
ISA
GLOBAL
CYBERSECURITY
ALLIANCE
A Global Consortium Working
to Secure Critical Infrastructure
ISAGCA Webinar Series

Curricular guidance to develop a new generation of industrial cybersecurity professionals

Sean McBride, PhD

Sean McBride, PhD

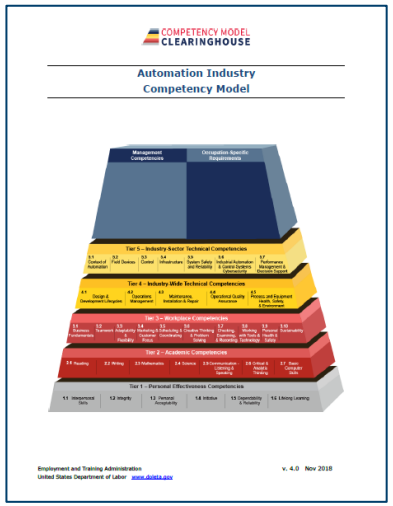
- 2006 SFS Graduate (MBA)
- 2006-2009 INL
  - Precursor to ICS-CERT
  - On first vulnerability disclosure coordination call
- 2009-2016 Critical Intelligence – iSIGHT – FireEye/Mandiant
  - Worlds first CI/ICS threat intelligence company
  - Top flight customers
  - Acquired by iSIGHT Partners
  - Director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

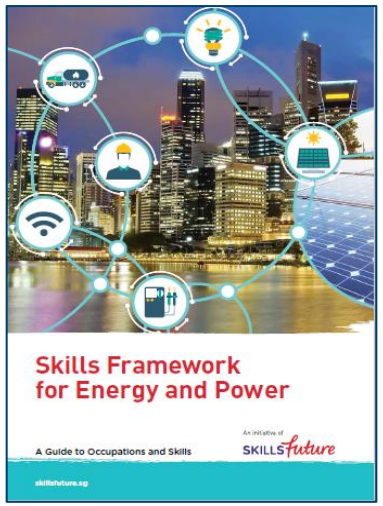
Pathway to here

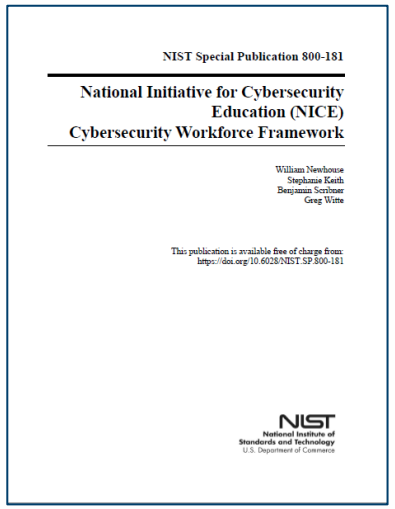
2018	2019	2020	2021	2021-22	2024
Lit Review →	Nominal Group Technique →	Focus Groups →	Strawman →	Survey →	Guidance Document

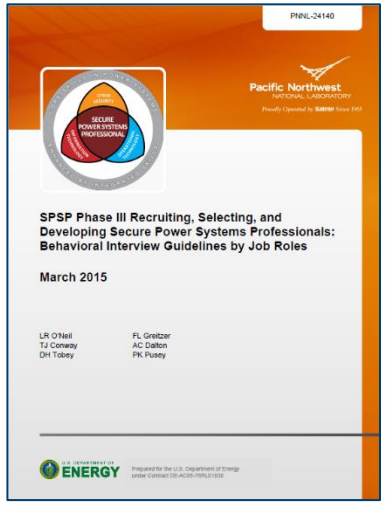
Searching for a standard

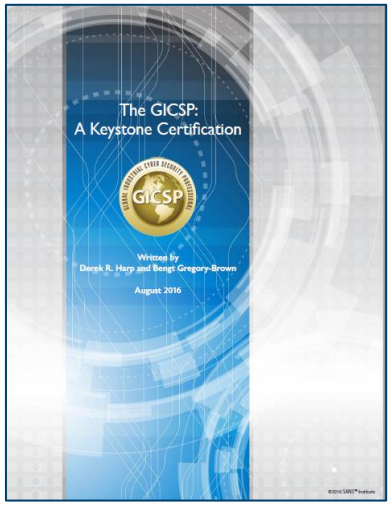
Idaho State University

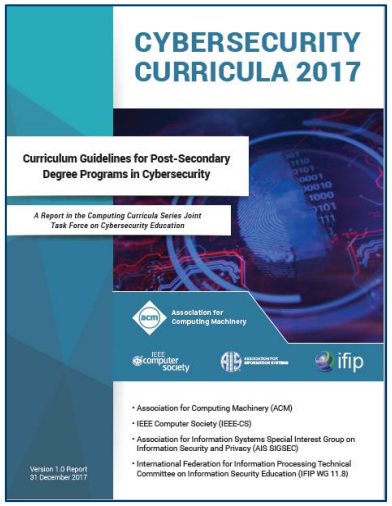


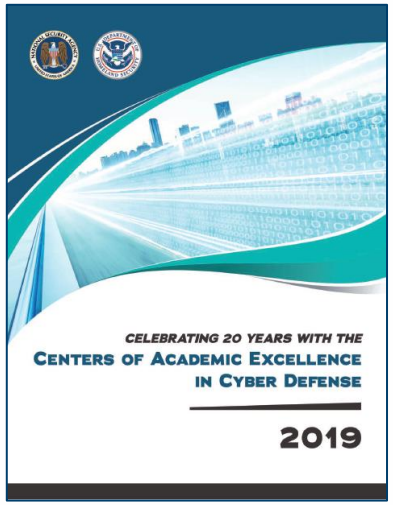










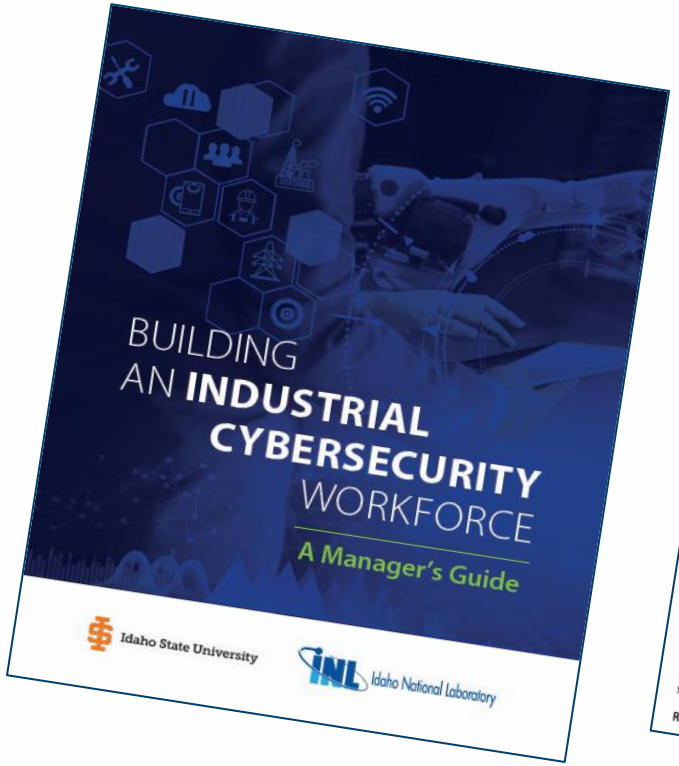


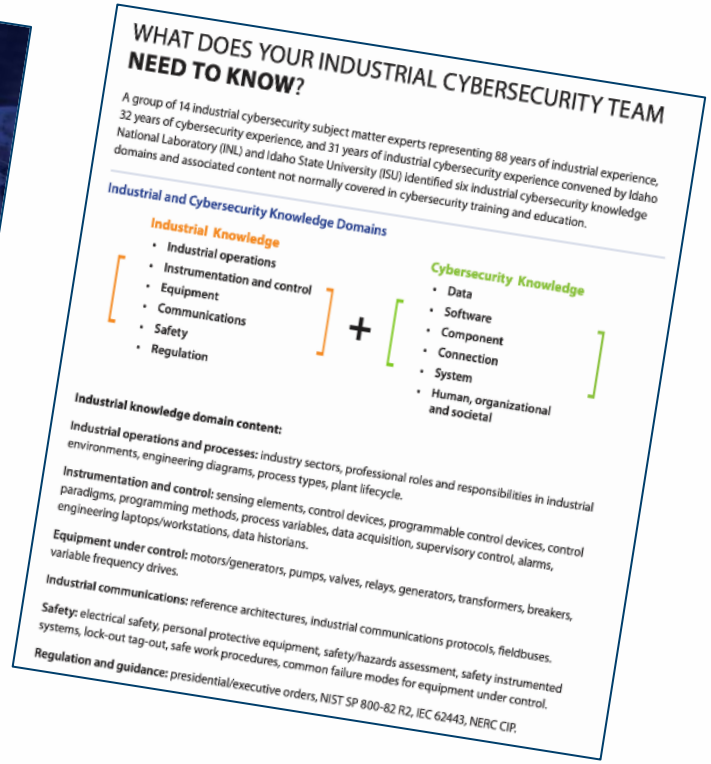
ISA GLOBAL CYBERSECURITY ALLIANCE

Deficiencies to address

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

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.

https://inl.gov/wp-content/uploads/2021/02/ICS_Workforce-ManagersGuide2021.pdf

Survey

Survey Questions Overview

~300 total questions

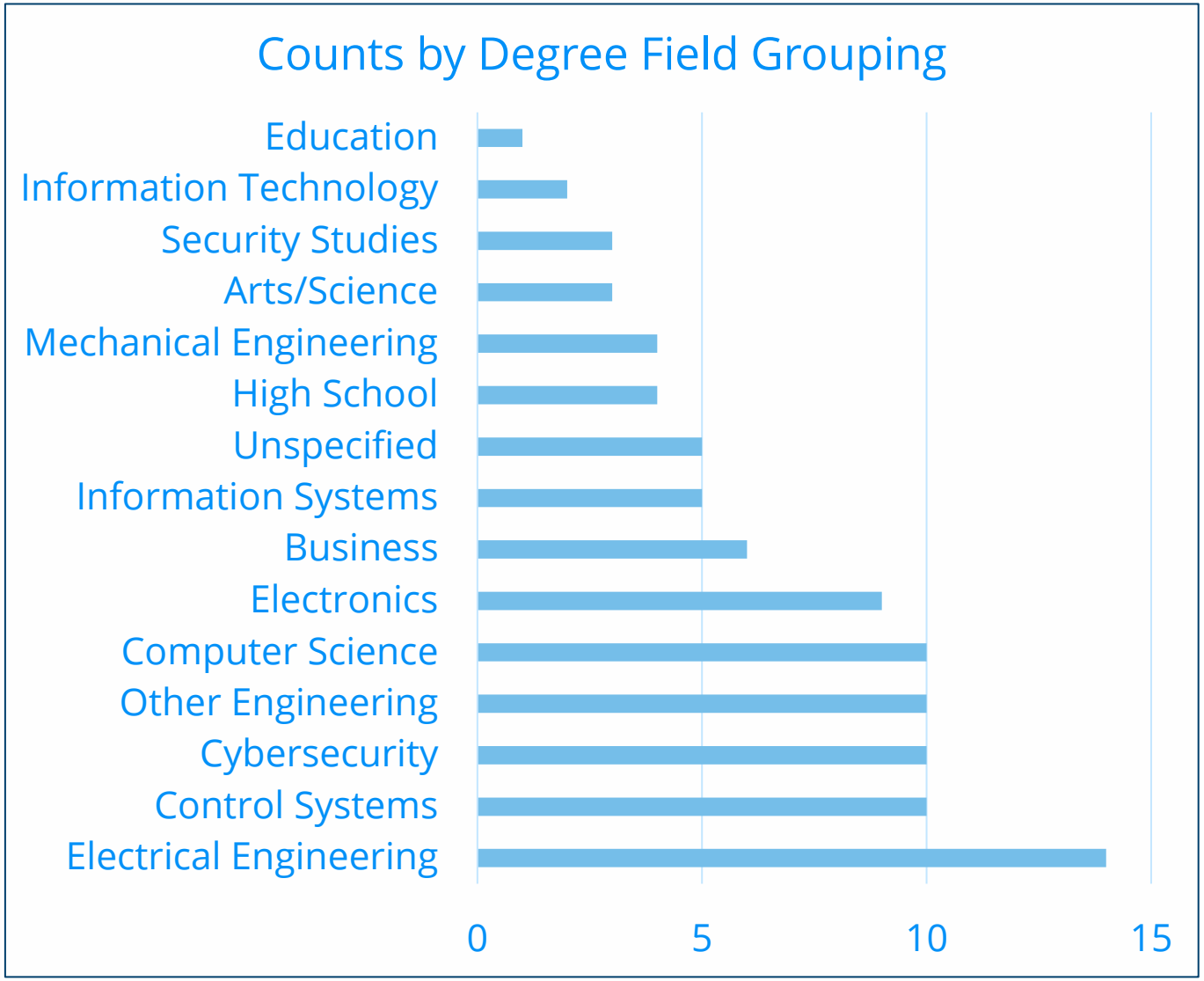
Three Sections

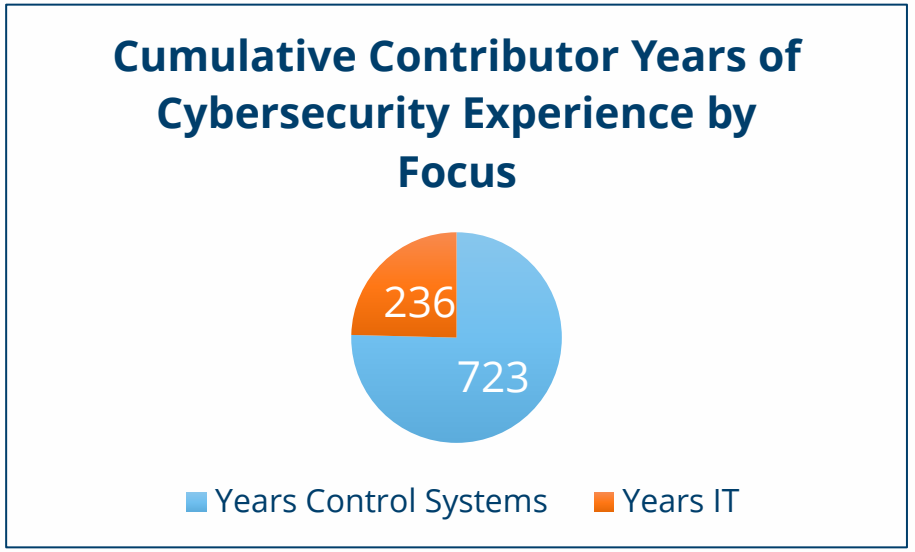
1. Respondent Background
2. Foundational ICS knowledge
   - Five categories
   - 41 Topics
3. ICS Cybersecurity knowledge
   - Four categories
   - 29 Topics

For each category and topic

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

Respondents: New Voices!





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.

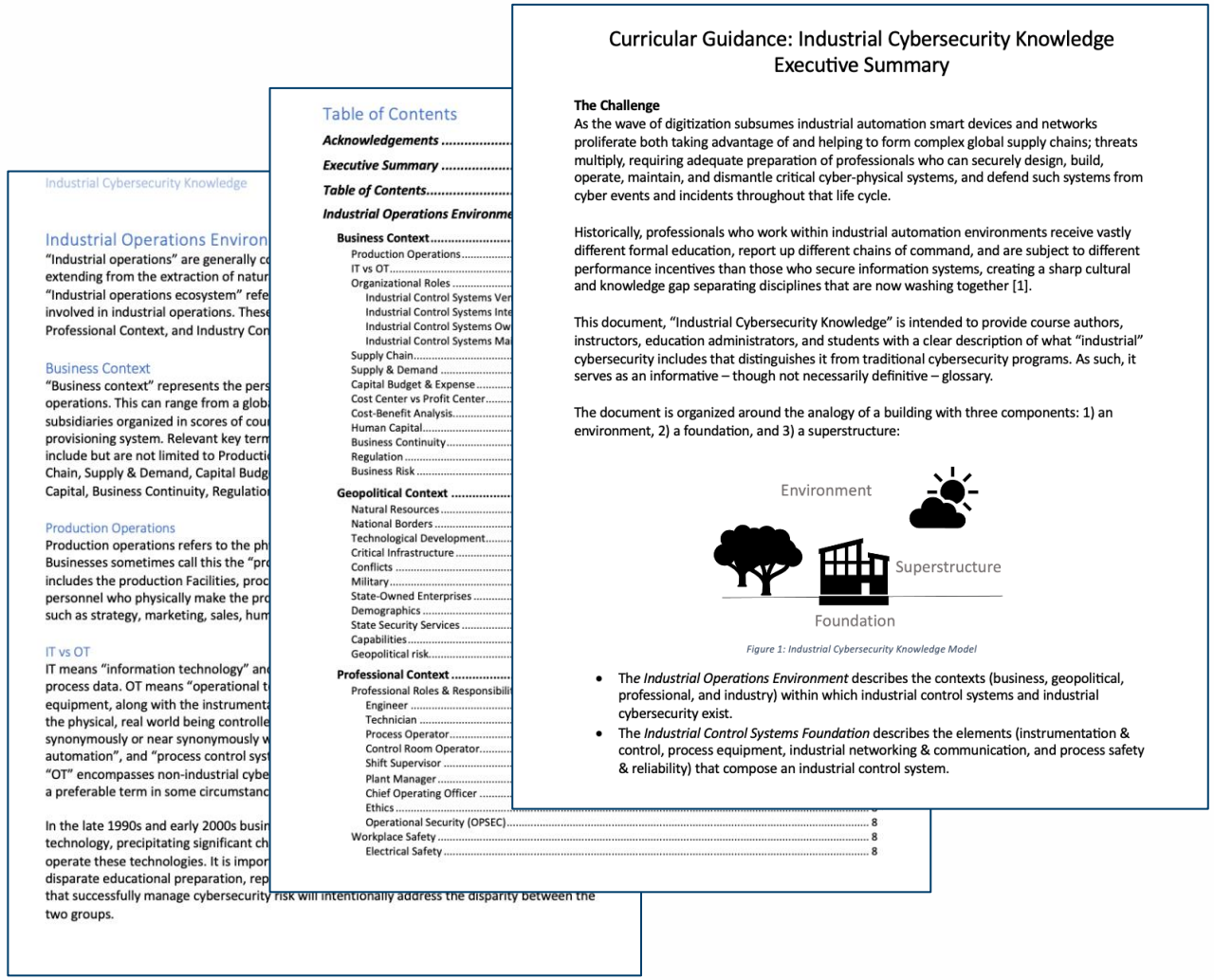
The Document

Essential reference for students and educators

3 Sections:

- Environment
- Foundation
- Superstructure

- 125 Pages
- 579 entries
- 7 hierarchical levels



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.

Table of Contents

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 globa
subsidiaries organized in scores of cou
provisioning system. Relevant key term
include but are not limited to Productio
Chain, Supply & Demand, Capital Budg
Capital, Business Continuity, Regulatio

Production Operations
Production operations refers to the ph
Businesses sometimes call this the "pro
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

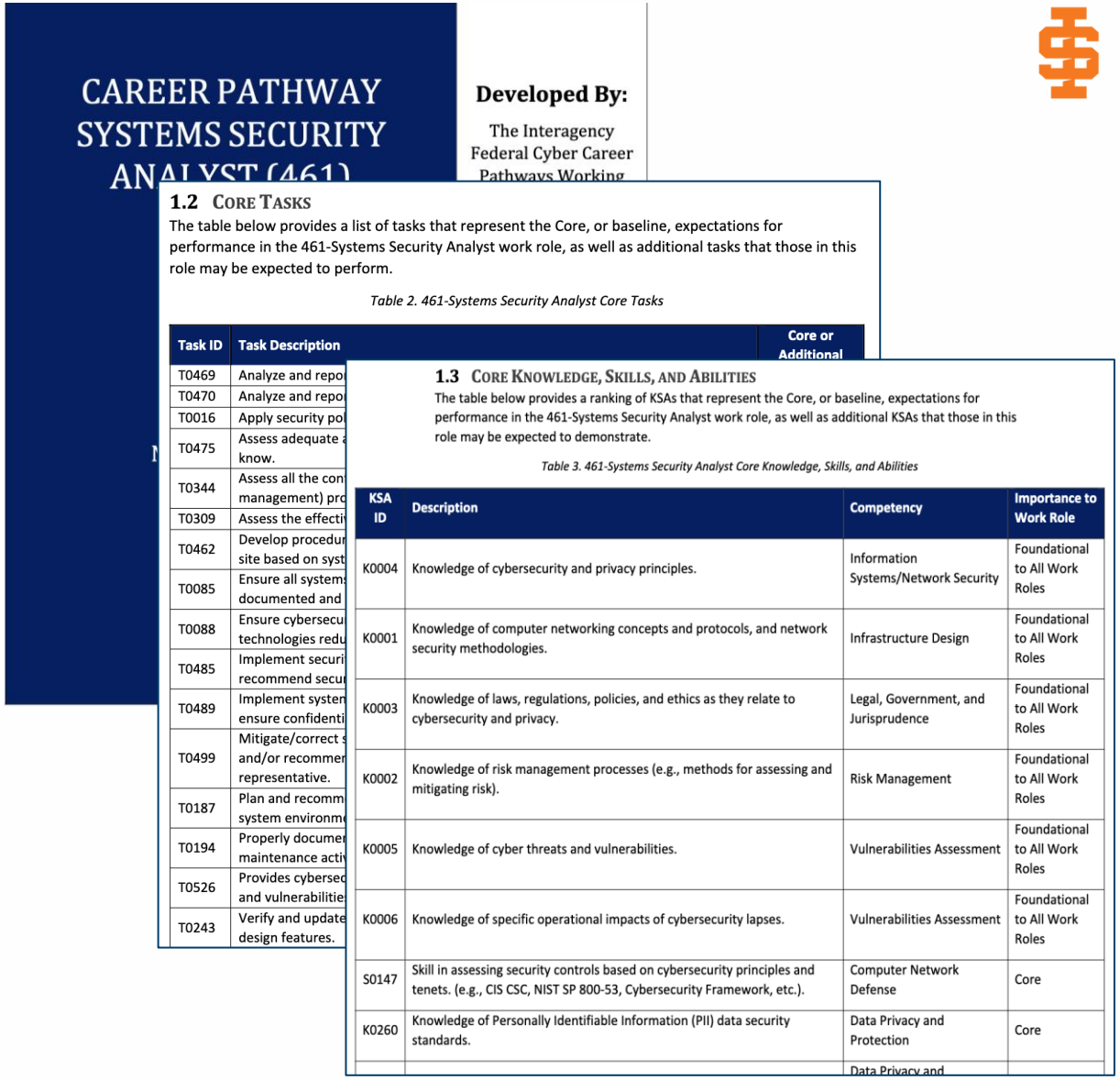
In the late 1990s and early 2000s busir
technology, precipitating significant ch
operate these technologies. It is impor
disparate educational preparation, rep
that successfully manage cybersecurity risk will intentionally address the disparity between the
two groups.

Publication!

- ISA (April 2024)
  - ISAGCA Webinar
  - ISAGCA Blog
  - Research materials hosted on ISAGCA Learning Technical Resources, (Training, Education, & Org Capabilities) include:
    - *Curricular Guidance: Industrial Cybersecurity Knowledge (Link)*
    - Analyses Survey question and Survey response data
  - ISA OT Cybersecurity Summit in London, June 2024
- Academic Journal/Conference (November 2024)
  - Academic paper on effort and results

Next Steps

- New ISA99 WG15: Automation and Control Systems Workforce Security Competencies and Models
- DOD and NIST have well-developed work roles and pathway documents for non-OT roles
- Need to refine and publish **OT-centric** Roles, KSABs, Tasks
- Use cognitive and behavioral approaches
- Develop model curriculum
- Align with current NIST NICE and DOE CIE efforts



CAREER PATHWAY SYSTEMS SECURITY ANALYST (461)

Developed By:

The Interagency Federal Cyber Career Pathways Working

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 repo	
T0470	Analyze and repo	
T0016	Apply security pol	
T0475	Assess adequate know.	
T0344	Assess all the con management) pro	
T0309	Assess the effecti	
T0462	Develop procedur site based on syst	
T0085	Ensure all system documented and	
T0088	Ensure cybersecu technologies redu	
T0485	Implement securi recommend secur	
T0489	Implement systen ensure confidenti	
T0499	Mitigate/correct and/or recommer representative.	
T0187	Plan and recomm system environm	
T0194	Properly documer maintenance acti	
T0526	Provides cybersec and vulnerabilitie	
T0243	Verify and update design features.	

1.3 Core Knowledge, Skills, and Abilities

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

Table 3. 461-Systems Security Analyst Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to All Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to All Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense	Core
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Core
		Data Privacy and	

Sean McBride
SeanMcBride@isu.edu

Be Part of the Movement to Prioritize OT Cybersecurity

Change the Culture

Recognize cybersecurity as a fundamental workplace tenet alongside functionality, efficiency, and safety

Learn more | www.isagca.org

ISA Cybersecurity Resources

Idaho State University

Free guidance, training, and more:

ISA Global Cybersecurity Alliance - www.isagca.org

A collaborative forum to advance OT cybersecurity and understanding of ISA/IEC 62443

ISASecure
www.isasecure.org

The world's leading conformance certification program for ISA/IEC 62443

ICS4ICS
www.ics4ics.org

Improve how cybersecurity incidents are managed with training, processes, and exercises

Get involved:

- ISA/IEC 62443 standards available from ISA (free access with ISA professional membership!)
- Cybersecurity training and certificate program
- Help develop the standard – open to all at no charge – www.isa.org/ISA99

ISA GLOBAL CYBERSECURITY ALLIANCE