Criteria for International Industrial Cybersecurity Education and Training Standards

Sean McBride
PhD Student
La Tobe University
Melboure, Australia
s.mcbride@latrobe.edu.au

Jill Slay
Chair of Cybersecurity
La Trobe University
Melbourne, Australia
j.slay@latrobe.edu.au

***Abstract*—Industrial cybersecurity is an emerging global concern. Researchers of various nationalities examine the security of products from leading control system vendors. Cybersecurity events disrupt critical industrial processes that rely on those products throughout the world. Starting from the assertion that an appropriately prepared workforce is key to a resilient future, this paper critically reviews six efforts related to the development of education and training standards for industrial cybersecurity. It identifies criteria we expect would define such a standard, compares the efforts identified against those criteria, and makes recommendations for addressing this crucial need.**

Keywords—industrial cybersecurity, industrial control systems, education and training standards, international

I. INDUSTRIAL CYBERSECURITY IS A GLOBAL CONCERN

Since the early 2000s, the threat environment has evolved to include a constant stream of vulnerability disclosures affecting industrial control systems (ICS) software [1]. A review of those disclosures finds that firms and individuals from numerous countries were involved in their discovery. The companies that created the vulnerable software were likewise headquartered around the world.

Table I presents leading control systems vendors from four countries. It provides the number of vulnerabilities disclosed for each vendor as recorded in the U.S. National Vulnerability Database (NVD) as of May 26, 2020. This number includes third party products which the vendor product incorporates. The table also highlights a sample vulnerability disclosed in the identified vendor's products by a researcher with a differing nationality.

While vulnerability disclosures broadly indicate boots-on-the-ground international involvement in ICS security, actual incidents highlight the seriousness of the challenge. Table II summarizes key events industrial cybersecurity events in four countries, providing the common name of the incident, the date it occurred, and the ICS vendor whose products were affected, which allows correlation to table 1. The events listed for Canada and the United states seemed like preparations for cyber-physical incidents, whereas those listed for Ukraine and Saudi Arabia caused actual physical consequence. Various other publications (some of which we reference) cover these events in greater detail.

TABLE I. VULNERABILITY INFORMATION BY COUNTRY AND ILLUSTRATIVE ICS VENDOR

Attribute	**Country and Illustrative ICS Vendor**			
	France ***Schneider Electric***	***Germany*** ***Siemens***	***Taiwan*** ***Advantech***	***USA*** ***Emerson + GE IP[b]***
Percieved geographic market strength	Various markets worldwide	EMEA	Asia	USA
Number of vulns in NVD[a]	305	579	154	34+23=57
Illustrative vuln and percieved nationality of discloser	CVE-2011-4859; Ruben Santamarta; Spain [2]	CVE-2015-1355; Aleksandr Timorin; Russia [3]	CVE-2018-18999; Jacob Baines; United States[4]	CVE-2017-12732; David Atch; Israel [5]

[a.] From a search of the given vendor name in the U.S. National Vulnerability Database April 28, 2020

[b.] Emerson acquired GE Intelligent Platforms in February 2019

TABLE II. ILLUSTRATIVE ICS SECURITY EVENT BY COUNTRY

Attribute	**Victim Country**			
	Canada	***USA***	***Ukraine***	***Saudi Arabia***
Media term	Telvent Compromise [6-7]	Black Energy [8-9]	Industroyer [10-11]	Triton [12-14]
Year of event	2012	2014	2016	2017
Impact	Vendor cancelled remote support of pipeline SCADA	Adversary presence in networks	Power outage	Petro-chemical facility shutdown
Vendor of invovled ICS technology	Telvent (acquired by Schneider Electric)	GE Intelligent Platforms (acquired by Emerson)	Siemens	Schneider Electric

II. Review of International Efforts to Establish Training and Education Standards for ICS Security

Given the global nature of the ICS security challenge described above, and considering education and training to be a key component to addressing the challenge, we set out to identify and compare English language efforts led by non-US government bodies related to developing an industrial cybersecurity workforce. Our search identified six candidates[1], which we address in turn.

1) Accreditation Board for Engineering and Technology (ABET)

Postsecondary engineering and computer science schools throughout the world are commonly held to educational standards maintained by the Accreditation Board for Engineering and Technology (ABET).

ABET is a non-governmental organization composed of 36 member societies, including the International Society of Automation (ISA) and the Institute of Electrical and Electronics Engineers (IEEE), as notable examples [15].

In November 2018, ABET approved specific accreditation criteria for "cybersecurity" programs [16]. These criteria were developed by ABET's Computing Accreditation Commission, and have no mention of industrial applications.

The ABET Commissions that oversees programs producing professionals who will work in industrial automation environments are the Engineering Accreditation Commission (baccalaureate and master programs) and Engineering Technology Accreditation Commission (associate programs). The accreditation criteria for programs overseen by these Commissions does not address or even mention security.

2) Joint Task Force on Cybersecurity Education

The Joint Task Force on Cybersecurity Education is a composed of notable academic organizations: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information, Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). In 2017, the group published its landmark report "Cybersecurity Curricula 2017", which sought to define and formalize "cybersecurity" as its own academic discipline [17].

The Joint Task force went to significant effort to involve interested individuals from around the world in workshops and online surveys. The document is remarkable in its description of the effort, and its provision of more than 300 individual names who participated in its creation.

The report lists eight knowledge areas, each composed of knowledge units, essentials, and learning outcomes, which it intends to collectively "represent the full body of knowledge within the field of cybersecurity".

The term "industrial control systems", appears as a Topic under the Knowledge Area "System Security". The Description/Curricular Guidance field for this topic simply states "This Topic includes SCADA".

The term "cyber-physical system administration" appears as a topic under the Knowledge Area "Organizational Security". The Description/Curricular Guidance field for this topic defines cyber-physical systems and gives examples of what might be included in that topic.

We can see that the authors and contributors to this effort were inconsistent about what terminology to use, and the area into which the concepts best fit. In addition, they provided almost no curricular guidance on the topic.

3) European Union Agency for Network and Information Security (ENISA)

ENISA is an organ of the European Union. Industrial control systems security was a significant focus are for ENISA during the years 2011 to 2015, but the Website shows little beyond those dates [18].

The major publication related to educational standards for industrial control environments, "Certification of Cyber Security skills of ICS/SCADA professionals: Good practice and recommendations for developing harmonized certification exams", makes two significant contributions:

1. A high level description of training and certification needs for ICS Cyber Security professionals
2. A separate list of 12 knowledge areas that came from interviews with industry experts.

The high level description includes three management roles and eight technical roles. Authors listed learning goals for the technical roles as "to be determined", but followed up with a list of "high level overview of the knowledge areas that need to be developed" within the domains of "Industrial Automation, Control & Safeguarding", "Cybersecurity & Information Risk Management", and "General Information Technology".

The document reports that this description "has been adopted by the industry consortium developing the list of certification objectives and outcome statements that has been used by GIAC to develop the GICSP certification."

The list of 12 knowledge areas produced from interviews with industry experts includes:

- *Industrial Control Systems*
- *ICS Architecture*
- *ICS Modules and Elements Hardening*
- *ICS Security Governance and Risk Management*
- *Cyber security Essentials for ICS*
- *ICS Security Assessments*
- *ICS Security Monitoring*
- *Access Management*
- *Configuration/Change Management*

[1] The ISA Automation Federation effort (treated herein as document 6) was published by the US Dept. of Labor; however, the document clarifies that content was provided primarily by the ISA.

- *Physical Security*
- *Disaster Recovery and Business Continuity*
- *Incident Management*

It is evident that the ENISA groups were close to identifying specific educational objectives, but rather than complete this work, they folded their efforts into the Global Information Assurance Certification (GIAC) Global Industrial Control System Professional (GICSP) certification (which is discussed below).

The ENISA authors made the following nine recommendations related to certifications (though they also appear to apply to educational standards and educational offerings):

- *Obtain stakeholders' support to advance adoption of certifications*
- *Avoid commercial interests that may compromise the value of certification*
- *Ensure participation of professionals who know not only IT and cyber security, but also have specific OT knowledge*
- *Deal appropriately with cross-sector contents*
- *Cover different positions involved with ICS security*
- *Obtain a critical mass of certificates to add credibility*
- *Avoid the appearance of too many similar certifications*
- *Adapt existing certifications to include ICS security topics*
- *Include practical aspects such as hands-on laboratories*

4) SANS GIAC

GIAC is the certification arm of the multi-faceted cybersecurity research and training company known as SANS. In 2013, GIAC launched the Global Industrial Cybersecurity Professional (GISCP) exam [19].

A 2016 document authored by Derek Harp, an employee of SANS, noted that the certification was led by a cross-industry steering committee composed of 12 individuals. A November 2018 telephone interview we conducted with Michael Assante, who spearheaded the GICSP certification for SANS/GIAC, indicated that more than 60 individuals had participated in the development process, mainly through online surveys [20].

Assante described the GICSP as a single general certification that did not account for differing roles. He used the analogy of medical professionals in the operating room - what must everyone know - from the surgical technician to the anesthesiologist.

Harp's report on the GICSP certification included 47 "competency objectives" . Each of these included a topic and a parenthetical list of example content. Of the objectives, we consider that only eight explicitly deal with concepts that would not normally be covered in an IT security course or certification [19].

A review of the SANS GICSP web site in May 2020 indicates that this list has been reduced to a more manageable set of ten "objectives and outcomes" statements [21]. However, other than using the term "ICS", none of the objectives elucidates anything that would be covered outside an IT security course or certification.

While Harp explained that one purpose of the GISCP exam was to "provide the springboard for ICS security training programs", the reduction of publicly available information useful for external organizations to create training programs indicates a move away from community advancement and towards commercial success of SANS training and GIAC certification. It is noteworthy that the ENISA report (discussed above) warned against this commercialization effect.

5) Singapore SkillsFuture (SF)

In October 2018, Singapore SkillsFuture, produced a set of documents aiming to match evolving workforce needs. This work lists cybersecurity competencies desired for some 25 specific occupations across Power Generation, Distributed Generation, Electricity Transmission and Distribution, Gas Systems Operations, Town Gas Production and Plant Maintenance, and Gas Transmission and Distribution [22]. These occupations required various combinations of seven "Operational Technology Cybersecurity" competencies:

- *Access Control Management*
- *Cyber Incident Management*
- *Cybersecurity Framework Application*
- *Detection and Monitoring Management*
- *Operational Technology Security Audit Management*
- *Operational Technology Security Design*
- *Threat and Vulnerability Management*

Close examination of the reference documents for each of these competencies reveals that just two of them -- Operational Technology Security Audit Management, and Operational Technology Security Design -- deal with specific "operational technology" knowledge or tasks [23-24].

Although each of these repeatedly employs the term "operational technology" neither one describes what differentiates "operational technology security" from information technology security.

For example, one Ability listed under the "Operational Technology Security Design" Task reads "Set direction for the organisation's operational technology security policies, frameworks and protocols, in line with business requirements and the external environment". But nowhere does the SkillsFuture framework elucidate why an information security person could not do that.

While SkillsFuture work should be applauded for its ambitious approach of building operational technology cyber security into a broad variety of job positions, it has not provided sufficient detail to guide training or education of these individuals.

6) International Society of Automation (ISA) and Automation Federation (AF)

The International Society of Automation is a professional society serving those involved in automating industrial facilities. ISA provides both training opportunities and certification for these professionals [25].

ISA has established two principal certifications of industrial automation professionals: Certified Automation Professional (CAP) and Certified Control System Technician (CCST) [26] -- neither or which are security-related. For both certifications, the ISA makes publicly available its common body of knowledge domains, task categories, task lists and supporting knowledge [27].

The ISA99 Committee has developed a series of standard practices related to industrial automation and control systems, which are published through the International Electrotechnical Commission (IEC) as the IEC 62443 series. The body has proposed 14 standards, seven of which have been published; four of those published are undergoing revision [28].

Though ISA does offer cybersecurity trainings based on the contents of the IEC 62443 standards [29], a review of the actual IEC 62443 series shows that the group has not advanced education or training standards. IEC 62443-2-1 Security Program Requirements for IACS Asset Owners encourages individuals be trained in accordance with their security responsibilities, but does not identify or describe individual roles and responsibilities for industrial cybersecurity. An April 2020 email exchange with Eric Cosman, who manages the ISA 99 standards development effort indicates that ISA views development of specific standards within the scope of interests, but without the scope of standards development.

In 2009, the Automation Federation, an organization sponsored by the International Society of Automation, released its Automation Competencies Model, developed in conjunction with the United States Department of Labor [30]. The document includes a two-page section "Industrial Automation and Control Systems Cybersecurity". The document clearly recognizes that differences between IT and OT exist, and provides a list of eight critical work functions:

5.6.1 Differentiate between IT and OT architectures and the operation of these architectures

5.6.2 Manage Cybersecurity risk as it relates to IACS

5.6.3 Determine and implement the appropriate tools and methods for IACS Cybersecurity

5.6.4 Understand zones and conduits identification

5.6.5 Understand Security Level (SL) per zone

5.6.6 Professional development to stay current on threats and remediation methodologies

5.6.7 Incorporate new and emerging cybersecurity defense technologies and trends into proposed solutions

5.6.8 Reassess risk as automation systems evolve

The document also identifies 13 Technical Content Areas: General, Networks, Operating Systems, Telecommunications, Information Assurance, System Lifecycle, Governance, Identify, Protect, Detect, Respond, Recover, and Standards. Unfortunately, the document does not elucidate exactly what the differences between IT and OT cybersecurity are, or how these differences should be treated. It does not divide cybersecurity tasks among differing roles.

III. Criteria for Establishing a Standard

Based on our review of the preceding documents, we created a list of criteria which we would expect to describe an acceptable international industrial cybersecurity education and training standard. We discuss these criteria below by providing a brief description and rationale for each. Then, in table 3, we map the criteria to the international efforts we identified.

1) Addresses industrial cybersecurity.

Description: An appropriate standard would include the terms "industrial control", "SCADA", or "cyber-physical".

Rationale: This criterion provides an initial point of departure for the study. If the effort does not include the appropriate terminology it is not a candidate for considerations as a standard.

2) Differentiates industrial cybersecurity

Description: An appropriate standard would affirm that unique competencies are required for industrial cybersecurity in comparison with traditional cybersecurity education and training.

Rationale: This criterion takes criteria 1 to a greater depth. That industrial cybersecurity requires differentiated training and education is a cornerstone of this work, established by reasoning provided above.

3) Consensus-based

Description: An appropriate standard must intentionally involve diverse participants and perspectives, and ostensibly considered the full range of input provided.

Rationale: The quality of a standard is thought to depend on a full consideration of diverse perspectives.

4) Qualified participants

Description: An appropriate standard must address and record the qualifications of its participants.

Rationale: Broad consensus must be tempered with the academic and professional experience of participants.

5) Publicly available

Description: An appropriate standard and supporting detail must be publicly available on an official web site.

Rationale: For an educational standard to be of use, it must be readily available for application.

6) Includes job roles

Description: An appropriate standard must include a list of job titles to which the educational or training content relates.

Rationale: In order to be useful in career planning, and for human resource professionals including training

providers, the standard will link to possible position titles.

7) Includes tasks

Description: An appropriate standard must include a listing of tasks performed by specific job roles.

Rationale: While job titles are a positive step (Criterion 6), knowing the principle tasks each role performs facilitates instructional design, and enables assessment and evaluation.

8) Includes knowledge

Description: An appropriate standard must include a list of nouns that represent the working vocabulary of the field.

Rationale: Inclusion of vocabulary is an absolute necessity. This builds the first two criteria.

9) Sector-specific component

Description: An appropriate standard must include a way to address knowledge and skills that apply to a specific sector rather than generally across all sectors.

Rationale: Industrial processes differ across industries. Fundamental knowledge transfers, but a solid standard allows for sector-specific content.

10) Evidence of empirical validation

Description: An appropriate standard must justify that it is relevant in real life.

Rationale: If our goal is to develop an improved workforce, a solid standard would demonstrate its applicability.

IV. Candidate Standards to Criteria Mapping

Table III compares the cybersecurity education standards efforts identified above across these criteria. A "Y" represents adequate achievement or incorporation of criteria. "P" represents existence of evidence, but inadequate performance. "N" represents no effort made. "Unk" represents the documentation was insufficient to discern.

TABLE III. Candidate Standards Mapped to Iidentified Criteria

Criteria	Standards Efforts					
	ABET	***ENISA***	***GIAC***	***SF***	***AF***	***JTF***
Addresses Industrial cybersecurity	N	Y	Y	Y	Y	N
Clearly differentiates industrial	N	P	P	N	Y	N
Consensus-based	Y	Y	Y	Unk	Unk	Y
Qualified participants	Y	Y	Y	Unk	Unk	Y
Publicly available	Y	Y	P	Y	Y	Y
Includes job roles	N	N	N	Y	N	N
Includes tasks	N	N	N	Y	Y	N
Includes knowledge	P	P	P	P	Y	P
Sector specific content	N	N	N	Y	N	N
Evidence of empirial validation	N	P	P	N	N	N
Industrial cybersecurity standard	**3.5/10**	**5.5/10**	**5/10**	**5.5/10**	**5/10**	**3.5/10**

It is important to recognize that the efforts reviewed above approached the issue of industrial cybersecurity standards from differing objectives. ABET, for example would not be expected to lead out in establishing new educational standards, but would seek to reasonably incorporate them into its program reviews.

ENISA sought to promote a broad policy solution to the industrial cybersecurity challenge, and thus explored professional certification (an outcome-orientation) rather than educational or training standards (a process-orientation). This explains the absence of roles, tasks, and sector-specific contents SANS is a for-profit company specializing in professional bootcamp style trainings. Its effort relied on heavily on industry professionals, with limited input from academics. This explains its choice to closely hold the details.

Singapore SkillsFuture was an effort of the Singaporean government that appears to have relied heavily on input from Singaporean utilities. This explains the focus on formalized roles and tasks, and sector-specific content, but limited inclusion of detailed cybersecurity security knowledge.

Automation Federation worked closely with the US Department of Labor, providing a format intended for use by employers. This was the only effort to include tasks – though it calls these "Critical Work Functions", and treats them at a purely conceptual level.

The Joint Task Force on Cybersecurity Education report was spear-headed and written by leading academics with U.S. government grant support, that incorporated input from industry professionals. This explains the focus on knowledge rather than roles and tasks. It also accounts for the report's sound documentation.

If we consider the criteria as a 10-point scale, where a Y earns one point, a P earns half a point, and an N or Unk earn 0 points, we conclude that SkillsFuture and ENISA came closest to producing an industrial cybersecurity educational standard, with a 5.5/10.

As we look across the ten criteria, we can see that at least one of the efforts earned a Y for criteria 1 to 9, with evidence of empirical validation – Criterion 10 – partially provided by ENISA and SANS. This indicates that the criteria are reasonable and achievable.

V. Charting a Path Forward

As international organizations progress towards a set of education and training standards that meets the 10 criteria, we

make the following recommendations for collaboration, methodology, format, and governance.

A. Collaboration

From our review flows the idea that the various organizations identified should participate in and collaborate on creating said standards. This participation could include: using email and social media to invite members to provide expert input, sending representatives to working group meetings, and publicly endorsing the results.

We warn though, that the collaboration could turn sour and even unfruitful without the firm commitment of a single, appropriately funded organization in the lead role.

B. Methodology

Our review indicates that the various organizations whose efforts we reviewed not only had differing objectives, but that they had differing methods. Hence, we recommend that the methodology for creating the standards incorporate:

1. Participation of a reasonable number of experts to support a claim of "consensus". We think that about 100 participants representing at least 50 distinct organizations is a reasonable number. It is round and large, yet achievable – considering the number of true experts in the field with a willingness to participate is still relatively small when compared to cybersecurity in general. This number appears to be easily larger than the number involved in any of the previous efforts.
2. A variety of elicitation approaches to ensure diversity of input and cross-checking of results. Methods may include: nominal group technique, focus groups, surveys, interviews, and perhaps most-importantly, field observation. Use of all or several of these methods will help ensure an appropriate mixture of cognitive and behavioral approaches, thereby tempering prescription with description, and theory with practice.

C. Format of results

Our review also finds that the format for communicating educational standards varied widely, as did the use of supporting educational terminology. We recommend that the standard:

1. Clearly define and justify the educational terminology it adopts.
2. Provide enough depth to meet the needs of both potential employers and educators. This should leverage previously knowledge domains where possible. It should incorporate job descriptions and job tasks. These tasks should be linked to supporting knowledge, skills, attitudes, and behaviors.

D. Governance/maintenance

As technology and the threat environment continue to evolve, so will workforce needs. The standards governance framework should include a mechanism for periodic review and improvement. We recommend that a governing body which already has a process in place for reviewing education and training standards, undertake this responsibility. Governance should include an openly accessible proposed change submission process that encourages creation of an evolving body of documented professional practice. Submissions should be reviewed no less than annually.

REFERENCES

[1] S. McBride, "Overload: Critical Lessons from 15 Years of ICS Vulnerabilities", 2016. [Online]. Available: https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security/rpt-industrial-control-systems-vulnerability-trend-report-2016.html. [Accessed: 05- Jun- 2020].

[2] U.S. Dept. of Homeland Security, "ICS Advisory (ICSA-12-018-01B)", [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-12-018-01B. [Accessed: 05- Jun- 2020]

[3] U.S. Dept. of Homeland Security, "ICS Advisory (ICSA-15-048-01)", [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-15-048-01. [Accessed: 05- Jun- 2020].

[4] U.S. Dept. of Homeland Security, "ICS Advisory (ICSA-18-352-02)", [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-18-352-02. [Accessed: 05- Jun- 2020].

[5] U.S. Dept. of Homeland Security, "ICS Advisory (ICSA-17-278-01A)", [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-17-278-01A/. [Accessed: 05- Jun- 2020].

[6] B. Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent", 2012. [Online]. Available: from https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/. [Accessed: 05- Jun- 2020].

[7] D. Peterson, "Telvent Compromised!" [Online]. Available: https://dale-peterson.com/2012/09/26/telvent-compromised/. [Accessed: 05- Jun- 2020].

[8] U.S. Department of Homeland Security, (2014). ICS Alert (ICS-ALERT-14-281-01E). [Online]. Available: from https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B. [Accessed: 05- Jun- 2020].

[9] K. Wilhoit, "A Virus in Your Pipes: The State of SCADA Malware", 2015. [Online]. Available: https://www.first.org/resources/papers/conf2015/first_2015_-_wilhoit-_kyle_-_malware_in_your_pipes_20150630.pdf. [Accessed: 05- Jun- 2020].

[10] A. Cherapanov, and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", 2017. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. [Accessed: 05- Jun- 2020].

[11] A. Geenberg, "'Crash Override': The Malware That Took Down A Power Grid. Wired", 2017. [Online]. Available: https://www.wired.com/story/crash-override-malware/. [Accessed: 05- Jun- 2020].

[12] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer,"Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html. [Accessed: 05- Jun- 2020].

[13] L.H. Newman, "Menacing Malware Shows the Dangers of Industrial System Sabotage", Wired, 2018. [Online]. Available: https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/. [Accessed: 05- Jun- 2020].

[14] B. Sobczak, "The inside story of the world's most dangerous malware", EENews, 2019. [Online]. Available: https://www.eenews.net/stories/1060123327. [Accessed: 05- Jun- 2020].

[15] ABET, "Member societies" 2019. [Online]. Available: https://www.abet.org/about-abet/member-societies/. [Accessed: 05- Jun- 2020].

[16] ABET, "ABET Approves Accreditation Criteria of Undergraduate Cybersecurity Programs", 2018. [Online]. Available: https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/. [Accessed: 05- Jun- 2020].

[17] 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. [Accessed: 05- Jun- 2020].

[18] European Union Agency for Network and Information Security, "ICS SCADA", 2019. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada. [Accessed: 05- Jun- 2020].

[19] D. Harp, "The GICSP: A Keystone Certification", 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/training/gicsp-keystone-certification-37232. [Accessed: 05- Jun- 2020].

[20] McBride, S. Personal telephone interview with Michael J. Assante. 2018.

[21] GIAC, "Cyber Security Certification: GICSP", 2020. [Online]. Available: https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp. [Accessed: 05- Jun- 2020].

[22] SkillsFuture Singapore, "Skills Framework for Energy and Power: A guide to occupational skills", 2018. [Online]. Available: https://www.skillsfuture.sg/-/media/SkillsFuture/Initiatives/Files/SF-for-Energy-and-Power/Collateral.pdf?la=en. [Accessed: 05- Jun- 2020].

[23] SkillsFuture Singapore, "Operational Technology Security Design", 2018. [Online]. Available: https://www.skillsfuture.sg/-/media/SkillsFuture/Initiatives/Files/SF-for-Energy-and-Power/TSCs/PDF/11-Operations-and-User-Support/Operational-Technology-Security-Design.pdf?la=en. [Accessed: 05- Jun- 2020].

[24] SkillsFuture Singapore,"Operational Technology Security Audit Management", 2018. [Online]. Available: https://www.skillsfuture.sg/-/media/SkillsFuture/Initiatives/Files/SF-for-Energy-and-Power/TSCs/PDF/11-Operations-and-User-Support/Operational-Technology-Security-Audit-Management.pdf?la=en. [Accessed: 05- Jun- 2020].

[25] ISA, "About ISA", n.d. [Online]. Available: https://www.isa.org/about-isa/. [Accessed: 05- Jun- 2020].

[26] ISA, "Certification Programs", n.d. [Online]. Available: https://www.isa.org/training-and-certifications/isa-certification/. [Accessed: 05- Jun- 2020].

[27] ISA, "CCST Level I, II, III Examination Content Outline", n.d. [Online]. Available: https://www.isa.org/uploadedFiles/Content/Training_and_Certifications/ISA_Certification/CCST%20Level%20I%20II%20III%20Blueprint%20Comparison%20Final%2020180430.pdf. [Accessed: 05- Jun- 2020].

[28] ISA, "Industrial Automation and Control Systems Security", 2019. [Online]. Available: https://www.isa.org/isa99/. [Accessed: 05- Jun- 2020].

[29] ISA, "ISA/IEC 62443 Cybersecurity Certificate Programs", [Online]. Available: https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/. [Accessed: 05- Jun- 2020].

[30] U.S. Department of Labor, "Automation Industry Competency Model V. 4", 2009 (updated 2018). [Online]. Available: https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=automation. [Accessed: 05- Jun- 2020].