Open Access License Notice

BEST PAPER AWARD

What Does An OT Security Professional Need To Know?

Sean McBride
Informatics Research Institute
Idaho State University
Sean.McBride@isu.edu
0000-0002-4234-7358

Glenn Merrell
Freelance Consulting
Controls@FreelanceConsulting.com
0009-0003-3794-1728

Abstract—Industrial Cybersecurity is an emerging interdisciplinary field of study and practice. This paper presents the results of research and collaboration to create a data-supported and consensus-based curricular guidance document describing the knowledge needed of professionals in the field.

Keywords—*control system security, curriculum development*

I. INTRODUCTION

Industrial cybersecurity is an emerging interdisciplinary field, composed primarily of industrial automation and cybersecurity, but including elements of many other fields. It is the result of the global trend of technology advancement and digitization, wherein computers increasingly interact with and influence the physical world.

Since about the early 2000s, industrial cybersecurity has been shaped by 1) the discovery and disclosure of software vulnerabilities affecting industrial control systems, 2) unintentional safety events precipitated by flawed control systems design or maintenance, and 3) intentional cyberattacks motivated by enthusiasts, criminals, and geopolitical actors [1-3].

The trend of increasing automated control of the physical world creates a national and global security imperative to ensure these intelligent systems do not cause physical damage (or disaster) through either accident or intentional abuse.

This paper presents the results of a collaboration among government (U.S. Department of Energy Office of Cybersecurity, Energy Security and Emergency Response, and the Idaho National Laboratory), academia (Idaho State University), and industry (the International Society of Automation) to establish an appropriate educational foundation for creating a new class of engineering and technology professional – capable of moving seamlessly among previously disparate domains.

The paper is organized in typical academic fashion including a review of relevant literature, discussion of research method, presentation of results, and proposal of future work.

II. LITERATURE REVIEW

For this effort, the researchers were particularly interested in existing official guidance for creating cybersecurity professionals – with a focus on industrial automation and operational technology.

The researchers began by reviewing education and training guidance from nine organizations, including Accreditation Board of Engineering and Technology (ABET) [4], European Union Agency for Network and Information Security (ENISA) [5] , Global Information Assurance Certification (GIAC) [6], International Society of Automation (ISA) & Department of Labor [7], Task Force on Cybersecurity Education [8], National Institute of Standards and Technology [9], National Security Agency [10], Pacific Northwest National Laboratory [11], the Singapore Cyber Security Agency [12], and INL [13].

As the researchers examined the documents, they created a list of criteria that one would expect from a truly foundational curricular guidance document. The researchers then compared the criteria across the existing documents. A more-detailed treatment of the criteria can be found at [14]. The results of the comparison are summarized in Table I, where Y means yes, P means partial, N means no, and U means unknown.

TABLE I. Comparison of Curricular Guidance Efforts

Criteria	Curricular Guidance Efforts/Documents										Total Ys
	ABET	**ENISA**	**GIAC**	**ISA**	**JTF**	**NIST**	**NSA**	**PNNL**	**SF**	**INL**	
1. Addresses Industrial cybersecurity	N	Y	Y	Y	N	N	Y	Y	Y	Y	8
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	N	5
4. Qualified participants	Y	Y	Y	U	Y	U	U	Y	U	U	6
5. Publicly available	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	11
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	P	0
TOTAL Ys	3/8	5/8	5/8	4/8	4/8	2/8	3/8	5/8	3/8	3/8	

Perhaps the most important finding is that all the documents exhibited two complete deficiencies: 1) None of the documents "justified knowledge". That is, none of them provided a reason each term was included – its relevance to the field. 2) None of them provided "evidence of empirical validation". That is, none of them provided a detailed description of how their guidance was created, or the qualifications of their creators/contributors. They provided results, but only limited discussion of methods, and no raw data or data analysis.

In conclusion, a review of literature found a concerning lack of appropriately detailed and validated guidance among the bodies expected to advise the formal preparation of professionals to secure critical cyber-physical systems.

III. METHODOLOGY

Starting in Jan 2019, authors of [14-15] used the nominal group technique to engage a group of 14 professionals from the Idaho National Laboratory in creating an initial list of knowledge topics that would not normally be covered in a traditional cybersecurity course or program of study. The nominal group technique encourages broad perspectives by relying on anonymous, written responses rather than potentially political and emotional implications of verbal discussion/debate. The 14 professionals came from a variety of educational and professional backgrounds, totaling 31 years in industrial cybersecurity, 32 years in non-industrial cybersecurity, and 88 years in industrial operations.

The results of that work, ultimately published as "Industrial Cybersecurity Workforce Development: A Manager's Guide" by the Idaho National Laboratory [16], included two lists – one dealing with "industrial knowledge" and another dealing with "industrial cybersecurity". "Control systems knowledge" consisted of 45 items distributed across five categories. "Industrial cybersecurity knowledge" included 33 items spread across four categories.

As the researchers reviewed those lists, they recognized that while comprehensive curricular guidance would require program level learning objectives, course objectives, course sequence, schedule of topics, proposed learning activities, and evidence-based assessment methodologies, *knowledge* would be the most essential and straightforward component of consensus-based curricular guidance.

Recognizing that input from just 14 professionals was not sufficient to claim a consensus, the researchers determined to use the combined list from [16] as a strawman about which to elicit further expert insight.

Between November 2021 and March 2022, and with the assistance of the International Society of Automation (ISA) Global Cybersecurity Alliance (which advertised via an email to its members), the researchers administered a survey to professionals with interest and/or experience in industrial cybersecurity.

The survey included 363 possible inputs (some inputs were only displayed if the respondent answered in a certain way) divided into three sections:

1) Respondent Background – 19 possible inputs
2) Foundational Industrial Control Systems Knowledge – 205 possible inputs
3) Industrial Cybersecurity Knowledge – 139 possible inputs

As seen in Table II, the survey had 170 total respondents, 96 of which (56%) answered at least one question in survey Section 2. This group of "Contributors" spent an average of 49 minutes on the survey.

TABLE II. Respondents

Respondents	Number
Total	170
Contributors (answered at least one question in Section II)	96
Section II Finishers	70
Section III Finishers	65
Writers (provided textual input)	58

IV. RESULTS AND ANALYSIS

A. Analysis of Respondent Background

The survey asked up to 32 questions (depending on responses) to ascertain the education background, professional certifications, and professional experience of respondents.

Of the 96 Contributors, most had bachelor's degrees; engineering disciplines, including in control systems, accounted for 34 degrees, while computer science and cybersecurity accounted for 20 (see Tables III and IV). Of the 29 contributor respondents who had a Professional Engineer (PE) license, 23 reported a specialization in control systems (see Tables V and VI).

Contributor respondents claimed industry experience across a variety of industry sectors – predominantly in petrochemical and electric power (see Table VII) – and reported 1,085 cumulative years working for control system asset owners and control system integrators (see Table VIII). This experience was complemented by a cumulative total of 959 years working in cybersecurity, with more than ¾ of this time dedicated to control systems rather than IT (see Table IX). More than half of the contributor respondents held a professional cybersecurity certification, and one third held a certification specialized in industrial cybersecurity (See Tables X and XI).

TABLE III. Contributor Degree Levels

Highest Degree	Count
Bachelor	47
Master	33
Associate	6
Doctorate	6
High School Diploma/GED	4
Total	**96**

TABLE IV. Respondents by Degree Groupings

Degree Group	Count of Degree Grouping	Percent
Electrical Engineering	14	14.58%
Control Systems	10	10.42%
Cybersecurity	10	10.42%
Other Engineering	10	10.42%
Computer Science	10	10.42%
Electronics	9	9.38%
Business	6	6.25%
Information Systems	5	5.21%
Unspecified	5	5.21%
High School	4	4.17%
Mechanical Engineering	4	4.17%
Arts/Science	3	3.13%
Security Studies	3	3.13%
Information Technology	2	2.08%
Education	1	1.04%
Total	**96**	**100.00%**

TABLE V. Respondent Licensure

Licensed Professional Engineer?	Count
No	67
Yes	29
Total	**96**

TABLE VI. Respondent Licensure Specialty

PE Specialty (multiple allowed)	Count	Percent
Control Systems	23	79.31%
Electrical	10	34.48%
Industrial	6	20.69%
Other	5	17.24%
Mechanical	4	13.79%
Chemical	3	10.34%
Civil	1	3.45%

TABLE VII. Respondent Industry Focus

Industry (multiple allowed)	Total	Percent
Aerospace	15	16%
Power	42	44%
Chemical & Petroleum	48	50%
Mining & Metals	21	22%
Construction & Design	30	31%
Food & Pharmaceuticals	25	26%
Water & Wastewater	25	26%
Manufacturing	29	30%

TABLE VIII. Respondent Organizational Roles

Organizational Role	Cumulative Years
Asset Owner	543
ICS Integration Provider	532
ICS Supplier	200
ICS Maintenance Service Provider	161

TABLE IX. Respondent Cybersecurity Certifications

Cybersecurity Experience Category	Count
Control Systems	55
IT	41
Total	**595**

TABLE X. Respondent Cybersecurity Certifications

Cybersecurity Certification	Count
With	55
Without	41

TABLE XI. Respondent Industrial Cybersecurity Certifications

Industrial Cybersecurity Certification	Count
With	34
Without	62

The key take-away from the analysis of respondent background is that the survey reached an appropriately qualified group of professionals to address the important topic of industrial cybersecurity.

B. Analysis of Responses Relative to Strawman

Sections 2 and 3 of the survey, dealing with foundational control system knowledge and industrial cybersecurity knowledge, respectively, asked respondents to rank each category and topic provided in the strawman for relevance, and then choose whether to: keep as-is, change name, or remove entirely. If respondents chose “change name” or “remove entirely” they were prompted to make an alternate suggestion or justify their desire to remove the category or

topic in writing. All response data and associated analysis can be found at [16].

1) Analysis of Responses to Survey Section 2 – Foundational Control Systems Knowledge

a) Relevance

Respondents were asked to rank each term on a scale of 1 (irrelevant) to 10 (extremely relevant) for the field of industrial cybersecurity. Table XII shows the Kendall's Tau sub b correlation for "Years in Industrial Automation / Control Systems" with each category within the strawman.

TABLE XII. Correlation Among Categories and Respondent Experience in Industrial Automation

Term	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

This data shows that those with more experience in industrial automation tend to think that Safety and broad knowledge of the Industrial operations ecosystem are, respectively, more relevant than those with less experience. Correlations for both of these categories meet a p-value of .05 for statistical significance.

The researchers also ran the Kendall's Tau sub b correlation analysis using "Years in cybersecurity" as the comparative variable – as seen in Table XIII.

TABLE XIII. Correlation Among Categories and Respondent Experience in Cybersecurity

Term	KTb	Sig	N
Industrial operations ecosystem	*0.227	0.005	87
Instrumentation and control	0.141	0.091	87
Equipment under control	*0.188	0.020	87
Industrial communications	0.058	0.492	87
Safety	0.137	0.107	87

Those with most experience in cybersecurity considered the Industrial operations ecosystem and Equipment under control as highly relevant. Both of these categories meet a p-value of .05 for statistical significance.

When comparing the two correlation analyses, the most salient findings are that 1) those with more experience in industrial automation or more experience in cybersecurity tend to emphasize the relevance of the industrial operations ecosystem; and 2) those with more experience in industrial automation emphasize the relevance of safety

b) Keep, Change, or Remove

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

TABLE XIV. Respondent Choice Among Keep, Change, Remove by Topic

Cat.	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%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Industrial Communications		93	90%	8%	2%
	Industrial Communication Protocols	70	99%	1%	0%
	Reference Architectures	70	97%	1%	1%
	Transmitter Signals	70	94%	1%	4%
	Fieldbuses	63	95%	0%	5%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Safety		93	86%	10%	4%
	Safety Instrumented Functions	68	97%	1%	1%
	Electrical Safety	68	97%	0%	3%
	Safety/Hazards Assessment	68	96%	0%	4%
	Common Failure Modes for Equipment Under Control	68	96%	1%	3%
	Safe Work Procedures	68	93%	1%	6%
	Lock-out Tag-out	68	91%	1%	7%
	Personal Protective Equipment	68	90%	0%	10%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Valves	70	96%	3%	1%
	Motors	70	94%	3%	3%
	Pumps	70	94%	3%	3%
	Variable frequency drives	70	93%	3%	4%
	Generators	69	94%	1%	4%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Relays	70	91%	7%	1%
	Breakers	70	91%	3%	6%
	Transformers	69	91%	1%	7%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Equipment Under Control		93	85%	11%	4%
	Valves	70	96%	3%	1%
	Motors	70	94%	3%	3%
	Pumps	70	94%	3%	3%
	Variable frequency drives	70	93%	3%	4%
	Generators	69	94%	1%	4%
	Relays	70	91%	7%	1%
	Breakers	70	91%	3%	6%
	Transformers	69	91%	1%	7%

Cat.	Topic	Count	Keep as-is	Change title	Remove
Industrial Operations Ecosystem		92	82%	16%	2%
	Industry Sectors	77	97%	3%	0%
	Professional Roles and Responsibilities	77	96%	4%	0%
	Organizational Roles	77	96%	0%	4%
	Process Types	78	95%	3%	3%
	Industrial Lifecycles	77	96%	3%	1%
	Facilities	77	95%	5%	0%
	Engineering Diagrams	76	93%	5%	1%

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

Notwithstanding this general indication of acceptability, the researchers wanted to consider each suggestion for improvement on its own merits. Seventy-six respondents provided a total 342 suggestions for improvement. As some responses included multiple parts, this gave an atomized quantity of 461 responses.

One respondent offered 47 suggestions. Forty-five respondents offered just one or two suggestions. In addition, four responses from the Industrial Cybersecurity Knowledge Section were moved into the Foundational Industrial Control Systems Knowledge Section, for a grand total of 465.

Of the 465 responses provided, 278 (60%) were incorporated into the guidance. A summary of the final dispositions into the mutually exclusive dispositions appears in Table XV.

TABLE XV. Final Dispositions of Respondents Input by Category

Final disposition	**Count**
Directly accepted	91
Indirectly accepted	158
Note made in guidance document	29
Referred to cybersecurity section	53
Insufficient detail provided	53
No change	81
Total	**465**

c) Survey Responses for Which No Change Was Made

Table XVI shows that the 81 suggestions for which no change was made were place in four explanatory categories:

TABLE XVI. Categories Within Disposition "No Change Made"

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

The most common suggestion for which no change was made dealt with networking technologies. While such suggestions were generally out of scope (because the scope was limited to topics not covered in a traditional IT, computer science, or cybersecurity program), these suggestions highlight the importance of including traditional networking topics to adequately prepare industrial cybersecurity professionals in other forms of curricular guidance (such as a model curriculum).

Ultimately, the researchers chose to not change the term that received the highest score (16%) for "change title": Industrial Operations Ecosystem. To address the expressed concerns, the researchers chose to add four subcategories: Business Context, Geopolitical Context, Professional Context, and Industry Context.

d) Description of Changes to Survey Section 2

The most significant changes resulting from the review of each written response were: 1) alterations to category titles; and 2) the addition of subcategories and subtopics.

Changes to category titles are shown in the Table XVII

TABLE XVII. Strawman Categories VS. Final Categories

Strawman Categories	**Final Categories**
Industrial Operations Ecosystem	Industrial Operations Ecosystem
Instrumentation and Control	Instrumentation & Control
Equipment Under Control	Process Equipment
Industrial Communications	Industrial Networking & Communications
Safety	Process Safety & Reliability

2) Analysis of Responses to Survey Section 3 – Industrial Cybersecurity Knowledge

a) Relevance

Respondents were asked to rank each term on a scale of 1 (irrelevant) to 10 (extremely relevant) for the field of industrial cybersecurity. Table XVIII shows the Kendall Tau sub b (KTb) correlation coefficients for "Years in Industrial Automation / Control Systems" with each category in the strawman.

TABLE XVIII. Correlation Among Terms and Respondent Experience in Industrial Automation

Strawman Category	**KTb**	**Sig**	**N**
Regulation and guidance	0.172	0.073	65
Common weaknesses	0.025	0.797	65

Strawman Category	KTb	Sig	N
Events and incidents	0.152	0.114	65
Defensive technologies and approaches	0.169	0.091	65

This correlation analysis indicates weak positive correlation between experience in industrial automation and category titles, but this correlation is not statistically significant.

The researchers also ran the correlation analysis using "Years in cybersecurity" as the independent variable – as seen in Table XIX below.

TABLE XIX. Correlation Among Terms and Respondent Experience in Cybersecurity

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

This correlation analysis shows weak positive correlations between respondent years in cybersecurity and each of the category titles. None of these correlations was statistically significant.

b) Keep, Change, or Remove

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

TABLE XX. Response for Count, Keep As-is, Change Title, Remove for Section 3 – Industrial Cybersecurity Knowledge

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

Cat.	Topic	Count	Keep as-is	Change title	Remove
	ICS Network Monitoring	65	100%	0%	0%
	Cyber informed engineering	64	100%	0%	0%
	Process hazards assessment based	64	98%	0%	2%
	Cyber-physical failsafes	64	95%	0%	5%
	Awareness and Training for ICS personnel	64	100%	0%	0%

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

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

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

TABLE XXI. Final Disposition of Suggestions Provided in Survey Section 3 – Industrial Control Systems Knowledge by Category

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

c) Survey Responses for Which No Change Was Made

The 54 suggestions for which no change was made were classified into the four categories displayed in Table XXII.

TABLE XXII. Counts of Responses for Which No Change was Made

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

d) Description of Changes to Survey Section 3

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

A comparison between the strawman and the final list of categories and topics can be found at [17].

C. Creation of Category and Topic Descriptions

Once the list of categories and topics had been identified, the researchers set out to define and describe each of the key terms in a way that highlighted its importance to industrial cybersecurity. The researchers produced the 122-page "Curricular Guidance: Industrial Cybersecurity Knowledge" document [18].

The document is intended to provide authors, instructors, education administrators, and students with a foundational point of reference for knowledge items common in the field of industrial/OT cybersecurity. As such, it serves as an informative – though not necessarily definitive – hierarchical glossary.

The document is organized in two main sections: Foundational Industrial Control Systems Knowledge, and Industrial Cybersecurity Knowledge. Each section is further decomposed into categories, topics, and subtopics to reach a level of reasonable granularity.

While some topic names are identical to those found in traditional cybersecurity contexts, it describes the unique or

special considerations of those topics for operations environments.

The document makes extensive use of cross-referenced hyperlinks to facilitate navigation. A link at the bottom of each page quickly takes the reader back to the table of contents to navigate within the hierarchical structure.

V. CONCLUSIONS, LIMITATIONS, AND FUTURE WORK

A. Conclusions

This work set out to address two key deficiencies among existing curricular guidance for industrial cybersecurity: a) lack of a clear description of what was meant by the term "OT" or "industrial" cybersecurity; and b) lack of description of how the guidance was created.

To accomplish these objectives researchers implemented a multi-stage research methodology that 1) ensured broad participation from qualified professionals by recording respondent background, 2) administered the survey to a reasonably sized group, 3) performed a statistical analysis of respondents' perception of relevance, 4) considered every written suggestion for improvement, 5) incorporated nearly 2/3 of suggestions for improvement, 6) made the raw data and analysis freely available, and 7) crafted descriptions of each term to differentiate "industrial" or "OT" cybersecurity from traditional cybersecurity.

B. Limitations

The work presented herein is subject to limitations of both methodology and results.

1) Methodology Limitations

From a methodological point of view, it is possible that 65 survey finishers are not sufficient to claim consensus. The term "consensus" implies a group capable of raising meaningful objections has expressed satisfaction with the result. While the methodology employed showed that a vast majority of respondents (between 82% and 100%) chose "keep as is" for each term in the strawman, and the researchers incorporated each suggestion they considered possible, the researchers did not circle back to the survey respondents with the resulting guidance for another round of review.

To deal with these methodological limitations, the researchers suggest the creation of a web-based input form whereby interested individuals could provide ongoing suggestions for improvement, and that those suggestions receive consideration when the knowledge-based curricular guidance is updated from time to time.

In addition, during review of respondent comments, the researchers realized it was necessary to add some 292 unrequested topics, representing more than half (292 of 560) of the final term count. These additions were not subject to the same level of review as the initial strawman. However, a review of the actual dispositions shows that these terms clearly fall under/within the strawman categories or respondent-provided suggestions, and are consistent with the stated purposes of this research because they clearly describe what is meant by "OT" or "industrial" cybersecurity.

It should also be recognized that while the methodology did achieve its stated objective of clearly describing "OT" and "industrial" cybersecurity, it did not explore the question of what would be an optimal level of depth. Coverage may be too deep in some cases and not deep enough in others.

2) Results Limitations

From a content point of view, it is apparent that as the field of industrial cybersecurity evolves, the knowledge document will require periodic updates to address new developments. This is a struggle faced by any curricular guidance. Second, because the knowledge document intended to cover knowledge that is different from traditional cybersecurity, additional work will need to describe required knowledge that is the same as traditional cybersecurity. Finally, because the field is by nature interdisciplinary, topics such as industry sectors, process equipment, and communications protocols will require some discretion for appropriate implementation by instructors.

C. Future Work

From the perspective of the researchers, this work should be followed-up with the development of a model curriculum (or curricula). Such a curriculum should describe one way the knowledge described in this work can guide the development of engineering (engineers) or engineering technology professionals (technicians) who design, build, operate, maintain, dismantle, and defend operational technology environments.

A model curriculum should include IT, networking, and computer science topics not covered in the knowledge document. It should describe program level learning objectives, course objectives, course sequence, schedule of topics, proposed learning activities, and advance evidence-based assessment methodologies. Ideally learning activities would incorporate cognitive and behavioral instructional modalities that reflect both descriptive (what is currently done) and prescriptive (what should be done) practices.

REFERENCES

[1] Miller, A., Erickson, K. (2004). Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity. https://apps.dtic.mil/sti/tr/pdf/ADA447337.pdf, accessed August 2024.

[2] National Transportation Safety Board, Pipeline Accident Report Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire San Bruno, California September 9, 2010. https://www.ntsb.gov/investigations/accidentreports/reports/par1101.pdf, accessed August 2024.

[3] Falliere, N., O Muchu, L, Chien, E. "W32.Stuxnet Dossier". https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en, accessed August 2024.

[4] ABET. "Criteria for Accrediting Computing Programs , 2023-2024". (no date). https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/, accessed September 2024.

[5] European Union Agency for Network and Information Security, (2014). "Certification of Cyber Security skills of ICS/SCADA professionals". https://www.enisa.europa.eu/sites/default/files/publications/Certification%20Schemes%20at%20European%20level%20for%20Cyber%20Security%20Skills%20of%20ICS%20SCADA.pdf, accessed April 2025.

[6] Harp D., Gregory-Brown B. (2016.) The GICSP: A Keystone Certification. https://www.sans.org/reading-room/whitepapers/training/gicsp-keystone-certification-37232, accessed September 2024.

[7] Department of Labour (2009). Automation Industry Competency Model V. 4. (updated 2018). https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=automation, accessed September 2024.

[8] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E., Kaza, S., Levy, Y., Parrish, A. (2017). Cybersecurity Curricula 2017:Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, accessed September 2024.

[9] Peterson, R., Santos, D., Smith, M., Wetzel, K., Witte, G. (2020) "Workforce Framework for Cybersecurity (NICE Framework)". Accessed September 2024.

[10] Information Assurance Directorate (2020). "2020 Knowledge Units". https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf, accessed September 2024.

[11] O'Niel, L., Conway, T., Tobey, D., Grietzer, F., Dalton, A., Pusey, P. (2015). SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioral Interview Guidelines by Job Roles. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24140.pdf, retrieved September 2024.

[12] Cybersecurity Agency of Singapore "Operational Technology (OT) Cybersecurity Competency Framework" (2021). https://www.csa.gov.sg/resources/publications/operational-technology-cybersecurity-competency-framework--otccf-, accessed April 2025.

[13] Lampe, B., et al. Idaho National Laboratory "Cyber Informed Engineering (CIE) Curriculum Guide" https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_141694.pdf, accessed January 2025.

[14] McBride, S. (2021) Foundations of Industrial Cybersecurity Education and Training. https://opal.latrobe.edu.au/articles/thesis/Foundations_of_Industrial_Cybersecurity_Education_and_Training/19119443?file=33966695, accessed August 2024.

[15] S. McBride, C. Schou, J. Slay (2023). "Curricular Guidance to Bridge the IT-OT Cybersecurity Gap" in "Practical Guide to Security and Privacy in Cyber-Physical Systems" edited by P. Sharma and S. Goel. https://doi.org/10.1142/9789811273551_0007

[16] S. McBride (2020). "Building an Industrial Cybersecurity Workforce: A Manager's Guide". https://inl.gov/content/uploads/2023/07/ICS_Workforce-ManagersGuide2021.pdf, accessed April 2025

[17] "Supporting Docs" zip file. https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/Supporting%20docs.zip, accessed August 2024.

[18] McBride, S. (2024). "Curricular Guidance: Industrial Cybersecurity Guidance", https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/Industrial%20Cybersecurity%20Knowledge%20FINAL.pdf, accessed September 2024.