A Security Workforce to Bridge the IT-OT Gap

Sean M. McBride, La Trobe University

Corey D. Schou, Idaho State University

Jill Slay, La Trobe University

September 2020

Abstract

The security ramifications of key differences between information technology (IT) and operational technology (OT) are now reaching the consciousness of professionals and academics alike. This paper presents a prototype education and training standard aimed to guide development of cybersecurity professionals who comfortably interact with both IT and OT systems.

Do you know OT?

Professionals and academics feel comfortable with the ubiquitous information technology (IT) ostensibly intended to make their lives more productive and enjoyable. Email, apps, video-calls, servers, memory and bandwidth, are essential techno-vocabulary employed in professional, educational, and even social settings.

But those professionals are only recently employing the term "OT" – operational technology – to describe the systems that connect IT systems with the real, physical world around them – bringing electricity to their businesses, natural gas to their stovetops, and water to their faucets.

As a blanket term, OT covers industrial control systems, supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), industrial sensors/transmitters, and actuators – likely arising from the fact that industrial firms often referred to the branch of the organization concerned with operating the aforementioned systems as "operations", or the "operations side of the house".

A desktop analysis and structured literature review of the term "operational technology" in academic and professional literature we performed (results in Table 1; details in the Appendix) found that the term "operational technology" is coming into more common usage, and that such usage frequently matches the definition described above (85% of all results; 95% since 2014). Notably, the term is used in *IEEE Std 1934-2018: IEEE Standard for Adoption of Open Fog Reference Architecture for Fog Computing*, giving it some official status.

Table 1. Use of "operational technology" in academic and professional literature.

Year published	**Includes term "operational technology"**	**Use matches definition**	**Primary focus is cybersecurity**	**Mentions gap between IT and OT**
1984-2013	11	0	0	0
2014	7	5	5	0
2015	7	5	1	1
2016	12	12	10	2
2017	20	19	7	6
2018	23	23	14	7
2019	25	24	20	13
Totals	104	88	57	29

What is the "IT-OT gap"?

The IT-OT gap refers to key differences between OT systems and IT systems. About one third of the papers that use the term "operational technology" consistent with our definition mention the gap (29 of 88).

The term is particularly common within the context of cybersecurity. Nearly two thirds of the papers that use the term consistent with our definition focus on cybersecurity (57 of 88). In fact, cybersecurity professionals were employing the term by at least August 2011, when Pescatore included it in an editorial comment to the SANS Newsbites newsletter [1]. We believe the term was advanced on the

SCADA Perspectives [2] or SCADASEC mail lists [3] from an earlier date, but remain unable to examine the complete archives of these lists to confirm that belief.

A personal experience

In 2016, a leading U.S. industrial control systems integration firm invited author McBride to address a group of operations personnel from the firm's key clients. Author discussed how the threat environment for industrial environments had evolved from the early 2000s, emphasizing how prevailing operational technologies were inherently vulnerable to cyber attacks due to inadequate consideration of abuse cases when the technologies were designed.

On the second day of the conference, the CEO of the integrator firm which had invited McBride, recapped day 1, including the cybersecurity presentation and discussion. A refinery operator, who likely possessed the most life experience of anyone in the room, raised his hand, and then explained in an annoyed tone of voice, "I appreciated everything about yesterday except the part about cybersecurity. I've been operating my refinery for 30 years. Never once has cybersecurity been an issue. I've been using the Modbus protocol for much of that time. It works exactly as intended. To me, cybersecurity is a self-fulfilling prophecy. The last thing I need is someone from IT showing up to tell me how to do things. They will shut down my plant."

Other personal experiences, and discussions with cybersecurity consultants who work regularly in industrial environments, confirm a common unfamiliarity, suspicion, and even distrust between the OT and IT groups.

Description of the IT-OT gap

Careful reflection led us to create the following table that characterizes various aspects of the IT-OT gap.

Table 2. Aspects of the IT-OT gap.

Aspect	**IT**	**OT**
Being controlled	Data	Physics
Measurement	Bits & bytes	Temperature, pressure, level, flow
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Lifecycle	System lifecycle	Facility lifecycle
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Controllability
Educational background of professionals	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical, Chemical, Mechanical Engineering

Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Accounting	Cost center	Profit center

We observe, that the "technology" of information technology is information-oriented – essentially an abstraction of the real world, used by humans to make decisions; whereas the "technology" of operational technology includes many technologies – information, mechanical, chemical, electrical – used by humans to control the real, physical world.

We quantify the data IT controls in terms of bits and bytes, but we quantify the physics that OT controls as temperatures, levels, flows, and in a variety of other ways. The security implications of this difference are enormous. Losing control of data can result in competitive disadvantage, embarrassment, financial loss; but, losing control of physics can mean loss of life. An IT security professional, who has never seen a temperature transmitter or a PLC or been through a facility safety briefing – much less set foot on a factory floor – is simply not prepared to grasp the impact of his or her decisions in the real world.

A cybersecurity analyst who is used to thinking only in terms of software lifecycles, is not prepared to consider the decade-long process of planning, designing and building a power plant, from environmental impact assessment and other regulatory approvals, to the quantity and diversity of suppliers and contractors that access the facility during buildout, commissioning, operations, and maintenance – a lead-time, quantity and diversity which provide nation-states adversaries an enormous advantage.

Traditionally trained cybersecurity personnel know well the desired system characteristics of confidentiality, integrity, and availability; but, they are not accustomed to thinking in terms of safety, reliability, and controllability. This difference in engineering mindset is hard to overstate – in part because it is engrained in the disparate educational pathways that professionals often travel. Instrument technicians, who calibrate flow meters, or engineers who program PLCs directly from their laptop have little idea about verifying the integrity of software they have downloaded or only running signed code. On the other hand, cybersecurity personnel may not realize that Windows machines in the control room cannot be patched without 1) the approval of the vendor whose software runs on Windows, and 2) sufficient preliminary in-house testing in order to keep the plant safe and reliable. Electrical engineers aren't often taking classes on cybersecurity, and cybersecurity personnel aren't often taking digital control theory.

This difference in world-view is strongly reinforced by job descriptions, reporting chains, and longstanding management objectives. Some facilities operate 24-7-365. Technicians, operators, and managers are always at the plant or on-call. Chain of command is clear and constant. Issues are reported to the shift supervisor and escalated to the plant manager – whose job is to keep quality product streaming onto waiting semi-trucks. The plant is a profit center. If it stops, the money stops flowing in. Consistency is expected. Emergency fixes, and even Patch Tuesday fall outside this operational reality.

In summary, what on the surface might look like a simple technology difference – or even a similarity – quickly runs into a deep chasm.

In case of a show-down between the plant manager and cybersecurity, the plant manager wins, because they are making the money – until the plant goes down due to a cyber event. And as plants continue to adopt conveniences of IT within and OT environment – events seem to increasingly occur. That is where we find ourselves now.

How this work fits in

While the term “operational technology” aptly highlights its key differences with information technology, professionals working in operational technology have historically called these systems “industrial automation” or “industrial control”. In deference to this fact, we prefer the term “industrial cybersecurity” over “OT cybersecurity” when referring to the security of OT systems. In support of this preference, we also note that the term “IT cybersecurity” is almost never used.

In previous work [4], we examined the lack of education and training standards for industrial cybersecurity in the United States. That work noted importantly that cybersecurity workforce development efforts often missed the formalized education pathways that industrial operations professionals travel – such as technical and engineering programs outside of computer science.

In [5], we found that international standards for industrial cybersecurity also lacked development. That work emphasized the desirability of differentiating among roles, and describing the tasks which each role performs.

Noting these needs, we set out to create a prototype workforce development framework consisting of 1) a role-oriented structure; 2) task-specific detail; 3) a description of foundational OT knowledge necessary for industrial cybersecurity professionals not normally covered in traditional cybersecurity training and education. We address each of these in turn.

Structuring an industrial cybersecurity workforce development standard

The structure proposed for the prototype industrial cybersecurity education and training standard is displayed in Figure 1, with the archetype role as the key organizing principle. Each role has a description and tasks. Each task has a responsibility level and subtasks. Subtasks may be divided farther into knowledge, skills, attitudes, and behaviors. We intend to develop, verify, and refine the items shown in grey boxes in future work.

We chose to include knowledge, skills, attitudes, and behaviors as opposed to grouped competencies because we find the detailed categories are more informative to instructional design than are competency lists. Moreover, we consider that a task list (included in this paper) along with a general knowledge list (to be provided in future work) is substantially similar to a competency list.

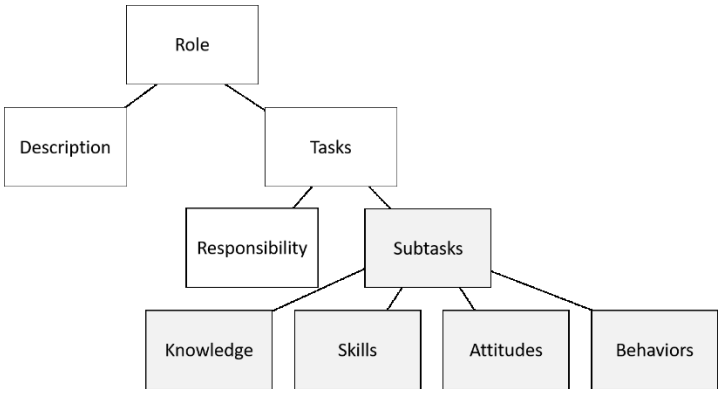

Figure 1. Hierarchical view of proposed structure.

Terminology

This section describes the key terminology advanced for use in the prototype standard, together with a rationale, and references to related previous work, which guided the descriptions. The order of the terms below matches the order one will likely encounter them within the prototype standard.

- Archetype Role

A general category of cybersecurity employee, intended as notionally rather than specifically prescriptive. The concept of archetype role was the result of a research effort using the nominal group technique described in [6].

- Description

A sentence or two that captures the essence of an archetype role, including key organizational relationships and key tasks.

- Task

Identifiable activities that form a significant part of the job role. Tasks are verb statements that may require specific knowledge, skills, and attitudes.

- Responsibility

A determination as to whether that archetype would have primary responsibility, shared primary responsibility, or supporting responsibility for the task.

- Sub-task

An identifiable step in accomplishing a task. Like a task, a sub-task is also a verb statement that may require specific knowledge, skills, and attitudes. The proposed structure adopts the simple task-detailing approach described by Mager [7].

- Knowledge

Cognitive ability dealing primarily with vocabulary. Knowledge is primarily a noun or noun-phrase.

- Skill

Psychomotor ability, requiring or implying corporal activity. Skills are verbs or verb phrases.

- Attitude

Emotional ability, requiring or implying emotional control. Emotions are generally knowns, but may include additional description.

- Behavior

Behaviors are identifiable habits of practice developed over time to improve efficiency and effectiveness. They describe techniques by which knowledge, skills, and attitudes may be combined to effectively accomplish a task or subtask. It is the "how" and "why-how" an expert performs a task or sub-task, not normally captured as part of the task. We note that this concept resembles aspects of Mager's Goal Analysis [7].

Differences from NIST NICE

As NIST NICE 2017 framework [8] is the most widely known workforce development framework for cybersecurity, it is worthwhile to describe key differences between it and the prototype herein advanced. Firstly, NIST NICE's primary organizational component is the security category; in the proposed prototype, it is the job role. We perceive that work roles commonly span the NIST security categories, making the categories a convoluting principle of organization.

Secondly, while the specialty areas used in NIST NICE seem like a useful distinction within each security category, this should be dealt with as a specialized role requiring specialized knowledge. Consequently, the proposed prototype eliminates the specialty areas within each category to preserve the flexible extensibility of the standard.

Thirdly, NIST NICE keeps KSAs separate from tasks. While we see the utility of using each KSA as an independently cataloged building block that can be adopted into roles as desired, and recognize that many tasks rely on similar KSAs – potentially making documentation discouragingly repetitive, we assert that significant value to all stakeholders lies in the ability to identify specific key KSAs for key tasks. Our structure, therefore, maintains the linkage.

Fourthly, the NIST NICE framework uses the term "ability", and the prototype uses "attitude". We prefer "attitude", as it maintains consistency with Bloom's domains (where knowledge corresponds to the cognitive domain, skill to the psychomotor domain, and attitude corresponds to the affective domain) [9], and to intentionally address the emotional aspect of human performance in professional settings, which is often overlooked in task or competency analysis (for example, NIST NICE mentions neither "attitude" nor "emotion"). We further note that the NIST NICE usage of "ability" seems practically indistinguishable from its use of "skill".

Fifthly, where NIST NICE does not incorporate the idea of sequenced decomposition of tasks, the prototype standard provides sub-tasks to describe the steps an individual would take to perform the identified task. Again, such decomposition is of use for instructional design.

Sixthly, NIST NICE does not explore the degree of responsibility any role has for the task: primary, shared primary, or supporting. Indicating responsibility is particularly useful for educators and students in describing possible workplace relationships, and prioritizing the amount of time and attention to dedicate to a task or concept.

Finally, the prototype standard employs the term "behavior" very differently. NIST NICE defines an ability as "competence to perform an observable behavior or a behavior that results in an observable

product". To us, a behavior is a technique an experienced professional has acquired or created to conduct tasks more efficiently and effectively. A behavior is not adequately reflected in knowledge, skills, or attitudes. One might think of "behavior" within the prototype model as "expert behavior". This difference, like those above, is of significant value for instructional design.

Task-oriented detail

In support of this effort, the Idaho National Laboratory, which has significant interest in developing industrial cybersecurity professionals, provided two collaborators with relevant experience in each archetype role. The collaborators met with the principal author to begin filling in the details of the proposed structure.

Archetype role: Industrial Cybersecurity Technician

Description:

The Industrial Cybersecurity Technician works among plant operations personnel to assure safety, reliability, controllability and cybersecurity of industrial control systems during installation, monitoring, troubleshooting, and restoration of industrial process operations.

Tasks:

Task No.	Task	Responsibility
1	Maintains ICS device inventory for security purposes	Primary
2	Participates in cyber security assessments affecting the industrial environment	Supporting
3	Reviews security architecture of ICS networks	Primary
4	Segments industrial control networks	Shared
5	Updates process software and firmware during process stoppages	Primary
6	Maintains backups of process control software	Primary
7	Maintains awareness of evolving external threat environment relative to internal systems	Primary
8	Controls physical access to systems	Shared
9	Provides input to development of internal ICS security policies and procedures	Supporting
10	Advises on secure implementation of process control equipment	Shared
11	Securely implements process control equipment	Primary
12	Advises incident response team relative to industrial environment	Supporting

13	Identifies and reports anomalies and suspected incidents	Supporting

Archetype Role: Industrial Cybersecurity Engineer

Description:

The Industrial Cybersecurity Engineer works within the engineering department to design and create systems, processes and procedures that maintain the safety, reliability, controllability and security of industrial systems in the face of intentional and incidental cyber events. Interfaces with Chief Information Security Officer, plant managers and industrial cybersecurity technicians.

Tasks:

Task No.	Task	Responsibility
1	Generate realistic, hypothetical cyberattack scenarios of serious physical consequence pertinent to the organization	Shared
2	Direct creation of industrial systems inventory and model for cybersecurity purposes	Primary
3	Design physical fail-safes to counteract potential cyber sabotage	Primary
4	Create prototype defensive technologies and approaches pertinent to the industrial environment	Shared
5	Advise development and operation of security operations center relative to the industrial environment	Primary
6	Propose cybersecurity policy and procedures related to industrial operations	Shared
7	Recommend security techniques, technologies, and approaches for adoption in industrial environment	Primary
8	Create cybersecurity inspection and test procedures for industrial systems	Primary
9	Review industrial system engineering plans and documentation for cybersecurity concerns	Primary
10	Review proposed cybersecurity policies and procedures related to industrial environments	Primary
11	Review equipment and software based on cybersecurity criteria	Primary
12	Optimize industrial system designs for security effectiveness and efficiency	Primary
13	Plan security related projects for industrial environment	Shared

14	Engage with external entities to ensure cybersecurity issues pertinent to industrial environment are addressed	Shared

Archetype Role: Industrial Cybersecurity Analyst

Description:

The Industrial Cybersecurity Analyst works among enterprise cybersecurity personnel to contextualize and synthesize threats, vulnerabilities and consequences relevant to industrial environments to provide strategic, tactical, and operational decision makers with perspective, options, and recommendations. The analyst liaises frequently with industrial operations personnel to gain perspective and vet practicality of possible courses of action.

Tasks:

Task No.	Task	Responsibility
1	Stays abreast emerging developments relevant to industrial cybersecurity	Primary
2	Dissects analytical requests	Primary
3	Collects information	Primary
4	Synthesizes information	Primary
5	Analyzes threats, vulnerabilities and consequences pertinent to industrial environments	Primary
6	Produces analytical products	Primary
7	Presents results	Primary
8	Proposes new work	Primary

Archetype Role: Industrial Cybersecurity Researcher

Description:

The Industrial Cybersecurity Researcher works to increase detailed knowledge about ways an industrial cyber-physical system may be compromised, and advance novel ways they may be protected. The researcher employs specific tools and techniques suited to their assignment, and often works alone, but engages expert-level resources as necessary. Reports must meet standards for clarity of technical content.

Tasks:

Task No.	Task	Responsibility

1	Understand system	Primary
2	Design and conduct tests	Primary
3	Discover vulnerabilities	Primary
4	Develop adversarial perspective	Primary
5	Recommend mitigations	Primary
6	Document and report findings	Primary

Archetype Role: Industrial Cybersecurity Manager

Description:

The Industrial Cybersecurity Manager is responsible to direct and oversee the work of industrial cybersecurity for all phases of the plant, product, and system lifecycles. The manager interfaces continuously with operations, IT, and cybersecurity personnel.

Tasks:

Task No.	**Task**	**Responsibility**
1	Prioritize efforts	Primary
2	Describe requirements per effort	Primary
3	Obtain and manage budget	Primary
4	Build the team	Primary
5	Run and improve the industrial cybersecurity program	Primary

Discussion of task-oriented detail

Given the imperative for developing an industrial cybersecurity workforce, and the weaknesses in previous efforts described in [4] and [5], we recommend that educational institutions and human resources departments inform their workforce development efforts with the prototype standard advanced herein.

We echo the warning advanced in [6] that the archetype roles are notionally rather than specifically prescriptive – meaning that educational institutions and employers should use their best judgement in creating a capable workforce.

We propose that the Industrial Cybersecurity Technician and Industrial Cybersecurity Engineer roles are the most significant contribution of this work, and are likely to have the largest influence on the actual security of industrial environments.

Of these, we assert that Technicians are the most often overlooked archetype, and note that technicians will require significant effort and resources to adequately train. We recommend close vertical integration between employers and education providers.

We anticipate that Industrial Cybersecurity Manager, Analyst, and Researcher archetypes will differ from non-ICS roles mostly in the knowledge they apply to the task rather than the task itself.

We anticipate significant value creation where individuals begin as technicians and advance into the other archetype roles where their hands-on recognition of how things work becomes a catalyst for creative and practical solutions.

We anticipate value creation where individuals with non-cybersecurity technician or engineer roles are introduced to cybersecurity tasks with accompanying KSAs.

We intend to conduct additional research that elaborates tasks into subtasks, and describes the knowledge, skills, attitudes and behaviors required of each task for each role. This work should rely on a suitable number of qualified participants as well as a variety of research methodologies, such as surveys, interviews, and field observations to account for both cognitive and behavioral aspects of task performance.

Foundational OT knowledge

Noting that since about 2014, the idea of a "knowledge unit" or "knowledge area" has become the prevailing organizational approach for cybersecurity curricula (two prominent examples include the National Science Foundation Centers of Academic Excellence Knowledge Units [10], and the CSEC 17 knowledge areas [11]), we determined to create a "knowledge unit" for industrial cybersecurity using the NSA CAE organizational structure.

As inputs, we considered first, the current NSA CAE Industrial Control Systems knowledge unit (Analysis Included as Appendix B); and second, the results of a nominal group technique session with 14 industrial cybersecurity subject matter experts, as described in [6].

Methodology

The author's reasoned that the statement of intent should be to prepare students to confidently interact with industrial control environments, and chose the phrase "ensure cybersecurity practitioners obtain a foundational understanding" to so indicate.

The author's reasoned that they could use the expert input from the sessions with INL subject matter experts as the topic areas – given that the experts had already produced a reasonable number of categories with clear, specific examples.

These were amplified by keeping the "common vulnerabilities" topic from the original list and adding a topic on defensive technologies and approaches – into which the original topic on "SCADA Firewalls" reasonably fits.

To create the outcomes, we sought to merge the "foundational understanding" phrase from the statement of intent with the detailed topics to describe what a student should reasonably be able to do

upon completion of the educational experience. So, verbs were limited to lower-level cognitive domain from Bloom's taxonomy: "describe", "identify", and "explain".

Finally, we employed key nouns from the outcomes to imbue the intent statement with foreshadowing continuity.

Proposed OT/ICS knowledge unit

Intent

The intent of the Industrial Control Systems (ICS) Knowledge Unit it is to ensure cybersecurity practitioners obtain a foundational understanding of industrial control systems, including their role in operating critical infrastructure, their key differences from information systems, their common vulnerabilities, and approaches to advancing their resilience.

Outcomes

Upon successful completion of this knowledge unit, participants should be able to:

1. Describe industrial control systems, including the names and functions of their common components
2. Identify several industry sectors and processes supported by industrial control systems
3. Explain how industrial control system environments differ from information system environments
4. Describe common weaknesses in industrial control system environments
5. Describe approaches to address common weaknesses while considering unique ICS characteristics and requirements

Topics

The following topics must be covered

- Industrial processes and operations (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)
- Common weaknesses (indefensible architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, 3rd party access)
- Defensive technologies and approaches (firewalls, data diodes, independent sensing and backhaul, ICS network monitoring, cyber-informed engineering, cyber process hazards assessment, cyber-physical fail-safes, awareness and training for ICS-related personnel)

Analysis of proposed OT knowledge unit

Anticipated Use

It is anticipated that this knowledge unit will be used to design or validate the content of a single course, or several modules within a course, taken by cybersecurity students. It is a solid starting point, yet insufficient to guide the creation of an entire industrial cybersecurity program.

We believe that Outcomes 3-5 (IT/OT differences, common weaknesses, unique defensive approaches) and Topics 6-8 (regulation, common weaknesses, defensive approaches) presented above would be helpful in developing cybersecurity awareness, training and education for individuals who already have an OT-related background.

Validation

In order to validate the topics 1-5 in the proposed knowledge unit, their content was compared to the Automation Competency Model developed by the United States Department of Labor (DoL) with support from the International Society of Automation (ISA) [12].

Of the 33 terms provided as parenthetical examples in the new topics, 27 are also found in the DoL model. Table 1 displays the locations of matches, as a useful resource for instructors seeking to use the updated knowledge unit. It is noted that five of the six terms missing a match are in the "Equipment under control category", which one might expect to find in the field of mechanical engineering rather than industrial automation. We maintain that these should still be included because this equipment directly influences the physical consequences of a cyber attack, and cannot be ignored. The remaining term not found in the DoL Automation Competency Model is "electrical safety". Here, we strongly propose that any cybersecurity professional who opens up a control enclosure in order to capture network traffic or update controller firmware requires a basic awareness of electrical safety.

Table 3. Comparison of proposed knowledge unit topic terms with Automation Industry Competency Model

Topic	**Term**	**Location in Automation Industry Competency Model**		
Industrial processes and operations	professional roles and responsibilities in industrial environments	3.2.1.1	5.6.19.3	
	engineering diagrams	5.2.14	5.3.13	5.5.13
	process types	4.2.7	5.1.6	
	plant lifecycle	4.1	4.1.6	4.1.7
Instrumentation and control	sensing elements	5.2		
	control devices	5.2		

	programmable control devices	5.3.12		
	control paradigms	5.3		
	programming methods	5.3.17		
	process variables	5.2.2		
	data acquisition	5.7		
	supervisory control	5.3.12		
	Alarms	5.5.7		
	engineering laptops/workstations	4.3.11.6		
	data historians	5.7.6		
Equipment under control	Motors	5.2.13		
	Pumps			
	Valves	5.2.4	5.2.5	
	Relays			
	motors/generators	5.2.13		
	Transformers			
	Breakers			
	variable frequency drives			
Communications	reference architectures	5.6.1	4.2.9.2	
	communications protocols	5.4.7	5.4.8	5.6.12.1
	Fieldbuses	5.4.7		
Safety	electrical safety			
	personal protective equipment	3.9.2.3		
	safety/hazards assessment	4.5.5	4.5.11.3	
	safety instrumented systems	5.5		
	lock-out tag-out	4.5.11.4		
	safe work procedures	4.5.11		
	failure modes for equipment under control	5.5.8.3		

Recommendations related to knowledge unit

We recommend that the NSF CAE effort adopt and incorporate the proposed knowledge unit, replacing the previous version (which the author's review in Appendix B).

While recognizing the importance of the role of the U.S. federal government in securing critical national infrastructures – which, importantly, include industrial control systems – we express concern that the great demand for all types of cybersecurity professionals, and the relative lack of this industrial cybersecurity expertise, is likely to keep industrial cybersecurity "lost in the crowd" to both educators and students.

A review of the CAE program web site reveals that only two CAEs have specialized in industrial control systems security (Idaho State University, and University of Houston) [7]. We opine that the availability of an optional knowledge unit (even an improved and robust version) is, by itself, unlikely to incentivize the level of professional development required by the dynamic technological and threat environments. Thus we recommend that the US government incentivize qualified individuals and institutions to develop entire programs that infuse engineering professionals – who design, build, operate, and maintain industrial control systems on which the industrial base of developed economies relies – with required cybersecurity competencies.

To this end, future work will leverage the research methods and results presented herein to develop more comprehensive curricular guidance styled after the CSEC-17 Cybersecurity Knowledge Areas [8] that can be used by such programs.

Acknowledgements

The authors acknowledge assistance of ten subject matter experts from the Idaho National Laboratory, including Matthew Anderson, Eric Burgan, Jeffry Hahn, and Curtis St Michel.

This work was supported in part by a scholarship from La Trobe University.

References

[1] J. Pescatore, in *SANS NewsBites Volume XIII - Issue #63*, Aug. 2011. Accessed July 2, 2020. [Online]. Available: https://www.sans.org/newsletters/newsbites/xiii/63

[2] SCADA Mail List. Internet Archive. Archive dated April 21, 2008. [Online]. https://web.archive.org/web/20080506124651/http://scadaperspective.com/

[3] SCADAGUARD, About scadasec. Internet Archive. Archive dated 8 February 2008. [Online]. Available: https://web.archive.org/web/20080620035757/http://news.infracritical.com/mailman/listinfo/scadasec

[4] S. McBride and J. Slay, "Towards Standards-Based Industrial Cybersecurity Education in the United States," 2020. [Online]. Available: https://industrialcyberforce.org/wp-content/uploads/2020/07/Towards-Standards-based-ICS-Security-Education-in-the-United-States.pdf

[5] S. McBride and J. Slay, "Criteria for International Industrial Cybersecurity Training and Education Standards," 2020. [Online]. Available: https://industrialcyberforce.org/wp-content/uploads/2020/07/Criteria-for-International-ICS-Security-Education-Standards.pdf

[6] S. McBride, C. Schou, J. Frost, and J. Slay, "An Initial Industrial Cybersecurity Workforce Development Framework," 2020. [Online]. Available: https://industrialcyberforce.org/wp-content/uploads/2020/08/An-Initial-Industrial-Cybersecurity-Workforce-Development-Framework.pdf

[7] R.F. Mager, *Making Instruction Work*, 2nd ed. Center for Effective Performance, 1997.

[8] W. Newhouse, S. Keith, B. Scribner, and G.White, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," 2017. National Institute of Standards and Technology, Washington, DC. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[9] B. S. Bloom, M.D. Engelhart, E.J. Furst, W.H Hill, D.R. Krathwohl, Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain. New York: David McKay Company, 1956.

[10] National Security Agency, "2020 Knowledge Units", n.d. [Online]. Available: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf

[11] D.L. Burley, M. Bishop, S. Buck., J.J. Ekstrom, L. Futcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattford, A. Parrish, "Cybersecurity Curricula 2017," 2017. [Online]. Available: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.

[12] Employment and Training Administration, United States Department of Labor, "Automation Competency Model" v.4, 2018. [Online]. Available: https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=automation

Appendix A

To gauge the evolving use of the term "operational technology", we reviewed the contents of the IEEE Xplore database. This search returned 104 results with publication dates between 1984 and 2020. We reviewed each paper to determine whether the term matched the definition provided above. We looked at the context of each paper to determine whether or not its focus was cybersecurity, and identified whether each paper mentioned a gap between IT and OT.

Pub. Year	Document Title	AR number*	Use of "Operational Technology"	Security primary context?	Gap?
1984	30/20-GHz domestic satellite communication system in the public communication network of Japan: Design and operation	1457328	unrelated	n	n
1991	Analysis tools in preparation for Radarsat revisited: Evaluation tools for SAR data exploitation	579595	not found	n	n
2001	A new method for valuing R&D investments: a qualitative and quantitative evaluation	952294	unrelated	n	n
2001	OSCAR-object oriented segmentation and classification of advanced radar allow automated information extraction	977114	unrelated	n	n

2002	The aeronautical data link: taxonomy, architectural analysis, and optimization	1067938	not found	n	n
2003	An integrated service and network management system for MPLS traffic engineering and VPN services	1251226	unrelated	n	n
2008	A Distributed Simulation Environment for Simulation Modeling in Operational Risk Management	4606672	unrelated	n	n
2012	Managing Technology in a 2.0 World	6136222	unrelated	n	n
2012	Next generation emergency management common operating picture software/systems (COPSS)	6223101	unrelated	n	n
2012	Implementation of Fuzzy neural-network genetic algorithm based on MCGS	6273257	unrelated	n	n
2013	Relative Navigation and Guidance Technologies for Rendezvous and Docking	6840663	unrelated	n	n
2014	Industrial systems: cyber-security's new battlefront [Information Technology Operational Technology]	6905657	related	y	n
2014	Remote monitoring and control of wastewater assets delivering reduced whole life costs	7129221	related	n	n
2014	Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety	7111736	related	y	y
2014	Optimizing Operational and Strategic IT	6908963	unrelated	n	n
2014	Observation and measurement in disaster areas using industrial use unmanned helicopters	7017671	unrelated	n	n
2014	Challenges & opportunities towards smart grid in Turkey; Distribution system operator perspective	7028940	related	n	n
2014	A new data classification methodology to enhance utility data security	6816451	related	y	n
2015	Eyes on the Ocean applying operational technology to enable science	7404390	unrelated	n	n
2015	Optimal control of Spacecraft Docking System using integral LOR controller	7229586	unrelated	n	n
2015	Leveraging Internet of Things Technologies and Equipment Data for an Integrated Approach to Service Planning and Execution	7166235	related	n	n
2015	6TiSCH centralized scheduling: When SDN meet IoT	7390418	related	n	n
2015	Factors for successfully integrating operational and information technologies	7273136	related	n	n
2015	State Based Network Isolation for Critical Infrastructure Systems Security	7070087	related	y	y

2015	A new integrated charging infrastructure analytics service platform and applied research	7324600	related	n	n
2016	Active defence using an operational technology honeypot	7857401	related	y	y
2016	IET: cyber security in modern power systems: IT and operational technology integration	7835824	related	y	n
2016	Cyber norms for civilian nuclear power plants	7836627	related	y	y
2016	Security threats of Internet-reachable ICS	7749239	related	y	n
2016	A private machine-cloud architecture and self-reliant controllers for operational technology systems	7822458	related	y	n
2016	Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security	7857397	related	y	n
2016	Using a knowledge-based security orchestration tool to reduce the risk of browser compromise	7849910	related	y	n
2016	The importance of testing Smart Grid IEDs against security vulnerabilities	7914920	related	y	n
2016	Cyber security in modern power systems defending the grid	7835822	related	n	n
2016	Grid-aware VPP operation	7514128	related	n	n
2016	Towards a new generation of industrial firewalls: Operational-process aware filtering	7906996	related	y	n
2016	Security intelligence for industrial control systems	7523351	related	y	n
2017	Practical security education on operational technology using gamification method	8284420	related	y	n
2017	Combining cybersecurity and cyber defense to achieve cyber resilience	8327227	related	y	n
2017	Cyber Security in the Energy World	8168583	related	y	n
2017	Industrial IoT business workshop on smart connected application development for operational technology (OT) system integrator	8289864	related	n	y
2017	Enhancing integrity of modbus TCP through covert channels	8270454	related	n	y
2017	Practical cybersecurity for protection and control system communications networks	8188738	related	y	n
2017	Poster Abstract: Design of Intelligent Software Systems for Cyber-Physical Systems	7946900	related	n	y
2017	Intelligent network assets supervision and control in Enedis	8316099	related	n	n
2017	Research on evaluation method for operation economy and technology of regional smart energy grid	8311207	related	n	n
2017	Challenges for citizens in energy management system of smart cities	7973850	related	n	n

2017	IEC 61850 beyond compliance: A case study of modernizing automation systems in transmission power substations in Emirate of Dubai towards smart grid	8356501	related	y	n
2017	A framework for consumer electronics as a service (CEaaS): a case of clustered energy storage systems	8013255	not found	n	n
2017	Cyber security in production networks â€" An empirical study about the current status	8247725	related	y	n
2017	RAMI 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges	8216593	related	n	n
2017	Benchmarking Cloud-Based SCADA System	8241099	related	n	y
2017	Big data and cloud computing platform for energy Internet	8388531	related	n	y
2017	Pay up - or else [IT Ransomware]	7908776	related	y	y
2017	Elektro Gorenjska CIM project	8316137	related	n	n
2017	Semantic communication between components for smart factories based on one M2M	8247690	related	n	n
2018	Effect of security education using KIPS and gamification theory at KOSEN	8405480	related	y	y
2018	VOTNET: HYBRID SIMULATION OF VIRTUAL OPERATIONAL TECHNOLOGY NETWORK FOR CYBERSECURITY ASSESSMENT	8632410	related	y	n
2018	On the Secure and Stable Operational Technology for Multi-DC Asynchronous Power-Sending Grid With High Proportion of Renewable Energy	8592525	related	y	n
2018	IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing	8423800	related	n	n
2018	IEEE Approved Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing	8388755	related	n	n
2018	Helping IT and OT Defenders Collaborate	8539125	related	y	y
2018	Ontology Based Resource Management for IoT Deployed with SDDC	8648642	related	n	y
2018	IT-OT Integration Challenges in Utilities	8586807	related	y	y
2018	IEEE Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing	8304857	related	n	n
2018	Implementing a performant security control for Industrial Ethernet	8642758	related	y	y
2018	Security Education Using Gamification Theory	8434432	related	y	y
2018	Dimensioning wireless use cases in Industrial Internet of Things	8402370	related	n	n
2018	Healthcare data classification â€" Cloud-based architecture concept	8337557	related	n	n

2018	SHARP: Towards the Integration of Time-Sensitive Communications in Legacy LAN/WLAN	8644124	related	n	n
2018	METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security	8659367	related	y	n
2018	Optimizing the Scheduling of Autonomous Guided Vehicle in a Manufacturing Process	8471979	related	n	n
2018	Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Networks	8585632	related	y	n
2018	Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems	8353121	related	y	n
2018	Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5	8350708	related	y	n
2018	Peer-to-peer Detection of DoS Attacks on City-Scale IoT Mesh Networks	8587518	related	y	n
2018	Cyberattacks on Primary Frequency Response Mechanisms in Power Grids	8625915	related	y	n
2018	Challenges and prospects of communication security in real-time ethernet automation systems	8402338	related	y	y
2018	The Industrial Internet of Things	8390825	related	n	y
2019	Integrating Cyber Security Requirements into a Power Management System	9074514	related	y	y
2019	Towards Virtualization of Operational Technology to Enable Large-Scale System Testing	8861980	related	n	n
2019	Technical risk synthesis and mitigation strategies of distributed energy resources integration with wireless sensor networks and internet of things â€“ review	8804868	related	y	y
2019	A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard	9035260	related	y	y
2019	Performance analysis of a Solar Photovoltaic Power Plant	8894937	unrelated	n	n
2019	Preventing False Tripping Cyberattacks Against Distance Relays: A Deep Learning Approach	8909810	related	y	n
2019	Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0	8858454	related	y	y
2019	Enhanced Uptime and Firmware Cybersecurity for Grid-Connected Power Electronics	8925027	related	y	n
2019	Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era	8651671	related	y	n
2019	Coexistence Standardization of Operation Technology and Information Technology	8667427	related	n	n

2019	MimePot: a Model-based Honeypot for Industrial Control Networks	8913891	related	y	n
2019	Towards Optimal Cyber Defense Remediation in Cyber Physical Systems by Balancing Operational Resilience and Strategic Risk	9021076	related	y	n
2019	Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure	8756895	related	y	y
2019	Securing connection between IT and OT: the Fog Intrusion Detection System prospective	8792884	related	y	y
2019	Cyber security threats in industrial control systems and protection	9079981	related	y	y
2019	Wireless Network Design for Emerging IIoT Applications: Reference Framework and Use Cases	8692410	related	n	y
2019	Factors Affecting Cyber Risk in Maritime	8899382	related	y	y
2019	A reference architecture for IIoT and industrial control systems testbeds	9038033	related	y	y
2019	Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins	8869197	related	y	n
2019	Forensic Readiness within the Maritime Sector	8899642	related	y	y
2019	Analyzing availability and QoS of service-oriented cloud for industrial IoT applications	8869274	related	n	n
2019	Intelligent Edge Control with Deterministic-IP based Industrial Communication in Process Automation	9012680	related	n	y
2019	Analysis and Detection of Cyber Attack Processes targeting Smart Grids	8905716	related	y	n
2019	Design and Development of Modbus/MQTT Gateway for Industrial IoT Cloud Applications Using Raspberry Pi	8997492	related	n	n
2019	Replacement Controller for IoT-Enabled Dependable Control Systems	9074603	related	n	n

* To retrieve the document, append the AR number to the following link:
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=

Appendix B: Analysis of Existing National Science Foundation Centers of Academic Excellence (NSF CAE) Industrial Control Systems Security Knowledge Unit

This section the contents of the existing 2020 Industrial Control Systems Knowledge Unit, found on page 64 of [10]. We look primarily at the Intent, Outcomes, and Topics.

Intent

The intent statement provides:

The intent of the Industrial Control Systems Knowledge Unit is to provide students with an understanding of the basics of industrial control systems, where they are likely to be found, and vulnerabilities they are likely to have.

Analysis

The statement of intent seems to target a student whose primary role will not deal with industrial control systems – it provides basics and focusses on the "likely". We would expect that the outcomes which follow the statement of intent would align with these three areas – but a careful review shows they do not.

We express particular concern that the statement of intent does not address key differences between industrial control systems and information systems – which would be a pivotal concern for anyone approaching this field.

The clause "where they are likely to be found" strikes us as strange, given that unlike hunting morels, the locations of industrial control systems, including the industries in which they exist and the processes they control, can be concretely described.

Outcomes

To complete this KU, students should be able to:

1. *Describe the use and application of PLCs in automation.*
2. *Describe the components and applications of industrial control systems.*
3. *Explain various control schemes and their differences.*
4. *Demonstrate the ability to understand, evaluate and implement security functionality across an industrial network.*
5. *Understand and compare the basics of the most used protocols.*

Analysis

Outcomes 1-3 and 5 seem reasonable for a student who only needs peripheral awareness of industrial control systems – they lack specificity and do not address the differences associated with securing OT vs IT environments. Based on the statement of intent, we would expect to see an outcome dealing with industries and processes which employ industrial control systems, but such an outcome is not provided.

We note that objective 4 is among the most complex and demanding of all objectives contained within the 2020 knowledge units: it requires demonstration of understanding, evaluation, and implementation of security across a contextual space to which most universities have limited access; it seems to surpass the scope of the statement of intent, and appears inconsistent with the nature of the other objectives within the same knowledge unit.

Topics

To complete this KU, all topics must be completed:

1. *SCADA Firewalls*
2. *Hardware Components*
3. *Programmable Logic Controllers (PLCs)*
4. *Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL)*
5. *Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25)*
6. *Types of ICSs (e.g., power distribution systems, manufacturing)*
7. *Models of ICS systems (time driven vs. event driven)*
8. *Common Vulnerabilities in Critical Infrastructure Systems*
9. *Ladder Logic*

Analysis

These nine topics offer little intuitive categorization or prioritization versus other topics or terminology not in the list. For example, are SCADA firewalls more useful than non-SCADA firewalls? To what does "hardware components" refer? Why does the protocol list not include HART or EtherNet/IP? Doesn't "Critical Infrastructure Systems" merit its own entry? Is ladder logic a higher priority than function block logic?

In addition to a more-intuitive structure, it would be more reasonable to see an appropriate pedagogical framework for industrial environments, as well as specific ICS-related regulatory requirements, included among the topics.