

# **Foundations of Industrial Cybersecurity**

## **Education and Training**

Submitted by Sean Michael McBride, MBA, MGM

Thesis submitted in total fulfilment of requirements for Doctor of Philosophy (PhD)

Department of Computer Science and Information Technology  
School of Engineering and Mathematical Sciences  
College of Science, Health and Engineering

La Trobe University  
Victoria, Australia

July 2021



## TABLE OF CONTENTS

TABLE OF CONTENTS .....	iii
TABLE OF FIGURES .....	ix
TABLE OF TABLES .....	x
1 INTRODUCTION.....	1
1.1 Divergent Tracks .....	1
1.2 Threat Environment Evolves Towards Industrial Control Systems .....	2
1.2.1 Presentations at Security Conferences .....	2
1.2.2 Vulnerability Disclosures .....	3
1.2.3 Attacks Affecting Industrial Environments.....	3
1.3 Broad Research Questions .....	4
1.3.1 What would constitute a firm foundation for developing industrial cybersecurity professionals? .....	4
1.3.2 What are the key philosophical differences between industrial cybersecurity and traditional cybersecurity? .....	4
1.3.3 What is the global breadth of the need for industrial cybersecurity education? .....	4
1.3.4 Do existing educational guidance efforts meet foundational requirements? .....	5
1.3.5 What programs and institutions are positioned to foster development of qualified professionals? .....	5
1.3.6 How might capable students become interested in pursuing this field?.....	5
1.3.7 What facilities and equipment would a sound education require? .....	5
1.3.8 What individuals can provide the necessary guidance to establish educational programs and instruct students? .....	5
1.3.9 What education and training experiences are likely to yield results? .....	5
1.3.10How might one assess the effectiveness of emerging educational programs? .....	6
1.3.11What might impede progress of industrial cybersecurity education? .....	6
1.3.12How might impediments be overcome? .....	6
1.3.13How might educational approaches to industrial cybersecurity be effectively and efficiently rolled out across the world? .....	6
1.4 Methodology .....	6
1.5 Research Contribution to Academic Knowledge .....	7
1.5.1 Clarification of differences between industrial cybersecurity and common cybersecurity for use in guiding education and training .....	7
1.5.2 Comprehensive review of current state of industrial cybersecurity education and training guidance documents/efforts .....	7
1.5.3 Proposed workforce development framework for industrial cybersecurity .....	8
1.5.4 Archetype industrial cybersecurity job roles.....	8
1.5.5 Knowledge categories, topics and justifications .....	8
1.5.6 NSA CAE-style knowledge unit for industrial control systems .....	8
1.5.7 Key tasks for each archetype role .....	9
1.5.8 Leverage point for future standard development .....	9
1.5.9 Historic documentation of process used to create the world's first cybersecurity education and training standards .....	9
1.6 Conclusion.....	9

2	LITERATURE REVIEW .....	10
2.1	Foundations of Cybersecurity Education .....	10
2.1.1	Analysis .....	12
2.2	Emergence of “Operational Technology” .....	13
2.2.1	What is the “IT-OT gap”? .....	14
2.2.2	A Personal Experience .....	14
2.2.3	Description of the IT-OT gap .....	15
2.2.4	Terminology .....	15
2.3	Global Need for Industrial Cybersecurity Education and Training.....	16
2.4	Industrial Cybersecurity Guidance Documents.....	17
2.4.1	NIST SP 800-82 R2.....	17
2.4.2	ISA 99/ IEC 62443 .....	20
2.4.3	North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP).....	23
2.4.4	Conclusion from review of industrial cybersecurity practice standards .....	26
2.5	Papers on Industrial Cybersecurity Education and training .....	26
2.6	Conclusion.....	28
2.6.1	Key Research Question .....	28
3	METHODOLOGY .....	30
3.1	Research Validity.....	30
3.2	Human Ethics Considerations .....	32
3.3	Preview of Research Methods Employed and Corresponding Validity Techniques .....	32
3.4	The Role of the Researcher .....	33
3.4.1	Academic preparation at Idaho State University.....	34
3.4.2	Professional experience at the INL .....	35
3.4.3	Critical Intelligence .....	36
3.4.4	Founding of the Energy Systems Technology and Education Center (ESTEC).....	37
3.4.5	Cyber-Physical Security Program at Idaho State University .....	38
3.5	Conclusion.....	39
4	CRITICAL REVIEW OF INDUSTRIAL CYBERSECURITY EDUCATION AND TRAINING GUIDANCE DOCUMENTS .....	40
4.1	Problem .....	40
4.2	Research Design.....	40
4.2.1	Review of industrial cybersecurity curricular guidance efforts/documents.....	41
4.2.2	Criteria for establishing a foundation.....	65
4.3	laboraResults .....	69
4.4	Analysis.....	70
4.4.1	Vertical analysis .....	70
4.4.2	Horizontal analysis .....	72
4.4.3	Validity.....	74
4.5	Conclusion.....	77
5	DIFFERENTIATED INDUSTRIAL CYBERSECURITY KNOWLEDGE.....	78
5.1	Problem .....	78
5.2	Research Design.....	78
5.3	Results of the Nominal Group Session .....	84
5.3.1	Results of Question 1 .....	84

5.3.2	Results of Question 2 .....	85
5.4	Analysis .....	86
5.4.1	Validity of Archetype Roles and Knowledge Categories .....	87
5.5	Conclusion.....	90
5.5.1	Archetype roles .....	90
5.5.2	Knowledge categories .....	90
6	INDUSTRIAL CYBERSECURITY SPECIFIC KNOWLEDGE ITEMS.....	92
6.1	Problem .....	92
6.2	Research design.....	92
6.3	Results .....	93
6.4	Analysis .....	93
6.4.1	Industrial processes and operations .....	94
6.4.2	Instrumentation and control .....	96
6.4.3	Equipment under control .....	101
6.4.4	Industrial communications .....	104
6.4.5	Safety.....	105
6.4.6	Regulation and guidance .....	108
6.4.7	Common weaknesses .....	110
6.4.8	Events and incidents.....	112
6.4.9	Defensive technologies and approaches.....	116
6.4.10	Validity. ....	118
6.4.11	Limitations .....	127
6.5	Conclusion.....	127
7	INDUSTRIAL CYBERSECURITY WORKFORCE DEVELOPMENT MODEL.....	129
7.1	Problem .....	129
7.2	Research design.....	129
7.2.1	Key ideas in workforce development models .....	130
7.2.2	Characterisation of workforce models used in candidate documents/efforts.....	132
7.3	Results – Archetype Model .....	146
7.3.1	Archetype Role.....	147
7.3.2	Role Description.....	147
7.3.3	Key Tasks .....	147
7.3.4	Sub-tasks .....	147
7.3.5	Knowledge .....	147
7.3.6	Skill .....	148
7.3.7	Attitude.....	148
7.3.8	Behavior .....	148
7.3.9	Proficiency .....	148
7.3.10	Role-task responsibility .....	148
7.3.11	Management confidence .....	148
7.3.12	Specific content.....	149
7.4	Analysis .....	149
7.4.1	Comparison with models used by candidate educational guidance .....	149
7.4.2	Validation .....	156
7.5	Conclusion.....	159
8	INDUSTRIAL CYBERSECURITY TASKS .....	160

8.1	Problem .....	160
8.2	Research Design .....	160
8.2.1	laboralaboralaboralaboraSession details .....	162
8.3	Results .....	163
8.3.1	Archetype Role: Industrial Cybersecurity Engineer .....	163
8.3.2	Archetype Role: Industrial Cybersecurity Technician .....	164
8.3.3	Archetype Role: Industrial Cybersecurity Analyst .....	164
8.3.4	Archetype Role: Industrial Cybersecurity Researcher .....	165
8.3.5	Archetype Role: Industrial Cybersecurity Manager.....	165
8.4	Analysis .....	166
8.4.1	Implications .....	166
8.4.2	Validation .....	167
8.4.3	Limitations .....	170
8.5	Conclusion.....	171
9	FUTURE WORK .....	172
9.1	Future Effort 1 – Establish an Industrial Cybersecurity Education and Training Community of Practice.....	172
9.2	Future Effort 2 – Extend Proposed Content to Create CSEC 17-style Knowledge Area .....	174
9.3	Future Effort 3 – Contribute to Foundational Paradigms.....	174
9.3.1	Industrial Cybersecurity Publications Relying on the CIA Triad .....	175
9.3.2	Concerns with CIA Triad as the guiding paradigm for industrial cybersecurity .....	177
9.3.3	Counterarguments and response.....	181
9.3.4	Seven Ideals as a guiding paradigm .....	181
9.3.5	Restatement .....	182
9.3.6	Analysis of restatement .....	182
9.3.7	Recommendations .....	185
9.4	Future Effort 4 – Perform Additional Validation Incorporating Cognitive and Behavioral Approaches .....	186
9.5	Future Effort 5 – Establish Career Pathways .....	186
9.5.1	Career and Technical Education (CTE) .....	189
9.5.2	Raspberry Pis and dehydrated potatoes.....	190
9.5.3	Engaging middle school and high school students.....	191
9.5.4	Engaging high school students.....	191
9.5.5	Pathway to bachelor degree.....	193
9.5.6	Graduate options .....	194
9.5.7	A cycle of vertical integration.....	194
9.5.8	Summary of career paths discussion .....	194
9.6	Future Effort 6 – Example Curriculum .....	195
9.6.1	Example curricula for industrial cybersecurity technicians .....	195
9.6.2	Challenges and objections faced .....	204
9.7	Other Future Efforts .....	205
9.7.1	Sustainability/governing body.....	205
9.7.2	Incentives for curricular development and program offerings.....	205
9.7.3	Development of hands-on curricular materials .....	206
9.7.4	Evaluation.....	208
9.8	Conclusion.....	208

10	CONCLUSION .....	210
10.1	Limitations .....	212
10.2	Future Research Directions .....	213
	APPENDIX A: Details of structured literature review on “Operational Technology” .....	214
	APPENDIX B: NSA-CAE STYLE KNOWLEDGE UNIT .....	220
	Characterization of The NSA CAE Knowledge Unit .....	220
	Methodology .....	220
	Resulting NSA CAE-Style Knowledge Unit. ....	221
	Intent .....	221
	Outcomes .....	221
	Topics.....	221
	Anticipated Use.....	222
	APPENDIX C DATA FROM NOMINAL GROUP TECHNIQUE.....	223
	Specific job titles within this ICS field .....	245
	Good ideas w/o a home.....	245
	Manager .....	245
	Engineer .....	246
	Technician .....	247
	Analyst .....	248
	Education .....	249
	Job roles that merit immediate development .....	250
	Unique ICS Knowledge .....	252
	Control Knowledge.....	252
	Communications .....	255
	Regulations .....	256
	Instrumentation & Control.....	256
	ICS Knowledge for immediate development with verbs for action .....	257
	Control Knowledge.....	261
	Equipment .....	265
	Communications .....	266
	Regulations .....	267
	Instrumentation & Control.....	267
	Introduction of researcher .....	269
	Introduction of collaborcollaborators .....	269
	Review of the purpose of the effort .....	269
	Review of the results of the nominal group technique .....	270
	Allow the collaborcollaborator to ask any questions they may have.....	270

Collaborative discussion of the question .....	270
Note taking.....	270
Wrap up.....	270
APPENDIX E ESET 181 IT-OT FUNDAMENTALS – ABBREVIATED SYLLABUS .....	271
APPENDIX F BUILDING AN INDUSTRIAL CYBERSECURITY WORKFORCE: A MANAGERS GUIDE.....	273
APPENDIX G MATERIALS FOR SURVEYS, INTERVIEWS, AND FIELD OBSERVATION.....	285
REFERENCES .....	309



## TABLE OF FIGURES

Figure 1. McCumber’s Comprehensive Model for Information Systems Security. ....	11
Figure 2. Information Assurance Model .....	11
Figure 3. Cybersecurity Curricula 2017 thought model .....	12
Figure 4. ISA/IEC 62443 family of standards .....	20
Figure 5. Selection of archetype roles for development. ....	85
Figure 6. Conklin (2014) comparison of training and education using archetype role terminology. ....	90
Figure 7. ENISA structure.....	133
Figure 8. GIAC/SANS Workforce Model Graphic.....	134
Figure 9. ISA DOL Competency Model structure .....	135
Figure 10. Joint Task Force Knowledge Area Links to NIST NICE Framework .....	136
Figure 11. NIST NICE Framework organisation. ....	137
Figure 12. NIST NICE Revision structure.....	138
Figure 13. Competencies used as part of a position description.....	139
Figure 14. 4011 Structure.....	140
Figure 15. CNSSI 4012 structure.....	141
Figure 16. CNSSI 4013 structure.....	141
Figure 17 CNSSI 4014 structure.....	142
Figure 18. NSISSI 4015 structure .....	143
Figure 19. CNSSI 4016 structure.....	143
Figure 20. NSA CAE Knowledge Units 2020 structure .....	144
Figure 21. PNNL Secure Power Systems Professional structure.....	145
Figure 22. SkillsFuture Singapore structure .....	146
Figure 23. Archetype model structure.....	147
Figure 24. Vertically integrated pathway from student perspective .....	189
Figure 25. ISU Organisational Structure .....	190
Figure 26. NSA CAE Knowledge Unit organization.....	220

## TABLE OF TABLES

Table 1. Use of the term OT in professional and academic literature by year.....	14
Table 2. Key differences among IT and OT.....	15
Table 3. Vulnerability Information by Country and Illustrative ICS Vendor.....	16
Table 4. Illustrative ICS Security Event by Country .....	17
Table 5. Mentions of "education" and "training" within ISA/IEC 62443 standards.....	21
Table 6. Requirements for staff training and security awareness .....	21
Table 7. NERC CIP Standards .....	23
Table 8. Validity Procedures Within Qualitative Lens and Paradigm Assumptions .....	31
Table 9. Products with corresponding method and validation technique .....	32
Table 10. Candidate Curricular Guidance Mapped to Identified Foundational Criteria.....	69
Table 11. Development of National Cybersecurity Education and Training Standards .....	81
Table 12. Comparison of proposed knowledge unit topic terms with Automation Industry Competency Model.....	122
Table 13. Terms from Common Weaknesses category and external location.....	123
Table 14. Terms from Defensive Techniques and Approaches category and external location .....	123
Table 15. Correlation of industrial cybersecurity specific knowledge with industrial cybersecurity events.....	124
Table 16. Mapping of remaining items to other events .....	127
Table 17. Details of focus group sessions .....	162
Table 18. Industrial Cybersecurity Engineer tasks. ....	163
Table 19. Industrial Cybersecurity Technician tasks.....	164
Table 20. Industrial Cybersecurity Analyst tasks.....	164
Table 21. Industrial Cybersecurity Researcher tasks. ....	165
Table 22. Industrial Cybersecurity Manager tasks.....	165
Table 23. Workshop participants most-significant needs for industrial cybersecurity education and training. ....	173
Table 24. <i>Sample industrial cybersecurity publications relying on the CIA Triad.</i> .....	175
Table 25. Industrial Cybersecurity Engineering Technology program courses .....	197
Table 26. Category totals for Industrial Cybersecurity Engineering Technology.....	198
Table 27. Introduce (I), reinforce (R), assess (A) map .....	198

Table 28. Alignment between proposed knowledge and ISU's industrial cybersecurity program .....	199
Table 30. Foundational criteria for industrial cybersecurity education and training addressed in this thesis.....	211
Table 31. IEEE publications using term "operational technology" .....	214

# **Abstract**

This thesis intends to help establish the foundation for educating and training industrial cybersecurity professionals. It begins with a historic description of how industrial automation developed in a world devoid of cybersecurity foresight, and summarises the key events that hurled the fields of industrial automation and cybersecurity back together.

The broad literature review in Chapter 2 samples key developments in cybersecurity education and the emergence of industrial-focused education and training content.

Chapter 3 describes the mixed methods the author used to investigate the adequacy of the existing education and training foundations, and to propose improvements.

Chapter 4 presents a critical review of existing cybersecurity curricular guidance documents one might expect to deal with industrial cybersecurity, identifying eleven characteristics that should be met to have a firm foundation.

Chapter 5 discusses the application of the nominal group technique to identify 1) archetype roles within the field of industrial cybersecurity; and 2) knowledge categories that one would not expect to be covered in a traditional cybersecurity program.

Chapter 6 proposes the specific content that each of the knowledge categories identified in Chapter 5 should contain. The chapter validates the proposed contents via comparison with external documentation and key industrial cybersecurity events.

Chapter 7 compares 16 existing workforce development models. It concludes that no standard taxonomy for such models exists, and advances a combined model to compensate for identified weaknesses.

Chapter 8 presents the results of focus group sessions in which the collaborators identified key tasks for five archetype roles identified in Chapter 5 building on the workforce development model proposed in Chapter 7.

Chapter 9 describes ongoing efforts to continue the work presented in previous chapters. This includes, notably, the author's thoughts on establishing education and training pathways for industrial cybersecurity professionals, and a proposed paradigm to unify industrial cybersecurity with traditional cybersecurity.

## **Statement of Authorship**

Except where reference is made in the text of the thesis, this thesis contains no material published elsewhere or extracted in whole or in part from a thesis accepted for the award of any other degree or diploma. No other person's work has been used without due acknowledgment in the main text of the thesis. This thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.

Sean McBride

8 July 2021

# Acknowledgements

My wife, Kari, made great sacrifices so I could pursue a long-term goal of obtaining a PhD. Our children were oblivious to those sacrifices. I cannot thank her enough.

My friends with PhDs told me that the most important factor of doctoral work is your supervisor. My supervisor, Dr. Jill Slay, is beyond amazing. When we planned my visit to Australia, she invited me to stay at the Slay residence. Every time I talked with Jill, I felt strengthened by her confidence in me. I think she has that effect on nearly everyone!

Dr. Corey Schou, my external supervisor, is among the most intellectually powerful men I have known. His ability to recall precise details years after they occurred is astounding. His openness, advice and use of the Simplot Decision Support Center, along with the help of friendly staff at the Informatics Research Institute, are greatly appreciated. Dr. Schou's educational philosophy will live on in me.

The cybersecurity team at the Idaho National Laboratory – led by Eleanor Taylor, Wayne Austad, Zach Tudor, and Scott Cramer were so supportive – constantly asking how they could help.

This work was supported by a La Trobe University Full Fee Postgraduate Research Scholarship, for which I express deep appreciation.

# 1 INTRODUCTION

## 1.1 Divergent Tracks

January 1, 1968 demarcates divergence among the world of industrial control and computer science. Anecdotally, on that date, the energetic and unconventional MIT drop-out, 35-year-old Richard Morley emerged from a New Year's hangover to document the first programmable logic controller (PLC [Dunn, 2008]), the central component of what we recognise today as an industrial control system.

Having applied microcomputers in manufacturing environments for several years, Morley wanted a single controller he could apply to every project. His controller would meet the following criteria:

- Rugged enough to work in industrial environments without a cabinet
- No interrupts for processing
- Direct mapping into memory
- Hardware handling of repetitive chores
- Standard language for programming

Morley harbored such technological animosity towards the minicomputer for his line of work that he categorically avoided the use of the term “computer” in relation to his device. He would erase the word from blackboards and trash papers that used it to characterise the PLC.

By November 1969, Modicon, the firm Morley and his associates launched to produce the PLCs, had entered a million-dollar contract to function as an original equipment manufacturer under the General Electric (GE) label. Soon, other vendors from around the world offered similar products (Young, n.d.).

PLC technology disrupted the manufacturing world in much the same way the personal computer disrupted the business world. The devices control everything from chlorine injection in municipal water provisioning systems to coal conveyors in power plants replacing both relay rooms and workers within industrial facilities. Today (2021), the annual global market for PLCs is estimated to exceed \$9 billion (Liu, 2017), which represents only a sliver of the estimated \$250 billion (Research and Markets, 2018; Transparency Market Research, 2019) global market for industrial automation -- which the PLC helped develop.

Meanwhile, computer security emerged as a discipline in the 1980s, well after industrial automation was on its own track. Significantly, the United States Department of

Defense issued its first computer security standard “Trusted Computer System Evaluation Criteria” (also known as the Orange Book) in August 1983 (Department of Defense).

While a rainbow of additional security guidance appeared throughout the 1980s and 90s (Federation of Concerned Scientists, n.d.), and international bodies such as (ISC)<sup>2</sup>, ISACA, ISSA, formed to promulgate standards, recommend practice, and certify professionals, none of these efforts placed attention on the security of non-computers, such as PLCs, then revolutionising industrial environments.

In 1979, Modicon released its Modbus protocol, which allowed connections among controllers and programming devices, over serial cables (Schneider Electric, n.d.). The simplicity of the standard and its open nature catalysed widespread adoption by various vendors (National Instruments, 2019). By 1999 the community of Modbus users had developed a Modbus TCP/IP standard, formally adapting it for interoperability with business computers (Modbus Organization, n.d.). In 2004, the International Electrotechnical Committee approved Modbus/TCP as publicly available standard 62030 (Modbus-IDA, 2004), thus marking the official re-convergence of the PLC with mainstream computing.

## **1.2 Threat Environment Evolves Towards Industrial Control Systems**

In the early 2000s cybersecurity enthusiasts began to investigate industrial environments and PLCs. To demonstrate the significance of this evolution, this section briefly addresses historical developments in three categories:

1. Presentations at security conferences
2. Vulnerability disclosures
3. Attacks affecting industrial environments

### **1.2.1 Presentations at Security Conferences**

The first publicly-identifiable “hacker” presentation on industrial control systems occurred in 2003 at the Brumcon conference in Birmingham, England (Barnes, 2003). It was entitled, “How Safe is Glass of Water?” Other than a brief summary on The Register web site, explaining that it “was a detailed breakdown of the RF systems that are used by water management authorities in the UK and how these systems can be abused, interfered with and generally messed” little documentation exists in openly available web sources, and the presenter was left unnamed.

By 2019 numerous conferences around the world had come to specialise in industrial cybersecurity. These include, SCADA Security Scientific Symposium (S4 [S4 Events, n.d.]),



ICS Cyber Security Conference (n.d.), Stockholm International Summit on Cyber Security in SCADA and Industrial Control Systems (CS3 [n.d.]). Other conferences such as BlackHat, Defcon, and PacSec frequently cover the topic from a variety of perspectives.

Some of the most significant presentations, such as those by Larsen (2015) and Krotofil (2015), address how adversaries might plan to cause specific types of physical damage via cyber-attack.

### **1.2.2 Vulnerability Disclosures**

In 2004, at a North Atlantic Treaty Organisation (NATO) conference, a pair of professors from the University of Missouri - Rolla, provided the first public disclosure of a PLC vulnerability (Miller, 2004). Their paper described denial of service vulnerabilities affecting a Rockwell Automation PLC-5/20E PLC, a Rockwell Automation SLC-5/05 PLC, and a Rockwell Automation ControlLogix ENET module. They also described a password disclosure vulnerability allowing an attacker to reprogram a Modicon Quantum NOE771-10/FactoryCast PLC.

Since this initial disclosure, researchers have disclosed over 1,500 vulnerabilities affecting industrial environments, including PLCs, HMIs, industrial network switches, and variable frequency drives (VFDs [McBride, 2016]).

Among the most concerning vulnerabilities are that the most commonly deployed industrial protocols such as Modbus and Common Industrial Protocol (also known as Ethernet/IP) do not support authentication. This means that any device on the network can communicate with a PLC allowing it to manipulate the way the process operates (Batke, 2015; Benbenishi, 2017).

### **1.2.3 Attacks Affecting Industrial Environments**

In 2009, Stuxnet became the first attested attack to intentionally cause physical consequence by manipulating an industrial environment. This worm targeted centrifuges at Iran's Natanz uranium enrichment facility (Langner, 2013).

Nearly six years later, in 2015, the world experienced its first confirmed power outage due to cyber-attack. Attackers infected dispatcher workstations, which they then used to disconnect electricity service in Western Ukraine (Whitehead, 2017).

Then, in 2017, malware targeting a safety system in a Saudi Arabian oil refinery shut down the facility (Greenberg, 2019).

In addition, numerous security incidents have harmed industrial control systems without explicitly targeting them. These include the Wannacry ransomware, which halted manufacturing at a Honda plant in June 2017 (Tajistsu, 2017), and the NotPetya ransomware, which stopped pharmaceutical production at a Merck facility the same month. Merck informed its investors that the attack cost the company an estimated \$310 million (O'Neill, 2017).

### **1.3 Broad Research Questions**

Given the longstanding divergence between computer science and industrial automation noted above, and the significant evolution of the threat environment towards industrial systems, researchers must ask: how do we ensure the security of the converged industrial technology ecosystem on which modern Western society depends? A key component of ensuring that security is the preparation of the individuals who design, develop, implement, and maintain it. This leads to numerous additional questions about the nature of cybersecurity and the development of a cybersecurity workforce:

#### **1.3.1 What would constitute a firm foundation for developing industrial cybersecurity professionals?**

Every field of study and practice seems to require foundational concepts and structure – ideas which educators can confidently teach. What would one expect this foundation to include? How could one know that the foundation was complete?

#### **1.3.2 What are the key philosophical differences between industrial cybersecurity and traditional cybersecurity?**

That industrial cybersecurity is different appears to be widely held. But how different? What perspectives can and should be brought to bear when preparing industrial cybersecurity professionals? Are existing cybersecurity philosophies sufficient? Who says they are? Who says they are not? If they are, how could we know it? If not, why not? If they are not, can they be extended, or should something new replace them?

#### **1.3.3 What is the global breadth of the need for industrial cybersecurity education?**

Given the existing state of information systems and industrial control systems, how significant is the education and training challenge? Who needs to be educated? How many people need to be educated – and over what time frame? Should new jobs be created? What are the ramifications of not educating and training industrial cybersecurity professionals? Do certain countries need more professionals than others?

#### **1.3.4 Do existing educational guidance efforts meet foundational requirements?**

What is the current state of educational guidance for industrial cybersecurity? How was this guidance created? How was it validated? Who created it? What evidence has been preserved and documented? How do the efforts stand up against foundational criteria?

#### **1.3.5 What programs and institutions are positioned to foster development of qualified professionals?**

Imagining that significant demand for industrial cybersecurity professionals emerges, how will that demand be met? What organizations currently create such professionals? What is the capacity of those organizations? What limits or promotes their capacity? What could stakeholder organizations such as employers, professional societies, governments and academia do to promote growth in the field?

#### **1.3.6 How might capable students become interested in pursuing this field?**

When would and should youth first be exposed to a career in industrial cybersecurity? Could this occur as part of secondary education? In what types of classes? From what types of instructors? What learning experiences might ignite their interest?

#### **1.3.7 What facilities and equipment would a sound education require?**

Given the perception that industrial equipment is less commonly available than computer and network equipment, what equipment would be necessary for students to observe, configure and use? How much does this equipment cost? From where would it be procured? Would providers be willing to donate equipment? Is it a matter of having the equipment alone, or must the equipment be shown in its intended environment for best instruction?

#### **1.3.8 What individuals can provide the necessary guidance to establish educational programs and instruct students?**

What qualifies an instructor to cover this space? What relevant professional certifications exist? How does one know the certifications are relevant? How many qualified instructors are available? Imagining that the demand for qualified professionals in the field is more economically attractive than teaching, how would qualified instructors be recruited?

#### **1.3.9 What education and training experiences are likely to yield results?**

With key theories, equipment and instructors in place, what experiences would be of greatest value to students? How can one know what experiences are most important? Can

these experiences be effectively delivered in the classroom, the training laboratory, or in a professional environment?

#### **1.3.10 How might one assess the effectiveness of emerging educational programs?**

Given that frameworks exist for assessing educational programs, how might these be applied to emerging programs? What proficiency measures might be established for students performing key tasks? How might one compare across programs and instructors?

#### **1.3.11 What might impede progress of industrial cybersecurity education?**

What inaccurate perceptions about industrial cybersecurity already exist? Given the perception that industrial cybersecurity is interdisciplinary by nature, what conflicts are likely to arise such as between colleges or departments? Might industrial cybersecurity programs have to compete for resources against other cybersecurity focus areas?

#### **1.3.12 How might impediments be overcome?**

Assuming that impediments can be identified, what approaches could allow emerging programs to flourish? What alliances should form? What types of organizations should participate in such alliances? How should those alliances formalise? What funding sources should exist? Do appropriate funding sources exist? What requirements should funding opportunities include?

#### **1.3.13 How might educational approaches to industrial cybersecurity be effectively and efficiently rolled out across the world?**

Assuming that individuals, programs, institutions, and alliances begin to have success, what models might allow such success to scale? What are the limits of scalability? How might limits such as culture and language be addressed? What existing relationships might be leveraged to effectively scale? How quickly is scale advisable? Who can oversee and ensure the success of efforts to scale?

### **1.4 Methodology**

The research presented in this thesis adopts a predominantly qualitative mixed-methods approach, including the use of critical review of literature, nominal group technique, and focus groups. The researcher's critical paradigm allows him to be an active participant in the research, intending to identify transformative concepts and stimulate new dialog. The primary validation technique for research within the critical paradigm (though not the only validation technique employed) is researcher reflection – written in first person – which encourages the reader to appraise the criticality and integrity of the author and the work.

This stands in contrast to many studies in cybersecurity which adopt a systematic paradigm, relying on triangulation and audit trails for validity. The benefit to employing the critical paradigm, is that it encourages the author to confront his own strengths and limitations. Such humanistic nuance is of special value to those who wish to understand not only what the results were, but the experiences that led the author to pose the questions in the first place.

This approach aligns particularly well with many of the broad research questions, which are oriented towards practical answers that drive change.

## **1.5 Research Contribution to Academic Knowledge**

Against the backdrop of the questions listed above, this thesis focused in especially on the first broad question: *What is the foundation for the formal preparation of industrial cybersecurity professionals?*

In the course of the study to reach the answer, the thesis makes the following contributions to the academic body of knowledge:

### **1.5.1 Clarification of differences between industrial cybersecurity and common cybersecurity for use in guiding education and training**

The point of departure for examining the education and training needs for industrial cybersecurity is a demonstration by literature review and deductive reasoning that foundational elements of general information security training and education insufficiently address industrial environments. In anticipation of incredulity on this point, the thesis advances a hypothetical dialogue intended to help demonstrate key differences.

Further, while differences between information systems and industrial control systems have been discussed in many documents and formats, this thesis expands this discussion beyond the technical details of the two types of systems to consider the broader educational and managerial context. This clarification is presented in Table 2 (page 15).

### **1.5.2 Comprehensive review of current state of industrial cybersecurity education and training guidance documents/efforts**

This thesis critically examines the current state of content guidance for educating and training industrial cybersecurity practitioners and professionals. The comprehensive review reported in this thesis resulted in a list of ten criteria one would expect a solid foundation to incorporate, with a description, justifying rationale, key insight, and anticipated challenges

for each criterion. This will be of use to those seeking to establish or improve cybersecurity education and training content guidance in the future.

By comparing the existing curricular guidance efforts to these criteria, the thesis tells a story of weaknesses across international efforts that would otherwise be ignored. These results are summarised in Table 10 (page 98).

### **1.5.3 Proposed workforce development framework for industrial cybersecurity**

As evidenced from the documents reviewed, there is currently no widely accepted workforce development framework for cybersecurity – much less industrial cybersecurity. This thesis extracts the models used by 16 different documents, analyses their strengths and weaknesses and proposes a new model to address identified weaknesses. The model intends to allow various entities and organisations to intuitively contribute and use content structured thereby. This proposed model is found in Section 7.3.

### **1.5.4 Archetype industrial cybersecurity job roles**

This thesis identifies five archetype job roles for industrial cybersecurity practitioners. This is useful to industrial cybersecurity managers building teams, human resources personnel helping hire employees and encourage their professional development, educators preparing students to enter the workforce, and students setting career ambitions. These roles are incorporated into the document “Building an Industrial Cybersecurity Workforce: A Manager’s Guide” published by the Idaho National Laboratory – provided in Appendix F (Idaho National Laboratory, 2020).

### **1.5.5 Knowledge categories, topics and justifications**

Recognising that previously advanced industrial cybersecurity education and training curricular guidance efforts did not define or describe the justification for the knowledge they recommended, this thesis advances and validates nine knowledge categories. It describes each category, each content term, and provides a paragraph justifying the terms inclusion. This content can be found in Section 6.4.

### **1.5.6 NSA CAE-style knowledge unit for industrial control systems**

A significant and concrete contribution of the thesis is the advancement of an NSA CAE-style knowledge unit for industrial control systems. The critical review section identifies significant weaknesses in the original knowledge unit. The methods applied in the thesis resulted in a clear set of nouns that anyone educated or trained in the field of industrial cybersecurity should know related to industrial control systems, and justify why

each of these terms should be covered. The thesis provides this in the format of a ready-to-use NSA CAE style knowledge unit – provided in Appendix B.

#### **1.5.7 Key tasks for each archetype role**

In addition to identifying five archetype roles for industrial cybersecurity professionals, this thesis advances key tasks to be performed by each of those roles. This provides important guidance about what each archetype role does – useful to educators, human resources personnel, managers, and students. These key tasks are also included in “Building an Industrial Cybersecurity Workforce: A Manager’s Guide” published by the Idaho National Laboratory – provided in Appendix F (Idaho National Laboratory, 2020).

#### **1.5.8 Leverage point for future standard development**

The Future Work section of this thesis advances several new ideas to further the state of industrial cybersecurity training and education, including work on establishing a unifying paradigm, and integrated educational pathways.

#### **1.5.9 Historic documentation of process used to create the world’s first cybersecurity education and training standards**

The methodology section to chapter 5 of this thesis includes historic documentation on the process by which the U.S. federal government created its first information security training standards – which played a critical role in establishing the National Security Agency (NSA) Centers of Academic Excellence (CAE) effort. Even though it was a by-product of the thesis rather than its principal objective, the fact that it has not yet appeared elsewhere will make it useful to historians of cybersecurity education and of Idaho State University.

### **1.6 Conclusion**

In conclusion, this thesis is written within the context of a time when technological innovation and digitization are transforming individual lives, societies, and economies. New global reliance on these technologies has the potential for significant if not devastating physical consequences. This digital evolution will require similarly evolved educational approaches. The contributions made in this thesis aim to guide a firm foundation for developing a new generation of interdisciplinary cyber defenders.

## 2 LITERATURE REVIEW

With the above listed broad questions set forth, this section presents a review of relevant literature in five principal categories – which descends from the general to the specific:

- Foundations of Cybersecurity Education
- Emergence of “Operational Technology”
- Global Need for Industrial Cybersecurity Education and Training
- Industrial Cybersecurity Standards
- Papers on Industrial Cybersecurity Education and Training

The literature review chapter then summarises key observations, and concludes with identification and characterisation of the key research question.

### 2.1 Foundations of Cybersecurity Education

Cybersecurity can trace its roots to the concepts of confidentiality, integrity, and availability. These terms describe the core attributes of information within what might be termed a “secure system”. Confidentiality means that information can only be accessed by those who have a need or permission to view the information, but not by those who do not. Integrity means that information has not been changed or manipulated by error or intention – as this would compromise any decision the information was used to make. Availability means that the information can be obtained when it is needed – information encased in a cement vault at the bottom of the ocean may be confidential, and integral, but is not available for use.

These three characteristics are found enshrined in notable publications that establish cybersecurity as a field of professional and academic endeavor stretching over three decades. First, *Information Security: A Comprehensive Model*, presented by McCumber in 1991, depicts information security as a three-dimensional cube consisting of critical information characteristics, information states, and security measures. The critical information characteristics include confidentiality, integrity, and availability (McCumber, 1991). Information states describes where the information exists – with a view towards computer systems – be it in storage (on a disk drive), in processing (loaded into random access memory) or transmission (sent across the wires). The security measures describe the general categories whereby confidentiality, integrity, and availability may be achieved, which are technology (for example, a password), policy (for example, a set of password requirements),



and education, training and awareness (for example, explaining to the user why passwords should not be re-used). McCumber’s model is graphically reproduced in Figure 1.

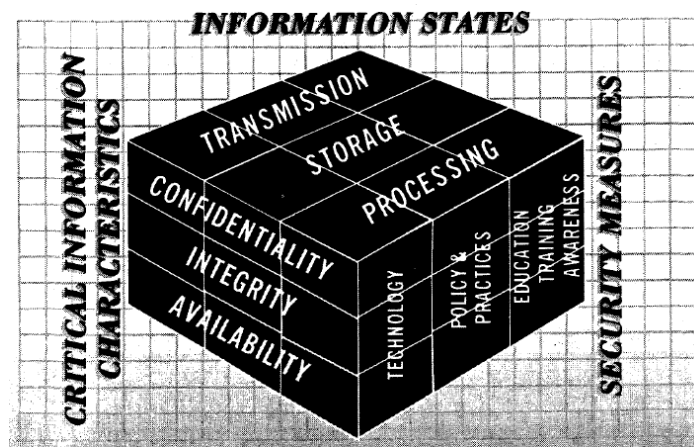


Figure 1. McCumber’s Comprehensive Model for Information Systems Security (McCumber, 1991).

A decade later, Maconachy and colleagues established “Information Assurance” as the guiding paradigm for the defensive mission of the National Security Agency. That paradigm, presented in *A Model for Information Assurance: An Integrated Model* (Maconachy, 2001) expands the McCumber model by changing the dimension “critical information characteristics” to “security services” and “security measures” to “security countermeasures”. It also adds the component of time, and advances a learning continuum that leads successively from awareness to literacy to training and to education. Figure 2 shows the updated cube portion of the model.

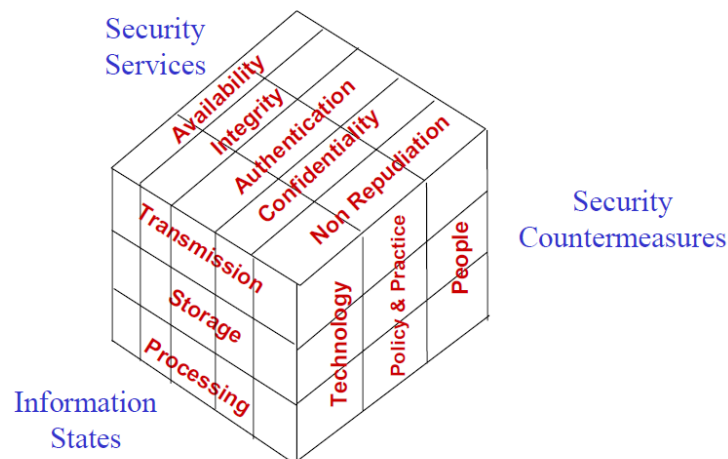


Figure 2. Information Assurance Model (Maconachy, 2001)

Approximately 15 years later, Burley led an impressive collaborative effort to formalise cybersecurity as an academic discipline from an international perspective: *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (Burley, 2017). That effort “draws from the foundation fields of information security and information assurance”, and describes cybersecurity as “a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries” (p. 16). As can be observed in Figure 3, like predecessor models, it builds on the foundation of confidentiality, integrity and availability.

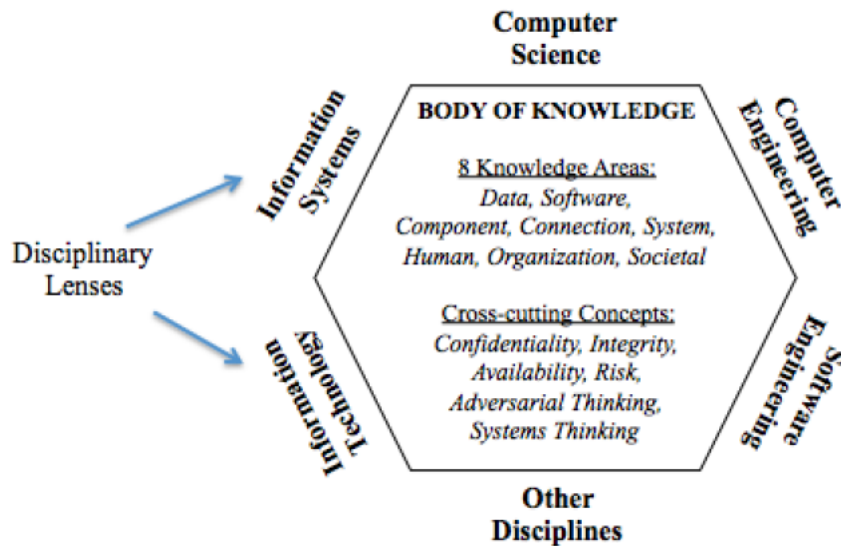


Figure 3. *Cybersecurity Curricula 2017 thought model* (Burley, 2017)

### 2.1.1 Analysis

As noted in the Introduction, the first broad question requires exploration of the key philosophical differences between industrial cybersecurity and traditional cybersecurity.

The immediate observation from the review of the three significant documents above is that their authors created them for the purpose of assuring the *information characteristics* of confidentiality, integrity, and availability. The publications provide no clues that their authors carefully considered their application to industrial environments.

The key difference between an information system and an industrial control system is that the former exists to create and control information, not the physics of manufacturing actual computers – that is the domain of the latter. Information systems are concerned with national secrets, trade secrets, intellectual property, personally identifiable information, and

financial details. Industrial control systems are concerned with speeds, temperatures, pressures and positions of machinery that provides electricity, gasoline, and drinking water. Each type of system requires its own expertise, and carries its own consequences of disruption.

## **2.2 Emergence of “Operational Technology”**

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 industrial control systems – the systems that 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 refer to the branch of the organisation concerned with operating the aforementioned systems as “operations”, or the “operations side of the house” (Causey, 2012; City of San Diego, 2019; Vickers, 2019; Public Utilities Fortnightly, 2019).

The term is particularly common within the context of cybersecurity. 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 (Pescatore, 2011). A semi-formalised definition of the term occurs in an August 2013 cybersecurity training document by O’Niel (2013).

A desktop analysis and structured literature review of the term “operational technology” in academic and professional literature the researcher performed (results in Table 1; details in Appendix A) 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. Nearly two thirds of the papers that use the term consistent with the authors’ definition focus on cybersecurity (57 of 88).

Table 1. Use of the term OT in professional and academic literature by year

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
<i>Totals</i>	<i>104</i>	<i>88</i>	<i>57</i>	<i>29</i>

### 2.2.1 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 the authors’ definition above mention the gap (29 of 88).

### 2.2.2 A Personal Experience

In 2016, a leading U.S. industrial control systems integration firm invited the author to address a group of operations personnel from the firm’s key clients. The author discussed how the threat environment for industrial environments had evolved from the early 2000s, emphasising 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 author, 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 the author has had with cybersecurity consultants who work regularly in industrial environments, confirm a common unfamiliarity, suspicion, and even distrust between the OT and IT groups.

### 2.2.3 Description of the IT-OT gap

Careful reflexivity led the author to create the following table to characterise various aspects of the IT-OT gap. Naturally, edge cases may not fit precisely, but the author asserts the differences – particularly those that transcend technology – are significant and justify an intentional effort to overcome.

*Table 2. Key differences among IT and OT*

<b>Aspect</b>	<b>IT</b>	<b>OT</b>
<i>Being controlled</i>	Data	Physics
<i>Measurement</i>	Bits & bytes	Temperature, pressure, level, flow
<i>Lifecycle</i>	System lifecycle	Plant lifecycle
<i>Consequences</i>	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
<i>Desired system characteristics</i>	Confidentiality Integrity Availability	Safety Reliability Functionality
<i>Educational background of professionals</i>	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
<i>Reporting chain</i>	ISO CISO CIO	Shift Supervisor Plant Manager COO
<i>Accounting</i>	Cost centre	Profit centre

### 2.2.4 Terminology

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, the author prefers the term “industrial cybersecurity” over “OT cybersecurity”; however, “OT security” and “ICS security” are also reasonable. “Industrial cybersecurity” is the expression most commonly used in this thesis.

## 2.3 Global Need for Industrial Cybersecurity Education and Training

Since the early 2000s, the threat environment has evolved to include a constant stream of vulnerability disclosures affecting industrial control systems (ICS) software (McBride, 2016). 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 3 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 2020, highlighting more than 1,000 entries across just four vendors. The table also highlights a sample vulnerability disclosed in the identified vendor's products by a researcher with a differing nationality.

*Table 3. Vulnerability Information by Country and Illustrative ICS Vendor*

Attribute	Country and Illustrative ICS Vendor			
	France	Germany	Taiwan	USA
	Schneider Electric	Siemens	Advantech	Emerson + GE IP <sup>b</sup>
<b>Perceived geographic market strength</b>	Various markets worldwide	EMEA	Asia	USA
<b>Number of vulns in NVD<sup>a</sup></b>	305	579	154	34+23=57
<b>Illustrative vuln and perceived nationality of discloser</b>	CVE-2011-4859; R. Santamarta; Spain (US DHS, 2012)	CVE-2015-1355; A.Timorin; Russia (US DHS, 2015)	CVE-2018-18999; J. Baines; USA (US DHS, 2018)	CVE-2017-12732; D. Atch; Israel (US DHS, 2017)

<sup>a</sup> From a search of the vendor name in the U.S. National Vulnerability Database April, 2020

<sup>b</sup> Emerson acquired GE Intelligent Platforms in February 2019

While vulnerability disclosures broadly indicate researcher involvement in ICS security, actual incidents highlight the seriousness of the challenge. Table 4 summarises key 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 3. 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.

The empirical evidence presented in these two tables supports the global nature of the industrial cybersecurity challenge.

*Table 4. Illustrative ICS Security Event by Country*

Attribute	Victim Country			
	Canada	USA	Ukraine	Saudi Arabia
<b>Event( Media term)</b>	Telvent Compromise	Black Energy	Industroyer	Triton
<b>Year of event</b>	2012	2014	2016	2017
<b>Impact</b>	Vendor cancelled remote support of pipeline SCADA	Adversary presence in networks	Power outage	Petro-chemical facility shutdown
<b>Vendor of involved ICS technology</b>	Telvent (acquired by Schneider Electric)	GE Intelligent Platforms (acquired by Emerson)	Siemens	Schneider Electric
<b>References</b>	Krebs, 2012; Peterson, 2012	US DHS 2014; Wilhoit, 2015	Cherapanov, 2017; Greenberg, 2017	Johnson, 2017; Newman, 2018; Sobczak, 2019

## 2.4 Industrial Cybersecurity Guidance Documents

Due to both evolving technology (addressed in section 2.1) and the evolving threat environment (addressed in section 2.2), two leading guidance documents on industrial cybersecurity have emerged: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Revision 2 “Guide to Industrial Control Systems (ICS) Security” (Stouffer, 2015) and the International Society of Automation (ISA)/International Electrotechnical Committee (IEC) 62443 series on “Industrial Automation and Control Systems Security” (ISA). The documents are not intended to provide curricular guidance, but security practice guidance. The following subsections briefly characterise each document and provide special attention to the guidance they provide relative to training and education.

### 2.4.1 NIST SP 800-82 R2

#### 2.4.1.1 Characterisation

NIST SP 800-82 and its revisions were a follow-on document to NIST Interagency Report 6859 “IT Security for Industrial Control Systems” originally published in 2002

(Falco). The 247-page document intends to provide guidance on the security of US federally-owned systems; however, the guidance is also helpful for privately owned systems.

The document is comprised of six main sections – Introduction, Overview of Industrial Control Systems, ICS Risk Management and Assessment, ICS Security Program Development and Deployment, ICS Security Architecture, Applying Security Controls to ICS, and a series of helpful appendices. It dedicates significant effort to comparing ICS and IT Systems security across 10 categories:

- Performance Requirements
- Availability Requirements
- Risk Management Requirements
- System Operation, Resource Constraints
- Communications
- Change Management
- Managed Support
- Component Lifetime
- Components Location

Throughout the entire document, its authors describe what these key differences should mean to those implementing industrial cybersecurity programs.

Because the document intends to guide security efforts for government-owned systems consistent with the Federal Information Security Management Act (FISMA), it describes how industrial control systems should be mapped into the FISMA risk management process. That process involves “For each information type and information system under consideration, the three FISMA-defined security objectives—confidentiality, integrity, and availability—are associated with one of three levels of potential impact should there be a breach of security. It is important to remember that for an ICS, availability is generally the greatest concern” (p. 6-2). The impact levels are then used to guide the selection of appropriate security controls.

#### ***2.4.1.2 Education and training***

The document uses the term “education” – in the form of “educational” five times. None of these provide much insight into who should be educated or what education they should receive. It mentions “training” 72 times, mostly within the context of using training as a security control. It states:

*For the ICS environment, this must include control system-specific information security awareness and training for specific ICS applications. In addition, an organisation must identify, document, and train all personnel*



*having significant ICS roles and responsibilities. Awareness and training must cover the physical process being controlled as well as the ICS (p. 6-13).*

*[T]raining programs should be carefully developed to ensure that each employee has received training relevant and necessary to his job functions. Further, ensure that the employees have demonstrated their competence in their job functions (p. 6-32).*

*A documented formal security training and awareness policy and program is designed to keep staff up to date on organisational security policies and procedures as well as threats, industry cybersecurity standards, and recommended practices (p. C-4).*

It emphasises that training should address “the unique properties and requirements of ICS and the relationship to non-ICS systems,” and include “initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities” (p. G-20).

#### **2.4.1.3 Analysis**

The categories the authors use to describe the differences between IT and ICS reveal a focus on technological differences rather than cultural or managerial aspects. For example, it does not consider what is being measured or controlled, the associated lifecycle, the educational background of professionals, the reporting chain, or the managerial approach. This omission is significant because these non-technological factors provide the context into which a security program must be introduced, and failure to fully consider them cannot be expected to produce effective results.

A second key flaw in the document is its attempt to fit industrial cybersecurity within the pre-established FISMA paradigm, which is built on impacts to confidentiality, integrity, and availability. Section 2.1.1.1 of this literature review asserted that foundational documents for the field of cybersecurity do not demonstrate that their authors considered industrial control applications at the time they proposed confidentiality, integrity, and availability as the foundational concepts. On the other hand, strong evidence supports that the authors of those documents were at the time focused on information and information systems. The proposal to apply a security paradigm to a use case for which it was never intended is striking.

In this regard, SP 800-82 R2 contradicts itself by claiming that “It is important to remember that for an ICS, availability is generally the greatest concern” (p. 6-2), while simultaneously explaining “Human safety is paramount, followed by protection of the process” (p. 2-16). For both of these statements to be true, “availability” and “human safety”

would have to be interchangeable terms; but, clearly, they are not. In short, the document adopts the same approach portrayed by Mallory in the hypothetical dialog.

In terms of its education and training component, the document describes what a program should include and what controls it may implement, but it does not describe who should take what actions, or what knowledge is necessary to take those actions.

## 2.4.2 ISA 99/ IEC 62443

### 2.4.2.1 Characterisation

The International Society of Automation (ISA) is a professional society dedicated to advancing automation within industrial environments, with more than 40,000 members. The organisation creates standards, guidance, and informational content. It puts on conferences and offers trainings. It also provides professional certifications (ISA, “About ISA”).

ISA/IEC 62443 is a series of 14 standards for cybersecurity in industrial automation and control systems, as shown in the figure below. Of the 14 titles, seven have been published to date: 1-1, 2-1, 2-3, 3-1, 3-2, 3-3, 4-1, 4-2 (ISA Global Cybersecurity Alliance, 2020).

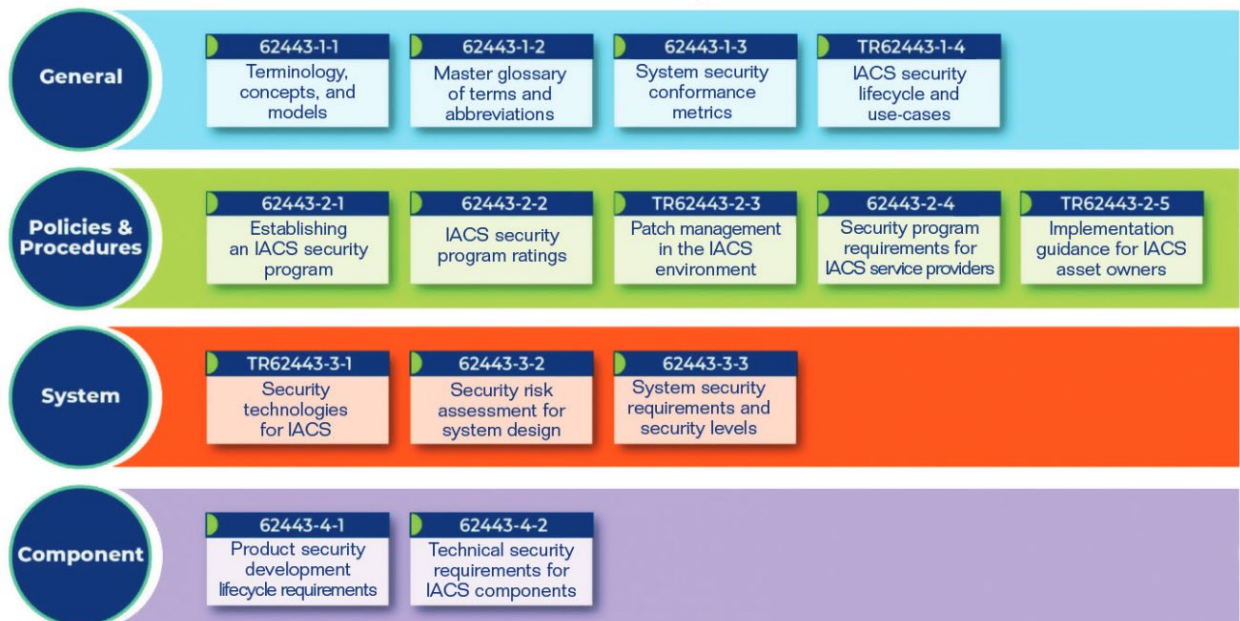


Figure 4. ISA/IEC 62443 family of standards

The documents within the series advance the use of four primary organisation roles involved with industrial automation and control systems: asset owner, maintenance service provider, integration service provider, and product supplier. They divide automation system functions into control, safety, and complementary; they propose the use of zones and

conduits as an approach to secure architecture; and they encourage the designation of security levels to guide the choice of what security control to apply.

#### **2.4.2.2 Education and training**

The ISA standards repeatedly emphasise the importance of training, with the term occurring about 150 times across the published standards (See Table 5). ISA 62443-2-1 “Establishing an IACS Security Program” discusses “training” most directly.

*Table 5. Mentions of "education" and "training" within ISA/IEC 62443 standards*

<b>Publication</b>	<b>Occurrences of “Education”</b>	<b>Occurrences of “Training”</b>
62443-1-1	2	13
62443-2-1	0	117
62334-2-3	0	9
62334-2-4	0	0
62443-3-2	0	0
62443-3-3	0	1
62443-4-1	0	5
62443-4-2	0	1

Page 28 states “All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering,” and establishes the following requirements for staff training and awareness (p. 29):

*Table 6. Requirements for staff training and security awareness*

<b>Description</b>	<b>Requirement</b>
<b><i>Develop a training program</i></b>	<i>The organization shall develop and implement a cyber security training program</i>
<b><i>Provide procedure and facility training</i></b>	<i>All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities</i>
<b><i>Provide training for support personnel</i></b>	<i>All personnel that perform risk management, IACS engineering, systems administration/maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks</i>
<b><i>Validate the training program</i></b>	<i>The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training.</i>

<b><i>Revise the training program over time</i></b>	<i>The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities</i>
<b><i>Maintain employee training records</i></b>	<i>Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis.</i>

The document explains that beyond general training, role-based training should be aimed at individuals with specific duties and responsibilities:

*Role-based training should focus on the security risks and responsibilities associated with the specific role a person fills within the organization. These individuals will need more specific and intensive training. Subject matter experts should be employed to contribute this training. Role-based training may be conducted in the classroom, may be web-based or hands-on. (p. 86)*

In terms of what these professional or job roles may be, the document provides limited insight, describing only the professional roles of a cross-functional risk management team:

- *IACS person(s) who may be implementing and supporting the IACS devices*
- *Operations person(s) responsible for making the product and meeting customer orders*
- *Process safety management person(s) whose job it is to ensure that no HSE incidents occur*
- *IT person(s) who may be responsible for network design and operation, support of desktops, servers, and the like.*
- *Security person(s) associated with physical and IT security at the site*
- *Additional resources who may be in the legal, human resources and customer support/order fulfilment roles (p. 80)*

#### **2.4.2.3 Analysis**

The documents prominently mention the concepts of confidentiality, integrity, and availability, and emphasises that of this triad, availability should be prioritised. However, the documents treat these as part of a broader approach that clearly prioritises safety:

*[Because] industrial automation and control systems equipment connects directly to a process, loss of trade secrets and interruption in the flow of information are not the only consequences of a security breach. The potential loss of life or production, environmental damage, regulatory violation, and compromise to operational safety are far more serious consequences. These have ramifications beyond the targeted organization; they may grievously damage the infrastructure of the host region or nation.*

Interestingly, IEC 62443-2-1 employs the term “operational integrity” four times – once within the body and three times in the Annex. While this term appears to have promise for reconciling safety and security, the document provides it no formal definition; and, the term does not occur in the other published 62443 standards.

The additional frameworks the series of 62443 documents employ, such as organisation roles, system functions, and associated lifecycles encourage rich perspective. The fact that the standards originated from a professional society with deep interest in engineering means the standards appeal to those who have a background outside of computer science or informatics. The value of security level designations as a key component of the standards seems less obvious – potentially an attempt to cross-apply other ISA standards that designate safety levels.

From an education and training perspective, the 62443 documents make clear that cybersecurity training should occur for all parties involved in IACS-related lifecycles. They do not, however, clearly identify the professional roles that should receive that training. They describe what an IACS cybersecurity program should include, but do not describe what each professional role is responsible to do. They state that training should be validated and revised, but do not describe how effectiveness of the training should be evaluated.

### **2.4.3 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)**

#### **2.4.3.1 Characterisation**

NERC is a nonprofit self-regulatory organisation, composed of more than 1,900 members, mostly electric utilities, charged to maintain the reliability of the North American bulk electric system. In this role, it creates regulatory standards and oversees their enforcement (NERC, 2013). Among these are a set of 12 standards dealing with cybersecurity, known as CIP (NERC, “CIP Standards”), as presented in table 7.

Each standard includes a title, number, purpose, description of applicability, a listing of requirements and measures, a description of how compliance may be demonstrated, a matrix describing violation severity levels, and a rationale for each requirement.

*Table 7. NERC CIP Standards*

<b>Number</b>	<b>Name</b>	<b>First effective</b>
CIP-002	Cyber Security - BES Cyber System Categorization	2006

CIP-003	Cyber Security - Security Management Controls	2006
CIP-004	Cyber Security - Personnel & Training	2006
CIP-005	Cyber Security - Electronic Security Perimeter(s)	2006
CIP-006	Cyber Security - Physical Security of BES Cyber Systems	2006
CIP-007	Cyber Security - System Security Management	2006
CIP-008	Cyber Security - Incident Reporting and Response Planning	2006
CIP-009	Cyber Security - Recovery Plans for BES Cyber Systems	2006
CIP-010	Cyber Security - Configuration Change Management and Vulnerability Assessments	2014
CIP-011	Cyber Security - Information Protection	2014
CIP-013	Cyber Security - Supply Chain Risk Management	2020
CIP-014	Physical Security	2015

#### **2.4.3.2 Education and training**

CIP-004 deals specifically with personnel and training. Its purpose is:

*To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems (NERC, “CIP-004-6”).*

Requirement 2 states:

*Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.*

Table R2 then requires:

*Training content on:*

- 2.1.1. Cyber security policies;*
- 2.1.2. Physical access controls;*
- 2.1.3. Electronic access controls;*
- 2.1.4. The visitor control program;*
- 2.1.5. Handling of BES Cyber System Information and its storage;*
- 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan;*
- 2.1.7. Recovery plans for BES Cyber Systems;*
- 2.1.8. Response to Cyber Security Incidents; and*

*2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.*

*Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.*

*Require completion of the training specified in Part 2.1 at least once every 15 calendar months.*

The document provides the following statements of guidelines and technical basis for

Requirement R2:

*Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.*

*One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.*

*Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.*

The document supplies the following rationale for Requirement R2:

*To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.*

#### **2.4.3.3 Analysis**

It is evident that training is an important element of the NERC CIP regulatory regime. It says nothing about education; and, does not aim to describe the qualifications of cybersecurity professionals working in bulk electric system environments. It does not describe any particular pedagogical foundation (for example, safety, or confidentiality, integrity, and availability).

While it does name nine elements a training program should include, none of those elements deal specifically with industrial control systems or specific implications for industrial environments. The rationale statement regarding transient devices and removable media does state “Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations;” but, it does not require the training to cover those incidents.

The requirement does mention the different roles and responsibilities exist within an industrial environment, but emphasises that as long as all named topics are covered, “a single training program for all individuals needing to be trained is acceptable.” The document does not require the training to be updated and revised in accordance with emerging threats, and does not mention evaluation of training effectiveness.

#### **2.4.4 Conclusion from review of industrial cybersecurity practice standards**

This section of the literature review examined three influential practice standards for industrial cybersecurity, representing the perspectives of government, international professional society, and self-regulation. While each of the documents emphasised the importance of training, there were significant inconsistencies among their approaches – especially when specifying the contents of training. Notably, none of them described roles that should receive the training.

#### **2.5 Papers on Industrial Cybersecurity Education and training**

Discussions about industrial control systems and critical infrastructure cybersecurity education emerge in the early 2000s. Two key early examples occur in papers authored by Julie Ryan of George Washington University discussing the benefits received by engineers



attending GWUs information security management courses (Ryan, 2003) and the applicability of information assurance principles to systems controlling more than information – such as industrial operations (Ryan, 2004).

By at least 2013, academics were questioning the efficacy of educating a cybersecurity generalist. A 2013 National Research Council report concluded that “the cybersecurity workforce encompasses a variety of contexts, roles, and occupations and is too broad and diverse to be treated as a single occupation or profession. Whether and how to professionalize will vary according to role and context” (National Research Council, 2013, p.2). Providing one concrete example of this, McGettrick (2014) specifically pointed out that very few electrical engineering departments offered specialisation in cybersecurity.

Yardley, et al. (2014) discussed efforts to incorporate smart grid cybersecurity content into an existing cybersecurity course at the University of Illinois at Urbana Champaign. The authors found that incorporating industrial cybersecurity into university courses was desirable, but presented several challenges:

*Specialized training is traditionally a money-driven and mission-oriented business, focused on bringing a particular audience up to speed with the intended knowledge. This approach, while sometimes quite effective, does not put the material into the hands of the broad general public instead limiting it to those that can afford to pay for the often costly training. This often does not include public entities or academia, as the training tends to be out of reach of most of those participants. Further, it necessitates the direct involvement of subject matter experts to actively teach the topic areas which therefore is limited by instructor availability both in location and timing. In many cases, this material is just a derivation of prior material from another sector that is adapted slightly for the new domain. While adaptation can be effective, it is not an optimal solution for something as specific and critical as the electric power grid.*

Karampidis, et al. (2019) reported that industrial technicians “Operational technicians in industrial companies are not sufficiently aware of the threats nor do they have the competences to take adequate preventive security or response measures.” The authors proposed that future technicians receive 30-50 hours of cybersecurity awareness from three modules: 1) Industrial Systems: Components And Characteristics - Integration of IT/OT; 2) Security Concepts In Industrial Environments; Module 3) Confidentiality, Integrity, Availability in Industrial Environments.

## 2.6 Conclusion

The broad literature review examined foundational cybersecurity education literature, the emergence of “operational technology” as a term to designate the application of digital technologies to industrial control systems, a list of vulnerabilities and events affecting global implementations of these “operational technologies”, and three leading cybersecurity standards that intend to mitigate the occurrence of additional cybersecurity events affecting the physical world.

From the review, it is clear that:

- 1) Cybersecurity is an important and evolving educational and career field with increasingly interdisciplinary implications
- 2) Professionals working with industrial control systems need cybersecurity education and training, but are not receiving it as part of their formalised educational pathway.
- 3) The consensus is that such instruction should be based on the confidentiality, integrity, and availability paradigm, which has historically formed the backbone of cybersecurity education.
- 4) There is a tenuous nexus between academic education – which focuses on knowledge; and, professional training – which focuses on tasks. That is to say, it is unclear what material should be taught to whom, and when and how.

Interestingly, these documents did very little to describe how to fuse cybersecurity and engineering concepts within formalised education and training paradigms.

### 2.6.1 Key Research Question

In light of the findings of this literature review, the most pressing question to address, and that taken up by this thesis is: *What is the foundation for the formal preparation of industrial cybersecurity professionals?*

It is the question on which to the other broad research questions most depend, and as such, will open not only additional avenues of research, but avenues of application. Drilling into this question, the first meaningful word is “foundation”. When designing a curriculum, from a course to a program of study, it is customary to start with a standard for curricular guidance – and such documents are generally widely available; however, a foundation must come before the standard. It should be the research and consensus on which the standard is based. Like the foundation to a building, it must be firm and withstood critical

evaluation from a variety of perspectives, else the building could collapse under its own weight. This question of foundation is significant in a field as young and subject to evolving technology and threats as cybersecurity. In particular, to establish a foundation, it is useful to establish the criteria for what would reasonable constitute a solid foundation. With such a list in hand, a plan of work could be established to create the foundation.

The term “formal preparation” is the next key idea from the research question. Formal preparation implies that certain stakeholders are interested in the educational outcome and intend to apply rigor in their approach to shape the student – who is the product of their intentional effort. The approach to formal preparation must therefore identify and involve the key stakeholders. Examples of formal education include degree and certificate programs, apprenticeships, and professional development opportunities. These stakeholders will be among the key beneficiaries of the research presented in this thesis.

The final key term is “industrial cybersecurity professionals”. Professionals generally means someone skilled in the field who is paid for their work. But this leaves us with the important question of what constitutes an “industrial cybersecurity” professional. This leads to questions such as, what knowledge is required by an industrial cybersecurity professional? what job roles are involved? What tasks do those job roles perform? What skills do they possess? What framework describes the relationships among these job roles, knowledge skills, and tasks? How do experts differ from novices? And many other follow-on questions.

The remainder of this thesis is dedicated to the investigation of this important key question.

### 3 METHODOLOGY

Chapter 1 introduced the broad research problem, and Chapter 2 presented a correspondingly broad literature review. This prepared the way to identify the specific research question forming the central component of this thesis: What is the foundation for formal preparation of industrial cybersecurity professionals?

This chapter provides a general discussion of the methods used in the research approach aimed to answer this question. Given the social, policy, and educational nature of the broad research questions, and the researcher's strength in humanities and business, the researcher adopted a critical pragmatic paradigm to carry out a mostly qualitative multi-phase mixed-methods approach (Creswell, 2014, p. 21).

#### 3.1 Research Validity

A leading concern of any researcher seeking to make a meaningful contribution to a field is naturally the validity of their work. Leading guidance on validity in qualitative research provided by Creswell and Miller (2000) notes that ensuring research validity is a topic with the potential to overwhelm inexperienced researchers. Creswell and Miller attempt to simplify the discussion by introducing a two-dimensional framework meant to help new researchers intentionally identify a rationale for selecting a validity-ensuring technique for themselves.

The two dimensions include 1) the lens used by the researcher; and, 2) paradigm assumptions. The former is composed of using the perspectives of those who: a) conduct the research, b) participate in the research; and c) review the research. The researcher can use any of those lenses to help ensure validity of results. The latter is composed: of x) postpositivist, y) constructivist, and z) critical perspective. Paradigm is not necessarily a choice, but a recognition of researcher preference based on the researcher's worldview – which is not necessarily mutually exclusive of the other two worldviews.

When reviewing the paradigms in light of the researcher's worldview, the critical perspective resounded clearly, with additional value placed on the postpositivist paradigm. Referring to Denzin and Lincoln (1994, p. 9), Creswell and Miller characterise critical perspective as “a challenge and critique of the modern state, [which] holds that researchers should uncover the hidden assumptions...”

Creswell and Miller then provide the following matrix to match validity procedures across lenses and paradigms.

*Table 8. Validity Procedures Within Qualitative Lens and Paradigm Assumptions*

<b>Paradigm assumption/Lens</b>	<b>Postpositivist or Systematic Paradigm</b>	<b>Constructivist Paradigm</b>	<b>Critical Paradigm</b>
<b>Lens of the Researcher</b>	Triangulation	Disconfirming evidence	Researcher reflexivity
<b>Lens of Study Participants</b>	Member checking	Prolonged engagement in the field	Collaboration
<b>Lens of People External to the study (Reviewers, Readers)</b>	The audit trail	Thick, rich description	Peer debriefing

A review of the matrix indicates that researcher reflexivity, collaboration, peer debriefing, triangulation, and member checking are relevant procedures to ensure validity given the researcher’s prevailing paradigms – critical and postpositivist, in that order.

Researcher reflexivity as described by Creswell and Miller, involves self-disclosure of beliefs and biases, to help the researcher suspend them as research progresses, and to aid reviewers and readers in fully comprehending the cultural, historic, or social forces motivating the inquiry. Creswell and Miller advance the use of a section on “the role of the researcher” and interspersing interpretive commentary in written results.

Collaboration refers to the close relationship between the participants and the researcher, which assures validity by “building the participant’s view into the study”.

Peer debriefing involves the use of an external third party who has some familiarity with the research area or method, as a critical sounding board, and to ask the researcher hard questions.

Triangulation incorporates the use of differing information sources, research methods, and researchers (in the case of citing previous research) to identify common themes. Creswell and Miller point out that narrative accounts are valid as a study method because “researchers go through this process and rely on multiple forms of evidence rather than a single incident or data point in their study.”

Member checking, which Lincoln and Guba (1985, p. 314) call the “most crucial technique for establishing credibility”, requires the study participants themselves (rather than the researcher) to confirm the information, which is provided back to them by the researcher as the study progresses.

### 3.2 Human Ethics Considerations

As the researcher is a citizen of the United States and the research was conducted in the United States, involving US citizens, the researcher received responsible research training, including human subjects training, through the Collaborative Institutional Training Initiative Program (CITI Program). Details regarding La Trobe University's Human Ethics committee relative to the research presented in this thesis can be found in Appendix G.

### 3.3 Preview of Research Methods Employed and Corresponding Validity Techniques

Identifying foundations for curricular guidance for an emerging educational field, is a significant undertaking with the potential for broad long-term impact. A novice researcher, even with strong critical thinking, leadership, and professional experience may fail without the input of those who have a similar grasp of the challenge and guidance from those who have successfully addressed similar challenges in the past. Hence, the principal research methodologies used to pursue the research within this thesis will include: 1) structured critical literature review; 2) nominal group technique; 3) focus groups.

The research discussed in this thesis produced a prototype workforce development framework for industrial cybersecurity professionals. Deliverables down the research path included: 1) a list of criteria for creating foundational industrial cybersecurity education and training guidance; 2) identification of key industrial operations knowledge categories and contents not normally covered in cybersecurity education and training; 3) identification of archetype job roles in industrial cybersecurity; 4) identification of key tasks and subtasks for each job role.

The table below presents the method and validation techniques that correspond to each sub-product. The selection of differing research methods and validation techniques enhances the robustness and usefulness of the research products.

*Table 9. Products with corresponding method and validation technique*

<b>Sub-Product</b>	<b>Primary Research Method</b>	<b>Validation Technique</b>
Criteria for foundational guidance (Chapter 4)	Critical literature review	Researcher reflexivity  Triangulation due to cross-comparison of nine documents created by disparate individuals, organisations, and with differing objectives
Key knowledge categories	Nominal group technique	Collaboration via selection of group members

(Chapter 5)		<p>Member checking through 14-member group interacting anonymously</p> <p>Audit trail of formalised method and results</p> <p>Triangulation with published research</p>
Archetype roles (Chapter 5)	Nominal group technique	<p>Peer debriefing</p> <p>Member checking through 14-member group interacting anonymously</p> <p>Triangulation with other documentation</p> <p>Audit trail of formalised method and results</p>
Content per knowledge area (Chapter 6)	Autonomous Proposal	<p>Deductive reasoning based on key events</p> <p>Triangulation via comparison with broadly recognised external documentation</p> <p>Researcher reflexivity</p>
Workforce development framework (Chapter 7)	Critical Literature Review	<p>Triangulation due to cross-comparison of 16 documents created by disparate individuals, organisations, and with differing objectives</p> <p>Researcher reflexivity</p>
Key tasks (Chapter 8)	Focus Groups	<p>Collaboration via selection of group members</p> <p>Member checking</p>

Each chapter discusses the methods used in greater detail. A corresponding validity section for each method addresses potential weaknesses.

### **3.4 The Role of the Researcher**

Recognising – as described in the preceding sections – that the research presented herein is undertaken primarily from the critical, pragmatic paradigm, and that its validity therefore depends significantly on the researcher’s own view, this section describes that view.

To attempt to interpret this thesis and the research it contains without that background may be academically possible, but would severely limit the robustness of such interpretation.

Description of the researcher's role is most readily approachable (for both the author and the reader) in the form of a first-person narrative. While the contents of this section may at first appear of questionable direct importance to the key research elements of the thesis, they have been carefully chosen to provide an appropriate background. Creswell and Miller (2000) affirm that, "The narrative account is valid because researchers go through this process and rely on multiple forms of evidence rather than a single incident or data point in the study."

### **3.4.1 Academic preparation at Idaho State University**

My professional preparation for cybersecurity began as a student in the Scholarship for Service (SFS) program sponsored by the United States National Security Agency (NSA) at Idaho State University (ISU) – one of the first seven schools in the United States to receive that designation (National Centers, 2020). The Principal Investigator of that program was Dr. Corey Schou.

Three particularly noteworthy elements of Schou's own preparation for the role of Professor and Principal Investigator, which he mentioned to his students included: 1) childhood engagement with computer programming when he accompanied his father to work; 2) post-doctoral experience at Florida State University under leading educational psychologist Robert Gagne; 3) creation of airline pilot training software for Federal Express.

Schou came to Idaho State University from Florida State University in about 1985. One of his accomplishments was leading the creation of the Simplot Decision Support Center (SDSC) on the 4<sup>th</sup> floor of ISU's Business Building, to facilitate decision making among medium sized groups.

Schou told his students that his professional interest in cybersecurity began to include security when he realised that sensor data from important tests with which he was working was not carefully protected. From roughly 1989 to 2006, Schou and his colleagues used the SDSC to help create the U.S. government's first information security education and training standards. These standards became the basis for the NSA Centers of Academic Excellence in Information Assurance (now Cybersecurity) and Scholarship for Service programs.



The Scholarship for Service program provided a full-tuition-and-books scholarship and living stipend for students who agreed to study cybersecurity and then work for the government for at least two years after graduation.

At Idaho State University, Schou ran the program under what I characterise as an educational-professional experience. Students were treated as employees working a mandatory 20 hours a week creating high-quality educational materials related to information security. Students had ID badges, filled out time cards, devised projects, and worked in teams. The academic portion of the program was covered by dreaded, yet highly informative “Saturday Classes” lasting from 8:00 to 2:30 or 3:00, with Schou providing pizza for lunch.

All of this was external to the degree the student earned while part of the program – a Masters of Business Administration (MBA) – over which Schou exercised no control. This arrangement reflected his core belief that information security is by nature an interdisciplinary field, and that doing something securely may be more important than doing security by itself.

I graduated from the SFS program with an MBA degree in 2006, and took my first job at the Idaho National Laboratory (INL), a 45-minute drive north of ISU’s main campus.

### **3.4.2 Professional experience at the INL**

I joined INL as about its twentieth employee dedicated to supporting external government customers on cybersecurity-related projects. The INL is a contractor-operated research institution focusing on national challenges to energy and homeland security. In the early 2000s, the INL and other national labs collaborated on an initiative known as the “National SCADA Testbed”. The initiative brought leading energy management systems, and later, turnkey industrial control systems software into the Lab for security evaluation.

Researcher teams thoroughly investigated the software to identify and describe significant vulnerabilities. The results were documented and shared with sponsoring agencies and the control systems vendor under a public-private partnership model.

At the INL, I was involved in three related tasks: 1) authoring and reviewing assessment reports; 2) maintaining situational awareness of the evolving cyber threat environment for industrial control applications; 3) presenting findings at government-sponsored training events.

Maintaining situational awareness of the threat environment involved using a variety of open source intelligence tools to monitor a breadth of security sources such as mail lists

and web sites for any mention of industrial control systems vendors or controlled processes. This honed my skills using relevant tools, forced me to write and communicate clearly, and allowed me to explore world of individuals with differing motivations discussing control system security.

When I presented these findings at training events, I was surprised by the enthusiasm attendees expressed. A colleague and I requested the INL invest its own funds to make our situational awareness effort what we thought it needed to be. Our request was declined. We asked the INL to work with us to spin our concept into a stand-alone company. Our petition was similarly denied. Convinced of the relevance of our work, the colleague and I decided to leave the INL and start our own firm, which we named Critical Intelligence.

### **3.4.3 Critical Intelligence**

Critical Intelligence launched in January 2009 with the mission of being the best in the world at explaining the evolving threat environment to critical infrastructure and industrial control systems stakeholders. This meant my personal job was to know everything I could about the confluence of control systems and cybersecurity.

We landed early customers from the energy sector, including notably, the Electric Sector Information Sharing and Analysis Center (ES-ISAC), operated by the North American Electric Reliability Corporation (NERC). This gave us a platform to share our findings and thereby attract additional customers.

Business growth, though slow for first-time entrepreneurs in a field with no pre-existing category demand, was also advanced by the defining moment for industrial control systems security – Stuxnet, which came to light in mid-2010. I viewed it as my job to update our customers on the latest insights involving the event – to be a one-stop-shop for quality information and links to the most-primary sources available.

While the full story of Stuxnet emerged slowly, my familiarity with open source techniques and knowledge of disparate sources led me to propose a theory of how the organisations behind Stuxnet hatched the idea and carried out the attack. This theory was first published to my customers, and later appeared in the Christian Science Monitor (Clayton, 2014) on the day I delivered it in a talk at the RSA Security Conference.

The theory differed from prevailing accounts because rather than focus on what the worm attacked or how it worked from a technological perspective, it highlighted the profound significance of control systems integrators, engineers, and technicians to

adversaries who were planning attacks. We might say that it examined the targeting element of structured attack. Even today, there appears to very little academic or practitioner discussion about nation-state targeting of cyber-attacks. Those procedures and capabilities remain a closely held secret.

The theory explained that in order to create the complex Stuxnet malware – which would only truly attack a specific process within a specific plant, and then remove itself if that specific target were not found by a certain date – its authors must have had previous access to precise details about the target process, including, for example, the piping and instrumentation diagram, the exact model of variable frequency drive employed, and the actual logic on the PLCs. This precise level of detail could only be obtained from the engineering workstation or lap top used to design and program the uranium enrichment process. Hence, the control system integrator firm, and the engineers and technicians who work in the plant are the indispensable high value targets. My investigation was able to show – by relying entirely on freely available public sources – the identity of the integrator firm. It also began to explore the implications of how Stuxnet creators would have organised themselves to plan and launch such attacks.

I became acutely aware that most control systems integrator firms, engineers, and technicians were ignorant of the risks they faced by virtue of their access to the PLCs and the software used to program them.

#### **3.4.4 Founding of the Energy Systems Technology and Education Center (ESTEC)**

Idaho State University is fairly unique in that it houses a two-year technical college within the university. The College of Technology electronics program dates to 1940 (Summers, 2015). In 2007 with the support of the Idaho National Laboratory, ISU partitioned this program into two halves: Robotics & Communications, and the Energy Systems Technology and Education Center (ESTEC [Idaho State University, 2008]). ESTEC took the mission of preparing technicians to enter industrial fields, offering two-year degrees across four engineering technology programs: Instrumentation, Electrical, Mechanical, and Nuclear Operations (Idaho State University, n.d.).

In 2015, the state approved ISU's proposal to add a cyber-physical security degree to ESTEC's offerings, thus creating the first cyber-physical security degree program in the country (Idaho State Board, 2015).

### **3.4.5 Cyber-Physical Security Program at Idaho State University**

Knowing my experience in the field of industrial control systems, and as an alumni living in the area, Dr. Corey Schou put me in touch with the Executive Director of ESTEC to see whether I would be interested in teaching a course as adjunct faculty. I agreed to dedicate one night a week to one class in each fall and spring semester.

This gave me time to meet students, get teaching, and feel-out the culture of the ESTEC department. Most impressive to me was the millions of dollars invested in instructional laboratories. Students learned to create AC and DC circuits, align motors and pumps, deploy and calibrate transmitters, and program PLCs. The cyber-physical security program needed a leader – a program coordinator.

Recognising an opportunity to meet the exact problem I had noted as an analyst – the lack of cybersecurity training and awareness among engineering professionals working within industrial environments – and that the state of Idaho had already invested millions of dollars and approved the first of its kind degree program, I decided to leave FireEye (which had since acquired the firm that acquired my firm), and join ISU.

To further my own professional development in this role, and in support of my PhD studies, I completed four education-related courses at the graduate level at Idaho State University:

- CTE 5501: Foundations of Career and Technical Education
- CTE 5502: Course Analysis and Construction
- CTE 5503: Methods of Training
- CTE 5504: Evaluation in Teaching Career and Technical Education

As a Program Coordinator, my responsibilities included curriculum development, student recruiting, teaching, creating and operating an industry-led technical advisory committee. The most pressing of these responsibilities was curriculum development.

My coursework in curriculum development emphasised the importance of aligning program and course content with existing educational standards. It also introduced me to the topic of task analysis, relying heavily on the approach described by Robert Mager (1997). As I began to develop the program, I searched for what I might consider a compelling content standard for industrial cybersecurity education and training. That search would become my thesis topic.

### **3.5 Conclusion**

This chapter has provided an overview of the mixed-methods approach, research paradigm, and validity techniques used to address the principle research question. Because it is primarily an overview chapter, specific details on methodology, including validation, are provided within each chapter.

## **4 CRITICAL REVIEW OF INDUSTRIAL CYBERSECURITY EDUCATION AND TRAINING GUIDANCE DOCUMENTS**

### **4.1 Problem**

The specific research question of this thesis is “What is the foundation for formal preparation of industrial cybersecurity professionals?” Chapter 2 – the broad literature review – identified and briefly discussed nine candidate documents/efforts that might contain insights to such a foundation. This chapter compares those documents/efforts, individually and collectively with what might be considered an ideal foundation for a standard. The term “document/effort” is employed to note that in some cases, the identified effort is composed of multiple documents.

### **4.2 Research Design**

The method selected for this endeavor is a two-part structured literature review. Where a broad literature review, such as that presented in Chapter 2 of this thesis, is useful in forming a baseline orientation about the current state of knowledge relevant to the broad set of research questions (Creswell, 2014), the integrative approach (Snyder, 2019) used in this chapter involves first, creation of an analytical framework that will allow the literature to be systematically searched for specific detail, and; second, the application of the framework to obtain the desired insight.

Before conducting the review, the researcher must identify the body of documents to be reviewed. Search techniques play a crucial role in this process. In this case, the researcher relied on both academic and non-academic search engines employing terms such as: cybersecurity education and training, workforce development, industrial control systems, and standards. The researcher also employed the names of countries in which industrial control systems security initiatives were underway in the English language.

The two parts of the structured review did not occur in isolation from one another, but rather emerged as an iterative process as the documents were read and re-read. While structured text analysis techniques may be helpful in some literature review scenarios, in this case, creation of the framework required uniquely human synthesis because it sought to establish not only key commonalities, but key disparities among documents with differing lexicons.

#### **4.2.1 Review of industrial cybersecurity curricular guidance efforts/documents**

The search process identified nine efforts/documents potentially relevant to industrial cybersecurity. The following subsections explore each one.

##### ***4.2.1.1 Accreditation Board for Engineering and Technology (ABET)***

Postsecondary engineering and computer science schools – particularly in the United States – commonly adhere to educational guidance maintained by the Accreditation Board for Engineering and Technology (ABET).

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

In November 2018, ABET approved specific accreditation criteria for “cybersecurity” programs. 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 degree programs) and Engineering Technology Accreditation Commission (mostly associate degree programs). The accreditation criteria for programs overseen by these Commissions does not address or even mention security.

##### ***4.2.1.2 European Union Agency for Network and Information Security (ENISA)***

ENISA is an organ of the European Union dedicated to informing cybersecurity policy for the European Union (ENISA, n.d.). Industrial control systems security was a significant focus area for ENISA from 2011 to 2015, but its website shows little beyond those dates.

ENISA’s major publication related to educational guidance for industrial control environments, “Certification of Cyber Security skills of ICS/SCADA professionals: Good practice and recommendations for developing harmonised certification exams” (Pauna, 2014), clearly addresses the need for developing industrial cybersecurity professionals separate from information systems. It does not however describe why or how this is the case.

The effort drew from the input of 64 professionals from various countries, employers, and industries (Pauna, pp. ii-iv).

The document 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 nine “technical roles”, as presented below:

*ICS/SCADA Cyber Security professionals that have specific accountability or responsibility for ICS/SCADA Cyber Security. This is the group that needs to be trained (and if needed) certified. This group can be divided in groups as well:*

*Management roles:*

- *ICS/SCADA Security Manager (e.g., responsible person for central team of specialists/Centre of Excellence).*
- *Manager in the business with accountability for ICS/SCADA Cyber Security (often line manager, such as engineering manager, plant manager, OT manager, IT Manager, maintenance manager, Integrator of IT and OT environments).*
- *Management of process control systems and associated maintenance responsible control system engineers.*

*Technical roles:*

- *ICS/SCADA focal points in the business*
- *ICS/SCADA Security Operations Centre personnel*
- *ICS/SCADA (Forensic) Analysts*
- *ICS/SCADA Incident Response professionals*
- *ICS/SCADA Cyber Security Architects*
- *ICS/SCADA Cyber Security Analyst*
- *ICS/SCADA Cyber Security R&D personnel*
- *Cyber Security professionals in ICS Development organisations*
- *ICS/SCADA Cyber Security testers*

Authors listed learning goals for the technical management roles as

- *How to build a security program*
- *Risk management and compliance in the IACS domain*

The list of 12 knowledge areas and content included (Pauna, pp. 16-18):

<b><i>Knowledge areas</i></b>	<b><i>Content</i></b>
<i>ICS Security Governance and Risk Management</i>	<i>*Basic process control systems (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, Ethernet I/O, buses, Purdue Model (ISA 9539))</i>



	<p><i>*Critical infrastructure subsectors (e.g., chemical, waste water, drinking water and water quantity management, electricity, oil and gas, manufacturing, transport)</i></p> <p><i>*Safety and protection systems (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring)</i></p>
<i>ICS Architecture</i>	<p><i>Communication medium (e.g., VSAT, RF, cell, microwave)</i></p> <p><i>Defence in depth (e.g., layered defines, IDS sensor placement, security system architecture, virtualisation)</i></p> <p><i>External network communications (e.g., access points into ICS/SCADA systems, VPNs, vendor/third party access points, mobile devices)</i></p> <p><i>*Field device architecture (e.g., relays, PLC, switch, process unit)</i></p> <p><i>*Industrial protocols (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC)</i></p> <p><i>Network protocols (e.g., DNS, DHCP, TCP/IP, UDP)</i></p> <p><i>Network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs)</i></p> <p><i>Wireless security (e.g., Wi-Fi, wireless sensors, wireless gateways, controllers)</i></p>
<i>ICS Modules and Elements Hardening</i>	<p><i>Anti-malware implementation, updating, monitoring, and sanitization</i></p> <p><i>Application security (e.g., OWASP40, database security)</i></p> <p><i>*Embedded devices (e.g., PLCs, controllers, RTU, analysers, meters, aggregators, security issues, default configurations, embedded applications (e.g., Windows XP embedded)</i></p> <p><i>End point protection including user workstations and mobile devices (e.g., anti-virus, white listing)</i></p> <p><i>Network security/hardening (e.g., switch port security)</i></p> <p><i>Operating System security (Unix/Linux, Windows, Windows XP embedded, least privilege security, virtualisation)</i></p> <p><i>Removable media (e.g., USB device security, optical) media, external drives)</i></p>

	<i>Persistent memory (hard disks)</i>
<i>ICS Security Governance and Risk Management</i>	<p><i>*Global security standards, practices, and regulations (e.g., IEC/ISA 62443, NIST 800-8241, ISO 27000 standards)</i></p> <p><i>*Risk management (e.g., PHA/HAZOP usage, risk acceptance, risk/mitigation plan)</i></p> <p><i>Security lifecycle management (e.g., acquisition and selling of an asset, procurement, commissioning [e.g., secure deployments], maintenance, decommissioning)</i></p> <p><i>Security policies and procedures development (e.g., exceptions, exemptions, requirements)</i></p>
<i>Cyber security Essentials for ICS</i>	<p><i>Attacks and incidents (e.g., man in the middle, spoofing, social engineering, denial of service, denial of view, data manipulating, session hijacking, foreign software, unauthorized access)</i></p> <p><i>Availability (e.g., health and safety, environmental, productivity)</i></p> <p><i>Cryptographic (e.g., encryption, digital signatures, certificate management, PKI, public private key, hashing, key management, resource constraints)</i></p> <p><i>Security awareness programs (e.g., employees / management)</i></p> <p><i>Security tenets (e.g., CIA, AIC, non-repudiation, least privilege, separation of duties)</i></p> <p><i>Threats (e.g., nation states, cyber criminals, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious such as errors and omissions)</i></p>
<i>ICS Security Assessments</i>	<p><i>Device testing (e.g., communication robustness, fuzzing)</i></p> <p><i>Penetration testing and exploitation</i></p> <p><i>Security assessments (e.g., risk, criticality, vulnerability, attack surface analysis, supply chain)</i></p> <p><i>Security tools (e.g., packet sniffer, port scanner, vulnerability scanner)</i></p> <p><i>Device testing</i></p>
<i>ICS Security Monitoring</i>	<p><i>Archiving</i></p> <p><i>Event monitoring and logging</i></p>

	<i>Network monitoring and logging</i> <i>Security monitoring and logging</i>
<i>Access Management</i>	<i>Access control models (e.g., MAC, DAC, role-based)</i> <i>Directory services (e.g., active directory, LDAP)</i> <i>User access management (e.g., user accounts, service accounts, temporary accounts, default accounts, guest accounts, account expiration, access control list, access reconciliation)</i>
<i>Configuration/Change Management</i>	<i>Change management, baselines, equipment connections, and configuration auditing</i> <i>Distribution and installation of patches</i> <i>Software reloads and firmware management, software version management</i>
<i>Physical Security</i>	<i>Physical Security</i>
<i>Disaster Recovery and Business Continuity</i>	<i>Site redundancy (e.g., hotsite, off-site backup)</i> <i>System backup (e.g., security, data sanitisation, disposal, redeploying, testing backups, operational procedures)</i> <i>System restoration (e.g., full, partial, procedures, spares)</i>
<i>Incident Management</i>	<i>Incident recognition and triage (e.g., log analysis/event correlation, anomalous behaviour, intrusion detection, egress monitoring, IPS)</i> <i>Incident remediation/recovery</i> <i>Incident response (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine)</i>

\* indicates content not normally be covered in a traditional cybersecurity course (\*added)

While this is the most comprehensive and descriptive list of knowledge provided across the efforts/documents reviewed, the methodology the group used to create it remains somewhat unclear.

Of the 51 “Contents” entries, it seems that only eight explicitly deal with concepts that would not normally be covered in an IT security course or certification.

The document reports that its work “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.”

In addition, the ENISA authors made the following nine recommendations related to certifications – though they also appear to apply to educational guidance documents 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*

This final recommendation is of particular interest and importance because it differentiates between what someone knows and what someone can do. It is also challenging to accomplish because it requires more detailed consideration of *how* to appropriately address a challenge.

#### ***4.2.1.3 Global Information Assurance Certification (GIAC)***

GIAC is the certification arm of the multi-faceted cybersecurity education and training company SANS. SANS is perhaps the most recognisable cybersecurity training company in the world. It provides primarily working professionals with high-quality online and in-person training experiences led by engaging instructors.

In 2013, GIAC launched the Global Industrial Cyber Security Professional (GICSP) certification exam. A 2016 document, *The GICSP: A Keystone Certification* authored by SANS employee Derek Harp, describes at a high level, the process of its creation (Harp, 2016). Addressing industrial cybersecurity is the document’s clear objective. It implies that differences exist between industrial control and information technology environments, but does not identify or describe these differences. The document notes that development of the GICSP certification was led by a cross-industry steering committee composed of 12 individuals from various nationalities and industries, whose names it provides.

A November 2018 telephone interview with Michael Assante, who spearheaded creation of the GICSP certification for SANS/GIAC, indicated that more than 60 individuals had participated in the development process, mainly through online surveys (this corresponds closely with the number 64 provided by ENISA [McBride, 2018]). While he did not describe precisely how decisions were ultimately made, it seems reasonable to call this a consensus.

Harp's report on the GICSP certification included 47 "competency objectives". These objectives mirror, almost exactly, the "Knowledge areas" and "Contents" listed in the ENISA document.

It is clear that the GICSP steered away from identifying differing roles or sector-specific content. In the interview, Assante described the GICSP as a single general certification. He used the analogy of medical professionals in the operating room: what must everyone know – from the surgical technician to the anesthesiologist – in order to be in the room?

A review of the SANS GICSP web site in December 2020 indicates that the original list of 47 objectives has been coalesced to a more manageable set of ten "objectives and outcomes" statements (GIAC, 2020):

*Hardening ICS Operating Systems*

*The candidate will be able to describe how to implement endpoint security software along with hardening and patching, to secure the Windows and Unix style operating systems commonly found in an ICS environment.*

*ICS Communications and Compromises*

*The candidate will be able to describe the basic structures, protocols, and defense of communications within an ICS and summarize how they can be compromised. The candidate will also be able to, at a basic level, describe the cryptography used to protect communications.*

*ICS Intelligence Gathering*

*The candidate will be able to determine the threat landscape of an ICS through the investigation of information leakage points and logs, and honeypots, when appropriate.*

*ICS Level 0 and 1 Technology Overview and Compromise*

*The candidate will be able to describe level 0 and level 1 devices and technologies and summarize how those devices and technologies are targeted and attacked.*

*ICS Level 2 and 3 Technology Overview and Compromise*

*The candidate will be able to describe level 2 and level 3 devices and technologies and summarize how those devices and technologies are targeted and attacked.*

#### *ICS Overview and Concepts*

*The candidate will be able to summarize the function of high-level assets that comprise Purdue model levels zero through three. The candidate will be able to compare and contrast DCS systems with SCADA systems.*

#### *ICS Procurement, Architecture, and Design Fundamentals*

*The candidate will be able to compare and contrast ICS architectures with traditional IT architectures. The candidate will demonstrate understanding of how procurement and physical security can complement a secure and defensible ICS network architecture. The candidate will be able to summarize the use of levels and zones in defining a secure ICS architecture as well as the devices deployed at each level and zone.*

#### *ICS Program and Policy Development*

*The candidate will be able to summarize the steps and best practices used in building a security program and creating enforceable security policies for an ICS.*

#### *ICS Wireless Technologies and Compromises*

*The candidate will be able to summarize the different wireless communication technologies used in an ICS, how they are targeted, and how they can be defended.*

#### *Risk Based Disaster Recovery and Incident Response*

*The candidate will be able to describe how risk is measured and how it can be used to inform disaster recovery and incident response.*

The most striking difference between the initial list of objectives provided by Harp and the current web page is the reduction of specific detail that would be useful to students or instructors.

#### **4.2.1.4 International Society of Automation (ISA)**

The International Society of Automation is a professional society serving those involved in automating industrial operations. ISA provides both training opportunities and certification for these professionals (International Society, n.d. *About ISA*,).

ISA has established two principal certifications of industrial automation professionals: Certified Automation Professional (CAP) and Certified Control System Technician (CCST [International Society, n.d., *Certification Programs*]) -- neither or which are security-focused. For both certifications, the ISA makes publicly available its common

body of knowledge domains, task categories, task lists and supporting knowledge (International Society, n.d. *CCST*).

The ISA Committee charged with developing cybersecurity standards, ISA99, has proposed a series of 14 standards documents known as the IEC 62443 series. Seven of documents have been published; and four of those published are undergoing revision (International Society, n.d., *Industrial*).

Though ISA does offer cybersecurity trainings based on the contents of the IEC 62443 standards (International Society, n.d., *62443*), a review of the actual IEC 62443 series shows that the group has not yet advanced education or training curricular guidance. IEC 62443-2-1 Security Program Requirements for IACS Asset Owners encourages individuals receive training in accordance with their security responsibilities, but does not identify or describe individual roles and responsibilities for industrial cybersecurity.

In 2009, the Automation Federation, an organisation sponsored by the International Society of Automation, released its Automation Competencies Model, developed in conjunction with the United States Department of Labour (U.S. Department of Labour, 2009). The document includes a two-page section “Industrial Automation and Control Systems Cybersecurity”. The document clearly recognises that differences between IT and industrial control systems exist, and lists eight critical cybersecurity work functions:

- *Differentiate between IT and OT architectures and the operation of these architectures*
- *Manage Cybersecurity risk as it relates to IACS*
- *Determine and implement the appropriate tools and methods for IACS Cybersecurity*
- *Understand zones and conduits identification*
- *Understand Security Level (SL) per zone*
- *Professional development to stay current on threats and remediation methodologies*
- *Incorporate new and emerging cybersecurity defense technologies and trends into proposed solutions*
- *Reassess risk as automation systems evolve*

The document also identifies 13 Technical Content Areas with example content:

#### *General*

- *Understand policies and procedures - IT and OT*
- *Technologies –Security Lifecycle - assess, implement and maintain*
- *People – training and motivation*

#### *Networks*

- *Recognize the impact on OT systems of security hardware and software options such as encryption and intrusion detection*
- *Explain guidance on separation of OT and IT system networks and components*
- *Identify zones and conduits and implement controls*

#### *Operating systems*

- *Describe how to manage patches to IT and OT operating systems*
- *Recognize the implications of installed patches to IT and OT systems*

#### *Telecommunications*

- *Describe the communications protocols used in OT architectures, with their relative pros and cons*
- *Information assurance - The standards, procedures, and applications used to protect the confidentiality, integrity and availability of information and information systems*
- *Identity management and authentication*
- *Access control*
- *System integrity*
- *Data confidentiality*
- *Restricted data flow*
- *Timely response to events*
- *Resource availability*

#### *Security Lifecycle – The overall business process for managing security of information and information systems*

- *Understand that security management is a continuous process*
- *Recognize the key elements which must be present in any security lifecycle: governance, identify, protect, respond and recover*

#### *Governance - The knowledge and skills, and abilities needed to successfully manage the process*

- *Policies and procedures – defining what will be done and how*
- *Oversight – ensuring the process is working*

#### *Identify – The knowledge and skills, and abilities needed to identify the assets to be managed*

- *Differences between OT and IT systems - recognize the specialized system requirements of OT systems*
- *Asset management*
- *Risk management – the systems, tools, and concepts used to minimize the risk to an organisation's cyberspace and prevent a cybersecurity incident*
- *Computer defense - describe the impact of computer defense techniques and tools (such as penetration testing and vulnerability scanning) on IT and OT systems and know when to use such techniques or tools*



- *Contracting and procurement - describe critical IT and OT procurement requirements*
- *Enterprise strategies - explain the rationale of and adhere to IT and OT supply chain security/risk management policies, requirements, and procedures*

*Protect – The knowledge and skills, and abilities needed to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services*

- *Technologies and architectures – how to make systems secure (firewalls, DMZ, zones, conduits, VPNs)*
- *Access control – limiting access to systems (role-based access and account management)*
- *Awareness and training – making users aware*
- *Data security – protecting valuable information*
- *Maintenance – managing updates safely and securely – virus scanning, patch management*
- *Outsourcing – safely outsourcing the entire technology environment (cloud computing, etc.), taking into account the limitations of outsourcing OT systems*
- *Safe internet behavior – not accessing email or internet on OT system computers; not installing unauthorized software on OT system computers*
- *Remote working - restrictions on accessing OT systems at home or outside the secure work areas of the business*

*Detect - The knowledge, skills, and abilities needed to identify threats or incidents*

*Intrusion detection tools*

- *Network monitoring resources*
- *Attack stages*
- *Evasion strategies and techniques*
- *Incident classification*

*Respond - The knowledge, skills, and abilities needed to respond to and remediate an incident, as well as restore functionality to the system or infrastructure*

- *Response/business continuity planning/resilience*
- *Analysis – investigate anomalies, perform forensics, classify the incident*
- *Communications – understand roles and order of operations; report incidents consistently within established criteria; share information in accordance with plans; coordinate with stakeholders*
- *Mitigation – contain and mitigate incidents*

*Recover – The knowledge, skills, and abilities needed to ensure timely restoration of systems or assets affected by cybersecurity events and adoption of lessons learned*

- *Recovery planning – execute recover plan*
- *Communications – manage public relations; repair reputation; communicate with stakeholders*
- *Improvements – incorporate lessons learned into plans and update response strategies*

*Standards*

- *ISO 27001 – International Information Security Management Guidance*
- *Office of Homeland Security System and Physical Security Regulations (US only)*
- *ISA/IEC 62443 – Security for Industrial Automation and Control Systems*
- *NIST Cybersecurity Framework*

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. The only clue it provides as to the method used for its creation is “Development of the technical competencies relied heavily on A Guide to the Automation Body of Knowledge, 3rd Edition, Nicholas P. Sands and Ian Verhappen, Editors” (p. 5).

It is interesting to note that the ISA effort maps its technical content areas to the NIST Cyber Security Framework categories (discussed in greater detail below). More intriguing is the fact that the original version of the NIST NICE framework published in 2017 made this mapping, but the revised version of 2020 does not.

It is also interesting that cybersecurity is treated only in tier 5, and are not incorporated into Tier 2 under “Basic Computer skills” or Tier 3 under “Working with Tools and Technology”.

#### **4.2.1.5 Joint Task Force on Cybersecurity Education**

The Joint Task Force on Cybersecurity Education is composed of notable academic organisations: 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). Each of these (sometimes competing) academic and professional organisations seeks to further the state of

science for computer-based fields, are the publication and presentation outlets for thousands of scholars around the globe.

In 2017, the Joint Task Force published its landmark report “Cybersecurity Curricula 2017”, which sought to define and formalise “cybersecurity” as its own academic discipline (Burley, 2017).

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 the Joint Task Force effort provided limited curricular guidance on the topic.

#### ***4.2.1.6 National Institute of Standards and Technology***

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce tasked to create, promote, and maintain common standards for the purposes of improving shared understanding, and interoperability that underlie economic progress. NIST has led out on cybersecurity training guidance for the US government since at least 1998 when it published Special Publication 800-16 “Information Technology Security Training Requirements: A Role- and Performance-Based model” (DeZafra).

In 2017, the United States National Institute of Standards and Technology (NIST), working with the Department of Homeland Security (DHS), published its National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The framework,

codified in NIST Special Publication 800-181, represents a significant undertaking to classify responsibilities of the US cybersecurity workforce. The document, when published, included 7 workforce categories, 34 specialty areas, and 52 work roles. Each work role included tasks as well as knowledge, skills and abilities (KSAs). Each KSA is an independent entry, and can be mapped to any applicable work role. The original document performs these mappings (Newhouse, 2017).

A 2020 revision of the Framework (featuring four of five new authors) deprecated the workforce categories and specialty areas, but explained that they may still be used to the extent those using them find beneficial. The revision combined skills and abilities into a single “skills” category – presumably because there was no clear distinction between them anyway. It moved work roles, knowledge and skills, from the framework proper and included them as supplementary materials (Peterson, 2020).

A review of the 2017 Framework shows that the authors paid almost no attention to industrial control systems. First, the NICE framework never mentions the term “industrial control system”. Instead, it uses the term “SCADA”, which is a particular application of industrial control. Second, the term “SCADA” appears only at the KSA level, rather than as a specialty area or work role. Finally, of the three occurrences of term “SCADA” two are in parenthetical references:

- *Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access*
- *Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)*

The third occurrence is a single broad swipe

*Knowledge of general Supervisory control and data acquisition (SCADA) system components*

The Framework maps these KSAs to the Specialist, Target Developer, and Threat/Warning Analyst work roles. Interestingly, none of these roles correspond to individuals assigned to actually protect or defend operational industrial control systems that ultimately provide critical services such as electricity or drinking water. The document includes no additional coverage of industrial cybersecurity, leading to the conclusion that the authors and contributors of the NICE framework considered ICS only tangentially.

#### 4.2.1.7 *National Security Agency*

The United States National Security Agency (NSA) is the executive agency that uses cybersecurity both offensively and defensively to “gain decision advantage” for the nation and its allies (National Security Agency, n.d. *Mission and Values*).

In an effort to improve the quality and quantity of the U.S. cybersecurity workforce, the NSA helped establish the Centers of Academic Excellence in Information Assurance (now Cybersecurity). Since 1999, the NSA has required participating schools to demonstrate adherence to NSA’s educational standards, much as they would for any other program accreditation (Bishop, 2009).

In 2014, the NSA adopted a “knowledge units” approach for schools to demonstrate their compliance with its curricular guidance (Conklin, 2014). Under this shift, the NSA created a Knowledge Unit for Industrial Control Systems (ICS). This unit is optional, meaning that schools are not required to include its content unless they desire to offer a specialisation in this field.

The 2020 Knowledge Unit is clearly labeled for Industrial Control Systems. It offers no description of how industrial control systems or their security differ from common information systems. It provides no insight into how it was created or who created it. It is publicly available, though not necessarily easy to find. As the name “knowledge unit” implies, it covers knowledge, but does not cover job roles or tasks (Information Assurance Directorate, 2020).

The intent statement for the Knowledge Unit 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.*

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”. One 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.

The clause “where they are likely to be found” seems 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.*

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, one would expect to see an outcome dealing with industries and processes which employ industrial control systems, but such an outcome is not provided.

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*

These nine topics offer little intuitive categorisation or prioritisation 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 discuss ICS-oriented defensive techniques, as well as specific ICS-related security guidance and regulatory requirements included among the topics.

#### ***4.2.1.8 Pacific Northwest National Laboratory***

The Pacific Northwest National Laboratory (PNNL) of the U.S. Department of Energy is a research lab focusing on energy, environmental, and national security issues, founded as an offshoot of the nuclear bomb development project during the 1940s (Department of Energy, n.d.).

Working with external contractors, PNNL created a workforce development guidance document entitled “Secure Power Systems Professional” (SPSP), which it published in several documents between 2012 and 2015, aiming to “identify and understand the competencies necessary to perform cybersecurity functions and to assess the need to develop a set of guidelines for a certification program for future power system cybersecurity specialists” (O’Neil, 2015).

One of the reports, a 182-page document entitled “Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional Project” (O’Neil, 2013) specifically identifies industrial control systems and classifies power systems under this broad category.

The document asserts there is a “very challenging blend of control engineering and security that is required to protect the OT in smart grid networks and advanced energy control systems”; but it never describes this “blend”. Instead, it focuses on “What domains of knowledge and types of cybersecurity-associated skills and abilities are necessary for [power system] engineers?” (p. 1.5). In other words, it assumes that the individual receiving the additional education or training is already an engineer involved in industrial operations.

The amount of detail regarding the methodology used to develop the guidance surpasses that provided by all other efforts reviewed in this thesis. The authors of the document created a 33-member SPSP subject matter expert panel representing the power industry, technology vendors, professional services firms, government agencies, and research organisations. Membership was about equal across categories if one combines government agencies and research organisations (p. 2.1). The effort disclosed the names and employers of these participants, though it did not disclose their titles (p. A.1).

The SME panel and others, participated in exercises that identified target job roles for secure power systems professionals, mapped the job roles to existing certifications, and mapped responsibility areas to existing documents and courses to find areas of match and need.

Ultimately the work identified four Secure Power Systems Professional (SPSP) job roles and details the associated knowledge, skills, and abilities of each, with the intent of aiding managers and HR personnel in conducting performance reviews, creating professional development plans, specifying learning objectives, and creating job descriptions.

The four roles are: Secure Power Systems Engineer, Intrusion Analyst, Incident Responder, and Operator. Related to the topic of roles, the document does express concern that operators and technicians of power systems should also be trained (pp. 1.6-1.7)

The list below presents the KSAs from the work that most relate to industrial control systems:

- “Access an up-to-date power systems inventory and asset list.”
- “Understand North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) and audit requirements.”
- “Configure Security Information and Event Management (SIEM) rules and alerts for unsupported devices such as those used in the power systems and Advanced Metering Infrastructure (AMI).”
- “Analyse vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific smart grid components.”
- “Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints.”
- “Collect vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments.”
- “Review checklist for implementing a device or system for necessary sign-offs.”

Besides including the four terms “power systems”, “Advanced Metering Infrastructure”, “smart grid components”, and “device”, there is nothing control systems-specific about the specified content. By removing those terms, they could be accurate (and useful) descriptions related to the cybersecurity of many technological contexts.

In summary, the authors of the SPSP effort went to great lengths to reach consensus on how existing cybersecurity workforce development frameworks related to the needs of



power systems professionals, but they did not describe what minimum set of control systems knowledge is common to industrial cybersecurity professionals, nor what makes industrial cybersecurity differ from non-industrial applications.

#### 4.2.1.9 *Singapore SkillsFuture (SF)*

SkillsFuture is an effort by the government of Singapore to intentionally align workforce development with the country’s critical needs (SkillsFuture, n.d.).

In October 2018, Singapore SkillsFuture, produced a set of documents related to numerous occupations across Power Generation, Distributed Generation, Electricity Transmission and Distribution, Gas Systems Operations, Town Gas Production and Plant Maintenance, and Gas Transmission and Distribution (SkillsFuture, 2018, *Skills Framework*). Twenty-five of these occupations require 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

Each of these competencies is described within its own document, which decomposes the competency into six levels of proficiency, and identifies required knowledge and tasks for each level.

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 (Skills Future, 2018, *Operational Technology Security Design*, *Operational Technology Security Audit Management*):

Technical Skills and Competencies	Operations and User Support
-----------------------------------	-----------------------------

(TSC) Category			
TSC	Operational Technology Security Audit Management		
TSC Description	Manages audit and penetration testing on operational security measures		
TSC Proficiency	Level 4	Level 5	Level 6
Proficiency Description	Perform audits on operational technology security systems through penetration testing and vulnerability assessments	Lead the implementation of vulnerability assessments and penetration testing activities and identify areas of non-compliance based on audit findings	Formulate frameworks conducting penetration testing and vulnerability assessments
Knowledge	<ul style="list-style-type: none"> <li>– Application and usage of basic vulnerability assessment tools and tests</li> <li>– General process and technical requirements of penetration testing</li> <li>– Internal and external operational security standards</li> <li>– Methodologies and tools for the conduct of audit activities</li> <li>– Interpretation and analysis of audit results</li> <li>– International Electrotechnical Commission (IEC) 62443</li> <li>– International Organisation for Standardisation (ISO) 27001/19</li> </ul>	<ul style="list-style-type: none"> <li>– Organisational objectives of vulnerability assessment and penetration testing</li> <li>– Key components and methodologies in the design of operational security testing activities</li> <li>– Elements and considerations in development of compliance processes</li> <li>– Evolving statutory and regulatory standards Application and relevance of external standards to organisation's context</li> <li>– Process gap analysis for business and operational technology (OT) operations</li> </ul>	<ul style="list-style-type: none"> <li>– Design guidelines and best practices for threat modelling, vulnerability assessment, penetration tests and review</li> <li>– Process and key considerations in audit and compliance strategy development</li> <li>– Emerging trends, approaches and industry best practices in internal audit and compliance</li> <li>– Impact of business priorities and external regulations on audit strategy</li> <li>– Root cause evaluation of non-compliance in business and operational technology (OT) processes</li> </ul>

	– Regulatory guidelines on compliance		
Abilities	<ul style="list-style-type: none"> <li>– Perform technical coordination of vulnerability assessments and penetration testing according to test plan templates</li> <li>– Execute vulnerability scans on smaller systems, using basic vulnerability assessment tools and tests</li> <li>– Document the results of security assessments and tests, according to test plan guidelines</li> <li>– Identify security lapses in the system or security mechanisms, based on issues documented from vulnerability scan results</li> <li>– Record evidence of controls which are inadequate or not duly enforced</li> <li>– Conduct audit activities in line with the organisation's compliance processes and guidelines, using appropriate methodologies and tools</li> <li>– Analyse audit results and highlight identified process gaps or key</li> </ul>	<ul style="list-style-type: none"> <li>– Design security testing plan and evaluation criteria for vulnerability assessments and penetration testing activities</li> <li>– Manage implementation of vulnerability assessments and penetration testing activities, in line with organisation-wide strategy</li> <li>– Develop compliance processes in accordance with organisation's strategy and internal and external guidelines</li> <li>– Evaluate audit results to identify reasons for gaps or non-compliance in business and OT operations</li> <li>– Recommend enhancements to compliance processes to strengthen the organisation's internal controls</li> </ul>	<ul style="list-style-type: none"> <li>– Establish organisation guidelines and methodologies for the design and conduct of vulnerability assessments and penetration testing activities</li> <li>– Formulate implementation strategies for vulnerability and penetration testing activities to ensure organisation-wide consistent of information security plans</li> <li>– Authorise penetration testing activities on organisation's systems, in line with business priorities and security requirements</li> <li>– Synthesise key organisational implications from vulnerability assessment and penetration testing reports</li> <li>– Evaluate future readiness of the organisation's security posture in light of organisation's mission and the evolving technological environment</li> </ul>

	<p>instances of noncompliance</p> <ul style="list-style-type: none"> <li>– Propose improvements to existing compliance processes and measures to address major risks</li> <li>– Implement changes in the performance of audits in alignment with changes in internal compliance standards or external regulatory guidelines</li> </ul>		<ul style="list-style-type: none"> <li>– Establish audit and compliance strategy and objectives for the organisation, considering emerging trends, approaches and industry best practices</li> <li>– Oversee alignment of audit and compliance strategy with internal business requirements and priorities as well as external regulations and standards</li> <li>– Evaluate root causes and potential organisational impact or risks of non-compliance to prioritise the areas that require further enhancement</li> <li>– Endorse enhancements to critical compliance processes, to improve the robustness of organisation's internal controls</li> </ul>
Range of Application	<p>Range of application includes, but is not limited to:</p> <ul style="list-style-type: none"> <li>– Power Generation</li> <li>– Distributed Generation</li> <li>– Town Gas Plant Maintenance</li> </ul>		

Technical Skills and Competencies (TSC) Category	Operations and User Support		
TSC	Operational Technology Security Design		
TSC Description			
TSC Level	4	5	6
Proficiency Description	Implement operational technology security	Develop the operational technology	Set the strategy for the operational technology

	frameworks, standard operating procedures and risk mitigation plans for operational technology security of daily operations, research on the latest operational technology security trends	security frameworks, standard operating procedures and risk mitigation plans for operational technology security of daily operations, recommend improvements to operational technology based on research conducted	security framework, standard operating procedures and risk management for operational technology of daily operations, and establish process improvements for operational technology
Knowledge	<ul style="list-style-type: none"> <li>– Organisation operational technology security procedures</li> <li>– Implementation process and considerations for operational technology security policies and protocols</li> <li>– Types of operational technology security controls and implementation procedures</li> <li>– Techniques for assessment of processes against operational technology security standards</li> </ul>	<ul style="list-style-type: none"> <li>– Operational technology security threat analysis and system vulnerabilities</li> <li>– operational technology security policies</li> <li>– operational technology security frameworks</li> <li>– Communications of operational technology security standards</li> </ul>	<ul style="list-style-type: none"> <li>– Potential threats to organisational operational technology security</li> <li>– Emerging trends and developments in operational technology security management and practices</li> <li>– Industry standards and best practices for organisational security</li> <li>– Impact of changes in operational technology security protocols on the organisation</li> <li>– Industry best practices and benchmarks for operations security framework</li> </ul>
Abilities	<ul style="list-style-type: none"> <li>– Inspect adherence of applications and infrastructure components to operational technology security standards and baselines</li> <li>– Analyse lapses in organisational security standards or issues that may endanger</li> </ul>	<ul style="list-style-type: none"> <li>– Determine existing operational technology security risks, threats and vulnerabilities and analyse gaps in current organisational operational technology security policies</li> <li>– Develop operational technology security policies based on</li> </ul>	<ul style="list-style-type: none"> <li>– Set direction for the organisation's operational technology security policies, frameworks and protocols, in line with business requirements and the external environment</li> <li>– Endorse proposals for updates or</li> </ul>

	<p>operations security and integrity</p> <ul style="list-style-type: none"> <li>– Evaluate technologies and tools that can address operations security gaps and facilitate alignment with operations security policies</li> <li>– Introduce operational technology security controls in line with operations security policies and frameworks</li> <li>– Implement operational technology security guidelines and protocols, ensuring understanding and compliance</li> <li>– Analyse the adequacy of operational technology security controls</li> <li>– Highlight areas for improvement and propose solutions or revisions to operational technology security guidelines</li> </ul>	<p>organisation's direction, to ensure operational technology are well protected</p> <ul style="list-style-type: none"> <li>– Review improvements, updates or modifications to current operational technology security policies and practices, to address potential security gaps</li> <li>– Initiate suitable technologies, processes and tools to monitor, guide and maximise compliance with operational technology security policies</li> <li>– Drive communication of operations security policies and implementation of operational technology security protocols</li> <li>– Establish internal processes to review adequacy of operational technology systems' security controls against set benchmarks</li> </ul>	<p>enhancements to operational technology security policies</p> <ul style="list-style-type: none"> <li>– Establish benchmarks and targets for operational technology security systems operations and processes to be reviewed against</li> </ul>
Range of Application	<p>Range of application includes, but is not limited to:</p> <ul style="list-style-type: none"> <li>– Power Generation</li> <li>– Distributed Generation</li> <li>Town Gas Plant Maintenance</li> </ul>		

Although each of these competencies 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 a traditionally trained information security person could not do that.

While SkillsFuture ambitiously approaches incorporating operational technology cybersecurity into a broad variety of industries, job positions, competencies, and tasks it has not provided sufficient detail to guide specialised ICS training or education of these individuals.

#### **4.2.2 Criteria for establishing a foundation**

In order to answer the question “What is the foundation for formal preparation of industrial cybersecurity professionals?” one must establish expectations for what an appropriate foundation would include.

Incorporating the researcher’s prevailing critical paradigm, which seeks to uncover hidden assumptions, the criteria were created with a combination of two approaches. First, each document was reviewed to identify the assumptions that undergirded its creation – that is, what were the authors’ own criteria for legitimacy, and how did the authors show they met these criteria? The result of this review was a list of nine foundational criteria. Second, the researcher asked whether any other desirable criteria exist that none of the efforts/documents addressed. This resulted in the identification of two additional criteria, for a total of eleven foundational criteria. Careful consideration led the author to create for each criterion: 1) a description; 2) a rationale for inclusion; 3) key insights for use by those who seek to develop foundational curricular guidance in the future; and, 4) anticipated challenges for implementation.

##### ***4.2.2.1 Criterion 1 – Addresses industrial cybersecurity***

- **Description:** An appropriate foundation for industrial cybersecurity education and training must proclaim its coverage of this topic area. It would clearly, if not prominently, include the terms “industrial control”, “SCADA”, or “cyber-physical” security.
- **Rationale:** This criterion provides an initial point of departure for reviewing a document/effort. If the effort does not clearly include the appropriate terminology it is obviously not a candidate for direct consideration.

- Key insight: Industrial cybersecurity should be prominently displayed and not buried inaccessibly as part of a larger document.
- Anticipated challenges: None.

#### **4.2.2.2 *Criterion 2 – Differentiates industrial cybersecurity***

- Description: An appropriate foundation must affirm that unique competencies are required for industrial cybersecurity in comparison with traditional cybersecurity education and training.
- Rationale: This criterion expands Criterion 1. That industrial cybersecurity requires differentiated training and education is a cornerstone of this work, established by reasoning provided in the literature review.
- Key insight: A description of why industrial cybersecurity is different as part of an introduction establishes confidence of the individual using the curricular guidance.
- Anticipated challenges: Appropriate consideration of challenges (which this thesis summarises in the Literature Review) that extends beyond the technology and into organisational and educational culture may be challenging to fully identify and describe.

#### **4.2.2.3 *Criterion 3 – Consensus-based***

- Description: An appropriate foundation must intentionally involve diverse participants and perspectives, and ostensibly consider the full breadth of input provided. The foundational guidance would clearly explain and document the range and qualifications of its participants at each stage of its development.
- Rationale: The quality of a curricular guidance is thought to depend on a full consideration of diverse perspectives. A strong perception of the guidance's validity is nearly as important as the contents themselves.
- Key insight: A reasonably thorough description of by whom and in what way consensus was achieved, perhaps in an appendix would reinforce reader/user confidence.
- Anticipated challenges: Few organisations have access to a sufficient quantity and breadth of expertise willing to devote hard thought time to create curricular guidance.

#### **4.2.2.4 *Criterion 4 – Qualified participants***

- Description: An appropriate foundation must ensure and record the qualifications of those who participated in its creation.



- Rationale: Validity comes from people who “know what they are talking about” through both study and application.
- Key insight: A reasonably thorough description of the qualifications of key participants, and how their particular expertise was brought to bear, perhaps in an appendix would reinforce reader/user confidence.
- Anticipated Challenges: Academics working on the creation of foundational guidance may struggle to obtain find appropriately experienced collaborators, or to obtain appropriate input therefrom.

#### **4.2.2.5 Criterion 5 – Publicly available**

- Description: An appropriate foundation and supporting detail must be publicly available on an official web site.
- Rationale: For foundational educational guidance to be of use, it must be readily available for application.
- Key insight: None.
- Anticipated challenges: Funding the creation of a standard, taking credit for it, and allowing others to claim compliance with it, are concerns in a competitive educational environment.

#### **4.2.2.6 Criterion 6 – Includes knowledge**

- Description: An appropriate foundation must include a list of nouns that represent the working vocabulary of the field.
- Rationale: Inclusion of vocabulary is an absolute necessity. This expands on the first two criteria.
- Key insight: None.
- Anticipated challenges: None.

#### **4.2.2.7 Criterion 7 – Justifies knowledge**

- Description: The list of terms must include a description of why each is included – that is, each term’s relevance to the field.
- Rationale: Describing why a set of terms has been included adds depth to criterion 2 “differentiates industrial cybersecurity”, and simplifies the process of instructional design.
- Key insight: Reducing the guesswork required of non-experts should enhance the effectiveness and the adoption of the guidance.

- Anticipated challenges: Convincing explanation of why a term should be included requires deep expertise that may be difficult to obtain and then to validate.

#### **4.2.2.8 *Criterion 8 – Includes job roles***

- Description: An appropriate foundation 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, and hiring managers, the foundational guidance will link to possible position titles.
- Key insight: The creation of foundational guidance aiming to guide the creation of a real workforce must not stop at knowledge, but extend to specific roles.
- Anticipated challenges: The identification of job roles notionally marks the transition from education to training, which may fall outside the historic strength of purely academic approaches. Inconsistent use of education- and training-related terminology such as “job role” across training and education literature will require those creating a foundational guidance to clearly define terms used. Job titles and responsibilities associated with those roles vary widely across organisations.

#### **4.2.2.9 *Criterion 9 – Includes tasks***

- Description: An appropriate foundation must include a listing of tasks performed by specific job roles.
- Rationale: While job titles (Criterion 6) are a positive step, knowing the primary tasks each role performs facilitates instructional design, and enables assessment and evaluation.
- Key insight: None.
- Anticipated challenges: Perhaps more than even job roles, tasks vary across organisations. Organisations relying on the guidance should not perceive that the guidance is limiting or overly prescriptive.

#### **4.2.2.10 *Criterion 10 – Recognises sector-specific component***

- Description: An appropriate foundation should provide 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 foundation allows for sector-specific content.

- Key insight: Extensibility and a process to extend should be an intentional part of the curricular guidance effort
- Anticipated challenges: None.

#### **4.2.2.11 Criterion 11 – Provides evidence of empirical validation**

- Description: Appropriate guidance must justify that it is relevant in real life.
- Rationale: The ultimate goal of having a foundational guidance is to improve the quality and quantity of the workforce. The various components of the guidance therefore require empirical validation.
- Key insight: Developers of curricular guidance should plan to incorporate behavioral (not just cognitive) approaches.
- Anticipated challenges: Behavioral approaches require trusted relationships with qualified participants and their organisations, and are more time consuming and costly to conduct.

### **4.3 laboraResults**

Table 10 compares the cybersecurity education curricular guidance efforts identified above across the ideal criteria. A “Y” represents adequate achievement or incorporation of criteria. “P” represents existence of evidence, but inadequate performance. “N” represents no effort made. “U” represents the documentation was insufficient to discern.

*Table 10. Candidate Curricular Guidance Mapped to Identified Foundational Criteria*

Criteria	Curricular Guidance Efforts/Documents									Total Ys
	ABET	ENISA	GIAC	ISA	JTF	NIST	NSA	PNNL	SF	
<b>1. Addresses Industrial cybersecurity</b>	N	Y	Y	Y	N	N	Y	Y	Y	6
<b>2. Clearly differentiates industrial</b>	N	P	P	Y	N	N	P	N	N	1
<b>3. Consensus-based</b>	Y	Y	Y	U	Y	N	N	Y	U	5
<b>4. Qualified participants</b>	Y	Y	Y	U	Y	U	U	Y	U	5
<b>5. Publicly available</b>	Y	Y	Y	Y	Y	Y	Y	Y	Y	9
<b>6. Includes knowledge</b>	P	Y	Y	Y	Y	Y	Y	Y	Y	8
<b>7. Justifies knowledge</b>	N	N	N	N	N	N	N	N	N	0
<b>8. Includes job roles</b>	N	N	N	N	N	Y	N	Y	Y	3
<b>9. Includes tasks</b>	N	N	N	Y	N	Y	N	Y	Y	4
<b>10. Sector specific content</b>	N	N	N	N	N	N	N	Y	Y	2

Criteria	Curricular Guidance Efforts/Documents									Total Ys
	ABET	ENISA	GIAC	ISA	JTF	NIST	NSA	PNNL	SF	
<b>11. Evidence of empirical validation</b>	N	N	N	N	N	N	N	N	N	0
<b>TOTAL</b>	3.5/11	5.5/11	5.5/11	5/11	4/11	4/11	3.5/11	8/11	6/11	

## 4.4 Analysis

This section explores the results of the structured review. It includes: 1) An analysis by curricular guidance effort/document (which we call vertical due to its comparison along the vertical axis of the table); 2) an analysis by criteria (which we call horizontal due to its comparison along the horizontal axis of the table); 3) a listing of conclusions; 4) a discussion of validity.

### 4.4.1 Vertical analysis

By considering the criteria identified on a 10-point scale, where a Y earns one point, a P earns half a point, and an N or U earn 0 points, it is evident that none of the efforts meets all criteria. PNNL came closest, with an 8/11, while ABET and NSA were furthest away with 3.5/11. For insight about the reasons behind these differences, one can consider the myriad perspectives with which each group approaches the challenge.

ABET, for example, would not be expected to lead out in establishing new educational guidance documents, 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 guidance (a process-orientation). This explains the absence of roles, tasks, and sector-specific contents.

International Society of Automation worked closely with the US Department of Labour, 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.

The United States, NSA CAE Knowledge Units are used as a set of criteria to guide curriculum development at institutions seeking NSA designation as CAEs. As a project of a government agency accustomed to working in secret, it may not be surprising that little documentation about the process or individuals involved in the creation of the knowledge units is provided. The lack of detailed attention to industrial control systems may be explained by the otherwise great breadth of the document's coverage.

The NIST NICE framework addressed the daunting task of breaking down a complex career field; an emerging topic like industrial cyber could easily be overlooked.

GIAC (SANS) is a for-profit company specialising in professional bootcamp style cybersecurity trainings. Its effort relied on industry professionals, with limited input from academics. This explains its choice to closely hold the details of the process and results. As the group focuses on teaching cyber skills rather than industrial operations skills, details about the later are underrepresented. Assante's operating room analogy make sense from the perspective that everyone involved in an endeavor needs to know some of the same things. In that analogy, everyone in the room is focused on restoring the patient's health. In the case of industrial cybersecurity, the patient is foremost an industrial environment. The cybersecurity professional must understand the industrial context into which that professional is entering.

Singapore SkillsFuture was an effort of the Singaporean government. A city-state may have the luxury of collaborating closely with a small number of important utilities. This explains the focus on formalised roles and tasks, and sector-specific content, but limited inclusion of detailed cybersecurity security knowledge.

The PNNL work notably seeks to address a single domain – power systems – which seems appropriate for a U.S. Department of Energy Laboratory. As the effort was based on work from similar authors as SANS (GIAC), the effort likewise misses a description of what makes industrial cybersecurity different.

Beyond the analysis of each effort/document, one particularly salient observation is that one-third of the efforts were significantly influenced by a single individual – Mike Assante of SANS. Assante was the principal force behind both the GIAC effort (as an employee) and the PNNL effort (as a contractor); and, as mentioned above, the ENISA authors ultimately chose to fold their work in with the GIAC effort that produced the GICSP certification – which is generally considered the most-relevant industrial cybersecurity

certification today. Considered as a trio, these efforts would have reached 8.5 out of 10 criteria. The efforts excelled in their engagement of appropriate industry stakeholders.

This observation indicates the strong motivational factor that a single individual can bring to bear – particularly when a for-profit motive as expressed in the SANS/GIAC business model of training and certifying currently-employed professionals enters the equation. The lack of academic involvement in those efforts meant that the educational pathways of new professionals entering the field remained unaddressed.

The first two recommendations of the ENISA report: 1) “Obtain stakeholders’ support to advance adoption of certifications”, and 2) “Avoid commercial interests that may compromise the value of certification” relate to this exact issue. The decision of the ENISA group to hand-off their work to SANS/GIAC, may represent a vote of confidence that SANS had indeed obtained appropriate stakeholder support, but a simultaneous expression of concern about the longer-term results of such commercialisation.

#### **4.4.2 Horizontal analysis**

As we look across the ten criteria, we can see that at least one of the efforts earned a Y for all criteria except 7 and 11 – indicating that these nine criteria are reasonable and achievable. Criteria 7 and 11 require additional discussion.

##### **4.4.2.1 Criterion 7**

Criterion 7 requires that a firm foundation justify why certain knowledge should be included. This justification goes beyond the fact that supposed experts have identified the topic as important, by requiring a brief definition of each topic (not just the category), and a description of why each topic is included. In the case of industrial cybersecurity, these terms and concepts may be new to many cybersecurity instructors. The justification statement helps these instructors frame their teaching within the intended context.

This is a demanding criterion, particularly for large efforts such as the CSEC 17 and NSA CAE. It is probably more achievable for interdisciplinary content – such as the specific terminology that a cybersecurity professional needs to be able to function within an industrial environment. But even for that more limited case, none of the efforts addresses the criterion.

Several possible reasons for the lack of justification include (though are not limited to):

- It simply did not occur to the authors

- The authors used methodologies that did not allow for such an intimate level of engagement with subject matter experts
- Authors did not assemble the balance of academics and practitioners that would have brought this idea to light
- At the time of the previous efforts, the field had not yet evolved to the point where such details were readily articulable.

Regardless of the explanation for the lack of justification, its inclusion would be of clear value to instructional designers – even if that justification is incomplete or imperfect. For that reason alone, the criteria should be included.

#### **4.4.2.2 Criterion 11**

It is notable that none of the candidate guidance documents reviewed requires empirical validation. One interpretation could be that empirical validation is not necessary. While a rationale for including this criterion is provided above, it is worth noting that both the PNNL and ENISA documents emphasise the importance of a practical, hands-on component in awarding certification. Such emphasis would be deeply ironic if the authors of those documents themselves were unwilling to determine whether practitioners/participants actually *did* the things they said professionals should be able to do.

More compelling, is the interpretation that these efforts did not incorporate behavioral approaches to validation because such approaches require deeper researcher involvement, such as travel to practitioner work locations, creation of observation and interview protocols, and approval of human subjects review boards. Furthermore, behavioral approaches could open up messy questions about what methods and tools practitioners use to achieve their objectives; and, perhaps most frighteningly, the approaches could force a confrontation with the specter of determining cybersecurity effectiveness. Proceeding down this path may ultimately mean that providers of education and training would have to attempt to carefully specify the value they really provide.

Perhaps the greatest value to be garnered from behavioral approaches would not be the curricular guidance documents themselves, but the foundation they would provide for detailed discussion and robust development of instructional materials.

#### **4.4.3 Validity**

As the research paradigm for this portion of this thesis is primarily a critical perspective, and secondarily postpositivist, involving only the lens of the researcher, the key validation techniques are researcher reflexivity, and triangulation.

##### ***4.4.3.1 Researcher reflexivity***

Due to my decade of experience closely covering the threat environment to industrial control systems – in which I authored over 3,000 situational awareness and threat intelligence reports – I felt that I was quite capable of identifying educational objectives for the industrial cybersecurity program I was hired to lead at Idaho State University. However, my education coursework emphasised the importance of linking curricula to established standards, and even required me to show that linkage in curricular materials I had actually developed.

Of course, I could also see how someone newer to the field than myself would benefit from a well-written standard. I did not know, when I first set out to identify any existing standards, the breadth of approaches and results that I would find from various sources worldwide. This sharpened my appreciation for the value of a reliable, robust, easy-to-find standard. Which, my research shows did not yet exist.

In order to fully appreciate the longer-term nature of my perspective, it is necessary for me to address my relationship with Michael Assante – who was a motivational force behind three of the efforts/documents described above.

Mike joined the Idaho National Laboratory from American Electric Power shortly before I joined from Idaho State University in 2006. While at the INL, our paths crossed occasionally: he was a high-powered strategic hire eight years my senior; I was just starting my first job. Our interactions showed we had a similar outlook and related analytical mindset. Mike left the INL to become the first Chief Security Officer at the North American Electric Reliability Corporation (NERC) in Fall 2008, at about the same time another colleague – Bob Huber – and I left the INL to start Critical Intelligence.

As mentioned previously, NERC became one of Critical Intelligence’s first customers – due to Mike’s decision to purchase a subscription to our service. Bob and I knew that the travel schedule and life in Princeton, New Jersey, where NERC was based, was hard on Mike. As soon as he moved back to Idaho Falls, we met him for lunch – really to ask him to join our startup. Mike did not say “no”, but he did not say “yes” either. Instead, he agreed to serve as pro bono advisor, and if things got exciting he might join with us.



In the meantime, Mike joined SANS with the mission of developing new training and certification offerings. He joined us in renting office space on 17<sup>th</sup> street in Idaho Falls. He would come in several days each week, and had good conversations.

Mike would tell us about the educational efforts he was leading at SANS. Bob Huber was a respondent to one or two of the surveys that formed part of the PNNL SPSP effort. I literally watched Bob fill out one spreadsheet survey. It was a tedious, mind-numbing process, which we wondered might compromise the value of the results. One could not do that work for very long without a desire to rush through it.

As Critical Intelligence grew, we brought Mike on as a formal advisor, offering him phantom stock in our company. In the end, when Bob and I sold Critical Intelligence to iSIGHT Partners, were able to reward him for his service.

I worked at iSIGHT Partners for a year before it, in turn, was acquired by FireEye. I was at FireEye for almost two years before I took the job offer at Idaho State University. When I did, and word circulated among colleagues, Mike was one of the first people to call me. He said “Congratulations on your new position, Sean. I want you to know that however SANS can help you, it will. Just let me know.”

I told him “Thanks Mike. You know I’ve always looked up to you and valued your collaboration.”

It takes a new instructor about two years to fully wrap his head around things. It takes probably four years to begin feeling comfortable in the role. By then, juggling of flaming swords (playing with the professional future of your students) suddenly doesn’t seem so dangerous. As I got into my new job, and the idea for the PhD thesis got rolling, I decided to take Mike up on his offer.

Unfortunately, early in 2019, the cancer Mike had fought off in 2004 returned. During this time of hospitalisation, and later, hospice, Mike was extraordinarily welcoming. Former Secretary of the Navy, Richard Danzig, remarked at Mike’s funeral that he had never seen anyone die like Mike chose to die – meaning that he invited anyone who wanted to see him, or spend time with him, or talk with him on the phone to do so – even if it was uncomfortable or inconvenient for him and his family.

So, when I talked with Mike regarding the GIAC GICSP as referenced above, Mike was lying in a hospital bed in Seattle. At times we talked about the GICSP, at times we talked

about cancer treatment. That's why the analogy of "what everyone in the operating room needs to know" was so fitting – and so like him to create on the fly.

Mike passed away in July 2019. I attended his funeral in beautiful Driggs, Idaho – right at the base of the Grand Teton range. During the service at the Alta, Wyoming cemetery, just several miles up Ski Hill Road, I recalled one evening a couple of years before. I had purchased a home in the same neighborhood as the Assantes, and went to pay him a visit. His wife invited me in and we chatted for a few minutes. She said Mike wasn't home, and informed me of their plans to move to Alta. She said Mike's greatest fear was that his cancer would return, and he wanted to enjoy every moment he had with his children. He wanted to do that from the most majestic spot he could.

As I examine my truest thoughts and feelings, I feel inspired by Mike's commitment to the cause of protecting critical infrastructure from cyber events and incidents. The opportunity to advance that work, to build on that foundation, is exciting to me.

I don't think my relationship with Mike has unduly biased my review. I have attempted to be objective in my analysis, and if anything, when it comes to SANS/GIAC, that analysis probably comes across a bit too critical.

#### ***4.4.3.2 Triangulation***

The structured literature review presented here is valid by its diverse nature. It examines nine documents, created by differing organisations, and organisation types, relying on the input of dozens of individuals, across several different countries. All but two of the 11 foundational criteria exist in at least one of the candidate guidance documents. The other two criteria: number 7 "Justifies knowledge" and number 11 "Evidence of empirical validation" are key innovations that will be addressed later within this thesis.

#### ***4.4.3.3 Limitations***

The primary limitation of this critical review is its reliance only on English language sources. It is also possible that the research missed some formalised effort in the search process.

An alternate approach (which this work did not take) may be to work from the ground up – that is, use a comprehensive review of existing industrial control systems training and educational content from providers around the world, and systematically compare their stated learning objectives. The PNNL effort incorporated this technique.

While this approach would provide a more-granular perspective, it would have taken much longer, as existing courseware exists in larger quantities than do curricular guidance documents. It may have also been more prone to errors of omission. Other drawbacks include that course materials may not be publicly available, and course objectives may change more frequently than do intentionally developed curricular guidance documents. Finally, and perhaps most importantly, course objectives have gone through the adulterating hands of educators rather than coming directly from practicing subject matter experts. Evidence from the critical comparison shows that no firm foundation existed to guide educators in the first place.

#### **4.5 Conclusion**

From the review and analysis above, it follows that despite useful work by various groups around the globe, no ideal foundation for industrial cybersecurity education and training currently exists:

- Efforts to differentiate industrial cybersecurity from traditional cybersecurity require additional elaboration.
- Efforts to identify appropriate roles within industrial cybersecurity lack development.
- Academic efforts have not yet appropriately addressed industrial cybersecurity education and training.
- Behavioral research into industrial cybersecurity has not yet informed the creation of curricular content standards.

## **5 DIFFERENTIATED INDUSTRIAL CYBERSECURITY KNOWLEDGE**

### **5.1 Problem**

The intent of the research effort presented in this chapter (5) is to address key conclusions of the critical comparison of candidate guidance documents/efforts for industrial cybersecurity education and training, namely:

- What job basic roles exist or should exist within the field of industrial cybersecurity?
- What knowledge differentiates industrial cybersecurity from traditional cybersecurity?

### **5.2 Research Design**

A first step in research design is the selection of an appropriate technique. Techniques to address issues like those named above will naturally be based on the input of subject matter experts. Common techniques used for such input includes simple surveys, written questionnaires, interviews, and focus groups. Perhaps less common is the nominal group technique. The candidate curricular guidance documents/efforts reviewed in Chapter 4 relied on the first three of these techniques.

Simple surveys commonly allow respondents to select from a menu of choices; or, in some cases to provide short answers. While design may be challenging, they are relatively straightforward to administer and complete. They are most useful when attempting to gain insight regarding discrete, previously identified items or categories, but less effective for dealing with open-ended inquiries (Kelley, 2003).

Questionnaires often require written response. They are good for gaining insight that can be expressed concisely. They provide sound documentation, useful in validation or future study. They take longer than surveys to complete, and thus are constrained by the participants' interest level. They may limit the researcher's ability to probe the participant for additional detail (Kelley, 2003).

Interviews provide for robust interaction with the participant, but require the researcher to keep a detailed record, and appropriately code the responses, potentially introducing researcher bias. Also, even though identical initial questions can be asked, adaptivity of the interview, and other factors can produce varying results across the set of participants (Kelley, 2003).

Focus groups involve discussion relative to a research question among a small group of participants. They can provide robust interaction, and may surface perspectives the researcher

otherwise would not have anticipated. They allow for insights to come from various sources during a single session; but, they are subject to the influence of personality. Like interviews, they require creation of an accurate record, and the subsequent coding process can lead to the introduction bias (Stewart, 2007 p.117).

The nominal group technique relies on anonymous written interaction among a medium sized group of participants, which reduces the negative effects of personality, creates an accurate record, and diminishes coding bias. It allows the researcher and the participants to interact with one another for a robust treatment of the key question. Because written communication can occur among various parties simultaneously, it encourages broad participation within a relatively short timeframe. Van de Ven and Delbecq report the technique effectively elicits diverse perspectives (Van de Ven, 1974; Delbecq, 1975).

It is important to note that the results of the nominal group technique depend highly on the willingness of the participants to fully engage in writing. While writing can encourage thoughtful responses, it can also limit depth because it is slower than speaking, and depending on the number of participants, may not always result in the right question or concern being raised to the right participant. For example, participants writing to one another in real time, may ignore responses to their comments if they are simultaneously engaged in interactions with others. While a capable facilitator and well-developed nominal group technique software can help mitigate this concern, it cannot entirely overcome it. In addition, some participants may communicate more effectively verbally than in writing, blunting their contributions, and strengthening the contributions of those who are more efficient and effective in writing.

Given the pros and cons of the research methods alone, the nominal group technique was a clear choice.

The next step for using this technique is the identification of a suitable group of expert participants. In this case, participants should have experience in the fields of industrial operations, cybersecurity, and industrial cybersecurity. For the nominal group technique to work correctly, a group of about 15 participants would be ideal. Obtaining participants could be done by personal contacts, through group or industry association, or through collaboration with a single large and diverse employer, who would be interested in the results of such a project.

Due to its interest in industrial cybersecurity, the Idaho National Laboratory, which is geographically proximate to Idaho State University, would have such a group of qualified participants, and given its mission and vision would be interested in the results.

The Idaho National Laboratory is a U.S. Department of Energy Laboratory with offices in Idaho Falls, and a complex of nuclear research and development facilities in the desert west of that city. INL employs more than 100 individuals who focus exclusively on industrial cybersecurity, providing a variety of services, including industrial cybersecurity training, for its government customers. When senior INL management heard about the research project they agreed to send 14 experienced professionals from various backgrounds to participate.

Finally, the nominal group technique also requires a suitable facility (when done in-person) and specialised software. This already existed at Idaho State University.

#### ***5.2.1.1 Historic contribution to cybersecurity education standards***

Idaho State University has a deep, if often unrecognised, history of leadership in cybersecurity education and training. In the late 1980s, Dr. Corey Schou and a handful of colleagues hosted a series of workshops that produced some of the first educational materials for information security, including the 409-page “Comprehensive Information Assurance Dictionary” (Schou, 1988) and 326-page “Integrating Information Security” modules (Schou, 1989, Spafford, 2019).

Beginning in 1987, the National Security Agency (NSA) in cooperation with the Federal Information Systems Security Educators Association (FISSEA) funded an expert session at ISU with the mission of creating the first US federal government standard for information systems security education. This effort (Schou, 1993) resulted in the publication of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, published in 1998 (de Zafra).

Between 1991 and 2005, the NSA, under the guidance of W. Victor Maconachy, Michael Jacobs, and Richard Marshall – and influenced by Richard Clarke at the White House – engaged the Informatics Research Institute at ISU to host additional sessions to deepen and elaborate the original work, moving from general knowledge to specific information security roles. The output of these sessions became the National Security Telecommunications and Information Systems Security (NSTISS) – later known as the Committee on National Security Systems (CNSS) – Instructions 4011-4016. Table 11 displays the numbers and titles of these documents as well as their formal release dates. It

should be noted that documents CNSSI 4012 and 4014 replaced NSTISSI documents of the same number, and that both NSTISSI documents were dated August 1997 (Committee on National Security Systems, n.d. *Instructions*).

*Table 11. Development of National Cybersecurity Education and Training Standards*

<b>Document</b>	<b>Title</b>	<b>Study Start</b>	<b>Release Date</b>
NSTISSI 4011	National Training Standard for Information Systems Security (INFOSEC) Professionals	1991	06/20/1994
CNSSI 4012	National Information Assurance Training Standard for Senior Systems Managers	1993	06/01/2004 First Released 08/1997
CNSSI 4013	National Information Assurance Training Standard For System Administrators (SA)		03/01/2004
CNSSI 4014	Information Assurance Training Standard for Information Systems Security Officers		04/01/2004 First Released 08/1997
NSTISSI 4015	National Training Standard for Systems Certifiers		12/01/2000
CNSSI 4016	National Information Assurance Training Standard For Risk Analysts		11/01/2005

These Instructions formed the basis for training US federal employees in the field of information assurance. It seems that in order to leverage existing academic institutions to produce the information security personnel required for government agencies to fulfil their national security missions, the NSTISSC, with NSA in its role as secretariat, could not wait for traditional academic accrediting bodies, such as ABET, and opted to create its own set of curricular examples and criteria.

By demonstrating compliance with these criteria, schools could qualify for designation as a “Center of Academic Excellence (CAE)” in Information Assurance (now Cybersecurity) (Bishop, 2009; National Security Agency, n.d., *National Centers*).

### ***5.2.1.2 Simplot Decision Support Center and the nominal group technique***

The Simplot Decision Support Center (SDSC) is an in-person electronic meeting room located on the fourth floor of Idaho State University's Business Administration building. The Center, as a small, 15-seat amphitheater, was designed to implement the nominal group technique for decision making.

The technique requires synchronous deliberations be held in writing, anonymously, and in vocal silence. These criteria work to counteract dominant personalities, pre-existing political relationships, and social pressure, thereby enhancing group effectiveness. In the Center, each participant can view their own monitor, the group display at the front of the room, and the moderator. They cannot view the monitor used by other participants (Idaho State University, n.d. *Simplot*).

Doctors Corey Schou and James Frost – who have implemented the technique in the SDSC hundreds of times – empirically report that the technique places significant pressure on the moderator to carry the group through a decision-making process that achieves the objective. As such, it is important that the moderator have a strong understanding of the decision-making process, including approaches and options to give participants, know the software well, display general familiarity with the subject matter, and suspend his or her own bias. They find an assistant moderator particularly useful in simultaneously performing these tasks.

Prior to the session, the moderator reviews the objective of the session, and prepares a script of the questions the group intends to address. The moderator uses a set of techniques, such as brainstorming, nominations, rankings, and voting to guide the process.

It is important to note that the SDSC is a decision support centre. The participants themselves are not considered subjects of study, but collaborators who impart what they know to address a specific issue. Software used in the SDSC produces an anonymous log of the input and records the decisions made by the group.

### ***5.2.1.3 Session narrative***

On February 11, 2019, the primary researcher met with the session moderator, Dr. James Frost, to refine the session script. The resulting document is provided below:

#### ***5.2.1.3.1 Proposed Session Flow***

*I. Discuss What makes this field different*

*II. Brainstorm Job titles within this field*



- *Categorize titles*

### *III. Brainstorm unique ICS Knowledge used by individuals across all titles*

- *Categorize knowledge*

### *IV. Select three titles that merit immediate development*

### *V. Match Blooms taxonomic verbs to ICS knowledge*

### *IX. Brainstorm Who, outside of INL, would you recommend as a valuable contributor in a later session?*

On February 12, 2019, the INL sent 14 subject matter experts to Idaho State University to use the SDSC with the objective of creating a foundational framework for eventual development of industrial cybersecurity education and training standards.

#### *5.2.1.3.2 Participant qualifications*

Group participants sent their resumes to the author to aid in documenting their qualifications. The group's professional background included titles such as Power Plant Operator, HVAC Specialist, Field Electrician, Information Security Technology Officer, Computer Technology Analyst – SCADA, ICS, and Cybersecurity Consultant, among others. The group's former employers included Northern California Power Agency, Raytheon, National Security Agency, Virginia Transformer, El Paso Electric, and Phillips 66, among others. In total, the group reported 31 years' experience in industrial cybersecurity, 32 years in non-ICS information security, and 88 years in industrial operations.

#### *5.2.1.3.3 Session narrative*

At about 8:30 a.m. the group filed into their seats in the SDSC. Participants heard introductory comments from Dr. Corey Schou, University Professor of Informatics, ISU; and Scott Cramer, Directory of INL's Cybercore Division. The participants then introduced themselves to one another.

Dr. Frost, who served as moderator for all of the previous NSA-sponsored information assurance education and training standards development sessions, took the moderator's chair for this session. The group first engaged in a warm-up brainstorming exercise intended to stimulate mental activity relevant to the topic, and introduce them to the software with its flow of written interaction. The warm-up centred on the question, "how does industrial cybersecurity differ from standard information security?"

Following the warm-up exercise the group addressed the issue: What job roles exist in the field of industrial cybersecurity?

The group then addressed “what knowledge does an ICS security professional need to know that is not covered in standard information security?”

After lunch, the group spent a taxing session in which it mapped verbs from Bloom’s taxonomy (Bloom, 1956) to the knowledge list generated in the morning.

Data captured and produced by the software during the day is provided in Appendix C.

### **5.3 Results of the Nominal Group Session**

This section presents the results of the nominal group technique session.

#### **5.3.1 Results of Question 1**

In response to the question: “What job roles exist in the field of industrial cybersecurity?”, the group identified 81 separate job titles, which it then organised into five categories:

- Technician
- Engineer
- Analyst
- Manager
- Educator

Three titles were not easily assigned to these groups, and were set aside for future investigation: Control Systems Vendor Relations Specialist, ICS Cyber Security Intern, ICS Insurance Agent.

When asked to pick which two categories were most important to elaborate, the group chose first, Engineer, and second, Analyst.

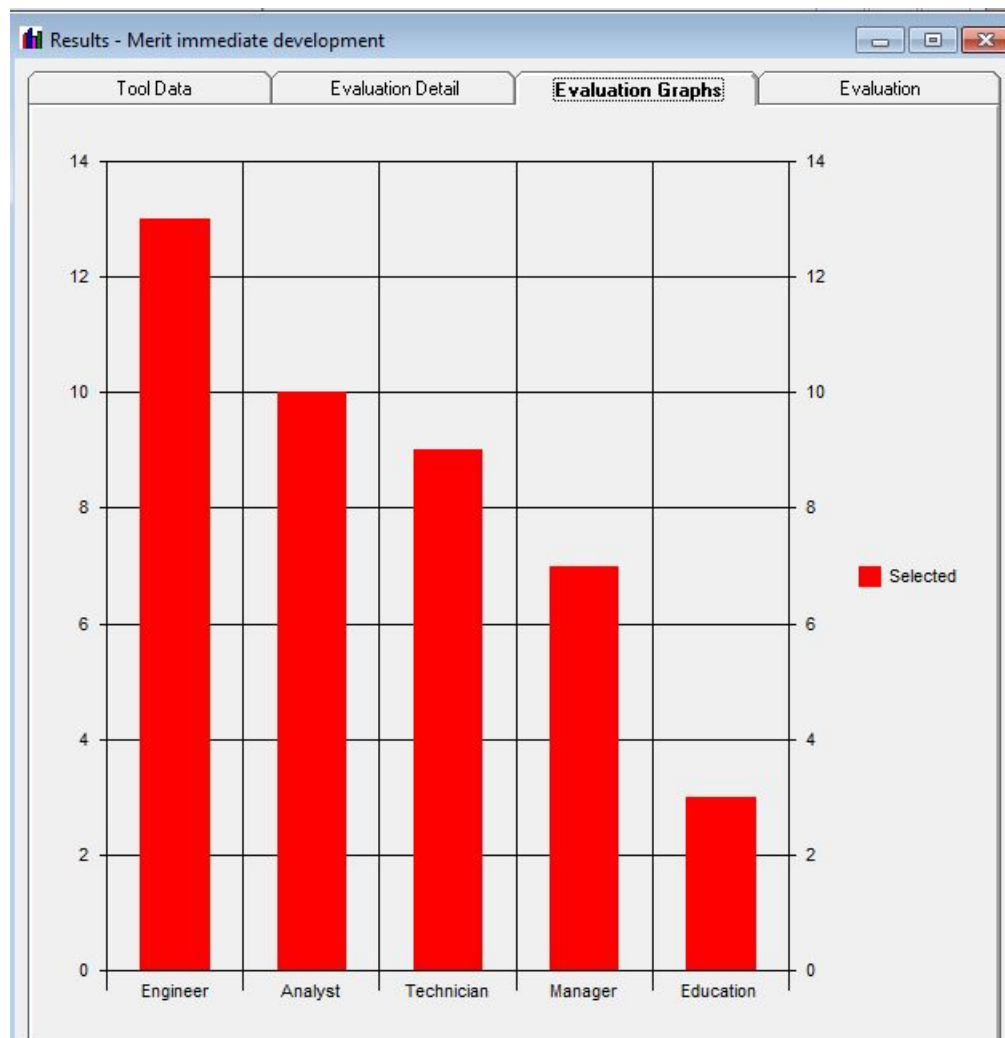


Figure 5. Selection of archetype roles for development.

### 5.3.2 Results of Question 2

In response to the question, “What knowledge does an ICS security professional need to know that is not covered in standard information security?” The group identified 86 terms and concepts, which it organised into five categories – which one can call “knowledge categories”:

- Control Knowledge
- Equipment
- Communications
- Regulations
- Instrumentation & Control

The group recognised that this final category would also exist in traditional information security, but the contents of this category would be different.

#### **5.4 Analysis**

Contemplation of the job categories identified led to calling them “archetype professional roles”. The major benefit of archetype roles is their intuitive simplicity:

- Those with limited workplace experience or domain expertise, such as a high school student or even an average citizen, may at least notionally recognize differences among a manager, an analyst, and a technician.
- The use of archetypes bypasses potential convolution associated with using security-specific duties as primary categories (which we note is the approach used by the CNSS Instructions (Committee on National Security Systems, n.d.), and the original NIST NICE framework (Newhouse, 2017).
- Reliance on these simple roles may help incorporate cybersecurity into existing positions rather than overtly promoting separate cybersecurity specialists (while leaving the door open to the latter), which also seems a significant need.
- Intuitively, five seems a manageable number of archetype roles.

Moreover, starting with roles helps alleviate the methodology-related challenge of determining who is qualified to identify and describe the types of tasks that should be completed by each role. In other words, we will more effectively create relevant task lists and descriptions by enlisting individuals who already identify with one of these roles.

One chief concern related to the archetype roles is that individuals or organisations attempting to apply them may consider them to be specifically prescriptive rather than notionally prescriptive. This misuse should be carefully avoided in order to preserve the ingenuity and flexibility of employers to meet their own workforce needs.

As mentioned above, the INL SME group identified Engineers and Analysts as the most important archetypes to elaborate. While the moderator did not ask the experts to defend this conclusion, it seems reasonable to surmise that engineers wield enormous influence on the cybersecurity of industrial environments throughout their lifecycle. It also seems reasonable that “cybersecurity analyst” is a common role-title, making it an obvious choice for achieving near-term impact.

### **5.4.1 Validity of Archetype Roles and Knowledge Categories**

As mentioned previously, the primary or preferred lens of the researcher in this case is the critical paradigm, in which the researcher seeks to “uncover hidden the hidden assumptions” (Creswell, 2000). Validity of this approach under the researcher lens calls for researcher reflexivity, collaboration, and peer debriefing. Given the limitation that nominal group technique may lack depth or favor proficient writers, deep in-person verbal collaboration would be a particularly important validation technique.

#### ***5.4.1.1 Critical paradigm.***

##### ***5.4.1.1.1 Researcher Reflexivity***

In approaching this research, I was confident that the individuals and the methods were both readily available in southeast Idaho. To convince Dr. Corey Schou at ISU, and cybersecurity leaders at INL of this opportunity, I wrote a memo expressing the results of my critical review of existing industrial cybersecurity education and training standards. Both Dr. Schou and Zachary Tudor readily agreed – seeing the evidence that confirmed what they may have previously intuited. I asked the INL to provide up to 15 individuals with a broad range of experience in industrial control environments and cybersecurity.

Of those the INL identified, I had significant pre-existing relationships with three: Dr. Shane Stailey, Scott Anderson, and Curtis St. Michel. I will address each of these in detail.

Dr. Shane Stailey is the Industrial Control Systems Cybersecurity Training Opportunities and Strategy Lead for the INL. Shane, like myself, holds a joint appointment between the INL and ISU. His work has focused on workforce development topics from a strategic point of view. When Shane learned of my work, he was naturally interested in participating. We met for lunch several times and discussed how identifying a core set of standards would be useful in his efforts to help employers chart the developmental pathway for their employees.

Scott Anderson was an instrumentation and control technician working in INL’s nuclear energy facilities. Scott was a previous graduate of ISU’s Instrumentation Engineering Technology associate degree program. He had worked for Phillips 66 as a pipeline instrumentation technician for several years, then taken a job at the INL. Scott was one of the first students to graduate from my industrial cybersecurity degree program. As such, he was especially interested to ensure that the program was successful over the longer term. After

completing the program, he transferred from a facilities-oriented job to a cybersecurity-oriented job at the INL.

Curtis St. Michel is an extraordinarily passionate engineer with decades of experience. He is noted for his work, together with Michael Assante, to establish the Consequence Driven Cyber Informed Engineering (CCE) methodology to set an upper boundary on the consequences of cyberattacks on critical infrastructure industrial control systems (LocalNews8, 2019; Idaho National Laboratory, 2018).

Knowing the background of these three individuals within the group increased my confidence in the quality of the perspective output.

#### *5.4.1.1.2 Collaboration*

In addition to identifying the key questions, designing the flow together with the session moderator, and securing the participants and facility, I joined the nominal group technique session as a collaborator. Such participation is consistent with my prevailing critical paradigm to the research. While that collaboration is a validation technique, it could potentially introduce bias. As I reflect on my contribution to the results, I believe I was able to push the collaborators to see alternate viewpoints, and I had a strong influence on the topics beneath the knowledge categories. On the other hand, I don't think my absence would have changed the groupings of job roles.

The next step in validation was to review the results with the most trusted participants. This is a hybrid between the validation technique of Collaboration and Peer Debriefing. I viewed this as appropriate because I consider true experts in the field of industrial cybersecurity difficult to come by.

I consider St. Michel one of those experts. St. Michel and I discussed the grouping of roles, and were mostly satisfied. But, St. Michel pointed out that in his mind, there was a key distinction between an analyst and a researcher. A review of the groupings showed we had treated them together. Moreover, he asserted, and I agreed, that it did not make much sense to work on the educator role until we had "the rest of this stuff figured out".

I have historically considered an analyst to be very similar to a researcher in terms of their professional responsibilities. This was a reasonable bias to develop through working as an analyst for more than a decade. But, I was prevailed upon to agree that a researcher is focused more on what is new and unknown, where an analyst deals more with gathering and synthesising existing information – and that while they involve some similar approaches,

there is indeed a fundamental difference. As a result, we inserted “researcher” and moved “educator” to the list of items for possible later consideration.

In terms of the knowledge produced, St. Michel also expressed particular concern that the use of the word “control” in the heading of two categories could cause confusion, even if an appropriate description could be crafted. St. Michel proposed replacing the title “Control Knowledge” with the title “Industrial Processes & Operations”. I thought this was a wise recommendation and made the change.

#### *5.4.1.1.3 Additional reflexivity and collaboration*

Later reflexivity on these results within the context of the critical literature review caused me to recognise that we had categorised safety as a topic beneath what was now “Industrial Processes & Operations”; but, that because of its role as an essential differentiator between information systems and industrial control systems, and the role these titles would play on later curricula development, it should be its own category. St. Michel agreed.

As a final note, while the process of mapping terms from Bloom’s taxonomy to the knowledge for the engineer role which we completed in the nominal group technique sessions mirrored that used in NSA sessions to create the 4011-4016, the expert participants expressed concerns over possible incompleteness of the knowledge list produced, its unclear connection to cybersecurity tasks, and the monotony of producing the mapping. In light of these concerns, I determined to explore alternate methodologies for correlating knowledge to roles – which will be discussed in chapter 8.

#### *5.4.1.2 Postpositivist validity*

As described previously, the secondary researcher paradigm is postpositivist. Under this paradigm, key techniques of audit trail, member checking, and triangulation help assure the validity of the results.

##### *5.4.1.2.1 Audit trail*

The audit trail helps ensure validity through the lens of the reviewer. In this case, the effort started with careful consideration of the questions the group would address, used an experienced moderator and assistant, and employed a facility and software known to have been used to create national-level cybersecurity education and training standards in the past. Moreover, the data acquired/produced through this method is available in Appendix C for further review.

#### 5.4.1.2.2 Member checking

Member checking – which is participant review and approval of the results – helps ensure validity through the lens of the study participants. The nominal group technique by nature incorporates an element of member checking – because the group came to its own consensus regarding both professional role identification and knowledge category identification. In this case, the breadth of the participants previous experience is particularly notable.

#### 5.4.1.2.3 Triangulation

Triangulation – which involves comparison of research results with external data points – helps ensure validity through the lens of the researcher. In this case, a significant external data point is provided by Conklin, who used nearly identical archetype roles to describe the relationship between training and education in cybersecurity (Conklin, 2014).

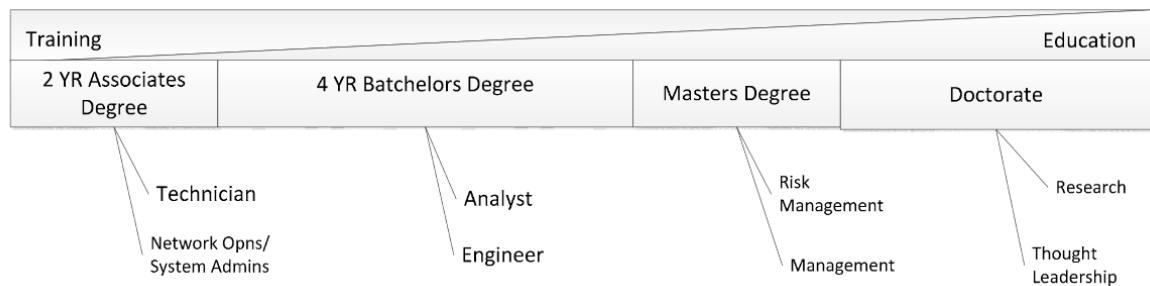


Figure 6. Conklin (2014) comparison of training and education using archetype role terminology.

## 5.5 Conclusion

The methods employed in this effort left us with five archetype roles and six knowledge categories – summarised below:

### 5.5.1 Archetype roles

- Technician
- Engineer
- Analyst
- Researcher
- Manager

### 5.5.2 Knowledge categories

- Industrial processes and operations
- Instrumentation and control
- Equipment under control
- Industrial communications
- Safety
- Regulation and guidance





## **6 INDUSTRIAL CYBERSECURITY SPECIFIC KNOWLEDGE ITEMS**

### **6.1 Problem**

Once the knowledge topic areas had been enumerated, as described in Chapter 5, the next question to address became: What specific content should fall into each of the topic areas?

The question is among the most significant of the research effort because it is not a theoretic framework dealing with generalities, but begins to represent what students or trainees will actually be taught. This drives what instructional equipment will be procured, and what instructional methods will be chosen. In short, the answer to this question will significantly affect student learning.

### **6.2 Research design**

The first step in research design is selection of an appropriate technique. In order to select a technique, one should characterise the general research question. In this case, the question, “what specific content should fall into each of the topic areas?”, is not essentially open-ended, creative, or looking for new insight. Instead, it involves identifying a relevant body of knowledge and selecting which items from that body meaningfully fall within categories identified in the previous stage of research (see Chapter 5).

As the question is not open-ended, interviews and focus groups are generally not an ideal fit. A survey would be a good fit assuming the participants were appropriately qualified, and allowed the participants to choose among options; however, the options from which the participants could choose must be identified in the first place. One perceived challenge would be maintaining an appropriate level of detail for content within each topic area. For example, a topic of PLC seems reasonable, but should greater details related to the PLC, such as architecture, form-factor, operating system, programming languages, and other device titles also be specified?

Given the researcher’s guiding pragmatic critical paradigm in addressing the key question of this thesis, the simplest approach is to allow the researcher to draw on his own expertise by 1) reviewing the categories and items suggested by the nominal group technique session; 2) suggesting items to be covered based on previous professional experience, documenting the researcher’s potential biases and reasoning; and 3) triangulating the results with literature review.

### 6.3 Results

Based on this approach, the researcher identified the topics shown in parentheses for each of the categories that resulted from the effort described in Chapter 5:

- Industrial processes and operations (industry sectors, professional roles and responsibilities in industrial environments, organisational roles, engineering diagrams, process types, industrial lifecycles)
- 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, transmitter signals, fieldbuses)
- Safety (electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented functions, lock-out tag-out, safe work procedures, common failure modes for equipment under control)
- Regulation and guidance (presidential/executive orders, ISA/IEC 62443, NIST SP 800-82 R2, NERC CIP)
- Common weaknesses (indefensible network architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, third-party access, unverified supply chain)
- Events and incidents (DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, Taum Sauk Dam, DC Metro Red Line, San Bruno)
- Defensive technologies and approaches (firewalls, data diodes, process data correlation, ICS network monitoring, cyber-informed engineering, process hazards assessment-based approaches, cyber-physical fail-safes, awareness and training for ICS-related personnel)

### 6.4 Analysis

Reflexivity on the knowledge categories identified by the nominal group technique discussed in Chapter 5 led the researcher to recognise that the categories lacked a way to

bridge the content “not normally covered in traditional cybersecurity” with what normally would be included.

After considering the significance of criterion 7 “justifies knowledge” from the critical review of candidate industrial cybersecurity education and training documents/efforts (discussed in Chapter 4), the researcher determined this bridge should include a description and rationale for each of the knowledge categories and its contents – which is provided below.

After considering the researcher’s own experience working as an industrial cybersecurity threat analyst, and his experience as an industrial cybersecurity instructor, the researcher determined that the bridge should also include three additional categories:

1. Common vulnerabilities
2. Defensive technologies and approaches
3. Events and incidents

The sections below (6.4.1 to 6.4.9) provide a general description of and justification for each of the knowledge categories and its contents.

#### **6.4.1 Industrial processes and operations**

Industrial processes and operations are the bigger-picture concepts that define the “industrial” aspect of industrial cybersecurity.

##### ***6.4.1.1 Industry sectors***

These are the types of services provided by organisations that operate industrial control systems. These include, but are not limited to electric power, oil & natural gas, water & wastewater, manufacturing, building automation, and food & agriculture. These do not necessarily have to align to the US Department of Homeland Security listing of critical infrastructures. They are essentially a categorisation that allows one to express the type of good or service provided. Students need to be able to think in terms of sectors, so they might express consequences and possible attacker reasoning, as well as to consider applicable policy and governance paradigms.

##### ***6.4.1.2 Professional roles and responsibilities in industrial environments***

These are the types of professionals one will encounter working in an industrial setting. At a minimum they include the archetype roles of technician, engineer, analyst, manager, and researcher – both within and without of the cybersecurity context.

A student or trainee seeking to work in or with industrial control systems should be familiar with the other individuals they will encounter there, including the types of things they do and why those things are necessary. This encourages not only successful interpersonal interaction with these parties, but also fosters detailed thoughts about the applicability of security controls. Among the most important concepts these professionals must collaborate to answer is whether an incident was caused by a physical failure or a cyber-attack.

#### **6.4.1.3 *Organisational roles***

Organisational roles refer to the functions performed by different companies relative to an industrial control system. These include, but are not limited to the asset owner, engineering firms, control systems vendors, communications providers, control systems integrators, operations and maintenance firms.

A security professional who does not recognise that entirely separate companies make choices that affect the security of an industrial control system or critical infrastructure is ill-prepared to address the associated complexities, or work with counterparts from those entities.

#### **6.4.1.4 *Engineering diagrams***

Diagrams are models of how a system operates. They are among the most useful and efficient ways to communicate essential details. Process flow diagrams, piping and instrumentation diagrams (P&IDs), facility blueprints, and network diagrams together provide key details about a facility that are useful to a variety of security professionals.

The inability to understand these diagrams puts an individual at severe disadvantage in comparison with an attacker who can read them. Professionals who reach high levels of proficiency understanding diagrams can quickly spot areas of potential weakness or attractiveness to attackers. Understanding this key point helps defenders recognise that these documents are of high value and must be appropriately protected.

#### **6.4.1.5 *Process types***

Process types refers to the industrial processes carried out within a facility. Examples include but are not limited to heat exchange, motor control, flow control, motion control, electricity generation & distribution. Process types will also address the continuum of discrete vs. continuous processes and their implications. Process types are in some cases related to industry sectors, but can also be found across sectors.

Industrial cybersecurity professionals who understand the core concepts behind given process types can recognise and describe specific physical consequences associated with potential cybersecurity events and incidents. They can then apply elements of that understanding to other industrial environments that employ similar processes. This allows them to interact confidently with industrial operations professionals.

#### **6.4.1.6 *Industrial lifecycles***

An industrial lifecycle is a description of how an entity, be it a product, an industrial control system, or a facility, pass through stages of design, specification and procurement, build, operation & maintenance, and dissolution during its existence.

While cybersecurity professionals may be familiar with the concepts of systems development lifecycle, software development lifecycle, or secure development lifecycle, they may not recognise similar lifecycles that extend to the facility in which a good or service is produced, the good or service itself, and the control systems used within the facility to produce the good. Recognition of these alternate lifecycles allows defenders to more comprehensively examine the opportunities available to attackers with long-term planning horizons. Such recognition emphasises the complexity of the security challenge, and enables the security professional to contribute to the creation and implementation of early warning systems and other mitigations.

### **6.4.2 Instrumentation and control**

The Instrumentation and Control category deals with the elements that compose the actual control system – that is, the system that controls the industrial process.

#### **6.4.2.1 *Sensing elements and transmitters***

A sensing element is a device that takes a reading of a value at a (ideally, an appropriate) location within a process. This can be, but is not limited to, temperature, pressure, level and flow. These sensors operate on a variety of principles. Sensing elements are commonly integrated into transmitters, which convert the measured value to a human consumable value, which it transmits over an electronic signal (known as a process input) to the programmable control device. The signal sent in some cases depends on the calibration and scaling of the transmitter – which is frequently accomplished handheld calibrator.

Sensor values form the piece of information on which process control decisions are made. As such, accurate sensor values are fundamental to safe and reliable system operation. A security professional who does not understand the importance of the sensor/transmitter and

how the values it produces are used by the control system is not prepared to prescribe ways to safeguard the process. The micro-processor-based capabilities being implemented into sensors/transmitters make them an increasingly attractive target to attackers.

#### **6.4.2.2 Control devices**

A control device is a way in which detection of a certain condition results in a particular output. These devices can generally be classified as mechanical, electromechanical, and intelligent (programmable). An example of a mechanical control device can be the float mechanism in a toilet tank. An example of electromechanical control can be an electromechanical “ice cube” relay. An example of an intelligent control device can be a PLC.

The ability to distinguish the type of control used, and especially the difference between an intelligent control and non-intelligent control mechanism a key skill for characterising the potential impact of cyberattacks. The ability to conceive of effective mechanical control mechanisms at key locations due to the inherent security weaknesses of intelligent devices is among the most important industrial cybersecurity engineering abilities.

#### **6.4.2.3 Programmable control devices**

A programmable control device is the brain – the decision-making mechanism – of the industrial process. It may accept a variety of input types (provided by a transmitter), making decisions based on the values, and sending commands to output devices such as motors and positioners depending on the input value. Programmable devices normally accept control logic – the rules that govern the decision, and a set point or points – the sensor values that the system seeks to maintain. They rely on a variety of operating systems, including embedded or real-time versions, but can also be built on a common Windows OS. Programmable control devices include but are not limited to residential thermostats, PLCs and protective relays. These commonly connect to a variety of other devices within a control system network.

To the industrial cybersecurity professional, programmable control devices form the heart of the focus as they are the bridge between the information system world and the process control world. Understanding how these devices work, including their inherent limitations is of pivotal importance as the industrial cybersecurity professional seeks to safely and securely get data to and from these devices.

#### **6.4.2.4 Control paradigms**

A control paradigm refers to the theory that guides the way an industrial control system is designed to meet the needs of the process it controls. Key concepts include, but are not limited to proportional, integral, derivative, advanced process control, and feed-forward. Additional concepts include error, dead-band, and lag time.

While not every industrial cybersecurity professional is expected to master control systems theory, these concepts inform an understanding of ways in which the process can be placed in a dangerous state via cyber-attack.

#### **6.4.2.5 Programming methods**

Programming methods refers to the language by which an engineer or technician creates the logic – the decision-making rules – that govern the behavior of the programmable control device. These methods include, but are not limited to ladder logic, function block, and structured text. These methods are available through programming software that does not rely on the controller itself, but on an engineering computer. The logic is transferred from the engineering computer to the programmable control device using a communications medium of some sort.

An industrial cybersecurity professional does not necessarily need to be proficient at creating PLC logic. However, the awareness that re-programming a device is a viable attack technique is an essential bit of knowledge that must inform the creation and implementation of defensive measures. Industrial cybersecurity professionals will also find it useful to understand the capabilities of the programming environment and the way in which the programming software interacts with the programmable control device in order to accurately characterise vulnerabilities. Some professionals must know how to review logic written in various methods in order to identify dangerous conditions – intentional and incidental.

#### **6.4.2.6 Process variables and set points**

The actual reading of a variable used in making a control decision is the process variable. This may be, but is not limited to, a temperature (such as degrees centigrade), pressure (such as milligrams of mercury), level (such as inches) or flow (such as liters per minute). A transmitter may scale this value to a continuous electronic signal as an input to the programmable control device.

The programmable control device frequently compares this value with the desired set point – the point at which the process should be maintained for optimal operation.



An industrial cybersecurity professional who is not prepared to recognise the meaning of the terms “process variable” and “set point” is not prepared to discuss details with other industrial professionals. Likewise, if units of measure and conversions are unfamiliar, such as professional will have a difficult time comprehending or expressing scope or impact of an incident. Similarly, if the relationship between the process variable and transmitter scaling are unrecognised, an entire attack technique may be ignored.

#### **6.4.2.7 *Data acquisition***

Data acquisition refers to acquiring sensor data for more detailed decision making than can be done by a PLC. This data can go generally to two locations: to the process operator via an operator interface screen; and/or to a specialised database that is used to conduct advanced analysis. If the data goes to the process operator, it may trigger an alert, which requires the operator to take a manual action, such as to shut down the process, or call a technician to examine the situation in person. If the data goes into a specialised database, it may trigger someone other than the process operator to take an action. For example, vibration data on a piece of rotating equipment may be used to schedule preventative maintenance; or, fill level on an ingredient bin could be communicated directly to the supplier of that ingredient, which would then schedule a new shipment.

An industrial cybersecurity professional who does not grasp the meaning of “data acquisition” will be at a loss when dealing with process operators or plant managers. That professional is unprepared to think about ways data currently being gathered by the system could be leveraged for security purposes, or ways to add additional data of security value to existing databases. Finally, that professional will not recognise the value that data may have to attackers.

#### **6.4.2.8 *Supervisory control***

Supervisory control normally refers to the human operators who oversee all the processes at an entire facility. Supervisory control and data acquisition systems are often combined under the umbrella acronym “SCADA”. A programmable control device is not capable of dealing with all potential situations. Hence a process operator, or human in the loop, is needed to supervise the entire system. Operators are trained to understand how the system normally operates and what to do when the system operates abnormally.

Unanticipated events may trigger alarms to appear on the operator’s screen. From their SCADA human machine interface (HMI) screen, the operator can interact with various

parts of the process via point and click commands. Process operators are typically present in the control room any time the process within the facility is operational. They rely on what the screen shows them to make decisions.

Due to the capabilities of the SCADA software to issue commands to many parts of the process, industrial cybersecurity professionals must recognise that such software is a high value target to attackers. Industrial cybersecurity professionals will want to ensure safeguards are in place to detect and mitigate man-in-the-middle attacks against this software. They will want to ensure process operators receive specialised cybersecurity training and participate in cybersecurity incident response exercises.

#### **6.4.2.9 Alarms**

In the context of industrial processes, there are several meanings of the word “alarm”. To the operator at the SCADA HMI interface, an alarm is a message that requests the operator’s immediate attention. For example, a high pressure or high-high pressure reading may trigger an alarm on the interface.

A second meaning of alarm may refer to a hazard alarm system within a facility. This may involve flashing lights of various colors, bells or rings of various frequencies, or annunciators.

Significant damage can result from both false positive alarms and alarms that fail to sound/display. Because alarm systems are frequently connected to computerised resources, they are potentially subject to abuse, and must be considered by industrial cybersecurity professionals.

#### **6.4.2.10 Engineering laptops/workstations**

The phrase “engineering laptops and workstations” refers to the computers that are used to design and build the software elements of the industrial control system. These computers create the SCADA/HMI display. They can generally interact with that display after it is programmed. They are used to write the control logic that is pushed to the programmable logic devices. They may be used to create the process historian and interact therewith. Technicians may use these computers to download logs from various devices.

The specialised software on these devices and their role in designing and controlling the system make them, the information on them, and individuals who regularly use them among the highest value targets in an industrial control setting. An industrial cybersecurity professional must recognise that protecting these devices is of utmost priority.

#### ***6.4.2.11 Configurator/calibrator device***

A configurator is commonly a hand-held device used by an instrumentation technician to ensure a sensor or transmitter is calibrated or configured correctly. In some cases, laptops can function as configurators. In other cases, data is downloaded from configurator onto a laptop.

Configurators are an often-overlooked piece of equipment because it may only be connected to the network on occasion or not at all. As these devices continue their technological evolution, they will more commonly connect to networks. They represent a valuable hinge-point for the distribution of malicious code.

#### ***6.4.2.12 Data historians***

The data historian is a specialised database to collect, analyse, and visualise data about the industrial process under control. Historians can contain a wide range of data useful to individuals with industrial operations roles, and business management roles. As such, these historians frequently provide a bridge from the industrial control network to the enterprise business network.

Industrial cybersecurity professionals should be aware of the risks that attend historians due to the way they may connect across networks. They should also be familiar with leading historian software, in order to accurately characterise disclosed vulnerabilities. Emerging cloud-based paradigms may have significant security implications. Data contained within historians may be valuable to industry competitors. In addition, historians may provide a useful resource for finding security related details or managing security data.

### **6.4.3 Equipment under control**

Equipment Under Control refers to the equipment actuated by the control system. Commands to control this equipment are the outputs of the programmable control devices.

#### ***6.4.3.1 Generators***

Generators create the flow of electrons down a conductor. Stated in a simplified form, this is done by spinning a magnet within coils of a conductor. When connected to a mechanism for transmission and distribution, this electric energy is then available to do work. A control system can turn a generator on or off by controlling relays. The generator in turn can be used to power additional processes with their own control systems. On-site

generators (of various sizes) are used to provide at least backup power to nearly every industrial facility.

An industrial cybersecurity professional who does not understand the basic principles of electricity generation is not prepared to consider the most fundamental resource on which the facility relies.

#### **6.4.3.2 *Electric motors***

Electric motors perform the inverse task of generators, taking the electrons flowing down the wire and turning them back in to kinetic energy – frequently in the form of a rotating shaft. As such, motors are the key piece of machinery in any industrial facility. These are almost always controlled from a group of panels called motor control centre.

An industrial cybersecurity professional who does not recognise the basics of how electric motors work, including ways in which they could be turned off, damaged or destroyed, and the ways they are connected to information systems, is not prepared to defend that facility.

#### **6.4.3.3 *Pumps***

Pumps are connected to a motor and provide the primary method whereby fluids are moved as part of an industrial process. Various types of pumps exist, which are chosen according to their advantages and disadvantages to match a given application.

An industrial cybersecurity professional should recognise the physical failure modes associated with pumps and the fluids they move in order to identify and describe impacts that cyberattacks may attempt to achieve. Examples include but are not limited to cavitation and water hammer.

#### **6.4.3.4 *Compressors***

Compressors are generally connected to motors and provide the primary method whereby gasses are moved as part of an industrial process. Various types of compressors exist, which are chosen according to their advantages and disadvantages to match a given application. Compressed gasses may be stored in vessels or flow through tubes and pipes.

An industrial cybersecurity professional should recognise the physical failure modes associated with compressors and the gasses they move in order to identify and describe impacts that cyberattacks may attempt to achieve. Examples include but are not limited to overpressure and under-pressure.

#### **6.4.3.5 Valves**

Valves regulate the flow of gas or liquid within a pipe. Numerous types of valves exist, which include, but are not limited to ball, butterfly, gate, globe, and solenoid. The valve type is chosen based on its characteristics for a specific application. Valves are connected to manually, mechanically, pneumatically, or electromechanically controlled positioners. Valve positions are common outputs in industrial control applications.

Industrial cybersecurity professionals should understand the significant safety implications of valves, as their positions can be manipulated from the PLC. Of particular concern is the ability to control primary and safety valves simultaneously which would put a system in an unsafe state.

#### **6.4.3.6 Relays and switches**

Relays are the essential electrically controlled on-off device. They determine the position of a switch that can make or break an electrical circuit. Relay position is a common output in industrial control applications. More complex control programs use relay positions as inputs.

Industrial cybersecurity professionals should recognise what different on-off signals control. This is determined by the physical wiring and the logic within a programmable control device. Of particular concern is the ability to control primary and safety relays simultaneously, putting the system into an unsafe state.

#### **6.4.3.7 Transformers and regulators**

Transformers alter the voltage of electricity for safe use by equipment, ranging from heavy, industrial motors, to sensitive electronics. Where voltage is the electromotive force, a mismatch between required and supplied voltage can quickly damage and even destroy equipment.

Industrial cybersecurity professionals must recognise that changes of voltage or current can cause foreseeable and un-foreseeable consequences, and is of enormous concern when it can be controlled by software, such as in tap changes for high voltages, and in regulators for lower voltages.

#### **6.4.3.8 Breakers**

A breaker is the moving part that can open or close a circuit. Breakers are often associated with system protection and human safety. These are found in all industrial

facilities that require electricity. They are found in electrical substations to switch feeders or isolate transformers.

An industrial cybersecurity professional must understand the key safety and protection role provided by breakers – especially when these can be actuated via software, as lives depend on their working correctly.

#### **6.4.3.9 *Variable frequency drives (VFDs)***

As a relatively simple, physics-based machine, an electric motor is normally energised or it is not. That is to say, that it is converting electricity to rotational force or it is not. A variable frequency drive (VFD) alters the characteristics of the incoming electricity in order to control the speed of the motor. This allows for a more efficient use of electricity, and prolongs motor life.

VFDs are frequently connected to programmable control devices, and are often programmable by themselves. Some have their own network connections. These facts make them a high consequence target for cyberattack.

### **6.4.4 Industrial communications**

Industrial communications refers to the methods of communicating information within industrial environments. While communications are common to all networks, industrial environments have several distinguishing attributes.

#### **6.4.4.1 *Reference architectures***

A reference architecture is a standard way of describing network design within industrial environments. Common reference architectures include the Purdue Enterprise Reference Architecture, the Rockwell Automation Converged Plantwide Ethernet Model, and the ISA Zones and Conduits model. Additional models may be forthcoming. Cloud-oriented architectures are transforming the relevance of these models – particularly from a cybersecurity perspective.

Industrial cybersecurity professionals should be familiar with these architectures in order to accurately characterise vulnerabilities and communicate clearly with other professionals functioning within the industrial environment.

#### **6.4.4.2 *Industrial communications protocols***

Industrial communications protocols are the standardised ways that elements within the industrial environment, such as sensors, actuators, programmable control devices, engineering lap tops, process historians communicate with one another. These protocols may

vary by industry, process type, and geography. Different protocols frequently correspond with different locations within reference architectures. Examples include but are not limited to HART, Foundation Fieldbus, Modbus, DNP3, EtherNet/IP, S7 Comm, Profinet, OPC, OPC UA.

The lack of authentication support in many of these protocols represents one of the most fundamental vulnerabilities within industrial control environments, which, in many cases, allows any device on the network to change set points or alter control logic. An industrial cybersecurity professional must be acutely aware of this weakness.

#### **6.4.4.3 *Transmitter signals***

Transmitter signals refers to the electronic signals produced by a transmitter that corresponds to a certain value for the control variable. In other words, it is the way the programmable logic device determines the temperature, pressure, level, flow, or other value sent to it by the transmitter. This is commonly, though not exclusively, a 4-20mA value.

Because the values communicated over these signals are the basis for decision making within industrial environments, industrial cybersecurity professionals must assure their accuracy and integrity in order to avoid undesired physical consequences.

#### **6.4.4.4 *Fieldbuses***

Fieldbuses are a digital way for communicating control values and other diagnostic information from a transmitter to the programmable logic device or configurator device. Examples include, but are not limited to HART, Foundation Fieldbus, and Profibus. Information from these fieldbuses may be mapped onto TCP/IP protocols.

Like transmitter signals, fieldbus communications are used by programmable logic devices to make decisions that result in outputs. As such, manipulation of the communications could result in physical damage. Vulnerabilities have been discovered in the way these communications work, and hardware attack devices have been designed to exploit them.

#### **6.4.5 *Safety***

Safety refers to the preservation of life and health of humans. This can be employees, contractors, and the public. In a broader sense, safety can also include avoiding damage to a product, to the equipment and the facility used to produce the product, and the surrounding environment. This is a core differentiator between an industrial control system and an information system.

Electrical safety refers to the ability to avoid damage and injury due to electricity. Any industrial cybersecurity professional who will be on the plant floor – tracing cables, opening control enclosures, deploying security technologies, or connecting equipment should have a basic understanding of electrical safety.

Personal protective equipment (PPE) refers to the clothing or gear worn by industrial personnel in safe performance of their duties. Industrial facilities include a variety of hazardous areas. Simply entering the building or complex frequently requires proper use of PPE. This may include, but is not limited to specifying the material of which clothing and underclothing are made, requiring outer clothing such as a smock, specialised footwear, eye and ear protection, gloves, and helmets. Specialised environments require specialised PPE, which may include but is not limited to a climbing harness, life jacket, or hazardous materials suit.

Industrial cybersecurity professionals entering these environments to perform tasks such as tracing cables, conducting inventories of control system devices, placing or directing the placement of video cameras or other security sensors, opening control enclosures, deploying firewalls or network monitoring hardware must understand and be fully committed to the use of PPE.

#### ***6.4.5.1 Safety/hazards assessment***

“Safety/hazards assessment” refers to the process by which potential dangers are identified and plans are created to ensure safe work performance. Conditions in an industrial facility are constantly changing, and potentially subject to drastic change.

Personnel performing security related tasks within the industrial environment must be familiar with reading safety plans that have resulted from hazards assessments, and have develop a critical eye to identify new and emerging hazards. The safety hazards assessments themselves are valuable security documents in that they detail the conditions the system should not permit, and should be protected accordingly.

#### ***6.4.5.2 Safe work procedures***

“Safe work procedures” describes the way specific work is to be done within an industrial environment that minimises the chance of harm to personnel – but also extends to product, equipment, and the environment. These work procedures are designed beforehand to ensure their effectiveness and simplify their performance. They include a description of the



work to be performed, the steps that should be taken and the protective equipment that should be used.

An industrial cybersecurity professional working within an industrial environment should be familiar with the location the standard operating procedures are stored. They may need to create procedures for security-related tasks that do not yet exist. They must be dedicated to strictly following the procedures. Of particular importance is the principle of safety supervision when cybersecurity personnel, who may be less accustomed to being within the industrial environment enter that environment.

#### ***6.4.5.3 Safety instrumented functions/special protection systems***

Safety instrumented functions are the automated systems dedicated to the specialised purpose of ensuring safety of personnel, but naturally extends to preserving the product, equipment and the environment. These systems prevent the simultaneous occurrence of dangerous conditions within the industrial process. For example, safety valves may be placed next to process control valves. If the process control valve or its controlling communication should fail, the safety valve would take over a critical task. Specialised protection systems are similar, but their task is geared towards preventing physical damage of critical equipment such as generators, motors, and transformers.

Specialised safety and protective equipment are of utmost importance. The designs of these safety systems should be treated as privileged information. Dependencies of their operation on the same networks as the basic process control systems should be carefully considered and avoided where possible to ensure common points of compromise and failure do not exist. Access to these systems must be closely controlled and monitored.

#### ***6.4.5.4 Lock-out tag-out***

Lock-out tag-out refers to the process of removing equipment from service. This is a frequent practice when maintaining equipment within an industrial environment.

Any cybersecurity professional entering an industrial environment, and opening control enclosures or control panels to deploy monitoring solutions or other security controls must be familiar with proper lock-out tag-out procedures. This will require coordination with maintenance personnel, and includes checking for proper lock-out tag-out prior to performing work, followed by proper reporting completion of work before the tags can be removed and the system re-energised.

#### **6.4.5.5 Failure modes**

Failure modes refers to the process of identifying and describing ways in which an activity or product can fail. Some of these may be classified into categories that correspond to types of processes or equipment – these are common failure modes.

The more frequent incorporation of microprocessors and network interfaces into industrial environments introduces new modes and effects of failure. Industrial cybersecurity professionals must be familiar with common failure modes, including their precursors, to avoid them if possible. They should be able to create mechanisms to differentiate between physical failures and cybersecurity events. They must help incorporate cybersecurity into discussions about root cause. They may employ specific cyber-physical failure mode terminology such as loss of control, loss of supervisory control, and manipulation of view (Assante, 2015)<sup>1</sup>.

#### **6.4.6 Regulation and guidance**

The term “regulation and guidance” refers to intentionally developed security practices and enforcement of security policies. The regulatory environment for industrial control systems varies by country and industry. The guidance and regulation provided below are well-recognised and illustrative, but are centred on the United States, and certainly not comprehensive.

##### **6.4.6.1 Presidential/executive orders**

“Executive orders” refers to the authority of the President of the United States to direct policy of executive branch agencies. Presidents Bill Clinton, George W. Bush, Barack Obama and Donald Trump each issued executive orders regarding the cybersecurity of critical infrastructure, which includes industrial control systems. These orders include:

- Executive Order 13010 “Critical Infrastructure Protection” (Clinton, 1996)
- Executive Order 13321 “Critical Infrastructure Protection in the Information Age” (Bush, 2001)
- Executive Order 13636 “Improving Critical Infrastructure Cybersecurity” (Obama, 2013)

---

<sup>1</sup> Assante and Lee introduced “methods to achieve functional impact” grouped into three categories: loss, denial, and manipulation of: view, control, sensors & instruments, and safety”; however, they never fully describe or define those terms. These are potentially useful pedagogical concepts, but lack refinement and formalization. Macaulay (2016 ) begins such refinement.

- Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (Trump 2017)
- Executive Order 13920 “Securing the United States Bulk-Power System” (Trump, 2020)

Industrial cybersecurity professionals should be aware of the visibility that industrial cybersecurity can have at the national level, and the geopolitical implications of that visibility. They should be aware of the impact that these decisions can have on the cybersecurity environment; and, they should recognise that regulatory regimes may be subject to significant change.

#### **6.4.6.2 ISA/IEC 62443**

ISA/IEC 62443 is the set of 14 standards – published, proposed, and under development – to guide the cybersecurity of industrial automation and control systems. The documents are created and maintained by the International Society of Automation (ISA) – a professional society composed of more than 40,000 automation professionals.

The 62443 series is the most comprehensive cybersecurity guidance specifically intended for industrial control systems, and incorporates important frameworks and concepts missing from documents not produced by automation professionals. Like all standards, certain components may have strengths and weaknesses but, every industrial cybersecurity professional should be familiar with the concepts included. Most of the 62443 standards are available to all ISA members free of charge.

#### **6.4.6.3 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Revision 2**

NIST SP 800-82 R2 is a medium-sized document that introduces industrial control systems and advises those US federal entities on how to secure ICS within the Federal Information Security Management Act (FISMA) framework. The document is also useful for those attempting to secure non-federally owned industrial control systems.

Industrial cybersecurity students will generally find SP 800-82 R2 a more approachable document than IEC 62443 because the document introduces industrial control systems to those not familiar with them. It is a single document, and is downloadable without an account or membership.

#### ***6.4.6.4 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)***

The North American Electric Reliability Corporation (NERC) is quasi-governmental agency composed of its members who own and operate the U.S. bulk electric system. It creates and oversees enforcement of regulations that ensure the reliability of the North American grid, including a set of cybersecurity regulations called CIP, that are among the most stringent cybersecurity regulations in the world – carrying the potential of large fines for non-compliance.

NERC CIP cybersecurity practice standards are structured as requirements that entities must simultaneously follow and demonstrate their compliance. The level of prescribed detail and supporting interpretations provide a valuable resource for industrial cybersecurity professionals even outside of the electric sector.

#### **6.4.7 Common weaknesses**

Common Weaknesses is a topic area that describes where industrial control systems historically suffer from significant vulnerabilities – which may not be entirely unique to industrial environments.

##### ***6.4.7.1 Indefensible network architectures***

Industrial control systems were often designed as stand-alone, non-networked controllers connected only to sensor inputs and actuator outputs. When ICS devices began to include network capabilities, the new functionality was implemented by individuals with little network or security training. As a result, many ICS networks lack subnets, firewalls, VLANs, access control lists, logging, VPN access or two-factor authentication.

##### ***6.4.7.2 Unauthenticated protocols***

An unauthenticated protocol is one that does not support passwords or cryptographic integrity checking. Because widely deployed industrial control system protocols do not incorporate these features, any device on the network with the software to communicate via these protocols can perform commands without any requirement for authentication. In other words, any laptop that can communicate to a programmable control device such as a PLC, can change the set point or alter the logic on the device. Examples of these protocols include but are not limited to DNP3, EtherNet/IP, Modbus, and BACnet. This represents one of the most significant weaknesses in industrial environments.

#### ***6.4.7.3 Unpatched and outdated hardware/firmware/software***

Because industrial control systems were not originally intended for connection to the Internet (even outbound-initiated connections), to communicate with the corporate network, or to be updated on a frequent basis, long term maintainability such as software/firmware patching was not a core design consideration. As a result, programmable control devices such as programmable control devices, SCADA servers, and historians are often out-of-date. In some environments, no one is assigned to monitor for new software releases or patches. Because processes often run 24 hours a day, deploying patches and upgrades presents a significant challenge.

#### ***6.4.7.4 Lack of cybersecurity training and awareness among ICS-related personnel***

Historically, technicians, engineers, and operators come through career pathways that seldom cover cybersecurity topics. Corporate security awareness trainings are only tangentially relevant to the tasks these industrial professionals routinely carry out.

#### ***6.4.7.5 Transient devices***

Transient devices refers to lap tops and other hand held devices, such as configurators or calibrators that are only temporarily connected to a network, and frequently carried from location to location and network to network. Engineering lap tops that include PLC programming software used by an engineering firm that does work for dozens of customers around the world are one example. Handheld diagnostic devices are another. The transient nature of these devices, coupled with the fact that they are at times not connected to networks, makes them difficult to identify, locate, and manage. From an attacker's perspective, they are ideal for spreading malicious code.

#### ***6.4.7.6 Third-party access***

Third-parties are firms or individuals involved in the design, build, operations or maintenance of industrial control systems or the facilities in which they reside. Specialised knowledge of these firms and individuals makes them indispensable partners for industrial operations. This reliance creates a challenging requirement to manage both physical and logical access to control system resources, and creates security dependencies outside the control of the organisation that actually owns the industrial control system. Some of these dependencies may be with small firms, who do not have resources dedicated security, making them attractive and easy targets.

#### **6.4.7.7 *Unverified supply chain***

The supply chain refers to the provenance of all of the parts and programming that compose an industrial control system. For example, the PLC vendor may not have designed the device's CPU. The operating system came from another vendor, which in turn incorporated an open source web server. Each of the suppliers may have operations located in various locations of the globe, that incorporate products from still other suppliers. Devices are often shipped in boxes and containers that cannot be considered tamper-evident. The result is a web of unrecognised dependencies that the product's end user cannot possibly understand.

#### **6.4.8 Events and incidents**

The term "events and incidents" refers to the industrial safety and cybersecurity experiences that resulted in significant impacts. Recognising what went wrong and why it went wrong provides powerful motivation to ensure that one's own organisation does not experience similar consequences. The following list of events is instructive, but by no means comprehensive. The list should be updated from time to time to include additional relevant emerging events.

##### **6.4.8.1 *DHS Aurora***

DHS Aurora is a proof-of-concept cyber-attack against the protection system for a diesel generator paralleling the grid, conducted at the Idaho National Laboratory in 2007. The attack sent rapid open and close commands from the protective relay to the circuit breaker, pulling the generator out-of-sync with the electric grid. Repeatedly reconnecting the generator to the grid in this out-of-phase condition caused the generator to accelerate rapidly, damaging the generator beyond repair.

Key take-aways from the proof-of-concept include that specialised malware may not be necessary to cause expensive damage to important equipment. If an attacker is on the network, the attacker may simply be able to abuse the functionality built into the safety system to achieve its destructive objective. Any spinning equipment that can be brought into or out of the sync with the grid can be subject to similar effects.

##### **6.4.8.2 *Stuxnet***

Stuxnet is the first widely recognised malware to attack industrial control systems. In July of 2009, it altered the control logic on the programmable control devices at Iran's Natanz uranium enrichment facility in a way that changed the output speeds set by variable

frequency drives controlling the motors that spun centrifuges. When an infected programmable control device was asked to provide its logic, it returned the unaltered version. Unused code within Stuxnet appeared to target safety pressure relief valves within the facility.

Key observations include that those who conducted the attack must have had access to precise engineering details about the facility, including the legitimate control logic, before unleashing the attack. The control network at Natanz did not assure the integrity of logic within the controller. Stuxnet was not an overly stealthy attack as the rapidly accelerating motors would have been noticed by technicians within the facility based on the audible change in pitch. Centrifuge motor speed may not have been an independently monitored or controlled variable. Key elements of the Stuxnet worm indicate that it intended to get caught as a way to send a message to the victims.

#### **6.4.8.3 *Ukraine 2015***

Ukraine 2015 refers to a simultaneous set of power outages affecting at least three regional electricity distribution utilities in western Ukraine. The attack shut off power to about 225,000 customers. It was the first well-documented power outage due to cyber-attack.

Key observations include the fact that no automated control system-specific malware was used to turn off the power. However, several industrial control system components were targeted, in particular the dispatcher computers that allow operators to open and close breakers, and equipment used to translate serial industrial control protocols to TCP/IP protocols.

#### **6.4.8.4 *Ukraine 2016***

Ukraine 2016 refers to a single power outage at Ukraine's leading electricity transmission company, Ukrenergo, which provides electricity to the Ukrainian capital, Kiev. The attack employed malware to send a breaker open command using a common substation automation protocol. This opened all the breakers serving a section of Kiev in December 2016, causing in a power outage of greater consequence than the triple-utility attack did in 2015.

Key observations include that the attackers had developed malware specifically to send a breaker open command as part of a cyber-attack, and that transmission providers may be higher value targets than distribution providers.

#### **6.4.8.5 *Triton***

Triton is a piece of malware found within an oil refinery in Saudi Arabia on an Schneider Electric (formerly Invensys) Triconnex safety controller. The adversaries, in the course of attack planning, caused several process shut-downs. These gave rise to the investigation that uncovered the malware. Investigation showed that the adversaries had made their way from Internet-facing systems all the way to the safety controller. The safety controller was left in a “program” mode, which enabled the attackers to interact with the controller.

Key observations include the fact that adversaries were capable of reverse-engineering the proprietary Triconnex communications protocol. This represents a significant investment in time and energy, and should be interpreted as building a re-usable cyber weapon. Only after several process shut-downs did the plant suspect cyber-attack, and called in professional incident response assistance. Communications between the incident response investigator, the control systems vendor, and potentially at-risk asset owners was not smooth.

#### **6.4.8.6 *Taum Sauk Dam***

Taum Sauk Dam is a pumped storage electric generation facility positioned on a hilltop in Missouri. The facility had a poor track record of conducting maintenance, and the housing for fill-level sensors had become detached from their locations, resulting in inaccurate fill-level readings. This caused facility operators to regularly dismiss alarms and change set points to compensate – without conducting in-person or video observation of the actual fill level. Perhaps most importantly, the dam was constructed without a spillway. When the dam overfilled in 2005, it released all its contents down the hillside, causing extensive environmental harm. One family on a camping trip in the area was affected by the release, but no one was killed (Rogers, 2010).

While this event was not the result of a cyber-attack, it is instructive due to a thorough investigation that provides in rich documentation. Inaccurate sensor readings due to cyber-attack can lead to a manipulation of control, and potentially, similar physical impact.

#### **6.4.8.7 *DC Metro Red Line***

In June 2009, two mass transit trains from the DC Metro Red Line collided near Fort Totten Station in Washington, D.C. when the track sensor system failed to recognise a train stopped on the track (National Transportation Safety Board, 2010). The software instructed a following train to accelerate. By the time the conductor of the following train noticed the



stopped train, and hit the emergency brake, it was too late. Nine people were killed and 52 hospitalised.

Root cause analysis revealed the sensor system was not properly installed and tested. In an interesting case for software liability in industrial environments, software vendors for the safety system were sued and settled out of court.

Although this incident was not the result of an intentional cyber-attack, the idea that manipulated sensor values could result in a loss-of life mass transit scenario is relevant. The thorough root cause investigation and resulting materials provides a valuable resource.

#### **6.4.8.8 *San Bruno***

In September 2010, a 30-inch diameter natural gas transmission line running beneath a neighborhood in San Bruno, California exploded, destroying 38 homes, damaging 70 homes, killing eight people, and injuring many more (National Transportation Safety Board, 2011).

The incident occurred when maintenance technicians were upgrading backup battery power supplies at a line terminal station. De-energising a specific portion of the system resulted in loss of power to an unanticipated part of the station.

While the technicians reconnected power, they ran into what they suspected was a software issue and called the control system vendor to help troubleshoot. Meanwhile, this loss of power caused the control system to determine that pressure within the pipeline was low, and that the valves should be opened and the pressure increased.

The system operators in the control room were unable to see the pressure measurement until the system generated high-high pressure alarms, indicating that the maximum allowable operating pressure was reached. These values were confirmed via manual readings by the technicians.

Downstream, the high pressures caused a previously undetected faulty weld to burst the giant pipeline, resulting in a fireball that spewed flames hundreds of feet into the air. Because the transmission pipeline valves nearest the incident were manually operated – that is, they could not be closed remotely – the fire raged for 95 minutes.

This case, like Taum Sauk and DC Metro, was not the result of intentional cyber-attack. However, the effect of inaccurate sensor values on the physical state of the system is particularly instructive to would be cyber-attackers and defenders. The rich investigative documentation available for the case, including discussion of a software flaw, and debate

about which elements should and should not be remotely controlled, make it of significant instructional value.

#### **6.4.9 Defensive technologies and approaches**

The term “defensive technologies and approaches” describes a foundational list of approaches of particular use to industrial environments. In many cases, the defensive technologies and approaches align to the common weaknesses discussed in the previous sections. Some of the approaches are unique to industrial environments.

##### ***6.4.9.1 Firewalls, data diodes***

Firewalls are network control devices that allow or disallow use of network resources based on criteria such as IP address, port number, and protocol field content. Firewalls with high levels of protocol awareness can be configured to allow setpoint changes or control logic pushes from only certain IP addresses, for example. Data diodes enforce one-way communication of data through photo-electric diodes. In a TCP/IP connection the diodes spoof expected responses to the sending party to ensure that communications continue. These are effective for environments that require data to flow out of a control network, but not in. Elements of these two technologies are well aligned to mitigating both weak network architectures and use of unauthenticated protocols.

##### ***6.4.9.2 ICS network monitoring***

Network monitoring involves the creation of rules that trigger alarms and alerts. This differs from firewall and diodes in that it does not prevent use of network resources, but encourages a human analyst to make a better-informed decision. One approach involves creating a baseline of network activity and then alerting the analyst when this deviation from the baseline occurs. For example, a new IP address appears on a network, or a previously recognised IP address begins using a new TCP/IP port. This defensive technique helps mitigate some aspects of weak network architectures, transient devices, and third-party access. It’s greatest value to industrial personnel is the added visibility it provides personnel to network-related incidents such as misconfigurations or faulty software – which are not necessarily malicious in nature.

##### ***6.4.9.3 Awareness and training for ICS-related personnel***

Because of the important physical consequences of cyber-attack against industrial control systems, personnel who regularly access these systems require industrial cybersecurity awareness and training tailored to their roles.

#### **6.4.9.4 *Cyber-informed engineering***

Cyber-informed engineering refers to the process of incorporating cybersecurity into all facets of the engineering discipline, rather than considering cybersecurity a special task that is only aligned with computer science or information systems. It encourages application of cybersecurity principles as a fundamental component of system design. Researchers have advanced numerous methods to unify the safety and cybersecurity elements of engineering, as indicated by Kavallieratos (2020).

One particular instance of cyber informed engineering is the consequence-driven cyber-informed engineering process, which seeks to eliminate cyber risk where possible by incorporating cyber-physical fail-safes for the most critical aspects of an infrastructure, service, or process. Where such fail-safes cannot be designed or deployed, it encourages the creation of early warning systems. This methodology is developed and advanced by the Idaho National Laboratory (Idaho National Laboratory, 2018).

#### **6.4.9.5 *Process hazards assessment-based approaches***

“Process hazards assessment-based” refers to extending the prevailing process hazards assessment (PHA) safety methodology to include cybersecurity as well. This approach requires practitioners to identify possible failure conditions, and engineer safeguards that minimise the possibility of such occurrences. Cyber PHA (Morella, 2019) and Security PHA (Marszal, 2019). are two examples.

#### **6.4.9.6 *Cyber-physical fail-safes***

Cyber-physical fail-safes are the intentional choice of process control and safety mechanisms that cannot be manipulated by cyber-attack.

#### **6.4.9.7 *Process data correlation***

Process data correlation is a technique that makes use of data gathered by process historians to detect potential manipulation or attack. This can include correlation of existing data or the strategic placement of new process sensors that rely on diverse principles of operation with independent network backhaul. Such data provides warning, but not control.

## **6.4.10 Validity.**

### ***6.4.10.1 Critical paradigm***

Under the critical paradigm, the researcher views their role to include uncovering hidden assumptions. This allows the researcher to become involved in the research, but they must ensure they disclose their perspectives and biases (Creswell, 2000).

#### ***6.4.10.1.1 Researcher reflexivity***

As I have mentioned briefly in previous chapters, my perspective relative to industrial cybersecurity education and training grew out of my work as an intelligence analyst covering the industrial cybersecurity threat environment since 2006. As an analyst, one focuses a large amount of thought-energy on significant events and incidents. An analyst teases out the insights from those events and then shares those insights with customers – who are more properly considered “intelligence consumers”.

Having started my own company in January 2009, I was entirely consumed in the broader analysis of Stuxnet events. Some of the most important insights from the list and justifications provided in sections 6.4.1 to 6.4.9 came from my coverage of the Stuxnet event. The key insight relative to industrial cybersecurity education and training was this: In order to carry out the Stuxnet attack, its authors had to understand the industrial process in great detail. They needed to fully comprehend how centrifuge-based uranium enrichment worked. They had to understand what line of reasoning the Iranians were following, including what innovations they intended to apply. They had to grasp the global supply chain for the equipment the Iranians would need. They must have identified the Iranian engineering firms that were most qualified to do the work. They would have to steal process diagrams, and even the PLC logic from those firms – potentially after the plant was operational. Then they would have to come up with a list of attack options – physical consequences they wanted to achieve via cyber-attack. Without a detailed understanding of the process and the equipment, the attackers could not even generate viable options. Then, the attackers would carefully consider one or more options to pursue. This would require detailed discussion of an impressively cross-functional team. Discussions would include motors, frequencies, pressures, valves, fieldbuses, protocols, software versions, device identifiers, and so forth.

The team would divvy up the work, and build out various elements of the attack code. The attack would have to be tested to various levels of fidelity in simulated environments to ensure it could achieve its consequence. Then the attack would have to be deployed into the

target environment, probably relying on the supply chain, including procurement channels and engineering firms – the same firms from which the attackers had stolen the detailed information in the first place.

The profound multi-year collaboration the attackers demonstrated among highly skilled professionals from various disciplines, stood in stark contrast to the entire cluelessness of the victims – even if the victims were involved in a nuclear weapons program, which might have reasonably suspected cyber-attack. More impressive was the idea that the attackers could disclose or conceal their attack at will. They could release the code to various “victims” and allow the world to know what they had been up to after their attack had run its course.

Core concepts – if not actual attack code – were certainly re-usable, and would obviously be put to use in ongoing military programs. Targeting methodologies and attack toolkits for industrial control environments must be under constant development. The understanding of the Siemens communications protocols, and controller logic files could be used against any victim using those controllers throughout the whole world. To me, Stuxnet provided only a peek at what the growing U.S. cyber arsenal must include.

In fact, I thought, Stuxnet must be part of a larger cyber operation against Iran. One in which the object is to cyber-bully Iran into submission. I knew that the same engineering firms building control systems for Natanz were also building control systems for Iran’s petroleum industry – which was the country’s single largest source of revenue. The same tactics, techniques and procedures used against Natanz were certainly being used against Iran’s petroleum industry. Stuxnet was just a warning.

Then I thought, “Oh no. How is U.S. critical infrastructure any less vulnerable than these Iranian counterparts? No. Wait. The same basic technologies and vulnerabilities exist not in the United States alone, but in automated industrial processes throughout the world, that sustain modern life and economies across the globe”.

In the aftermath of Stuxnet, the New York Times had run an article claiming that the Idaho National Laboratory had been involved in creating the industrial control systems portion of the Stuxnet worm. The article advanced evidence of strong similarities between Stuxnet and the results of an assessment INL researchers had done of the Siemens S7 control system.

I thought to myself, if the results of INL-conducted assessments had informed the creation of Stuxnet, what other systems had INL assessed? What had those assessments found? What cyberweapons had the United States government created based on those results?

A short time later, a Russian cybersecurity research firm called Positive Technologies began pushing an effort to discover and disclose vulnerabilities in industrial control systems. They held contests, offered prizes, and presented numerous vulnerabilities at cybersecurity conferences. They documented default passwords, and appeared to be having a good time. Then results of their work began showing up in attack tools.

The world got a little bleaker for me as evidence of an industrial control systems cyber arms race began to stack up in my mind. As tools and know-how began to accumulate, actors involved would no longer consist of only state-nexus threat actors.

Simultaneously, I witnessed the accelerated adoption of smart technologies into industrial environments. This adoption is reflected in the “Emergence of Operational Technology” section of Chapter 2. Examples of technologies include a variety of cloud-based: SCADA (Inductive Automation, n.d.; Emerson n.d.), predictive analytics (GE Digital, n.d.), and “machine as a service” (Grenacher, 2018). I could envision web servers on transmitters, virtualised PLCs, and concentrated enterprise resource planning (ERP) systems allowing access to industrial facilities throughout the world.

This was concerning because it meant that the same weaknesses that could affect any cloud-enabled offering, could foreseeably spread to industrial environments and permit physical consequences. I doubted whether the individuals and organisations pushing such offerings, as well as those adopting them, had fully reasoned through the implications.

And so, back to my inquietude, “what should be done to appropriately secure and defend these industrial environments?”

I recognised that cybersecurity must become an integral part of engineering and engineering technology rather than its own domain hanging-off after the fact. After all, it is the engineers and technicians who are ultimately responsible to design, build, operate and maintain reliable systems and infrastructures.

In the case of Stuxnet, the engineers and technicians and the computers they used to do their work were high value targets. In the case of the Ukraine attacks, it was the process operator (dispatcher) computers.

These individuals were not receiving the industrial cybersecurity training and education they needed. So, when faced with the opportunity to lead the first of its kind program to help educate and train these exact employees, how could I turn it down?

I must admit that I have never received any formalised education or training related to industrial automation. This means that the final three knowledge categories, all of the content titles, the description of each content title, and the justification for each content title provided in this chapter (6), came directly from my head as a result of what I learned studying the threat environment.

The strength of this fact is that it is the precise combination of my academic training and professional experience that led me to identify and describe this content in an organic way – that is, a way that makes sense to me. Moreover, providing the justification for each item it is something that none of the previous efforts for guiding industrial cybersecurity training and education have ever done in a publicly accessible way.

The weakness of the results that came from the critical paradigm methodology is that I am a single, and potentially impeachable source of information for the contents of the first six areas – because I have never designed, built, operated or maintained an actual industrial control system.

#### ***6.4.10.2 Postpositivist paradigm***

Under the postpositivist paradigm, which is the secondary paradigm for this research, through the researcher lens, the researcher seeks to confirm findings through triangulation – which is a comparison to a variety of external sources (Creswell, 2000). This section seeks to validate the knowledge items via comparison with 1) external documents, and 2) concepts highlighted in recognised industrial cybersecurity incidents and research.

##### ***6.4.10.2.1 Triangulation with external documents***

In order to validate the topic contents for the first five knowledge categories, the contents were compared with the Automation Competency Model developed by the United States Department of Labor (DOL) with support from the International Society of Automation (ISA [Department of Labor, 2009]).

Of the 38 terms provided as parenthetical examples in the new topics, 30 are also found in the DOL model, representing an 79% match. Table 12 displays the locations of matches, which itself provides a useful resource for instructors seeking to use the proposed knowledge unit.

It is noted that six of the seven terms missing a match are in the “Equipment under control category”. This is not surprising, given that one might expect to find these terms in the field of mechanical engineering or electrical engineering rather than industrial automation. Despite the lack of match with the DOL model, these are appropriate because this equipment directly influences the physical consequences of a cyber-attack.

The remaining term not found in the Department of Labour Automation Competency Model is “electrical safety”. Here it is reasonable to assert 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 12. Comparison of proposed knowledge unit topic terms with Automation Industry Competency Model*

Knowledge Category	Term	Location in Automation Industry Competency Model		
Industrial processes and operations	Industry sectors	p. 4		
	Professional roles and responsibilities	3.2.1.1	5.6.19.3	
	Organisational roles			
	Engineering diagrams	5.2.14	5.3.13	5.5.13
	Process types	4.2.7	5.1.6	
	Industrial 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		
	Configurators/calibrators	4.1.7.1	4.2.8.1	4.3.9.2
	Data historians	5.7.6		
Equipment under control	Motors	5.2.13		
	Pumps			
	Compressors			
	Valves	5.2.4	5.2.5	
	Relays			
	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
	Transmitter signals	5.2.6		
	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 functions	5.5		
	Lock-out tag-out	4.5.11.4		
	Safe work procedures	4.5.11		
	Failure modes	5.5.8.3		

The content from the three additional topic areas (Common Weaknesses, Events & Incidents, and Defensive Technologies & Approaches) also require validation. For the Common Weaknesses topic, the topics do not differ greatly from content in traditional cybersecurity educational materials. But, they may have unique implications for industrial environments. These key terms are found in NIST SP 800-82 R2, and NERC CIP documents, as indicated in the following table.

*Table 13. Terms from Common Weaknesses category and external location*

<b>Term</b>	<b>Reference to External Location</b>
Indefensible network architectures	NIST SP 800-82 p. C-6
Unauthenticated protocols	NIST SP 800-82 p. C-9
Unpatched and outdated hardware/firmware/software	NIST SP 800-82 p. C-7
Lack of training and awareness among ICS-related personnel	NIST SP 800-82 p. C-4
Transient devices	NERC CIP-003-8 pp. 24, 51-54
Third-party access	NERC CIP-013-1 pp. 3-4, 11-13
Unverified supply chain	NERC CIP-013-1 pp. 3-4, 11-13

For the Defensive Technologies & Approaches category, some of the terms are found in NIST SP 800-82. Other terms, such as cyber-informed engineering, and process hazards assessment are newer approaches especially applicable to industrial environments. Matches between these concepts and supporting documentation is displayed in Table 14.

*Table 14. Terms from Defensive Techniques and Approaches category and external location*

<b>Term</b>	<b>External Location</b>
Firewalls	NIST SP 800-82 p. E-1

Data diodes	NIST SP 800-82 p. E-1
ICS network monitoring	NIST SP 800-82 p. E-1
Awareness and training for ICS-related personnel	NIST SP 800-82 pp. 4-1, 6-13, G-20,
Cyber-physical fail-safes	NIST SP 800-82 pp. 5-21 (as “fail-safe process”), G-64 (as “fail-safe procedures”)
Process data correlation	Krotofil, 2015 <i>The Process</i> Hadžiosmanović, 2014 Ahmed, 2018
Process hazards assessment (PHA)-based approaches	Marzal, 2018 Morella, 2019
Cyber-informed Engineering	Bochman, 2021

For the Events & Incidents knowledge category, triangulation may also provide validation; however, as avoiding and mitigating industrial cybersecurity events is the entire purpose of educating and training industrial cybersecurity professionals, such may hardly be necessary. A better question may be whether the chosen events are the most relevant or instructive from all possible events. While the research did not explore this question from the postpositivist paradigm, it is possible to “reverse triangulate” the chosen events with the validated concepts to at least demonstrate that the events are consistent with the knowledge categories and items. Such is the approach described in the following section.

#### 6.4.10.2.2 Triangulation with industrial cybersecurity events and incidents

A complementary triangulation technique is to align the terms (as described in the analysis section of this chapter) with the industrial cybersecurity incidents identified in Section 1.2.3, and covered under the “Events and Incidents Knowledge Category” in this chapter. As shown in Table 15, if an aspect of the attack, in the opinion of the researcher, clearly involves the concept, it is marked with an X.

*Table 15. Correlation of industrial cybersecurity specific knowledge with industrial cybersecurity events*

		<b>Industrial Cybersecurity Event</b>			
		Stuxnet	Black Energy 3	Crash Override	Triton
<b>Knowledge Category</b>	<b>Item</b>	Iran 2009	Ukraine 2015	Ukraine 2016	Saudi Arabia 2017
	Sectors	X	X	X	X

Industrial processes and operations	Professional roles and responsibilities	X	X	X	
	Organisational roles	X			
	Engineering diagrams	X			
	Process types	X	X	X	X
	Industrial lifecycle	X	X	X	X
Instrumentation and control	Sensing elements				X
	Control devices	X		X	X
	Programmable control devices	X		X	X
	Control paradigms				
	Programming methods	X			X
	Process variables	X			X
	Data acquisition	X			
	Supervisory control	X	X		
	Alarms	X			X
	Engineering laptops/workstations	X			
	Configurators/calibrators	X			
	Data historians	X			
Equipment under control	Motors				
	Generators				
	Pumps				
	Compressors				
	Valves	X			X
	Relays			X	
	Transformers		X	X	
	Breakers		X	X	
	Variable frequency drives	X			
Communications	Reference architectures		X		X
	Communications protocols	X		X	X
	Transmitter signals	X			
	Fieldbuses	X			
Safety	Electrical safety				
	Personal protective equipment				
	Safety/hazards assessment	X			

	Safety instrumented functions	X			X
	Lock-out tag-out				X
	Safe work procedures				
	Failure modes	X			
Common Weaknesses	Indefensible network architectures		X	X	X
	Unauthenticated protocols	X		X	X
	Unpatched and outdated hardware/firmware /software			X	
	Lack of training and awareness among ICS-related personnel		X		X
	Transient devices	X			
	Third-party access	X			
	Unverified supply chain	X			
Defensive Technologies & Approaches	Firewalls				X
	Data diodes				X
	ICS network monitoring	X		X	X
	Awareness & Training for ICS-related personnel		X	X	X
	Cyber-physical fail-safes	X			
	Process data correlation	X			
	Cyber process hazards assessment	X			
	Cyber-informed engineering	X			

Of the 50 terms in the list, eight did not match an ICS-specific attack. Of the eight, three dealt with safe work procedures, and as such were not relevant to this particular analysis. This left an 90% (45/50) match.

The eight unmatched items were: control paradigms, motors, generators, pumps, compressors, electrical safety, personal protective equipment, and safe work procedures.

While the relevance of these items may not have yet been proven by actual cyber-attack, all

but one is covered by the three safety events also included in the events and incidents category, as illustrated in the Table 16.

*Table 16. Mapping of remaining items to other events*

<b>Knowledge item</b>	<b>Event</b>			
	DHS Aurora	San Bruno	Taum Sauk	DC Metro
Control paradigms				
Motors				X
Generators	X			
Pumps			X	
Compressors		X		
Electrical safety				
Personal protective equipment				
Safe work procedures		X		

This mapping only left three items: control paradigms, electrical safety, and personal protective equipment without validation by external documentation.

#### **6.4.11 Limitations**

One important bridge area still missing from this analysis is incident response. A significant question for future consideration should be: what elements of incident response apply specifically to industrial environments?

#### **6.5 Conclusion**

This chapter has described the methodology used to identify the specific knowledge that differentiates industrial cybersecurity from traditional cybersecurity. Using a critical pragmatic research paradigm, this relied significantly on the researcher's own expertise. The results were validated and characterised by researcher reflexivity. Additional work may be performed to further validate and refine the content identified.

Finally, under the postpositivist paradigm, the same knowledge contents were validated via comparison with several external sources.

It is recognised that the contents of the Events & Incidents knowledge category will need to be changed and updated on a regular basis – especially as more instructive events and incidents occur.

Of the topics described in this chapter, the Defensive Technologies & Approaches category will merit the most attention moving forward because it describes how defenders interrelate the control systems specific knowledge to cybersecurity knowledge. Approaches

such as cyber process hazards assessment and consequence-driven cyber-informed engineering are gaining adherents, but relatively few experts exist. New approaches will emerge or gain popularity. As a result, contents of this topic must balance description – what practitioners in the field do, and prescription – what practitioners in the field should do.

The content descriptions and justifications provided in this chapter will be of particular use to administrators, educators, and training providers as they create content intended to infuse a new generation of engineering professionals with critical cybersecurity knowledge and skills.

In order to increase ease of adopting the results, an updated NSA-CAE style knowledge unit has been created. That knowledge unit, and additional supporting description are found in Appendix B.

## **7 INDUSTRIAL CYBERSECURITY WORKFORCE DEVELOPMENT MODEL**

### **7.1 Problem**

The key research question of this thesis is “What is the foundation for the formal preparation of industrial cybersecurity professionals?” The critical review of candidate industrial cybersecurity education and training documents/efforts presented in Chapter 4 found a variety of approaches and terminology. In particular, discussion associated with Criterion 8, “Includes job roles” found that:

*The identification of job roles notionally marks the transition from education to training, which may fall outside the historic strength of purely academic approaches. Inconsistent use of education- and training-related terminology such as “job role” across training and education literature will require those creating a standard to clearly define terms used.*

The key objective addressed in this chapter for advancing a foundation for industrial cybersecurity professionals is the establishment of a clear workforce development model – not the content – but the key terms used to describe the workforce, the definitions of those terms, and the relationships of those terms to one another. For example, such a model would begin to describe how the archetype roles identified in chapter 5 employ the knowledge identified and described in chapter 5 and 6 – providing a way to meet both the curriculum development perspective of academics and the workforce development perspective of employers.

### **7.2 Research design**

A first step in research design is to characterise the nature of the question being addressed. In this case, workforce development terminology is not necessarily an open-ended, creative, or new endeavor. Rather, it is a matter of understanding the foundational concepts of workforce development frameworks, and selecting among existing options or improving upon them.

As mentioned in the research methodology chapter (3), the prevailing research paradigm of the researcher is the critical paradigm, wherein the researcher seeks to reveal hidden assumptions. This is combined secondarily with the postpositivist paradigm, with its focus on structured approaches. As such, the core methodology for the research task addressed in this chapter involves 1) a review of key ideas in workforce model literature; 2) a critical characterisation and comparison of the of the structure of the workforce model

component of the candidate guidance documents/efforts presented in chapter 4; and, 3) synthesis of an appropriate model drawing on the strengths of the previous models.

### **7.2.1 Key ideas in workforce development models**

In common parlance the words “education” and “training” can also apply to any endeavor in which an individual consciously attempts to improve themselves, regardless of specific nuance. Of first priority was to ensure a reasonable definition of the terms “education” and “training”.

Generally, education deals with cognition – tasks performed by the mind – but is particularly linked to memory and recall. Training, on the other hand, is linked to tasks – what someone can do by applying the knowledge within a given context (Conklin, 2014, p. 2010; Masadeh, 2012).

One elementary difference, as has been pointed out by the prolific training writer Mager, is that training requires relevant practice. In “Making Instruction Work”, Mager points out that one learns to play the piano by practicing the piano rather than by answering multiple choice questions about music (Mager, 1997, p. 128).

In the industrial world, all personnel who work at some offshore oil rigs must undergo helicopter crash training, which requires every passenger to actually demonstrate the ability to extricate themselves from a helicopter fuselage that is submersed in water as part of a training simulation (Beilinson, 2012).

To drive home the difference between education and training, Dr. Corey Schou is wont to explain that most parents don’t mind if their sixth grader has an hour-long sex education session provided by the local school district; however, those parents would vehemently object to having their sixth grader participate in an hour-long sex training session! As the title of a text book used in the career and technical education department at Idaho State University proclaims “Telling Ain’t Training” (Stolovitch, 2011).

In general, the advantage to education is that it teaches students how to think, and it teaches them how to figure out what to do, not just what to do. The advantage to training is that it doesn’t waste time teaching students what they don’t need to know, and that students can see immediately how their knowledge applies to the real world.

Another key difference is that education normally leads to academic degrees and licensures, where training leads to industry recognised certifications. Education is generally



undertaken by younger, traditional students. Training is generally taken by working professionals.

It is also common to hear the word “training” applied to what might be more accurately called “awareness” or “literacy” efforts, wherein the “trainee” is exposed to knowledge content for a short time – and includes no relevant practice, no feedback on performance, and no checklist whereby the trainee can evaluate their own proficiency.

In general, the line of demarcation between education and training then, occurs when the instructional content deals with tasks a practitioner or professional will perform on the job. As the key research question for this thesis involves both education and training, the workforce model developed herein must include not only knowledge (as discussed in chapters 5 and 6), but the tasks the archetype roles are expected to carry out.

In the education world, Bloom colleagues categorised knowledge in three general areas: cognitive, psychomotor, and affective. Cognitive refers to the tasks that can be performed with the mind. Psychomotor refers to the tasks that can be performed with the body. Affective refers to the tasks that can be performed with attitudes. Bloom and colleagues then created a list of verbs that corresponded to each of these domains. They also grouped these verbs in categories of increasing complexity and abstraction (Bloom, 1956).

Some education practitioners recognise that Bloom’s three groupings of cognitive, psychomotor, and affective learning domains, align semantically to “knowledge” – cognitive, “skill” – psychomotor, and “attitude” – affective. This, they point out, was the original “KSA” acronym (Clark, 1999).

By at least 1975, the term “knowledge, skills and abilities” was used in U.S. government-publications describing job element examinations (Primoff, 1975 p. 31). Those who advanced this terminology may have interpreted Bloom’s “attitude” as broadly synonymous with “intellectual ability” which indicated a more complex cognitive task. Under this viewpoint, it remains unclear what happened to Bloom’s affective domain.

By 2000, “competencies” were supplanting “KSAs” as the term of choice in both professional opinion and academic human resources literature, apparently because the concept allowed for greater flexibility (Shippmann, 2020).

## **7.2.2 Characterisation of workforce models used in candidate documents/efforts**

This section provides a critical characterisation and comparison of the of the structure of the workforce model component of the candidate guidance documents/efforts presented in chapter 4, in addition to several others.

### **7.2.2.1 ABET**

ABET does not advance a workforce model, rather, it advances program criteria for programs with similar names. The criteria specify lists of topics that must be included in order for schools to meet the program criteria portion of the accreditation process. This list of topics generally correlates with Bloom’s cognitive domain (ABET, n.d.).

### **7.2.2.2 ENISA**

The ENISA model is organised around five levels of “target audience” (Pauna, 2014 p. 13-14)

- *Level 0: All people that enter an operational environment, where IACS is being deployed.*
- *Level 1: All People that have interaction with IACS.*
- *Level 2: People that have specific roles in developing, implementing, deploying and maintaining IACS.*
- *Level 3: People that have a specific security role within the IACS domain – junior, intermediate and senior level.*
- *Level 4: People with responsibility for the security in the IACS domain.*

Within these levels (apparently between levels 2 and 3) are two groupings: 1) the general workforce; and, 2) ICS/SCADA Cyber Security professionals. This latter group is then divided into management roles and technical roles (Pauna, 2014 pp. 13-14).

The document then lists knowledge areas and content for ICS/SCADA cyber security professionals, but does not attempt to relate the knowledge areas and content with the roles (Pauna 2014, pp. 15-18).

Figure 7 is the author’s visual hierarchical diagram of the ENISA model.

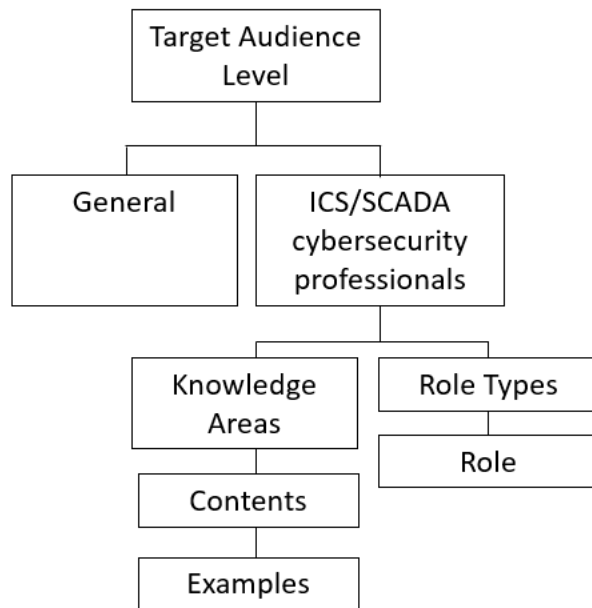


Figure 7. ENISA structure (created by the author)

### 7.2.2.3 GIAC

The document “The GICSP: A Keystone Certification” that describes elements of the creation of the GICSP, lists the Knowledge Areas, Contents, and Examples from the ENISA structure. Beyond that, it does not formally present a workforce development model. It does provide a graphic called “ICS-Related Job Role Mapping”, which “originally appeared in a SANS workforce consensus initiative developed with input and review from many ICS asset owners and operators across multiple industries. It suggests one way to model the intersection of job roles, competency levels and security functions” (Harp, 2016 p. 19).

This figure lists five competency levels and possible job role categories in which each of the competency levels could exist. It depicts that levels 1-4 are involved in support and maintain uses, and level 4 is involved in design uses.

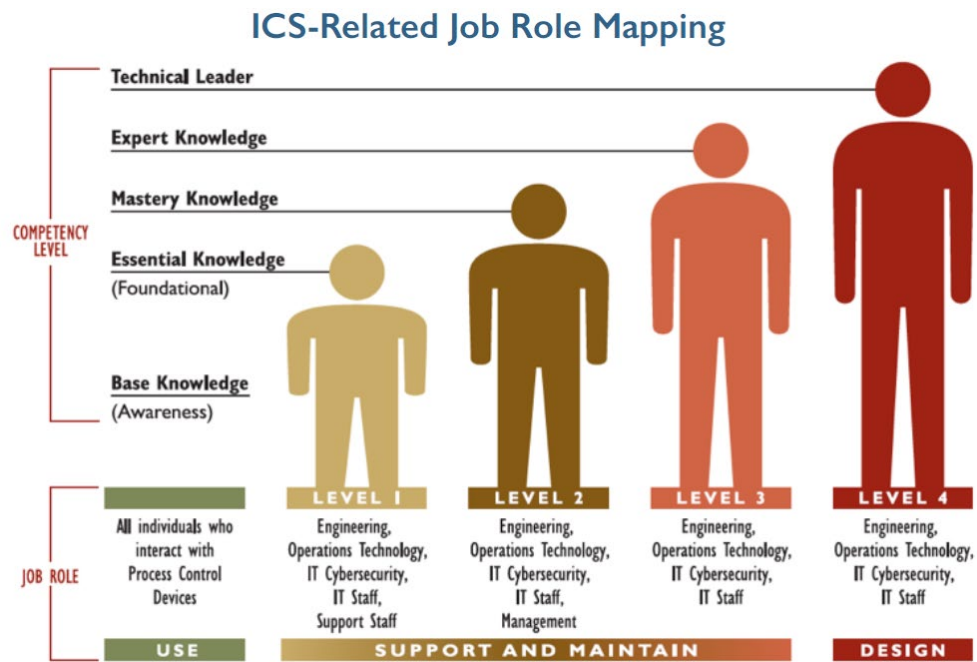


Figure 8. GIAC/SANS Workforce Model Graphic (Harp, 2016)

The document does not describe any relationship between knowledge and tasks, or otherwise elucidate how one might discern between a technical leader and someone who only possesses base knowledge.

#### 7.2.2.4 ISA & DOL

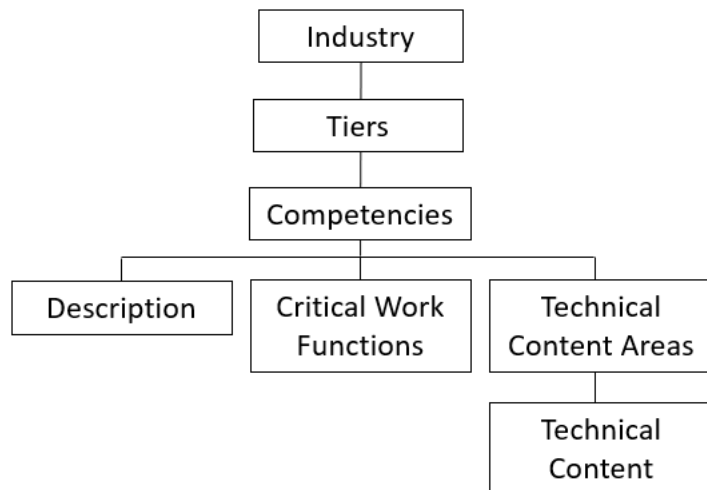
The Automation Competency Model produced by the International Society of Automation (ISA) in conjunction with the U.S. Department of Labour is based on the concept of “competencies”, which it defines as a “cluster of related knowledge, skills, and abilities that affects a major part of one’s job (a role or responsibility), that correlates with performance on the job, that can be measured against well-accepted standards, and that can be improved via training and development” (Department of Labour, 2018 p.4).

The model is shaped in a pyramid form, where the base competencies apply across industries and occupations, and succeeding ascending tiers apply more-specifically to the industry and occupation. The guidance provided with the model warns against assuming that the competencies at the top require a higher level of skill.

Tiers 1 through 3 are “foundational competencies” which individuals should possess in order to enter the workforce. Tier 1 are “personal effectiveness”, which are generally learned at home and reinforced at home or the workplace. Tier 2 are “academic competencies”, such as thinking styles learned in school. Tier 3 are “workplace competencies”, such as self-management styles developed in the workplace.

Tiers 4 and 5 are “industry competencies” which allow workers to move across industry subsectors in an agile manner. Tier 4 are “general technical competencies”, skills and knowledge basic across sectors of an industry. Tier 5 are “specific technical competencies,” that are specific to the industry.

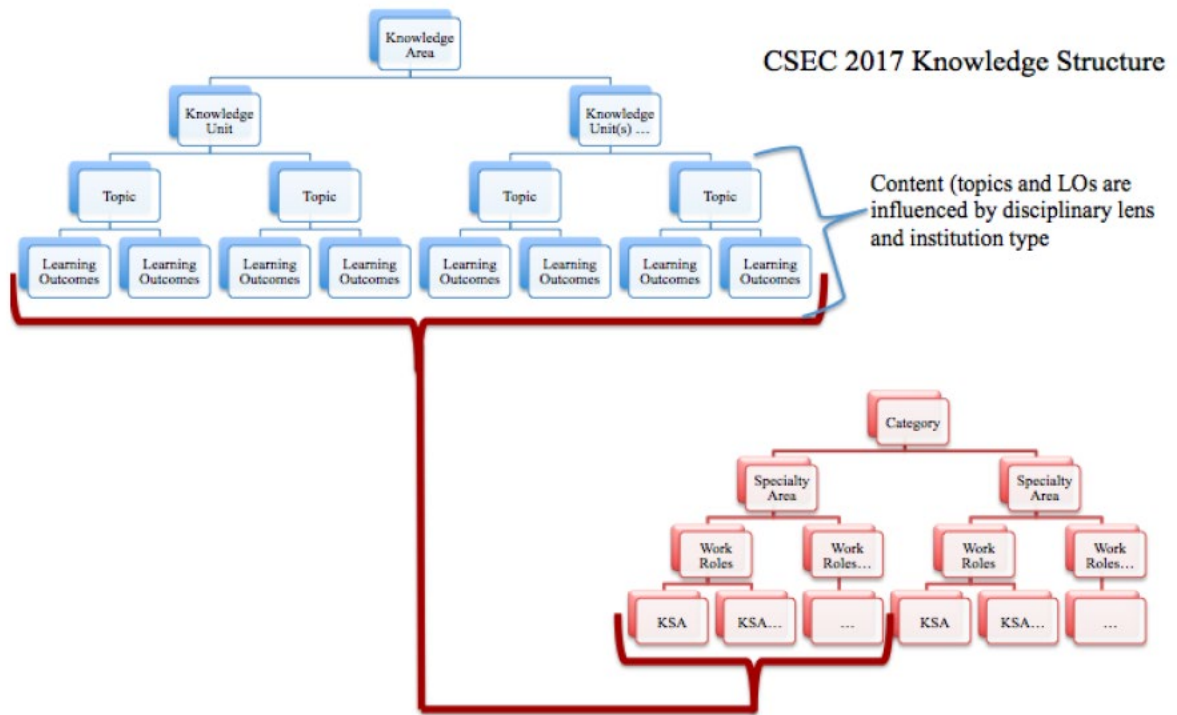
Starting at Tier 4, each competency grouping has a list of “Critical Work Functions” and “Technical Content Areas”. Critical Work Functions mostly begin with verbs, Technical Content Areas begin with a mixture of verbs and nouns.



*Figure 9. ISA DOL Competency Model structure (created by the author)*

#### **7.2.2.5 Joint Task Force**

The Joint Task Force curricular guidance includes primarily knowledge, and does not concern itself with roles or tasks (Burley, 2017). In educational theory, the learning outcomes would align to tasks that achieve important cybersecurity objectives, such as might be met by cybersecurity professionals and practitioners, as can be seen in Figure 8, below. In this case, the Joint Task Force decided to link their Learning Outcomes to the KSAs in the NIST NICE framework, which KSAs link, in turn, to Work Roles.



*Figure 10. Joint Task Force Knowledge Area Links to NIST NICE Framework (Burley, 2017)*

#### **7.2.2.6 NIST NICE Original (2017)**

The 2017 NIST National Initiative for Cybersecurity Education (NICE) framework was replaced by an updated version in November 2020. Because many cybersecurity education and training efforts have already linked with this model (including CSEC and ISA DOL), and significant insight might be gained from understanding how the authors approached the task, this section characterises the original framework. The 2020 revision will be treated in the following section.

The NIST NICE 2017 version categorises work into NIST NICE Framework Categories, Specialty Areas, Work Roles, Tasks, Knowledge, Skills, and Abilities. The Knowledge, Skills, and Abilities are not tied to Tasks. This structure can be seen in the diagram below (Newhouse, 2017 p. 6)

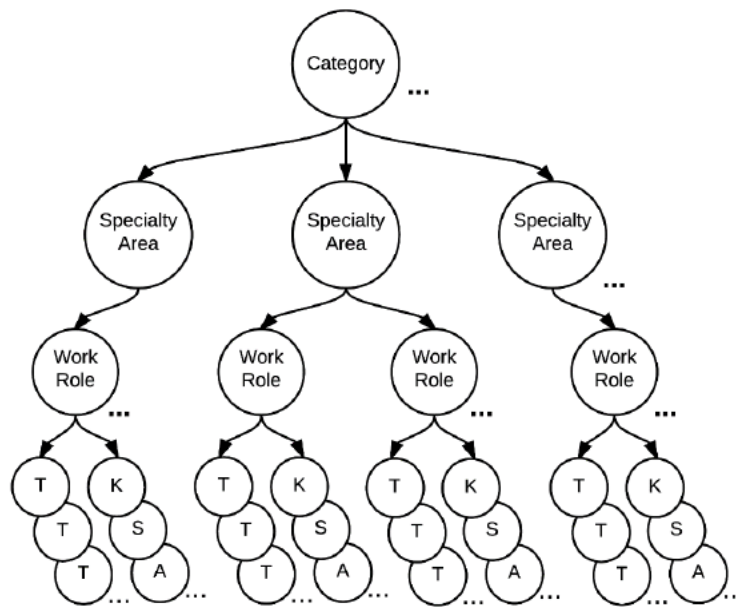


Figure 11. NIST NICE Framework organisation (Newhouse, 2017).

#### 7.2.2.7 NIST NICE Revision 1 (2020)

The revised version departs from its predecessor in significant ways. First, the document is merely the framework – that is, it does not describe actual tasks, knowledge etc., used by cybersecurity professionals; it merely defines the components of the framework and the relationships between those components. The key component of the revised version is the work role – which, it claims, “are a way of describing a grouping of work for which someone is responsible or accountable” (Peterson, 2020 p. 11).

Like its predecessor, the revision includes tasks; but unlike its predecessor, the revision explains that knowledge and skills should align to tasks. As can be observed in the following figure, the revision does not include abilities.

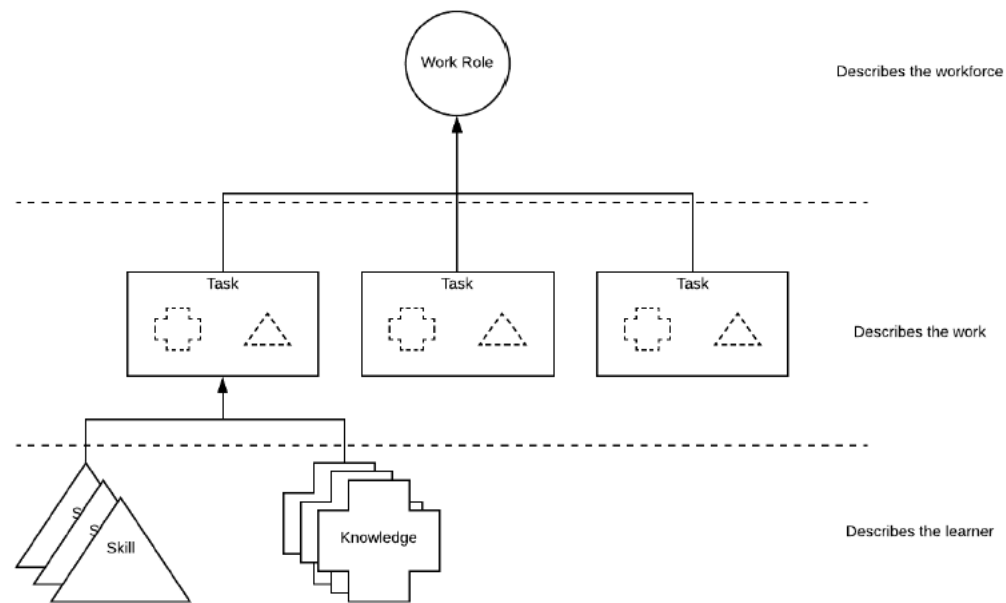


Figure 12. NIST NICE Revision structure (Peterson 2020 p.11)

A task is defined as “an activity that is directed toward the achievement of organisational objectives.” Task statements, it claims, should be “easy to read and understand, begin with the activity being executed,” and “do not contain the task objective”.

Knowledge is defined as “A retrievable set of concepts within memory.” Knowledge Statements, it claims, should “describe foundational or specific Knowledge”. It also explains that “multiple statements may be needed to complete a Task”, and “a single statement may be used to complete many different Tasks”.

Skill is defined as “The capacity to perform an observable action.” Skill Statements, it claims, “describe straightforward or complex skills”; moreover, “multiple Skill statements may be needed to complete a Task”, and “a single Skill statement may be used to complete more than one Task.”

The revision introduces the concept of “competency”, which it defines as “a mechanism for organisations to assess learners.” Competencies, it claims, are “defined via an employer-driven approach”, are “learner-focused” and, should be “observable and measurable.” The revision explains that competencies can be used to assess learners through a position description (as shown in the figure below) or through a credential.



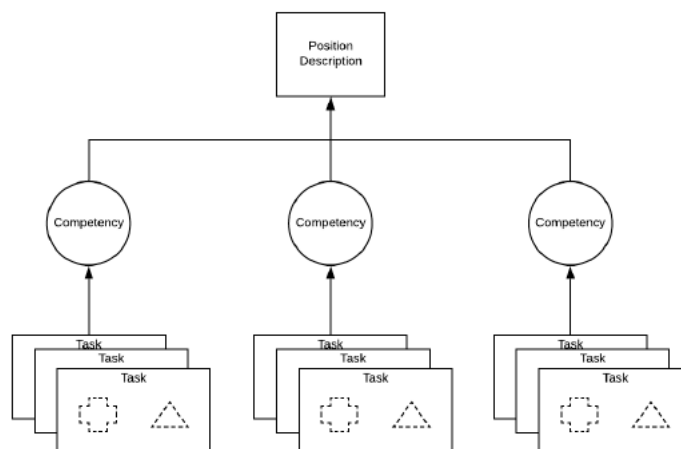


Figure 13. Competencies used as part of a position description (Peterson, 2020 p.7)

The revision further explains that “competencies consist of a name, description of the Competency, assessment method, as well as a group of associated TKS statements.” In essence, the competency allows the employer the flexibility to mix knowledge, skills and tasks in a way that meets their needs.

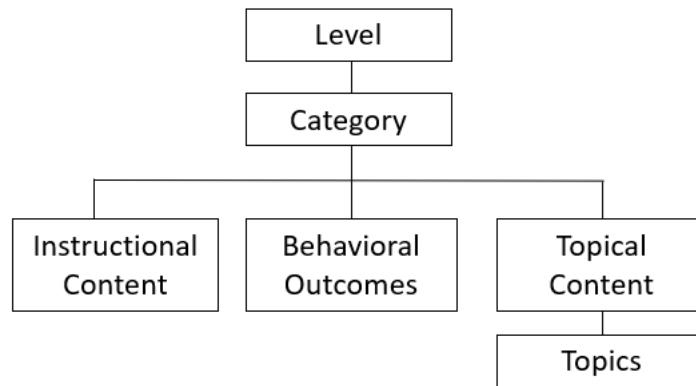
#### 7.2.2.8 NSA efforts

The National Security Agency, as the Secretariat for the Committee on National Security Systems (CNSS), directed the creation of several cybersecurity workforce development standards for professionals to work with classified information systems. These standards are represented in Instructions numbered 4011-4016.

##### 7.2.2.8.1 NSTISSI 4011

NSTISS Instruction 4011, “National Training Standard for Information Systems Security (INFOSEC) Professionals”, published in 1994 includes several elements of workforce development model – though it does this implicitly. The document describes two levels of knowledge: awareness and performance (National Security Telecommunications and Information Systems Security, 1994 p. 5.). The awareness level is intended for those who need a sensitivity to, awareness of, and working knowledge of INFOSEC principles and practices. The performance level is intended for employees who design, execute, or evaluate INFOSEC procedures or practices. The Instruction provides a category, which includes Instructional Content – intended for the instructor, and Behavioral Outcomes – intended for the student, and Topical Content – a list of topics within the category. While the Instruction

organises content into categories, it never formally defines what a category is. The researcher's interpretation of this model is shown in Figure 14.



*Figure 14. 4011 Structure (created by the author)*

#### 7.2.2.8.2 CNSSI 4012

Instruction 4012 “National Information Assurance Training Standard for Senior System Managers” (Committee for National Security Systems, 2004), includes basic literacy items which Senior Systems Managers need to know in order to proceed through the course material (these items are later used as subtopics). Then the Instruction lists Functions. The term Function is not formally defined within the document. Each Function has a brief description. Each Function contains what can best be described as topics (though topics are not otherwise defined within the document). Each topic is a noun or noun phrase. Each topic includes what can best be described as subtopics (though subtopics are not otherwise defined within the document). Each subtopic is a noun or noun phrase. Each subtopic includes what can best be described as learning objectives (though learning objectives are not otherwise defined within the document). Learning objectives are verb phrases, where the verbs correspond to Bloom’s verbs. The principal noun in these verb phrases is the subtopic noun. This relationship is described in the diagram below (created by the researcher).

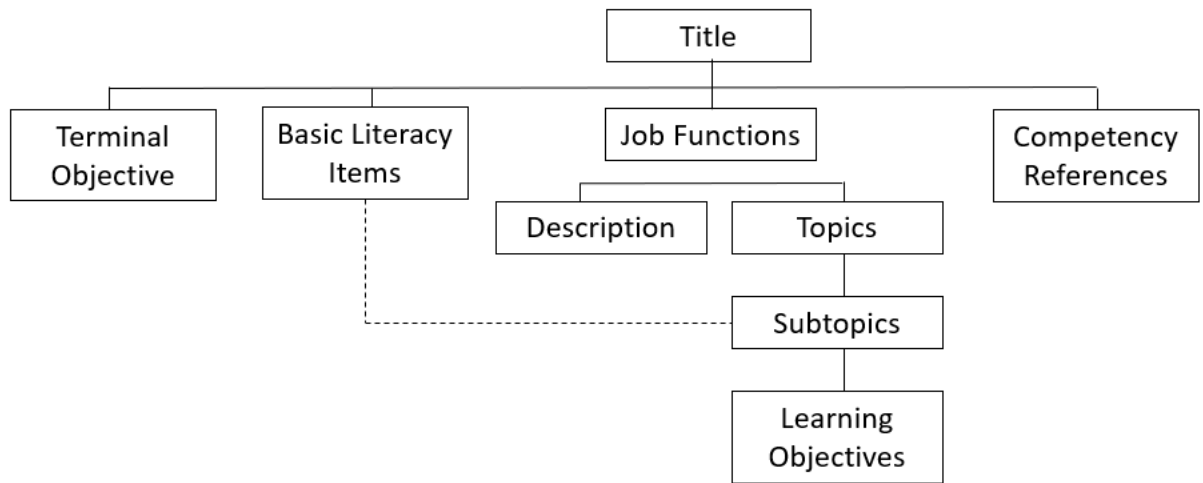


Figure 15. CNSSI 4012 structure (created by the author)

#### 7.2.2.8.3 CNSSI 4013

Instruction 4013 “System Administrator” (Committee for National Security Systems, 2004) adds levels beneath Terminal Objective: Entry, Intermediate, and Advanced. It implies that the entries identified in the characterisation of 4012 as “subtopics” are called “competencies”. It designates each competency as Entry, Intermediate, and Advanced. The designation aligns with whether the verb used aligns with low, middle, or upper levels of Bloom’s taxonomy. The Instruction does not have competency references, but does add ancillary Platform Specific Features/Procedures, which consist of knowledge and skills. The model can be seen in the figure below (created by the researcher).

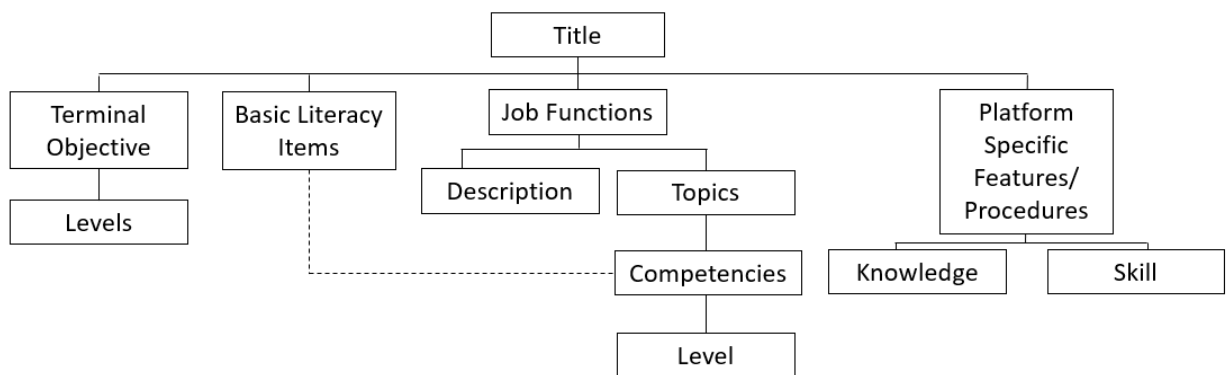


Figure 16. CNSSI 4013 structure (created by the author)

#### 7.2.2.8.4 CNSSIS 4014

CNSSI 4014 “Information Systems Security Officer” (Committee for National Security Systems, 2004) is somewhat simpler in comparison with 4012 and 4013 as it does not contain literacy items, competency references or platform specific features. It also does not include Topics under Job Functions.

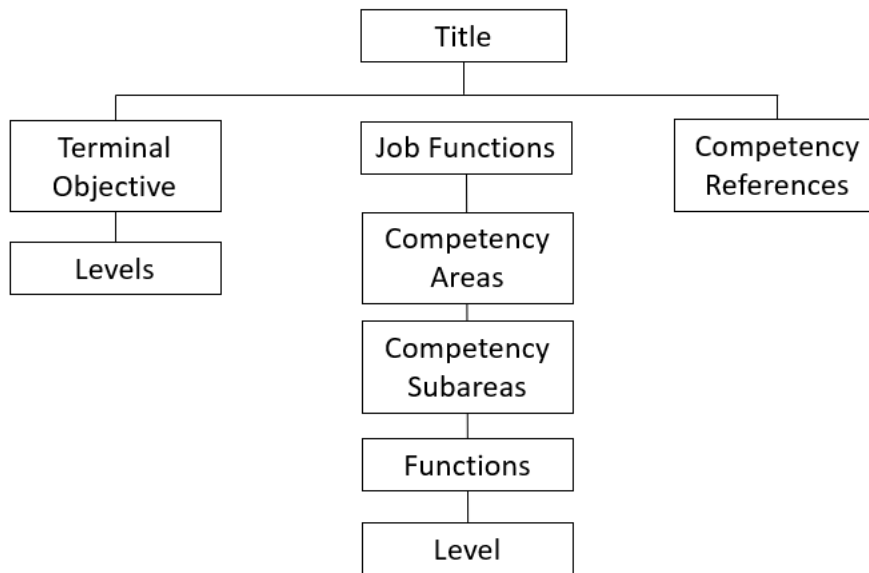


Figure 17 CNSSI 4014 structure (created by the author)

#### 7.2.2.8.5 NSTISSI 4015

NSTISSI 4015 (2000) Committee for National Security Systems “System Certifiers” is in some ways similar to 4012, and in other ways similar to 4013. It includes Competency references, but does not have levels for Terminal Objectives or Competencies. It has what might be described as “competency subareas” – categories beneath the competency statements into which the Functions, which are verb statements, are placed. It includes Concomitant Capabilities, which are composed of both noun and verb (gerund) phrases. These are categorised into Global Capabilities, and Specific Capabilities. A diagram of the model, created by the researcher, is presented below.

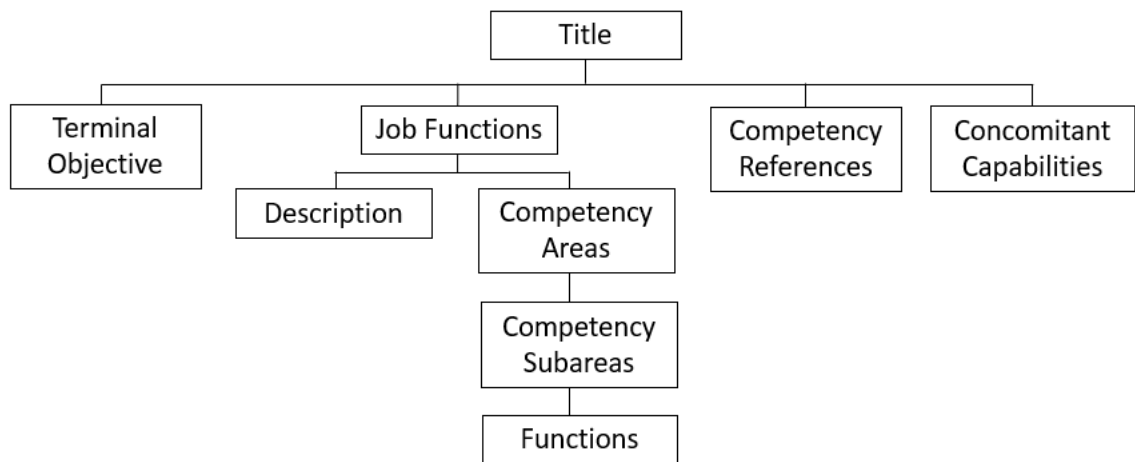


Figure 18. NSISSI 4015 structure (created by the author)

#### 7.2.2.8.6 CNSSI 4016

CNSSI 4016 “Risk Analysts” (Committee for National Security Systems, 2005), bears similarities with 4013 and 4014 in that it includes levels for terminal objectives and learning outcomes or functions. It is similar to 4012 and 4013 in its inclusion of basic literacy items; however, these literacy items do not correspond to topics as they did for 4012 or competencies as they did for 4013. It does not incorporate competency references, which are found in 4012, 4014, and 4015.

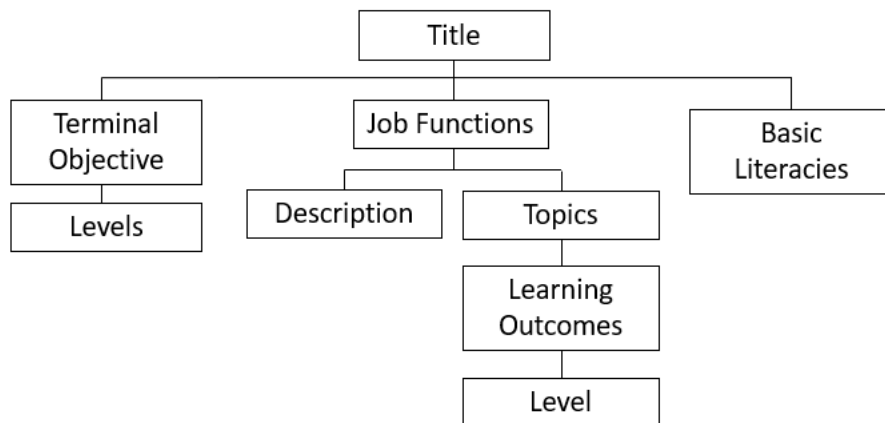


Figure 19. CNSSI 4016 structure (created by the author)

#### 7.2.2.8.7 NSA Knowledge Units

As of April 2021, while the Instructions are still in force, they are no longer the basis for the NSA Centers of Academic Excellence program. Rather, the function of guiding curricular content among participating universities is now contained within Knowledge Units

(Information Assurance Directorate, 2020). The Knowledge Units document defines outcomes, topics, and specialisations, as can be seen in Figure 20 below. The outcomes are almost all at the lower levels of Bloom’s taxonomy, meaning they don’t correlate well with tasks performed by cybersecurity professionals. The document links to the NICE framework at the Categories level (the 2017 framework’s most abstract level).

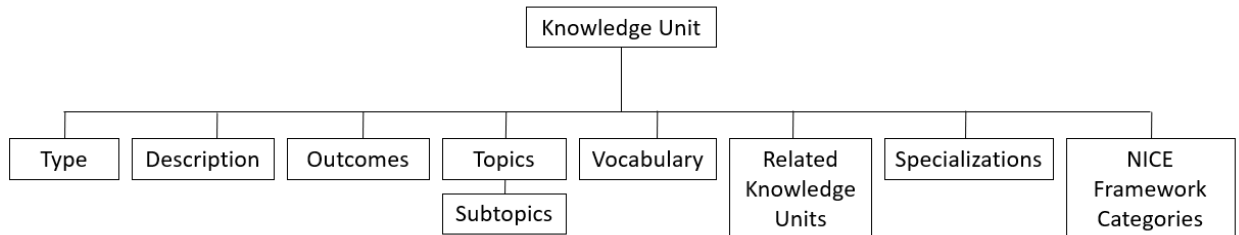


Figure 20. NSA CAE Knowledge Units 2020 structure (created by the author)

#### 7.2.2.9 Pacific Northwest National Laboratory

The Pacific Northwest National Laboratory Secure Power Systems Professional structure is ascertained by examining two reports (O’Neil, 2015 *Behavioral*) and (O’Neil, 2015 *Job*). The model is straightforward. It defines knowledge as “The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.” It defines skill as “The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.” It defines ability as “The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.” It is unique among the documents in that it maps the major responsibilities to NICE framework tasks, Energy Sector Cybersecurity Capability Maturity Model Objectives, and Applicable Certifications.

It is worth noting that the PNNL document defining the terms Knowledge, Skills, and Abilities (O’Neil, 2015 *Behavioral*), does not discuss how the provided list of KSAs was generated beyond the declaration that “The complete list of knowledge, skills and abilities required in each of the studied job roles was assembled into the Behavioral Interview Guidelines” (the Behavioral Interview Guidelines is the name of the document from which that quote was taken). The document does not describe the training theory on which the stated definitions are based.

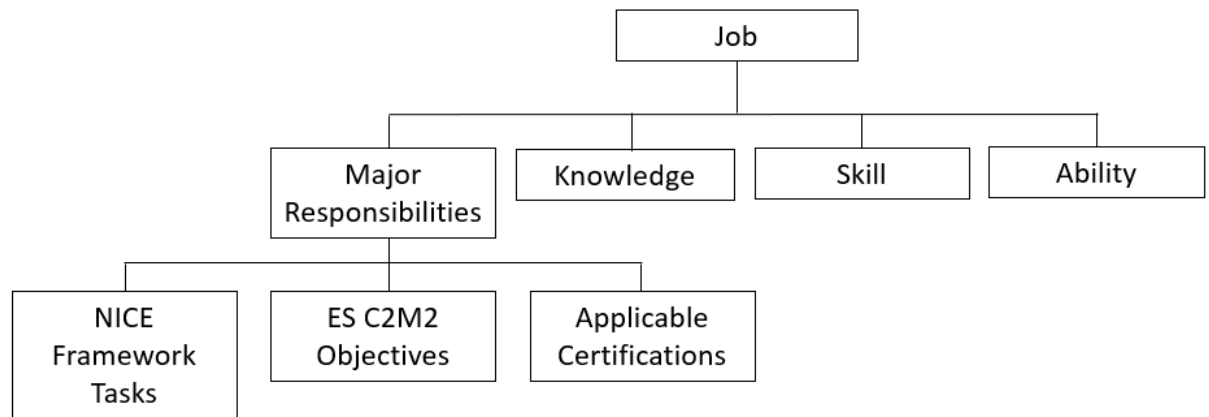


Figure 21. PNNL Secure Power Systems Professional structure (created by the author)

#### 7.2.2.10 Singapore SkillsFuture

The SkillsFuture framework includes Job Role titles and descriptions, and a list of Technical Skills and Competencies (TSCs) associated with each Job Role. Each TSC includes a Description – which is a single sentence that begins with a verb, and a Proficiency Description – which specifies how individuals perform that Description at five levels of proficiency. The TSCs in turn decompose to Knowledge and Abilities, also differentiated across five proficiency levels. An example TSC is provided in section 4.2.2.9 of this thesis.

When it comes to attitudes, the framework incorporates a list of five “desired attributes” that apply across all the 122 roles. The desired attributes are: Analytical, Team Player, Meticulous, Agile and Innovative, and Systems Thinker. The document provides a short sentence describing each characteristic (SkillsFuture, 2018, p.9).

The TSC Category and Range of Application fields show how specific competencies apply across sectors. Figure 22 (created by the researcher) displays these relationships.

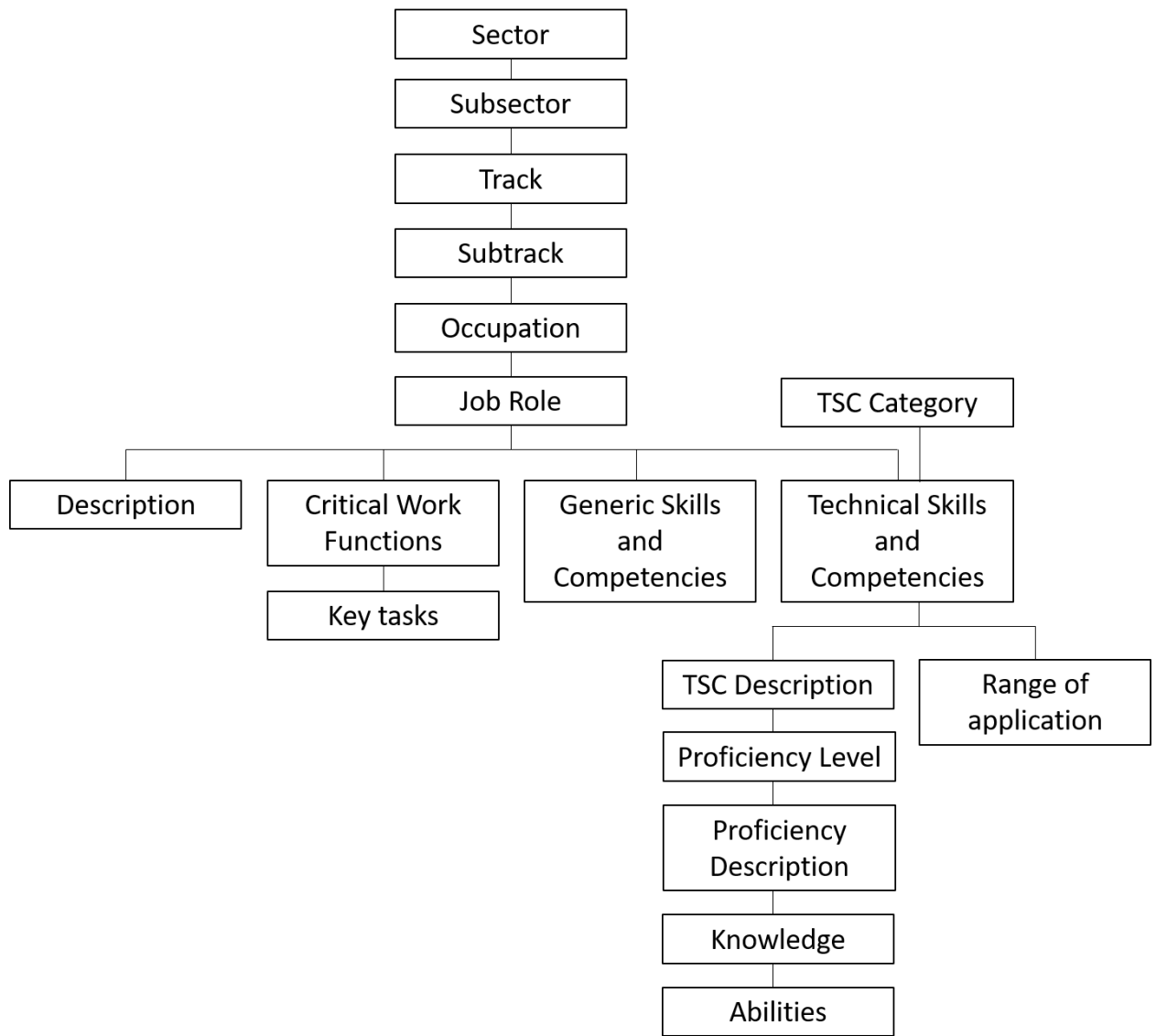


Figure 22. SkillsFuture Singapore structure (created by the author)

### 7.3 Results – Archetype Model

Based on a comparison with education and training theory and a review of the structure used in the guidance documents presented above, the following structure is proposed. The sections below refer to this structure as the Archetype model.



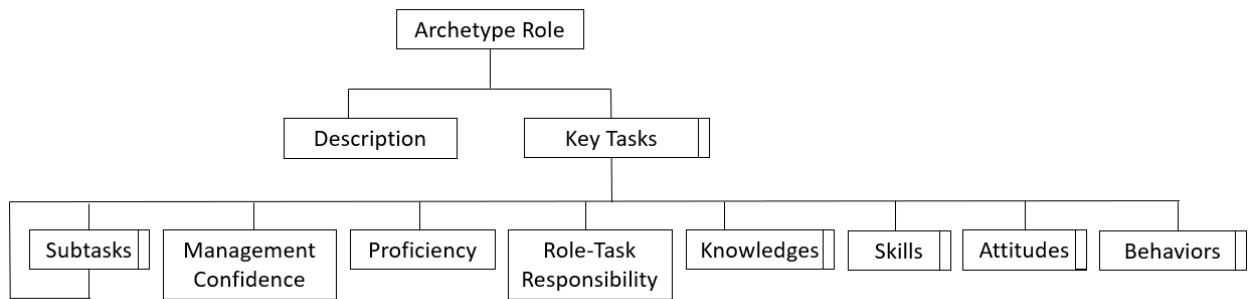


Figure 23. Archetype model structure (created by the author)

### 7.3.1 Archetype Role

A general category of cybersecurity employee, intended as notionally rather than specifically prescriptive. The archetypes discussed in this work are: Engineer, Technician, Manager, Analyst, and Researcher. The educator role was also identified though not elaborated. Other archetypes may also exist.

### 7.3.2 Role Description

A sentence or two that captures the essence of an archetype role, including insights into organisational relationships and tasks.

### 7.3.3 Key Tasks

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

### 7.3.4 Sub-tasks

An identifiable step in accomplishing a task. Like a task, a sub-task is a verb statement that may require specific knowledge, skills, and attitudes. Sub-tasks may be composed of additional sub-tasks, as indicated by the recursive line near the left edge of the Archetype model diagram in Figure 23.

### 7.3.5 Knowledge

Cognitive function, a noun or noun-phrase. Knowledge may extend across many or all archetype roles, as in the case of the industrial cybersecurity knowledge elaborated within Chapter 5 of this thesis. Knowledge may be grouped however convenient for purposes of workforce development. For example, an analyst may have industrial cybersecurity knowledge and additional specialised knowledge dealing with the electric sector as well as specialised knowledge pertaining to his or her company and facilities. Knowledge supports the tasks, but exists independent of them.

### **7.3.6 Skill**

Psychomotor function, requiring or implying corporal activity. Skills are verbs or verb phrases. Like knowledge, skills may also have various levels of specialisation.

### **7.3.7 Attitude**

Emotional function, requiring or implying emotional control. Emotions are generally nouns, but may include additional description. Attitudes will occur less frequently than Knowledges or Skills, but should be identified wherever possible. Attitudes may also be specialised.

### **7.3.8 Behavior**

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. They are the “how”, “when”, “where”, and “with whom” – each coupled with “why” – an expert performs a task or sub-task. Behaviors, like knowledges, attitudes and behaviors may also be specialised.

### **7.3.9 Proficiency**

Elements of selection, thoroughness, consistency, and timeliness with which an individual performs a task or sub-task. Selection is the ability of the individual to choose an effective technique. Thoroughness is the inclusion of all necessary and useful components. Consistency is performing the task the same way. Timeliness is the speed of performance. These components are not mutually exclusive, but are mixed together to fit a complex context. They are useful in richly assessing performance.

### **7.3.10 Role-task responsibility**

A determination as to whether an archetype would have primary responsibility, shared primary responsibility, or supporting responsibility for the task. Primary responsibility means that the archetype role normally accomplishes this task alone. Shared primary responsibility means that the task could not be accomplished without the aid of expertise provided by a differing archetype role. Supporting responsibility means that the individual with this archetype role contributes to a task for which another archetype is primarily responsible.

### **7.3.11 Management confidence**

An organisation’s official recognition of individual responsibility for a task within a management context. This recognition is communicated through specialised verbs such as,

“helps”, “applies”, “supervises”, “resolves”, “evaluates”, and “sets direction” for a specific task.

#### **7.3.12 Specific content**

Specific content refers to items of increasing content related to sector, process, employer, and facility added to Key Tasks, Subtasks, Knowledges, Skills, Attitudes and Behaviors. In the diagram, this is represented by an empty box within each of these components.

### **7.4 Analysis**

This proposed workforce development Archetype model incorporates components found variously in the candidate guidance, and some not found in the candidates. This section compares the proposed model with the content of the candidates, explaining why key choices were made. It then discusses validity of the result.

#### **7.4.1 Comparison with models used by candidate educational guidance**

This section compares the structure of the Archetype model with the structure found in the various guidance documents/efforts.

##### ***7.4.1.1 Comparison with ABET***

As ABET does not advance a workforce development model, there is little to compare. Program specific criteria correlate with Key Tasks in the Archetype model in some instances.

##### ***7.4.1.2 Comparison with ENSIA***

The approach taken by ENSIA is similar to that taken this thesis in that it focuses on all industrial cybersecurity professionals. Like Chapter 5 of this thesis, it treats general knowledge separately from professional roles. However, it does not delve into tasks. The ENSIA structure does not incorporate components comparable with Management Confidence, Proficiency, Role-Task Responsibility, Attitudes or Behaviors.

##### ***7.4.1.3 Comparison with GIAC***

GIAC structure is essentially identical to the ENSIA structure from which it was drawn, meaning its comparison with the Archetype model is similar. The GIAC document includes an “ICS-Related Job Role Mapping” graphic not present in the ENSIA work. This graphic introduces “competency levels”. This idea is similar to Proficiency in the Archetype model, though it provides no insight into how one can distinguish between the competency levels. The definition of Proficiency within the Archetype model does provide several ways

to characterise Proficiency. In the Archetype model, Proficiency refers to tasks, while in the GIAC graphic, Competency Level refers only to Knowledge. The top competency level is “technical leader” – a term which the graphic does not define, and which focuses on an individual rather than characterising their level of knowledge. The bottom of the graphic includes “job roles” which range from “use”, through “support and maintain” and into “design”. This seems to align roughly with Bloom’s taxonomy.

#### **7.4.1.4 Comparison with ISA DOL Automation Competency Model**

One key difference between the ISA DOL Model and the Archetype model is that the ISA DOL model deals with competencies – which are groupings of knowledge, skills, and abilities, where the Archetype models does not lump these subcomponents together. Moreover, the ISA DOL model uses “knowledge”, “skills”, and “abilities” where the Archetype model uses “attitudes” rather than “abilities”.

ISA DOL Critical Work Functions are similar to Key tasks in the Archetype model in that they can include verb statements that describe things a professional does. However, they can also describe things a professional needs to know – such as “understands”. The Archetype model makes a clear distinction.

The ISA DOL structure’s incorporation of Technical Content Areas and Technical Content aligns more closely with the Knowledge Categories discussed in Chapter 5 and Specific Knowledge Items discussed in Chapter 6 than it does with the Knowledges, Skills, Attitudes, and Behaviors in the Archetype model.

The ISA DOL model generally does not address “attitude”. The document provides limited content that could be considered relevant for the category of “attitude”. For example, Section 2.5 Communication – Listening and Speaking provides instructions on how to listen effectively, such as “consider other viewpoints”, but does not otherwise use emotional language. Section 3.4, “Marketing and Customer Focus” includes “be pleasant, courteous, and professional when dealing with internal or external customers”, but that is the extent of emotional guidance. Literature has recently highlighted the importance of emotionally-oriented content in engineering education (Elegbe, 2015; Mitrović Veljković, 2020; Lappalainen, 2015).

The ISA DOL model does not address proficiency, management confidence, or role-task responsibility, which are covered in the Archetype model.

#### **7.4.1.5 Comparison with JTF**

The Joint Task Force concerns itself with primarily knowledge – similar to the concepts advanced in Chapters 5 and 6 in this thesis. The document relies on the original NIST NICE framework to link its Outcomes to the NICE Work Roles. As these Outcomes deal primarily with the lower levels of Bloom’s taxonomy, they have no equivalent in the Archetype model.

#### **7.4.1.6 Comparison with NIST NICE 2017**

As NIST NICE 2017 framework (Newhouse, 2017) is the most widely known workforce development framework for cybersecurity, it is worthwhile to carefully describe key differences between it and the Archetype model. Firstly, NIST NICE’s primary organisational component is the security category – which are based on the NIST cybersecurity framework (Securely Provision, Operate & Maintain, Oversee & Govern, Protect & Defend, Analyze, Collect & Operate, and Investigate); in the Archetype model, it is the job role. It should be noted that because work roles commonly span the NIST framework categories, the categories convolute organisation.

Secondly, while the specialty areas used in NIST NICE 2017 seem like a useful distinction within each security category, the specialty areas, like the security categories, convolute organisation. Consequently, the Archetype model eliminates the specialty areas within each category to preserve flexible extensibility.

Thirdly, NIST NICE 2017 keeps KSAs separate from tasks. While using each KSA as an independently cataloged building block allows the KSAs to be adopted into roles as desired, the Archetype model recognises that significant value to all stakeholders lies in the ability to identify specific key KSAs for key tasks and hence, maintains the linkage.

Fourthly, the NIST NICE framework uses the term “ability”, and the Archetype model uses “attitude”. Attitude 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), 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”).

Fifthly, where NIST NICE 2017 does not incorporate the idea of sequenced decomposition of tasks, the Archetype model 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 prioritising the amount of time and attention to dedicate to a task or concept.

Finally, the Archetype model 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”. In the Archetype model, 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 Archetype model as “expert behavior”. This difference, like those above, is of significant value for instructional design.

#### ***7.4.1.7 Comparison with NIST NICE Revision 1***

The NIST NICE revision (Peterson, 2020) has many similarities with the Archetype model advanced herein. NICE Revision 1 Work Roles roughly correspond to archetypes; tasks and knowledge within the revision are nearly identical to the same terms in McBride. There is, however, some difference related to skills. In the Archetype model, a skill is specifically psychomotor (controlling one’s body), and begins with a verb. In the NICE Revision, the skill may or may not be psychomotor, and is stated as a gerund form of a verb, such as “skill in conducting queries and creating algorithms” (p.10). If they were not stated as gerunds, these skill statements would be similar to tasks and subtasks in the Archetype model (verb-centred statements that describe the actions a worker takes). The way the word “skill” is used in these statements leaves one wondering what the skill is – because it is not expressed as “the skill of”, which would designate the task or sub-task, but it is expressed as “skill in”, bringing to mind that the skill itself is not the ability to do the task (that is, carry out the verb) but the way the task is completed. It leads one to believe that there must be additional detail inside of that skill that the NIST Revision 1 model leaves unexpressed.

For example, within the NIST Revision 1 model, one might consider the competency of “playing offense in basketball”. A skill statement within that competency may be “skill in shooting a basketball”. This leaves one wondering what it is about shooting a basketball that is skillful. If a student bounces the basketball off their knee as part of that competency, is that

skillful? No, and why not? Because it is not effective. It is not a proven technique used to accomplish an objective, that can be used at will.

In the Archetype model, the concept that describes the “how”, “when”, “where”, and “with whom” of the task or sub-task, each coupled with an explanation of “why” is called a behavior. In short, the behavior characterises expert performance.

In the Archetype model, expert performance is then justified by proficiency – that is, the selection, thoroughness, consistency, and timeliness with which the individual carries out the task.

If one purpose of the revised NIST NICE framework is to encourage learners to align skills with tasks, then having both – one as a verb, and the other as a gerund of a verb – seems redundant. The revised NIST NICE framework even recognises this, explaining, “Skill statements describe what the learner can do, and Task statements describe the work to be done. Therefore, it is important to separate the language used between Skill statements and Task statements and to use terms that facilitate observability and assessment of the learner” (p.5). This explanation is strange because it could be interpreted as instructing those who follow this guidance to intentionally write hard-to-observe task statements! In short, the framework authors clearly foresaw that skill statements and task statements would use identical verbs.

The Archetype model does not advance competencies, but allows the employer the flexibility to determine their own competencies – consistent with NICE Revision 1 – using the defined components.

#### ***7.4.1.8 Comparison with NSA approach***

NSTISSI 4011 (National Security Telecommunications and Information Systems Security, 1994) provides a knowledge standard for classified information system users and INFOSEC employees. The list of topics and topical content in 4011 is functionally equivalent to the categories and topics advanced in Chapter 6 of this thesis.

The documents numbered 4012-4016 (Committee on National Security Systems, n.d.) provide minimum training standards for certain roles. Of the documents reviewed in chapter 7, they are the only documents in the set reviewed to overtly make the claim of being “standards”. Additionally, they are the only documents to include “terminal objectives” -- which are intended for use by training providers. It should be recognised that while the documents in the series include many similar elements, the terminology used and

relationships presented are not uniform across all. This can be interpreted as a signal that there is an element of art in the formulation of a workforce development model.

In the NSTISS/CNSS documents, the Title roughly aligns to Archetype Role in the Archetype model. The former (Title) is specifically prescriptive – that is to say that government agencies are expected to have individuals who possess that exact title. The latter (Archetype Role) is only notionally prescriptive – as that exact title may not exist within an employer organisation.

Job Functions in the NSTISS/CNSS Instructions are roughly equivalent to Key Tasks in the Archetype model. The Basic Literacy Items and the Competencies to which they link correspond roughly to Knowledge and Skills in the Archetype model. The Levels in the NSTISS/CNSS Instructions correspond in some ways to Management Confidence in the Archetype model – connoting the level of supervision required to perform a competency. However, the NSTISS/CNSS Instructions correlate this competency level to more advanced verbs in Bloom’s taxonomy. The Archetype model decouples Bloom’s taxonomy, and instead uses the concept of Proficiency to describe how well the individual performs the task.

4013 and 4015 include lists of knowledge and skills that do not fall directly under Key Functions within the documents. This is reasonable given that knowledge and skills can be tedious and repetitive to correlate to specific tasks or functions, and may be used across numerous tasks.

The Instructions do not provide insight into emotional requirements for performing tasks effectively – which the Archetype model calls “Attitudes”. Nor does it offer insight into how and why experts perform a task the way they do – which the Archetype model calls “Behaviors”.

#### **7.4.1.9 Comparison with PNNL**

The PNNL structure has several strong similarities with the Archetype model (O’Neil, 2013; O’Neil, 2015 *Job*; O’Neil, 2015 *Recruiting*). The PNNL Job is functionally equivalent to the Archetype role of the Archetype model; but, the PNNL Jobs are much more specific categories than the McBride Archetypes. PNNL Major Responsibilities is functionally equivalent to McBride Key Tasks. PNNL relies on NICE Framework Tasks for greater detail regarding Tasks; and, these are roughly equivalent to Subtasks in the Archetype model. PNNL Knowledge, Skills and Abilities are all verb statements that align closely to Bloom’s



taxonomy where Knowledge is a low level and Abilities are high level. Archetype model does not overtly align to Bloom's taxonomy. Because PNNL Skills and Abilities are verb statements, they are also similar to McBride Tasks. PNNL does not use any term to cover psychomotor or affective domains.

PNNL asserts that Knowledge, Skills, and Abilities can be measured: Knowledge by depth of understanding, Skill by degree of reliability, and Ability by extent of Skill transfer. The "degree of reliability" measurement of PNNL Skill maps as part of McBride Proficiency; however, McBride Proficiency suggests a more-robust set of measurement techniques for its Tasks.

Because PNNL focuses on a single sector – electric – it also incorporates some sector-specific content by default. It did not attempt to describe a model whereby content specific to other sectors may be incorporated into its Model. Nor does it include a way to include process-, organisation-, or facility-specific content.

PNNL does not include equivalent concepts as McBride Management Confidence, Role-Task Responsibility, Skills (which for McBride are psychomotor), Attitudes, or Behaviors.

#### ***7.4.1.10 Comparison with SkillsFuture Singapore***

The SkillsFuture framework (SkillsFuture Singapore, 2018 *Skills*); begins at a higher level than the Archetype model – extending five levels up to "Sector". The Archetype model deals with sector as an add-on component to Key Tasks, Subtasks, Knowledges, Skills, Attitudes and Behaviors.

The SkillsFuture framework does not deal with cybersecurity-specific job roles, where such job roles are the entire purpose for the Archetype model. This is an important distinction when considering the overarching goal of enhancing the security of industrial control system environments. Cybersecurity focused individuals may be expected to lead out in securing these environments; however, individuals with primarily non-cybersecurity roles, such as industrial process operators, purchasing officers, compliance personnel, a variety of engineers and technicians, and managers will make decisions that influence – or even determine – the security of the system. These individuals must not be overlooked for security and workforce development purposes. Some of them are likely to need specific education and training to perform certain tasks securely – education and training that transcends basic

awareness and literacy. The SkillsFuture approach is the most robust of all the frameworks examined in this regard – because it emphasises that cybersecurity should be a component of job roles that are essentially non-cybersecurity in nature. The Archetype model does not provide an analogous concept.

While the TSC Category and Range of Application fields show how specific competencies apply across sectors, this approach is not as flexible as the sector specific component of the Archetype model, which allows for sector specific cybersecurity content.

Critical Work Functions and Key Tasks in the Skills Future structure correspond roughly to Key Tasks and Subtasks in the Archetype model.

SkillsFuture uses the term “Proficiency” in a way that equates to “Management Confidence” in the Archetype model. Skills Future does not offer a counterpart to McBride’s “Proficiency”. The SkillsFuture structure does not include “Attitudes”.

#### **7.4.2 Validation**

The Critical paradigm, which is the principal paradigm of this research, allows the researcher to be closely involved in the creation of the results as long as the researcher discloses potential biases and perspectives, collaborates with participants, and/or incorporates input from peer debriefing.

In this case, the research methodology involved drawing from key and well-established workforce development literature, including Bloom and Mager, and then engaging in a critical and comparative review of 16 different structures for workforce development models applicable to cybersecurity.

The variety of documents, coming from differing types of organisations, located in disparate countries, over the past 25 years, is a respectable cross-section. While there were many similarities across the documents, there were also great differences. These differences and the accompanying analysis show that even though the Archetype model does not adopt any of the 16 structures in its entirety, it would be difficult to claim that the Archetype model is patently invalid.

The weakness of this approach is that the researcher is not writing this thesis on the topic of workforce development models. Hence the work did not involve a detailed literature review of that important topic, and there is doubtlessly more that could be considered.

#### **7.4.2.1 *Researcher reflexivity***

My exposure to workforce development frameworks began with my work as a graduate student in the National Information Assurance Training and Education Center (NIATEC) at Idaho State University from 2004 to 2006. During that time, I helped create educational materials dealing with cybersecurity. I learned about Bloom's taxonomy as I wrote my first learning objectives. I learned about the CNSS and NSTISS Instructions as I mapped both the materials I created and the courses I was taking to those instructions.

At that time, I was merely doing as instructed. I did not wonder whether an improved structure might exist. It wasn't until I took an Instructional Design Course as a graduate student in Spring 2020 that I was introduced to Mager. I was impressed by his straightforward approach and his assertion that it is not entirely complicated to perform a job task analysis. I was deeply impressed with his emphasis on relevant practice. My interpretation of what a workforce development model ought to include was strongly influenced by his work.

Mager spends time explaining "Goal Analysis" which deals primarily not with what individuals are trained to do, but with how to do things effectively. Some of these items are linked to how an individual feels about their tasks.

At roughly the same time as I was exposed to Mager, I read a book and participated in several formalised training sessions (as an instructor in my department) around the idea of emotional intelligence. As I reflected, I recognised that Bloom's affective domain was originally intended to deal with emotions, but that somehow, over time, emotions had been taken out of the formalised educational construct. Hence, emotions (or attitudes) almost never appear in learning objective statements. This is reasonable because, conventional wisdom holds that learning objectives should be observable and measurable, and learner's emotions are difficult to measure.

Then I started thinking about the way I approach my own work, and the way the true experts I know approach their work – there is a clear emotional aspect that I believe makes them effective in that particular line of work. So, I determined to include Attitudes. I recognised there would be vastly fewer attitudes than knowledges or skills, but I believe that we could empower instructors and students by including a component that Bloom originally identified, but that many instructors have been taught to neglect.

Then I began to consider the people I know who are exceptionally good at what they do. Drew Robinson of iSIGHT Partners is a fantastic example. His attention to detail, and his ability to recognise patterns in technical data – as described in Andy Greenberg’s book “Sandworm” about Russia’s military and security units tasked with carrying out cyber-attacks with physical consequences – is astounding (Greenberg, 2019). I am not sure how many people in the world could have discovered what he discovered.

About that same time, I had an email conversation with Corey Schou about behaviors – which he described as expert habits of practice. I thought, while we cannot train everyone to become an identical expert, we can certainly identify experts. We can also ask them about how they do their work. We can ask them what they do different – what they think sets them apart. And we can ask them why they do it that way. Their answers are likely to be extremely valuable and insightful, and may help instructors identify techniques and create relevant practice opportunities. Hence, I added Behaviors to the model.

Further contemplation led me to recognise that cybersecurity is a team sport. The nominal group technique effort described in Chapter 5 identified five archetype roles. Why is it that the 16 models I examined do not openly describe the relationships that need to exist between the roles relative to their key tasks? As a result, I decided to add Role-Task Responsibility.

As I looked over the 16 documents, I recognised that the various authors shared a desire to classify how good someone was or how difficult a task was to perform. To address this, many of the approaches at least implicitly aligned to Bloom’s taxonomy of verbs along levels of complexity and abstraction. SkillsFuture and SANS efforts provide good examples of this. SkillsFuture called this difference “proficiency levels”, and SANS called it “competency levels”. It seemed to me that there were two separate challenges that the models struggled to address: 1) how much trust an organisation could have in an individual relative to a task; and, 2) how good an individual was at doing a task. The difference is nuanced, but significant.

I reasoned that an individual may be very good at doing a specific task – even a highly complex and abstract cognitive task, but not necessarily good at evaluating how others perform the task. I recognised that in my own professional experience there had been managers – like a road construction foreman, or mail-room manager – who had done every single job on the crew and could instruct just about anyone on every aspect of every task; but,

there had also been managers – like a director of synthesis – that would not be able to explain much about how an intelligence analyst drew key conclusions. It seemed to me that the way these workforce models interpreted Bloom frequently conflated the two. I decided to deal with each issue separately – by introducing 1) Proficiency and 2) Management Confidence.

The great benefit of introducing Proficiency is that it empowers the employer to think about measurement in terms of primarily quality and speed. This approach is also a greater value to instructors because they can more specifically align their content and characterise their effectiveness relative to a particular task.

The final piece of the puzzle was to ensure the extensibility of the model. This would require 1) a way to add additional layers into the model; and, 2) to move from the general to the specific. In order to address the first, the visual model includes a looping line to the left of the Subtasks box; and, to address the latter, the visual model includes an empty box within Key Tasks, Tasks, Subtasks, Knowledges, Skills, Attitudes, and Behaviors. This empty box allows these items or elements thereof to be designated as “specific”. Specificity can exist at the sector, process, organisation, or facility levels.

## **7.5 Conclusion**

As can be seen from the foregoing, the various organizations interested in promoting formalized cybersecurity workforce development have defined (either implicitly or explicitly) their own models and lexicons – and some organizations have developed more than one.

The result of the effort described in this chapter resulted in a proposed workforce model, that 1) was justifiable, 2) was as simple as possible, and 3) could be leveraged to fit a variety of needs. It is foreseeable that the Archetype model could be used to help assess and describe workforce readiness for cybersecurity in general. It intuitively suggests personnel certifications for attainment of increasingly specialised knowledge, skills and tasks. It would also lend itself for assessment of workforce cybersecurity preparation across a facility, organisation, or archetype role.

Achieving implementation of the proposed Archetype model will remain a significant challenge. While such implementation pushes beyond the scope of the major question addressed in this thesis, ideas for its achievement are incorporated into sections 9.1 and 9.7.4.

## **8 INDUSTRIAL CYBERSECURITY TASKS**

### **8.1 Problem**

Recalling that the key research question treated in this thesis is: “What is the foundation for the formal preparation of industrial cybersecurity professionals?” and having identified: 1) the criteria for such a foundation (see Chapter 4); 2) five archetype roles these professionals fill (see Chapter 5); 3) the key knowledge categories needed by industrial cybersecurity professionals (see Chapter 5); 4) specific contents aligned to those knowledge categories (Chapter 6); and a workforce development model to follow (Chapter 7); the next object of investigation became: “what tasks do individuals with the identified archetype roles perform?”

### **8.2 Research Design**

A first step in research design is to characterise the research questions. In this case, the question is relatively open-ended. Because industrial cybersecurity archetypes are a key innovation of this line of research, literature does not exist to describe the tasks they perform. The research would require a qualified expert to describe the tasks they perform.

A survey would not be an optimal choice because this is an open-ended question. A questionnaire would be a better than a survey, because it would allow the participants to express themselves freely in a documented format. However, the quality of responses provided on a questionnaire can vary greatly; and, a questionnaire does not allow the researcher to directly interact with the participant in search of additional insight.

An interview would provide a deeper level of insight and interaction. Interviews are time consuming because they occur one-on-one. They require significant effort to code and compare among respondents, and because they occur at different times and under different circumstances are prone to variability.

Like the interview, the small sized focus group is effective at dealing with open ended questions. It allows the researcher to prompt for additional insight, and allows the participants to spark ideas from one another because they may have similar experiences. A focus group may produce better insight than an interview in cases where the expertise of the participants differs from the expertise of the researcher – meaning the other participants’ perspective can compensate for the researcher’s lack of knowledge and understanding.

The nominal group technique works well for coming up with discrete new ideas, but not for probing specific expert insight. Moreover, the method is not effective with fewer than

five participants, because the participants may be able to figure out who is who in their written responses (especially if they have worked with one another previously), thus diminishing the value of anonymity.

For these reasons, the researcher determined to run five collaborative focus group sessions – one with qualified experts in each of the archetype roles.

It is interesting to note that despite the advantages of the focus group reviewed above, the candidate documents/efforts (from chapter 4) that identify roles and provide tasks – ISA (tasks but not roles), NICE (tasks and roles), PNNL (tasks and roles), SkillsFuture (tasks and roles) – never mention the focus group among the methodologies used to generate their content.

In order to find qualified collaborators, the researcher turned again to the Idaho National Laboratory, asking that managers identify two or three qualified collaborators per archetype role. The INL readily agreed.

The collaborators met with the researcher to describe a baseline set of tasks for each role. Ten of the eleven collaborators differed from those who participated in the nominal group technique method which advanced the concept of archetype roles and five of the knowledge categories. The exception was St. Michel who also served as an expert on the engineer archetype focus group.

- The INL provided three technicians with a combined 65 years of experience in process operations, process control, and control instrumentation across nuclear, oil, and natural gas industries. The three had experience with cybersecurity, but only one had a major focus on industrial cybersecurity.
- Two engineers totaled 58 years in engineering across chemical and nuclear applications with about 20 years total combined experience in industrial cybersecurity.
- The two analysts totaled 17 years of analytical work, about 15 of those focused on industrial cybersecurity.
- Two researchers totaled 24 years in research, about 19 of those specifically related to industrial cybersecurity.
- Two managers had 14 years total cybersecurity management experience, about 8 specifically related to industrial cybersecurity management.

The listing of tasks to be performed as part of a job role is generally called a “job task analysis”. Many publications describe methodologies for conducting such analyses (Jonassen 1998). A comparative review by Levine (1983) concluded that there is no single best methodology, and that combining methodologies was worth the additional effort.

Of particular interest were the job tasks guidance provided by Mager (1997), Bell (2010), and Hoffman (2005). The researcher found the practical approach advanced by Robert Mager to be most compelling (Mager, 1997 pp. 55-72).

The protocol used for the focus group sessions can be found in Appendix

### 8.2.1 laborallaborallaborallaborsession details

The following table presents key details of focus groups sessions.

*Table 17. Details of focus group sessions*

<b>Archetype Role</b>	<b>Date</b>	<b>Location</b>	<b>No. of Collaborators</b>	<b>Gender of participants</b>	<b>Approx. Combined Years in Archetype</b>
Technician	June 25, 2019	In person University Place	3	3 males	20
Engineer	July 18, 2019	In person University Place	2	2 males	20
Analyst	June 25, 2019	In person University Place	2	1 male 1 female	15
Manager	May 26, 2020	Virtual	2	2 males	8
Researcher	May 6, 2020	Virtual	2	1 male 1 female	20

The researcher listened carefully, took notes, asked additional clarifying questions, read the notes back to the participants. The session lasted approximately two hours. On his own, the researcher further categorised the results and standardised the language, then sent the final results to the participants for review via email, and incorporated comments received.



### 8.3 Results

The following subsections present the description and key tasks identified for each archetype role.

#### 8.3.1 Archetype Role: Industrial Cybersecurity Engineer

##### 8.3.1.1 Description

The Industrial Cybersecurity Engineer works within the engineering or operations 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.

##### 8.3.1.2 Tasks

Table 18. Industrial Cybersecurity Engineer tasks.

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

### 8.3.2 Archetype Role: Industrial Cybersecurity Technician

#### 8.3.2.1 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.

#### 8.3.2.2 Tasks

Table 19. Industrial Cybersecurity Technician tasks.

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

### 8.3.3 Archetype Role: Industrial Cybersecurity Analyst

#### 8.3.3.1 Description

The Industrial Cybersecurity Analyst works among enterprise cybersecurity personnel to contextualise and synthesise 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.

#### 8.3.3.2 Tasks

Table 20. Industrial Cybersecurity Analyst tasks.

Task No.	Task
1	Stays abreast emerging developments relevant to industrial cybersecurity
2	Dissects analytical requests
3	Collects information

4	Synthesises information
5	Analyses threats, vulnerabilities and consequences pertinent to industrial environments
6	Produces analytical products
7	Presents results
8	Proposes new analytical work

### 8.3.4 Archetype Role: Industrial Cybersecurity Researcher

#### 8.3.4.1 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 they produce must meet requirements for clarity of technical content.

#### 8.3.4.2 Tasks

Table 21. Industrial Cybersecurity Researcher tasks.

Task No.	Task
1	Understands system
2	Designs and conducts tests
3	Discovers vulnerabilities
4	Develops adversarial perspective
5	Recommends mitigations
6	Documents and reports findings

### 8.3.5 Archetype Role: Industrial Cybersecurity Manager

#### 8.3.5.1 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.

#### 8.3.5.2 Tasks

Table 22. Industrial Cybersecurity Manager tasks.

Task No.	Task
1	Prioritise efforts
2	Describe requirements per effort
3	Obtain and manage budget
4	Build the team

5	Run and improve the industrial cybersecurity program
---	--

## 8.4 Analysis

The focus group sessions resulted in significantly more tasks for the Engineer and Technician archetype roles than for Analyst, Manager and Researcher. A preferred explanation is that those former roles have a more direct influence on the security of the industrial environment, and hence require greater detail. In addition, it is foreseeable that the 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 tasks themselves.

It is possible, nevertheless, that this difference is the result of other factors, such as date, location, gender, number of collaborators or years of experience, as indicated in Table 17. Interestingly, there appears to be no correlation between the number of tasks identified for each archetype role, and any of these variables. For example, the Technician session and the Analyst session occurred in person, on the same day, in the same location, yet the Technician session produced 13 tasks, and the Analyst session produced just 8. It is true that the sessions with female participants produced fewer tasks than two of the all-male sessions, but one all-male session produced the fewest tasks of all.

Finally, it is noteworthy that the Manager group had substantially less experience in the industrial cybersecurity archetype than did the participants for the other archetype roles.

### 8.4.1 Implications

Given the imperative for developing an industrial cybersecurity workforce, and the gaps in previous documents/efforts described Chapter 4, it appears that 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, it seems that Technician is the most oft-overlooked archetype, and that technicians will require significant effort and resources to adequately train. Employers and education providers should work together to address workforce needs.

Significant value creation will occur where individuals begin as technicians and advance into the other archetype roles where their detailed understanding of how things work becomes a catalyst for creative – yet practicable --solutions.

Value will be created where individuals with non-cybersecurity technician or engineer roles are introduced to cybersecurity tasks.

The author recommends that educational institutions and human resources departments inform their workforce development efforts with the prototype workforce development content advanced herein.

#### **8.4.2 Validation**

Under the researcher's preferred critical paradigm for research, validity requires the researcher to disclose perspectives and potential biases. The following sections provide reflection and examination of potential bias for each of the focus group sessions.

##### ***8.4.2.1 Researcher reflexivity***

In this case, the research again benefited from the breadth and depth of expertise and experience available at the Idaho National Laboratory. My personal relationships with industrial cybersecurity leadership played a key role in accessing that expertise.

When I approached leadership about this step in the research they were very supportive, and agreed to pass me the names and some preliminary background information on the individuals they thought would be a good fit for the project. This allowed me to consider first, whether I knew the suggested individuals through previous experience, and second, review their public LinkedIn profiles (if such profiles were available). There was some minor back and forth with the leadership team, but ultimately, I was very pleased with the quality of candidates identified. I was also pleased to have the perspective of two women in the group.

##### ***8.4.2.1.1 Technician session***

The technician group was composed of two individuals. One of them I knew through recent involvement in another INL industrial cybersecurity project. He had deep experience as a technician, technical engineer, and training supervisor. Cybersecurity was a relatively recent addition to his career, but from the perspective of "what types of things do technicians do?", he was very good. During the session, he wanted to talk about the entire research project, and about the technical elements of the program I ran at ISU. He was confident and talkative.

The other collaborator was significantly younger than the first. He had graduated from ISU's electronics program some 15 years earlier and gone to work as an instrumentation technician, ultimately adding cybersecurity to his repertoire. He likewise had a fantastic feel for the types of things technicians do, but was not impressively deep from the cybersecurity perspective. He talked less, and seemed to have an agreeable disposition.

These two individuals did not previously know one another, and so the conversation took a while to get going.

In the session, I listened intently and took notes, but I also played a strong leadership role, and used their feedback to fine tune the descriptions to the point where they were both comfortable with the results.

In the end, no one really knows what an industrial cybersecurity technician is. It doesn't really exist yet. But after my interaction with these two individuals, we all felt much more confident about the importance of this role.

#### *8.4.2.1.2 Engineer session*

The two engineers identified included my respected colleague, Curtis St. Michel, and another engineer, each with more than 20 years of engineering experience -- the latter less involved in cybersecurity than the former.

The two participants knew one another well, and had started at INL at about the same time, directly out of university (they had attended separate universities) working on several of the same projects earlier in their careers. This of, course has the potential to bias the results toward their shared professional perspective.

Because of our previous relationship, and St. Michel's outspoken personality, he did much of the talking, but he – and I – did invite his colleague to provide his opinion. St. Michel came across as a strong advocate for incorporating cybersecurity within the entire engineering domain.

What was most impressive to me about the session was the breadth of engineering tasks identified. I do not have a background in engineering, and so, while the input the two collaborators provided seemed very valuable to me, I don't have any personal experience doing those tasks.

#### *8.4.2.1.3 Analyst Session*

The two analysts identified had each worked in the field for seven or eight years. One came from an analyst undergraduate degree program, and the other had studied humanities. I had met one of them previously, but never engaged deeply. Both of these individuals had notional familiarity with some of my analytical work. Their former program manager – who had suggested their names – was a close friend of mine.

The two analysts evidently knew one another, but I did not investigate how closely they had worked together in the past.

My experience is that many analysts take time to warm-up their minds to a brainstorming exercise, and, if they understand the point, think their input is accurately understood and recorded, will participate fully. So, in this session and all others, I recorded their input on a screen visible to them in real time.

The analysts took turns leading out and following-up; I estimate each contributed evenly. After all of us were content with the initial documentation, the analysts helped categorise and order tasks and subtasks. They seemed to engage more carefully in the categorisation than did any other of the groups.

Due to my own previous experience as an industrial cybersecurity analyst, I found myself taking a more active role in this session than the previous sessions. I would say that a sense of emotional concurrence existed – and even a satisfaction with the conciseness of eight-item list.

#### *8.4.2.1.4 Researcher session*

INL provided two researchers from differing backgrounds – one in vulnerability discovery, and the other in human factors (often within a security context). I had worked with each of these individuals previously. The two only occasionally worked together, and thus had two different perspectives on the role of researcher. The collaborator who specialised in human factors held a PhD. The vulnerability researcher held a Masters degree in computer science.

The two collaborators provided richly descriptive answers and appeared to have spent considerable time considering what they were trying to accomplish, why they were trying to accomplish it, and how they could be most effective.

As a researcher myself, I appreciated this thoughtfulness; but, because their expertise was focused by years of specialised practice, I did not have the same level of emotional engagement as I had with the analysts. The richness of the session is obscured by the simplicity of the six tasks – but the collaborators concurred with the intuitive nature of the results as an appropriate level of detail for an archetype role.

#### *8.4.2.1.5 Manager Session*

The INL provided two managers with differing perspectives. One had spent several years managing the security of INL's own networks. During this time, he was tasked to help secure the Lab's industrial control systems, and he had learned some important lessons he wanted to share. The second collaborator had worked for many years helping provide

industrial cybersecurity training for federal and industry partners, then left the lab to manager product security teams at leading industrial control system vendors, before returning again to the INL.

As with several of the other focus group sessions, I knew both of these individuals; however, I had only interacted with them on a few occasions. Each collaborator had a different perspective, which the focus group approach seemed to effectively elicit. As I have run several analytical teams I have my own experience in this archetype. Because my experience differed significantly from the experiences of these two professionals, I did not feel emotionally invested in the outcome.

I would characterise the five tasks identified as simple and intuitive. Both participants expressed the contentment with the results.

### **8.4.3 Limitations**

The work presented in this Chapter (8) is subject to several significant limitations:

Firstly, the key challenge that the focus group sessions attempt to address, but from which they cannot escape, is that no one knows what an industrial cybersecurity expert is. Expertise can be difficult to identify where comparable, objective measures of capability are cannot be found. That is to say, how can one assure that these participants were truly qualified? How can one know their expertise is truly effective?

Secondly, this lack of easily-recognisable expertise is compounded by a need (particularly an emerging field) to balance a) describing existing practices with b) prescribing what improvements should be made in the future.

Thirdly, the approach employed in these sessions was only cognitive. A collaborator may sound as if he or she is good at something or as if they have done something, but there is no effort made to ensure what they are describing can actually be done – or how good they are at doing it. Essentially, it leaves criterion 11 from Chapter 4 “Evidence of empirical validation” unfulfilled.

Fourthly, the task lists associated with each archetype role produced by the focus group sessions do not reflect all of the detail provided in the sessions. Additional work is necessary to decompose the tasks into sub-tasks, and align these with knowledge, skills, attitudes and behaviors as described in workforce development model proposed in Chapter 7. This will naturally include the foundational differentiated knowledge identified in Chapters 5 and 6.



Finally, the fields of industrial automation and information technology are constantly evolving, as are the threats to systems using these technologies. As such, education and training guidance in general will benefit from regular review and revision.

## **8.5 Conclusion**

Building from the work described in previous chapters, this chapter focused on the question: “what tasks do individuals with the identified archetype roles perform?” The question was addressed using focus group sessions with subject matter experts who had professional experience in each of the five archetype roles. The result was a list of 46 tasks carried out by industrial cybersecurity professionals, divided by archetype role.

Of the task titles identified, those pertaining to the engineer and technician archetype roles appeared to differ most from tasks performed by traditional, non-industrial cybersecurity professionals. Stated in the inverse, the tasks of the manager, analyst, and researcher archetype role seemed quite similar to what one would expect a non-industrial cybersecurity manager, analyst, and researcher to do. While this should not be surprising given the intentional broad applicability of the Archetype model, it indicates that future work should focus on elaborating how and why the tasks are done differently in an industrial setting than for a traditional IT setting.

It is anticipated that this future work will require a more detailed approach – possibly using techniques such as the nominal group technique with qualified individuals (who have experience in each archetype), interviews seeking cognitive input, and field observation to corroborate and elucidate the cognitive input.

The insight gained from such work can be used to populate the details of the archetype model, thus identifying subtasks, and linking them with required knowledge and skills. This will allow for the identification of specialized knowledge and skills; and, of great importance, it will foster the identification and description of effective professional behaviors.

It is important that these future studies be carefully planned and executed, and that the results (potentially including recordings of interviews and videos of field observations) be made publicly available to help inform future professionals, educators, human resources personnel, managers, and functioning professionals about the details of the career field, and to establish measures of individual and organisational effectiveness and proficiency.

## 9 FUTURE WORK

The work presented thus far in this thesis has responded to the key research question: “What is the foundation for the formal preparation of industrial cybersecurity professionals?”

Building from this response, Chapter 9 will present six suggested “Future Efforts” already underway to advance the cause of industrial cybersecurity education and training, and four ideas for additional consideration.

### 9.1 Future Effort 1 – Establish an Industrial Cybersecurity Education and Training Community of Practice

One of the challenges faced by the work presented in this thesis is the perception held by some that industrial cybersecurity is not all that different from what we might call traditional cybersecurity. If educators seeking to address industrial cybersecurity continue to work beneath the broad banner of cybersecurity, they may not make a notable difference. One way to counter this perception is to establish a group of interested education and training professionals to share ideas and collaborate.

In a meeting held in August 2020, the author met with several representatives from the Idaho National Laboratory on the campus of Idaho State University in Pocatello, Idaho to discuss how to bring appropriate attention to industrial cybersecurity education and training. The author suggested that INL host an Industrial Cybersecurity Education and Training conference. The idea was readily accepted and a conference planned for November 2020. The INL and the author identified key individuals to serve as a steering committee members and conference participants. These were influential individuals in cybersecurity education at the national and international levels:

- Zachary Tudor, Chairperson of the (ISC)<sup>2</sup> Board of Directors
- Jim Risch, Senator from Idaho
- Sean Plankey, Principal Deputy Assistant Secretary for Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the Department of Energy
- Diana Burley, Vice Provost for Research at American University, Lead author of CSEC 17 curriculum standards

A pre-workshop survey designed by the author for administration to workshop registrants for the purpose of planning the workshop included the question: “In your experience, what is the most significant challenge in delivering quality industrial

cybersecurity education and training?” Choices and responses are presented in the table below:

*Table 23. Workshop participants most-significant needs for industrial cybersecurity education and training.*

<b>Response</b>	<b>Percent</b>	<b>Number</b>
Lack of compelling education and training standards	45.57	36
Lack of qualified instructors	24.05	19
Lack of quality instructional material	15.19	12
Limited hands-on training opportunities	51.90	41
Insufficient educational pathways for industrial operations personnel	34.18	27
Inability to measure learner/practitioner proficiency	24.05	19
Total respondents: 79		

Interestingly, the lack of hands-on training opportunities was perceived as the most significant challenge, while lack of compelling standards was second. This response, while not part of a formalised research effort, nevertheless tended to confirm the significance of the work presented in this thesis.

The workshop featured a keynote, three panels, and two plenary addresses. Each panel centred on a disparate aspect of the industrial cybersecurity education and training challenge: education and training, workforce development, and career pathways. The author made a plenary presentation on “Building Towards Standards in Industrial Cybersecurity Education and Training”, which included an overview of results of the work presented in this thesis to that date.

At the end of the workshop, participants were informed about two primary working groups they could join: one for workforce development, and the other for standards and curriculum development. The author was to be the facilitator of the latter group. Subsequently, on January 13, 2021 the author held a meeting which described the type of work to be done, and asked for volunteers to lead additional subgroups: landscape, standards, hands-on, and materials repository. The author volunteered to be the leader of the standards subgroup.

An initial meeting of the standards subgroup convened on February 2, 2021 to address the need for the development of standards. This group attracted about 20 participants,

and most of these volunteered to help out with the standards development work. The plan is for the subgroups to convene monthly and then reconvene with the larger group in May to share their progress.

Simultaneously with this effort, the author engaged with the International Society of Automation (ISA) Global Cybersecurity Alliance (GCA) workforce development working group. This group seeks to advance industrial cybersecurity on the basis of the ISA 62443 industrial automation and control systems cybersecurity practice standards. ISAGCA is composed of leading industrial automation firms and sector participants throughout the world.

In January 2021, the author agreed to serve as the working group champion to the entire ISAGCA committee.

It is anticipated that these two engagement efforts will result in meaningful work products that allow the results of this thesis and follow-on work to roll out nationally and globally.

## **9.2 Future Effort 2 – Extend Proposed Content to Create CSEC 17-style Knowledge Area**

While the work presented herein has already resulted in a proposed CAE-style Knowledge Unit (Appendix B), the work is yet insufficient to create a CSEC-17 style knowledge area because it does not differentiate between essential and non-essential information, consistent with the CSEC-17 knowledge areas. The effort to refine and reach consensus on the items presented in Chapter 5 will result in a CSEC-17 style knowledge area for industrial cybersecurity, which as evidenced in Chapter 3, does not currently exist.

## **9.3 Future Effort 3 – Contribute to Foundational Paradigms**

One of the broad research questions identified in chapter 2 includes “What are the key philosophical differences between industrial cybersecurity and traditional cybersecurity”?

The concepts of confidentiality, integrity, and availability – which we refer to in this paper as the CIA Triad or simply, the Triad – have long provided the paradigm guiding information assurance and cybersecurity as an academic and professional discipline (McCumber, 1991; Maconachy, 2001; Burley 2017). The author is developing the following concept to address perceived weaknesses with this reliance.

### 9.3.1 Industrial Cybersecurity Publications Relying on the CIA Triad

An examination of the emerging field of industrial cybersecurity, shows that leading publications, including international guidance, government standards, text books, and blog posts have employed the Triad for many years. Table 24 summarises key examples, ordered by date. The sections below describe how the CIA paradigm is employed in each publication.

*Table 24. Sample industrial cybersecurity publications relying on the CIA Triad.*

<b>Publication</b>	<b>Type</b>	<b>Date</b>	<b>Page dealing with Triad</b>
<i>Architecting Information Assurance</i>	Academic paper	2004	669, 671, 672
<i>IEC 62443-1-1 Security for Industrial Automation and Control Systems</i>	International standard	2007	36
<i>NIST SP 800-82 R2 Guide to Industrial Control Systems (ICS)</i>	U.S. government guidance	2015	1, 6-2, B-1
<i>Developing a Security Strategy to Cover ICS Assets</i>	Blog post	2016	n/a
<i>IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience</i>	Academic paper	2016	1, 2
<i>Industrial Cybersecurity</i>	Textbook	2017	12
<i>Mission Critical Operations Primer</i>	Textbook	2018	6-7
<i>A Hybrid Cyber-attack Model for Cyber-Physical Power Systems</i>	Academic paper	2020	1

#### 9.3.1.1 Architecting Information Assurance

This 2004 paper by Julie Ryan at George Washington University points out that it is rare for any system today, even those that can cause physical harm to human beings – such as dams and automobiles, to not include information technology. The paper clearly advocates application of the CIA triad during system design for any such system (Ryan, 2004).

#### 9.3.1.2 International Electrotechnical Commission (IEC) 62443 – Security for Industrial Automation and Control Systems Part 1-1 Terminology, Concepts, and Models

IEC 62443-1-1 is the foundational standard dealing with Security for Industrial Automation and Control Systems, which establishes the terminology, concepts and models used throughout the set of 14 proposed documents (International Society of Automation, 2007). The CIA triad appears near the top of Section 5: Concepts (p.36), where it states “Security in these systems is primarily concerned with maintaining the availability of all

system components. There are inherent risks associated with industrial machinery that is controlled, monitored, or otherwise affected by industrial automation and control systems. Therefore, integrity is often of second importance. Usually confidentiality is of lesser importance, because the data is raw in form and must be analysed within context to have any value.”

In section 5.2.1 Foundational Requirements, the document explains that the Triad is not adequate for a full understanding of control systems security, and advances eight additional requirements: access control, use control, data integrity, data confidentiality, restrict data flow, timely response to event, and resource availability – which are obviously still rooted in the Triad.

#### ***9.3.1.3 NIST SP 800-82 R2 Guide to Industrial Control Systems (ICS) Security***

This document, beginning on page 1, emphasises the importance of safety and reliability within an industrial environment, but then goes directly to the CIA paradigm, stating, “ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality” (Stouffer, 2015).

In the section on applying security controls to ICS, rather than directly prioritising potential consequences to safety and reliability (p. 6-3), the document first requires characterising losses of confidentiality, integrity, and availability. This seems to be an unnecessarily winding path. In addition, within the definitions on page B-1, the document defines “attack” (relying on CNSSI 4009) *only* in terms of the CIA Triad.

#### ***9.3.1.4 Developing a Security Strategy to Cover ICS Assets***

A 2016 blog post by Dan Scali (who ran the control systems security consulting business of the publicly traded cybersecurity firm FireEye) described that industrial control systems security objectives are availability and integrity, with confidentiality last (Scali, 2016).

#### ***9.3.1.5 IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience***

This article, written by Art Conklin of University of Houston (one of only two Centers of Academic Excellence to specialise in ICS security) described that the Triad has provided a useful security framework for IT, but proposes adding “Resilience”, which would make the Triad into a quartet. Conklin adopts the following definition of “operational resilience”: “The emergent property of an organisation that can continue to carry out its mission after disruption that does not exceed its operational limit” (Conklin, 2016).

### **9.3.1.6 Industrial Cybersecurity**

Industrial Cybersecurity is a 456-page textbook written by Pascal Ackerman, a former cybersecurity specialist at industrial automation firm Rockwell Automation. Near the beginning of chapter 1, Ackerman lists the Triad, and laments that that “for most industrial control systems availability ends up being the only design consideration when architecting the system” – emphasising the need for greater confidentiality and integrity (Ackerman, 2017, p. 12).

### **9.3.1.7 Mission Critical Operations Primer**

Mission Critical Operations Primer is a short textbook written by Steve Mustard, P.E. and published by the International Society of Automation. The CIA Triad is featured prominently at the top of chapter 2, “Mission Critical Operations Concepts”, where it states that “OT is responsible for monitoring and controlling industrial processes; and failure could have significant impact on safety, production, and the environment. For OT, the relative order of importance is: Availability, Integrity, Confidentiality” (Mustard, 2018).

### **9.3.1.8 A Hybrid Cyber-attack Model for Cyber-Physical Power Systems**

A 2020 paper by international authors entitled “A Hybrid Cyber-attack Model for Cyber-Physical Power Systems” anchors on the Triad concepts to describe attack consequences (Tu, 2020).

## **9.3.2 Concerns with CIA Triad as the guiding paradigm for industrial cybersecurity**

A review of the diverse documents described above show how prevalent the Triad paradigm has become for discussing industrial cybersecurity. But, one should clearly recognise that an industrial control system is not an information system in the strictest sense. The key element of an information system is data. Data is an abstraction about the physical world that helps humans think. The key element of an industrial control system is physics. Physics is the physical world.

Physical world means actual matter existing in space: liquids, gasses, and solids; temperatures, pressures, levels, and flows; motors, pumps, valves, compressors, transformers, and breakers. This translates to clean water, reliable electricity, and affordable manufactured goods.

A review of the literature that originally expounded the CIA triad, does not reveal any evidence that its authors explicitly considered its applicability to industrial control systems. In fact, terms related to “industrial control” and “industrial automation” never appear.

It should be pointed out that in an industrial control system, an entirely legitimate command issued by the operator or engineer or technician (or an attacker) can reasonably cause significant physical impact – up to and including loss of life – with no loss of information system confidentiality, integrity, or availability. This could be done by a set point change, a new control logic push, or a mis-timed process start command. A prevalent example of this is the DHS Aurora test which involved simple commands that rapidly opened and closed breakers connecting a large diesel generator to the electric grid (Greenberg, 2020). The system intentionally permitted such commands. This is a gaping hole within the paradigm.

#### ***9.3.2.1 Hypothetical dialog***

To illustrate this concept, one may consider a hypothetical conversation between two individuals, who we will call Alice and Mallory.

“You know”, says Alice to Mallory as they walk down the hall, “I’ve been reading about the foundations of cybersecurity, and I don’t think the discipline really addresses industrial control systems.”

“What?” responds Mallory, incredulously.

“Yeah,” says Alice. “I can imagine a cyberattack where there is significant physical damage, maybe even loss of human life, without any impact to confidentiality, integrity, or availability of information – on which the whole discipline is based.”

“I don’t believe it,” Mallory says, “if people die, that’s an impact on the availability of human life.”

“Well,” says Alice “I think you are bending the model. The entire paradigm is built on ‘information’, not ‘human life’. If we take your viewpoint, a machete could become a real hacker tool!”

“Ok,” responds Mallory, “but if a cyber-attacker sends a message that results in an unintended physical consequence, there must have been a compromise of integrity.”

“Hold on,” Alice responds, “integrity implies that the information hasn’t been fiddled with – no error, no man-in-the middle. In this case, the exact command sent – like a command for compressors to increase the pressure in a natural gas pipeline above the pipeline’s safety rating – would be the exact command received. The system is intentionally allowed to control the physical world. The characteristic violated is not integrity of information, but safety.”



“Ok,” says Mallory “but there must have been some compromise of integrity, confidentiality or integrity before-hand that allowed someone to send that command.”

“Maybe,” says Alice, as Mallory follows her into the elevator; “but would you recommend we strip the mechanical fail-safe brakes off elevators at the same time we give elevator controls cloud-connected IP addresses?”

“I see your point,” says Mallory. “When we replace the mechanical fail-safe brakes with intelligent safety systems, we need to be sure the web interface requires complex passwords. What floor are you going to?”

“You know?” says Alice, pushing by Mallory back out of the elevator before the doors can close, “I think I’ll take the stairs!”

This hypothetical interchange between Alice and Mallory demonstrates the important nexus between information systems and industrial control systems. Reliance on the information characteristics of confidentiality, integrity, and availability alone is insufficient to achieve the desired characteristics of the industrial control system – notably physical safety.

In this exchange, Alice represents the engineers charged with designing, building, operating and maintaining industrial control systems. Mallory represents the cybersecurity professionals charged with ensuring the “security” of information systems component of the industrial environment. The elevator represents the complex and interdisciplinary cyber-physical world into which they are both entering.

Mallory, by the fundamentals on which she has been educated and trained, approaches the problem without the intellectual tools with which to approach the challenge. The term “fail-safe” is a fuzzy concept to her. Mallory’s inability to fully grasp the consequences of the evolving situation is so deeply concerning to Alice, that she would rather not even entertain the conversation – highlighting a rift between them that must be overcome.

#### ***9.3.2.2 Safety as a foundational concept for industrial cybersecurity education***

To the engineer, Alice, in the hypothetical dialog, safety is a paramount concept with at least an equal history in engineering as the CIA triad has in cybersecurity; and, to omit it, or subsume it beneath information system integrity, would be a grave mistake, and dismissive of the importance of safety throughout the fields of engineering.

As another example, consider a rifle. Every rifle has a small stopper switch, that, when engaged, physically prevents the trigger from actuating the firing pin, which strikes the primer at the rear of the cartridge. When struck, the primer releases a spark, which in turn

ignites the gunpowder within the casing, sending the bullet down the barrel at fantastic speed. This stopper switch is frequently called “a safety”, and prevents accidental discharge of the weapon and associated injury.

If a firearm is connected to a network, such that the press of a keyboard button now actuates the trigger, would it be appropriate for cybersecurity academics and practitioners to call such a stopper switch “an integrity”? Such an approach seems to bulldoze the lexicon of the discipline that designed the firearm in the first place, and that of the firearm user, replacing it with a term for which its own foundational literature offers no support.

To more fully grasp the incompleteness of the CIA toolset, one can consider the way in which the triad is commonly used to frame the consequences of cyber events and incidents – first in risk management, and then in software vulnerability analysis.

The NIST risk management framework – required for use by US federal agencies and encouraged for use by private organisations around the world – offers exactly three options for categorising impacts of cybersecurity events – confidentiality, integrity and availability. Safety – loss of human life – is not even on the list. It is circuitously buried in some abstract way beneath integrity and availability (Stouffer, 2015, p. G-12).

Furthermore, the Common Vulnerability Scoring System (CVSS), created and maintained by the Forum of Incident Response and Security Teams (FIRST), is the leading framework to describe the significance of a software vulnerability (FIRST, n.d.). Analysts around the world rely on CVSS; it is prominently featured in the National Vulnerability Database. CVSS offers exactly three options for categorising the impacts of successful vulnerability exploitation – confidentiality, integrity, and availability. Safety – loss of human life – is not even on the list – though software vulnerabilities (particularly in safety instrumented systems) could clearly lead to that consequence.

In an analogy, this glaring weakness is like taking a plane trip to pick up a gallon of milk on the way home after work. It seems obvious that protecting human life is paramount, but the triad tool set actually discourages this direct consideration. It seems patently inappropriate, then, to rely solely on the foundation of the Triad where it was not intended for use.

This observation leads to the disquieting question: is the triad an effective foundational pedagogical paradigm in the increasingly cyber-physical world? While even

asking this question may be met with cries of heresy, it does not seem beyond reason that the evolving techno-centric physical world requires evolving cybersecurity paradigms.

### **9.3.3 Counterarguments and response**

Several counterarguments may exist to the assertion that the CIA triad alone is insufficient as the guiding paradigm for industrial cybersecurity. Firstly, it may be argued that the terms “confidentiality”, “integrity”, and “availability” have useful meanings outside of the information systems context in which they were established. While this could be the case, considering it would require a robust discussion about whether other terms may be more foundationally useful across all cybersecurity.

A second counterargument could be that the Triad is too engrained – even in industrial control systems; and, that changing it now is futile. One response to this counterargument may be that when dealing with critical systems on which evolving society increasingly depends, the most applicable and effective paradigms must be developed and used, regardless of what has been done in the past.

A third counterargument could be that the Triad should merely be adapted or extended to compensate for its weaknesses. This seems a reasonable compromise; however, such extensions (such as adding “resilience” and/or “safety”) appear to let stand the previously established definitions of the Triad, without further questioning. Given what is at stake, and the apparent consistent trends of cybersecurity events and incidents, should cybersecurity thinkers shy away from this uncomfortable discussion?

### **9.3.4 Seven Ideals as a guiding paradigm**

Starting in 2007, Miles McQueen and Wayne Boyer of the Idaho National Laboratory wrote three papers on cybersecurity metrics, in which they advanced an ideal-driven approach to cybersecurity. The approach intentionally encompassed both information systems and industrial control systems. Their work focused exclusively on developing security metrics to enable risk management. A brief summary of each paper follows:

“Ideal-Based Cyber Security Technical Metrics for Control Systems” (Boyer, 2008) aimed to provide a basis on which cybersecurity metrics – useful in cybersecurity management and decision making – could be designed. The work proposed seven dimensions of security along with their ideal states.

“Measurable Control System Security Through Ideal Driven Technical Metrics” was presented at the SCADA Security Scientific Symposium (S4) in January 2008. It examined

the ideal-based metrics presented in the “Ideal-Based Cyber Security Technical Metrics” paper, through two real-life case studies (McQueen, 2008).

“Primer Control System Cyber Security Framework and Technical Metrics” intended to take the work presented in the previously mentioned two papers and make it more easily consumable by a non-academic audience (McQueen, 2008).

### **9.3.5 Restatement**

This section includes a restatement of the original ideals advanced by Boyer and McQueen:

**Ideal 1** – Those responsible to maintain the trustworthiness of the system (the security group) know the current system perfectly

**Ideal 2** – Those who desire to abuse the system (the attack group) know nothing about the current system

**Ideal 3** – The system is inaccessible to the attack group

**Ideal 4** – The system has no vulnerabilities

**Ideal 5** – The security group detects any attack immediately

**Ideal 6** – The security group restores the system to a trustworthy state instantly

**Ideal 7** – The system cannot cause damage

### **9.3.6 Analysis of restatement**

This section describes innovations over the original Seven Ideals, then discuss the paradigm’s strengths and weaknesses.

#### **9.3.6.1 Innovations**

In the interest of the thought-guiding structure the paradigm provides rather than any specific application, the restatement removed the ideals from their security measurement context; that is to say that they are used as guiding principles rather than a framework for developing metrics.

Boyer, 2008 included a detailed treatment of security principles, which consisted of examples of common wisdom or rationale. This rationale led to the identification of abstract security dimensions, from which the ideals were derived. The restatement does not include the same background, but lets the ideals stand for themselves.

In Boyer, 2008, the concepts of “security group” and “attack group” were explained separately from the ideals. The restatement incorporates the explanatory language within Ideals 1 and 2.

Ideal 1 originally read “Security group knows current control system perfectly”. It now reads “Those responsible to maintain the trustworthiness of the system (the security group) know the current system perfectly”. This relies on the concept of trustworthiness to unlink “security” from the Triad because “security” is often defined using the Triad. Moreover, it is foreseeable that “trustworthiness” is understood more readily than are the terms of the Triad.

Ideal 5 originally read “Security group detects any attack instantly”. It now reads “Security group detects any attack immediately”. “Immediately” better connotes the time between when the attack occurs and when detection occurs – where “instantly” could be taken to refer to the detection process itself. This distinction becomes more significant considering the way the word “instantly” is used in the subsequent ideal.

Ideal 6 was modified from “Security group can restore control system integrity instantly” to “security group restores the system to a trustworthy state instantly”. Here, instantly clearly refers to the speed of the restoration process. The word “can” was replaced with the present tense verb “restores” to maintain consistency with the phrasing of other ideals. The removal of the word “control” emphasises the holistic nature of the ideals – including both industrial control and information systems. The concept of “system integrity” is replaced with “trustworthy state” to avoid possible confusion about the meaning of “integrity” as a member of the Triad, and to maintain consistency with “trustworthiness” as used in Ideal 1.

The restatement also moves the original Ideal 5 replaces it as the final ideal – Ideal 7. Firstly, this re-ordering emphasises that engineered fail-safes provide the ultimate protection/defense to cyber-attack against industrial control systems. Secondly, no evidence in the three papers by McQueen and Boyer supports that they intentionally placed their ideals in a specific order.

#### **9.3.6.2 *Strengths***

The Seven Ideals Restated provides an enticing foundational paradigm for industrial cybersecurity for the following reasons:

- It is memorable

The term “Seven Ideals” has a sticky sound to it. The number seven is already associated with wholeness and completeness – as in the number of days in the week.

Cognitive research has established the threshold of 7 plus or minus 2 as the general limit of operational short-term human memory (Miller, 1955).

- It aligns with other existing security concepts

A longstanding security maxim states “Know yourself... Know your adversary” (Sunzi). The first two ideals reflect this wisdom, with a twist on denying the adversary’s ability to obtain knowledge. This denying an adversary’s ability to obtain knowledge has played a role in U.S. military doctrine on Information Operations (McConville, 1997). In addition, McQueen and Boyer asserted that “we successfully mapped security principles from Bishop, Neumann, Schneier, NIST and Summers to our seven ideals” (Boyer, 2008).

- It has evidence of empirical validation

The papers written by McQueen and Boyer include three case studies that indicate the model is useful at least as a basis for designing cybersecurity metrics.

- It encompasses both industrial control and information systems

The entire concept was born with industrial control systems in mind – which, as noted above, is not the case with the CIA Triad.

- It has an intuitive systems-oriented approach

The ideals are arranged in a cascading manner, such that the failure to obtain the preceding ideal is mitigated by achieving the following ideals – giving form to the concept of defense-in-depth – and encouraging thinkers to consider security as an inter-connected system.

- It naturally suggests courses of action

The Triad does not naturally suggest courses of action because it does not, and cannot include statements of ideal. For example, the ideals of confidentiality and availability would be diametrically opposed at the most basic level.

- It emphasises physical consequences

The final ideal addresses damage – which includes physical damage. This emphasises that the industrial control system should be engineered in such a way that it is physically impossible to damage products, human health, or the environment via a cyberattack.

- It incorporates offensive and defensive perspectives

The Triad model does not even recognise the attack-and-defend nature of cybersecurity.

### **9.3.6.3 Weaknesses**

An obvious critique of the Seven Ideals model is that the ideals are not achievable – at least they are not entirely within the direct control of those charged to maintain the trustworthiness of the system. This un-achievability could demotivate practitioners from using it. This critique could be countered by asking, “towards what does a security practitioner work if it is not an ideal?” If the answer is “cost-effectiveness”, one could reply, “does not ‘effectiveness’ imply the existence of an ideal?”

Another critique may be that the paradigm does not aid in prioritising which ideals are more important at any given moment. While this point seems accurate, this paradigm excels the Triad in this regard because it naturally suggests actions.

Finally, an ideal security system might do things for which this model does not easily account. Examples may include learning about the attacker or reconfiguring itself. This is a clear limitation of the Seven Ideals, but the Seven Ideals appears to excel the Triad in this regard.

Other weaknesses are likely to exist which have yet to be identified.

### **9.3.7 Recommendations**

A primary recommendation is that industrial cybersecurity instructors introduce the Seven Ideals Restatement before the Triad paradigm. While it may be a controversial recommendation, the critical nature of industrial cybersecurity to an increasingly technology-dependent society requires a new and comprehensive approach.

Second, cybersecurity thinkers should create and explore alternate foundational, instructional paradigms that apply to industrial cybersecurity. A field as diverse and interdisciplinary as cybersecurity provides ample room and opportunity for alternate points of view, inviting a robust discussion about the meaning of cybersecurity.

Finally, instructors and researchers should seek to devise ways to measure the effectiveness of foundational cybersecurity paradigms. This will prove a significant challenge, given the complexities of human learning, the difficulty of maintaining appropriate control groups, and the highly dynamic technological and threat environment. But, such research should ultimately benefit all society as the information age accelerates across every domain of human endeavor.

#### **9.4 Future Effort 4 – Perform Additional Validation Incorporating Cognitive and Behavioral Approaches**

The initial industrial cybersecurity task list per archetype role was the result of focus group sessions, as described in Chapter 8. Because these results came from only two or three collaborators, working at a single organisation, the Idaho National Laboratory, they would benefit from additional validation. Per the criteria for an industrial cybersecurity education and training guidance presented in Chapter 4, such validation should include both cognitive and behavioral approaches.

Appendix G addresses the preparations to conduct an additional three phases of research: 1) A survey, designed to validate and refine the task list; 2) An interview protocol to gather a deeper level of insight; 3) A field observation protocol – all of which have been approved by the La Trobe University Human Ethics Committee. Implementing these three additional phases would meet many of the criteria set out by Shippmann (2000) for a robust approach to job competency modeling.

It is anticipated that these future efforts will result in additional refinements that compensate for the weaknesses inherent in the initial nominal group technique session as described in sections 5.2 and 5.4.1.

#### **9.5 Future Effort 5 – Establish Career Pathways**

While advancing a set of foundational guidance for industrial cybersecurity is a significant challenge, it will be of little benefit without appropriate deployment of the guidance.

We are aware that the instrumentation and control technicians that configure sensors, program PLCs, and troubleshoot control loops, often come from specialised two-year technical career programs. One prominent case is Marty Edwards, who served as Director of the US Department of Homeland Security (DHS) Industrial Control Systems Computer Emergency Response Team (ICS-CERT) from 2011 to 2017. Edwards is a graduate of the British Columbia Institute of Technology where he studied electrical and electronics engineering, earning a technical diploma (Edwards, n.d.). This hands-on experience prepared and qualified him for a career as an automation technician and enabled him to make sense of the security details affecting industrial environments following his professional experience in the paper and pulp industry.



It is practical to recognise that the individuals who will have influence to cause, notice, and respond to cyber incidents in industrial environments are the people who work there every day – that is the control technicians and engineers who design, program, install, commission, operate, and maintain them. In order to successfully defend critical infrastructure, educational standards must apply to institutions and programs that produce these professionals.

One approach is to provide a vertically integrated pathway for these technicians – who are most familiar with the way the industrial environment operates – to add industrial cybersecurity to their various competencies.

Vertical Integration refers to intentionally coordinated relationships among instructors from different stages of the educational process, as shown in Table 1. These relationships – spanning institutional boundaries – allow faculty to clearly indicate the next steps an interested student may consider.

	<b>Institution Type</b>	<b>Faculty Role</b>	<b>Vertical Integration Actions</b>
Stage 1	Middle/High School	STEM-related instructor	<ul style="list-style-type: none"> <li>• Co-teach at college summer camp</li> <li>• Invite college instructor to visit classroom</li> <li>• Incorporate college program content</li> </ul>
Stage 2	Technical College	Program Coordinator	<ul style="list-style-type: none"> <li>• Co-teach with HS instructor at summer camp</li> <li>• Serve on HS advisory committee</li> <li>• Lead hands-on experiences in HS classrooms</li> <li>• Provide program tours</li> <li>• Invite employer to visit</li> <li>• Invite employer to advisory committee</li> </ul>
Stage 3	University	Major Faculty Advisor	<ul style="list-style-type: none"> <li>• Articulate with college programs</li> <li>• Coordinate scholarships for desired pathways</li> <li>• Introduce to student to graduate faculty</li> </ul>
Stage 4	Employer	Hiring Manager	<ul style="list-style-type: none"> <li>• Support summer camp with funds or other contributions</li> <li>• Participate on college program advisory committee</li> <li>• Visit college classroom</li> <li>• Provide internships</li> <li>• Hire graduates</li> </ul>
Stage 5	Graduate School	Graduate Supervisor	<ul style="list-style-type: none"> <li>• Meet promising undergraduates</li> <li>• Coordinate course offerings (times, locations, topics) with local employers</li> </ul>

Speaking from the author's empirical observation as a student, graduate student, professional, and instructor, the prevailing formalised educational model focuses on what a student learns within each stage – and often within a particular component of the stage – without intentional focus on transition between stages. One could consider a hypothetical case of how improved vertical integration could benefit a middle school student, Alice.

In a required math class, Alice learns of a hands-on STEM summer camp opportunity from her teacher, who hands out a promotional flyer. Alice attends the camp, where she meets a high school teacher (helping run the camp) who encourages Alice to take the teacher's class as an elective. Even though two years go by, Alice sees the same teacher in the hall, and decides to sign up for her class. There, Alice participates in a hands-on activity brought to the school by a technical college instructor, who leaves behind contact information and promotional materials. The high school teacher coordinates a field trip to tour the college program. Alice attends the tour, likes what she sees, and enrolls.

During the college program, Alice hears from various employers who come to speak and seek potential new hires. She ends up interning with one of these employers. The employer recognises Alice's great potential, and offers her a full-time job. She chooses instead to stay in school believing that a bachelor degree will serve her better in the long run. Her instructor points out which upper division classes will ensure employability. While taking these classes, her faculty advisor at the bachelor level offers to introduce Alice to a graduate-level faculty friend at another institution. Simultaneously, the company with which Alice first interned, offers her a full-time job at a higher wage, and describes its educational benefit that will pay for her to take a part time Master's Degree. Alice takes the job and signs up for online Master's classes.

In this scenario (summarised in Figure 1), it was the vertical integration (in addition to appropriate instruction), that ensured Alice obtained a job, the employer obtained an employee, and the graduate program continued advancing employee value.



ISU's Energy Systems Technology and Education Center (ESTEC) within the College of Technology has the mission of creating hands-on technicians and field engineers that work in power plants, water treatment facilities, and manufacturing facilities (Idaho State University, n.d. *Energy Systems*). ESTEC has instructional Laboratory space designed to produce technicians in mechanical engineering, electrical engineering, instrumentation engineering, and nuclear operations.

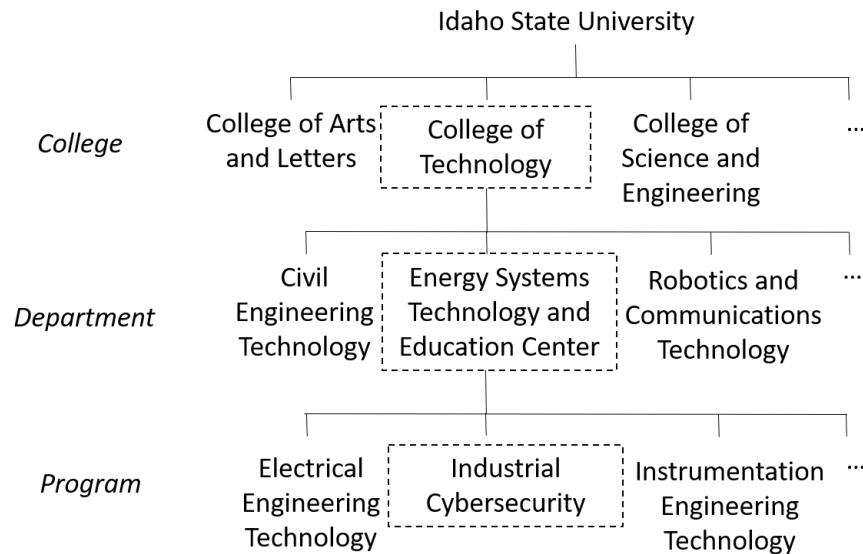


Figure 25. ISU Organisational Structure

### 9.5.2 Raspberry Pis and dehydrated potatoes

Content for vertical integration revolves around ESET 181: IT-OT Fundamentals. The premise of this project-based course is that students design and build a notional industrial control system based on the needs of a real local potato processing firm – Basic American Foods (BAF). Students read local press articles explaining that BAF is closing one facility in favor of increasing automation at another. They visit the BAF web site to see the products the firm produces.

Through a series of 43 hands-on learning activities, students rely on Raspberry Pis to explore and experience: IT-OT environments, computing platforms & operating systems, coding, basic process control, web technologies, supervisory control and data acquisition (SCADA), networking, industrial networks, the IT-OT gap, network monitoring, security, and the future of OT. At the end of the semester, the students present their project, which

combines the elements named above. This provides students with an exciting view of what their future holds. See Appendix E for an abbreviated syllabus.

### **9.5.3 Engaging middle school and high school students**

ISU's ESTEC organises an annual "Ignite Their Future" summer camp for middle school and high school students held on campus (Idaho State University, n.d. *Ignite*). The objective of the camp is to excite students about a career in a STEM-related field. In 2019, the camp included 12 strands, and served more than 100 students.

Middle school and high school teachers sign up to co-teach strands with ESTEC instructors. The week before the camp, the teachers sit with ESTEC instructors to learn the material and create/update lesson plans. The teachers earn continuing professional education (CPE) hours, and the camp offers them a stipend for their support.

Middle school and high school teachers have now set foot in the ESTEC buildings, and had positive experiences with college instructors. This increases their confidence in the system, and the likelihood of them mentioning the camp to their students. Next year they may sign up to co-teach a different strand.

Content for the "Build a Raspberry Pi computer" summer camp strand is taken directly from the IT-OT Fundamentals course. While the way it is taught to middle schoolers differs from the way it is taught to undergraduate students, re-use of content offers certain convenience.

Middle school students will now have set foot within ESTEC – many years before attending a program there, hopefully influencing their attitude about attending college.

### **9.5.4 Engaging high school students**

In addition to the effort and benefits described in the section above, ESTEC pays special attention to relationships with specific high school CTE instructors. The Association for Career and Technical Education claims that over 90% of high school students across the US are part of CTE (Association for Career and Technical Education, n.d.). This is a fantastic opportunity to identify interested students, and point them towards next steps.

ISU's Industrial Cybersecurity program has developed a relationship with several high school CTE instructors within the region. The college instructor visits these high school instructors and their students three or four times each year. During these visits, the instructor delivers a hands-on learning activity taken directly from the ESET 181 course.

Empirically speaking, most students are easily engaged – minds and hands – in a simple cybersecurity exercise using Raspberry Pis (RPis) – which the college instructor brings to the high school classroom. The RPis are configured with secure shell (SSH) open with a default username and password. Students warm up learning some basic Linux commands, including how to make a directory and create a file. They connect a network cable with their neighbor, and find their IP address. They use their smart phones to find the default SSH password credentials. They SSH to the other computer, and examine the contents of the file the other student made. They then leave their own file on their neighbors’ computer. Students are surprised to learn that the other person has no immediate indication that someone else is reading and leaving files. The exercise ends with a digital arms race where one student from each pair represents USA and one represents Russia. The instructor tells the students that whoever types the following command fastest will win the race and turn off the other person’s computer: `sudo shutdown now`. Students yell in excitement or disappointment as half the screens go dark.

The college instructor then leads a debrief in which he asks the students to describe what lessons they learned from the exercise. “How to hack”, says one. “Not to let anyone know your IP address”, says another. “Change your default password”, claims a third. These sincere responses offer fantastic opportunity to engage in conversation about ethics, networks, and security, respectively.

Normally, one or two students will have previous knowledge of Linux. Occasionally, a student will have previous exposure to security tools such as those included with the Kali distribution. The instructor may wish to pay special attention to these students and chat with them after class. The instructor leaves behind promotional materials and offers to set up a program tour for anyone interested.

Through this hands-on experience, high school students have actually seen a college instructor, and likely learned something from him or her. They now know how to find additional information, and can ask their high school instructor any questions they may have.

It is worthwhile for the college instructor to offer to serve on the high school instructor’s advisory committee. As many high school CTE students go on for more education rather than enter the workforce directly, the college instructor offers an important perspective.

As a next step for vertical integration with high schools, ISU's College of Technology plans to adjust the ESET 181 course for a high school audience, and pilot the course for dual credit with a high school instructor. Ideally the course would also qualify as a university general education course – providing additional incentive for high school students to enrol.

#### **9.5.5 Pathway to bachelor degree**

In Fall 2019, the State of Idaho created a Bachelor of Applied Science in Cyber Physical Systems Engineering Technology (BAS CPS) at Idaho State University. This pathway lays out the year 3 and 4 upper division classes for students who already have Associate degrees in the following fields, from any Idaho's six technical colleges:

- Instrumentation Engineering Technology
- Electrical Engineering Technology
- Mechanical Engineering Technology
- Nuclear Operations Technology
- Information Technology Systems
- Robotics and Communications Systems
- Civil Engineering Technology
- Diesel Onsite Power Technology

Year three of the program – which runs under a cohort model – earns the student an Intermediate Technical Certificate in Industrial Cybersecurity, and includes the courses shown in the table below. Depending on the Associate Degree the student has earned, they may substitute electives for the Industrial Operations or IT courses. The Industrial Cybersecurity courses are offered at the upper division level.

<b>Industrial Operations</b>	<b>IT</b>	<b>Industrial Cybersecurity</b>
Engineering Technology	IT-OT Fundamentals	Secure Systems Design
Energy Systems	Networking	Risk Management
Digital Control		Network Security
		Critical Infrastructure Defense
		Professional Certification
		Capstone

Year 4 of the program covers remaining general education requirements and the following upper division courses, to prepare a well-rounded professional: Technical Writing,

Individual and Organisational Behavior, Project Management, Operations and Production Management, Information Assurance, Informatics & Analytics.

As demand for this program grows, ISU is implementing a competitive entry model. Candidates with actual work experience in these fields receive preference for admission.

#### **9.5.6 Graduate options**

Currently Idaho State University offers two options for graduate students. First is National Information Assurance Training and Education Center (NIATEC) – a full time NSF Scholarship for Service program, where students earn a Master of Business Administration (MBA) degree in preparation for leadership-level employment within the federal government. Students who have graduated with the BAS CPS are well positioned for NIATEC because they 1) have previously developed an employable skill set; 2) have rounded out that skill set with management and communications courses; 3) have significant previous exposure to cybersecurity.

#### **9.5.7 A cycle of vertical integration**

As the cybersecurity industry grows in Southeast Idaho, ISU's graduates who have worked for diverse government entities (often in the Washington, DC area) since 2005, are now returning – many to find employment at the Idaho National Laboratory. They now serve as program advisors, guest lecturers, adjunct faculty, and hiring managers – turning vertical integration into a virtuous cycle, which will improve over the years.

#### **9.5.8 Summary of career paths discussion**

Vertical integration leveraging career and technical education appears a promising pathway for developing the unique combination of hands-on and academic competencies required to protect industrial infrastructures. While not all schools benefit from the CTE alignment present at Idaho State University, there is no intrinsic reason forward-thinking academic institutions cannot develop similar relationships and alignment.

Of course, successful vertical integration for industrial cybersecurity requires quality instructional capabilities, including appropriate pedagogical models, student learning outcomes, curricula design, and laboratories for hands-on instructional interventions. Future work will discuss efforts to develop these aspects of an effective program.

Given that industrial cybersecurity is a global concern, value may exist in exporting this vertically integrated curricular pathway model to educational environments in other countries. Future work will need to examine its applicability in alternate educational systems.



## **9.6 Future Effort 6 – Example Curriculum**

This section presents the curricular details of the Industrial Cybersecurity Engineering Technology degree program at Idaho State University – which, based on web searches and conversation with other educators, appears (as of the time of this writing) to be the only *degree program* with such a name within the United States. While these details do not yet represent a consensus about how to best create industrial cybersecurity professionals, they do provide a starting point from which a consensus model curriculum could be developed. The example presented in section 9.7.1 below includes the following components:

- Program educational objectives – which are things a student should be able to do within several years of graduation
- Student learning outcomes – which are things a student should be able to do upon graduation.
- Courses numbers, titles, and descriptions
- Course objectives

Section 9.7.2 will present the challenges and objections faced to establish the interdisciplinary pathway to bachelor degree. Such presentation aims to inform and prepare those who attempt to create similar programs.

### **9.6.1 Example curricula for industrial cybersecurity technicians**

Of the five archetype roles identified in chapter 5, this model curricula addresses the need for industrial cybersecurity technicians. Many of the concepts and approaches will also apply to the other archetype roles.

#### ***9.6.1.1 Program educational objectives***

In the accreditation model advanced by ABET (within which the Industrial Cybersecurity program at Idaho State University intends to operate), program educational objectives are things that a student should be able to do within a few years of graduation. The established objectives – approved by faculty and an industry advisory board, are as follows:

1. Identify and respond to security concerns relating to operational cyber-physical systems.
2. Coordinate among key stakeholders for matters dealing with the security of cyber physical-systems.

3. Promote stakeholder awareness and education relating to cyber-physical systems security.
4. Establish optimal policies for managing risk in cyber-physical systems.
5. Use security criteria to influence technology selection and deployment.

#### **9.6.1.2 *Student learning outcomes***

In the accreditation model advanced by ABET, student learning outcomes are things a student should be able to do upon graduation. The student learning outcomes, also approved by faculty and an industry advisory board, are as follows:

1. Apply the fundamental principles of cyber-physical systems.
2. Explain the need and purpose of securing cyber-physical systems.
3. Identify common weaknesses in cyber-physical systems.
4. Evaluate the security of cyber-physical systems by applying pertinent recognised standards.
5. Propose policies practices for managing cyber-physical systems risk.
6. Implement techniques for defending cyber-physical systems.

#### **9.6.1.3 *Target professional tasks***

Though not required by the program's accreditation body, the industrial cybersecurity program, under the author's leadership, has identified the following professional skills and knowledge which align primarily with student learning outcome number six (identified above):

- Maintains ICS device asset inventory for security purposes
- Reviews architecture of ICS networks
- Updates ICS software and firmware during stoppages
- Maintains backups of control software
- Maintains awareness of evolving threat environment
- Securely implements process control equipment

#### **9.6.1.4 *Courses and associated detail***

As noted in section 9.6, the curriculum can be taken as a part of a two-year Associate of Applied Science (AAS) in Industrial Cybersecurity Engineering Technology, or as part of a Bachelor of Applied Science (BAS) in Cyber-Physical Systems Engineering Technology. The courses presented below are those to be taken by a typical AAS degree seeker. Exact courses

would differ for a BAS seeker depending on the AAS degree the student already possesses (Idaho State University, 2021-2022 Academic Catalog).

*Table 25. Industrial Cybersecurity Engineering Technology program courses*

<b>Course</b>	<b>Title</b>	<b>Cr</b>
ESET 0100	Engineering Technology Orientation	1
ESET 0100L	Engineering Technology Orientation Lab	1
ESET 0181	Information Technology - Operational Technology Fundamentals	3
ESET 0282	Introduction to Networking	3
CYBR 3383	Security Design for Cyber-Physical Systems	3
CYBR 3384	Risk Management for Cyber-Physical Systems	3
CYBR 4481	Defending Critical Infrastructure and Cyber-Physical Systems	3
CYBR 4486	Network Security for Industrial Environments	3
CYBR 4487	Professional Development and Certification	3
CYBR 4489	Capstone in Industrial Cybersecurity	3
ESET 0121	Basic Electricity and Electronics	4
& 0121L	and Basic Electricity and Electronics Laboratory	
ESET 0140	Applied Technical Intermediate Algebra	5
ESET 0120	Introduction to Energy Systems	2
ESET 0120L	Introduction to Energy Systems Laboratory	1
ESET 0122	Electrical Systems and Motor Control Theory	3
ESET 0122L	Electrical Systems and Motor Control Theory Laboratory	1
ESET 0223	Digital Control Theory	2
ESET 0227	Digital Control Systems Laboratory	1
ESET 0242	Practical Process Measurements and Control	2
MGT 2216	Business Statistics	3
PHYS 1101	Elements of Physics	4
& 1101L	and Elements of Physics Laboratory	
Total Credits		54

Table 26. Category totals for Industrial Cybersecurity Engineering Technology

Category	Credits
Program Admission Requirements	0
General Education	16
Major Requirements (Required General Education credits removed.)	47
Free Electives	
Total Credits	63

### 9.6.1.5 Introduce, reinforce, master map

The map provided below describes the courses in which students are introduced to an outcome, reinforced in the outcome, or master an outcome.

Table 27. Introduce (I), reinforce (R), assess (A) map

Course						
	SLO1	SLO2	SO3	SO4	SO5	SO6
<b>Semester 1</b>						
ESET 0100: Engineering Technology Orientation	I	I				
ESET 0100L: Engineering Technology Orientation Lab	I					
ESET 0121: Basic Electricity and Electronics	I					
ESET 0121L: Basic Electricity and Electronics Lab	I					
ESET 0140: Applied Technical Intermediate Algebra						
ESET 0181: IT-OT Fundamentals	I	I	I	I	I	I
<b>Semester 2</b>						
ESET 0120: Introduction to Energy Systems	R	I	I			I
ESET 0120L: Introduction to Energy Systems Lab	R					
ESET 0122: Electrical Systems and Motor Control Theory	R					
ESET 0122L: Electrical Systems and Motor Control Lab	R					
<b>Semester 3</b>						
ESET 0223: Digital Control Theory	A	I	I			I
ESET 0227: Digital Control Systems Lab	A					
ESET 0242: Practical Process Control and Measurement	A					I
ESET 0282: Introduction to Networking						R
CYBR 3383: Security Design for Cyber-Physical Systems		R	R	R	A	R
CYBR 3384: Risk Management for Cyber-Physical Systems		R	R	R	R	R
<b>Semester 4</b>						
CYBR 4481: Defending Critical Infrastructure & CPS		A	R	A	R	R
CYBR 4486: Network Security for Industrial Environments		R	A	R	R	A
CYBR 4487: Professional Development and Certification		R	R		R	R
CYBR 4489: Capstone in Industrial CS		R	R			R

### 9.6.1.6 Alignment with proposed industrial cybersecurity content guidance

The table below shows the mapping between the program courses and the differentiated knowledge of industrial cybersecurity professionals presented in chapter 5 and Appendix B.

Table 28. Alignment between proposed knowledge and ISU's industrial cybersecurity program

Content	Courses
<b>Industrial processes and operations</b>	
industry sectors	ESET 0120, CYBR 4481
professional roles and responsibilities in industrial environments	ESET 0181, CYBER 4481
engineering diagrams	ESET 0122, 0122L, 0242
process types	ESET 0122, 0122L, 0242
industrial lifecycles	CYBR 4481
<b>Instrumentation and control</b>	
sensing elements	ESET 0223, 0227, 0242
control devices	ESET 0223, 0227, 0242
programmable control devices	ESET 0223, 0227, 0242
control paradigms	ESET 0223, 0227, 0242
programming methods	ESET 0181, 0223, 0227, 0242
process variables	ESET 0223, 0227, 0242
data acquisition	ESET 0181, CYBR 4486
supervisory control	ESET 0181, CYBR 4486
alarms	ESET 0181, CYBR 3383
engineering laptops/workstations	ESET 0181, CYBR 3383, 4486
configurators	ESET 0242
data historians	ESET 0181, CYBR 4486
<b>Equipment under control</b>	
motors/generators	ESET 0122, 0122L, 0242
pumps	ESET 0122, 0122L, 0242
compressors	ESET 0122, 0122L, 0242
valves	ESET 0122, 0122L, 0242
relays	ESET 0122, 0122L, 0242
generators	ESET 0122, 0122L, 0242
transformers	ESET 0122, 0122L, 0242
breakers	ESET 0122, 0122L, 0242
variable frequency drives	ESET 0122, 0122L, 0242
<b>Industrial communications</b>	
reference architectures	ESET 0181, CYBR 3383

industrial communications protocols	ESET 0181, 0282, CYBR 3383, 4486
transmitter signals	ESET 0122, 0122L, 0242
fieldbuses	ESET 0122, 0122L, 0242
<b>Safety</b>	
electrical safety	ESET 0100, 0121
personal protective equipment	ESET 0100, 0121
safety/hazards assessment	ESET 0100, 0121
safety instrumented functions	CYBR 3383, 4481
lock-out tag-out	ESET 0100, 0121
safe work procedures	ESET 0100, 0121
failure modes	CYBR 3383
<b>Regulation and guidance</b>	
presidential/executive orders	ESET 3384
IEC 62443	ESET 3383, 3384
NIST SP 800-82 R2	ESET 3384
NERC CIP	ESET 3384
<b>Common weaknesses</b>	
indefensible network architectures	ESET 2282, CYBR 4486
unauthenticated protocols	CYBR 3383, 4486
unpatched and outdated hardware/firmware/software	CYBR 3384
lack of training and awareness among ICS-related personnel	CYBR 3384
transient devices	CYBR 3384
third-party access	CYBR 3384
unverified supply chain	CYBR 4481
<b>Events and Incidents</b>	
DHS Aurora	CYBR 3383, 4481
Stuxnet	CYBR 3383, 4481
Ukraine 2015	CYBR 3383, 4481
Ukraine 2016	CYBR 3383, 4481
Triton	CYBR 3383, 4481
Taum Sauk Dam	CYBR 3383
DC Metro Red Line	CYBR 3383
San Bruno	CYBR 3383
<b>Defensive technologies and approaches</b>	
firewalls	CYBR 4486
data diodes	CYBR 4486
process data correlation	CYBR 4486
ICS network monitoring	CYBR 4486
cyber-informed engineering	CYBR 4481

cyber process hazards assessment	CYBR 4481
cyber-physical fail-safes	CYBR 3383, 4481
awareness and training for ICS-related personnel	CYBR 3384

#### **9.6.1.7 Course descriptions**

To provide greater detail about the course listed in the right column of Table 28, above, this section provides their catalog descriptions. This information may be of use for those seeking to design similar curriculum.

##### **ESET 0100 Engineering Technology Orientation: 1 semester hour.**

An introduction to the opportunities and responsibilities of engineering technicians and exposure to fields of technology. Introduction to the resources and college services that enable success in the ESTEC programs.

##### **ESET 0100L Engineering Technology Orientation Lab: 1 semester hour.**

A Laboratory introduction to the skills of an engineering technician. Includes an overview of industrial safety, tools, and electrical wiring.

##### **ESET 0121 Basic Electricity and Electronics: 4 semester hours.**

Fundamental principles of electricity, Ohm's law, Kirchhoff's laws, and circuit analysis applied to DC and AC circuits. COREQ: ESET 0121L.

##### **ESET 0121L Basic Electricity and Electronics Laboratory: 3 semester hours**

Basic principles of electrical measurement and testing of DC and AC circuits. COREQ: ESET 0121.

##### **ESET 0140 Applied Technical Intermediate Algebra: 5 semester hours.**

Topics in algebra, with an emphasis on solving equations and inequalities, systems of linear equations, quadratic equations, polar and rectangular coordinate systems, polynomial, absolute value, rational, and radical equations, inequalities, rational exponents, calculations and equations involving exponentials, logarithms and basic trigonometric functions. PREREQ: C- in MATH 0025, a Math ACT score of 18 or higher, an SAT score of 460 or higher, an ALEKS score of 30 or higher. COREQ: ESET 0101 or ESET 0121.

##### **ESET 0181 Information Technology - Operational Technology Fundamentals: 3 semester hours.**

Establishes fundamental understanding of information technologies for industrial control systems professionals. Topics include: operating systems, databases, programming,

and virtualisation. Establishes fundamental understanding of operational technologies for IT professionals. Topics include: PLCs, SCADA, HMIs, process diagrams.

**ESET 0120 Introduction to Energy Systems: 2 semester hours.**

Introduction to energy terminology, functions of power generation and mechanical processes, equipment, material, power cycles, mechanical physics and systems, and principles of heat transfer and fluid flow are covered. COREQ: ESET 0120L.

**ESET 0120L Introduction to Energy Systems Laboratory: 1 semester hour.**

Laboratory exercises in the maintenance and function of selected plant equipment, mechanical perspective of primary process equipment, and their sub-components are covered. COREQ: ESET 0120.

**ESET 0122 Electrical Systems and Motor Control Theory: 3 semester hours.**

Introduction to electrical system distribution and basic motor control including two- and three-wire control using a variety of devices and motor magnetic controllers. Control relays, time relays, solenoid valves, latching relays, and motor control centres. PREREQ: ESET 0121 and ESET 0121L or permission of instructor. COREQ: ESET 0122L.

**ESET 0122L Electrical Systems and Motor Control Theory Laboratory: 1 semester hour.**

Applications of electrical systems and motor controls. PREREQ: ESET 0121 and ESET 0121L or permission of instructor. COREQ: ESET 0122.

**ESET 0223 Digital Control Theory: 2 semester hours.**

Digital systems, digital control, analog-to-digital and digital-to-analog interfacing, signal conditioning, programmable controllers, computer application. PREREQ: ESET 0101, ESET 0101L, ESET 0102, ESET 0102L, ESET 0141, ESET 0142, or permission of instructor.

**ESET 0227 Digital Control Systems Laboratory: 1 semester hour.**

Computer and programmable controller interfacing with transmitters and final elements, PID loops, auto tuning, set up to complete control loops, computer graphics. PREREQ: ESET 0101, ESET 0101L, ESET 0102, ESET 0102L, ESET 0141, ESET 0142, or permission of instructor.

**ESET 0242 Practical Process Measurements and Control: 2 semester hours.**

Principles of temperature, pressure, strain, flow, force, and vibration measurements are covered. Techniques of computerised data acquisition, reduction, and statistical precision



and tolerance are reviewed. Signal for local indications and process control operation are also covered. Lecture plus Laboratory work in selected topics. PREREQ: ESET 0122 or permission of instructor.

**ESET 0282 Introduction to Networking: 3 semester hours.**

Facilitates competence in networking fundamentals: OSI model, TCP/IP, ports and services. Students identify networking equipment and functions, perform packet capture and conduct basic traffic analysis, and configuration.

**CYBR 3383 Security Design for Cyber-Physical Systems: 3 semester hours.**

Examines frameworks and practices for designing safety, reliability and security into critical cyber-physical systems, emphasising usability of these designs throughout the entire system lifecycle. PREREQ or COREQ: ESET 0181, ESET 0282, ESET 0223, ESET 0227 with a minimum grade of C-, or instructor approval.

**CYBR 3384 Risk Management for Cyber-Physical Systems: 3 semester hours.**

Course covers assessment and management of risk for industrial cyber-physical systems, including asset identification, threat analysis, vulnerability analysis, consequence assessment, mitigation techniques, and general incident response. Lecture/Lab Course. PREREQ or COREQ: ESET 0181, ESET 0282, ESET 0223, ESET 0227, CYBR 3383 with a minimum grade of C-, or instructor approval.

**CYBR 4481 Defending Critical Infrastructure and Cyber Physical Systems: 3 semester hours.**

Covers system of systems analysis and attack vector analysis as foundational frameworks to guide identification, selection and use of appropriate defensive techniques and technologies for critical infrastructure environments. Lecture/Lab. PREREQ: ESET 0282, CYBR 3383, CYBR 3384 with a minimum grade of C-, or instructor approval.

**CYBR 4486 Network Security for Industrial Environments: 3 semester hours.**

Provides review and analysis of security technologies and practices applicable to networks that support industrial environments. These include asset identification, network segmentation, access control, authentication, and anomaly detection. Examines security implications of wireless technologies. Lecture/Lab. PREREQ: ESET 0282, CYBR 3383 with a minimum grade of C-, or instructor approval.

**CYBR 4487 Professional Development and Certification: 3 semester hours.**

Covers theoretical knowledge and practical skills in preparation for international certification in cybersecurity. Emphasises professional ethics. PREREQ: CYBR 3383. PREREQ or COREQ: CYBR 3384, CYBR 4486, CYBR 4481 with a minimum grade of C-.

**CYBR 4489 Capstone in Industrial Cybersecurity: 3 semester hours.**

Professionally-oriented cybersecurity project, to synthesise knowledge and skills gained throughout the program. Develops lifelong professional learning strategies. Fosters professional communication proficiency. May be repeated once. PRE-OR-COREQ: CYBR 4486, CYBR 4481 with a minimum grade of C-.

**9.6.2 Challenges and objections faced**

As the author of this thesis has discussed this work in a variety of forums both internal and external to his institution, he reports significant opposition. The primary concerns fall in two categories: 1) that cybersecurity is a computer-science discipline and ought not to be taught outside a computer science department; and 2) that existing cybersecurity/information assurance-based paradigms and approaches adequately meet the education and training need for industrial, cyber-physical environments. These are both significant objections with significant consequences.

In regard to the former, it is noted that academic institutions tend to compartmentalise – to create silos due to the historic organisational structure of universities into colleges and departments. While such structure may be expedient in the academic environment, it can foster competition for scarce resources between departments with the potential to eliminate interdisciplinary approaches. In the case of Idaho State University, where the author has established the curricula described above, the Bachelor of Applied Science in Cyber-Physical Systems Engineering Technology, which incorporates a year of industrial cybersecurity courses, was able to overcome objections of a computer science department only with significant support from an external sponsor – the Idaho National Laboratory, whose leadership team (Associate Laboratory Director, Director of University Outreach, and Director of Supply Chain) wrote a letter to the University Provost in support of the Industrial Cybersecurity program that would incorporate cybersecurity skills specifically for engineering technicians.

In regard to the latter, established practitioners and academics often immediately disagree with the implication that the theoretical underpinnings of information assurance – namely the triad of confidentiality, integrity and availability is not sufficient. As noted in

section 2.1.1.1, and 9.4 of this thesis, compelling arguments exist that demonstrate this insufficiency; however, to be successful, such arguments require the objector to possess an open mind.

Empirically speaking, in the author's interactions with other industrial cybersecurity professionals, the discussion about the insufficiency of the triad is readily welcomed. The triad is also being questioned in more traditional cybersecurity events – for example, at the 2019 RSA Conference, Yu criticised the Triad, proposing an alternate approach (Yu, 2019).

## **9.7 Other Future Efforts**

In addition to the seven Future Efforts described above, for which some progress has occurred, there are four topics that may merit further consideration:

### **9.7.1 Sustainability/governing body**

As technology and the threat environment continue to evolve, so will workforce needs. The standards should include a mechanism for periodic review and improvement. 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 every-other year.

It will be desirable to engage with key international and global organisations, such as the Institute of Electrical and Electronics Engineers (IEEE), Association of Computing Machinery (ACM), and International Society of Automation (ISA) to promote adoption of the resulting standards through alignment with existing cybersecurity education and training standards.

### **9.7.2 Incentives for curricular development and program offerings**

The need for industrial cybersecurity education and training is not well understood. Speaking empirically, cybersecurity policy leaders, educators and practitioners alike seem to view industrial cybersecurity as a specialisation in the field rather than an area meriting a foundational level of attention. As the list of significant challenges in traditional cybersecurity continues to grow, this perception may not change easily. Policy leaders at the national and institutional levels should incentivise and support programs that explicitly provide education and training consistent with a robust content standard.

Professionals who understand industrial cybersecurity frequently command salaries with which educational institutions may not closely compete. Academically qualified (PhDs) professionals in the field generally do not exist. National policy makers and institutional leadership can foster relationships with potential instructors through unique approaches and incentives not available in the commercial world such as part-time fellowships, interaction with academic circles, bestowal of certain faculty benefits, and honorariums.

While recognising the importance of the role of governments in securing critical national infrastructures – which, importantly, include industrial control systems – it is concerning that the great demand for all types of cybersecurity professionals, and the relative lack of this industrial cybersecurity expertise, may keep industrial cybersecurity “lost in the crowd” to both educators and students.

The availability of an optional knowledge unit (even an improved and robust version) is, by itself, unlikely to incentivise the level of professional development the nation needs. As a result, governments should incentivise qualified individuals and institutions to develop entire programs that infuse engineering professionals – who design, build, operate, and maintain industrial control systems on developed economies rely – with required cybersecurity knowledge and skills.

### **9.7.3 Development of hands-on curricular materials**

Due to its cyber-physical nature, an industrial cybersecurity educational program carries equipment costs which schools may not be prepared to assume. It is unreasonable to prepare students to defend critical industrial systems when they have never seen or touched the core components of those systems. As noted in section 9.1, participants in the inaugural Industrial Cybersecurity Education and Training Workshop felt that hands-on training was the most significant challenge.

Using the knowledge areas and items advanced in Chapter 6, it is possible to identify elements that would benefit from hands-on experience – though the experience should not be limited to this list:

#### **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

- industrial communications protocols
- transmitter signals
- fieldbuses

#### Safety

- personal protective equipment
- safety instrumented functions
- lock-out tag-out

#### Defensive technologies and approaches

- Firewalls
- Data diodes
- Process data correlation software
- ICS network monitoring software
- Cyber-physical fail-safes

Because student learning will be enhanced when students can see and understand the physical consequences associated with cyber-attacks – instructional laboratories will require special foresight around student and instructor safety.

Government education policy makers and institutional leadership can fund capital expenditures and maintenance of educational ICS security laboratories, given that these programs adhere to the appropriate educational standards. Education policy makers and institutional leadership should seek opportunities to partner with ICS equipment suppliers and local industry partners who normally own and operate this equipment to achieve an appropriate balance of virtual, simulated, and hands-on learning experiences.

#### **9.7.4 Evaluation**

Another potential area of investigation is evaluating the effectiveness of industrial cybersecurity education and training offerings. One general standard for discussing evaluation of instruction is Kirkpatrick (Kirkpatrick Partners, n.d.), who has advanced four levels of evaluation, as follows:

*Level 1: Reaction -- The degree to which participants find the training favorable, engaging and relevant to their jobs*

*Level 2: Learning -- The degree to which participants acquire the intended knowledge, skills, attitude, confidence and commitment based on their participation in the training*

*Level 3: Behavior -- The degree to which participants apply what they learned during training when they are back on the job*

*Level 4: Results -- The degree to which targeted outcomes occur as a result of the training and the support and accountability package*

Several authors mention evaluation concepts in the context of industrial cybersecurity education, such as Sitnikova (2013), which explores the power of hands-on exercises; Deshmukh (2016), which discusses plans to evaluate the effectiveness of Laboratory interventions; and, Ban (2017), which explores the effectiveness of experiential learning.

Notwithstanding these examples, given the lack of consensus around what should be taught as highlighted in Chapters 1-8, and the concern that prevailing cybersecurity paradigms may be inadequate as discussed in section 9.4, evaluation along the lines of Kirkpatrick's four levels may merit additional attention.

#### **9.8 Conclusion**

This chapter has identified and described ten future efforts that build from the base of the research described in previous chapters. Six of these efforts (establish an industrial cybersecurity workforce development community of practice, create CSEC-17 style knowledge area, contribute to foundational paradigms, additional validation and refinement relying on a combination of cognitive and behavioral approaches, establish career pathways, and create an example curriculum) have begun to show promise, where four have (ensure sustainability, create incentives for curricular development, develop foundationally aligned

hands-on training materials, and evaluate the effectiveness of educational offerings/approaches) are important, but budding ideas.

This appears to be the opening of a fruitful field of research and practice involving hundreds or even thousands of academics and professionals from academia, government and industry across significant industry verticals and nations.

## 10 CONCLUSION

This work began with concern about developing a workforce supply chain capable of securing the critical cyber-physical systems on which modern economies and societies increasingly rely. An exploration of that concern led to the identification of the primary research question “What is the foundation for the formal preparation of industrial cybersecurity professionals?”

In order to address this question and the sub-questions it implies, the researcher undertook a mostly qualitative multi-phase mixed-methods approach.

The first sub-question for resolution became “what are the criteria for a strong foundation?” Relying on critical literature review, Chapter 4 of this thesis advanced eleven such criteria, which it derived from, and compared with, nine existing cybersecurity education and training documents/efforts. The thesis found each of the nine existing efforts was deficient in some significant way.

Noting that the identified criteria required inclusion of clearly differentiated industrial knowledge, the next sub-question became, “what does that knowledge include? Employing the nominal group technique with a group of industrial cybersecurity subject matter experts from the Idaho National Laboratory, the author described the identification of two starting blocks for progress towards a solid foundation: knowledge categories and archetype roles. The nominal group technique has strong inherent validity, and the results underwent additional triangulation and peer review, as described in Chapter 5.

With differentiated industrial cybersecurity knowledge established, the following sub-question became “why should those identified knowledge items be included?” This question is particularly important for an emerging field with significant differences from traditional cybersecurity given that some instructors may be unfamiliar with the proposed knowledge items and would need additional context to truly guide curricula development. Chapter 6 addressed this issue through the researcher’s own reasoning and careful triangulation with 1) the existing Automation Competency Model provided by the International Society of Automation; and, 2) a list of significant industrial cybersecurity events.

Recognizing that the education and workforce development models reviewed in chapter 4 lacked a common structure and lexicon, next sub-questions became “what model should be used?”, and what are the relationships among the components of the model?” In Chapter 7, relying on critical insights, and work of leading education and workforce



development theorists, the researcher advanced an alternate model built on the concept the Archetype role. The aim of the model is aid in conducting job task analyses, designing curricular materials, and evaluating both individual proficiencies, and educational program effectiveness.

With the archetype roles advanced in Chapter 5, and the workforce development framework advanced in Chapter 7, the next question emerged “what tasks does each archetype perform?” The researcher collaborated in five focus groups with ten additional subject matter experts from the Idaho National Laboratory tlaborao produce a list of key tasks performed by each archetype role. The resulting list of tasks is provided in Chapter 8. While additional work is necessary to ascertain the validity of these task lists, it provides a reasonable point of departure.

The table below addresses the degree to which the work advanced in this thesis meets matches against the 11 foundational criteria advanced in chapter 4.

*Table 29. Foundational criteria for industrial cybersecurity education and training addressed in this thesis*

<b>Criteria</b>	<b>Addressed in thesis?</b>
1. Addresses industrial cybersecurity	Yes
2. Clearly differentiates industrial	Yes
3. Consensus-based	Partial
4. Qualified participants	Yes
5. Publicly available	Yes
6. Includes knowledge	Yes
7. Justifies knowledge	Yes
8. Includes job roles	Yes
9. Includes tasks	Yes
10. Sector specific content	Partial
11. Evidence of empirical validation	No, but describes plans to validate empirically
<b>TOTAL</b>	<b>9/11</b>

The table shows that the work herein presented comes close to meeting the criteria. The most-pressing deficiencies are the attainment of broader consensus and the inclusion of empirical validation – using behavioral methods.

## 10.1 Limitations

The author's prevailing critical paradigm does not allow for satisfaction by merely providing an initial answer to the key research question: "What is the foundation for the formal preparation of industrial cybersecurity professionals?"; rather, it requires that the answer to the question be implemented to provide such a foundation. This aim gives rise to one significant critique and two significant limitations – or challenges.

The leading critique, as has been recognised several times throughout the thesis, is that the work lacks broad acceptance because it was developed with limited participation. Though the work in chapters 5, 6, and 8 regarding archetypes, differentiated knowledge, and tasks, involved about 25 different individuals (who were qualified subject matter experts), this does not yet reach the threshold for being "consensus-based." A consensus would require a much broader degree of input from a variety of qualified and documented professionals, who represent diverse experiences and perspectives.

The two prevailing challenges are interrelated. The first involves convincing traditional cybersecurity academics that industrial cybersecurity truly merits a differentiated approach. Academics require a long lead time to create. They are steeped in the traditions of their supervisors. They operate in siloed colleges and departments. They rely on established foundations to describe their work. They may be disconnected from the needs of practitioners. Academics often teach with words rather than with hands-on learning experiences. While none of those characteristics prevents adoption of a new approach, they do generally work against it.

The second is encouraging adoption of the work. Given the strong demand for cybersecurity professionals in general, the specialized needs of industrial cybersecurity could easily be overlooked – programs accustomed to preparing general cybersecurity professionals could claim that their preparation also applies to industrial environments, and no one would ever know the difference.

As a result of these limitations, chances for success will be maximized through alliances with influential organizations and thought-leading individuals, collaboration with like-minded academics, and publication of clear consensus-based foundational work.

## **10.2 Future Research Directions**

Owing to the quantity of work in progress, the author elected to dedicate a chapter to this topic (Chapter 9). This work-in-progress not only furthers the main thrust of foundations for industrial cybersecurity education and training, but begins to address the broad research questions raised during initial literature review. Of special note are: 1) plans to conduct a broad survey of industry professionals to push the differentiated knowledge identified herein toward a defensible “consensus”; and 2) plans to engage small groups of subject matter experts to explain how key cybersecurity tasks in industrial environments differ from similarly named tasks in traditional information system environments. Each of these will be addressed by engaging the budding Industrial Cybersecurity Workforce Development Community of Practice, co-founded by the author (Industrial Cybersecurity Community of Practice).

APPENDIX A:  
DETAILS OF STRUCTURED LITERATURE REVIEW ON “OPERATIONAL  
TECHNOLGY”

To gauge the evolving use of the term “operational technology”, the authors reviewed the contents of the IEEE Xplore database. This search returned 104 results with publication dates between 1984 and 2020. The authors reviewed each paper to determine whether the term matched the description that it “covers industrial control systems, supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), industrial sensors/transmitters, and actuators” advanced in Chapter 2 – Literature Review. The term as examined within 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.

*Table 30. IEEE publications using term "operational technology"*

<b>Pub. Year</b>	<b>Document Title</b>	<b>Author</b>	<b>Use of "operational technology"</b>	<b>Security primary context?</b>	<b>Addresses IT-OT Gap?</b>
1984	30/20-GHz domestic satellite communication system in the public communication network of Japan: Design and operation	Tanaka	unrelated	n	n
1991	Analysis tools in preparation for Radarsat revisited: Evaluation tools for SAR data exploitation	Saper	not found	n	n
2001	A new method for valuing R&D investments: a qualitative and quantitative evaluation	Naukkarinen	unrelated	n	n
2001	OSCAR-object oriented segmentation and classification of advanced radar allow automated information extraction	Benz	unrelated	n	n
2002	The aeronautical data link: taxonomy, architectural analysis, and optimization	Morris	not found	n	n
2003	An integrated service and network management system for MPLS traffic engineering and VPN services	Kim	unrelated	n	n
2008	A Distributed Simulation Environment for Simulation Modeling in Operational Risk Management	Aleksy	unrelated	n	n
2012	Managing Technology in a 2.0 World	Andriole	unrelated	n	n
2012	Next generation emergency management common operating picture software/systems (COPSS)	Balfour	unrelated	n	n
2012	Implementation of Fuzzy neural-network genetic algorithm based on MCGS	Xianghua	unrelated	n	n
2013	Relative Navigation and Guidance Technologies for Rendezvous and Docking	Kai	unrelated	n	n

2014	Industrial systems: cyber-security's new battlefield [Information Technology Operational Technology]	Piggin	related	y	n
2014	Remote monitoring and control of wastewater assets delivering reduced whole life costs	Rama	related	n	n
2014	Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety	Piggin	related	y	y
2014	Optimizing Operational and Strategic IT	Andriole	unrelated	n	n
2014	Observation and measurement in disaster areas using industrial use unmanned helicopters	Sato	unrelated	n	n
2014	Challenges & opportunities towards smart grid in Turkey; Distribution system operator perspective	Atasoy	related	n	n
2014	A new data classification methodology to enhance utility data security	Rajagopal	related	y	n
2015	Eyes on the Ocean applying operational technology to enable science	O'Neil	unrelated	n	n
2015	Optimal control of Spacecraft Docking System using integral LOR controller	Nandagopal	unrelated	n	n
2015	Leveraging Internet of Things Technologies and Equipment Data for an Integrated Approach to Service Planning and Execution	Jalali	related	n	n
2015	6TiSCH centralized scheduling: When SDN meet IoT	Thubert	related	n	n
2015	Factors for successfully integrating operational and information technologies	Kuusk	related	n	n
2015	State Based Network Isolation for Critical Infrastructure Systems Security	Conklin	related	y	y
2015	A new integrated charging infrastructure analytics service platform and applied research	Zhang	related	n	n
2016	Active defence using an operational technology honeypot	Piggin	related	y	y
2016	IET: cyber security in modern power systems: IT and operational technology integration	Hough	related	y	n
2016	Cyber norms for civilian nuclear power plants	Spirito	related	y	y
2016	Security threats of Internet-reachable ICS	Abe	related	y	n
2016	A private machine-cloud architecture and self-reliant controllers for operational technology systems	Tran	related	y	n
2016	Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security	Litherland	related	y	n
2016	Using a knowledge-based security orchestration tool to reduce the risk of browser compromise	de Leon	related	y	n
2016	The importance of testing Smart Grid IEDs against security vulnerabilities	Weerathunga	related	y	n

2016	Cyber security in modern power systems defending the grid	Gray	related	n	n
2016	Grid-aware VPP operation	Glomb	related	n	n
2016	Towards a new generation of industrial firewalls: Operational-process aware filtering	Hachana	related	y	n
2016	Security intelligence for industrial control systems	Amrein	related	y	n
2017	Practical security education on operational technology using gamification method	Yonemura	related	y	n
2017	Combining cybersecurity and cyber defense to achieve cyber resilience	Galinec	related	y	n
2017	Cyber Security in the Energy World	Ang	related	y	n
2017	Industrial IoT business workshop on smart connected application development for operational technology (OT) system integrator	Goto	related	n	y
2017	Enhancing integrity of modbus TCP through covert channels	Taylor	related	n	y
2017	Practical cybersecurity for protection and control system communications networks	Manson	related	y	n
2017	Poster Abstract: Design of Intelligent Software Systems for Cyber-Physical Systems	He	related	n	y
2017	Intelligent network assets supervision and control in Enedis	Lagouardat	related	n	n
2017	Research on evaluation method for operation economy and technology of regional smart energy grid	Yuan	related	n	n
2017	Challenges for citizens in energy management system of smart cities	Burbano	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	Obaidli	related	y	n
2017	A framework for consumer electronics as a service (CEaaS): a case of clustered energy storage systems	Oh	not found	n	n
2017	Cyber security in production networks – An empirical study about the current status	Nüßer	related	y	n
2017	RAMI 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges	Schulte	related	n	n
2017	Benchmarking Cloud-Based SCADA System	Yi	related	n	y
2017	Big data and cloud computing platform for energy Internet	Fu	related	n	y
2017	Pay up - or else [IT Ransomware]	Hayes	related	y	y
2017	Elektro Gorenjska CIM project	Rozic	related	n	n
2017	Semantic communication between components for smart factories based on one M2M	Willner	related	n	n
2018	Effect of security education using KIPS and gamification theory at KOSEN	Yonemura	related	y	y

2018	VOTNET: HYBRID SIMULATION OF VIRTUAL OPERATIONAL TECHNOLOGY NETWORK FOR CYBERSECURITY ASSESSMENT	Sarkar	related	y	n
2018	On the Secure and Stable Operational Technology for Multi-DC Asynchronous Power-Sending Grid With High Proportion of Renewable Energy	Wu	related	y	n
2018	IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing	IEEE	related	n	n
2018	IEEE Approved Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing	IEEE	related	n	n
2018	Helping IT and OT Defenders Collaborate	Fink	related	y	y
2018	Ontology Based Resource Management for IoT Deployed with SDDC	Koorapati	related	n	y
2018	IT-OT Integration Challenges in Utilities	Garimella	related	y	y
2018	IEEE Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing	IEEE	related	n	n
2018	Implementing a performant security control for Industrial Ethernet	Giehl	related	y	y
2018	Security Education Using Gamification Theory	Yonemura	related	y	y
2018	Dimensioning wireless use cases in Industrial Internet of Things	Liu	related	n	n
2018	Healthcare data classification – Cloud-based architecture concept	Miškuf	related	n	n
2018	SHARP: Towards the Integration of Time-Sensitive Communications in Legacy LAN/WLAN	Seijo	related	n	n
2018	METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security	Jillepalli	related	y	n
2018	Optimizing the Scheduling of Autonomous Guided Vehicle in a Manufacturing Process	Yao	related	n	n
2018	Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Networks	Stout	related	y	n
2018	Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems	Fraile	related	y	n
2018	Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5	Apriliana	related	y	n
2018	Peer-to-peer Detection of DoS Attacks on City-Scale IoT Mesh Networks	Rausch	related	y	n
2018	Cyberattacks on Primary Frequency Response Mechanisms in Power Grids	Krishna	related	y	n
2018	Challenges and prospects of communication security in real-time ethernet automation systems	Müller	related	y	y
2018	The Industrial Internet of Things	Hassan	related	n	y

2019	Integrating Cyber Security Requirements into a Power Management System	Preston	related	y	y
2019	Towards Virtualization of Operational Technology to Enable Large-Scale System Testing	Ansari	related	n	n
2019	Technical risk synthesis and mitigation strategies of distributed energy resources integration with wireless sensor networks and internet of things “ review	Payne	related	y	y
2019	A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard	Alem	related	y	y
2019	Performance analysis of a Solar Photovoltaic Power Plant	Cavalcante	unrelated	n	n
2019	Preventing False Tripping Cyberattacks Against Distance Relays: A Deep Learning Approach	Khaw	related	y	n
2019	Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0	Karampidis	related	y	y
2019	Enhanced Uptime and Firmware Cybersecurity for Grid-Connected Power Electronics	Moquin	related	y	n
2019	Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era	Polge	related	y	n
2019	Coexistence Standardization of Operation Technology and Information Technology	Felser	related	n	n
2019	MimePot: a Model-based Honeypot for Industrial Control Networks	Bernieri	related	y	n
2019	Towards Optimal Cyber Defense Remediation in Cyber Physical Systems by Balancing Operational Resilience and Strategic Risk	Hasan	related	y	n
2019	Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure	Kapellmann	related	y	y
2019	Securing connection between IT and OT: the Fog Intrusion Detection System prospective	Colelli	related	y	y
2019	Cyber security threats in industrial control systems and protection	Marali	related	y	y
2019	Wireless Network Design for Emerging IIoT Applications: Reference Framework and Use Cases	Liu	related	n	y
2019	Factors Affecting Cyber Risk in Maritime	Tam	related	y	y
2019	A reference architecture for IIoT and industrial control systems testbeds	Craggs	related	y	y
2019	Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins	Eckhart	related	y	n
2019	Forensic Readiness within the Maritime Sector	Tam	related	y	y
2019	Analyzing availability and QoS of service-oriented cloud for industrial IoT applications	Mustafa	related	n	n



2019	Intelligent Edge Control with Deterministic-IP based Industrial Communication in Process Automation	Badar	related	n	y
2019	Analysis and Detection of Cyber-attack Processes targeting Smart Grids	Cerotti	related	y	n
2019	Design and Development of Modbus/MQTT Gateway for Industrial IoT Cloud Applications Using Raspberry Pi	Sun	related	n	n
2019	Replacement Controller for IoT-Enabled Dependable Control Systems	Tran	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: NSA-CAE STYLE KNOWLEDGE UNIT

### Characterization of The NSA CAE Knowledge Unit

As a principal component of the CAE designation process, the NSA CAE Knowledge Units can be found publicly on the NSA National Information Assurance Education & Training Programs (NIETP) web site [9]. The Knowledge Units for organizations seeking designation in 2020 are organised into four categories: Foundational, Technical Core, Non-Technical Core, and Optional [10]. Each Knowledge Unit includes the following five components: statement of intent, outcomes, topics, specializations, and related knowledge units, as displayed in Figure 1.

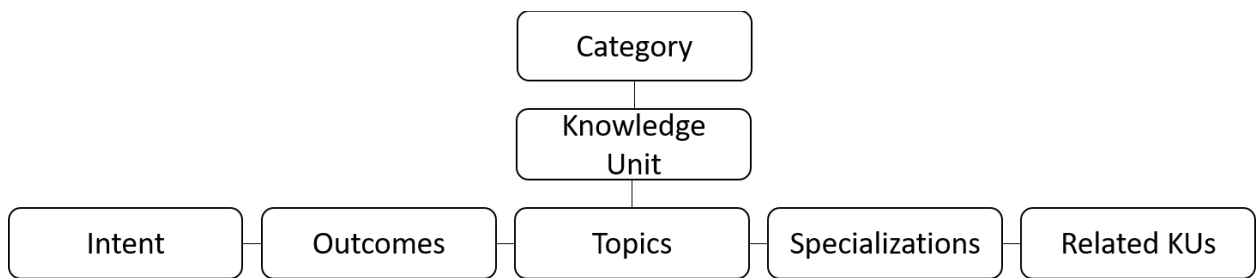


Figure 26. NSA CAE Knowledge Unit organization

This structure seems intuitively reasonable. The term “specialization” represents a group of related knowledge units that, when included in the designation or re-designation package, earns the qualifying institution said specialization [11].

### Methodology

Many of the elements of the NSA CAE Knowledge Unit structure were created by the efforts described in Chapters 5 and 6 of this thesis; however, two pieces of matching content were missing: a statement of intent and learning outcomes.

The researcher 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.

To create the learning outcomes, the researcher sought to merge the “foundational understanding” phrase from the statement of intent with the detailed topics generated in our session, to describe what a student should reasonably be able to do upon completion of the educational experience. So, the researcher limited verbs to lower-level cognitive domain from Bloom’s taxonomy: “describe”, “identify”, and “explain”.

Then, the researcher employed key nouns from the outcomes to imbue the intent statement with foreshadowing continuity. The result is produced below:

### **Resulting NSA CAE-Style 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, industrial lifecycles)
- Instrumentation and control (sensing elements, control devices, programmable control devices, control paradigms, programming methods, process variables, data acquisition, supervisory control, alarms, engineering laptops/workstations, configurators, data historians)
- Equipment under control (motors/generators, pumps, compressors, valves, relays, generators, transformers, breakers, variable frequency drives)
- Industrial communications (reference architectures, industrial communications protocols, transmitter signals, fieldbuses)
- Safety (electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented functions, lock-out tag-out, safe work procedures, failure modes)
- Regulation and guidance (presidential/executive orders, IEC 62443, NIST SP 800-82 R2, NERC CIP)
- Common weaknesses (indefensible network architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, third-party access, unverified supply chain)

- Events and Incidents ((DHS Aurora, Stuxnet, Ukraine 2015, Ukraine 2016, Triton, Taum Sauk Dam, DC Metro Red Line, San Bruno)
- Defensive technologies and approaches (firewalls, data diodes, process data correlation, ICS network monitoring, cyber-informed engineering, cyber process hazards assessment, cyber-physical fail-safes, awareness and training for ICS-related personnel)

### **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.

The author believes that Outcomes 3-5 (IT/OT differences, common weaknesses, unique defensive approaches) and Topics 6-9 (regulation, common weaknesses, events and incidents, defensive approaches) presented above would be helpful (though certainly not sufficient) in developing industrial cybersecurity awareness, training and education for individuals who already have an OT-related background.

## APPENDIX C DATA FROM NOMINAL GROUP TECHNIQUE

12 February 2019

Note: This appendix provides the actual collected from the 15 participants in the nominal group technique session. Spellings and punctuation have not been standardized.

Specific job titles within this ICS field .....	245
Good ideas w/o a home .....	245
Manager .....	245
Engineer .....	246
Technician .....	247
Analyst .....	248
Education .....	249
Job roles that merit immediate development .....	250
Unique ICS Knowledge .....	252
Control Knowledge .....	252
Communications .....	255
Regulations .....	256
Instrumentation & Control .....	256
ICS Knowledge for immediate development with verbs for action .....	257
Control Knowledge .....	261
Equipment .....	265
Communications .....	266
Regulations .....	267
Instrumentation & Control .....	267

## **Discuss Field Difference**

Description:

Question: Drag ideas into a sub-folder, originally, Describe why this field is different.

### **A. Availability is paramount**

Unlike IT OT requires that systems be always available. Sometimes there is never a good time for taking systems down. Sometimes it's during a planned outage.

### **B. CIA upside down**

Availability is the most important aspect of the security effort, not confidentiality.

#### **B.A. Establishing process on how to apply ICS security controls**

NIST 800-82 specifies the AIC overlay for NIST 800-53's CIA proposition for security control families when striving to apply some standardization on security approach.

However, 800-82 needs to be extended to specifically teach to ICS SCADA/Architecture components, controllers, and devices.

OR in conjunction with an effort, such as the one pursued today, there needs to be a new NIST document for formal process that bridges 'GENERAL' cyber security considerations into a more focused area of ICS cybersecurity focus. Potentially with categories specific to the cyber-physical realm and cyber-digital realm that are 'unique' to ICS.

### **C. Consequence**

We are not protecting information, we are protecting products, personnel, the environment, the public, our quality of life.

### **D. Nature of Data Communications**

The ICS data communications by necessity are typically deterministic in nature.

Interruptions causing delays in data traffic internal to devices and between devices can significantly impact normal operational behavior.

#### **D.A. Is CIA even the right paradigm?**

Aren't ICS really more about the physics than the information?

#### **D.A.A. Depends on the ICS**

The aggregation of measurements or processes could be considered information

#### **D.A.A.A. Process data is information, but that makes it similar to IT**

I thought we wanted to get at how IT is different from ICS. I am not sure CIA is the right approach for ICS at all.

#### **E. Safety**

Unlike IT systems OT systems have a direct physical consequence and therefore they can have a direct impact on the safety of workers and/or the public at large.

#### **F. ICS Cyber Pro's Understand Systems**

ICS Cyber professionals need to understand the systems being controlled so that they know where the vulnerability

##### **F.A. how to mitigate**

not just where the vulnerabilities lie but more importantly ICS Cyber Pros will need to understand the best way to mitigate the vulnerabilities in a way that will not adversely impact the process

##### **F.B. What is it about the system they need to understand?**

To protect the financial infrastructure those professionals must understand their systems too.

##### **F.B.A. the physical process**

But in ICS the Cyber and OT pros need to have an understanding of the physical process that is being controlled by their systems. In IT it ends with the systems.

##### **F.B.A.A. Agree with importance of understanding the process**

This is an important part of understanding the risk. If you don't understand the impact of failure in the differing parts of the ICS, you can't effectively assess the risk it poses.

A financial IT security person needs to know the information they must protect and can tweak their security posture to protect that information. A parallel could be drawn to the ICS security person knowing which are the most important components and why.

##### **F.B.A.B. Makes sense to me that we are talking about physical process**

Physics, chemistry, electricity, thermodynamics, failure modes, faults

##### **F.C. Unless its a small utility understanding is usually split**

The folks that understand the process generally are not managing the IT/OT systems even in utilities. When we arrive onsite for an incident usually only the IT/IT security people are in the room. If you ask OT questions to try to get context the utility's own IT people

generally do not know. If you ask OT personnel they generally have little to no knowledge of the cyber systems. How can we expect third parties such as government/academia to have a better handle on this if the utilities keep the knowledge separate and the government/academia have very little access to the devices, configuration, and context of the systems?

## **G. Expertise**

Individuals need to understand how industrial control works in addition to how information systems work.

### **G.A. Expertise**

I agree. Understanding of the whole system is needed, so the information system can work correctly.

## **H. Why ICS is Different**

Building Controls are, for the most part, not payed attention to and are therefore vulnerable.

## **I. Why ICS cyber security is different than IT Security**

Requires a different set of language - specifically NIST 800-82 is where most IT folks need to realize a different baseline for how to speak about ICS topics and architectural components

### **I.A. What specific language?**

Are there certain terms of art and practice that everyone needs to know?

#### **I.A.A. sector specific?**

It seems like some things are "OT" wide but in many cases each industry or sector has their own language

## **J. Needed security data missing**

In many cases the system information that has become common place in the IT world does not exist in the OT world (for a variety of reasons).

## **K. Utilities are Extremely Risk Averse**

The utilities are most interested in safety and availability. Other security services (confidentiality, integrity, nonrepudiation) have a much lower priority. They are hesitant to share information to include architecture and configuration data to help facilitate



secure architecture design, vulnerability discovery, and to support hunting for adversaries because of fear of regulatory fines or loss of business.

#### **K.A. Lack of Information Sharing**

Across government and industry there is a distinct lack of information sharing.

##### **K.A.A. Doesn't the lack of information sharing apply elsewhere too?**

Fewer people are assigned to ICS, but normal security has poor info sharing too.

##### **K.A.B. Unfriendly Utilities**

Very accurate. Utilities typically do not play well together. They will typically only share pertinent electrical system info, i.e. short circuit, MVA, etc. never coordinating between systems.

#### **L. Management Chain**

In an industrial environment you have engineering and plant operations groups that you don't have in corporate IT.

#### **M. Obsolescence**

Typical OT equipment can be designed to last for decades instead of a 3-5 year refresh cycle. Securing these "obsolete" devices in the OT space is much different than in the IT space where they can be replaced on the next refresh cycle.

##### **M.A. There are some pretty old IT systems out there too**

Windows XP is still all over the place globally. Maybe update practices aren't the same. Maybe it's really the linkage between hardware and software that is different. That is, once the ICS device is deployed it is more work to update than a common IT system. Maybe patch rates in ICS compare with BIOS updates in IT because they require a similar level of effort.

#### **N. Must have broad knowledge of multiple devices**

ICS Cyber professionals have to keep up to date on all of the various manufacturers physical devices and the differences between them

##### **N.A. Don't IT guys have to keep up on lots of device types too?**

Sure, the vendor names are different, but keeping up with the technology seems way harder on the IT side than the ICS side.

##### **N.A.A. How is it harder?**

There are so many resources available to the IT security professional, including conferences and training, online materials (websites, coursera and YouTube videos) and any number of books available at the local library or online bookstores.

Contrast that with the difficulty in getting technical documentation that describes the ICS system and devices that make up that system; often a mix of multiple vendors who's one job is to ensure inter-operability. Many ICS vendors are very reluctant to "give away" any of that information to someone who isn't purchasing their devices, posing another level of complexity to gaining access to ICS "training" resources. Even more scarce is ICS security-related information in similar forms available to the IT security professional mentioned above.

**N.A.A.A. Also, isn't that the whole reason we're here?**

see title

**N.A.B. ICS devices and training can be more difficult to obtain**

Unless you work for the vendor or a company that utilizes a particular ICS device it can be difficult to procure and realistically setup some types of ICS equipment given the lack of a real-world environment, funding constraints, or a vendor not wanting to sell you the device for research/testing. The device may no longer be made or sold. This limits how much 3rd parties such as government, academia, and other outsiders can adequately prepare to defend, assess, and recover from any attacks on these pieces of equipment. IT hardware is much more broadly available, better documented, and supported.

**O. Legacy Control Systems**

ICS systems are specific to a process that may not change for years. Updates to the ICS software are not implemented due to the potential impacts to the devices.

**P. Why ICS is Different**

Building controls are being integrated and must be able to co-exist and function across all systems. With security.

**Q. Systems are long term**

OT systems are long term investments that will stay in place for decades not months/years.

**R. Why ICS is different**

ICS Cybersecurity is different from IT cybersecurity because ICS could prove disastrous to lives, vs IT mostly affecting money. While companies can recover assets from loss of money, lives that are lost will never be recovered.

#### **S. Operational Impact to business and the public**

ICS systems are typically utilized to monitor and operate critical operations to an entity. Downtime or abnormal operations can cause direct safety implications, loss of revenue through interrupted process operations, direct loss of services with life safety implications to large service areas.

#### **T. Objectives**

ICS is interested in preserving the safety, reliability and controllability of the system/process rather than the confidentiality, integrity or availability of the information

#### **U. Why ICS Cybersecurity is different than IT Security**

The architectural components for ICS and how they interact are different than normal IT operations. Specifically there are 5 major blocks in an ICS system to consider: 1.) Control Systems (servers/workstations) 2.) HMI (Human Machine Interface) 3.) The communication (network) 4.) Field Controllers (PLC, RTU, IED...) 5.) Field Devices (sensors)... It is critical that these components are understood in order to secure an ICS system

#### **V. Why ICS is Different**

Security for all systems is important. If one is available for attack, then all are susceptible.

#### **W. Must understand multiple communication protocols**

Control systems generally provide integration between systems that use a wide variety of communication protocols. Each protocol has different strengths and weaknesses

#### **X. Why ICS cyber security is different**

There are many factors that make ICS cyber security different from IT cyber security. There's the timing of processes which must happen on set intervals. There are limitations on resources (embedded components which are designed to be very specialized to a given process). And there's the component of reliability; a failure in an IT system is an inconvenience, where as a failure in an ICS could very likely result in physical consequences (power loss, fire, flood...)

## **X.A. Resource limitations seems reasonable**

But don't older IT systems also suffer from resource constraints. Think about upgrading a Cisco switch. Older devices cannot run the newer versions of the OS.

### **X.A.A. IT equipment will most likely cost less to replace vs ICS**

Additionally, the argument about resource limitation was highlighted to point out that as an ICS security professional, adding in modern security protections (like anti-virus or host-based monitoring) is unrealistic when it comes to the limited resources of an ICS device.

## **Y. lack of authentication**

Many (if not most) field devices and communication protocols do not require any sort of authentication basically the PLCs are sitting there waiting for someone to tell them what to do .

### **Y.A. lack of authentication comment**

This is true. If you have access to the device and have the right program. You can do anything you want to the system, including re-programming.

#### **Y.A.A. Lack of authentication occurs elsewhere**

It might be more acute and widespread, but not necessarily a key differentiator

## **Z. Utility IT and OT personnel do not communicate**

There is a lack of IT knowledge among many Operational Technology personnel and a lack of OT knowledge among IT personnel. There is also a lack of trust and communication. When an incident occurs at a utility they usually start communicating and discovering issues on both sides of the system with the way things are designed, managed, and monitored. The utility Security Operations Center (SOC) is usually completely staffed with IT personnel. The SOC generally is unable to detect odd behaviors unless the impact is significant enough.

## **AA. Where you find the ICS devices is different**

ICS devices are designed to run in harsh environments and because of that, emphasis on engineering reliability often takes precedence over security

## **AB. Training Differences**

ICS requires a hands-on environment to truly deliver impactful training. The access to an extensive ICS hands-on environment or the funds to create one for students is out of reach for most academic institutes.

#### **AB.A. Roles for ICS are generally polarized**

Agree totally that an ICS environment requires hands on environments to deliver impactful training and difficult to provide.

Extending this thought it appears that in many industries, businesses, etc. that the group that does ICS is somewhat polarized by two factions:

- 1.) Operators who are segregated from IT and want to keep it that way and so they do not have the opportunity to learn about cyber nor is it in their 'worry'-list' Their job is to keep things running
- 2.) IT/business/management personnel who have some cyber training but do not understand the 'operating' characteristics of ICS systems so they think that operators should apply all company policies and procedures to their area

#### **AB.A.A. Non Cyber Savvy management**

Often Management over operations/production don't have the background to understand all of the differences in cyber.

#### **AC. Sustainability**

The majority of today's power systems are connected remotely, typically through communication protocols which are vulnerable to attack.

#### **AC.A. Aren't certain IT protocols vulnerable to attack too?**

Sure the protocols are different, but essentially it is the same problem as exists with HTTP or FTP, right?

#### **AC.A.A. The consequence is different**

in the OT space the consequence is different. If you send a signal to a PLC that tells it to open the breakers that provide power for a whole city (in December?) then the PLC will do just that. The lack of encrypted protocols or protocols/devices that require authentication raises this risk and must be mitigated.

#### **AC.A.A.A. Consequence**

It seems that consequence is a key differentiator

#### **AD. Patching**

ICS is patched 'yearly' vs. on a regular schedule due to the inability for a company to provide down time in an industrial setting. Specifically, IT's answer for vulnerabilities is to apply the latest patch but the need for system availability trumps the need for changing the vulnerability

#### **AE. ICS Design and Risk Management**

The "rules" and methods used for risk management and the design and implementation of ICS were developed long before digital technology was incorporated into the systems. The foundational principles of functionality, reliability, and safety have driven the "rules" and methods, and a balance is achieved between them that reflects the realities of applications. Security as a principle has traditionally been achieved through isolation

#### **AF. Support from vendors using own PC**

Vendors usually want to come to a facility and use their own PC that could introduce risk

#### **AG. Lack of Field Controller capability**

Typical legacy PLC, RTU and other types of field controller devices do not have the processing capability or configurability to support implementation of basic security controls.

#### **AH. System used against itself**

Attacks may not look malicious at all. In fact, the system may behave as intended other than a process or a portion of the process happens outside of intended schedule or design bounds.

#### **AI. ICS Incident Response Procedures are not Documented**

The context, tools, and techniques for preserving the necessary information and accurately analyzing the data to support detecting and responding to an incident on ICS equipment is not well defined. Vendors are often the only good source for such data and the generation of that information is ad hoc and reactionary to current events not proactive.

#### **AI.A. Is it that the problems are not documented?**

Is it a lack of documentation or a lack to tools and techniques?

#### **AJ. Apprenticeships can Fill Gaps**

Utilizing an apprenticeship approach, such as in the medical fields, to degree programs can address learning gaps for students, business owners/operators, universities, and researchers.

**AJ.A. Like the idea, but how to ensure an element of security?**

Agree that it could fill the gap of gaining exposure to OT, but how might you ensure that good security training is happening at the same time?

And what about the impact to the host providing the apprenticeship opportunity. I anticipate reluctance in participating if there's too much of a cost to providing the opportunity (risk of messing something up, time spent, etc...)

Is there some sort of benefit for the host?

**AK. Lack of Info Sharing**

Different Utilities do not want to share THEIR system security with other companies, as they are in it for profit. If everyone has the same security feature, then what is to stop one from "snooping" on the other.

**AK.A. See Utilities are Risk Averse title above**

The two topics are following the same line of discussion....

**AL. legacy "wireless" communications**

There is still a lot of un-encrypted "wireless" communication going on in various industries.

**AL.A. There are lots of wireless comms in regular IT too**

Not sure that unsecure wireless is different from non-ICS industries

**AL.B. More to come**

With everyone wanting the convenience of modern IT access (from a mobile device, or remote location via vpn), it seems that this is only the beginning.

**AL.B.A. Seems that you are getting at the design paradigm**

It's not that wireless is different, its that the systems being connected were not designed with that idea in mind.

**AM. Operational Orgs not Cyber Resourced**

Typically find smaller ICS organizations have not implemented policy and procedures related to cybersecurity and are often stovepiped from their own enterprise IT security

capabilities that can be leveraged to help them improve. Alongside this is a gap in OT to IT understanding of the differing needs of the two organizations.

#### **AN. Integration with business networks**

I guess this could be titled the air gap is dead, nearly every business has a distinct business need that requires the Process control network and the business network to be connected. This connection brings a higher degree of risk and must be managed.

#### **AO. Physical access to PLC must be restricted**

If someone with malicious intent has physical access to an ICS network and a basic understanding of the system real damage can occur

##### **AO.A. Physical Access**

In other industries, Physical access is not needed. Just access to the network or workstation.

##### **AO.A.A. remote facilities**

Remote facilities with PLCs and/or extensions of the control network must be protected differently than facilities on the 'main campus'. Physical control and monitoring not just of the "shack" but of the PLC cabinet, network control and monitoring.

#### **AP. Adoption of New Technology**

IT world has driven much of the new technology that has been developed in the resiliency and cyber security world. Accordingly, there are efforts to force the OT world to adopt these advancements without an understanding of risks. This coupled with a long lifetime, makes it difficult to positively react to the realization of these risks.

#### **AQ. The Learning Environment for Cybersecurity has no Boundary**

Unlike other static degree subjects, the dynamic threatscape of cyber (IT & OT) warrants that a continual learning environment must be developed that does not end at completion of a degree. Possibly the legacy hierarchical degree system (BS, MS, etc.) does not apply to this field and a totally new system of board certifications tied to dates (or like software versions) is the measure of a person's level of expertise.

#### **AR. Control from your couch**

There has been a push for the convenience of mobile device apps to be added to the ICS systems. This convenience of allowing an operator to have visibility and control from the



break room must be balances with the ability to monitor and control from across the globe.

#### **AR.A. Use of Mobile Devices in ICS**

New technology does not necessarily mean good technology for implementation into ICS operations. Security ramifications must be weighed and implemented as policy vs perceived convenience.

#### **AS. OT Personnel Not Cyber Aware**

OT groups often lack understanding of the cybersecurity field. Why they should care? How to properly protect their ICS resources while supporting business access to operational data, appropriate methods for password implementation and compensating security controls that support operations.

#### **AS.A. Grew up from Process Engineering**

I think that this speaks to the general lack of OT and OT Cyber pros. Many OT groups are comprised of people who "grew up" from their process engineer roles or from the I&C roles.

#### **AS.B. Training paradigm**

I agree that cyber has not been baked into engineering/technician trainings

#### **AT. ICS cyber security monitoring non-existent or immature**

Tools that can reliably understand the ICS protocols, behaviors, and unique configurations are often non-existent due to a lack of research and investment. There are many protocols that lack publicly available parsers for helping understand the behaviors. It can be difficult to obtain the necessary real-world and synthetic data for the development and validation of these parsers to support more advanced detection tools and analytics. Deployment of such tools often requires partnering with vendors that have hardened industrial platforms where the tools can be run. Commodity based hardware is unlikely to receive support from OT staff for deployment in harsh environments.

#### **AU. Reliance on Physical Defenses**

Often physical countermeasures are relied upon to mitigate against cyber-attacks. While this is a good failsafe, it also discourages the development of appropriate first-line defenses that could be used as a more cost-effective/scalable solution.

## **AV. ICS Policies and Procedures**

Many companies do not have specific 'documented' policy, procedures, or process specific to ICS. They do have procedures and processes that they follow but often it is not documented and is only carried through generations of tribal knowledge from operator to operator -

## **AW. System components**

Many earlier products that control ICS have very weak cyber engineering. For example, a PLC controller that allows a 4 digit PIN/password may be easily cracked. Much of the ICS equipment in industry is dated and performed way beyond its service life.

## **AX. Business risk associated with OT Cybersecurity**

OT cybersecurity is generally underfunded and staffed due to the inability of OT managers to adequately quantify cybersecurity impact and consequence to the overarching business operations and leadership.

### **AX.A. Don't security groups always lack funding?**

Security folks always want more stuff to do their job. Isn't the problem really a lack of leadership awareness?

## **AY. Use of Digital Technology in ICS accepted risk**

The incorporation of digital technology in ICS without adapting traditional design and risk management principles (failure mode analysis) has allowed the misuse of digital technology in ICS to become an "unanalyzed" but possible outcome. Reliance on separation as the fundamental design principle for security is a single point failure in our engineering processes.

## **AZ. Data Collection is Hard**

The collection of needed cyber related data is difficult to do (provided that it exists). This is true for both network and host based data.

## **BA. Automation systems assigned to IM or Mech. Eng.**

Most facility owners do not know who to put in charge of the automation system. Since it has a network connection it usually defaults to the IM staff or because it controls a piece of mechanical equipment the Mechanical Engineer gets put in charge.

### **BA.A. Well put**

Being able to establish who should be in charge is highly significant.

#### **BB. OT Design Participation**

OT Operations and Management is often not involved in business design efforts to ensure that appropriate cybersecurity requirements are not considered in project implementation.

#### **BC. ICS Change Control mechanisms and Asset Control Inventory**

Many companies expend thousands of dollars on change control for software development, software installation and upkeep, but do not have a formal change control process because they may not even know what is on their ICS systems. It is critical to have an accurate asset control inventory and then only append, delete, or modify this through some form of change control

##### **BC.A. lack of staff**

minimal staffing levels have made this worse, as most companies are at a point where a physical walk down will be necessary for a proper inventory but there is barely enough time to put out the fires.

##### **BC.B. Lack of purpose built tools**

I think this goes back to the training paradigm. Those building these systems never thought about lifecycle management or an evolving threat environment.

#### **BD. IT/OT Divide**

Too often the IT group and the OT group are at odds with each other instead of leveraging the strengths that each group brings to the table.

#### **BE. Support from Vendors**

In the Fire Alarm Industry, each company has their own software on their own PC. If they don't update their PC security or have none at all, this could be cause for concern.

##### **BE.A. a real threat**

This is a real threat/risk that most companies do not address. Unfortunately it's not limited to vendor machines. It's fairly common for I&C techs to have a single laptop that they use for work in the field and that they also use for internet browsing and email. This effectively bypasses all of the network access controls that the entity has implemented.

##### **BE.B. Out-moding**

Often times vendors cannot patch or fix discovered vulnerabilities, so they will force asset owners to purchase new equipment. This is costly and time intensive as processes may need to be redesigned.

## **BF. Testing and Demonstration of Changes**

OT ICS production systems require fully testing of changes through patches, modifications and operational set points and controls prior to implementing into the production operations. ICS cannot sustain downtime due to operational misconfigurations and patches that may result in unintended machine operations or failures. Offline testing is needed to validate.

### **BF.A. IT systems have to undergo testing before deployment too**

Testing before deployment seems quite similar across IT and OT. Maybe the issue has more to do with timelines or lack of test set-ups.

## **BG. How does Academia Adapt to Dynamic Learning**

In some academic subjects, a Professor can teach for 20+ years with no substantial changes in their subject areas. That is not the case with cyber security. Does the creation of ICS learning standards also apply in some way to the Professors teaching the curriculum? Should Professors teaching in cybersecurity related fields be required to "re-certify" or test every few years on subject matter regarding the latest cyber threats, impacts, mitigation methods, cyber tools, new AI, etc.?

## **BH. Ignore ICS until it doesn't work**

ICS a lot of times are deployed by a vendor and the system owner does not really pay attention to what was done or how they are configured until something breaks and it doesn't work.

## **BI. Data Analytics are a nascent capability**

Provided the needed security data exists and can be collected, the ability to determine what is good/bad or expected/abnormal is just be looked at. The IT world is already moving to automate much of this process away from the human analyst into computer-aided solutions.

### **BI.A. Most OT operations not implementing**

Generally, data collection is not being performed in OT ICS environments, or if it is collected, it is not being monitored routinely or having rules updated to keep current with

threatscape. Analytics are way out on the horizon and only being dreamed of in the OT world.

#### **BJ. Utilities not Incentivized to Hire Cyber Security Experts**

Unless an incident has been detected it can be difficult to justify the money needed to obtain individuals with OT cyber security experience. These individuals are hard to find and therefore more expensive. Electric utilities can justify charging customers for cyber security sensors in their rate cases; however, the personnel hired to manage these systems are funded out of profits. Reducing profits to fund something where the value is difficult to quantify usually means that the investment is not made.

#### **BJ.A. Not sexy to be an operator - where is the \$**

Agree with this comment and would add -- one more reason why ICS standards should exist and perhaps lead to an ICS cert or engineering credential like PE for ICS.

Not generally is an ICS operator dinner table conversation with your high-school sophomore or junior when you ask them 'what do you want to be when you grow up?'

#### **BJ.B. Security is not a profit center**

The fact that security "cuts into profits" is the same for IT and OT. It seems to me that the difference is the management chain that has to make the pitch or the spend.

#### **BJ.C. Operators Excluded from Cybersecurity Responsibilities**

The operator is generally the first line of defense or detection of an anomaly to their system. They have a unique sense of when something just doesn't look right. They are not part of the cybersecurity discussion in many OT organizations. Those roles are typically SCADA/ICS administrators or engineers and they don't want to bother the operators since the operations staff typically rise up from technical or craft roles in the organization and won't understand it anyway.

#### **BJ.C.A. agree 100%**

I always used my operators as the canary in the coal mine

#### **BK. Support from Vendors**

If different companies install the same Fire Alarm Panels, then they all have the program to access the panel. All they need is physical access or access to a network.

#### **BL. Dated components**

Much of the ICS hardware is so dated that the companies that built them no longer support them. This means patches and other maintenance into the system is unavailable.

#### **BM. ICS updates/redundancy cost prohibitive - virtualization**

Many ICS systems are so antiquated because the mantra in business is if it aint broke don't fix it. Give me a business reason to put in a PLC that is 'more secure' and I will pay for it -- if not my 'concrete batching' system is running just fine, thanks. Due to the holistic and interconnected nature of ICS systems it is very difficult cost wise for a public utility, or really any business to have a redundant system with which to perform cyber exercises (planned or unplanned failure analysis) As such understanding how to create virtual means of impacts on upgrades to ICS and redundancy is a critical step in providing a semblance of ICS security without impacting production

#### **BN. ICS security and the "trust" paradigm**

Traditional ICS was a closed system built using electro-mechanical and analog devices. The failure modes of each of these devices could be defined, tested, and documented to develop a "trust" in the system. This trust has been directly translated to digital "general purpose" devices that have a potential for misuse in addition to the nominal "failure" modes that defined and tested for. This trust paradigm is a defining weakness in existing risk and design processes.

#### **BO. ICS network device sensitivity**

Most ICS systems have a significant mixture of legacy and newer technology devices that tend to be sensitive to security scanning operations. It is recommended to not scan these networks due to the potential of disruption to operations.

#### **BP. ICS Device Logs Are Not Well Documented/Understood**

ICS devices may log events that indicate bad activities; however, the analysts and even the security tools may have never seen such events before and the monitoring systems may not provide sufficient alerting capability. The logging capability may lack the fidelity needed in order to determine what actually occurred. The vendor most likely had other reasons besides cyber security for developing the logging capability.

#### **BQ. System Components**

This is true in the Fire Alarm Field as well. We are asked to keep panels running passed their end date. To the point where parts have to be purchased off of eBay. (I'm not kidding!)

### **BR. Downstream Impacts**

ICS systems and their various components don't work in a bubble. Attacks that affect one piece may provide unforeseen (or actually planned) multi-order effects. Butterflies and Hurricanes are real problems.

### **BS. Resiliency**

Today's utilities are focusing as much on resiliency as they have been on safety and finances. Unplanned outages are costly and detrimental.

### **BS.A. Enemy is among us**

IT Cyber security has been trying to adopt a mentality that the enemy is already within the system. This is even more important on the OT side. How does one maintain process availability while sustaining an attack?

### **BT. Unknown devices**

Many organizations either don't know that they have control systems or are just becoming aware of them. Even then, they don't fully understand what kind of impact could result from the system being attacked.

### **BU. Missing Tactical Understanding**

Many engineers and operators don't fully understand the impacts of adding cyber to their systems, or not adding cyber to their systems. This becomes more complex when early career staff are integrated with mid and late career staff.

### **BV. Operations Good at what they Do**

Disagree with this comment. Operations are generally very good at running and maintaining their operations given the funding levels they have to work with. Their operations staff are often taught on the job and are very competent. They may not know cyber but they know their process and their systems well.

### **BW. New components**

Some of the new IC components are not engineered with any security in mind. It is a race to connect as much as you can. It would be nice if there was a requirement of security or

an industry standard that manufacturers had to implement in order to produce/market some of their networked components.

#### **BX. leverage the safety culture**

Most if not all ICS operate in a business that has a very strong safety culture. It seems to me that if we leverage the physical safety culture to promote cyber security "safety" we will be more successful in changing the culture.

##### **BX.A. Safety is enormous**

Agree that safety is one thing not nearly as present in IT

#### **BY. Agile Method to Impart New Threat/Mitigation Information**

New cyber threat and mitigation information is broadcasted weekly to an unsuspecting audience. The audience is not truly unsuspecting, but unknowing. Unknowing that is of their control system/network architecture and types of devices it contains. So receiving the weekly broadcasts of new cyber threats and mitigations goes unnoticed. The new ICS learning standards must incorporate a mechanism for students to take the cyber "broadcasts" and apply them to actual control systems.

#### **BZ. ICS shares enterprise network**

As ICS devices have been deployed over the years they typically were assigned an IP address and placed on the network without any cyber security concern. With the explosion of the IoT more and more people are adding devices at break neck speed without consideration of security. In many cases the IM staff are finding devices on their networks that they do not know what to do with, so they end up together. In the end you have an ICS network that was not coordinated or designed with the potential for conflicts between devices.

##### **BZ.A. IOT and IIOT**

Agree that IOT and IIOT devices are an area that needs focus, how do we recommend that infrastructure be set up. In the past we would tell people to have a process control network with no internet access and very limited and controlled access to the business network through a DMZ. Now we have devices that require internet access to function properly (AI and cloud analytics).....

#### **CA. Models and versions**



Even as vulnerability information is released, many organizations don't know what equipment they have and what versions are being used. This type of inventory makes it difficult to utilize the information that is being provided.

### **CB. ICS unique operator/cyber skill based on sector/manufacturer**

Depending on the type of control system an operator may or may not be 'easily' portable from one system to the other. In IT a router is a router and a switch is a switch -- no matter if it is Cisco or an IBM device. With ICS, depending on the system there may be a different manufacturer that focuses on that specific sector. It is really difficult to say that if you train an ICS operator in cyber techniques that all learning ports to multiple sectors. One more reason business justification for a cyber-operator is hard to build, manage, and keep employed.

#### **CB.A. Working environment/interfaces are definitely different**

IT folks don't deal with I&C technicians, operators, etc.

### **CC. Context is critical in understanding system**

Even if you use the same devices, the way they are configured and the downstream equipment that they are attached to cannot be easily ascertained through passive monitoring. That information is not found within the raw data collection. There is no geolocation database, no whois, sometimes no DNS to help you identify the appropriate behaviors and prioritize which systems should be reviewed even if the devices are using IT based protocols for communication.

### **CD. One Size fits all Security for ICS will not be as effective**

ICS systems are purpose built to control different physical processes in different operations contexts. IT systems only handle information in different operational contexts. The added complexity of designing for both different processes and operations will diminish the effectiveness of "one size fits all" security solutions that work in IT. Functionality, reliability, Safety, and Security need to be considered and balanced for most applications on a more individual basis

#### **CD.A. agree**

I agree that one size fits all will not work mainly because the process networks we are protecting are not one size fits all. With rare exceptions each and every ICS environment was custom built to solve a particular problem with a particular process.

### **CE. Cyber Sec with ICS vs BMS**

Almost every discussion that I have been involved in focuses on ICS, PLCs, SCADA, very few people seem to care about the BMS (Building Management System). In my mind these two systems are on a collision course where they are becoming more and more integrated. At the INL we have two distinct groups one that does PLC work and the other that does the BMS work. More and more system operators want to have data from both systems together in one place which means that they will need to be integrated. Most BMS systems use BACnet that is designed to be open without a whole lot of security.

### **CF. IT / OT convergence - dependence (IoT)**

It is interesting that one can focus on the differences between IT and OT. However, one way of helping those who only know IT is to provide them with how OT and IT are alike. In many instances the IT and OT system(s) are integrated in a cyber security sense. With the world of IoT this convergence and dependence is increasing and in order to secure your OT is probably not an independent exercise from securing IT.

### **CG. There are no good serial monitoring systems**

ICS equipment often uses various flavors of serial communications. There are a few proprietary devices/software packages for collecting the serial traffic; however, they are usually designed for troubleshooting/development purposes and not for monitoring many serial connections on a massive scale for cyber security. These proprietary software packages often make it difficult to export the collected traffic to be used in other tools. Parsing the serial traffic into events that can be timestamped is also problematic. What is an event? There are some devices that packetize the serial communications; however, these are usually packetized based on data volume not on particular communication events. It can also be difficult to analyze multiple serial collections in aggregate form when there are not unique addresses to identify the source devices.

## **Specific job titles within this ICS field**

Description:

Question: What are specific job titles within this ICS field? Click on the light bulb looking icon to enter a **title** to initiate **your** Brainstorm and tab down to a description area and define your brainstormed title. When you submit your idea it is forwarded to the group by clicking on the letter looking icon and then the group will view your idea. This is strictly brainstorming and the ideas can be viewed; however there is not a discussion on any idea.

### **Good ideas w/o a home**

#### **A. ICS Cyber Security Trainer**

ICS engineer or operator versed in practices and processes for securing ICS systems with relevant training background

#### **B. ICS Instructor**

#### **C. Control Systems Vendor Relations Specialist**

#### **D. ICS Cyber Security Intern**

#### **E. ICS Insurance Agent**

### **Manager**

#### **A. operations manager**

#### **B. Chief ICS Security Officer**

CICSSO?

#### **C. Cybercore Tech Director**

#### **D. Control System Cybersecurity Officer**

#### **E. ICS Administrator**

#### **F. CICSSO**

Chief ICS Security Officer

#### **G. project manager**

#### **H. CEO**

#### **I. CIO/CISO**

#### **J. Chief Operations Officer**

#### **K. Facility/Plant Manager**

Needs a basic understanding of the vulnerabilities of the systems under their preview

**L. ICS Cyber Plant Manager**

Individual that has ICS operator and/or ICS engineering experience that has ICS security responsibilities for an entire plant or manufacturing process that covers one or multiple Infrastructure sectors

**M. Copy of operations manager**

**N. Copy of operations manager**

**Engineer**

**A. Process Control Engineer**

**B. ICS Cyber Engineer**

An ICS cyber expert that knows both IT and ICS cyber security practices and is proficient in securing ICS systems within an IT rich environment

**C. ICS Network Engineer**

**D. Protection and Relay Engineer**

Utility-based

**E. OT Cyber Engineer**

**F. ICS Design Engineer**

**G. Industrial Cybersecurity Engineer**

Responsible for conducting and overseeing cyber informed engineering

**H. I&C design engineer**

**I. ICS Security Architect**

**J. operations (systems) engineer**

**K. project engineer**

**L. Resiliency Analyst/Engineer**

**M. quality assurance engineer**

**N. safety engineer**

**O. Commissioning Agent/Engineer**

**P. IT/ICS Integrations Engineer**

**Q. DCS/Utility Engineer**

**R. Control System Engineering Specialist**

**S. Microgrid/SCADA Engineer**

**T. Sales engineer**  
**U. ICS Fault Detection Engineer**  
**V. process engineer**  
**W. Grid Integration Engineer**  
**X. Engineering Specialist - Security**  
**Y. vendor hardware developer**  
**Z. vendor software developer**  
**AA. Sector Subject Matter Expert**  
**AB. ICS System Programmer**

### **Technician**

#### **A. Operators**

Need cybersecurity awareness

#### **B. Industrial Cybersecurity Technician**

Graduate from 2 year program much like I&C technician who is responsible for doing cyber things on the plant floor.

#### **C. ICS Cyber Technician**

#### **D. ICS Network Technician**

#### **E. Control System Cybersecurity Specialist**

#### **F. I&C Technician**

Needs to have some cyber background to securely deploy, implement, and configure

#### **G. Commissioning Technician**

#### **H. ICS Change Control Specialist**

An engineer, operator, or manager that has experience with change control mechanisms and is able to participate in/within other boards and structures to illuminate the uniqueness of ICS change management

#### **I. instrument technicians**

#### **J. lineman**

#### **K. Control System Specialist**

#### **L. electrician**

#### **M. dispatcher**

**N. ICS Network Technician**

**O. field service representative**

**P. ICS Graphical Interface Specialist**

**Q. Control System Inventory Specialist**

Tracks device make, model, versions, software, etc...

**R. Relay Technician**

**S. ICS Cyber Field Control Specialist**

An individual with ICS operations or ICS engineering experience that can provide secure recommendations for the purchase, placement, replacement, maintenance, and secure practices for one or more infrastructure sectors in the field controller and field device space of ICS.

**T. ICS Design Drafter**

**U. HVAC technician**

**Analyst**

**A. Analyst**

ICS Security Analyst

**B. Operations risk analyst**

**C. Controls System Forensic Analyst**

**D. ICS SOC Analyst**

**E. ICS Incident Response Analyst**

**F. ICS cyber risk analyst**

Maps the current internal ICS environment against the evolving external threat environment to provide a continuous picture cyber risk

**G. OT SOC Analyst**

**H. ICS Cyber Researcher**

**I. ICS Incident Response Analyst**

**J. Vulnerability Analyst**

**K. Junior Cyber Security researcher**

**L. ICS Analyst**

**M. ICS Network Analytics Officer**

**N. ICS Auditor**

**O. Help Desk analyst**

As more and more OT stuff becomes IT stuff the help desk needs to be aware of the differences

**P. ICS Assessor**

An individual that has ICS operator or cyber information assurance experience that is able to 'assess' an ICS environment and illuminate vulnerabilities and threats in a prioritized fashion

**Q. ICS Threat analyst**

**R. ICS threat analyst**

Analyses the external environment. Sets up indications and warnings system. Provides early warning of attack against ICS.

**Education**

## Job roles that merit immediate development

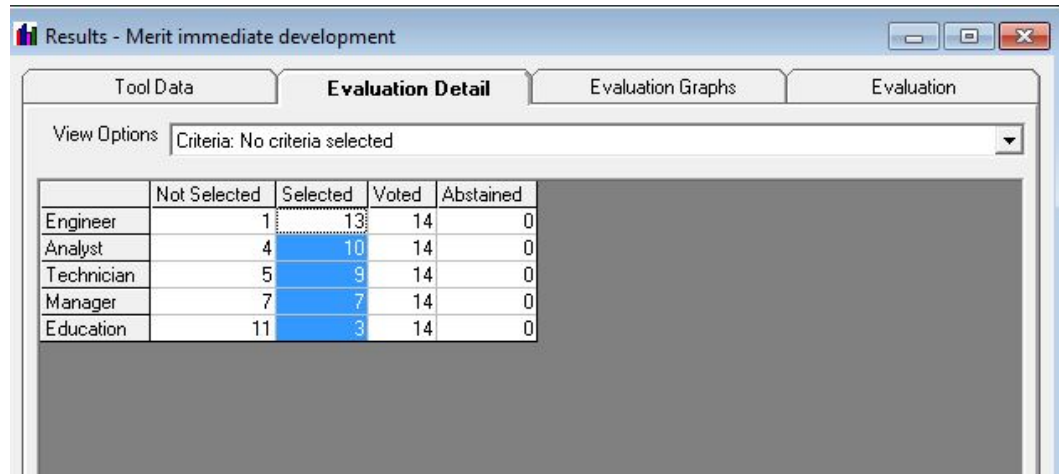
Description:

Question: Select Three titles that merit immediate development

The evaluation was executed against root level folders.

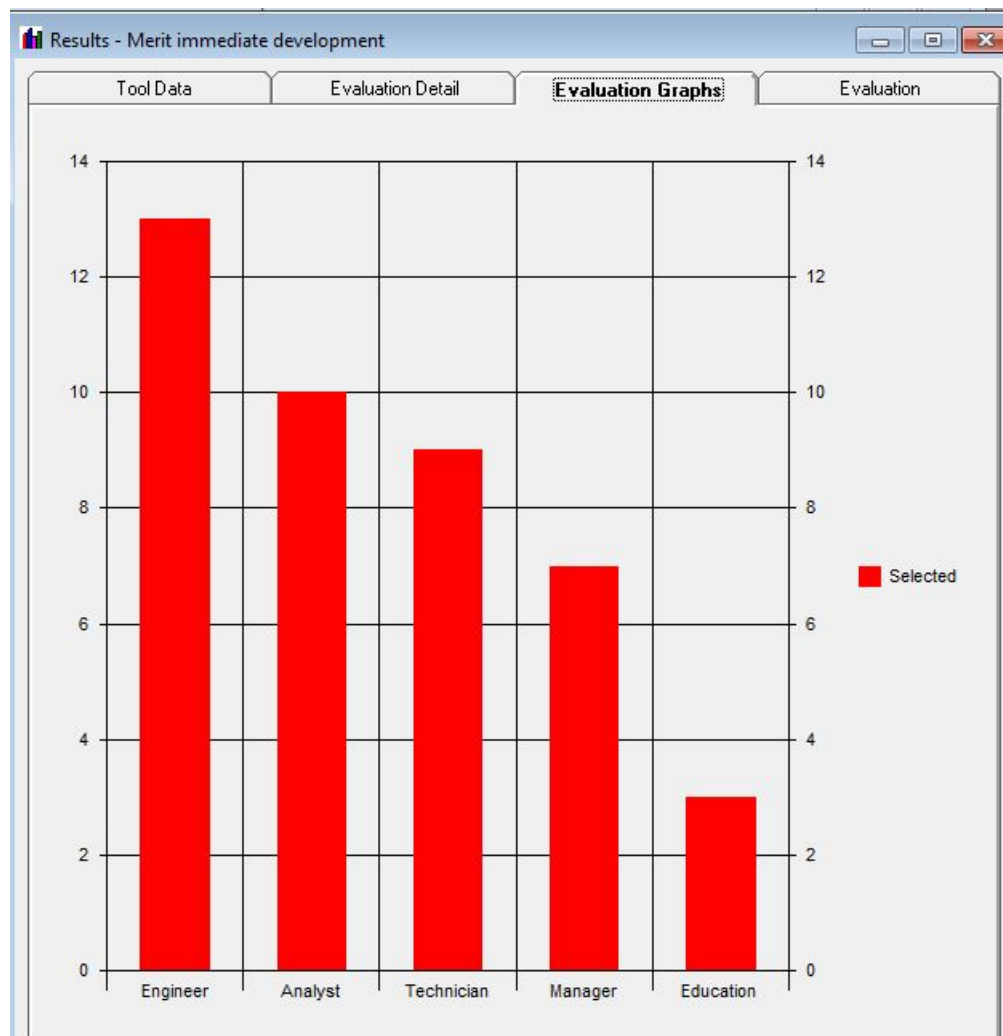
No criteria selected

Select Three titles that merit immediate development



	Not Selected	Selected	Voted	Abstained
Engineer	1	13	14	0
Analyst	4	10	14	0
Technician	5	9	14	0
Manager	7	7	14	0
Education	11	3	14	0





## **Unique ICS Knowledge**

Description:

Question: What unique ICS Knowledge used by individuals across all titles?

### **Control Knowledge**

**A. common language**

**B. Knowledge of Mechanical Systems**

**C. System Integration**

**D. fail safe mode**

**E. common language defined**

Need to be able to have common terms and definitions for ICS, components, and security mechanisms unique to ICS

**F. Availability**

The process needs to be up.

**G. Ladder logic**

**H. interconnections between systems**

common interfaces and communication media

**I. Building Administration**

**J. Understand the Physical Process**

Need to understand the physical properties of the process the ICS is measuring and controlling. How can you sense or measure the parameters that matter, and how you can control the physical variables

**K. ICS Systems are generally unique**

Seen one IT system seen them all -- ICS Cyber professionals likely need 'sector' specific knowledge and understanding

**L. process control**

**M. Safety Issues**

**N. fairly static environments**

In general ICS environments are more static than IT

**O. Basics of electrical substations (for the power ICS)**

Power transfer and storage

**P. Process Hazards Assessment**

What physically could go wrong

**Q. patching**

Patching is not always viable

**R. Maintenance**

cyber maintenance for ICS differs from IT traditional systems

**S. Process Specific Paradigm**

ICS is used to monitor and control many different types of processes in many Sectors. An ICS support person must understand the process to the level that it can or may be impacted by the work being performed.

**T. Real-time Requirements**

The process demands real-time information to function.

**U. live with vulnerabilities**

Sometimes we will choose to live with documented vulnerabilities and mitigate the issue.

**V. preventative maintenance****W. Historical examples of what did go wrong**

Some examples of past events which were either caused by cyber incidents or other errors, and how they could've been prevented

**X. resiliency/sustainability****Y. Legacy hardware vs new hardware (firmware differences)****Z. Common failure types**

Welded contacts, loose wires

**AA. Understanding of the operational context of the process**

Need to understand the operational context of the physical process that is being controlled. this can be functional - private industry vs government or physical - on land vs on a ship,

**AB. Educational / training differences**

Most IT Cyber professionals have a strong computer science background - Operators / ICS Cyber expertise does not have a 'mapped' path to success - varies - mostly home grown within a business or industry

**AC. Common areas where ICS and IT overlap/mesh**

**AD. configuration management**

**AE. Motion control**

**AF. Determinism**

**AG. Piping and instrumentation diagrams**

**AH. Engineering prints**

**AI. ohms law**

**AJ. deadband**

**AK. Physics-based restrictions**

OT deals with the constraints of the real world. Just because you can tell a computer to do it, doesn't mean that the system can handle it.

**AL. oscillation**

of control loop toward set point

**AM. set point**

**AN. ladder logic**

**AO. function block**

programming language

**AP. Existence of Legacy Systems**

Many entities utilize old and unsupported operating systems and controllers that are no longer supported by vendors.

**AQ. Major ICS vendors**

**AR. 'Working' is King**

If a solution works, then there will be resistance to change it.

**AS. ICS failure modes**

Loss of supervisory control loss of local control stale data

**AT. Need to understand the risk profile of the ICS**

Need to understand the impact if the system fails or is misused. Describe the function it performs and the criticality of that function.

**Equipment**

**A. vfd**

**B. power systems**

**C. Long-life equipment**

Systems are designed to be in place for decades.

**D. Powered backup systems**

**E. Motor control centers**

**F. pumps**

**G. Valves**

**H. pneumatics**

**I. hydraulics**

**J. ups**

**K. electric circuits**

**L. transformers**

**M. boilers**

**N. generators**

**Communications**

**A. serial protocols more common**

**B. Deterministic Data Communications**

Generally Process logic relies on data being sent and received on a fairly strict timing sequence or logic in order to allow the process control logic to function properly.

**C. Specific communication protocols used in the ICS world**

modbus, BACnet, Profibus, CCN, Lonworks ect.

**D. communication medium differences**

IT connectivity is different then OT connectivity mechanisms (protocols, cabling...)

**E. Industrial Ethernet Protocols**

EtherNet/IP (CIP), Modbus, DNP3, ICCP, OPC, BACnet, Profinet

**F. weak network stack**

No active scanning

**G. Fieldbus protocols**

HART, Foundation Fieldbus

## **H. ICS Protocols**

Different industries and applications tend to utilize different types of protocols specifically designed for ICS applications.

## **I. Propriety protocols/architectures**

Many of the systems do not use common/open protocols and/or architectures.

## **J. ICS Data Communications Mediums**

ICS systems utilize a wide diversity of communications systems which leverage different technologies internal and external to the entities they support. Includes fiber, copper, wireless, satellite, etc. All require different understanding of cybersecurity implementations.

### **Regulations**

#### **A. Different regulatory frameworks**

#### **B. regulatory environment**

NERC CIP, CFATS, API

### **Instrumentation & Control**

#### **A. PLCs**

#### **B. instrumentation**

#### **C. plc**

#### **D. hmi**

#### **E. Controllers**

programmable controllers, remoter terminal units

#### **F. panel-mount HMI**

#### **G. transmitter**

#### **H. SCADA/HMI**

#### **I. relays**

#### **J. process control**

#### **K. vibration monitoring**

#### **L. Control element**

#### **M. sensing methods**

thermocouples, flow meters

## **ICS Knowledge for immediate development with verbs for action**

Description:

Question: These are the ICS knowledge for immediate development. Drag the verbs to define what action is performed in a standard for each brainstormed knowledge.

### **Instrumentation & Control**

Acts

Address

Addresses

Adhere

Allocates

Alters

Analyze

Analyzes

Answers

4.2.10. Apply

4.2.11. Apply

4.2.12. Appraise

4.2.13. Arrange

4.2.14. Assemble

4.2.15. Assign

4.2.16. Assist

4.2.17. Breaks Down

4.2.18. Build

4.2.19. Build-In

4.2.20. Categorize

4.2.21. Change

4.2.22. Choose

4.2.23. Cleans

4.2.24. Cognizant-Of

4.2.25. Combine

4.2.26. Compare

4.2.27. Compile  
4.2.28. Comply  
4.2.29. Comply-With  
4.2.30. Compose  
4.2.31. Conforms  
4.2.32. Connects  
4.2.33. Constructs  
4.2.34. Contrast  
4.2.35. Control  
4.2.36. Coordinate  
4.2.37. Corrects  
4.2.38. Create  
4.2.39. Criticize  
4.2.40. Defend  
4.2.41. Define  
4.2.42. Demonstrate  
4.2.43. Describe  
4.2.44. Design  
4.2.45. Destroys  
4.2.46. Determine  
4.2.47. Develop  
4.2.48. Devise  
4.2.49. Diagrams  
4.2.50. Differentiate  
4.2.51. Directs  
4.2.52. Discover  
4.2.53. Discovers  
4.2.54. Discuss  
4.2.55. Dismantle  
4.2.56. Displays  
4.2.57. Distinguish  
4.2.58. Documents



4.2.59. Drills  
4.2.60. Enforce  
4.2.61. Estimate  
4.2.62. Evaluate  
4.2.63. Example  
4.2.64. Exemplify  
4.2.65. Explain  
4.2.66. Extends  
4.2.67. Follows  
4.2.68. Follows-Up  
4.2.69. Generalize  
4.2.70. Generates  
4.2.71. Give  
4.2.72. Helps  
4.2.73. Identify  
4.2.74. Illustrate  
4.2.75. Implement  
4.2.76. Influence  
4.2.77. Initiate  
4.2.78. Integrate  
4.2.79. Interpret  
4.2.80. Inventories  
4.2.81. Invite  
4.2.82. Justify  
4.2.83. Labels  
4.2.84. Listens  
4.2.85. Lists  
4.2.86. Locate  
4.2.87. Maintain  
4.2.88. Modify  
4.2.89. Monitor  
4.2.90. Name

4.2.91. Operate  
4.2.92. Orders  
4.2.93. Organise  
4.2.94. Outline  
4.2.95. Paraphrase  
4.2.96. Perform  
4.2.97. Plan  
4.2.98. Points Out  
4.2.99. Points To  
4.2.100. Practice  
4.2.101. Predicts  
4.2.102. Prepare  
4.2.103. Prescribes  
4.2.104. Present  
4.2.105. Prevent  
4.2.106. Prioritize  
4.2.107. Produce  
4.2.108. Promote  
4.2.109. Propose  
4.2.110. Questions  
4.2.111. Read  
4.2.112. Reads  
4.2.113. Recommend  
4.2.114. Relate  
4.2.115. Reorganise  
4.2.116. Reply  
4.2.117. Report  
4.2.118. Reproduce  
4.2.119. Request  
4.2.120. Responds  
4.2.121. Review  
4.2.122. Revise

- 4.2.123. Rewrite
- 4.2.124. Select
- 4.2.125. Shows
- 4.2.126. Solve
- 4.2.127. Specify
- 4.2.128. State
- 4.2.129. Store
- 4.2.130. Study
- 4.2.131. Summarize
- 4.2.132. Support
- 4.2.133. Synthesizes
- 4.2.134. Test
- 4.2.135. Use
- 4.2.136. Verify
- 4.2.137. Weighs
- 4.2.138. Words
- 4.2.139. Write

### **Control Knowledge**

#### **A. common language**

Word List: Develop

#### **B. Knowledge of Mechanical Systems**

#### **C. System Integration**

Word List: Design

#### **D. fail safe mode**

Word List: Define, Review, Test, Verify

#### **E. common language defined**

Need to be able to have common terms and definitions for ICS, components, and security mechanisms unique to ICS

Word List: Addresses

#### **F. Availability**

The process needs to be up.

### **G. Ladder logic**

Word List: Develop

### **H. interconnections between systems**

common interfaces and communication media

Word List: Analyze

### **I. Building Administration**

Word List: Cognizant-Of

### **J. Understand the Physical Process**

Need to understand the physical properties of the process the ICS is measuring and controlling. How can you sense or measure the parameters that matter, and how you can control the physical variables

Word List: Cognizant-Of

### **K. ICS Systems are generally unique**

Seen one IT system seen them all -- ICS Cyber professionals likely need 'sector' specific knowledge and understanding

### **L. process control**

Word List: Analyze, Apply, Cognizant-Of, Demonstrate, Develop, Diagrams, Documents, Explain, Integrate

### **M. Safety Issues**

Word List: Analyze, Categorize, Cognizant-Of, Describe, Determine, Documents, Evaluate, Identify, Review, Verify

### **N. fairly static environments**

In general ICS environments are more static than IT

### **O. Basics of electrical substations (for the power ICS)**

Power transfer and storage

Word List: Describe

### **P. Process Hazards Assessment**

What physically could go wrong

Word List: Generates, Review, Write

**Q. patching**

Patching is not always viable

Word List: Support

**R. Maintenance**

cyber maintenance for ICS differs from IT traditional systems

Word List: Coordinate, Documents, Perform, Prescribes, Prioritize

**S. Process Specific Paradigm**

ICS is used to monitor and control many different types of processes in many Sectors. An ICS support person must understand the process to the level that it can or may be impacted by the work being performed.

**T. Real-time Requirements**

The process demands real-time information to function.

Word List: Develop, Documents

**U. live with vulnerabilities**

Sometimes we will choose to live with documented vulnerabilities and mitigate the issue.

**V. preventative maintenance****W. Historical examples of what did go wrong**

Some examples of past events which were either caused by cyber incidents or other errors, and how they could've been prevented

**X. resiliency/sustainability**

Word List: Design

**Y. Legacy hardware vs new hardware (firmware differences)****Z. Common failure types**

Welded contacts, loose wires

Word List: Analyze, Study, Test

**AA. Understanding of the operational context of the process**

Need to understand the operational context of the physical process that is being controlled. this can be functional - private industry vs government or physical - on land vs on a ship,

Word List: Cognizant-Of, Develop

**AB. Educational / training differences**

Most IT Cyber professionals have a strong computer science background - Operators / ICS Cyber expertise does not have a 'mapped' path to success - varies - mostly home grown within a business or industry

Word List: Identify

**AC. Common areas where ICS and IT overlap/mesh**

Word List: Address

**AD. configuration management**

Word List: Implement, Perform, Analyze, Develop

**AE. Motion control**

Word List: Cognizant-Of

**AF. Determinism****AG. Piping and instrumentation diagrams**

Word List: Create, Design, Develop, Documents, Maintain, Review

**AH. Engineering prints**

Word List: Design, Develop, Maintain, Produce

**AI. ohms law**

Word List: Use

**AJ. deadband****AK. Physics-based restrictions**

OT deals with the constraints of the real world. Just because you can tell a computer to do it, doesn't mean that the system can handle it.

Word List: Verify

**AL. oscillation**

of control loop toward set point

**AM. set point**

Word List: Monitor, Verify

**AN. ladder logic**

Word List: Analyzes, Design, Documents, Test, Verify, Write

**AO. function block**

programming language

Word List: Analyzes, Design

**AP. Existence of Legacy Systems**

Many entities utilize old and unsupported operating systems and controllers that are no longer supported by vendors.

Word List: Cognizant-Of, Comply-With, Verify

**AQ. Major ICS vendors**

Word List: Analyzes, Select, Study

**AR. 'Working' is King**

If a solution works, then there will be resistance to change it.

**AS. ICS failure modes**

Loss of supervisory control loss of local control stale data

Word List: Addresses, Analyzes, Design, Explain, Identify, Predicts, Test

**AT. Need to understand the risk profile of the ICS**

Need to understand the impact if the system fails or is misused. Describe the function it performs and the criticality of that function.

Word List: Analyzes, Determine, Identify

**Equipment**

**A. vfd**

Word List: Cognizant-Of, Control

**B. power systems**

Word List: Maintain, Study

**C. Long-life equipment**

Systems are designed to be in place for decades.

**D. Powered backup systems**

**E. Motor control centers**

Word List: Assemble, Control

**F. pumps**

Word List: Control

**G. Valves**

Word List: Control

**H. pneumatics**

Word List: Control

**I. hydraulics**

Word List: Control

**J. ups**

Word List: Control

**K. electric circuits**

Word List: Control

**L. transformers**

Word List: Control

**M. boilers**

Word List: Control

**N. generators**

Word List: Control

**Communications**

**A. serial protocols more common**

**B. Deterministic Data Communications**

Generally Process logic relies on data being sent and received on a fairly strict timing sequence or logic in order to allow the process control logic to function properly.

Word List: Analyze

**C. Specific communication protocols used in the ICS world**

modbus, BACnet, Profibus, CCN, Lonworks ect.

Word List: Analyze

**D. communication medium differences**

IT connectivity is different then OT connectivity mechanisms (protocols, cabling...)

Word List: Differentiate



## **E. Industrial Ethernet Protocols**

EtherNet/IP (CIP), Modbus, DNP3, ICCP, OPC, BACnet, Profinet

## **F. weak network stack**

No active scanning

## **G. Fieldbus protocols**

HART, Foundation Fieldbus

Word List: Analyze

## **H. ICS Protocols**

Different industries and applications tend to utilize different types of protocols specifically designed for ICS applications.

Word List: Implement

## **I. Propriety protocols/architectures**

Many of the systems do not use common/open protocols and/or architectures.

## **J. ICS Data Communications Mediums**

ICS systems utilize a wide diversity of communications systems which leverage different technologies internal and external to the entities they support. Includes fiber, copper, wireless, satellite, etc. All require different understanding of cybersecurity implementations.

## **Regulations**

### **A. Different regulatory frameworks**

Word List: Adhere

### **B. regulatory environment**

NERC CIP, CFATS, API

Word List: Adhere

## **Instrumentation & Control**

### **A. PLCs**

Word List: Integrate

### **B. instrumentation**

Word List: Cognizant-Of, Documents, Integrate

**C. plc**

**D. hmi**

Word List: Control, Integrate

**E. Controllers**

programmable controllers, remoter terminal units

**F. panel-mount HMI**

Word List: Integrate

**G. transmitter**

**H. SCADA/HMI**

Word List: Build, Cognizant-Of, Integrate

**I. relays**

**J. process control**

Word List: Cognizant-Of, Integrate

**K. vibration monitoring**

Word List: Cognizant-Of

**L. Control element**

**M. sensing methods**

thermocouples, flow meters

Word List: Cognizant-Of

## APPENDIX D PROTOCOL FOR FOCUS GROUP SESSIONS

The protocol used for the focus group included the following:

### **Introduction of researcher**

Thank you again for being here. I am Sean McBride, the Industrial Cybersecurity Program Coordinator at Idaho State University. As explained in our previous email, I am engaged in a project to develop an industrial cybersecurity workforce development model. INL Cybercore management suggested you as especially qualified to provide input about the tasks that an industrial cybersecurity INSERT ARCHETYPE performs. I worked at the Idaho National Laboratory from 2006 to 2008 when I helped build out the DHS ICS Situational Awareness Effort that evolved into the ICS-CERT. I left the INL with a colleague to start Critical Intelligence, the first cyber threat intelligence firm to focus exclusively on industrial control systems and critical infrastructure. That business was acquired by iSIGHT Partners, which was in turn acquired by FireEye. I ended up at FireEye's Director of Industrial Control Systems Security, responsible for setting strategy across intelligence, product, and professional services. I left FireEye to take advantage of what I considered a great opportunity to build an educational program at ISU that could not exist anywhere else in the world. Simultaneously, I am a PhD student at La Trobe University where my research deals with how to effectively train and educate industrial cybersecurity professionals. As INL is deeply interested in this work, since 2017, I have been an INL joint appointee – meaning ISU is my home organisation, but INL pays about half of my salary.

### **Introduction of collaboratorcollaborators**

I know a little about your background, based on my discussion with INL cybersecurity leadership, but will you tell me why you think they selected you?

### **Review of the purpose of the effort**

Thank you. I am so pleased you agreed to be here. As the email I sent you explained, our purpose today is to create a list of the tasks that an INSERT ARCHETYPE ROLE performs. We don't expect this list to be perfect, but we do expect it will give us a great place to start. Follow-on work will be necessary to validate and refine the results. I will take notes as we go, and ask additional clarifying questions. When we are done, we will review the list together. Once I have fully processed the list, I will send it back to you for your review and any additional input you wish to provide. I anticipate that this session should take between two and three hours as we have scheduled.

## **Review of the results of the nominal group technique**

In order to understand this effort you need to know what work we have already done. In February 2019, I met with a group of 14 INL industrial cybersecurity subject matter experts. The group came up with a list of five “archetype roles” – which you can consider as general job titles. The researcher recognises that actual job titles and responsibilities will vary by organisation, but the roles allow us to make some general assumptions about the different types of things that industrial cybersecurity professionals do.

## **Allow the collaborator to ask any questions they may have**

Does that make sense? Do you have any questions for me before we get started?

## **Collaborative discussion of the question**

Great. Let’s get started with the core question: What tasks does this archetype role perform?

Follow on questions are to be asked as the situation evolves, using a prompt similar to: That’s great. Very insightful. I think I heard you say that “123”; am I capturing that correctly? Participant 2 – is that accurate from your point of view? What else would you add?

Goal is to characterise the essence of the tasks in a way that satisfies the expert.

## **Note taking**

The researcher took notes in real-time on a monitor visible to the collaborators.

## **Wrap up**

I can’t think of any additional questions to ask. Is there anything you think we’ve missed?

Do you feel that the core task categories we’ve identified capture the tasks one would expect an INSERT ARCHTYPE ROLE performs?

Thank you again for your fantastic input. Once I process these notes into a more consumable format, I will send them to you for your review and additional input.

## APPENDIX E ESET 181 IT-OT FUNDAMENTALS – ABBREVIATED SYLLABUS

### *Course Description*

Hands-on survey of engineering technologies -- including sensors, networks, and computers -- used to drive the modern industrial economy, including the Internet, the electric grid, and potato processing facilities. Provides frameworks and vocabulary for analyzing the effects of these technologies on individuals, businesses, and nations.

### *Course Objectives*

Upon successful completion of this course, students will be able to:

- Describe operational technologies such as SCADA, HMI, PLC engineering laptop, and common ICS network communication protocols
- Describe common roles and responsibilities that deal with IT and OT within industrial environments
- Explain common information technologies used in OT, including: computer hardware, operating systems, programming, applications, networks, databases, and virtualization
- Build and interact with an elementary SCADA system
- Identify common cybersecurity concerns within industrial environments

### *Required Materials*

<b>Computer/Laptop</b>	<b>Electronic components for Raspberry Pi</b>
<ul style="list-style-type: none"><li>• Web browser</li></ul>	<ul style="list-style-type: none"><li>• Plenty of male to female jumpers</li></ul>
<ul style="list-style-type: none"><li>• University network account</li></ul>	<ul style="list-style-type: none"><li>• One set of coloured LEDs (RBG)</li></ul>
	<ul style="list-style-type: none"><li>• Adafruit DHT 11 sensor</li></ul>
<b>Raspberry Pi</b>	
<ul style="list-style-type: none"><li>• Model 4</li></ul>	
<ul style="list-style-type: none"><li>• Mini HDMI to HDMI adapter</li></ul>	
<ul style="list-style-type: none"><li>• 32 GB MicroSD card with NOOBS</li></ul>	

### *Weekly Schedule*

<b>Topic 1: Introduction to IT-OT Fundamentals</b>	<b>Topic 6: Supervisory Control</b>
Identify Computer Components	Turn On/Off LED using Node-RED
Rack a Server	Display Temperature trend using Node-RED
Create Process Flow Block Diagram	

Design SCADA Interface	<b>Topic 7: Intro to Networking</b>
	Explore Network Settings on Rpi
<b>Topic 2: Raspberry Pi Computing Platform</b>	Network Pi's Together
Explore BIOS/UEFI	Assign static IP address to your RPi
Make Bootable USB	
Register RPi on ISU DeviceNet Folder	<b>Topic 8: Industrial networking</b>
Navigate Command Line	Draw a network diagram
Update and upgrade Linux	Configure Cisco switch in packet tracer
Explore password files	Describe industrial switch
Add user and manage permissions	
	<b>Topic 9: IT-OT Gap</b>
<b>Topic 3: Coding</b>	Create skit demonstrating IT-OT gap
Use Turtle Python library to make a shape	
Use Turtle to make a spiral of spirals	<b>Topic 10: Network Monitoring</b>
Use Turtle to make an interactive spiral shape	Use Nmap to scan a network
Review and modify pre-written code	Install and use TCPDUMP
	IoT fingerprinting
<b>Topic 4: Cyber-Physical Systems</b>	Explore ICS network monitoring solutions
Connect LED	
Connect Temperature Sensor	<b>Topic 11: Security</b>
Create six light traffic control system	Create asset inventory
Investigate leading ICS vendors	Review and improve network architecture
	Add security to Node-RED on RPi
<b>Topic 5: Web Technologies</b>	Configure Firewall in Packet Tracer
HTML source within your Browser	Test Firewall in Packet Tracer
Create a Web Page Folder	
Explore Web Hosting Options Folder	<b>Topic 12: Future of OT</b>
Explore DNS Data Folder	Create VM in AWS cloud
Control LED from Web page	Control RPi LED from your phone
	Current events briefing

## APPENDIX F BUILDING AN INDUSTRIAL CYBERSECURITY WORKFORCE: A MANAGERS GUIDE



# BUILDING AN **INDUSTRIAL** **CYBERSECURITY** WORKFORCE

---

**A Manager's Guide**



# INDUSTRIAL CYBERSECURITY AWAKENING

As smart devices and networks push deeper into power grids, oil refineries, and water treatment plants, we must consciously prepare professionals to securely design, build, operate and maintain such infrastructures so that they are prepared to protect and defend them.

This document, “A Manager’s Guide” is the first in a series of guidebooks dedicated to the important topic of developing an industrial cybersecurity workforce. Other publications will include “A Human Resources Guide” for Human Resource (HR) personnel seeking to ensure the effectiveness of industrial cybersecurity personnel, and “A Career Development Guide” for individuals seeking to develop industrial cybersecurity competencies.

**This guide will aid managers in answering four pivotal questions:**

- 1. Are you ready to build an industrial cybersecurity team?**
- 2. How do you structure your industrial cybersecurity team?**
- 3. What does your industrial cybersecurity team need to know?**
- 4. What does your industrial cybersecurity team need to do?**



# ARE YOU READY TO BUILD AN INDUSTRIAL CYBERSECURITY TEAM?

Many managers fail to fully appreciate the intense cultural, managerial, and educational differences between information technology (IT) systems and operational technology (OT) systems, which we call the IT-OT gap.



IT systems consist of desktops, laptops, web servers, communications networks, email, storage and backup systems used to help humans make better decisions.

OT systems consist of programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), control logic, sensors and actuators that provide reliable electricity, consistent transportation, and safe drinking water. Operational technology systems are the collection of technologies used to control and monitor industrial operations used in electric power, oil & natural gas, water & wastewater, and manufacturing sectors. These systems include:

- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)
- Programmable logic controllers (PLCs)
- Industrial control communications protocols, control logic, sensors and actuators.

**Figure: Information Technology (IT) Versus Operation Technology (OT)**

The table below shows some of the differing characteristics between information technology and operational technology.

	 <b>Information Technology</b>	 <b>Operational Technology</b>
<b>Being controlled</b>	Data	Physics
<b>Measurement</b>	Bits and bytes	Temperature, pressure, flow
<b>Lifecycle</b>	System lifecycle	Facility lifecycle
<b>Consequences</b>	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
<b>Desired system characteristics</b>	Confidentiality Integrity Availability	Safety Reliability Functionality
<b>Educational background</b>	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
<b>Reporting chain</b>	ISO CISO CIO	Shift Supervisor Plant Manager COO
<b>Managerial accounting</b>	Cost center	Profit center



Corporate boards, executives and officers are awakening to the challenges securing the operational technology (OT) systems that run their factories, support local economies, and undergird modern societies.

Failure to appreciate the IT-OT gap can hamper effective and sustainable approaches to industrial cybersecurity. The Industrial Cybersecurity Awakening Model describes the stages many organizations pass through as their OT security efforts mature. The materials in this guide help shift management mentality towards Stage 5.

### Industrial Cybersecurity Awakening Model

	STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
<b>Management mentality</b> 	<b>External consultants</b> "Get someone in here before that happens again."	<b>Allocated budget</b> "Here's some money to go make us secure."	<b>Appropriate technology</b> "Technology will help IT security staff cover OT too."	<b>Industrial cybersecurity program</b> "Let's do this right by following the guidance."	<b>Industrial cybersecurity team</b> "Let's build a team to make this sustainable."
	6 months	1 year	2 years	3 years	4 years

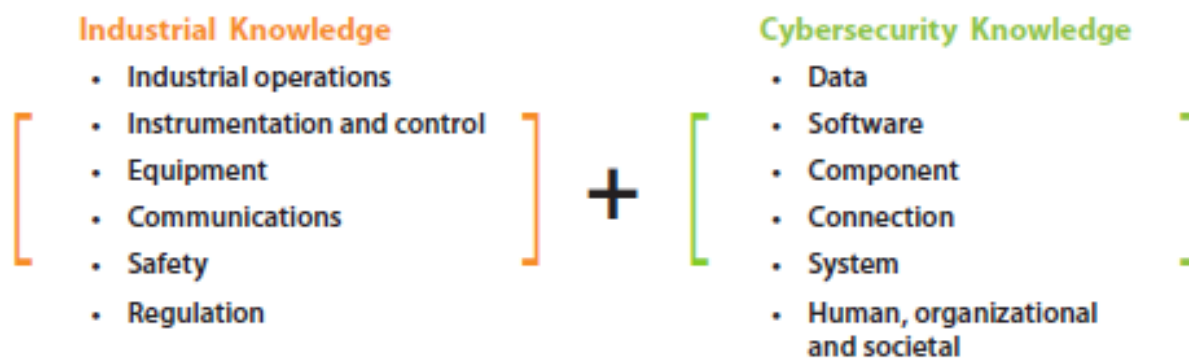


# WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM NEED TO KNOW?

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

---

## Industrial and Cybersecurity Knowledge Domains



### Industrial knowledge domain content:

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

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

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

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

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

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

**Common weaknesses:** indefensible architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, third-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.



# HOW DO YOU STRUCTURE AN INDUSTRIAL CYBERSECURITY TEAM?

Managers seeking to build an industrial cybersecurity team may rely on human resource development models (as exemplified below) to plan to meet organizational needs. This guide was developed to adhere to the following role-based workforce development structure. It presents the key role, position description, and tasks.



## KEY ROLES OF THE TEAM



# WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM NEED TO DO?

## MANAGER

An 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.

### MANAGER PRIMARY TASKS

- Prioritize efforts
- Understand requirements per effort
- Obtain and manage budget
- Build the team
- Run and improve the program.

### Qualifications and Certifications

- Master of Business Administration
- Project Management
- Information systems security
- Licensed Professional Engineer
- Industrial cybersecurity.

### HIRING GUIDANCE

- ☐ Ideal candidate has project management experience in cybersecurity AND engineering.
- ☐ One senior manager per strategic business unit.
- ☐ Intimately familiar with industrial cybersecurity good practice guidance.
- ☐ Comfortable in both corporate offices and industrial environments.
- ☐ Compliance and audit experience desired.
- ☐ Capable of keeping the big picture in mind while not afraid of technical details.



## ENGINEER

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.

### ENGINEER PRIMARY TASKS

- Direct creation of industrial systems inventory and model for cybersecurity purposes
- Design physical failsafes to counteract potential cybersabotage
- Advise development and operation of security operations center relative to the industrial environment
- Recommend security techniques, technologies, and approaches for adoption in industrial environment
- Create cybersecurity inspection and test procedures for industrial systems
- Review industrial system engineering plans and documentation for cybersecurity concerns
- Review proposed cybersecurity policies and procedures related to industrial environments; and equipment and software based on cybersecurity criteria
- Optimize industrial system designs for security effectiveness and efficiency.

### Qualifications and Certifications

- Master of Science in Electrical, Mechanical, or Computer Engineering
- Licensed Professional Engineer
- Industrial automation
- Information systems security.

### HIRING GUIDANCE

- ☐ **Most important role on the industrial cybersecurity team and may require skilled recruitment.**
- ☐ Requires 5 or more years of engineering experience in each of industrial automation, information technology, and cybersecurity.
- ☐ Demonstrates expert level familiarity with industrial safety and cybersecurity events including detailed root-cause analysis.
- ☐ Deep engineering experience and expertise and is capable of considering the mindset of a well-resourced adversary.
- ☐ Demonstrates proficiency in systems thinking and systems design, including production of policies, diagrams, drawings, and specifications.
- ☐ *For Team: One or two per facility or per type of facility.*





## TECHNICIAN

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

### TECHNICIAN PRIMARY TASKS

- Maintains ICS device asset inventory for security purposes
- Reviews architecture of ICS networks
- Updates ICS software and firmware during stoppages
- Maintains backups of control software
- Maintains awareness of evolving threat environment
- Securely implements process control equipment.



### HIRING GUIDANCE

- ☐ Demonstrates fascination and enthusiasm for knowing how things work.
- ☐ Demonstrates hands-on experience with industrial automation equipment.
- ☐ Demonstrates proficiency in safe work procedures.
- ☐ Provides technical experience and builds relationships that provide a fantastic foundation for all the other cybersecurity roles.
- ☐ Possess proficient IT and OT terminology and cultures to enable communications across the IT-OT gap.
- ☐ Understands common security weaknesses in OT environments.
- ☐ *For Team: At least one per facility.*

### Qualifications and Certifications

- Associate or Bachelor of Applied Science in Engineering Technology
- Control Systems Technician
- Industrial cybersecurity
- Basic networking
- Basic security.



# ANALYST

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 works with industrial operations personnel to gain perspective and vet practicality of possible courses of action.

## ANALYST PRIMARY TASKS

- Stays abreast emerging developments relevant to industrial cybersecurity
- Dissects analytical requests
- Collects information
- Synthesizes information
- Analyzes threats, vulnerabilities and consequences pertinent to industrial environments
- Produces analytical products
- Proposes new work.



## HIRING GUIDANCE

- ☐ Enjoys the professional writing process.
- ☐ Reads insatiably.
- ☐ Does not shy away from potentially controversial topics.
- ☐ Presents compelling arguments in written and verbal form.
- ☐ Has developed deep expertise in various subject areas.
- ☐ Works well with other analytical thinkers, and appreciates constructive critique.
- ☐ Never completely satisfied with work product.
- ☐ Quickly and accurately describes the threat environment pertinent to a given organization.

### Qualifications and Certifications

- Bachelor of Science or Arts in various fields
- Coursework in intelligence and analysis
- Cybersecurity certifications
- Military intelligence training
- Data visualization.

## RESEARCHER

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.

### RESEARCHER PRIMARY TASKS

- Describes and characterizes systems
- Designs and conducts tests
- Discovers vulnerabilities
- Develops adversarial perspective
- Recommends mitigations
- Documents and reports findings.

### HIRING GUIDANCE

- ☐ Thrives when working with technology.
- ☐ Must be capable of explaining and defending their findings.
- ☐ May enjoy technology interaction outside of work hours.
- ☐ Shares findings and techniques with other researchers.



### Qualifications and Certifications

- Bachelor or Master of Science in computer science
- Technical track presentations at security conferences
- Publicly referenced vulnerability disclosures
- Authored security-related tools.

## APPENDIX G MATERIALS FOR SURVEYS, INTERVIEWS, AND FIELD OBSERVATION

The research is being carried out in partial fulfilment of PhD under the supervision of Dr. Jill Slay. The following researchers will be conducting the study:		
Role	Name	Organisation
Supervisor	Dr. Jill Slay	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
Researcher	Sean McBride	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
<b>Research funder</b>	This research is supported by in kind support by La Trobe University.	

## 1. What is the study about?

This study aims to identify and describe the knowledge and skills required by industrial cybersecurity professionals.

## 2. Do I have to participate?

Being part of this study is voluntary. If you want to be part of the study we ask that you read the information below carefully and ask us any questions. You can read the information below and decide at the end if you do not want to participate. If you decide not to participate this won't affect your relationship with La Trobe University or any other listed organisation.

## 3. Who is being asked to participate?

We are seeking the participation of individuals with professional experience securing industrial control environments – the computerized systems controlling processes such as electricity generation, natural gas transmission, automotive manufacturing, and food production.

## 4. What will I be asked to do?

This is a three phase study. Phase I involves an online review of knowledge and tasks performed by industrial cybersecurity professionals. We estimate this review will take half-an-hour to an hour to complete. You may participate in phase I without participating in Phase II or Phase III. This consent form pertains only to Phase I.

Phase II involves telephone interviews delving more deeply into the results of phase I. We estimate this interview will take up to an hour. You may participate in Phase 2 without Participating in Phase III. A separate consent form is used for Phase II.

Phase III involves being observed at work performing key tasks at which you are an expert. The length of this observation will depend entirely on the task being observed. A separate consent form is used for Phase III.

## 5. What are the benefits?

By participating in this study, you can help inform the creation of an education and training standard to develop a capable industrial cybersecurity workforce. Education and training programs may then use this standard to ensure their efforts align with validated needs.

## 6. What are the risks?

With any study there are (1) risks we know about, (2) risks we don't know about, and (3) risks we don't expect. If you experience something that you aren't sure about, please contact us immediately so we can discuss the best way to manage your concerns.

Name/Organisation	Position	Telephone	Email
La Trobe University	PhD Researcher	1.208.339.6707	S.McBride@latrobe.edu.au

We do not foresee any risks associated with this study. We note, however, that if you choose to disclose your participation in this study, you and the organization for which you work may become a more likely target for cyber-attacks.

## 7. What will happen to information about me?

By clicking on the 'I agree, start questionnaire' button, this tells us you want to take part in the study.

We will **collect** information about you in ways that will reveal to the researcher who you are.

We will **store** information about you in ways that will not reveal who you are.

We will **publish** information about you in ways that will not be identified in any type of publication from this study, unless you opt-in to disclosure.

We will **keep** your information for 5 years after the project is completed. After this time we will destroy all of your data.

The storage, transfer and destruction of your data will be undertaken in accordance with the [Research Data Management Policy](https://policies.latrobe.edu.au/document/view.php?id=106/) <https://policies.latrobe.edu.au/document/view.php?id=106/>.

The personal information you provide will be handled in accordance with applicable privacy laws, any health information collected will be handled in accordance with the Health Records Act 2001 (Vic). Subject to any exceptions in relevant laws, you have the right to access and correct your personal information by contacting the research team. You may withdraw up to four weeks post participation.

## 8. Will I hear about the results of the study?

We will let you know about the results of the study via email if you indicate your permission below.

## 9. What if I change my mind?

If you no longer want to complete the questionnaire, simply close the web browser. If you change your mind after clicking on the 'Submit' button, we can withdraw your responses because we can link who you are with your questionnaire responses. You can withdraw up to four weeks post participation.

To withdraw from this study at any time, simply email the Withdrawal of Consent form below to [S.McBride@latrobe.edu.au](mailto:S.McBride@latrobe.edu.au)

.

Your decision to withdraw at any point will **not** affect your relationship with the researcher or La Trobe University.

## 10. Who can I contact for questions or want more information?

If you would like to speak to us, please use the contact details below:

Name/Organisation	Position	Telephone	Email
La Trobe University	PhD Researcher	1.208.339.6707	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>

## 11. What if I have a complaint?

If you have a complaint about any part of this study, please contact:

Ethics Reference Number	Position	Telephone	Email
HEC20042	Senior Research Ethics Officer	+61 3 9479 1443	<a href="mailto:humanethics@latrobe.edu.au">humanethics@latrobe.edu.au</a>

## Withdrawal of Consent

I wish to withdraw my consent to participate in this study. I understand withdrawal will not affect my relationship with La Trobe University of any other organisation or professionals listed in the Participant Information Statement. I understand the researchers cannot withdraw my information once it has been analysed, and/or all identifiers have been removed and results have been aggregated.

I understand my information will be withdrawn as outlined below:

- ✓ Any identifiable information about me will be withdrawn from the study
- ✓ The researchers will withdraw my contact details (if you have provided them) from the databank so I cannot be contacted by them or any other research group in the future.

## Participant Signature

Participant's printed name	
Participant's signature	
Date	

## Please forward this form to:

CI Name	Sean McBride
Email	S.McBride@latrobe.edu.au
Phone	1 208 339 6707
Postal Address	ESTEC Box 8380 Idaho State University, Pocatello, ID 83209

**Consent Form – Declaration by Participant**

I (the participant) have read understood the Participant Information Statement, and any questions have been answered to my satisfaction. I know I can withdraw at any time until my data have been analysed. Information I provide may be used only for this specific study. Information I provide can be included in a thesis, presented publicly, and published in journals. My identity will not be disclosed unless I opt-in to that disclosure.

**I agree, start questionnaire**

## Survey questions

### Section 1 – Professional Experience Related to the Field

**1.1 I have NN years specific professional experience in industrial control systems (NOT cybersecurity)**

- 0
- 1-5
- 6-10
- 10-15
- 16-25
- 25+

Enter job titles you have had for this experience <enter into text box>

**1.2 I have NN years specific professional experience in cybersecurity (NOT industrial control systems)**

- 0
- 1-5
- 6-10
- 10-15
- 16-25
- 25+

Enter job titles you have had for this experience <enter into text box>

**1.3 I have NN years specific professional experience in ICS cybersecurity (not reflected in previous answers)**

- 0
- 1-5
- 6-10
- 10-15
- 16-25
- 25+

Enter job titles you have had for this experience <enter into text box>

### Section 2 - Choose archetype role to review

Industrial Cybersecurity Technician – Read description – select

Industrial Cybersecurity Engineer – Read description – select

**Section 3 - Type in all knowledge (nouns) needed to perform this specific role THAT MAKE IT DIFFERENT from normal (non-ICS) cybersecurity. These are terms you would not expect to see in a standard cybersecurity education or training program.**

Separate nouns with a comma



## **Section 4 – Review tasks (Entire task list shown on one page)**

### **4.1 Are additional tasks warranted?**

- Choose Yes, No, I Don't Know
- If Y -- Describe the task.
- If Y – Select responsibility: Primary, supporting, shared

### **4.2 Should tasks be removed?**

Select task to be removed.

Provide reasoning (in text).

## **Section 5 Review of specific tasks**

### **For each task:**

- “I consider myself a <Master> <Journeyman> <Apprentice> <Informed Observer> <Unqualified Performer> of this task.”
- Select responsibility that you believe this role [Technician] [Engineer] has for this task: <Primary><Shared> <Supporting>
- If Shared, describe with what other role(s) it is shared with. Text box
- What alteration do you suggest to this task? <enter text into box>, <none>
- Briefly explain each suggested alteration <enter into text box>

### **5.1.1 - Per Task: Add clarifying skills**

A skill is a VERB STATEMENT that supports the task. It must begin with a verb, but may include nouns. It may be helpful to consider this a subtask. It may also be helpful to consider this a training experience the individual needs in order to perform the entire task.

Enter skills related to this task <enter into text box>

### **5.1.2 – Per task: Add clarifying attitudes**

An attitude is an EMOTION STATEMENT that supports the task. This describes emotions the [Technician] [ENGINEER] feels or exhibits while performing the task. These are often adverbs. Examples may include “safely”, “carefully” or “painstakingly”. They may be combined with a skill.

Enter attitudes related to this task <enter into text box>

### **5.1.3 – Per task: Add clarifying behaviors**

A behavior is a strategy that describes how a task is performed by someone who has mastered it. These are often expressed as prepositions or conjunctions, such as “before”, “after”, or “by”. They may be combined with a skill and combined with an attitude.

Enter behaviors related to this task <enter into text box>

## **Section 6 – Consents**

### **6.1 Are you willing to be interviewed regarding your responses?**

If Y

First name

Last name

Email address

**6.2 Are you willing to be observed performing one or more of these tasks?**

If Y

First name

Last name

Email address

**6.3 Would you like to be publicly identified as a participant of this work?**

If Y

First name

Last name

**6.4 Would you like to receive notice of publications resulting from this work?**

If Y

Email address (used only to notify of publications resulting from this work)

**7. Affirmation**

I affirm that my statements are true and accurate

Y/N

Submit button

The research is being carried out in partial fulfilment of PhD under the supervision of Dr. Jill Slay. The following researchers will be conducting the study:		
Role	Name	Organisation
Supervisor	Dr. Jill Slay	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
Researcher	Sean McBride	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
Research funder	This research is supported by in kind support by La Trobe University.	

**1. What is the study about?**

This study aims to identify and describe the knowledge and skills required by industrial cybersecurity professionals.

**2. Do I have to participate?**

Being part of this study is voluntary. If you want to be part of the study we ask that you read the information below carefully.

You can read the information below and decide at the end if you do not want to participate. If you decide not to participate this won't affect your relationship with La Trobe University or any other listed organisation.

**3. Who is being asked to participate?**

We are seeking the participation of individuals with professional experience securing industrial control environments – the computerized systems controlling processes such as electricity generation, natural gas transmission, automotive manufacturing, and food production.

**4. What will I be asked to do?**

This is phase II of a three phase study. It involves a telephone interview to discuss key participant responses to online surveys conducted in Phase I. We estimate this interview will take up to an hour. You may participate in Phase II without Participating in Phase III.

Phase III involves being observed at work performing key tasks at which you are an expert. We estimate this observation will depend entirely on the task being observed.

**5. What are the benefits?**

By participating in this study, you can help inform the creation of an education and training standard to develop a capable industrial cybersecurity workforce. Education and training programs may then use this standard to ensure their efforts align with validated needs.

**6. What are the risks?**

With any study there are (1) risks we know about, (2) risks we don't know about, and (3) risks we don't expect. If you experience something that you aren't sure about, please contact us immediately so we can discuss the best way to manage your concerns.

Name/Organisation	Position	Telephone	Email
La Trobe University	PhD Researcher	208.339.6707	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>

We do not foresee any risks associated with this study. We note, however, that if you choose to disclose your participation in this study, you and the organization for which you work may become a more likely target for cyber-attacks.

## 7. What will happen to information about me?

By clicking on the 'I agree, start questionnaire' button, this tells us you want to take part in the study.

We will **collect** information about you in ways that will reveal to the researcher who you are.

We will **store** information about you in ways that will not reveal who you are.

We will **publish** information about you in ways that will not be identified in any type of publication from this study, unless you opt-in to disclosure.

We will **keep** your information for 5 years after the project is completed. After this time we will destroy all of your data.

The storage, transfer and destruction of your data will be undertaken in accordance with the [Research Data Management Policy](https://policies.latrobe.edu.au/document/view.php?id=106/) <https://policies.latrobe.edu.au/document/view.php?id=106/>.

The personal information you provide will be handled in accordance with applicable privacy laws, any health information collected will be handled in accordance with the Health Records Act 2001 (Vic). Subject to any exceptions in relevant laws, you have the right to access and correct your personal information by contacting the research team.

## 8. Will I hear about the results of the study?

We will let you know about the results of the study via email if you indicate your permission below.

## 9. What if I change my mind?

You may withdraw from this study at any time before data analysis is complete. To do so, please email the Withdrawal of Consent form below to [S.McBride@latrobe.edu.au](mailto:S.McBride@latrobe.edu.au).

Your decision to withdraw at any point will **not** affect your relationship with the researcher or La Trobe University.

## 10. Who can I contact for questions or want more information?

If you would like to speak to us, please use the contact details below:

Name/Organisation	Position	Telephone	Email
La Trobe University	Researcher	1.208.339.6707	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>

## 11. What if I have a complaint?

If you have a complaint about any part of this study, please contact:

Ethics Reference Number	Position	Telephone	Email
HEC20042	Senior Research Ethics Officer	+61 3 9479 1443	<a href="mailto:humanethics@latrobe.edu.au">humanethics@latrobe.edu.au</a>

**Consent Form – Declaration by Participant**

I (the participant) have read understood the Participant Information Statement, and any questions have been answered to my satisfaction. I know I can withdraw at any time until after my data have been analysed. Information I provide may be used only for this specific study. Information I provide may be included in a thesis, presented publicly, and published in journals. My identity will not be disclosed as a participant contributor unless I opt-in to that disclosure by selecting the box below. If I opt into disclosure as a participant contributor, information I provide will not be publicly associated with my name.

<b>Name</b>	
<b>Date</b>	
<b>Signature</b>	

**Opt-in to disclosure as a participant contributor**

☐ Please list my name as a participant contributor to this study.

<b>Name</b>	<b>Email (optional)</b>

**Opt-in to receive results**

☐ Please send me a copy of the results via email.

<b>Name</b>	<b>Email (optional)</b>

## Withdrawal of Consent

I wish to withdraw my consent to participate in this study. I understand withdrawal will not affect my relationship with La Trobe University or any other organisation or professionals listed in the Participant Information Statement. I understand the researchers cannot withdraw my information once it has been analysed, and/or all identifiers have been removed and results have been aggregated.

I understand my information will be withdrawn as outlined below:

- ✓ Any identifiable information about me will be withdrawn from the study
- ✓ The researchers will withdraw my contact details (if you have provided them) from the databank so I cannot be contacted by them or any other research group in the future.

## Participant Signature

Participant's printed name	
Participant's signature	
Date	

## Please forward this form to:

CI Name	Sean McBride
Email	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>
Phone	1 208 339 6707
Postal Address	ESTEC Box 8380 Idaho State University, Pocatello, ID 83209

## Interview schedule

### I. Opening

- A. (Establish Rapport). Hello \_\_\_\_\_. I am Sean McBride, the primary researcher behind the Industrial Cybersecurity Education and Training Standards research effort. I greatly appreciate your agreeing to be interviewed.
- B. (Purpose) As industrial cybersecurity grows as a career field, we want to help provide a solid foundation. This phase of our research involves refining the prototype standards via interviews, which are more profound than the written survey you took.
- C. (Timeframe). I anticipate our discussion will take about an hour. Is now still a good time?
- D. (Participant Information and Consent). Thank you for reviewing and signing the information and consent form.

As indicated in the form, I would like to record this interview. Can you verbally verify that I have your consent to record this interview?

[START RECORDING].

Now that I've started recording, I'll ask the same question again: do have your permission to record this interview? Thank you.

I want to make sure you have a firm grasp of our research: What do you understand is the purpose of this research?

Why do you wish to participate?

Thank you.

While providing complete answers that display your expertise will be most useful for the purposes of the research, you are in no way obligated to answer my questions and may simply indicate you do not wish to answer.

Also, you are free to withdraw from the study until the final results have been compiled – which I estimate will be within the next 30 days. Simply email me at the same email address through which we have already corresponded requesting to be withdrawn. I will delete all data you have provided me, and send you a note confirming the same.

- E. (Questions). Do you have any questions for me about this research?
- F. (Transition). Fantastic. Let's get started.

## **II. Body – For those who responded to the survey**

- A. (Set background) In the written survey, you indicated that you have X years of specific professional experience in industrial cybersecurity. Can you tell me about your personal journey into the field of industrial cybersecurity?

### **SELECT AS REQUIRED**

- B. For proposed task <insert task> you responded that you consider yourself an <insert expertise level> at task <Insert task>. Can you explain why you characterize yourself in this way?
- C. For proposed task <insert task and description> you suggested altering the task to say <insert recommendation>. Please explain why.
  - a. [Elective follow-on: What do you mean by <insert phrase>?]
- D. For proposed task <insert task and description> you suggested adding the skill <insert skill>. Please explain why.
  - a. [Elective follow-on: What do you mean by <insert phrase>?]
- E. For proposed task <insert task and description> you suggested adding the attitude <insert attitude>. Please explain why.
  - a. [Elective follow-on: What do you mean by <insert phrase>?]
- F. For proposed task <insert task and description> you suggested adding the behavior <insert behavior>. Please explain why.
  - a. [Elective follow-on: What do you mean by <insert phrase>?]
- G. For proposed task <insert task> you suggested eliminating the task. Please explain why.
  - a. [Elective follow-on: What do you mean by <insert phrase>?]
- H. You suggested adding <insert task>, and explained <insert explanation>. Please clarify what you meant by <insert quotation>.



## II. Body – For those who did not respond to the survey

- A. (Set background) How many years of specific professional experience in industrial cybersecurity do you have? Will you please tell me about your personal journey into the field of industrial cybersecurity?

### SELECT AS REQUIRED

- B. For proposed task <insert task> do you consider yourself an <master> <journeyman><novice><informed observer> <unqualified performer>. Will you please explain why you characterize yourself in this way?
- C. For proposed task <insert task and description> you it was suggested the task be altered to say <insert recommendation>. Can you explain why this might be a reasonable change?
- a. [Elective follow-on: What do you mean by <insert phrase>?]
- D. For proposed task <insert task and description> it was suggested to add the skill <insert skill>. Please explain why this might be a reasonable change.
- a. [Elective follow-on: What do you mean by <insert phrase>?]
- E. For proposed task <insert task and description> it was suggested the attitude <insert attitude> be added. Please explain why this might be a reasonable addition.
- a. [Elective follow-on: What do you mean by <insert phrase>?]
- F. For proposed task <insert task and description> it was suggested the behavior <insert behavior> be added. Please explain why this might be a reasonable addition.
- a. [Elective follow-on: What do you mean by <insert phrase>?]
- G. It was suggested the task <insert task> be eliminated. Please explain why this might be necessary.
- a. [Elective follow-on: What do you mean by <insert phrase>?]
- H. It was suggested <insert task> be added. Please clarify why this might be a necessary.
- a. [Elective follow-on: What do you mean by <insert phrase>?]

### III. Closing

- A. (Summarize) You have provided some valuable and useful insight.
- B. (Maintain rapport) I sincerely thank you again for your time and attention.
- C. (Action I will take) I think I have all the information I need. I will transcribe and code your responses for analysis. This information may be used to improve the prototype standards.
- D. (Confirm consent of public identification) I note that you previously indicated that you <did or did not> want to be publicly identified as a contributor. Do you wish to maintain that response?
- E. (Confirm consent of publication notification) I note that you previously indicated that you <did or did not> want to receive notification of publications resulting from this research. Do you wish to maintain that response?
- F. (Goodbye). Thank you again. Good day!

The research is being carried out in partial fulfilment of PhD under the supervision of Dr. Jill Slay. The following researchers will be conducting the study:		
Role	Name	Organisation
Supervisor	Dr. Jill Slay	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
Researcher	Sean McBride	Science, Health, and Engineering/Engineering and Mathematical Science/ Computer Science and Information Technology
Research funder	This research is supported by in kind support by La Trobe University.	

## 12. What is the study about?

This study aims to identify and describe the knowledge and skills required by industrial cybersecurity professionals.

## 13. Do I have to participate?

Being part of this study is voluntary. If you want to be part of the study we ask that you read the information below carefully and ask us any questions.

You can read the information below and decide at the end if you do not want to participate. If you decide not to participate this won't affect your relationship with La Trobe University or any other listed organisation.

## 14. Who is being asked to participate?

We are seeking the participation of individuals with professional experience securing industrial control environments – the computerized systems controlling processes such as electricity generation, natural gas transmission, automotive manufacturing, and food production.

## 15. What will I be asked to do?

This is phase 3 of a three phase study. It involves being observed performing the following cybersecurity tasks as identified in previous phases of this study:

<INSERT KEY TASK(S)>

We estimate this observation will take <INSERT TIME>.

During the observation the researcher will take notes about your actions, take video recording of your actions, and record your answers to clarifying questions about your actions.

## 16. What are the benefits?

By participating in this study, you can help inform the creation of an education and training standard to develop a capable industrial cybersecurity workforce. Education and training programs may then use this standard to ensure their efforts align with validated needs.

## 17. What are the risks?

With any study there are (1) risks we know about, (2) risks we don't know about, and (3) risks we don't expect. If you experience something that you aren't sure about, please contact us immediately so we can discuss the best way to manage your concerns.

Name/Organisation	Position	Telephone	Email
La Trobe University	Researcher	208.339.6707	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>

We do not foresee any risks associated with this study. We note, however, that if you choose to disclose your participation in this study, you and the organization for which you work may become a more likely target for cyber-attacks.

## 18. What will happen to information about me?

Signing and returning this form tells us you want to take part in the study.

We will **collect** information about you in ways that will reveal to the researcher who you are.

We will **store** information about you in ways that will not reveal who you are.

We will **publish** information about you in ways that will not be identified in any type of publication from this study, unless you opt-in to disclosure.

Audio and video recordings will not be published or otherwise made available for use outside of this project.

We will **keep** your information for 5 years after the project is completed. After this time we will destroy all of your data.

The storage, transfer and destruction of your data will be undertaken in accordance with the [Research Data Management Policy](https://policies.latrobe.edu.au/document/view.php?id=106/) <https://policies.latrobe.edu.au/document/view.php?id=106/>.

The personal information you provide will be handled in accordance with applicable privacy laws, any health information collected will be handled in accordance with the Health Records Act 2001 (Vic). Subject to any exceptions in relevant laws, you have the right to access and correct your personal information by contacting the research team.

## 19. Will I hear about the results of the study?

We will let you know about the results of the study via email if you indicate your permission below.

## 20. What if I change my mind?

You may withdraw from this study at any time before data analysis is complete. To do so, please email the Withdrawal of Consent form below to [S.McBride@latrobe.edu.au](mailto:S.McBride@latrobe.edu.au).

Your decision to withdraw at any point will **not** affect your relationship with the researcher or La Trobe University.

## 21. Who can I contact for questions or want more information?

If you would like to speak to us, please use the contact details below:

Name/Organisation	Position	Telephone	Email
La Trobe University	Researcher	1.208.339.6707	<a href="mailto:S.McBride@latrobe.edu.au">S.McBride@latrobe.edu.au</a>

**22. What if I have a complaint?**

If you have a complaint about any part of this study, please contact:

Ethics Reference Number	Position	Telephone	Email
HEC20042	Senior Research Ethics Officer	+61 3 9479 1443	<a href="mailto:humanethics@latrobe.edu.au">humanethics@latrobe.edu.au</a>

**Consent Form – Declaration by Participant**

I (the participant) have read understood the Participant Information Statement, and any questions have been answered to my satisfaction. I know I can withdraw at any time until after my data have been analysed. Information I provide may be used only for this specific study. Information I provide may be included in a thesis, presented publicly, and published in journals. My identity will not be disclosed as a participant contributor unless I opt-in to that disclosure by selecting the box below. If I opt into disclosure as a participant contributor, information I provide will not be publicly associated with my name.

<b>Name</b>	
<b>Date</b>	
<b>Signature</b>	

**Opt-in to disclosure as a participant contributor**

☐ Please list my name as a participant contributor to this study.

<b>Name</b>	<b>Email (optional)</b>

**Opt-in to receive results**

☐ Please send me a copy of the results via email.

<b>Name</b>	<b>Email (optional)</b>

## Withdrawal of Consent

I wish to withdraw my consent to participate in this study. I understand withdrawal will not affect my relationship with La Trobe University of any other organisation or professionals listed in the Participant Information Statement. I understand the researchers cannot withdraw my information once it has been analysed, and/or all identifiers have been removed and results have been aggregated.

I understand my information will be withdrawn as outlined below:

- ✓ Any identifiable information about me will be withdrawn from the study
- ✓ The researchers will withdraw my contact details (if you have provided them) from the databank so I cannot be contacted by them or any other research group in the future.

## Participant Signature

Participant's printed name	
Participant's signature	
Date	

## Please forward this form to:

CI Name	Sean McBride
Email	S.McBride@latrobe.edu.au
Phone	1 208 339 6707
Postal Address	ESTEC Box 8380 Idaho State University, Pocatello, ID 83209

## Field Observation Plan and Protocol

1. A key task requiring clarification is identified from the surveys and interviews.
2. Researcher identifies an individual who reports a high level of expertise performing the task.
3. Via email, the individual introduces the researcher to the authoritative (legal) contact for their organization.
4. The researcher and authoritative contact discuss the purposes of the research and the methods to be used.
5. The organization provides written approval to observe, take notes, and/or record performance of the task.
6. This negotiation may include providing the organization the opportunity to review the notes or video taken, as well as to review the contents of any publication.
7. The researcher and individual schedule a day for observation of the key task.
8. Travel occurs.

## Protocol

1. Participant Information and Consent – on site review

Thank you for reviewing and signing the information and consent form.

As indicated in the form, I would like to record this interview. Can you verbally verify that I have your consent to record this field observation?

[START RECORDING].

Now that I've started recording, I'll ask the same question again: do have your permission to record this field observation? Thank you.

I want to make sure you have a firm grasp of our research: What do you understand is the purpose of this research?

Why do you wish to participate?

Thank you.

You are free to withdraw from the study until the final results have been compiled – which I estimate will be within the next 30 days. Simply email me at the same email address through which we have already corresponded requesting to be withdrawn. I will delete all data you have provided me, and send you a note confirming the same.

2. (Participant questions). Do you have any questions for me about this research?



3. (Onsite orientation by organization). Receive safety briefing and personal protective equipment if necessary.
4. Are you still ready to perform <insert task> today?
5. This research method is quite straightforward. You simply do the task, and I will record or take notes. As you perform the task, I may ask you ad hoc questions about what you are doing and why you are doing it.

#### Background information

Observer	
Participant	
Date	
Start time	
End time	

#### Workspace

Description	
Location within facility	
Workspace layout	

#### Other Individuals Involved

Title	Relationship, role relative to task at hand

#### Tools and Technologies Used

Tool	Description of tool

--	--

# Task

Task Name	
What are the goals of this task?	
What preparation does someone need to have in order to perform this task?	
Would you say you are novice, journeyman, or master at this task? Why?	
What circumstances make this task easy?	
What circumstances make this task difficult?	
What would you tell someone who is inexperienced about how to do this task?	
What are the basic steps this task involves?	

## REFERENCES

- Abe, S., Fujimoto, M., Horata, S. Uchida, Y., Mitsunaga, T. (2016). *Security threats of Internet-reachable ICS*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749239>, accessed February 2021.
- ABET (2018). *ABET Approves Accreditation Criteria of Undergraduate Cybersecurity Programs*. <https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/>, accessed June 2020.
- ABET (n.d.). Criteria for Accrediting Engineering Technology Programs, 2020 – 2021. <https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-technology-programs-2020-2021/>, accessed February 2021.
- ABET (n.d.). *What Programs Does ABET Accredite?* <https://www.abet.org/accreditation/what-is-accreditation/what-programs-does-abet-accredit/>, accessed June, 2020
- ABET. (2019). *Member societies*. <https://www.abet.org/about-abet/member-societies/>, accessed June 2020.
- Ackerman, P. (2017). *Industrial Cybersecurity*, Packt Publishing. ISBN 1788395158.
- Ahmed, C., Zhou, J., Mathur, A. (2018). *Noise Matters: Using Sensor and Process Noise Fingerprint to Detect Stealthy Cyber Attacks and Authenticate sensors in CPS*. In Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC '18). Association for Computing Machinery, New York, NY, USA, 566–581. DOI :<https://doi.org/10.1145/3274694.3274748>
- Aleksy, M., Seedorf, S., Cuske, C. (2008). *A Distributed Simulation Environment for Simulation Modeling in Operational Risk Management*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4606672>, accessed February 2021.
- Alem, S., Espes, D., Martin, E., Nana, L., De Lamotte, F. (2019). *A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9035260>, accessed February 2021.
- Amrein, A., Angeletti, V., Beitler, A., Nemet, M., Reiser, M., Riccetti, S., Stoecklin, M., Wespi, A. (2016). *Security intelligence for industrial control systems*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7523351>, accessed February 2021.
- Andriole S. (2012). *Managing Technology in a 2.0 World*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6136222>, accessed February 2021.
- Andriole, S., Bojanova, I. (2014). *Optimizing Operational and Strategic IT*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6908963>, accessed February 2021.
- Ang, C., Utomo, N. (2017). *Cyber Security in the Energy World*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8168583>, accessed February 2021.

- Ansari, S., Castro, F., Weller, D., Babazadeh, D., Lehnhoff, S. (2019). *Towards Virtualization of Operational Technology to Enable Large-Scale System Testing*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8861980>, accessed February 2021.
- Apriliana, A., Sarno, R., Effendi, Y. (2018). *Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8350708>, accessed February 2021.
- Assante, M., Lee, R. (2015). *The Industrial Control System Cyber Kill Chain*.  
<https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- Association for Career and Technical Education (n.d.). *What is CTE?* <https://www.actonline.org/why-cte/what-is-cte/>, accessed June 2020.
- Atasoy, T., Akdoğan, H., Erol, E., Ercin, O., Güreç, O., Benli, O. (2014). *Challenges & opportunities towards smart grid in Turkey; Distribution system operator perspective*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7028940>, accessed February 2021.
- Badar, A., Lou, D., Graf, U., Barth, C., Stich, C. (2019). *Intelligent Edge Control with Deterministic-IP based Industrial Communication in Process Automation*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9012680>, accessed February 2021.
- Balfour, R. (2012). *Next generation emergency management common operating picture software/systems (COPSS)*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6223101>, accessed February 2021.
- Ban, Y., Okamura, K., Kaneko, K. (2017). *Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education*, 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), Hamamatsu, pp. 699-704
- Barnes, A. (2003). *'We have your water supply, and printers' – Brumcon report*.  
[https://www.theregister.co.uk/2003/10/20/we\\_have\\_your\\_water\\_supply/](https://www.theregister.co.uk/2003/10/20/we_have_your_water_supply/), accessed February 2021.
- Batke, B., Wiberg, J., Dubé, D. (2015). *CIP Security Phase 1 Secure Transport for EtherNet/IP*.  
<https://docplayer.net/11561418-Cip-security-phase-1-secure-transport-for-ethernet-ip.html>, accessed February 2021
- Beilinson, J. (2012). *How to Escape a Sinking Helicopter*.  
<https://www.popularmechanics.com/adventure/outdoors/a8472/how-to-escape-a-sinking-helicopter-14821752/>, accessed February 2021.
- Bell, H., Andrews, D., Wulfeck, W., (2010). *Behavioral Task Analysis*, Book Chapter “Improving Performance in The Workplace” edited by Silber, K., Foshay, W. Pfeiffer. ISBN 9780470190685.
- Benbenishty, L. (2017). *SCADA MODBUS Protocol Vulnerabilities*. <https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/>, accessed February 2021, accessed February 2021.
- Benz, U., Baatz, M., Schreier, G. (2001). *OSCAR-object oriented segmentation and classification of advanced radar allow automated information extraction*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=977114>, accessed February 2021.

Bernieri, G., Conti, M., Pascucci, F. (2019). *MimePot: a Model-based Honeypot for Industrial Control Networks*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8913891>, accessed February 2021.

Bishop, M., Talyor, C. (2009). *A Critical Analysis of the Centers of Academic Excellence Program*, Proceedings of the 13th Colloquium for Information Systems Security Education. <https://cisse.info/resources/archives/category/12-papers?download=125:s01p04-2009>, accessed February 2020.

Bloom, B. (1956). as described by University of Toronto. *Appendix B: Useful Verbs for Developing Learning Outcomes*, (n.d.). <https://teaching.utoronto.ca/teaching-support/course-design/developing-learning-outcomes/appendix-b-useful-verbs-for-developing-learning-outcomes/>. Accessed June 2020.

Bochman, A., Freeman, S. (2021). *Countering Cyber Sabotage*. CRC Press.

Boyer W., McQueen M. (2008). *Ideal Based Cyber Security Technical Metrics for Control Systems*. In: Lopez J., Hämmerli B.M. (eds) Critical Information Infrastructures Security. CRITIS 2007. Lecture Notes in Computer Science, vol 5141. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-540-89173-4\\_21](https://doi.org/10.1007/978-3-540-89173-4_21)

Burbano, A., Martín, A., León, C., Personal, E. (2017). *Challenges for citizens in energy management system of smart cities*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7973850>, accessed February 2021.

Burley, D., Bishop, M., Buck, S., Ekstrom, J., Fatcher, 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://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017\\_web.pdf](https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf), accessed February 2021.

Bush, G. (2001). *Executive Order 13231 – Critical Infrastructure Protection in the Information Age*. <https://fas.org/irp/offdocs/eo/eo-13231.htm>, accessed February 2021.

Causey, W., Thielbar, B. (2012) *Merging the IT/Operations Silos*, Power Grid International. <https://www.power-grid.com/2012/01/01/merging-the-it-operations-silos/>, accessed July 2020.

Cavalcante, M., de Souza Silva, J., Villalva, M., Lins, M. (2019). *Performance analysis of a Solar Photovoltaic Power Plant*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8894937>, accessed February 2021.

Cerotti, D., Codetta-Raiteri, D., Egidi, L., Franceschinis, G., Portinale, L., Dondossola, G., Terruggia, R. (2019). *Analysis and Detection of Cyber Attack Processes targeting Smart Grids*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8905716>, accessed February 2021.

Cherapanov A., Lipovsky, R. (2017). *Industroyer: Biggest threat to industrial control systems since Stuxnet*. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>, accessed June 2020.

CITI Program (n.d.). <https://about.citiprogram.org/>, accessed November 2021.

City of San Diego Independent Rates Oversight Committee, (2019). *Independent Rates Oversight Committee (IROC) Meeting of March 18, 2019*. <https://www.sandiego.gov/sites/default/files/irocminutes190318.pdf>, accessed July 2020.

Clark, D. (1999). *Bloom's Taxonomy of Learning Domains*.  
<http://www.nwlink.com/~donclark/hrd/bloom.html>, accessed February 2021.

Clayton, M., (2014). *Exclusive: New thesis on how Stuxnet infiltrated Iran nuclear facility*. Cristian Science Monitor. <https://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility>, accessed February 2021.

Clinton, B. (1996). *Executive Order 13010—Critical Infrastructure Protection*.  
<https://www.hsdl.org/?view&did=1613>, accessed February 2021.

Colelli, R., Panzieri, S., Pascucci, F. (2019). *Securing connection between IT and OT: the Fog Intrusion Detection System prospective*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8792884>, accessed February 2021.

Committee for National Security Systems (2004). *CNSS Instruction 4013 National Information Assurance Training Standard for Systems Administrators (SA)*.  
<https://www.cnss.gov/CNSS/openDoc.cfm?ijdqRrw9p/GJn6C0m38UfA==>, accessed February 2021.

Committee for National Security Systems (2004). *CNSS Instruction 4014 National Information Assurance Training Standard for Information Systems Security Officers*.  
<https://www.cnss.gov/CNSS/openDoc.cfm?xgO7MssVotEuY1YtGU7jdg==>, accessed February 2021.

Committee for National Security Systems (2004). *CNSS Instruction No. 4012 National Information Assurance Training Standard for Senior Systems Managers*.  
<https://www.cnss.gov/CNSS/openDoc.cfm?A1zNmszmWbUXN09fXzO2sQ==>, accessed February 2021.

Committee for National Security Systems (2005). *CNSS Instruction No. 4016 National Information Assurance Training Standard for Risk Analysts*.  
<https://www.cnss.gov/CNSS/openDoc.cfm?G9w8i3mtNEIJ6Or5Mozewg==>, accessed February 2021.

Committee on National Security Systems (n.d.). *Instructions*.  
<http://www.cnss.gov/CNSS/issuances/Instructions.cfm>, accessed June 2020.

Conklin W, Cline R, Roosa T. (2014). *Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors*, 47th Hawaii International Conference on System Sciences, Waikoloa, HI, pp. 2006-2014.

Conklin, A. (2016). *IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience*, 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 2642-2647, doi: 10.1109/HICSS.2016.331.

Conklin, W. (2015). *State Based Network Isolation for Critical Infrastructure Systems Security*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7070087>, accessed February 2021.

Craggs, B., Rashid, A., Hankin, C., Antrobus, R., Åžerban, O., Thapen N. (2019). *A reference architecture for IIoT and industrial control systems testbeds*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9038033>, accessed February 2021.

Cresswell, J. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4<sup>th</sup> Ed. Sage Publications. ISBN 9781452226101

Creswell, J., Miller, D. (2000). *Determining Validity in Qualitative Inquiry*. Theory Into Practice, 39(3), pp.124

de Leon, D., Bhandari, V., Jillepalli, A., Sheldon, F. (2016). *Using a knowledge-based security orchestration tool to reduce the risk of browser compromise*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7849910>, accessed February 2021.

de Zafra, D., Pitcher, S., Tressler, J., Ippolito, J. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf>, accessed February 2021.

Delbecq, A., Van de Ven, A., Gustafson, D. (1975). *Group techniques for program planning : a guide to nominal group and Delphi processes*. Scott, Foresman.

Denzin, N., Lincoln, Y. (1994). *Introduction: Entering the field of qualitative research*. In N.K. Denzin & Y.S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 1-17). Thousand Oaks, CA: Sage.

Department of Defense (1983). *Trusted Computer System Evaluation Criteria*.

<https://www.cs.cmu.edu/afs/cs/usr/bsy/security/CSC-STD-001-83.txt>, accessed February 2021.

Department of Energy (n.d.). *Pacific Northwest National Laboratory*.

<https://www.energy.gov/ea/pacific-northwest-national-laboratory>

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 June 2020.

Deshmukh, P., Patterson, C., Baumann, W. (2016). *A hands-on modular Laboratory environment to foster learning in control system security*, 2016 IEEE Frontiers in Education Conference (FIE), Erie, PA, USA, pp. 1-9. <https://ieeexplore-ieee-org.libpublic3.library.isu.edu/document/7757669>

Dunn, A. (2008). *The father of invention: Dick Morley looks back on the 40th anniversary of the PLC*.

<https://www.automationmag.com/855-the-father-of-invention-dick-morley-looks-back-on-the-40th-anniversary-of-the-plc/>, accessed February 2021.

Eckhart, M., Ekelhart, A., Weippl, E. (2019). *Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8869197>, accessed February 2021.

Edwards, M. (n.d.). LinkedIn profile. <https://www.linkedin.com/in/%F0%9F%98%8Emarty-edwards-738aa313b/>

Elegbe, J. (2015). Emotional intelligence: Missing priority in engineering programs. *Journal of Business Studies Quarterly*, 7(2), 196-207. Retrieved from <https://search.proquest.com/scholarly-journals/emotional-intelligence-missing-priority/docview/1755024715/se-2?accountid=11563>, February 2021.

Emerson (n.d.) *Zedi Cloud SCADA Solutions*. <https://www.emerson.com/en-us/automation/control-and-safety-systems/scada-systems/zedi-cloud-scada-solutions>, accessed February 2021.

ENISA (n.d.). *About ENISA - The European Union Agency for Cybersecurity*.  
<https://www.enisa.europa.eu/about-enisa>, accessed February 2021.

Falco, J., Stouffer, K., Wavering, A., Proctor F. (2002). *IT Security for Industrial Control Systems*.  
<https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6859.pdf>, accessed February 2021.

Federation of Concerned Scientists (n.d.). *NSA/NCSC Rainbow Series*.  
<https://fas.org/irp/nsa/rainbow.htm>, accessed February 2021.

Felser, M., Rentschler M., Kleineberg, O. (2019). *Coexistence Standardization of Operation Technology and Information Technology*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8667427>, accessed February 2021.

Fink, G., Shulga, Y. (2018). *Helping IT and OT Defenders Collaborate*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8539125>, accessed February 2021.

FIRST (n.d.). *Common Vulnerability Scoring System version 3.1: Specification Document*.  
<https://www.first.org/cvss/specification-document>, accessed December 2021.

Fraile, F., Tagawa, T., Poler, R., Ortiz, A.. (2018). *Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8353121>, accessed February 2021.

Fu, R., Gao, F., Zeng, R., Hu, J., Luo, Y., Qu, L. (2017). *Big data and cloud computing platform for energy Internet*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8388531>, accessed February 2021.

Galinec, D. Steingartner, W. (2017). *Combining cybersecurity and cyber defense to achieve cyber resilience*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8327227>, accessed February 2021.

Garimella, P. (2018). *IT-OT Integration Challenges in Utilities*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8586807>, accessed February 2021.

GE Digital (n.d.). *Predix Platform*. <https://www.ge.com/digital/iiot-platform>, accessed February 2021.

Geenberg A. (2017). *'Crash Override': The Malware That Took Down A Power Grid*.  
<https://www.wired.com/story/crash-override-malware/>, accessed June 2020.

GIAC. (2020). *Cyber Security Certification: GICSP*. <https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp>, accessed June 2020.

Giehl, A., Plaga, S. (2018). *Implementing a performant security control for Industrial Ethernet*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8642758>, accessed February 2021.

Glomb, C., Kuntschke, R., Specht, M., van Amelsvoort, M., Wagler, M., Winter, M., Witzmann, R. (2016). *Grid-aware VPP operation*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7514128>, accessed February 2021.



Goto, S., Yoshie, O., Fujimura, S. (2017). *Industrial IoT business workshop on smart connected application development for operational technology (OT) system integrator*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8289864>, accessed February 2021.

Gray, S. (2016). *Cyber security in modern power systems defending the grid*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7835822>, accessed February 2021.

Greenberg, A. (2019). *A Peek into the Toolkit of the Dangerous Triton Attackers*.  
<https://www.wired.com/story/triton-hacker-toolkit-fireeye/>, accessed February 2021.

Greenberg, A. (2019). *Sandworm*. Anchor Books. ISBN 9780525564638

Greenberg, A. (2020) How 30 Lines of Code Blew Up a 27-Ton Generator,  
<https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/>, accessed February 2021.

Grenacher (2018). *Industry 4.0, The Smart Factory And Machines-As-A-Service*.  
<https://www.forbes.com/sites/forbestechcouncil/2018/04/11/industry-4-0-the-smart-factory-and-machines-as-a-service/?sh=60de4e241dff>, accessed February 2021.

Hachana, S., Cuppens, F., Cuppens-Boulahia, N. (2016). *Towards a new generation of industrial firewalls: Operational-process aware filtering*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7906996>, accessed February 2021.

Hadžiosmanović, D., Sommer, R., Zambon, E., Hartel, P. (2014). *Through the eye of the PLC: semantic security monitoring for industrial processes*. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14). Association for Computing Machinery, New York, NY, USA, 126–135. DOI: <https://doi.org/10.1145/2664243.2664277>

Harp D., Gregory-Brown B. (2016.) *The GICSP: A Keystone Certification*.  
<https://www.sans.org/reading-room/whitepapers/training/gicsp-keystone-certification-37232>, accessed June 2021.

Hasan, K., Shetty, S.; Hassanzadeh, A., Ullah, S. (2019). *Towards Optimal Cyber Defense Remediation in Cyber Physical Systems by Balancing Operational Resilience and Strategic Risk*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9021076>, accessed February 2021.

Hassan, Q. (2018). *The Industrial Internet of Things*.  
<https://ieeexplore.ieee.org/xpl/ebooks/bookPdfWithBanner.jsp?fileName=8390825.pdf&bkn=8390726&pdfType=chapter>, accessed February 2021.

Hayes, J. (2017). *Pay up - or else [IT Ransomware]*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7908776>, accessed February 2021.

He, W. (2017). *Poster Abstract: Design of Intelligent Software Systems for Cyber-Physical Systems*.  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7946900>, accessed February 2021.

Hoffman, R. (2005). *Protocols for Cognitive Task Analysis*.  
<https://apps.dtic.mil/dtic/tr/fulltext/u2/a475456.pdf>, accessed February 2021.

Hough, D. (2016). *IET: cyber security in modern power systems: IT and operational technology integration*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7835824>, accessed February 2021.

Idaho Career and Technical Education (n.d.) *Technical Advisory Committees*, <https://cte.idaho.gov/educators/technical-advisory-committees/>, accessed June 2020.

Idaho National Laboratory (2018). *Consequence-driven Cyber-informed Engineering*. [https://inl.gov/wp-content/uploads/2018/02/18-50019\\_CCE\\_R1-1.pdf](https://inl.gov/wp-content/uploads/2018/02/18-50019_CCE_R1-1.pdf), accessed February 2020.

Idaho National Laboratory (2020). *Building an Industrial Cybersecurity Workforce: A Manager's Guide*. [https://inl.gov/wp-content/uploads/2020/12/ICS\\_Workforce-ManagersGuide2020.pdf](https://inl.gov/wp-content/uploads/2020/12/ICS_Workforce-ManagersGuide2020.pdf) Accessed February 2021.

Idaho State Board of Education (2015). *State Board of Education Meeting*. [https://boardofed.idaho.gov/meetings/board/archive/2015/08\\_12-13\\_15/AgendaAll.pdf](https://boardofed.idaho.gov/meetings/board/archive/2015/08_12-13_15/AgendaAll.pdf), accessed February 2021.

Idaho State University (2008). *Regional benefits seen as ISU's new Energy Systems Technology and Education Center debuts*. <http://headlines.isu.edu/?p=1535>

Idaho State University (n.d.) *Ignite Their Future Summer Camp Series* <https://cetrain.isu.edu/enrolment/course/ignite-their-future-summer-camp-series/>, accessed June 2020

Idaho State University (n.d.). *Energy System Technology & Education Center (ESTEC)*. <https://www.isu.edu/estec/>, accessed February 2021.

Idaho State University (n.d.). *Simplot Decision Support Center*. <http://cobhomepages.cob.isu.edu/schou/SDSC.htm> accessed June 2020.

Idaho State University 2021-2022 Academic Catalog. <http://coursecat.isu.edu/undergraduate/technology/energysystemstechnologyandeducationcenter/aas-industrial-cybersecurity-engr-tech/>

IEEE. (2018). *IEEE Approved Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8388755>, accessed February 2021.

IEEE. (2018). *IEEE Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8304857>, accessed February 2021.

IEEE. (2018). *IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8423800>, accessed February 2021.

Inductive Automation (n.d.) <https://inductiveautomation.com/>, accessed February 2021.

Industrial Control Systems Cybersecurity Conference (n.d.). <https://www.icscybersecurityconference.com/>, accessed February 2021.

Industrial Cybersecurity Community of Practice (n.d.). <https://inl.gov/icscop/>, accessed November 2021.

Information Assurance Directorate (2020). *Knowledge Units*. Retrieved from: [https://www.iad.gov/NIETP/documents/Requirements/CAE-CD\\_2020\\_Knowledge\\_Units.pdf](https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf)

International Society of Automation ((2007). *ANSI/ISA-62443-1-1 (99.01.01)—2007 Security for Industrial Automation and Control Systems Part 1-1 Terminology, Concepts, and Models*.

International Society of Automation (n.d.) *ISA/IEC 62443 Cybersecurity Certificate Programs*. <https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/>, accessed June 2020.

International Society of Automation (n.d.). *About ISA*. <https://www.isa.org/about-isa/>, accessed June 2020.

International Society of Automation (n.d.). *CCST Level I, II, III Examination Content Outline*. [https://www.isa.org/uploadedFiles/Content/Training\\_and\\_Certifications/ISA\\_Certification/CCST%20Level%20I%20II%20III%20Blueprint%20Comparison%20Final%2020180430.pdf](https://www.isa.org/uploadedFiles/Content/Training_and_Certifications/ISA_Certification/CCST%20Level%20I%20II%20III%20Blueprint%20Comparison%20Final%2020180430.pdf), accessed June 2020.

International Society of Automation (n.d.). *Certification Programs*. <https://www.isa.org/training-and-certifications/isa-certification/>, accessed June 2020.

International Society of Automation (n.d.). *Industrial Automation and Control Systems Security, 2019*. <https://www.isa.org/isa99/>, accessed June 2020.

ISA (n.d.) *About ISA*. <https://www.isa.org/about-isa/>, accessed February 2021.

ISA (n.d.) *ISA99, Industrial Automation and Control Systems Security*. <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>, accessed February 2021.

ISA Global Cybersecurity Alliance (2020). *ISAGCA Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems*, <https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf>, accessed February 2021.

J. Mustafa; Sandström, K., Ericsson, N., Rizvanovic, L. (2019). *Analyzing availability and QoS of service-oriented cloud for industrial IoT applications*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8869274>, accessed February 2021.

Jalali, S., Bhatnagar, I. (2015). *Leveraging Internet of Things Technologies and Equipment Data for an Integrated Approach to Service Planning and Execution*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7166235>, accessed February 2021.

Jillepalli, A., de Leon, D., Johnson, B., Chakhchoukh, Y., Oyewumi, I., Ashrafuzzaman, M.; Sheldon, F., Alves-Foss, J., Haney, M. (2018). *METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8659367>, accessed February 2021.

Johnson, B., Caban D., Krotofil M., Scali, D., Brubaker, N., Glyer, C. (2017). *Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure*. <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>, accessed June 2020.

Jonassen, D., Tessmer, M., Hannum, W. (1998). *Task Analysis Methods for Instructional Design*, Rutledge.

Kai, A. Zhaoting, T. (2013). *Relative Navigation and Guidance Technologies for Rendezvous and Docking*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6840663>, accessed February 2021.

Kapellmann, D., Washburn, R. (2019). *Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8756895>, accessed February 2021.

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E., Papadourakis, G. (2019). *Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8858454>, accessed February 2021.

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E., Papadourakis, G. *Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0*, 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 2019, pp. 1-6, doi: 10.1109/CAMAD.2019.8858454.

Kavallieratos, G.; Katsikas, S.; Gkioulos, V. (2020). *Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey*. *Future Internet* 2020, 12, 65. <https://doi.org/10.3390/fi12040065>.

Kelley, K., Clark, B., Brown., V., Sitzia, J. (2003). *Good practice in the conduct and reporting of survey research*, *International Journal for Quality in Health Care*, Volume 15, Issue 3, Pages 261–266, <https://doi.org/10.1093/intqhc/mzg031>).

Khaw, Y., Jahromi, A., Mohammadreza, A, Kundur, D., Sanner, S., Kassouf, M. (2019). *Preventing False Tripping Cyberattacks Against Distance Relays: A Deep Learning Approach*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8909810>, accessed February 2021.

Kim, C., Choi, T., Jeong, T., Lee, Y. (2003). *An integrated service and network management system for MPLS traffic engineering and VPN services*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1251226>, accessed February 2021.

Kirkpatrick Partners (n.d.). *The Kirkpatrick Model*. <https://www.kirkpatrickpartners.com/Our-Philosophy/The-Kirkpatrick-Model>

Koorapati, K., Ramesh, P., Veeraswamy, S. (2018). *Ontology Based Resource Management for IoT Deployed with SDDC*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8648642>, accessed February 2021.

Krebs, B. (2012). *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*. <https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/>, accessed June 2020.

Krishna, V., Wu, Z., Ambardekar, V, Macwan, R., Sanders, W. (2018). *Cyberattacks on Primary Frequency Response Mechanisms in Power Grids*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8625915>, accessed February 2021.

- Krotofil, M. (2015). *Damn Vulnerable Chemical Processes*. <https://www.slideshare.net/phdays/damn-vulnerable-chemical-process>, accessed February 2021.
- Krotofil, M., Larson, J., Gollmann, D. (2015). *The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems*. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15). Association for Computing Machinery, New York, NY, USA, 133–144. DOI: <https://doi.org/10.1145/2714576.2714599>
- Kuusk, A., Gao, J. (2015). *Factors for successfully integrating operational and information technologies*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7273136>, accessed February 2021.
- Lagouardat, M., Wine, J., Carre, O. (2017). *Intelligent network assets supervision and control in Enedis*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8316099>, accessed February 2021.
- Langner, R. (2013). *To Kill a Centrifuge*. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>, accessed February 2021.
- Lappalainen, P. (2015) *Predictors of effective leadership in industry – should engineering education focus on traditional intelligence, personality, or emotional intelligence?*, European Journal of Engineering Education, 40:2, 222-233, DOI: 10.1080/03043797.2014.944102
- Larsen, J. (2015). *Physical Damage 101: Bread and Butter Attacks*. <https://www.blackhat.com/docs/us-15/materials/us-15-Larsen-Remote-Physical-Damage-101-Bread-And-Butter-Attacks.pdf>, accessed February 2021.
- Levine, E., Ash, R., Hall, H., Sistrunk, F. (1983). Evaluation of Job Analysis Methods by Experienced Job Analysts. *Academy of Management Journal*. Vol. 26, No. 2, 339-348. [https://www.researchgate.net/profile/Ronald-Ash/publication/275694539\\_Evaluation\\_Of\\_Job\\_Analysis\\_Methods\\_By\\_Experienced\\_Job\\_Analysts/links/5877ba5f08ae6eb871d15fb2/Evaluation-Of-Job-Analysis-Methods-By-Experienced-Job-Analysts.pdf](https://www.researchgate.net/profile/Ronald-Ash/publication/275694539_Evaluation_Of_Job_Analysis_Methods_By_Experienced_Job_Analysts/links/5877ba5f08ae6eb871d15fb2/Evaluation-Of-Job-Analysis-Methods-By-Experienced-Job-Analysts.pdf), accessed March 2021.
- Lincoln, Y., Guba, E. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage.
- Litherland, P., Orr, R., Piggin, R. (2016). *Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7857397>, accessed February 2021.
- Liu, R. (2017). *Led by compact PLCs, the global PLC market reached \$8.5 billion in 2017*. Retrieved from <https://technology.ihc.com/599840/led-by-compact-plcs-the-global-plc-market-reached-85-billion-in-2017>
- Liu, Y., Candell, R., Kashef, M., Benmohamed, L. (2018). *Dimensioning wireless use cases in Industrial Internet of Things*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8402370>, accessed February 2021.
- Liu, Y., Kashef, M., Lee, K., Benmohamed, L., Candell, R. (2019). *Wireless Network Design for Emerging IIoT Applications: Reference Framework and Use Cases*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8692410>, accessed February 2021.

LocalNews8 (2019). *INL tapped for four R&D awards*. <https://localnews8.com/news/2019/12/03/inl-tapped-for-four-rd-awards/>, accessed February 2020.

Macaulay, T. (2016). *RIOT Control*. Morgan Kaufmann. ISBN 0124199712.

Maconachy, V., Schou, C., Ragsdale, D. and Welch, D. (2001). *A Model for Information Assurance: An Integrated Approach*. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY. pp. 306-310.  
<http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf>, accessed February 2021.

Mager, R. (1997) *Making Instruction Work* 2<sup>nd</sup> ed. Center for Effective Performance. ISBN1879618028.

Manson, S., Anderson, D. (2017). *Practical cybersecurity for protection and control system communications networks*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8188738>, accessed February 2021.

Marali, M., Sudarsan, S., Gogioneni, A. (2019). *Cyber security threats in industrial control systems and protection*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9079981>, accessed February 2021.

Marszal, E., McGlone, J. (2019). *Security PHA Review for Consequence-Based Cybersecurity*. International Society of Automation.

Masadeh, M. (2012). *Training, Education, Development and Learning: What is the Difference?* European Scientific Journal, ESJ, 8(10). <https://doi.org/10.19044/esj.2012.v8n10p%p>.  
<https://core.ac.uk/download/pdf/236411025.pdf>, accessed February 2021.

McBride S. (2018). Telephone interview with Michael J. Assante.

McBride, S. (2016). *Overload: Critical Lessons from 15 Years of ICS Vulnerabilities*. <https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html>, accessed February 2021.

McBride, S. (2016). *Overload: Critical Lessons from 15 Years of ICS Vulnerabilities*. <https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security/rpt-industrial-control-systems-vulnerability-trend-report-2016.html>, accessed June 2020.

McConville, J. (1997). *U.S. Army Information Operations: Concept and Execution*. <https://fas.org/irp/agency/army/mipb/1997-1/mcconvl.htm>, accessed February 2021.

McCumber, J. (1991). *Information Systems Security: A Comprehensive Model*. Proceedings of the 14<sup>th</sup> National Computer Security Conference. Washington, DC. pp. 328-337.  
<https://csrc.nist.gov/csrc/media/publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-ncsc-proceedings-vol-1.pdf>, accessed February 2021.

McGettrick A., Cassel, L., Dark, M., Hawthorne, E., Impagliazzo, J. (2014). *Toward curricular guidelines for cybersecurity*. In Proceedings of the 45th ACM technical symposium on Computer science education (SIGCSE '14). Association for Computing Machinery, New York, NY, USA, 81–82. DOI:<https://doi.org/10.1145/2538862.2538990>, accessed February 2021.

McQueen, M., Boyer, W. (2008). *Primer Control System Cyber Security Framework and Technical Metrics*. <https://inldigitallibrary.inl.gov/sites/sti/sti/4012627.pdf>, accessed February 2021.

McQueen, M., Boyer, W., McBride, S., Farrar, M., Tudor, Z. (2008). *Measurable Control System Security Through Ideal Driven Technical Metrics*. <https://inldigitallibrary.inl.gov/sites/sti/sti/3881671.pdf>, accessed February 2021.

Miller, A., Erickson, K. (2004). *Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity*. <http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.214.6366>, accessed February 2021.

Miller, G. (1955). *The magical number seven, plus or minus two: Some limits on our capacity for processing information*. *Psychological Review*. 63 (2): 81–97. CiteSeerX 10.1.1.308.8071. doi:10.1037/h0043158

Miškuf, M., Zolotová, I., Mocnej, J. (2018). *Healthcare data classification: Cloud-based architecture concept*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8337557>, accessed February 2021.

Mitrović Veljković, S., Nešić, A., Dudić, B., Gregus, M., Delić, M., Meško, M., (2020). *Emotional Intelligence of Engineering Students as Basis for More Successful Learning Process for Industry 4.0*. *Mathematics* 2020, 8, 1321. <https://doi.org/10.3390/math8081321>.

Modbus Organization (n.d.). *Modbus FAQ*. <http://www.modbus.org/faq.php>, accessed February 2021.

Modbus-IDA (2004). *Modbus Protocol becomes IEC Publicly Available Specification : IEC PAS 62030 (pre-standard)*. [http://www.modbus.org/docs/IEC\\_PAS\\_PR-r2.pdf](http://www.modbus.org/docs/IEC_PAS_PR-r2.pdf), accessed February 2021.

Moquin, S., Kim, S., Blair, N., Farnell, C., Di, J., Mantooth, H. (2019). *Enhanced Uptime and Firmware Cybersecurity for Grid-Connected Power Electronics*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8925027>, accessed February 2021.

Morella, J. (2019). *Cyber PHA: A proven method to assess industrial control system cybersecurity risk*. <https://engineering.purdue.edu/P2SAC/presentations/documents/CyberPHA-P2SAC-Fall-2019-Jacob-Morella.pdf>, accessed February 2021.

Morris, A., Goode, P. (2002). The aeronautical data link: taxonomy, architectural analysis, and optimization. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1067938>, accessed February 2021.

Müller, T., Walz, A., Kiefer, M., Doran, H., Sikora, A. (2018). *Challenges and prospects of communication security in real-time ethernet automation systems*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8402338>, accessed February 2021.

Mustard, S. (2018). *Mission Critical Operations Primer*, International Society of Automation. ISBN 9781945541711.

Nandagopal J., Lethakumari, R. (2015). *Optimal control of Spacecraft Docking System using integral LOR controller*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7229586>, accessed February 2021.

National Academies of Sciences, Engineering, and Medicine (2016). *A 21st Century Cyber-Physical Systems Education*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/23686>. [Online]. <https://www.nap.edu/catalog/23686/a-21st-century-cyber-physical-systems-education>, Accessed June 2020.

National Centers of Academic Excellence in Cybersecurity (2020). *National Centers of Academic Excellence in Cybersecurity Journal*. [https://www.caecommunity.org/sites/default/files/CAE\\_Book\\_Version\\_2.0\\_Compressed.pdf](https://www.caecommunity.org/sites/default/files/CAE_Book_Version_2.0_Compressed.pdf), accessed February 2021.

National Institute of Standards and Technology, National Computer Security Conference, (16th) Proceedings, p. 462. (1993). [Online]. <https://books.google.com/books?id=vQEHUD51YNEC>, accessed June 29, 2020.

National Instruments (2019). *The Modbus Protocol In Depth*. <http://www.ni.com/en-us/innovations/white-papers/14/the-modbus-protocol-in-depth.html>, accessed February 2021.

National Research Council (2013). *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/18446>, accessed February 2021.

National Security Agency (n.d). *NSA/DHS National CAE in Cyber Defense Designated Institutions*. [https://www.iad.gov/NIETP/reports/cae\\_designated\\_institutions.cfm](https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm), accessed 2020.

National Security Agency (n.d.). *National Centers of Academic Excellence*. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/>, accessed June 2020.

National Security Agency (n.d.) *Mission and Values*. <https://www.nsa.gov/about/mission-values/>, accessed February 2020.

National Security Telecommunications and Information Systems Security (1994). *Instruction 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals*. <https://www.cnss.gov/CNSS/openDoc.cfm?PrazeVTB8qMcYxKqa+5bHw==>, accessed February 2021.

National Security Telecommunications and Information Systems Security (2000). *NSTISSI No. 4015 National Training Standard for Systems Certifiers*. <https://www.cnss.gov/CNSS/openDoc.cfm?xgO7MssVotEuY1YtGU7jdg==>, accessed February 2021.

National Transportation Safety Board (2010). *Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station Washington, D.C. June 22, 2009*. <https://www.nts.gov/investigations/AccidentReports/Reports/RAR1002.pdf>, accessed February 2021.

National Transportation Safety Board (2011). *Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire San Bruno, California September 9, 2010*. <https://www.nts.gov/investigations/AccidentReports/Reports/PAR1101.pdf>, accessed February 2021.

Naukkarinen, O., Palomaki, T, Vanharanta, H. (2001). *A new method for valuing R&D investments: a qualitative and quantitative evaluation*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=952294>, accessed February 2021.



NERC (2013). *Frequently Asked Questions*.

<https://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf>, accessed February 2021.

NERC (n.d.) *CIP-004-6 — Cyber Security – Personnel & Training*

[https://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training), accessed February 2021.

NERC (n.d.). *CIP Standards*. <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>, accessed February 2021.

NERC (n.d.). *CIP-003-8 - Cyber Security — Security Management Controls*.

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf>, accessed February 2021.

NERC (n.d.). *CIP-013-1 – Cyber Security - Supply Chain Risk Management*.

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf>, accessed February 2021.

Newhouse W., Keith S., Scribner B. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, Washington, DC. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>, accessed February 2020.

Newman, L. (2018). *Menacing Malware Shows the Dangers of Industrial System Sabotage*.

<https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/>, accessed June 2020.

Nüßer, W., Koch, E., Trsek, H., Schumann, R., Mahrenholz, D. (2017). *Cyber security in production networks: An empirical study about the current status*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8247725>, accessed February 2021.

O’Neil, L., Assante, M., Tobey, D., Conway, T., Vanderhorts, T., Januszewski, J., Leo, R., Perman, K. (2013). *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Development Programs for Phase 2 of the Secure Power Systems Professional project*.

[https://www.pnnl.gov/main/publications/external/technical\\_reports/PNNL-22653.pdf](https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-22653.pdf), accessed February 2021.

O’Neil, L., Conway, T., Tobey, D., Greitzer, F., Dalton, A., Pusey, P. (2015). *SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Job Profiles*,

[https://www.pnnl.gov/main/publications/external/technical\\_reports/PNNL-24138.pdf](https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24138.pdf), accessed February 2021.

O’Neill, P. (2017). *NotPetya ransomware cost Merck more than \$310 million*.

<https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/>, accessed February 2021.

O’Neil, 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](https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24140.pdf), retrieved February 2020.

Obaidli, S., Subramaniam, V., Alhuseini, H., Gupta, R., Dolezilek, D., Kalra, A., Sankar, P. (2017).

*IEC 61850 beyond compliance: A case study of modernizing automation systems in transmission power*

*substations in Emirate of Dubai towards smart grid.*

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8356501>, accessed February 2021.

Obama, B. (2013). *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*

<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>, accessed February 2021.

Oh, E., Son, S. (2017). *A framework for consumer electronics as a service (CEaaS): a case of clustered energy storage systems*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8013255>, accessed February 2021.

O'Neil, K., LeBlanc, L., Vázquez, J. (2015). *Eyes on the Ocean applying operational technology to enable science*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7404390>, accessed February 2021.

Pauna, A., (2014). *Certification of Cyber Security skills of ICS/SCADA professionals*.

[https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at\\_download/fullReport](https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport), accessed February 2021.

Payne, E., Wang, Q., Shulin, L., Wu, L. (2019). *Technical risk synthesis and mitigation strategies of distributed energy resources integration with wireless sensor networks and internet of things review*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8804868>, accessed February 2021.

Pescatore, J. (2011). in *SANS NewsBites Volume XIII - Issue #63*.

<https://www.sans.org/newsletters/newsbites/xiii/63>, accessed July 2020.

Peterson, D. (2012). *Telvent Compromised!* <https://dale-peterson.com/2012/09/26/telvent-compromised/> accessed June 2020.

Peterson, R., Santos, D., Smith, M., Wetzel, K., Witte, G. *Workforce Framework for Cybersecurity” NIST Special Publication 800-181 Revision 1*. (2020)

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>, accessed February 2020.

Piggin, R. (2014). *Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7111736>, accessed February 2021.

Piggin, R. (2014). *Industrial systems: cyber-security's new battlefield [Information Technology Operational Technology]*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6905657>, accessed February 2021.

Piggin, R., Buffey, I. (2016). *Active defence using an operational technology honeypot*.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7857401>, accessed February 2021.

Polge, J., Robert, J., Traon, Y. (2019). *Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8651671>, accessed February 2021.

Preston, R., Duck, M., Finnegan, C., Munoz, R. (2019). *Integrating Cyber Security Requirements into a Power Management System*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9074514>, accessed February 2021.

Primoff, E. (1975). *How to Prepare and Conduct Job Element Examinations*. Personnel Research and Development Center, U.S. Civil Service Commission.

Public Utilities Fortnightly (2019). *Top Innovators: Arizona Public Service*, Interview with Kim Wagie. <https://www.fortnightly.com/fortnightly/2019/11-0/top-innovators-arizona-public-service>, accessed 2020.

Rajagopal, N., Prasad, K., Shah, M., Rukstales, C. (2014). *A new data classification methodology to enhance utility data security*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6816451>, accessed February 2021.

Rama, D., Taylor, S. (2014). *Remote monitoring and control of wastewater assets delivering reduced whole life costs*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7129221>, accessed February 2021.

Rausch, M., Krishna, V., Gu, P., Chandra, R., Feddersen, B., Fawaz, A., Sanders, W. (2018). *Peer-to-peer Detection of DoS Attacks on City-Scale IoT Mesh Networks*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8587518>, accessed February 2021.

Research and Markets (2018). *Global Factory Automation Market 2018-2025 by Control & Safety System, Component and Industry Vertical - ResearchAndMarkets.com*. Retrieved from <https://www.businesswire.com/news/home/20180808005611/en/Global-Factory-Automation-Market-2018-2025-Control-Safety>, accessed February 2021.

Rogers, J., Watkins, C., Chung, J. (2010). *The 2005 Upper Taum Sauk Dam Failure: A Case History*. Environmental and Engineering Geoscience 2010; 16 (3): 257–289. doi: <https://doi.org/10.2113/gseegeosci.16.3.257>

Rozic, B., Mlakar, D., Gruden, M., Petrovic, N. (2017). *Elektro Gorenjska CIM project*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8316137>, accessed February 2021.

Ryan, J. *Architecting Information Assurance*. (2004). IEEE International Conference on Performance, Computing, and Communications, Phoenix, AZ, USA, 2004, pp. 669-673, doi: 10.1109/PCCC.2004.1395131. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1395131>, accessed February 2021.

Ryan, J. *Teaching Information Security to Engineering Managers*. (2003). <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1264755>, accessed February 2021.

S4 Events (n.d.). <https://s4xevents.com/>, accessed February 2021.

Saper, R., O'Neil, R., d'Apollonia, S.. (1991). *Analysis tools in preparation for Radarsat revisited: Evaluation tools for SAR data exploitation*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=579595>, accessed February 2021.

Sarkar, S., Agrawal, A., Teo, Y., Chang, E. (2018). *VOTNET: HYBRID SIMULATION OF VIRTUAL OPERATIONAL TECHNOLOGY NETWORK FOR CYBERSECURITY ASSESSMENT*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8632410>, accessed February 2021.

Sato, A., Naknishi, H. (2014). *Observation and measurement in disaster areas using industrial use unmanned helicopters*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7017671>, accessed February 2021.

Scali, D. (2016). *Developing a Security Strategy to Cover ICS Assets*. [https://www.fireeye.com/blog/executive-perspective/2016/08/developing\\_a\\_securit.html](https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_securit.html), (2016).

Schneider Electric (n.d.). *Schneider Electric Modicon History*, as referenced by Tim Young at plcdev.com. [http://www.plcdev.com/schneider\\_electric\\_modicon\\_history](http://www.plcdev.com/schneider_electric_modicon_history), accessed February 2021.

Schou, C., Frost, J. *Comprehensive Information Assurance Dictionary*, 1988.

Schou, C., Frost, J., Wingert, N., Larsen, J., LaFond, H., Munson, E. (1989). *Integrating Information Security* from Simplot Decision Support Center Report 162.

Schou, C., Maconachy, W., Frost, J. (1993). *Developing Awareness, Training and Education: A Cost Effective Tool for Maintaining System Integrity*, In Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security (IFIP/Sec '93). North-Holland Publishing Co., NLD, 53–63.

Schulte, D., Colombo, A. (2017). *RAMI 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8216593>, accessed February 2021.

Seijo, O., Fernández, Z., Val, I., López-Fernández, J. (2018). *SHARP: Towards the Integration of Time-Sensitive Communications in Legacy LAN/WLAN*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8644124>, accessed February 2021.

Shippmann, J., Ash, R., Battista, M., Carr, L., Eyde, L., Hesketh, B., Kehoe, J., Pearlman, K., & Prien, E. (2000). *The practice of competency modeling*. PERSONNEL PSYCHOLOGY, 53(3), 703–740.

Sitnikova E., Foo E., Vaughn R.B. (2013). *The Power of Hands-On Exercises in SCADA Cyber Security Education*, in: Dodge R.C., Fitcher L. (eds) Information Assurance and Security Education and Training. WISE 2013, WISE 2011, WISE 2009. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg.

Sitnikova, E., Foo, E., Vaughn, R. (2013) *The Power of Hands-On Exercises in SCADA Cyber Security Education*, [https://link.springer.com/content/pdf/10.1007%2F978-3-642-39377-8\\_9.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-642-39377-8_9.pdf), accessed February 2021.

SkillsFuture (n.d.) *About SkillsFuture*. <https://www.skillsfuture.gov.sg/AboutSkillsFuture>, accessed February 2020.

SkillsFuture Singapore (2018). *Operational Technology Security Audit Management*. <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 June 2020.

SkillsFuture Singapore (2018). *Operational Technology Security Design*. <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 June 2020.

SkillsFuture Singapore (2018). *Skills Framework for Energy and Power: A guide to occupational skills*. <https://www.skillsfuture.sg/-/media/SkillsFuture/Initiatives/Files/SF-for-Energy-and-Power/Collateral.pdf?la=en>, accessed June 2020.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines, *Journal of Business Research*, Volume 104, Pages 333-339, ISSN 0148-2963. <https://doi.org/10.1016/j.jbusres.2019.07.039>, accessed February 2021.

Sobczak, B. (2019). *The inside story of the world's most dangerous malware*. <https://www.eenews.net/stories/1060123327>, accessed June 2020.

Spafford, E. (2019). *An Anniversary of Continuing Excellence*, 2019. <https://www.cerias.purdue.edu/site/blog/2019/05/>, accessed June 2020.

Spirito, C. (2016). *Cyber norms for civilian nuclear power plants*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7836627>, accessed February 2021.

Stewart, D. W., Shamdasani, P. N. & Rook, D. W. (2007). *Analyzing focus group data*. In *Focus groups* (pp. 109-133). SAGE Publications, Ltd., <https://www.doi.org/10.4135/9781412991841>

Stockholm international summit on Cyber Security in SCADA and Industrial Control Systems (n.d.). <https://cs3sthlm.se/>, accessed February 2021.

Stolovitch, H., Keeps, E. (2011). *Telling Ain't Training*. ASTD Press. ISBN 9781562867010

Stouffer, K., Lightman, S., Pillitteri V., and Abrams, M. (2015). *Guide to Industrial Control Systems Security*. <https://doi.org/10.6028/NIST.SP.800-82r2>, accessed February 2021.

Stout, W. (2018). *Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Networks*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8585632>, accessed February 2021.

Summers, S. (2015). *75 Years of Electronics*. Idaho State University Magazine. <https://issuu.com/idahostateu/docs/isumag-fall15>, accessed February, 2021.

Sun, C., Guo, K., Xu, Z., Ma, J., Hu, D. (2019). *Design and Development of Modbus/MQTT Gateway for Industrial IoT Cloud Applications Using Raspberry Pi*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8997492>, accessed February 2021.

Sunzi, and Wutzu, (sixth century BC). *The Book of War: The Military Classic of the Far East*, Translated by Everard Ferguson Calthrop. <https://www.gutenberg.org/files/44024/44024-h/44024-h.htm>, accessed February 2021.

Tajitsu, N., (2017). *Honda halts Japan car plant after WannaCry virus hits computer network*. <https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI>, accessed February 2021.

Tam, K., Jones, K. (2019). *Factors Affecting Cyber Risk in Maritime*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8899382>, accessed February 2021.

- Tam, K., Jones, K. (2019). *Forensic Readiness within the Maritime Sector*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8899642>, accessed February 2021.
- Tanaka, R. (1984). *30/20-GHz domestic satellite communication system in the public communication network of Japan: Design and operation*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1457328>, accessed February 2021.
- Taylor, J., Sharif, H. (2017). *Enhancing integrity of modbus TCP through covert channels*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8270454>, accessed February 2021.
- Thubert, P., Palattella, M, Engel, T. (2015). *6TiSCH centralized scheduling: When SDN meet IoT*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7390418>, accessed February 2021.
- Tran, T. (2016). *A private machine-cloud architecture and self-reliant controllers for operational technology systems*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7822458>, accessed February 2021.
- Tran, T. (2019). *Replacement Controller for IoT-Enabled Dependable Control Systems*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9074603>, accessed February 2021.
- Transparency Market Research (2019). *Industrial Automation Market to Reach US\$352.02 Bn by 2024, due to Increased Manufacture and Low Labour Cost, Noted TMR*. Retrieved from <https://www.prnewswire.com/news-releases/industrial-automation-market-to-reach-us352-02-bn-by-2024--due-to-increased-manufacture-and-low-labour-cost-noted-tmr-300809825.html>, accessed February 2021.
- Trump, D. (2017). *Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. <https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>, accessed February 2021.
- Trump, D. (2020). *Executive Order 13920 – Securing the United States Bulk-Power System*. <https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system>, accessed February 2021.
- Tu, H., Xia, Y., Tse, C., Chen, X. (2020). *A Hybrid Cyber Attack Model for Cyber-Physical Power Systems*, in IEEE Access, vol. 8, pp. 114876-114883, doi: 10.1109/ACCESS.2020.3003323.
- U.S. Department of Homeland Security. (2014). *ICS Alert (ICS-ALERT-14-281-01E)*. <https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B>, accessed June 2020.
- U.S. Dept. of Homeland Security. (2012). *ICS Advisory (ICSA-12-018-01B)*. <https://www.us-cert.gov/ics/advisories/ICSA-12-018-01B>, accessed June 2020.
- U.S. Dept. of Homeland Security. (2015). *ICS Advisory (ICSA-15-048-01)*. <https://www.us-cert.gov/ics/advisories/ICSA-15-048-01>, accessed June 2020.
- U.S. Dept. of Homeland Security. (2017) *ICS Advisory (ICSA-17-278-01A)*. <https://www.us-cert.gov/ics/advisories/ICSA-17-278-01A/>, accessed June 2020.

U.S. Dept. of Homeland Security. (2018). *ICS Advisory (ICSA-18-352-02)*. <https://www.us-cert.gov/ics/advisories/ICSA-18-352-02>, accessed June 2020.

Van de Ven, A., Delbecq, A. (1974). *The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes*. *Academy of Management Journal*, 17(4), 605–621. <https://doi-org.libpublic3.library.isu.edu/10.2307/255641>. Accessed June 11, 2020.

Vickers, T. (2019). *Business Acumen (Do You Have It?)* in "The Goods", Kentucky Association of Manufacturers. <https://kam.us.com/wp-content/uploads/2019/07/Goods-Summer2019-Web.pdf>, accessed July 2020.

Weerathunga, P., Cioraca, A. (2016). *The importance of testing Smart Grid IEDs against security vulnerabilities*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7914920>, accessed February 2021.

Whitehead, D., Owens, K. Gammel, D., and Smith J. (2017). *Ukraine cyber-induced power outage: Analysis and practical mitigation strategies*. 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, pp. 1-8. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8090056&isnumber=8089819>, accessed February 2021.

Wilhoit, K. (2015). *A Virus in Your Pipes: The State of SCADA Malware*. [https://www.first.org/resources/papers/conf2015/first\\_2015\\_-\\_wilhoit\\_kyle\\_-\\_malware\\_in\\_your\\_pipes\\_20150630.pdf](https://www.first.org/resources/papers/conf2015/first_2015_-_wilhoit_kyle_-_malware_in_your_pipes_20150630.pdf), accessed June 2020.

Willner, A., Diedrich, C. Younes, R., Hohmann, S., Kraft, A. (2017). *Semantic communication between components for smart factories based on oneM2M*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8247690>, accessed February 2021.

Wu, C., Liu, X., Fu, C., Yang, J., Huang, W., Zhang, J. (2018). *On the Secure and Stable Operational Technology for Multi-DC Asynchronous Power-Sending Grid With High Proportion of Renewable Energy*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8592525>, accessed February 2021.

Xianghua R., Xuefeng, L, Jiqiang, Z., Feng, G. (2012). *Implementation of Fuzzy neural-network genetic algorithm based on MCGS*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6273257>, accessed February 2021.

Yao, F., Keller, A., Ahmad, M., Ahmad, B., Harrison, R., Colombo, A. (2018). *Optimizing the Scheduling of Autonomous Guided Vehicle in a Manufacturing Process*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8471979>, accessed February 2021.

Yardley, T., Uludag, S., Nahrstedt, K., Sauer, P. (2014). *Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application* 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, Madrid, pp. 1-9. <https://ieeexplore-ieee-org.libpublic3.library.isu.edu/document/7044273>, accessed February 2021.

Yi, M., Mueller, H., Yu, L., Chuan, J. (2017). *Benchmarking Cloud-Based SCADA System*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8241099>, accessed February 2021.

Yonemura, K., Komura, R., Sato, J., Hoga, T., Takeichi, Y., Chida, E., Matsuoka, M. (2018). *Effect of security education using KIPS and gamification theory at KOSEN*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8405480>, accessed February 2021.

Yonemura, K., Sato, J., Takeichi, Y., Komura, R., Yajima, K. (2018). *Security Education Using Gamification Theory*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8434432>, accessed February 2021.

Yonemura, K., Yajima, K., Komura, R., Sato, J., Takeichi, Y. (2017). *Practical security education on operational technology using gamification method*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8284420>, accessed February 2021.

Young, T. (n.d.). *PLC Timeline*. [http://www.plcdev.com/plc\\_timeline](http://www.plcdev.com/plc_timeline), accessed February 2021.

Yu, S. (2019). *New Paradigms for the Next Era of Security*. <https://www.rsaconference.com/library/webcast/35-new-paradigms-for-the-next-era-of-security>, accessed March 2021.

Yuan, W., Wei, L., Li, Y., Chi, Y. (2017). *Research on evaluation method for operation economy and technology of regional smart energy grid*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8311207>, accessed February 2021.

Zhang, J., Zhou, Q., Li, Z., Yang, Z. (2015). *A new integrated charging infrastructure analytics service platform and applied research*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7324600>, accessed February 2021.