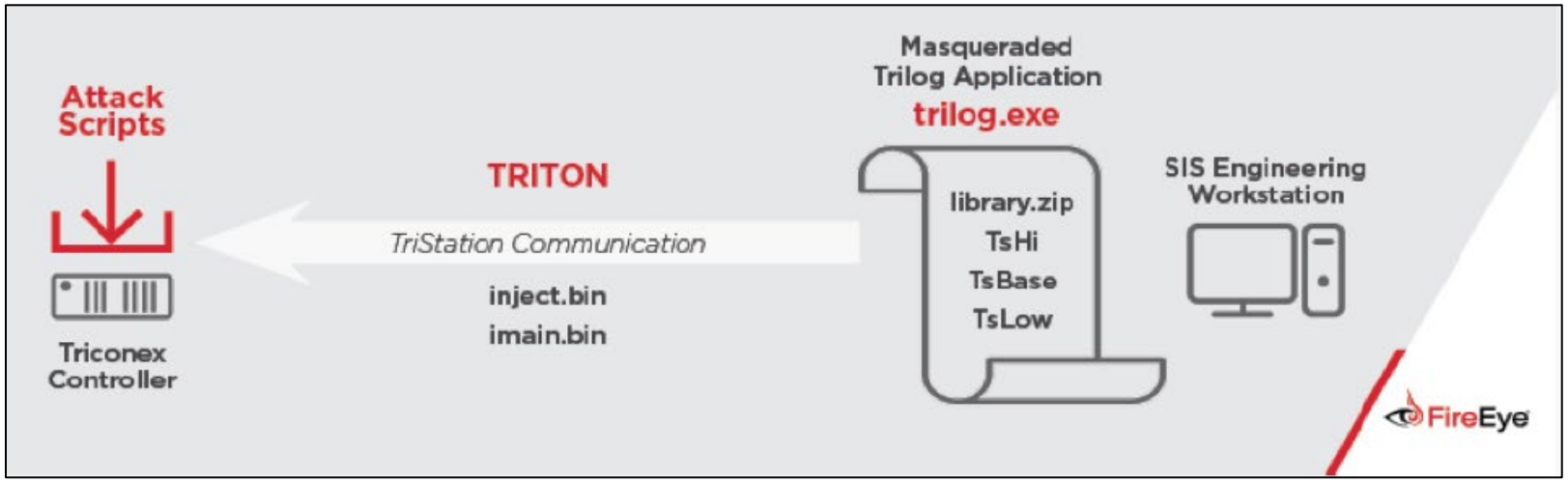
142.4.56.114
64.184.2.11

Several "silent" FQDNs are identified:

- Inactive for the moment:
  - ftel.maxbrother.com
  - FStel.bigish.net
  - frtel.bigish.net
  - ftel.businessmans.com
- Was active last week but inactive today as of 2012-09-24 12:20 CET
  - happy.hugesoft.org
  - squick.bigish.net

2015: Ukraine power outage caused by cyber attack

2017: Malicious code hits safety system at Saudi refinery



2023-2024 Automation Business Cyber Impacts

The Clorox Company

TECHNOLOGY AND IIOT

Updated: Clorox Cyberattack Cost $356 Million

Oct. 5, 2023

The bleach manufacturer this week begins the cleanup process to fully repair damage from an

Company News | Email Alerts

View All News →

Dole Experiences Cybersecurity Incident

TECHNOLOGY AND IIOT › CYBERSECURITY

Manufacturing Is #1 in Cyber Attacks for Third Straight Year. What Can Be Done?

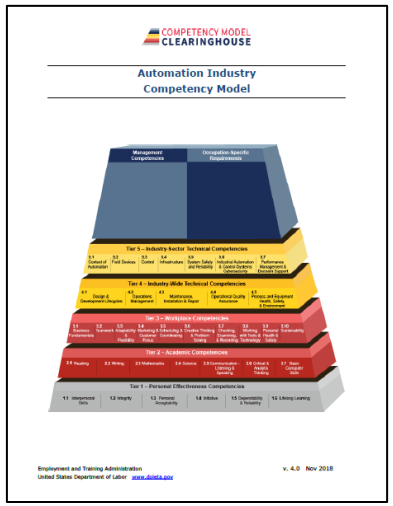
May 28, 2024

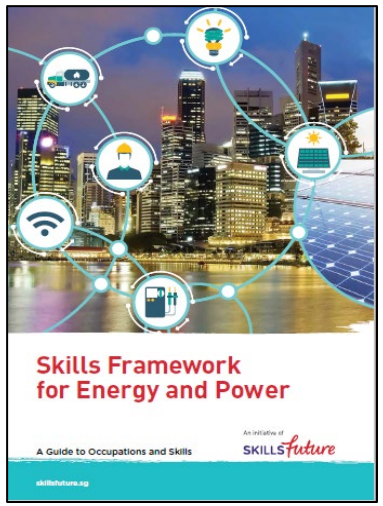
Eighty-five percent of incidents could have been mitigated with patching, multi-factor

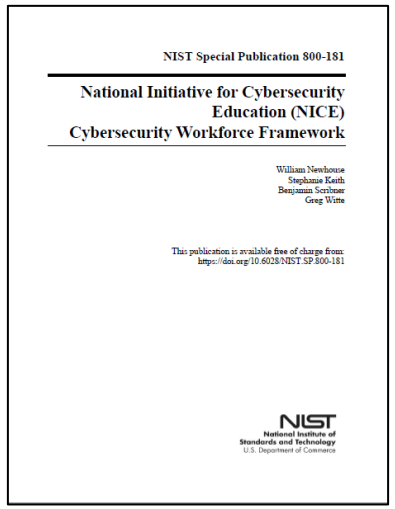
Pathway to here

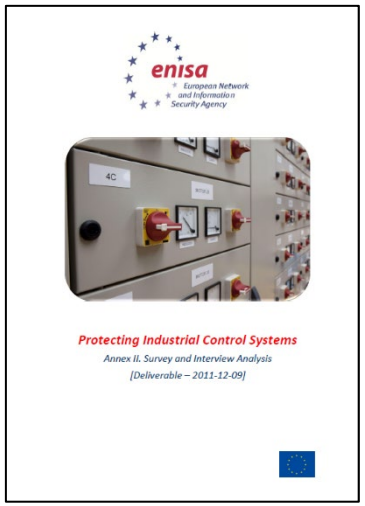
2019	2020	2021	2021-22	2024
Lit Review → Nominal Group Technique	→ Focus Groups	→ Strawman	→ Survey	→ Guidance Document

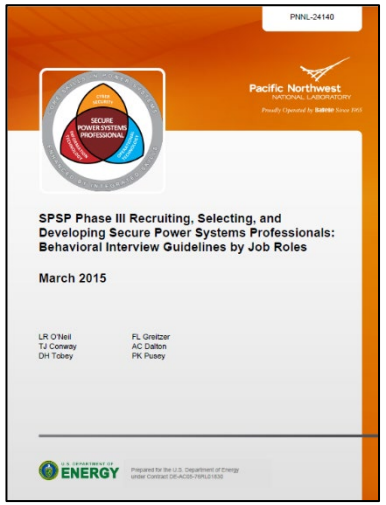
Searching for a Standard

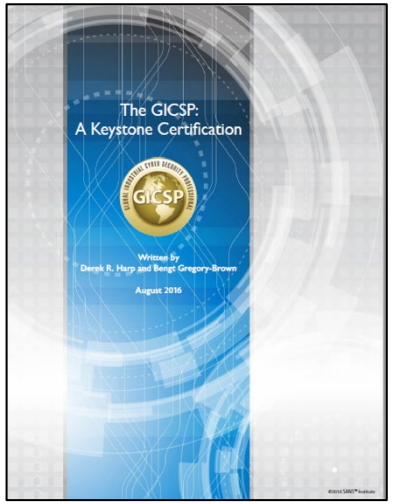


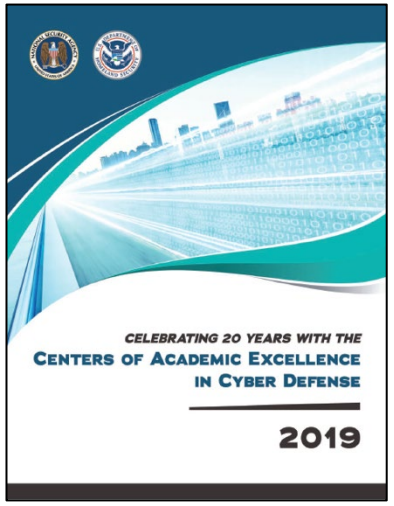










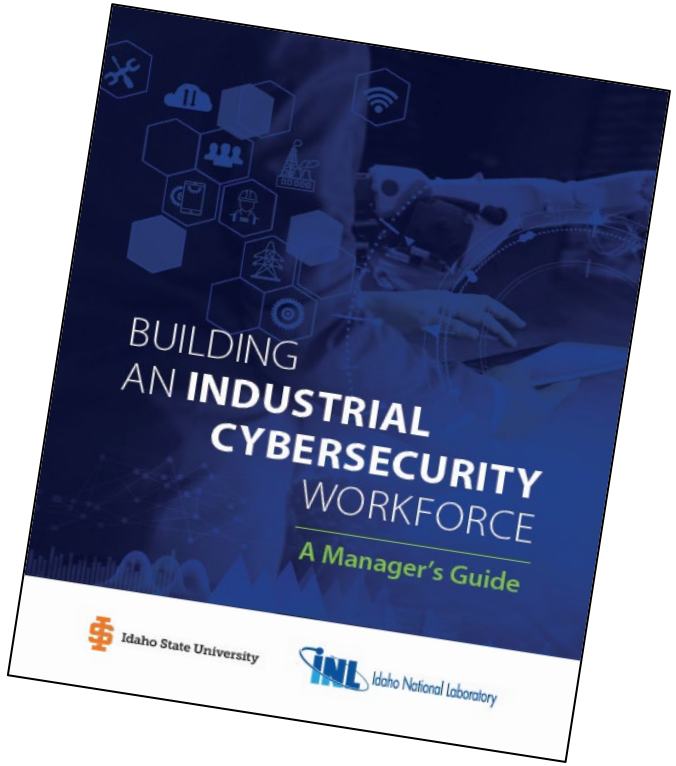


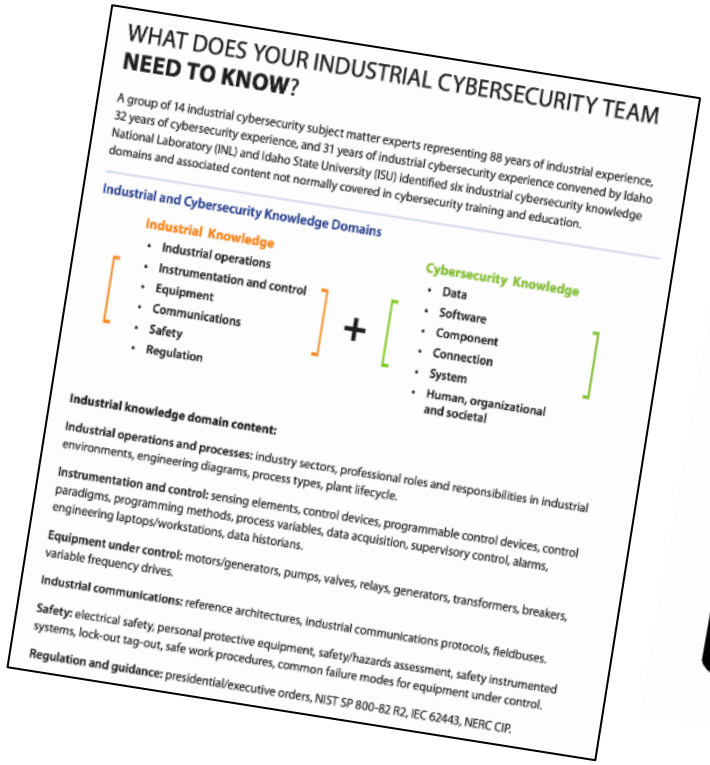
Criteria	Curricular Guidance Efforts/Documents										Total Ys
	ABET	ENISA	GIAC	ISA	JTF	NIST	NSA	PNNL	SF	CIE	
1. Addresses Industrial cybersecurity	N	Y	Y	Y	N	N	Y	Y	Y	Y	6
2. Clearly differentiates industrial	N	P	P	Y	N	N	P	N	N	Y	2
3. Consensus-based	Y	Y	Y	U	Y	N	N	Y	U	U	5
4. Qualified participants	Y	Y	Y	U	Y	U	U	Y	U	Y	6
5. Publicly available	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	9
6. Includes knowledge	P	Y	Y	Y	Y	Y	Y	Y	Y	N	8
7. Justifies knowledge	N	N	N	N	N	N	N	N	N	N	0
8. Evidence of empirical validation	N	N	N	N	N	N	N	N	N	N	0
TOTAL Ys	3/8	5/8	5/8	4/8	4/8	2/8	3/8	5/8	3/8	4/8	

Deficiencies to address

- Missing description of what is “OT” or “industrial” cybersecurity
- Missing description of why knowledge items are included
- Missing methodology and raw data that support claim to validity

Strawman





WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM **NEED TO KNOW?**

A group of 14 industrial cybersecurity subject matter experts representing 88 years of industrial experience, 32 years of cybersecurity experience, and 31 years of industrial cybersecurity experience convened by Idaho National Laboratory (INL) and Idaho State University (ISU) identified six industrial cybersecurity knowledge domains and associated content not normally covered in cybersecurity training and education.

Industrial and Cybersecurity Knowledge Domains

Industrial Knowledge
- Industrial operations
- Instrumentation and control
- Equipment
- Communications
- Safety
- Regulation

+

Cybersecurity Knowledge
- Data
- Software
- Component
- Connection
- System
- Human, organizational and societal

Industrial knowledge domain content:

Industrial operations and processes: industry sectors, professional roles and responsibilities in industrial environments, engineering diagrams, process types, plant lifecycle.

Instrumentation and control: sensing elements, control devices, programmable control devices, control paradigms, programming methods, process variables, data acquisition, supervisory control, alarms, engineering laptops/workstations, data historians.

Equipment under control: motors/generators, pumps, valves, relays, generators, transformers, breakers, variable frequency drives.

Industrial communications: reference architectures, industrial communications protocols, fieldbuses.

Safety: electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented systems, lock-out tag-out, safe work procedures, common failure modes for equipment under control.

Regulation and guidance: presidential/executive orders, NIST SP 800-82 R2, IEC 62443, NERC CIP.

Survey


ISA
GLOBAL CYBERSECURITY ALLIANCE
Idaho State UNIVERSITY
INL
Idaho National Laboratory
Introduction Block
This survey will take approximately 20 minutes to complete

Survey Questions Overview

~300 total questions

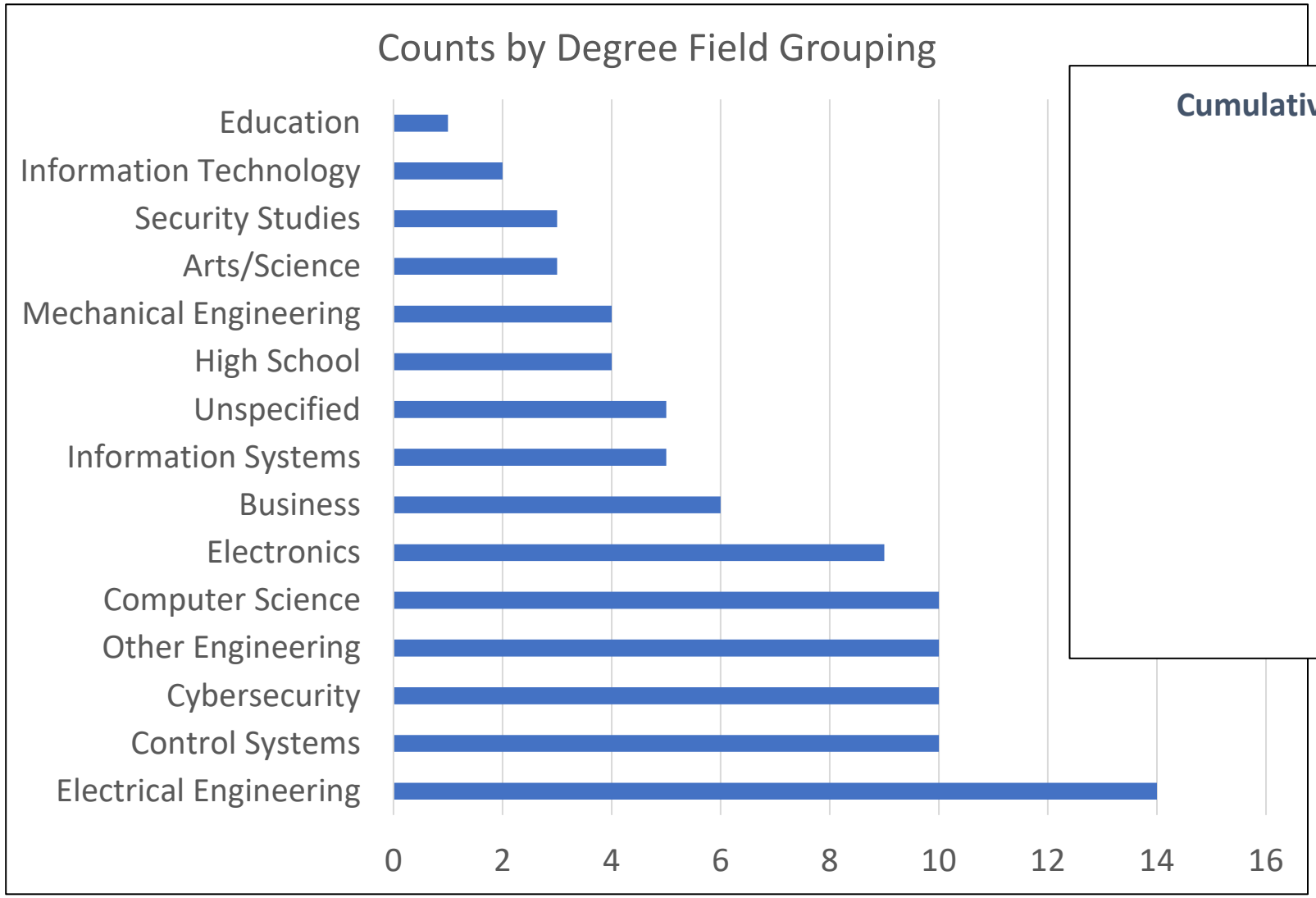
Three Sections

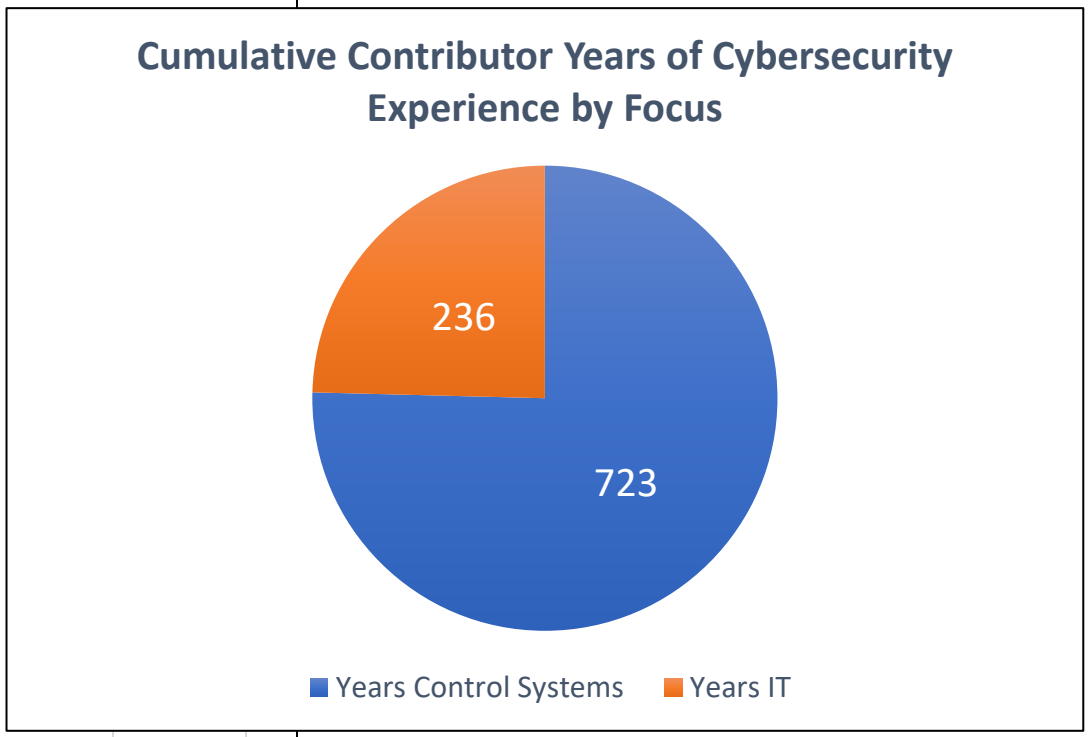
1. Respondent Background
2. Foundational ICS knowledge
   - Five categories
   - 41 Topics
3. ICS Cybersecurity knowledge
   - Four categories
   - 29 Topics

For each category and topic

- Rate relevance on a scale of 1-10
- Choose: Keep as is, Change, Remove

Respondents: New Voices!





Foundational ICS Knowledge

- 96 Respondents
- 342 Responses
- 461 atomized responses
- One respondent offered 47 suggestions
- 45 respondents offered one or two suggestions

Responses for Foundational ICS Knowledge: Instrumentation and Control

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%

Disposition of suggestions: Foundational ICS Knowledge

- Each response reviewed on its own merit
  (without considering respondent background)
- Of the 461 atomized responses, 275 (60%) were incorporated

Final disposition	**Count**
Directly accepted	90
Indirectly accepted	156
Note made in guidance document	29
Referred to cybersecurity section	53
Insufficient detail provided	53
No change	80

Dispositions of Foundational ICS Knowledge

Subtopics for *Control system components*: Sensors & Transmitters, Controllers, Operator interfaces, Engineering ~~laptops/workstations~~ computers, ~~Process data historians~~ Application servers, ~~Variable frequency drives~~ Motor controllers (6, 0 blue)

Subtopics for *Sensors & Transmitters*: Sensors, Transmitters, Units of measure, Transduction, Principles of Operation, Temperature, Pressure, Level, Flow, Calibration, Scaling, Meters, Smart instrumentation (11, 9 blue)

Subtopics for *Controllers*: Relays, Controller hardware, Memory, Input/output, Program scan, Programmable logic controllers (PLCs), Distributed control systems (DCS), Remote terminal units (RTUs), Intelligent electrical devices (IEDs), Protective Relays, Safety Controllers, Soft PLCs (13, 2 blue)

Subtopics for *Operator interfaces*: Supervisor interface (SCADA HMI), panel-based/skid-mounted interface (HMI), Human-machine interface design (3, 1 blue)

Red == changes due to respondent suggestions
Blue == additions after review of suggestions

Anecdotes for Foundational ICS Knowledge

In cybersecurity it is not necessary to understand process variables, it is important to focus on the infrastructure.

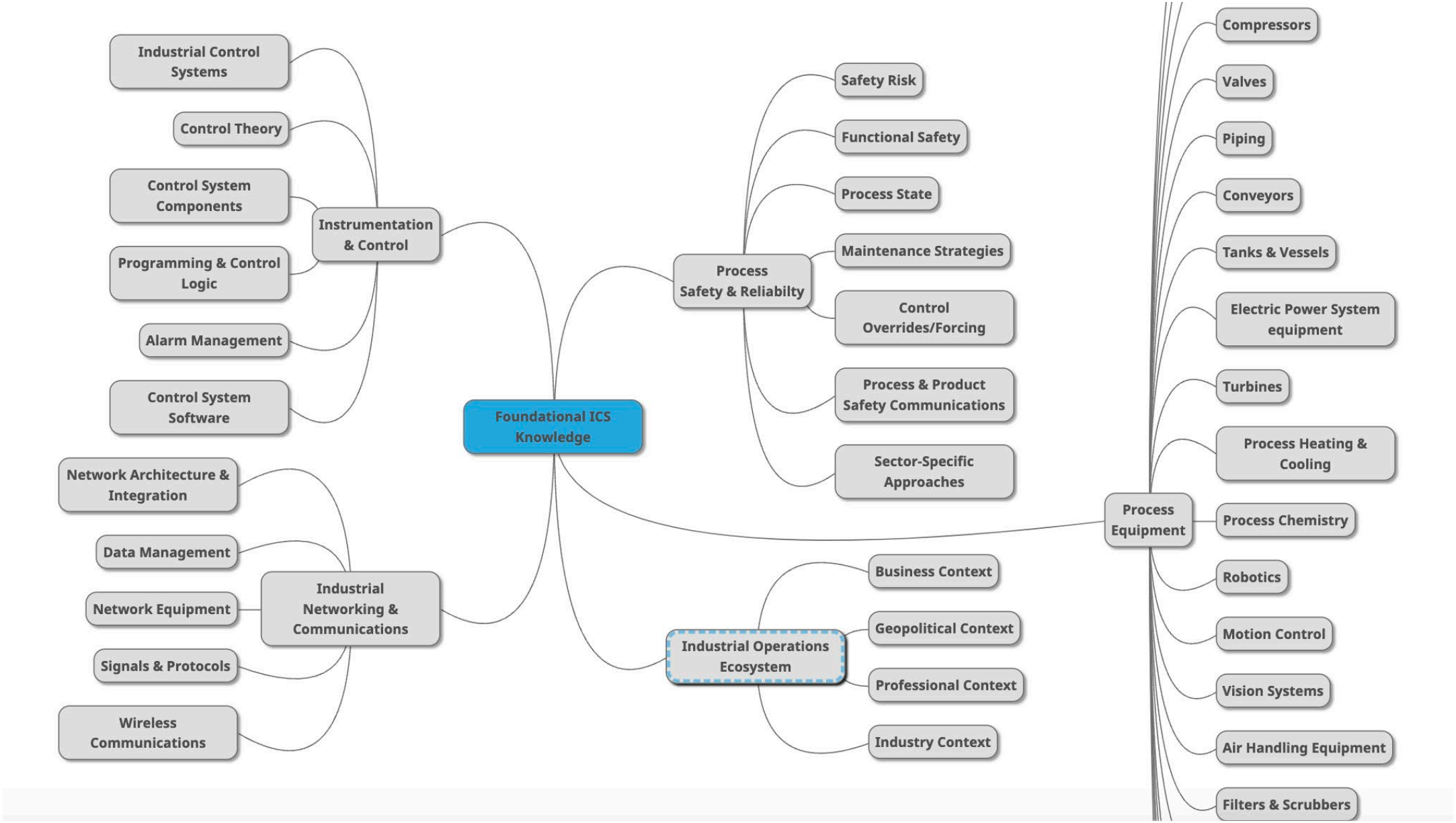
VFDs -- *Irrelevant to the cybersecurity discipline.*

A cybersecurity hazards assessment it's unnecessary. The only thing necessary is the architecture of the ICS.

Correlation of **years in industrial automation** and **relevance scores** for categories in Foundational ICS Knowledge

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

The TKb value for Safety and Ecosystem met the p value of .05 for statistical significance


Foundational ICS Knowledge
Instrumentation & Control
Industrial Control Systems
Control Theory
Control System Components
Programming & Control Logic
Alarm Management
Control System Software
Industrial Networking & Communications
Network Architecture & Integration
Data Management
Network Equipment
Signals & Protocols
Wireless Communications
Process Safety & Reliabilty
Safety Risk
Functional Safety
Process State
Maintenance Strategies
Control Overrides/Forcing
Process & Product Safety Communications
Sector-Specific Approaches
Industrial Operations Ecosystem
Business Context
Geopolitical Context
Professional Context
Industry Context
Process Equipment
Compressors
Valves
Piping
Conveyors
Tanks & Vessels
Electric Power System equipment
Turbines
Process Heating & Cooling
Process Chemistry
Robotics
Motion Control
Vision Systems
Air Handling Equipment
Filters & Scrubbers

Industrial Cybersecurity Knowledge

- 50 Respondents
- 154 Responses
- 266 Atomized responses
- One respondent offered 29 suggestions
- 33 respondents offered one or two suggestions

Select results:
Topics in Common Weaknesses Category

		Response		
Topic		*Keep as is*	*Change topic name*	*Remove topic*
Indefensible network architectures		65	0	0
Unauthenticated protocols		63	2	0
Unpatched systems		65	0	0
Lack of training		61	3	1
Transient devices		62	3	0
Third party access		62	3	0
Supply chain		60	3	2

Disposition of suggestions: Industrial Cybersecurity Knowledge

- Each response reviewed on its own merit
  (without considering respondent background)
- Of the 266 atomized responses, 192 (72%) were incorporated

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

Dispositions of Industrial Cybersecurity Knowledge

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)

Red == changes due to respondent suggestions
Blue == additions after review of suggestions

Anecdotes for Industrial Cybersecurity Knowledge

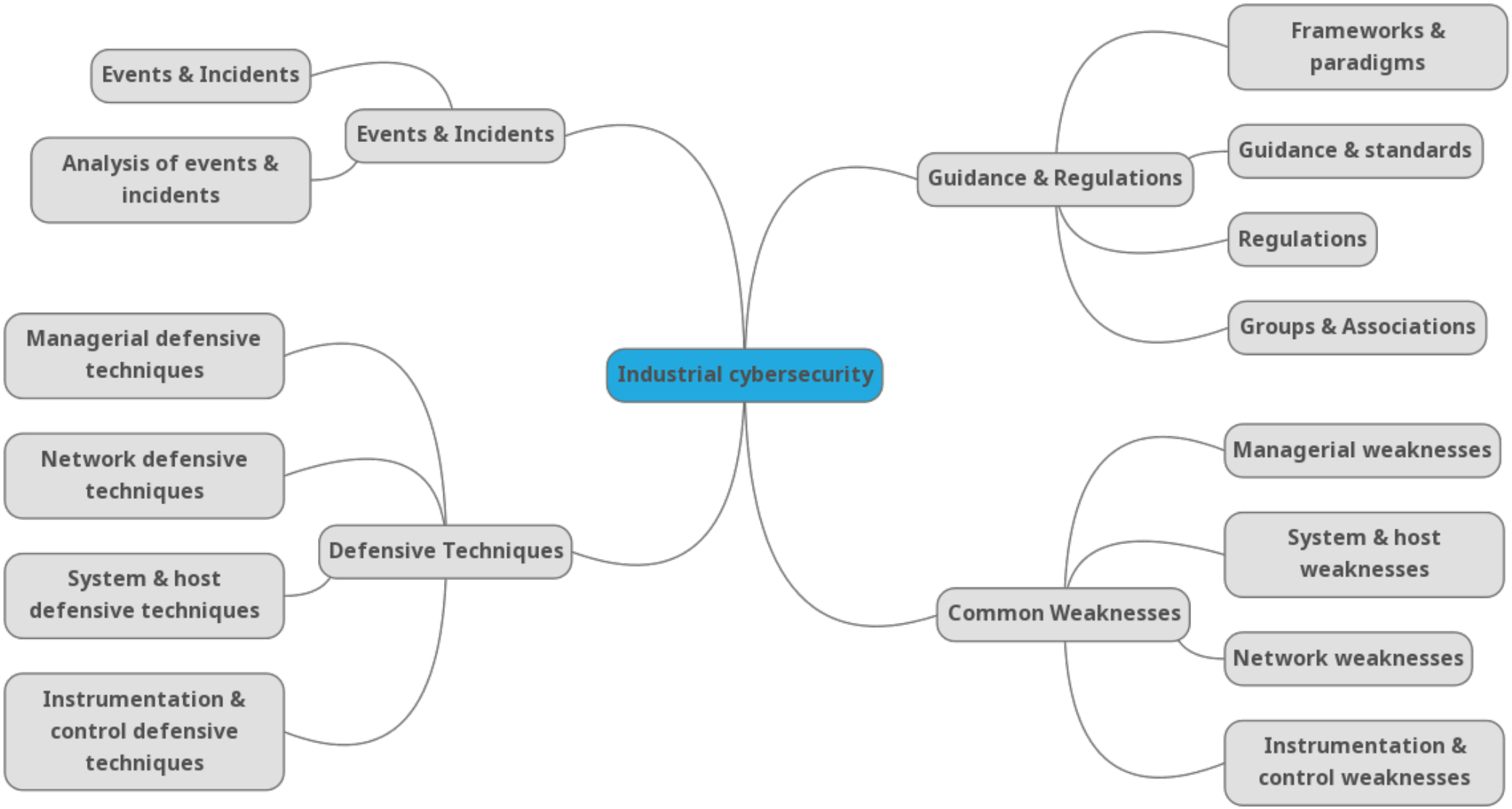
Process Data Analysis: Irrelevant for cybersecurity. Process and control engineers are monitoring the process 24/7.

Remove: Process Hazards and Assessment Based Approaches. Irrelevant for cybersecurity.

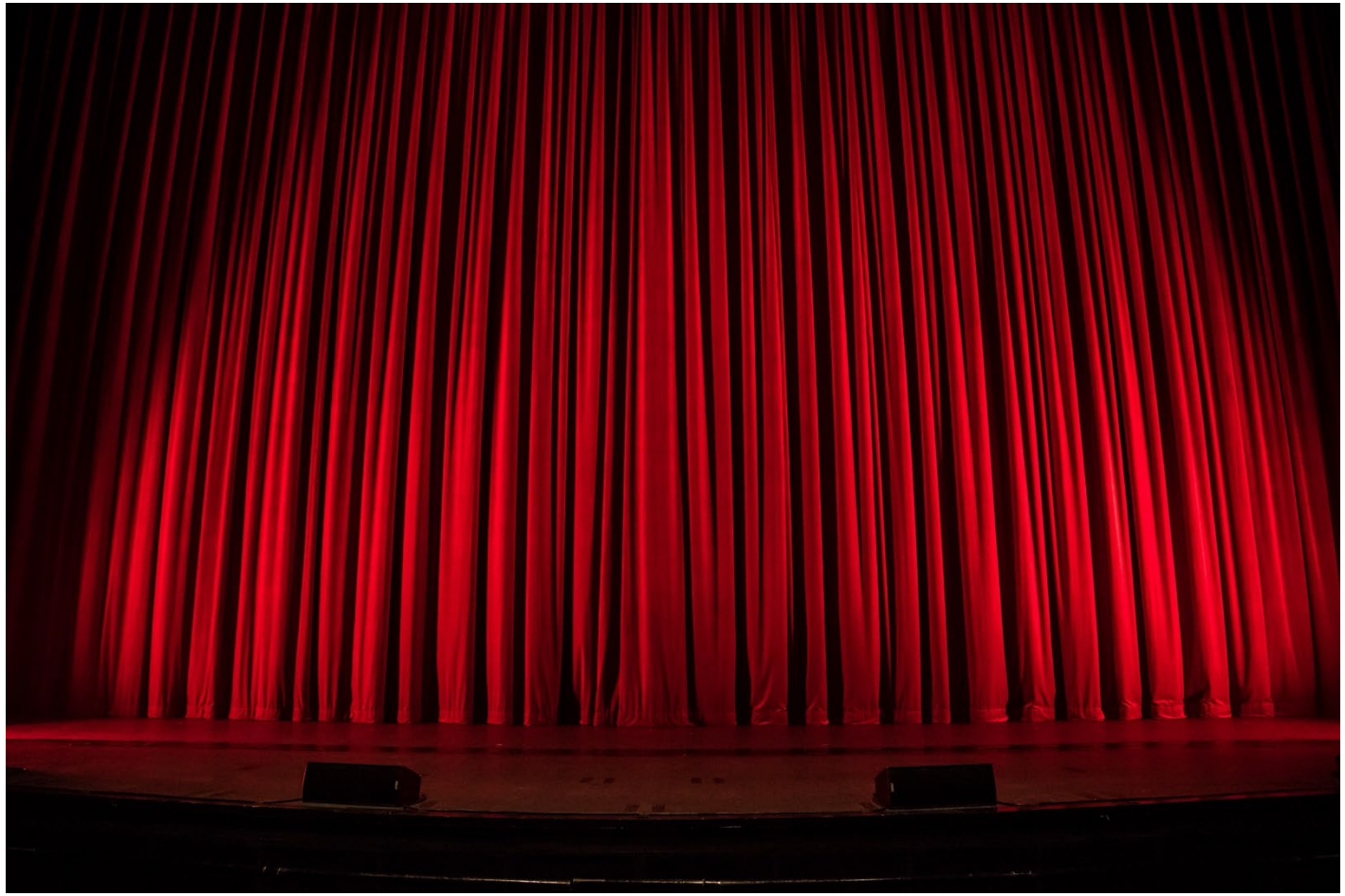
Correlation of **years in cybersecurity** and **relevance scores** for categories in Industrial Cybersecurity Knowledge

Strawman Category	**KTb**	**Sig**	**N**
Regulation and guidance	0.099	0.291	68
Common weaknesses	0.148	0.119	68
Events and incidents	0.157	0.095	68
Defensive technologies and approaches	0.008	0.938	68

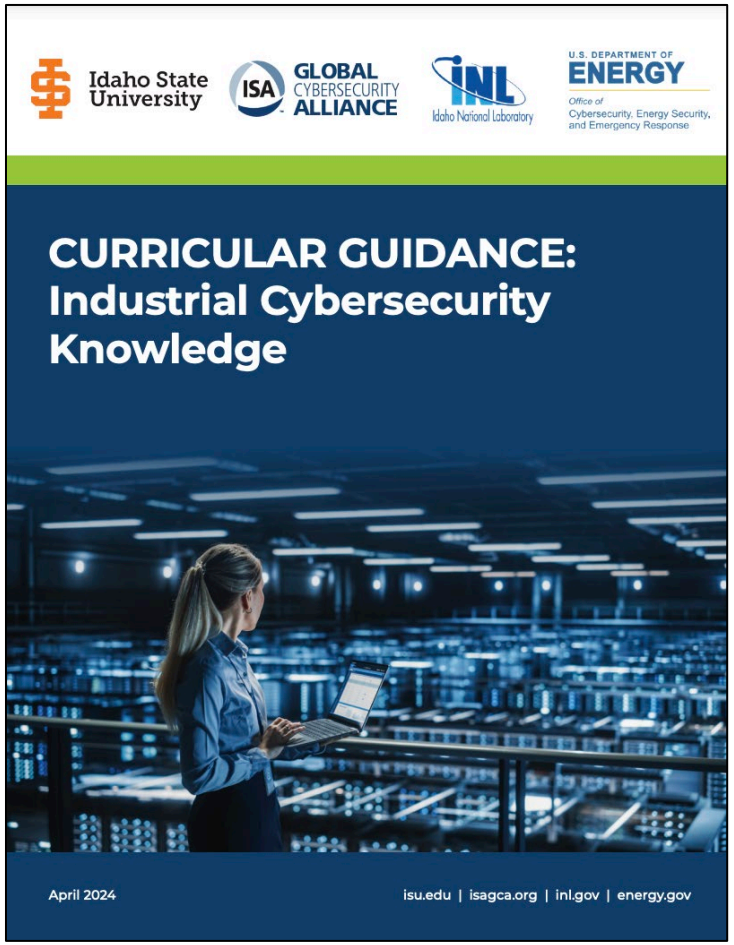
None of the KTb calculations meet the significance threshold of .05


Industrial cybersecurity
Events & Incidents
Events & Incidents
Events & Incidents
Analysis of events & incidents
Defensive Techniques
Managerial defensive techniques
Network defensive techniques
System & host defensive techniques
Instrumentation & control defensive techniques
Guidance & Regulations
Frameworks & paradigms
Guidance & standards
Regulations
Groups & Associations
Common Weaknesses
Managerial weaknesses
System & host weaknesses
Network weaknesses
Instrumentation & control weaknesses

“And now for the moment you’ve all waiting for…”



The Documents



Some errors in explanations have been identified.
ISA 99 WG 15 has agreed to manage change control

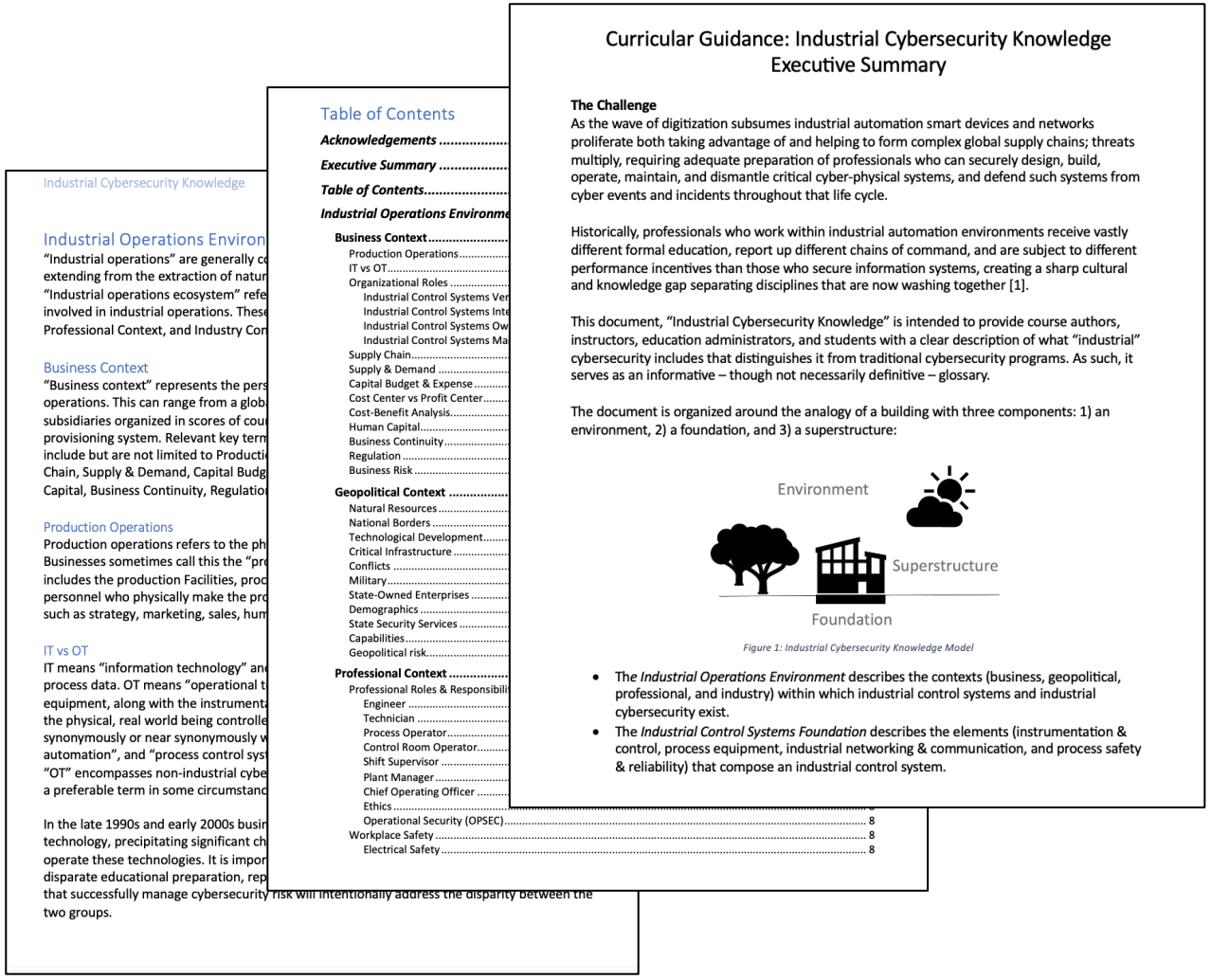
Overview

Essential reference for students and educators

3 Sections:

- Environment
- Foundation
- Superstructure

- 125 Pages
- 579 entries
- 7 hierarchical levels



Industrial Cybersecurity Knowledge

Industrial Operations Environ
"Industrial operations" are generally c
extending from the extraction of natur
"Industrial operations ecosystem" refe
involved in industrial operations. These
Professional Context, and Industry Con

Business Context
"Business context" represents the pers
operations. This can range from a glob
subsidiaries organized in scores of cou
provisioning system. Relevant key term
include but are not limited to Producti
Chain, Supply & Demand, Capital Budg
Capital, Business Continuity, Regulatio

Production Operations
Production operations refers to the ph
Businesses sometimes call this the "pr
includes the production Facilities, proc
personnel who physically make the pro
such as strategy, marketing, sales, hum

IT vs OT
IT means "information technology" an
process data. OT means "operational t
equipment, along with the instrumenta
the physical, real world being controlle
synonymously or near synonymously w
automation", and "process control syst
"OT" encompasses non-industrial cybe
a preferable term in some circumstanc

In the late 1990s and early 2000s busin
technology, precipitating significant ch
operate these technologies. It is impor
disparate educational preparation, rep
that successfully manage cybersecurity risk will intentionally address the disparity between the
two groups.

Table of Contents

Curricular Guidance: Industrial Cybersecurity Knowledge 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.

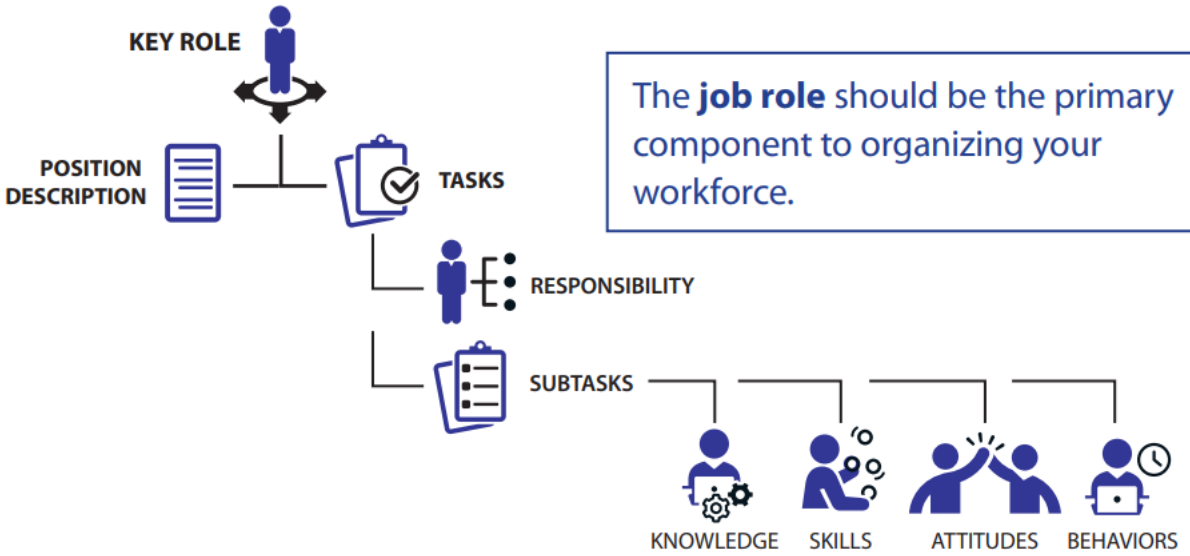
The document is organized around the analogy of a building with three components: 1) an environment, 2) a foundation, and 3) a superstructure:

Figure 1: Industrial Cybersecurity Knowledge Model

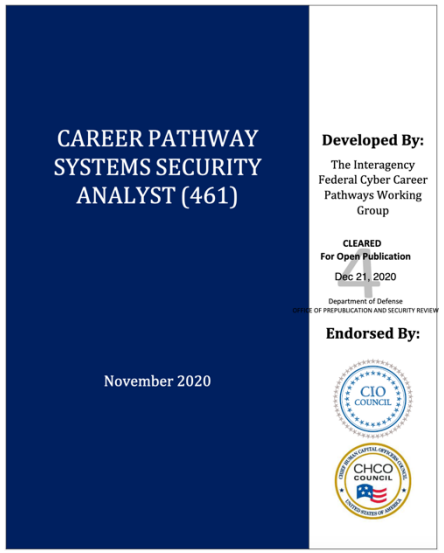
- The *Industrial Operations Environment* describes the contexts (business, geopolitical, professional, and industry) within which industrial control systems and industrial cybersecurity exist.
- The *Industrial Control Systems Foundation* describes the elements (instrumentation & control, process equipment, industrial networking & communication, and process safety & reliability) that compose an industrial control system.

Next Steps

- Need to refine and publish **OT-centric** Roles, KSABs, Tasks
- We have proposed an updated CAE KU for ICS
- We have worked with NIST to advance OT Security Engineering Work Role now open for comment
- Develop model curriculum



The **job role** should be the primary component to organizing your workforce.


CAREER PATHWAY SYSTEMS SECURITY ANALYST (461)

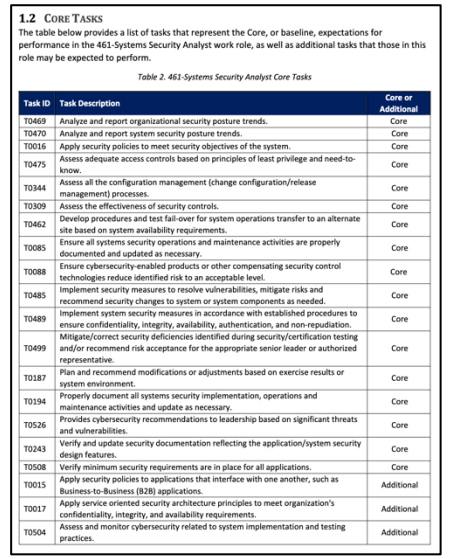
November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

CLEARED
For Open Publication
Dec 21, 2020
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Endorsed By:


1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 461-Systems Security Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 461-Systems Security Analyst Core Tasks

Task ID	Task Description	Core or Additional
T0469	Analyze and report organizational security posture trends.	Core
T0470	Analyze and report system security posture trends.	Core
T0016	Apply security policies to meet security objectives of the system.	Core
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.	Core
T0344	Assess all the configuration management (change configuration/release management) processes.	Core
T0309	Assess the effectiveness of security controls.	Core
T0462	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Core
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Core
T0088	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Core
T0485	Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.	Core
T0489	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Core
T0499	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Core
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.	Core
T0194	Properly document all systems security implementation, operations and maintenance activities and update as necessary.	Core
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Core
T0243	Verify and update security documentation reflecting the application/system security design features.	Core
T0508	Verify minimum security requirements are in place for all applications.	Core
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Additional
T0017	Apply service oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Additional
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.	Additional