CERIAS Tech Report 2021-01

Curriculum Guidance Document Industrial Control Systems

by Subia Ansari, Marlo Basil-Camino, Douglas C. Rapp, Isslam Alhasan, Ida Ngambeki, Eugene H. Spafford
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

This material is based upon work supported by the U.S. Department of Homeland Security under Basic Ordering Agreement No. HSHQDC-16-A-B0010. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S Department of Homeland Security.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Curriculum Guidance Document Industrial Control Systems

Deliverable 6.B
Contract: HSHQDC-16-A-B0010/70RCSA20FR0000103

Principal Investigator: Bill Cope, PhD
University of Illinois at Urbana-Champaign

Prepared by:
Purdue University
Subia Ansari, Marlo Basil-Camino, Douglas C. Rapp, Isslam Alhasan,
Ida Ngambeki, Eugene H. Spafford

August 30, 2021

Table of Contents

1. Context for the Scalable National Network of Cybersecurity Institutes Utilizing a Hub and Spoke Model 4

a. Unmet Curriculum Needs in Industrial Control Systems 4

b. Gap in the National Cybersecurity Workforce Pipeline 4

c. Contributing Factors that Exacerbate the Underrepresentation of Targeted Populations in Cybersecurity Education 5

d. Current Landscape of ICSS Curricula Nationwide 6

e. Unmet Needs for Industrial Control Systems Education and Training 7

f. Opportunities to Leverage Available Curricula to Address Gaps 10

g. Pedagogies that Currently Underpin Available Curriculum 11

h. Potential for Shared Curriculum Resources 12

2. Plan for Development of Shareable Curriculum for Industrial Control Systems Security 12

a. Core Concept Area in Industrial Control Systems Security 12

b. Learning Outcomes for ICSS 15

c. Basic ICSS Program Structure 15

d. Mapping to the NICE Framework 17

e. Online vs. In-Person Offerings 19

f. Strategies for Building Partnerships 19

g. Approaches for Work Integrated Learning 20

h. Processes for Recognition of Prior or Concurrent Work-based learning 21

i. ICSS Hands-on Curriculum Model 21

(i) Regional Specialties 52

(ii) Available Curricula 55

(iii) Process to Create Hands-On Curriculum 62

(iv) Assessment Plan 63

(v) Update Curriculum 64

(vi) Creating a Path for Students 65

3. Hub and Spoke Implementation Strategy for Industrial Control Systems Curriculum 67

a. Exemplar Hub and Spoke Models for Education and Training 67

b. Logistics of Hub and Spoke Models in FEMA Region 5 68

c. Common Core Functions for Spoke Schools 69

d. Inclusion Strategies for Diverse Learner Constituencies 69

e. Common Core Functions for Hub Schools 70

f. **Strategies for Curriculum Sharing** ... 71

g. **Strategies for Instructor Professional Development** ... 72

h. **Resources for Schools to Participate** ... 73

i. **Progress and Evaluation Metrics** ... 73

Appendix A4-1: A Sampling of ICS Programs ... 75

Appendix A4-2: Potential Hub and Spoke Locations in FEMA Region 5 ... 80

Appendix A4-3: Sample Descriptions of Work Roles and Their Mapping ... 90

Appendix A4-4: References ... 102

1. Context for the Scalable National Network of Cybersecurity Institutes Utilizing a Hub and Spoke Model

Industrial control systems are used to manage a multitude of computerized systems which interact with the physical world. This curriculum guidance document refers to Industrial Control Systems (ICS) and Industrial Control Systems Security (ICSS) as pertaining to topics encompassing Operational Technology (OT), Industrial Automation, Industrial Processes and their intersection with the elements of Information Technology including software, networking, data systems, and cybersecurity.

a. Unmet Curriculum Needs in Industrial Control Systems

ICSS professionals are needed to secure systems that control critical systems such as the electric grid, manufacturing facilities, pipelines, water treatment plants, drones, and various transportation systems. There is a need for more talent in cybersecurity generally and ICSS specifically. Most companies (77%) consider ICSS a major priority (Kaspersky Lab & PAC, 2018). A survey conducted in 2019 reported that 88% of participants responsible for ICSS at their company were concerned about cyberattacks. Sixty-six percent said that they expect to be victims of an ICS cybersecurity attack that could result in a catastrophic event (Dimensional Research Survey, 2019). ICSS threats increased 2,000% between 2017 and 2020 (IBM Security, 2020). The Colonial Pipeline ransomware cyberattack in May 2021, which endangered the supply of fuel in 17 states across the United States, is one of the more recent examples of the scale of the risk in ICSS. There is an urgent need to train a workface capable of planning for, responding to, and mitigating these attacks.

b. Gap in the National Cybersecurity Workforce Pipeline

The current national education curriculum lacks essential cybersecurity programs, degrees, and a strong foundation for building the role-specific knowledge necessary to meet ICSS workforce requirements (Sharkey, Morin, and Hunter, 2017); there is especially a lack of understanding and expertise in ICSS (Foreman & Heib, 2012). In Information Technology (IT), cybersecurity is strongly emphasized with the occasional integration of OT knowledge. In OT, cybersecurity concerns are mostly ignored altogether. Educational institutions attempting to bridge OT and cybersecurity to create an ICSS curriculum typically focus on theoretical programs rather than hands-on training, direct application, and implementation of ICSS solutions. While theory is an integral part of an education, hands-on experience and training is urgently needed to adequately equip and prepare students with tangible skills for cybersecurity jobs (NICE, 2017). Integrating hands-on learning opportunities directly within the cybersecurity program gives students a chance to apply what they have learned in class to real-world scenarios and environments. There needs to be a comprehensive curriculum that fully integrates control systems and cybersecurity, and which focuses on both theoretical aspects of ICSS and the hands-on training on specific ICSS products.

The proposed national Hub and Spoke network is intended to address this gap: the centralized hubs will have expertise and ability to develop, disseminate, and maintain curricula and hands-on learning environments (both face-to-face and virtual), the profile to attract and maintain partnerships with industry and other partners, and the capacity to perform ongoing research that will be integrated into the curricula. The Hub schools will be geographically distributed and responsible for establishing relationships with the Spoke schools and industry partners to conduct activity across the network. The Spoke schools are expected to provide ICSS education to their students as well as partner with the Hub institutes to adapt the curricula to their particular contexts, participate in and expand the industry partnerships, and support ongoing research.

c. Contributing Factors that Exacerbate the Underrepresentation of Targeted Populations in Cybersecurity Education

In addition to the workforce gap, there is a significant lack of diversity - participation of women and underrepresented groups - in the cybersecurity workforce (U.S. Government Publishing Office, 2017). The representation of women in cybersecurity stands at 11% and that of various minority groups added together at 23%. This lack of representation can be attributed to various factors: stereotypes of what cybersecurity professionals should look like, uneven access to educational opportunities at every educational level, to name a few.

As the U.S population's demographics continue to become more diversified, strategies to recruit and welcome all of society's segments are critical. In the face of the rising need to build a strong workforce and recruit new talent, we need to decrease the ICSS workforce gap. ICSS requires a multidisciplinary approach to solve complex issues. Having a team made up of diverse individuals can improve that team's outcome. Companies with better minority employment records had a 35% greater financial return than the industry median (McKinsey, 2015). This indicates that diverse professional cybersecurity teams are more likely to solve complex tasks than those with similar backgrounds and skills because of the variety of expertise across all team members.

Many factors contribute to the underrepresentation of targeted populations in cybersecurity education generally and ICSS specifically. These include:

1. Lack of resources. Many minority-serving schools (K-12 as well as higher education) do not have the proper resources to keep students interested in technology fields. They've read in books what computers are and how they work but rarely get to use them. Providing underprivileged schools with laptops, computers, and classes to use these technologies will help them pursue careers in technology.
2. Lack of representation. Many students follow the path of those surrounding them, such as mentors, teachers, and family members. Having a mentor with a shared identity and background who has been through similar experiences is valuable to students in developing personal comfort and role-modeling. A mentor who shares a mentee's social identity can engage the student holistically and give support and guidance because this person is considered similar, which helps the student feel recognized when they might otherwise feel ignored. Females and members of underrepresented populations in the cybersecurity profession need to make themselves seen and available to younger generations. Students seeing someone successful with the same background or identity can provide a boost of courage and confidence: it conveys that they can do it too.
3. Lack of awareness and exposure to these fields creates an opportunity gap for minorities and women. Many have never heard of areas in ICSS. These topics need to be introduced to students starting in elementary, middle, and high schools. Cybersecurity should be considered as important as computer or science classes.
4. Cybersecurity exclusivity. Cybersecurity typically revolves around protecting companies, governments, and corporate systems and is seen as the province of computing experts. Involving and including typical people - those not in the ICS field - as part of the discussion and educating the community about the importance of protecting ourselves and our devices at home shows that this is an 'us' issue. It gives the impression that we are working together as a

whole to combat cybersecurity attacks. Conversations, discussions, and community events all help increase typical home users' threat awareness levels. Feeling included and part of the holistic cyber defense plan will allow individuals to be interested in cybersecurity fields.

5. Stereotypes. The cybersecurity field is generally seen as male-dominated. The ICS field is even more stereotypically male having evolved from large industrial plants, which were traditionally the exclusive domain of men. Though the field is evolving, these stereotypes remain.

The Hub and Spoke network can be leveraged to help alleviate ICS education and training gaps for underrepresented populations, including minority, gender diverse, and veteran populations. This can be done in several ways:

1. Students do not continue their educational path or pursue higher education because of the high tuition cost. Providing some type of tuition assistance encourages students to join the field. The Hub and Spoke approach include a diverse range of institutions that can offer different services at different prices. Students have a range of opportunities and can select that which best fits their budget. Support could include scholarship opportunities to encourage new talent to join the industry, tuition reimbursements, and professional certification exam vouchers.
2. Different types of institutions and industry partners provide opportunities for diverse mentors. Having a positive role model and inclusive culture helps promote careers in this field and attract minority talent. Mentors have a significant impact on students in high school and college levels.
3. Multiple types of institutions provide a variety of entry points for students at different skill levels. Many underrepresented students have non-traditional career paths because of economic or other factors. The integration of community college courses, provision of certifications, and other programs would allow these non-traditional students (e.g., veterans) to transition their skills. This could expand the pipeline of diverse, qualified candidates.
4. The implementation of the Hub and Spoke model will raise the profile of ICSS and introduce the notion of the field across multiple institutions. This will help attract a larger population of students as many have not previously heard of the field.
5. The Hub and Spoke model will provide increased access to resources and technologies for institutions that could not otherwise afford them. This will attract and inspire younger students and have an add-on effect of attracting underrepresented minority students.
6. The Hub and Spoke network would allow investment in earlier education to promote ongoing academic success and form lifelong critical thinking skills. Topics related to ICS education can be integrated with Science Technology Engineering Math (STEM) concepts, lessons, and activities. This would result in a broader pool of students most likely to enter the workforce and more accessibility to a broader and more diverse range of students and educators ICSS.
7. The Hub and Spoke network will allow for the integration of schools that have high underserved populations (e.g., rural schools, Minority Serving Institutions).

d. Current Landscape of ICSS Curricula Nationwide

A nationwide review of ICSS programs was carried out to determine the extent of the gap in the academic offerings. There are several programs in ICS nationwide. These programs have various names (e.g., Operational Technology Security, Industrial Control Systems, Industrial Engineering Technology, Automation and Robotics). However, there are a limited number of ICSS programs. This further emphasizes the need for the Hub and Spoke approach. The identified programs fall into the following broad categories: degrees, certificates, and professional certifications. Degrees are multi-year programs offered by an academic institution, such as a university or a community college, that provides its students a plan of study to educate and train them for positions in an ICSS career. Certificates include small groupings of technical courses typically offered by academic institutions either for credit or as non-credit. Oft times, they are used for preparation of professional certifications, which are designed to fill in skills gaps or demonstrate knowledge gained on the job. Professional certifications are primarily geared towards professionals who wish to update their knowledge and skills.

Professional Certifications and Certificates

The following programs in ICSS were identified. These range from a few hours to a year in length (*see Appendix A4-1 for more information):*

- GIAC Global Industrial Cybersecurity Professional
- GIAC Response Industrial Defense
- GIAC Critical Infrastructure Protection
- ISC^2 Cybersecurity in ICS
- Tonex SCADA Security Training
- Tonex ICS Cybersecurity Training
- SANS Graduate Certificate in Industrial Control Systems Security
- CISA Introduction to Control Systems Cybersecurity
- CISA Intermediate Cybersecurity for ICS
- CISA ICS Cybersecurity
- CISA Operational Security for Control Systems
- CISA Differences in Deployment of ICS
- CISA Common IT Components on ICS
- CISA Cybersecurity within ICS & IT Domains
- CISA Attack Methodologies in IT & ICS
- CISA Mapping IT Defense-in-Depth Security Solutions to ICS
- CISA Industrial Control Systems Cybersecurity Landscape for Managers
- ISA Cybersecurity Fundamentals Specialist
- ISA Cybersecurity Risk Assessment Specialist
- ISA Cybersecurity Design Specialist
- ISA Cybersecurity Maintenance Specialist
- Industrial Control System Cybersecurity Institute
- Wilmington University SCADA Cybersecurity Certificate

Degrees

Multiple colleges and universities offer Associates or Bachelor's degrees in Industrial Technology, Industrial Control Systems, Engineering Technology, Industrial Engineering Technology, and Automation, and Instrumentation. However, we were not able to find any that offered more than a single course in cybersecurity, with one exception: a single fully integrated Bachelor's (4-year) degree in ICSS was identified (*see Appendix A4-1 for details about these degrees)* at Idaho State University - Industrial Cybersecurity Engineering Technology

e. Unmet Needs for Industrial Control Systems Education and Training

A survey of Federal Emergency Management Agency (FEMA) Region 5 needs for ICSS education and training was broken into three parts: workforce demand, industry concentration, and potential ICSS satellite school suitability. Several facts/trends were discovered during the survey. First, there are currently no resources available to determine workforce demand specifically for ICSS employees. Second, FEMA Region 5 includes a significant percentage of United States manufacturing. Most potential satellite schools for ICS training are lacking formal education and/or training of at least one of the following areas: engineering, cybersecurity, or industrial control systems. Also of note is that the schools best qualified to be ICSS satellite schools are not necessarily geographically located near advance manufacturing concentrations.

Workforce Demands:

Currently, the most reliable and comprehensive resource for determining cybersecurity workforce needs is the Cyber Seek tool (www.cyberseek.org). This tool was developed with funding from the National Initiative for Cybersecurity Education (NICE), and support from CompTIA and Burning Glass. However, since this tool was developed using the National Institute of Standards and Technology (NIST) Special Publication 800-181, *Workforce Framework for Cybersecurity* (*NICE Framework*), and the NICE Framework does little to identify ICSS skills, occupations, or career pathways, the Cyber Seek data can only be used anecdotally. FEMA Region 5 exhibits a significant deficit in cybersecurity workforce.

FEMA Region 5 Cybersecurity Vacancies from CyberSeek	
Illinois	15,838
Indiana	4,119
Minnesota	7,912
Michigan	7,129
Ohio	10,448
Wisconsin	4,664
	50,110

Table 1: FEMA Region 5 Cybersecurity Openings

Advanced Manufacturing Concentrations:

The Midwest currently produces around 60% of all US manufacturing. Significant manufacturing clusters exist throughout FEMA Region 5 with over one third of the cities within the six states with thriving manufacturing economies. With such a significant advanced manufacturing presence, it is reasonable to assume that the need for skilled ICSS workers would be proportionate to the total employment needs of these manufacturers:

Illinois	• Fourth largest manufacturing state in the nation • 10% of the State's workforce is employed in manufacturing • Over 576,000 employed
Indiana	• Highest concentration of manufacturing jobs in the nation • 2nd largest automotive manufacturer • 20% of the workforce is in advanced manufacturing
Minnesota	• The largest share of the state's Gross Domestic Product (GDP) (14%) with more than $52.7 billion • Nearly 324,000 employees • 8,200 manufacturers
Michigan	• 5th largest advanced manufacturing workforce in the country • 66,000 workers employed in advanced manufacturing industries in 2019 • 3,000 businesses serving the defense industrial base
Ohio	• 3rd largest manufacturing workforce in the U.S. • Nearly 700,000 skilled individuals • Ohio's total output from manufacturing was $112 billion in 2018
Wisconsin	• Over $64 million in GDP • 99,000 employees • Over 3% of all new hires are in manufacturing

Table 2: FEMA Region 5 manufacturing overview

Potential Satellite School Unmet Education/Training Programs:
Of the 30 potential ICSS satellite schools in Region 5 that were surveyed, none of them possessed a formal ICSS educational/training program. These schools were reviewed for formal programs in engineering, cybersecurity, and industrial control systems and identified for having strong engineering programs. Most of these schools had formal degree programs in cybersecurity/information security. However, the degree concentrations were varied (e.g., cybersecurity management, forensics, and network security). Schools were also reviewed for their proximity to relevant industry, military bases and critical infrastructure (*See Appendix A4-2 for details).*

A mapping of existing courses revealed major themes that cover the foundational content areas of Supervisory Control and Data Acquisition (SCADA) systems and their architecture, programmable logic control (PLC) devices, and basic cryptography concepts, while giving emphasis to employability skills (e.g., technical writing, project management, organizational communication). These themes reflect opportunities where existing curricula can be leveraged. However, upon consultation with industry professionals, we suggest the following content areas be included to cover the gaps that currently exist in the available curricula:

Major Area	Topic Area	Topic
General Background Concepts	**Safety**	**Electrical Safety**
		Personal protective equipment
		Safety/hazards assessment
		Safety instrumented systems
		Lock-out tag-out
		Safe work procedures
	Industrial operations and processes	Industry sectors
		Professional roles and responsibilities in industrial environments
		Engineering diagrams
		Process types
		Plant life cycle
Technical Concepts	Instrumentation and controls	Sensing elements
		Control paradigms
		Process variables
		Alarms
		Engineering laptops/workstation
	Equipment under control	Motors/generators, pumps, valves, relays, generators, transformers, breakers, variable frequency drives

Table 3: Missing Topics in ICSS

f. Opportunities to Leverage Available Curricula to Address Gaps

A survey of existing national educational programs and available curricula in ICSS revealed a limited number focusing on ICS. The survey revealed that curriculum either focused on cybersecurity (with a gap in ICS/OT concepts), or on OT (with a gap in cybersecurity concepts). This gap highlights the need to develop a curriculum that focuses on concepts relevant to ICSS. Opportunities that exist to leverage available curricula are limited and would require laying emphasis on cybersecurity topics relevant to ICSS from programs that focus exclusively on cybersecurity and merging these concepts with fundamentals of ICS and OT concepts.

There are a few samples of existing curricula in ICSS that may be leveraged as a basis to build on other existing courses. There are existing examples of curricula that may be used as a basis to support some of these courses. Section 2 next, provides an outline of what curricula in ICSS could contain and goes into greater detail on existing resources. These include:

1. Open-Source Projects: There are several open-source projects, most federally funded but developed by faculty, which lay out examples of ICSS curricula. One example is the SEED Security Labs: This project provides a set of labs and workshops that can be used to supplement ICSS learning, https://seedsecuritylabs.org/labs.html
2. Digital Repositories: There are a few repositories for educational material (e.g., the CLARK digital library, funded by the National Security Agency (NSA) and maintained by faculty and students at Towson University). This online repository of expert reviewed learning materials range from learning modules (e.g., lecture slides, hands-on lab exercises) to full courses, https://www.clark.center/home:
    a. Cybersecurity of Industrial Control Systems
    b. Industrial Control Systems Fundamentals and Security
    c. Security in Cyber-Physical Systems
    d. Introduction to Industrial Control Systems
    e. Industrial Network Protocols
    f. Securing Industrial Networks
    g. Introduction to ICS
    h. Overview of ICS Components and Processes
    i. Attacks on Industrial Control Networks
    j. Monitoring Industrial Control Networks
    k. Industrial Malware and Attack Cases
    l. Introduction to SCADA
    m. Secure Management of Control Systems
    n. SCADA Control System Networking
3. Industrial Cybersecurity Community of Practice (ICSCOP). This is a national group that brings together professionals from government, industry, and academia focused on ICSS and ICSS education. There are several working groups: one devoted to developing standards in ICSS and another developing a repository of ICSS educational materials and resources, https://inl.gov/icscop

g. Pedagogies that Currently Underpin Available Curriculum

Multiple pedagogical methods currently underpin the available curriculum. However, most of these focus on theoretical knowledge taught in a lecture-based format. Hands-on education and training are generally limited to a small fraction of the curriculum. The approach to teaching ICSS also tends to be siloed depending on the hosting department. For example, if the program is in a College of Engineering or Technology, the focus is on OT with elements of security tacked on. The opposite is true of Computer Science or IT departments where the focus is on cybersecurity with only a handful of courses dedicated to OT. A comprehensive program would have to integrate the two fields more effectively.

h. Potential for Shared Curriculum Resources

There is a great deal of potential to leverage shared curriculum resources to improve ICSS education. Given the current state of ICSS education nationally, a Hub and Spoke approach is necessary to significantly alter the educational landscape. There is a recognized need for more education in ICSS. However, a national survey of the ICSS educational programs found very few. Most focus exclusively on cybersecurity with minor elements of ICS or focus on OT with minor elements of cybersecurity. A full program in ICSS would require large investments to develop lab resources, to design the integrated program, to hire or develop faculty to teach the additional courses, and to recruit suitable students. This is especially true because ICSS requires a great deal of hands-on learning in specially designed laboratory spaces, with custom-built hardware, that utilizes work-integrated training. Most institutions would be reluctant to make this investment. However, the Hub and Spoke network could help address many of these concerns with a lower overall investment. The design of courses as well as the expertise needed to teach them can be sourced from multiple institutions alleviating the need for one institution bearing the full burden. Similarly, lab equipment could be shared across institutions alleviating the cost to any one school. The Hub and Spoke project also creates a natural pipeline which aids in recruitment of students. Lastly, this model also reduces the need for individual institutions to develop their own relationships with strategic partners to support work-integrated learning.

2. Plan for Development of Shareable Curriculum for Industrial Control Systems Security

The Hub and Spoke participating schools will oversee the development of a shareable curriculum for ICSS.

a. Core Concept Area in Industrial Control Systems Security

Course Content

Deciding on a set of concepts or content areas to be covered is one of the first tasks of any curriculum development effort. Sources of content can include accepted textbooks or existing standards. There are several standards that cover some of what should be in an ICSS educational program: the NICE Framework, the NSA Centers of Academic Excellence in Cybersecurity (NCAE-C) Knowledge Units, and the Association for Computing Machinery (ACM)/ Institute of Electrical and Electronics Engineers Computer Society (IEEE CS)/Association for Information Systems Special Interest Group on Security (AIS SIGSEC)/International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) Joint Task Force Cybersecurity Curriculum Guidance Document. These were all consulted to determine the content areas to be covered by an ICSS curriculum.

However, none of these were written with the full integration of ICS and cybersecurity in mind. We therefore used these as a basis to outline the major concepts in ICSS and then conducted a Delphi study to further refine the content area. The Delphi technique seeks to obtain consensus on the opinions of experts, termed *panel members*, through iterative structured questioning. As part of the process, the responses from each round are fed back in summarized form to the participants who are then given an opportunity to respond again to the emerging data. The Delphi is therefore an iterative multi-stage process designed to combine individual opinions into group consensus. In this case we consulted 25 experts from academia, industry, and government in three rounds. Most of these individuals were members of a national Community of Practice in ICSS mentioned previously (https://inl.gov/icscop).

The result was the concept map of ICSS in Figure 1 below. As the field continues to evolve, this concept map will be updated to reflect new needs, technologies, and challenges.

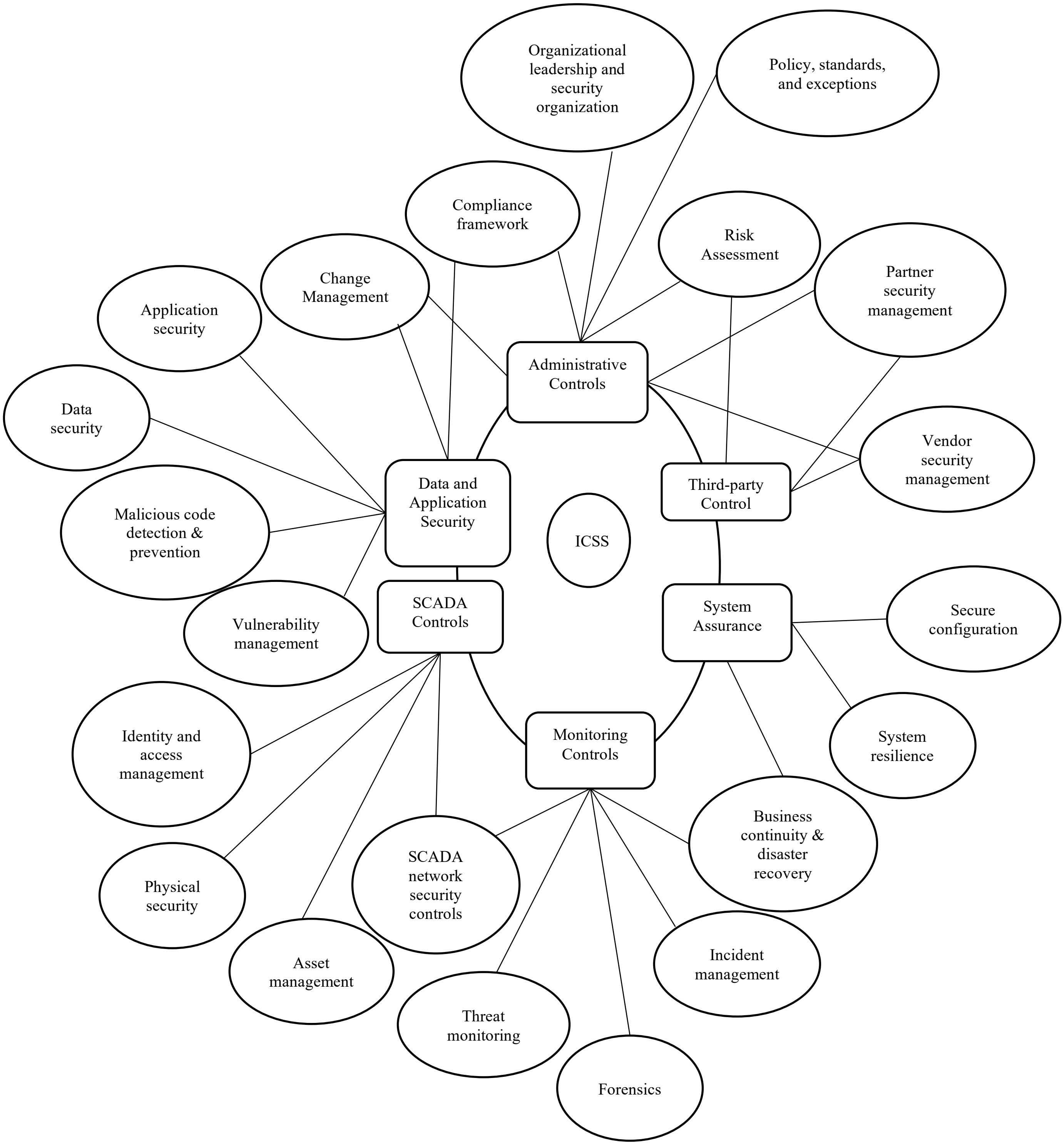


Figure 1: ICS Concept Map

A combined review of learning outcomes and concept areas above yielded the following three major areas:

1. General Background Concepts
2. Technical Concepts
3. Workforce/Employability Skills

Major Area	Topic Area	Topic
General Background Concepts	Technical Concepts	Workforce/Employability Skills
		College-level algebra
		Calculus
		Statistics
		Boolean Algebra
	Safety	Common failure modes for equipment under control
		OSHA safety rules
Technical Concepts	Computer Fundamentals	Fundamentals of computer programming
		Writing secure code
		Programming languages and type-safety
		Robust Programming
		Secure Programming
		Enterprise Linux
		Organizational Security
	Electrical Systems	SCADA Systems
		Embedded Systems
		Security of components
		Cyber-physical systems
	Instrumentation and Controls	Control devices
		Programmable control devices
		Programming methods
		Data acquisition
		Supervisory control
	IT Security	Incident Response and Forensics
		Vulnerability and Threat Management
		Security Configuration and Resilience
		Data and Application Security
	Technical Communications	Basic cryptography
		Connection security

Major Area	Topic Area	Topic
Workforce/Soft skills	Technical Writing	
	Project Management	
	Organizational Communication	

Table 4: Major Topics in ICSS

b. Learning Outcomes for ICSS

Another essential component in creating educational and training materials is the identification of desired outcomes. The purpose of any educational undertaking is to create an experience that results in a cognitive change in students. For most, this will take the form of the new knowledge and skills required for their work roles. Based on the content areas identified above in Figure 1, we developed the following learning outcomes to articulate what students graduating from programs in ICSS should know and be able to do:

1. Maintain ICS devices and attendant networks
2. Identify and mitigate evolving ICS security threats
3. Assess evolving risks to ICS systems
4. Maintain high standards of safety in ICS environments
5. Implement and maintain ICSS software
6. Communicate with OT and IT personnel

c. Basic ICSS Program Structure

The purpose of this curriculum guidance document is to make recommendations for the creation of ICSS programs. These programs will differ in both their length and the level of expertise of the learners they serve. Therefore, we have attempted to create a basic program structure that can be adapted for multiple levels of expertise and program length. This program structure addresses ICSS in five basic areas. This differs from the topic areas outlined above in Figure 1 because it groups these topics into units that make more sense for students when constructing a learning experience/mental model of the discipline. Having reviewed the major areas and major concepts, and having discussed the way that expertise in ICSS develops with subject matter experts in the field – we propose the following five knowledge areas:

1. Risk
2. Governance/Compliance
3. Information Security
4. ICS
5. Electrical Engineering

Programs in ICSS would therefore be structured with knowledge units that are clustered in these five knowledge areas, that address the three major areas articulated above in Table 4 (General Background Concepts, Technical Concepts, Workforce/Employability Skills), and that cover most of the elements of the concept map depending on the desired level of expertise.

Program Structure for ICSS

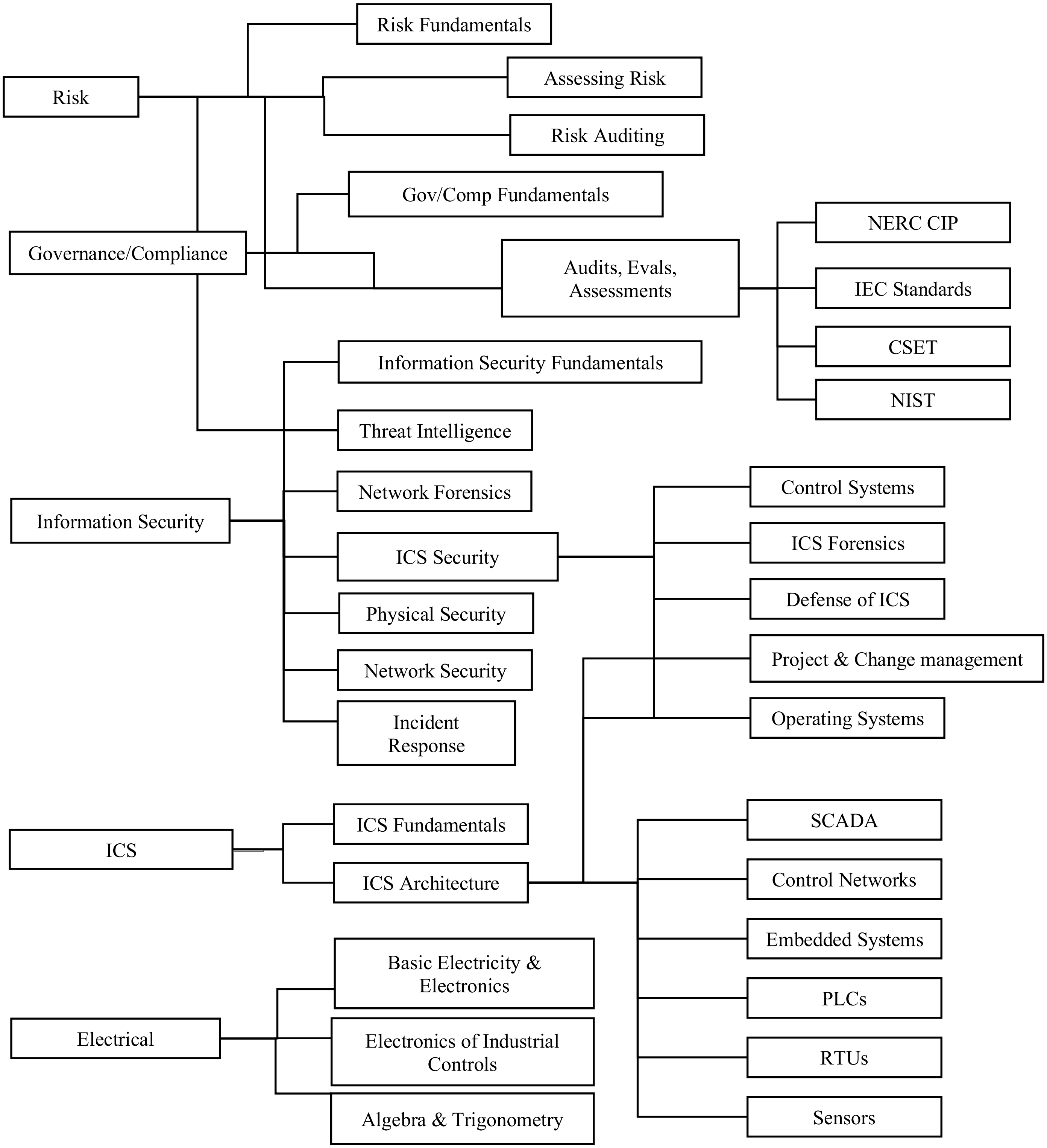


Figure 2: Program Structure for ICSS

The manner in which these courses are structured and stacked can vary among programs. Figure 3 shows a sample of the structure of a one-year program in ICS.

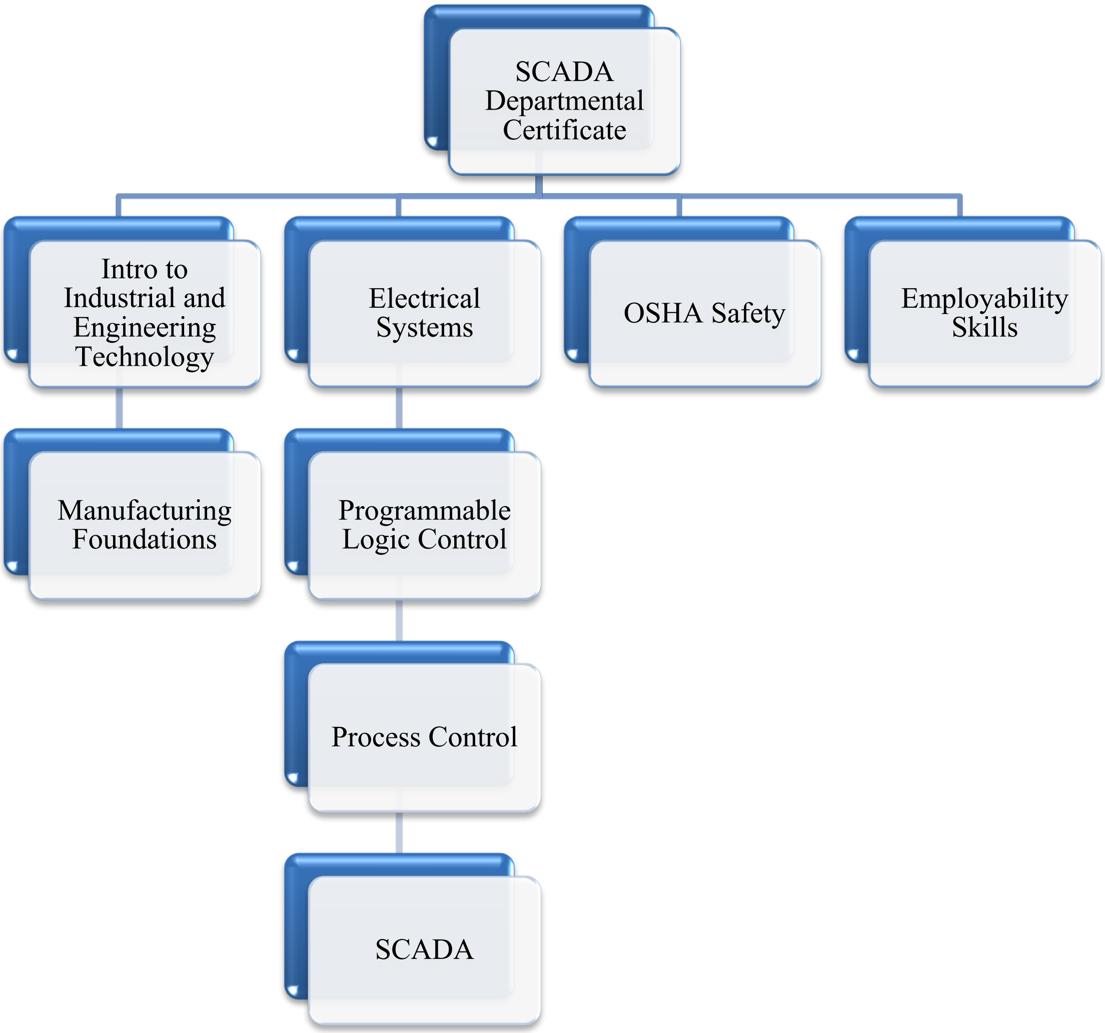

SCADA Departmental Certificate
Intro to Industrial and Engineering Technology
Electrical Systems
OSHA Safety
Employability Skills
Manufacturing Foundations
Programmable Logic Control
Process Control
SCADA

Figure 3: Sample 1-Year Program

d. Mapping to the NICE Framework

The NICE Framework (SP 800-181) was developed as a common reference for describing cybersecurity work roles and the knowledge, skills, and abilities necessary to fulfill those work roles. It is a useful reference to provide a common language to discuss cybersecurity roles. It is therefore a useful exercise to map the anatomy of ICSS to the NICE Framework. However, the NICE Framework does not mention ICS and contains only brief references to SCADA systems. Three Knowledge, Skills, and Abilities (KSAs) are identified as being particular to ICSes:

ID	Description

T0608	Conduct analysis of physical and logical digital technologies to identify potential avenues of access (e.g., wireless, SCADA, telecom)
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)
K0437	Knowledge of general supervisory control and data acquisition (SCADA) system components

Table 5: KSAs related to SCADA systems

A further investigation of the KSAs yields a set of cross-cutting knowledge areas that broadly map to an ICS work environment:

ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g. circuit boards, processors, chips, and computer hardware)
K0055	Knowledge of microprocessors
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
K0437	Knowledge of general supervisory control and data acquisition (SCADA) system components
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations

Table 6: Cross-cutting knowledge mapping to ICS work environments

The NICE Framework was developed within an IT/Computer Science/cybersecurity perspective. It therefore excludes multiple elements that are essential to ICS/ICSS. Those areas missing include elements that interact with and control the physical world, considerations of safety, instrumentation, and equipment. It should be noted however, that the NICE Program Office is conducting a workshop on August 24, 2021, bringing together subject matter experts from industry, academia, and government, to start addressing the lack of ICS and ICSS related work roles and KSAs in the NICE Framework.

Work Roles

The NICE Framework outlines work roles relevant to cybersecurity. However, again, none of these are specific to ICSS. Rather than depend on the NICE Framework, we conducted a search of job postings specific to ICSS. These were condensed according to the work tasks elaborated into a key set of ICSS jobs. They include:

- OT/ICS Cybersecurity Manager
- Industrial Cybersecurity Engineer
- Industrial Cybersecurity Technician
- Industrial Cybersecurity Analyst
- Industrial Automation and Control Systems Cybersecurity Specialist
- Senior Associate IT/OT Cybersecurity
- ICS Network Security Engineer
- Senior Industrial Control System Security Engineer
- SCADA Cybersecurity Solutions Architect
- Industrial Cybersecurity Researcher
- ICS/OT Consultant

See Appendix A4-3 for a detailed description of these ICSS jobs.

e. Online vs. In-Person Offerings

One of the strengths of the Hub and Spoke model is the opportunity to leverage online or hybrid learning delivery models. This would allow students to take courses from instructors at multiple institutions within the Hub and Spoke system. These courses are generally those without lab requirements. Specifically, the majority of the general education requirements (e.g., written and oral communication as well as many introductory courses (introduction to cybersecurity, cyber-physical systems, and governance/risk management)) might be taken remotely or from another participating school that is part of the Hub and Spoke network. However, no ICSS program can be fully online as students must have the opportunity to interact physically with exemplars of the equipment they will be working on in the field. Therefore, advanced courses in the areas of physical security, ICS systems, and electrical systems require in-person learning. See Tables 7-9 below for details on which courses would be most adaptable to online or hybrid delivery approaches.

f. Strategies for Building Partnerships

The success of the ICSS Hub and Spoke project partially depends on the development of strategic partnerships. These partnerships among participating Hub and Spoke schools are essential to the construction and success of this undertaking. Partnerships with industry and government are also essential for several reasons:

- These partnerships provide a pipeline for outgoing students to find gainful employment.
- These partnerships provide data and testbeds for research in ICSS.
- These partnerships provide mechanisms for hands-on learning for the students through visiting national labs e.g., INL and completing internships.

- These partnerships provide additional funding for programs from companies willing to invest in ICSS education and research.
- These partnerships provide expertise (e.g., guest lectures) from working professionals.
- These partnerships provide students (e.g., incumbent workers) looking to upskill.
- These partnerships provide input for the evolution of the educational materials to address real-world needs.

Developing these partnerships is a long-term investment in the success of the Hub and Spoke project. There are several considerations when building partnerships:

- *Alignment:* Identify locations with individuals interested in ICSS education as partners. For example, Idaho National Labs would be a likely partner in such an effort.
- *Effective Communication*: It is important for the success of these partnerships that all parties know what is expected of each other. Clear communication channels, regular communication, and available contact point persons are necessary.
- *Shared Governance*: To maintain the relationship, there must be a clear structure, and a reasonable, well understood decision-making process that is accessible to all.
- *Clear incentives*: The benefits to all parties (e.g., access to resources, name prestige, access to new graduates) must be clear to all.

One mechanism that has worked well in a variety of previous projects is the integrated academic center. A Hub school could be the home of a defined center for both education and research. It would have Spoke schools as affiliates, and organizations external to academia as partners. The center (Hub) would provide both incentives to partners and resources to Spoke schools. Examples of incentives include:

- *Preferential access to students for purposes of recruiting:* Hub schools could provide "match-making" for internships, host job fairs for industry partners, and otherwise increase the likelihood of partners hiring appropriate and diverse employees.
- *Preferential access for research:* At the upper end of the educational spectrum is advanced research with student participation. This education helps train students to take on research roles in industry and government. It also addresses difficult problems with novel solutions. By offering partners preferential access to this research - in the form of reduced licensing, advanced access to prototypes, and ability to influence/support the research agenda - partnership provides a key competitive advantage.
- *Tax credits for partners:* Contributions to non-profit educational institutions already provide potential tax benefits to industry. If it is viewed as a national priority, new tax credits may be enacted at state and federal levels for commercial partners of designated Hub schools.
- *Associational prestige for partners:* Partners of these ICSS centers will be seen by others in industry and government as playing an important role in the field.
- *Access to shared grants, Cooperative Research and Development Agreements, Small Business Technology Transfer programs, etc.:* Specific funding opportunities for research and development may be available for partners working with participating Hub universities.

g. Approaches for Work Integrated Learning

Work-integrated learning has the benefit of providing students with hands-on experiences, providing funding to support students' education, and helping students build their resumes. There are several approaches for work integrated learning:

- *Projects*: Projects are short term commitments to work collaboratively on a specific set of goals to achieve a fixed task. They are usually unpaid and serve purely as a learning experience for the student.
- *Internships*: Internships are commitments usually lasting one term (e.g., one summer or one semester). They are designed to expose the student to the work environment. Students take on a variety of tasks suited to their current level of education and professional experience and learn primarily by observation. They may be paid, unpaid, or for credit.
- *Cooperatives*: Cooperatives are longer-term commitments usually lasting a year. They are designed to expose the student to the work environment, but the student usually takes on a working role at the company. Students are usually placed through their institution and work for credit. These are sometimes referred to as *work-study* opportunities.
- *Apprenticeships*: These are loner-term commitments where the student is hired by the company, which then generally pays for the student to complete the educational and training program. Students are then expected to continue with the company when they complete the requirements of the program. Generally, these are paid positions. Government agencies and labs may offer these as well as companies.

h. Processes for Recognition of Prior or Concurrent Work-based learning

To ensure student success, there should be processes in place to recognize their prior expertise and work experiences, in addition to work-based learning. This can be achieved through several mechanisms:

- *Testing*: Students can receive credit for prior expertise by completing a test or testing out of certain classes. If students successfully complete the test provided, they are then exempted from certain courses or/and receive credit for them.
- *Credits for hours completed*: For students participating in work integrated learning, the completion of a designated number of hours would be considered equivalent to a certain percentage of a grade or a fixed number of credits.
- *Certifications*: Students who successfully pass certain professional certification exams may be exempted from or receive credit for certain courses. Prior degrees and certificates earned in military service should be included in this category.

i. ICSS Hands-on Curriculum Model

To assist with the development of ICSS programs, we provide specific examples for four different program levels:

- Certificates in ICSS
- Associate's degrees in ICSS
- Bachelor's degrees in ICSS
- Master's degrees in ICSS

These examples can be adopted and adapted appropriately to the desired course level. Each example provides an overview of the course structure and details of the component courses.

A. Curriculum Requirements for a Certificate in ICSS

Curriculum Overview

- Required units: 21 units
- Typical timeframe to complete a certificate: 1 year
- Average units per semester: 10-15 units
- General Education requirements: 0 units (less than 50%)
- Major Requirements: 21 units
- Core Courses (fixed): 21 units
- Students may transfer courses/units to an associate's or bachelor's degree before or after all 21 units
  No prerequisites are required if these courses are taught at an introductory level

Course Title	Duration (credit hrs.)	Delivery Method	Lab (Y/N)	NICE Specialty Areas
Algebra & Trigonometry	3	Online/Hybrid/In-person	N	N/A
Electricity and Electronics	3+2 Lab	In-person/Hybrid	N	N/A
Introduction to Cybersecurity	3	Online/Hybrid/In-person	Y	Cybersecurity Management
Industrial Control Systems (ICS) Foundations	3+2 Lab	In-person	Y	Network Services System Administration System Analysis
Cybersecurity for Industrial Control Systems	3+2 Lab	In-person/Hybrid	Y	Cyber Defense Analysis Incident Response Customer Service and Technical Support Exploitation Analysis Vulnerability Assessment and Management

Table 7: Summary of courses for a certificate in ICSS

Course: Algebra & Trigonometry

***Delivery Method**:* Online/Hybrid/In-person

***Description**:* In this course students will learn and explore the concepts of algebra and trigonometry. Students explore the connections within mathematics through critical thinking. Students will cover advanced algebraic concepts with a focus on polynomials, logarithms, functions, rational expressions and equations, rational exponents and radicals, statistics, sequences and series, and trigonometry. Students will also explore different mathematical concepts, theorems, and functions. Through the study of advanced algebra integrated with geometry, students will develop and refine problem solving skills with trigonometry. Learner will use multiple methods to solve problems efficiently by connecting different concepts. Students will learn critical thinking and how to develop a logical and coherent argument.

***Topics**:* Real numbers and polynomials, fractional equations, proportions and linear equations, exponents and radicals, trigonometric functions, radians, solutions of triangles, trig functions graphs, vectors, and basic identities.

***Assessment Methods**:* Multiple choice exams, examinations involving short and long answer responses.

***Learning Outcomes**:*

- Graph and extract information from graphs of polynomial, rational, exponential and logarithmic, and trigonometric functions
- Use symmetry and translation of axes, graph polynomial functions, use graphs to approximate irrational roots
- Understand the concept of a matrix, solve systems of linear and non-linear equations and inequalities using techniques of graphing, Cramer's Rule, determinants, matrices
- Use calculators or tables to find trigonometric values for any angle. Make radian conversions
- Solve any triangle, using the laws of sine and or cosine and find the components of vectors
- Solve applied problems in which several forces are acting at a point are in equilibrium
- Conduct mathematical operations with complex numbers. Find complex solutions or equations
- Identify, use notation, and calculate sums and terms or arithmetic and geometric sequences
- Represent situations and solve problems using algebraic equations and inequalities

***Prerequisites**:* Basic Algebra

NICE Mapping: N/A

***Lab**:* N/A

Course: Electricity and Electronics

Delivery Method: Hybrid/In-person

Description: The electricity and electronics course provide foundational information on the basic principles of electricity. The course introduces electron theory, electrons in motion, static electricity, alternating current (AC), and direct current (DC) electricity, and magnetism. Students learn methods of measuring voltage, current, and resistance, and associated numerical concepts. They also learn electrostatics, basic circuit concepts, circuit components and conductors, Ohm's Law, practical circuits, insulators, electromagnetism, resistors, capacitors, electrical measurements, and troubleshooting.

Topics: Basic electrical laws, conductors and insulators, electromotive force and voltage, current flow, resistance, series, parallel, and resistive circuits, sine waves, frequency, period, and wavelength, calculating sine wave voltage and current values, AC phase relationships, calculating resistance in AC circuits, inductance in AC circuits, capacitance in AC circuits, calculating power in AC circuits, and electrical safety precautions.

Assessment Methods: Multiple choice exams, examinations involving short and long answer responses.

Learning Outcomes:

- Define capacitive reactance
- Calculate the capacitive reactance for an AC circuit
- Define impedance
- Describe the relationship between true, apparent, and reactive power
- Explain voltage, current, and resistance
- Explain Kirchhoff's Current and Voltage Law
- Calculate equivalent resistance of series and parallel resistive circuits
- Define power factor, true power, and apparent power
- Calculate DC circuit parameters (Ohm's Law, Kirchhoff's current law, and Kirchhoff's Voltage Law)
- Identify the construction and operation of a simple AC generator
- Define inductive reactance
- Calculate the inductive reactance of a simple AC circuit
- Describe the characteristics of capacitors
- Describe the characteristics of inductors

Prerequisites: None

NICE Mapping: N/A

Lab: Students will design and build AC and DC series, parallel, and combination circuits. Students will also build and test transistor circuits, semiconductor circuits, and power supplies.

Course: Introduction to Cybersecurity

Delivery Method: Online/Hybrid/In-person

Description*:* This course offers in-depth coverage of the current risks and threats to an organization's data, combined with a structured way of addressing the safeguarding of these critical electronic assets. The course provides a foundation for those new to Information Security as well as those responsible for protecting network services, devices, traffic, and data. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields.

Topics*:* Governance and policy; network security and architecture; concepts of least privilege, separation of risk, defense in depth and secrecy; The CIA triad; security tools and security hardening techniques; identifying system and application security vulnerabilities; incident response. Global security standards, practices, and regulations (e.g., IEC/ISA 62443, NIST 800-8241, ISO 27000 standards), Risk management (e.g., PHA/HAZOP usage, risk acceptance, risk/mitigation plan), Security lifecycle management (e.g., acquisition and selling of an asset, procurement, commissioning [e.g., secure deployments], maintenance, decommissioning), Security policies and procedures development (e.g., exceptions, exemptions, requirements

***Assessment Methods**:* Multiple choice exams, examinations involving short and long answer responses.

***Learning Outcomes**:*

- Effectively communicate information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege (PLP)
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) triad
- Create effective and secure passwords
- Understand basic cryptography
- Finding and configuring network settings using Windows
- Understand and become familiar with security technologies
- Understand the wireless technologies
- Identify common cybersecurity attacks and attack vectors
- Understand basic browser security and privacy
- Explain system hardening and system patching
- Understand virtual machines and cloud computing
- Understand defense-in-depth and other defense strategies
- Understanding information classification, mapping, and data loss prevention
- Detect and react to cybersecurity threats
- Understand incident response
- Communicate cybersecurity issues and topics effectively to management and subordinates

***Prerequisites**:* None.

NICE Mapping: N/A

***Lab**:* N/A

Course: Industrial Control Systems (ICS) Foundations

Delivery Method: In-person

***Description**:* Students will gain a solid foundation of Industrial Control Systems and its components, understanding the integration of hardware and software with network connectivity, Supervisory Control and Data Acquisition (SCADA) systems, IT/OT devices, common ICS threats.
***Topics**:* local area networks (LANs); operator interfaces; MTU/HMI; security; data historian/back-end systems; safety, reliability, and redundancy; RTUs, PLCs and industrial computers; and planning

and managing SCADA projects. Designing, planning, and implementing industrial control systems networks; RTU and PLC configuration, analyzing security issues within ICS.

Assessment Methods*:* Multiple choice exams, examinations involving short and long answer responses.

Learning Outcomes:

- Describe industrial control systems to include basic devices and controls
- Understand safety in industrial control systems
- Understand Programmable Logic Controller (PLC) history and applications
- Demonstrate basic PLC skills
- Demonstrate programming fundamentals for coils, contacts, timers and counters
- Understand input/output modules and wiring
- Demonstrate arithmetic and advanced ICS instructions
- Identify Types of Industrial Sensors
- Understand types, uses and applications of robotics
- Classify and describe the fundamentals of process control
- Install, maintain, and troubleshoot PLCs

Prerequisites: Algebra & Trigonometry, Electricity and Electronics

NICE Mapping: All Source Analysis, Exploitation Analysis, Threat Analysis, Software Development, Risk Management, Network Services, System Administration, System Analysis

ICS Foundations Lab: Student will demonstrate the installing and wiring PLCs. Additionally, they will program, operate, test, and troubleshoot PLCs. Student will learn to integrate PLCs with other industrial devices such as programmable logic controllers with sensors, switches, pneumatics, and motors. Students will learn to set up, configure and troubleshoot numerous types of industrial sensors.

Course: Cybersecurity for Industrial Control Systems

Delivery Method: Hybrid/In-person

Description: Students will learn the basics of Industrial Control Systems (ICS) cybersecurity. They will compare and analyze both IT and ICS architectures and determine how they operate in relation to each other. They will learn the basics of risk management, risk assessment, risk reduction controls and strategies, and residual risk within the ICS domain. Student will earn security vulnerabilities within ICS environments and how to protect them using offensive and defensive methods. They will learn threats to their systems through threat collection and analysis, methods and vectors of attacks, intrusion detection, and incident response.

Topics: Communication medium (e.g., VSAT, RF, cell, microwave), external network communications (e.g., access points into ICS/SCADA systems, VPNs, vendor/third party access points, mobile devices), field device architecture (e.g., relays, PLC, switch, process unit), industrial protocols (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC), network protocols (e.g., DNS, DHCP, TCP/IP, UDP), network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs), wireless security (e.g., Wi-Fi, wireless sensors, wireless gateways, controllers), defense in depth (e.g., layered defines, IDS sensor placement, security system architecture, virtualization)

***Assessment Methods**:* Multiple choice exams, examinations involving short and long answer responses.

***Learning Outcomes**:*

- Understand active defense and incident response for ICS.
- Understand NERC critical infrastructure protection (CIP) policies and procedures.
- List strategies for the most recent version of NERC CIP.
- Detect different types of attacks to SCADA systems
- Understand the "Purdue" model in relation to OCS networks
- Apply risk management techniques to ICS.
- Assess risks for ICS.
- Apply IEC standard to ICS security.
- Design and implement an ICS security program.
- Identify and defend against ICS vulnerabilities.
- Understand the systems security lifecycle.
- Understand information assurance principles and tenets.
- Understand the security architecture for industrial control systems (ICS).
- Identify vulnerabilities in ICS networks, connected devices, software, and controls.
- Understand NIST SP 800-82 security standards and how to apply them to SCADA
- Use skills in computer network defense and implement incident response and handling methodologies.

***Prerequisites**:* Industrial Control Systems (ICS) Foundations, Introduction to Cybersecurity

***Nice Mapping**: N/A*
***Lab**:* Students will learn to program both a PLC and an HMI, learn fieldbus protocols
find remote access points, conduct network capture analysis, use SQL injection to bypass authentication, design a secure DCS, find passwords on embedded devices, conduct password fuzzing, Baseline using PowerShell, configure firewalls, conduct network forensics of an attack, analysis windows event logs and conduct incident response.

b. Curriculum Requirements for an Associate's Degree in ICSS

Curriculum Overview

- Required units: 60 credits minimum:
    - 20, 3 credit courses, OR
    - 15, 4 credit courses
    - Labs: 1-2 credits
- Typical timeframe to complete degree: 2 years
- Average credits per semester: 15 credits
- General Education requirements: 49% credits

- Major requirements: 51% credits
- Program pre-requisite - high school diploma or equivalent (Math & Science background is beneficial, not required)
- Course Categories
  - General
  - Major Core Requirements,
  - Major Electives.

Course Name	Duration (Credit Hours)	Delivery Method	Pre-Reqs	Assessment Methods	Lab (Y/N)	NICE Specialty Area
Computer & Programming Fundamentals	3	In-person	Algebra or High school math	Lab coding assessment, and projects.	Y	Software Development (DEV)
SCADA Systems & ICS Architecture	3	Online	Introduction to Operating Systems	Regular	N	Systems Architecture (ARC); Systems Development (SYS)
ICS Operations & Processes	3	Online	SCADA Systems & ICS Architecture	Regular	N	
Risk Management & Prevention	3	Hybrid		Industry linked projects, internships, semester exams, case studies	N	Risk Management (RSK); Knowledge Management (KMG); Systems Administration (ADM); Cybersecurity Management (MGT); Cyber Defense Analysis (CDA); Vulnerability Assessment and Management (VAM); Threat Analysis (TWA); Exploitation Analysis (EXP); All-Source

						Analysis (ASA)
Incident Management & Response	3	Hybrid		Industry linked projects, internships, semester exams, case studies	N	Incident Response (CIR); TWA; Customer Service and Technical Support (STS); MGT; CDA; VAM, Targets (TGT); Collection Operations (CLO)
Cybersecurity and Safety for ICS	3	Online		Industry linked projects, semester exams, case studies	N	MGT; CDA; Cyber Defense Infrastructure (INF); Cyber Operational Planning (OPL); Cyber Operations (OPS)
Network Security	3	Hybrid		Regular exams	Y	Network Services (NET)
Introduction to Operating Systems	3	In-person		Regular exams	Y	Software Development (DEV)
Digital Logic Design	3	In-person		Regular exams	Y	DEV
PLC Programming	2	In-person	Digital Logic Design	Lab assessment	Y	N/A
Electrical Power Systems	3	Online		Regular exams	N	N/A
Embedded Systems	3	Hybrid		Regular exams	N	N/A
Cryptography	3	In-person	Computer & Programming Fundamentals, Algebra, Pre-Calculus	Regular exams	Y	CDA; INF
Cyber-Physical Systems	2	Online		Regular exams	N	Systems Analysis (ANA); Cyber Investigation (INV); Digital

						Forensics (FOR)
Database Management Systems	3	In-person		Regular exams + Lab assessment	Y	Data Administration (DTA); ADM
Governance and Policy in IT	3	Online		Regular exams	N	Strategic Planning & Policy (SPP)

Table 8: Summary of courses for an Associate's degree in ICSS
M: Major Core, E: Major Elective, G: General, Y: Yes, N: No

General Education Requirements:

- **Math**: High school math knowledge if preferred but not required. The following subject areas are recommended to build a strong foundation in problem solving, critical thinking, and reasoning:
    - Algebra
    - Statistics
    - Pre-Calculus
    - Calculus
    - Discrete Mathematics

- **Social Sciences**: Students should have knowledge of cultures and civilizations, understand how society changed over time, and how it works today. They should be able to select between a variety of courses including but not limited to the following subject areas:
    - U.S. History
    - World History
    - Economics
    - American Government
    - Introductory Psychology
    - Introductory Sociology

- **Communications and Management**: Students need to have strong communication and management skills to succeed in a workplace. Courses in this domain will build strong verbal and non-verbal communications, develop interpersonal skills, and build management skills such as planning, organizing, leading, and controlling resource management. Courses include but are not limited to:
    - Technical Writing
    - Organizational Communication
    - Project Management
    - Professional Ethics

- **Natural Sciences**: Students will develop critical thinking, analytical, and problem-solving skills. They should be encouraged to perform experiments in laboratories. Courses include but are not limited to:
    - Introductory Physics

  - Environmental Sciences
  - Biology
  - Chemistry

- **Humanities & Fine Arts**: Students will learn about their society and culture, how societies are organized, and diversity appreciation. Courses in this area will encourage creative thinking. Courses include but are not limited to:
  - World Literature
  - American Literature
  - Religion & Culture
  - Women studies
  - Languages

Major Core Requirements:

Course: Computing Fundamentals + Lab

Description: This course will provide students with an understanding of computer science fundamentals. They will be introduced to the basic concepts of computer architecture, data structures, program flows, object-oriented programming, and programming languages. The lab will be designed to introduce students to programming in one language (e.g., C++, Python or Java). Labs will be designed to provide a gentle introduction to writing basic programs while keeping in mind good programming practices. Students should be able to write basic programs by the end of the course. This course should be taught in-person.

Topics: Programming fundamentals; Writing secure code; Object oriented programming; Robust programming (memory allocation and deallocation); and Linux programming.

Course: SCADA Systems & ICS Architecture

Description: This course will provide students with a basic understanding of SCADA systems' software and hardware and how they monitor, gather and process real-time data. They will also learn about ICS security design and architecture, network discovery, and mapping.
Topics: Communication medium (e.g., VSAT, RF, cell, microwave); Defense in depth (e.g., layered defenses, IDS sensor placement, security system architecture, virtualization); External network communications (e.g., access points into ICS/SCADA systems, VPNs, vendor/third party access points, mobile devices); Field device architecture (e.g., relays, PLC, switch, process unit); Industrial protocols (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC); Network protocols (e.g., DNS, DHCP, TCP/IP, UDP); Network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs); Wireless security (e.g., Wi-Fi, wireless sensors, wireless gateways, controllers).

Course: ICS Operations & Processes

Description: In this course, students will gain an in-depth understanding of ICS operations and processes. Students will learn how to secure ICS systems against attacks and vulnerabilities and common standards as well as best practices for ICS security.

Topics: Industry sectors; Professional roles & responsibilities in industrial environments; Process types; Instrumentation & Controls; Basic process control systems (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, Ethernet I/O, buses, Purdue Model (ISA 9539)); Critical infrastructure subsectors (e.g., chemical, wastewater, drinking water and water quantity management, electricity, oil and gas, manufacturing, transport); Safety and protection systems (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring).

Course: Risk Management & Prevention

Description: Students will be introduced to the risk management process to secure Industrial Control Systems. They will learn about risk management requirements (human safety, data confidentiality and integrity, fault tolerance, asset identification), system and process lifecycle, software maintenance, identifying ICS risk exposure, and risk compliance and auditing.

Topics: Global security standards, practices, and regulations (e.g., IEC/ISA 62443, NIST 800-8241, ISO 27000 standards); Risk management (e.g., PHA/HAZOP usage, risk acceptance, risk/mitigation plan); Security lifecycle management (e.g., acquisition and selling of an asset, procurement, commissioning (e.g., secure deployments, maintenance, decommissioning); Security policies and procedures development (e.g., exceptions, exemptions, requirements).

Course: Incident Management & Response

Description: Students will learn how to identify, analyze, and correct hazards to prevent future re-occurrence. This course will equip students with knowledge of the process of limiting potential disruption caused by an event, followed by a return to normal function.

Topics: Incident recognition and triage (e.g., log analysis/event correlation, anomalous behavior, intrusion detection, egress monitoring, IPS); Incident remediation/recovery; Incident response (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine).

Course: Safety and Cybersecurity for ICS

Description: This course will equip students with foundations in computer system threats and impacts and practices for optimizing security. Students will understand cybersecurity basics and how they relate to other areas of computer security and information technology.

Topics: 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); Availability (e.g., health and safety, environmental, productivity); Cryptographic (e.g., encryption, digital signatures, certificate management, Public Key Infrastructure (PKI), public versus private key, hashing, key management, resource constraints); Security awareness programs (e.g., employees/management); Security tenets (e.g., CIA, AIC, non-repudiation, least privilege, separation of duties); Threats (e.g., nation states, cyber criminals, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious such as errors and omissions); Common failure modes for equipment under control; OSHA Safety Rules; Electrical Safety.

Course: Network Security + Lab

Description: In this course, students will learn about breaches and threats that target a computer network, understand vulnerabilities of networks and how to secure them, network security management tools, layers of the network security model, and different controls in each layer. The laboratory will focus on introducing students to scripting for security and simulating attacks such as TCP/IP attacks, DNS attacks, packet sniffing attacks, firewall exploration and bypassing and securing against these attacks.

Topics: Network architectures and protocols; Network topologies; Attacks on networks - DoS attacks, DNS cache poisoning, Buffer overflow, Dictionary attacks.

Course: Introduction to Operating Systems + Lab (Optional)

Description: Students will learn basic Operating System (OS) services and mechanisms, functions, and applications as well as storage and hierarchy. The lab will introduce students to simulating job scheduling algorithms, paging algorithms, and inter-process communication coding.

Topics: Installing & configuring OS; OS Services; Storage Structure & Hierarchy; Inter process communication; CPU Scheduling; Dead lock prevention and avoidance; Paging Algorithms.

Course: Digital Logic Design + Lab

Description: Students will learn basic digital logic design concepts used to build circuit boards and microchip processors and will gain understanding of how logic circuits are analyzed, designed, verified, and tested. The laboratory will introduce students to simple circuit design using breadboards and programming logic gates, verifying, and testing them.

Topics: Number systems & representations; Boolean algebra & Logic gates; Combinational Logic Circuits; Flip-flops & Sequential circuits; Register & Counters; Memory & programmable logic.

Major Electives Requirements:

Course: PLC Programming + Lab (Optional)

Description: This course will introduce operational theory, systems terminology, PLC installation, programming, timers and counters, and relay logic instructions. Students will develop operational skills in maintenance and troubleshooting of ICS and automated equipment. The laboratory will provide students with the basics of ladder logic programming and implementing different logic functions using PLC.
Topics: Control circuits; Ladder Diagram; Functional Blocks; Structured Text; Continuous Flow Chart; Human-User Interface; Draw Schematics & design protection for electrical panels; Sensors in the industry.

Course: Electrical Power Systems

Description: This course will introduce students to general aspects of system design, electric generators, components of transmission and distribution systems, power flow analysis, system operation, and performance measures.

Topics: Transmission line parameters (JHU Whiting School of Engineering – Electrical Power Systems); Power flow analysis; Methods of symmetrical components; Renewable energy generation; Transformation of energy to industrial, military & transportation uses.

Course: Embedded Systems

Description: Students will learn the basics of designing, interfacing, configuring, and programming embedded systems.

Topics: GNU, GCC; Memory types, segments and management; Embedded & RTOS (Purdue); Bus protocols; Wired communication; Embedded networking; Secure embedded system design.

Course: Introduction to Basic Cryptography + Lab

Description: This course will provide an overview of basic cryptographic concepts and methods, knowledge of commonly used cryptographic protocols, an understanding of theory, and implementations as well as vulnerabilities. The laboratory will introduce students to implementing basic cryptographic algorithms (e.g., encryption techniques, message authentication codes).

Topics: Historical ciphers, polyalphabetic ciphers; Modern ciphers; RSA; Protocols; Modes of operation (block vs. stream ciphers, linear feedback shift registers, ECB, counter mode, block chaining); One-way functions; Network-based systems; Strength of encryption; Key distribution and generation.

Course: Cyber-Physical Systems (CPS)

Description: This course will introduce students to the core principles behind CPS, development of CPS models and controls, identify safety specifications and critical properties of CPS, abstraction and system architectures, verify CPS models, and understand the semantics of CPS models.

Topics: CPS design; CPS security; Detecting problems in CPS.

Course: Database Management Systems + Lab

Description: This course will focus on concepts related to designing and implementing a database management system. Modern data models, data security and integrity, and concurrency will also be discussed. The laboratory experience will provide students with an exposure to basic SQL query processing.

Topics: Data storage and physical design; Relational Model; Entity Relationship Model; Functional Dependencies; Query processing; Normalization.

Course: Governance and Policy IT

Description: This course will introduce students to cybersecurity policy, governance structures for policy creation, selection and implementation of policy, and audit and control functions to ensure compliance. Students will learn about national and international policy related to cybersecurity such as privacy, intellectual property, cybercrime, homeland security, cyberwarfare and the organizations that formulate these policies.

Topics: Discuss and analyze existing IT policies related to ICS security; ICS Security Standards; Government structures that create policies.

C. Curriculum Requirements for a Bachelor's Degree in ICSS

Curriculum Overview

- Required units: 121 -135 units
- The typical timeframe to complete a bachelor's degree: 4 years
- Average units per semester: 15 units (Fall and Spring semesters)
- General Education requirements: 60 units (less than 50%)
- Major Requirements: 30-36 units
- Core Courses (fixed): 30-36 units
- Students may transfer from an associate degree a maximum of 60 units, towards a bachelor's degree

Course Title	Duration (credit hrs)	Delivery Method	Type	Lab (Y/N)	NICE Specialty Areas
Introduction to Computer Science	3	Online	M	N	DEV; SYS; Test and Evaluation (TST)
Introduction to Operating Systems	3	Online	M	N	ARC; DEV; TST; ANA
Programming Courses	3	Online	M	N	DEV
Algorithms	3	Online	M	N	DEV
Introduction to Basic Computer Security Concepts	3	Online	M	N	CDA; -INF; VAM
Introduction to Databases	3	Online	M	N	ADM; ANA
Introduction to Computer Networking	3	Hybrid	M	N	NET; ANA; ADM
Information Technology	3	Hybrid	M	N	RSK; ANA; PMA
Cryptography	3	Hybrid	M	N	FOR

Course Title	Duration (credit hrs)	Delivery Method	Type	Lab (Y/N)	NICE Specialty Areas
Foundations of Cybersecurity	3	On campus	C	N	MGT; INV; TWA; OPL; OPS; EXL; Language Analysis (LNG)
Foundations of ICS/SCADA	3 + 1 Lab = 4	On Campus	C	Y	ASA; EXP; TWA; DEV, RSK
Industrial Control Systems (ICS) Foundations	3	On Campus	C	N	NET; ADM; ANA
Wireless Security	3	Hybrid	C	N	ADM; ANA; FOR
Penetration Testing	3 + 1 Lab = 4	Hybrid	C	Y	EXP; TWA; OPL; OPS
Computer & Network Security	3	Hybrid	C	N	FOR; NET ADM; ANA
ICS Defense and Incident Response	3	On Campus	C	N	CDA; CIR; STS; EXP; VAM
Database Management Systems	3	Hybrid			ADM; ANA; DTA; KMG
Algebra	3	Online	G	N	N/A
Discrete Mathematics	3	Online	G	N	N/A
Statistics	3	Online	G	N	N/A
Pre-Calculus	3	Online	G	N	N/A
Calculus 1	3	Online	G	N	N/A
Calculus 2	3	Online	G	N	N/A
Interpersonal Communications	3	Hybrid	G	N	N/A
Technical Writing	3	Online	G	N	LNG
Social Sciences	9	Online	G	N	N/A
Natural Sciences	9	In-person	G	N	N/A
Arts & Humanities	9	Online	G	N	N/A
Diversity & Cultural Understanding	6	Online	G	N	N/A
Internship	3	In-person	M	N	TEA

Table 9: Summary of Courses for a Bachelor's Degree in ICSS
M: Major Core, E: Major Elective, G: General, Y: Yes, N: No

General Education (60 units). These courses need to be aligned with those who pursue an Associate's degree (courses need to be equivalent to the courses students at a 4-year institution take). Students with an Associate's degree may transfer to a 4-year program (undergraduate) and can transfer up to 60 units.

High school students entering a 4-year institution need to have either a high school diploma or GED equivalency and can then start with the prerequisites/major requirements and core courses.

Math: Students need a solid foundation of math to build their problem solving, critical thinking, and reasoning skills.

1. Algebra (3)
2. Discrete Mathematics (3)
3. Statistics (3)
4. Pre-Calculus (3)
5. Calculus 1 (3)
6. Calculus 2 (3)

Communications: Students need to develop effective communication skills so that they are better prepared to speak confidently to diverse audiences. Technical communications are just as important for students pursuing a career in cybersecurity. It teaches students to practice writing and addressing a specific audience.

1. Interpersonal communication (3)
2. Technical writing/communication (3)

Social Sciences: (9)
Students can pick from a variety of courses, including but not limited to, philosophy, sociology, anthropology, economics, geography, sociology, history.

Natural Sciences: (9)
Students can pick from a variety of courses, including but not limited to, biology, chemistry, geology, environmental sciences, physics, astronomy. At least one 2-course lab sequence should be required.

Arts & Humanities: (9)
Students can pick from a variety of courses, including but not limited to, languages (e.g., Arabic, Chinese, French, German, Russian, Spanish, Japanese), literature courses, music

Diversity & Cultural Understanding: (6)
Students can pick from a variety of courses, including but not limited to international studies, Native Americans, religion and culture, diversity, women studies, and intercultural communications

Prerequisites/Major Requirements (30 units):

Introduction to Computer Science: students need a broad understanding of computer science and programming. This includes topics such as data structures, software engineering, familiarity of programming languages such as C++, C, Java, Python and SQL, and algorithms. Students should be able to write a small programming language by the end of the course. They should understand the fundamentals of computer science. This course should adopt an in-person learning model.

Introduction to Operating Systems

This course introduces basic operating system (OS) mechanisms, functions, and its applications. It will give an overview of the structures of an OS and analyze the major components of an OS. This course also focuses on UNIX (and related, e.g., Linux) operating systems.

Programming Courses

In depth knowledge of the selected programming language. Students may choose one of various programming languages. Each course will require students to implement functional projects. This course will include the theory, design, and implementation of the selected programming language. This course should adopt an in-person learning model.

Algorithms

Covers common algorithms and how to solve mathematical modeling of computational problems, algorithm designs, randomization, data structures, and sorting. This course should adopt an in-person learning model. (Note that may schools currently blend the Algorithms course with teaching a programming language. This approach can be used here, as well.)

Introduction to Basic Computer Security Concepts

Understanding of the protection of computer systems from attacks and unauthorized use and damage, firewalls, vulnerabilities, malware, securing applications from disruption, understanding different attacks against computers, understanding computer vulnerabilities, and security measures and mechanisms. Understanding the components of a computer (hardware, software, firmware) and how to protect each component.

Introduction to Databases

Understanding relational databases, introduction to data management concepts and database systems, introduction to interactive query language (SQL) queries and database development and programming. Students will learn how to design interactive and secure database applications as part of a project/assignment. This course should adopt an in-person learning model.

Introduction to Computer Networking

This course will cover the implementations of a computer network, management of computer networks, and computer network components. Topics include internetworking, reliability, error detection and correction methods, bandwidth allocation, routing, and security.

Information Technology

Students will learn how to design, develop, and implement a computer information system with an emphasis on software applications and computer hardware. Learners will also focus on techniques for processing data, computer concepts, and input/output systems.

Cryptography

Solid foundation of cryptography and communication security. Topics include cryptographic algorithms and procedures, message authentication code, public key encryption, and basic cryptanalytic techniques. Understanding the commonly used cryptographic protocols, vulnerabilities and basic protocols.

Cybersecurity Core Courses (30 units):

Foundations of Cybersecurity (3)
Solid foundation of computer system threats and its impacts, practices for optimizing security, understanding of the basics of cybersecurity and how it relates to other areas of computer security and information technology. Topics include social engineering, essential security principles, wireless and physical security, user authentication.

Computer and Network Security (3)
Protection of networks from breaches and threats, understanding network security and its vulnerabilities, network security management tools, layers of the network security model, policies addressing each layer, different controls of network security; physical, administrative, and technical.

Foundations of ICS/SCADA (3)
Fundamentals of ICS operation and security, hands-on training on protecting and securing ICS from cyberattacks, ICS vulnerabilities, network discovery and mapping, detection, identifying common ICS cyber security risks, assessing and managing these risks. Common standards and best practices for ICS security, ICS security design and architecture.

Information Security (3)
Learn about the practices and techniques of protecting, preventing unauthorized access, destruction, use of private information.

Ethical Hacking/Penetration Testing + Lab (3 + 1 lab)
Topics include techniques hackers use to hack systems, locating vulnerabilities, penetration testing, types of hackers, and how to secure systems against potential attacks. Lab experience is required. Students need to gain hands-on training performing a pen test and experience the process of attempting to gain unauthorized access (with prior authorization) to systems, data, or software applications.

Industrial Control Systems (ICS) Foundations (3)
Solid foundation of Industrial Control Systems and its components, understanding the integration of hardware and software with network connectivity, Supervisory Control and Data Acquisition (SCADA) systems, IT/OT devices, and common ICS threats.

Wireless Security (3)
Students will learn about the techniques used to access computers/data using wireless networks, techniques used to protect a wireless network from unauthorized access, as well as various wireless protocols (e.g., Bluetooth, NFA, Wireless Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2-Enterprise).

ICS Defense and Incident Response (3)
Understanding ICS networks and environments, monitoring for potential attacks, understanding defenses, and incident response to maintain the dependability of systems.

Database Management Systems (3)
Understanding the process of designing and implementing a database management system and its applications. Solid foundation of the practice of handling, storing, retrieving, and updating information

on computer systems, understanding the different types of database management systems (e.g., hierarchical, network, object oriented, relational).

Hands on Training /Internship (1-3)
Hands on training includes internships students can take to earn 3-unit credits. Typically taken in the summer. This allows students to gain experience while still in school.

D. Curriculum Requirements for a Master's Degree in ICSS

Curriculum Overview

- Required units: 60 units
- The typical timeframe to complete a master's degree: 2 years
- Average units per semester: 15 units (Fall and Spring semesters)
- General Education requirements: 0 units (less than 50%)
- Major Requirements: 30-36 units
- Core Courses (fixed): 30-36 units
- Previous experience: Industrial, electrical, or some engineering or OT background. No experience in infotech or cybersecurity

Course Title	Credit hrs	Delivery Method	Lab (Y/N)	NICE Specialty Areas
Administration and Supervision	3	Could be virtual	Optional	PMA; EXL; MGT)
Project Management	3	Could be virtual	Y	PMA; SPP
Info-Tech Architectures	3	Could be virtual	N	ARC
IT Policy and Strategy	3	Could be virtual	N	SPP
Cybersecurity Fundamentals	3	In person	Y	Brief introduction to the skills under Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and Investigate (IN)
System Admin	3	In person	Y	ADM
Network Admin and Engineering	6	In person	Y	NET; ADM

Course Title	Credit hrs	Delivery Method	Lab (Y/N)	NICE Specialty Areas
Network Security	3	In person	Y	NET; skills under AN
Incident Response	3	In person	Y	CIR

Table 10: Summary of courses for a Master's degree in ICSS

Course: Administration and Supervision

***Delivery Method**:* Distance (virtual) vs in person: In person is recommended, but it could be virtualized. Simulations could be prompts displace virtually where students type out their responses.

Credit Hours: 3

Description: This course's purpose is to teach the ICS professional industry standards in safety and longevity of the tools and equipment in an ICS environment. Students will learn safety standards, facilitation of work orders to workers in an ICS environment, and development of safety tests to determine the health of tools and equipment in the ICS operation.

Topics: Safety hazards and procedures, standards and regulatory codes, calibration procedures, maintenance techniques, decontamination procedures, interpreting operation manuals, equipment upgrading procedures, downtime procedures, automation supervision, documentation, subordinate supervisory techniques.

Potential Assessment Methods: ICS event simulation, incident response simulation, catastrophe relief simulations.

Prerequisites: Project management, incident response, system admin, network admin and engineering, network security.

NICE Mapping: PMA; EXL; MGT
Contents of lab (if applicable): Lab optional (e.g., simulations of events/mishaps in ICS environment and practice how they handle the situation).

Justification: A Master's degree implies some level of mastery in application and ability to oversee a process. This class would teach students how to achieve that level of oversight.

Course: Project Management

Delivery: Distance (virtual) vs in person: In-person preferred, could be easily done virtually

Credit Hours: 3

Description: This course's purpose is to introduce the application of knowledge, skills, tools, and techniques that ICS personnel use to plan, staff, estimate, and manage ICS projects and operations. Emphasis is place on learning and applying the concepts of managing scope, risk, budget, time, expectations, quality, people, communications, procurement, and externally provided services. (Description came from Purdue's CNIT 480 course descriptions, modified for ICS environments).

Topics: Organizational planning and scheduling methods, system upgrading procedures, documentation, operation procedures

Potential Assessment Methods: Multiple choice exams, assessments with Microsoft Project (or a similar software), simulations

Prerequisites: IT policy and strategy

NICE Mapping: PMA; SPP

Lab: Recitations of using project management software (e.g., Microsoft Project), simulations, etc.

Justification: Project management is a skill that should be learned by any professional in a STEM field, for it builds the skills needed for one to communicate in, building of, and execution of project deliverables

Course: Info-Tech Architectures

Delivery Method: Distance (virtual) vs in person: in person preferred, could be done distanced/virtually

Credit Hours: 3
Description: A conceptual and technological survey of information technology architectures inclusive of operating systems, network operating systems, distributed systems architectures, and distributed application architectures. Interoperability between these architectural components is explored. Current technology and trends in each architectural element are reviewed.

Topics: Operating systems, network architectures, application of architectures, introduction to information technology

Potential Assessment Methods: multiple choice exams

Prerequisites: N/A

NICE Mapping: ARC

Lab: N/A

Justification: This course builds fundamental understanding about information architectures that is keystone to any IT or cybersecurity application.

Course: IT Policy and Strategy

Delivery Method: Distance (virtual) vs in person: In-person is preferred, could be virtual

Credit Hours: 3

Description: Course examining key technology policy concepts.

Topics: Strategic perspective for aligning competitive strategy and information systems, development, and implementation of policies, defining systems and system requirements, role of CIO, CTO, CISO and other administration in IT policy.

Potential Assessment Methods: Exercises to prepare students to apply concepts in their area of work/research; class helps apply concepts to framing of a research thesis

Prerequisites: Info-Tech Architectures

NICE Mapping: SPP

Lab: N/A

Justification: Information policy is vital for local governmental administration and regulations as well as the ethics involved with handling sensitive information.

Course: Cybersecurity Fundamentals

Delivery Methods: Distance (virtual) vs in person: In-person is preferred, could be done virtually.

Credit Hours: 3

Description: Understanding underlying technologies of secure systems, gain awareness on the risks and related privacy issues. Learn to analyze the range of trade-offs in balancing a variety of security properties and the usability demands of computer and information systems. Learn how to select the appropriate tools and techniques to address and manage the concepts of risk, threats, vulnerabilities, and potential attacks. Apply and evaluate the concepts of trust in a cybersecurity context and apply controls related to authentication, authorization, and access control. Gain insight on the purpose of cybersecurity and the integral role of cybersecurity professionals.

Topics: Governance and policy; network security and architecture; concepts of least privilege, separation of risk, defense in depth and secrecy; The CIA triad; security tools and security hardening techniques; identifying system and application security vulnerabilities; incident response.

Potential Assessment Methods: Multiple choice exams, examinations involving short and long answer responses.

Prerequisites: Info-Tech Architectures

NICE Mapping: brief introduction to the skills under PR, AN, CO, and IN

Lab: Virtual machines provided, applying different threats to security systems and having students analyze, classify, and determine the correct response. Give the students the opportunity to create their own threats and attacks on simulated systems, record and analyze the results.

Justification: This course would build the keystone theories, principles, and applications of cybersecurity that should be the framework of any cybersecurity professional

Course: System Admin

Delivery Method: Distance (virtual) vs in person: in-person

Credit Hours: 3

Description: This course provides a comprehensive introduction to system administration in an industrial control system setting.

Topics: Authentication and authorization, directory services, system management, system security

Potential Assessment Methods: Multiple choice exams, lab assessments

Prerequisites: Info-Tech Architectures

NICE Mapping: ADM

Lab: In-person labs that gives students experience in building virtual domains on enterprise levels, use of access policy and other system admin topics.

Justification: System administration is at the forefront of any enterprise, including those in the industrial sector. This course will teach students to ensure the confidentiality, integrity, and availability of an ICS system.

Course: Network Administration and Engineering

Delivery Methods: Distance (virtual) vs in person: in-person

Credit Hours: 6

Description: This course focuses on the tasks and issues involved in the installation and administration of distributed computing systems. Presentation of the foundations and intermediate levels of understanding required to effectively design, implement, and manage today's industrial network environments.

Topics: Basic models; network addressing and operations; network protocol interactions; enterprise-class hardware applications; wired and wireless networks; administration of network OS; network infrastructure.

Potential Assessment Methods: multiple choice exams, lab assessments

Prerequisites: System Admin, Cybersecurity Fundamentals

NICE Mapping: NET; ADM

Lab: lab applications of the prior stated topics. Students would build different enterprise-level systems to be evaluated

Justification: Network Engineering is a keystone in any enterprise, including those in the industrial sector.

Course: Network Security

Delivery Methods: Distance (virtual) vs in person: in person

Credit Hours: 3

Description: This course explores business, conceptual, and technological aspects of network security for voice and data networks. The course deals with the analysis, design, implementation, and management issues surrounding effective network security.

Topics: Virus protection, firewalls, authentication, encryption, wireless security, security protocols, physical security, network security architecture, policy development.

Potential Assessment Methods: multiple choice exams, examination on firewall rules and application, lab assessments.

Prerequisites: Network Administration and Engineering

NICE Mapping: NET; skills under AN

Lab: Students getting hands on experience in the application of firewalls in a virtual enterprise system; applying network security tools in an enterprise environment.

Justification: Network security is the key front-line defense to any cyber-attack, especially one with as much potential for negative impact as a cyber-attack in the industrial sector.

Course: Incident Response

Delivery Methods: Distance (virtual) vs in person: in person.

Credit Hours: 3

Description: This course will bridge business operations to IT support of the critical systems that support day-to-day operations. Techniques to detect anomalous behaviors through the configuration and monitoring of modern Intrusion Detection systems, analyzing and decoding network flows, system logs, and reports is covered along with appropriate remediation actions. Multiple approaches, theories, standards, and suggestions for incident response handling will be examined.
Potential Assessment Methods: multiple choice exams

Prerequisites: Network Administration and Engineering; Network Security
NICE Mapping: CIR

Lab: TBD

Justification: In the case of a cyber incident, students would need to learn the fundamentals of responding to incidents while minimizing the harm done.

Course Title	Credit Hours	Delivery Method	Labs (Y/N)	NICE Specialty Area
Modern Control Theory	3	In person	Y	N/A
Operation and Maintenance	3	In person	Y	OM skillsets
SCADA Architecture	3	Could be virtual	N	ARC
SCADA Risk Management and Auditing	3	Could be virtual	N	RSK

SCADA Security Awareness and Auditing	3	In person	Y	Skills under PR and AN
Control Systems	3	In person	Y	N/A
Industrial Control System Security	3	In person	Y	Skills under PR and AN
Electrical Circuits and Mechanics	3	In person	Y	N/A
Independent study/individual project	Up to 6	Distance	N	N/A

Table 11: Summary of Courses for a Master's Degree in ICSS

Course: Modern Control Theory

Delivery Methods: Distance (virtual) vs in person: In-person.

Credit Hours: 3

Description: Introduction to dynamic systems, processes, and machines, and the application of control of system inputs and outputs to drive and maintain a system to a desired state. The objective of control theory is to maintain stability and optimization in any dynamic system.

Topics: Stability of linear and non-linear spaces and its operators; input/output algorithm; state variables and state transition matrix; state controllability and observability; state variable estimation; controller syntheses and state feedback; composite systems; open and closed loop control; model identification and robustness.

Potential Assessment Methods: Multiple-choice exams, simulations in an educational-purpose ICS facility.

Prerequisites: Control systems; electrical circuits, and mechanics.

NICE Mapping: N/A

Lab: labs in an educational-purpose ICS facility (e.g., a university-run power plant)

Justification: Contemporary theory in the process and application of modern control systems is vital to become an ICS professional.

Course: Operation and Maintenance

Delivery Methods: Distance (virtual) vs in person: In person.

Credit Hours: 3

Description: In this course, students will learn to determine if appropriate utilities and equipment are available and operational to safely execute various processes and testing. Students will learn to use and apply maintenance documentation and appropriate safety and operating procedures to perform maintenance functions in an ICS system.

Topics: Interpreting operational manuals and procedures; understanding troubleshooting and testing techniques in various systems; understanding specifications for various specific manufacturer tools and equipment; understand the functionality of loop components in a system; interpreting calibration documentation; understanding the fundamentals of electrical and mechanical engineering.

Potential Assessment Methods: Simulations where different segments and components in an ICS system fail and the student will be tested on the appropriate action and response needed to support the component. Verbal or written examination to test the student's knowledge and understanding of the role of different components and how to respond to incidents regarding component failure.

Prerequisites: Modern Control Theory; SCADA Architecture

NICE Mapping: OM skillsets

Lab: Labs where students have access to ICS components and the ability to interact with the various tools and systems. Labs will involve interaction with different segmentations and components in and ICS system and the various techniques to keep them operational.

Justification: course gives the students the fundamental understanding of operating an industrial control system required on all levels.

Course: SCADA Architecture

Delivery Methods: Distance (virtual) vs in person: In-person is preferred, could be distanced.

Credit Hours: 3

Description: This course gives the student a fundamental understanding of SCADA and its role in the ICS environment. Students will learn the basic components in any SCADA system and the role of network security in SCADA. Students will also learn the different types of SCADA systems, and how they are applied in different industries.

Topics: SCADA fundamentals; local processors; operating equipment; programmable logic controllers (PLC's); instrumentation; remote terminal unit (RTU); intelligent electronic device; master terminal unit; PC host computers; human-machine interface (HMI); architecture diagramming; networking fundamentals, including IP/TCP and UDP protocols, industrial protocols like Modbus TCP, and their application through cellular, radio, or satellite networks; the four generations of SCADA systems.

Potential Assessment Methods: Multiple choice exams on components in SCADA architecture, architecture diagramming within a provide industrial context, written exams where the student suggests a SCADA implementation based off a given scenario.

Prerequisites: Control Systems; Electrical Circuits and Mechanics

NICE Mapping: ARC

Lab: N/A

Justification: This course builds fundamental understanding of information technology architectures applied in a SCADA environment, a keystone for any ICS professional.

Course: SCADA Risk Management and Auditing

Delivery Methods: Distance (virtual) vs in person: Could be either in-person or distance.

Credit Hours: 3

Description: In this course, students will learn one of the best practices in cybersecurity - risk management - and how it can be applied in a SCADA/ICS environment. Students will learn how to identify, evaluate, and prioritize risks (as defined by ISO 31000), followed by application of resources to minimize, monitor, and control the probability or impacts of negative effects, while maximizing the probability and impact of positive effects.

Topics: Threat modeling; vulnerability identification; impact/consequences; how to ask the following questions: What can go wrong? What is the likelihood? What are the consequences? asset identification and system characterization; risk calculation and management; cybersecurity evaluation tool (CSET); NIST 800-82.

Potential Assessment Methods: Threat modeling based off a scenario, written exams testing students on identifying risks and how to control for them based off a given scenario, simulations.

Prerequisites: SCADA Architectures

NICE Mapping: RSK

Lab: N/A

Justification: Understanding how to identify risks in a SCADA security environment would help improve future defense against SCADA systems.

SCADA Security Awareness and Standards

Delivery Methods: Distance (virtual) vs in person: In person.

Credit Hours: 3

Description: In this course, students will assess, develop, and deliver SCADA/ICS security awareness programs within an organization. This course will provide training on industrial standards related to SCADA systems.

Topics: SCADA security standards, SCADA security components and configuration, implications non-secure SCADA system, threats and vulnerabilities in a SCADA system, SCADA risk management, managerial and operation controls, technical controls.

Potential Assessment Methods: Building/application of SCADA security programs based on standards and technologies learned over the course; midterms with multiple choice exams.

Prerequisites: SCADA Architecture

NICE Mapping: Skills under PR and AN
Lab: Current technologies, SCADA system security assessment, practice in application of SCADA systems.

Justification: Similar to risk management, this class helps students build stronger security skills to sharpen the defense in future SCADA systems.

Course: Control Systems

Delivery Methods: Distance (virtual) vs in person: in-person.

Credit Hours: 3

Description: Application of programmable logic controllers (PLCs) as control devices, with emphasis on discrete input/output systems. Application of calculus in the design of control systems for industrial processes.

Topics: PLC programming and application skills; current industrial standard plant network protocols; HMI's; instrumentation; basic measurements.

Potential Assessment Methods: multiple choice exams.

Prerequisites: Electrical Circuits and Mechanics.

NICE Mapping: N/A

Lab: in person experience with PLC's and HMI's, mock control systems for educational purposes.

Justification: This class will help students understand the daily process in control systems in all levels, to better understand how to secure it.

Course: Industrial Control Systems Security

Delivery Methods: Distance (virtual) vs in person: in person.

Credit Hours: 3

Description: Students will research how ICS functions, the critical infrastructure that they support, as well as steps that can be taken to improve the overall security of ICS systems.

Topics: Fundamentals of cybersecurity in ICS, including network, protocol, and application characteristics; relevant standards and organizations relating to industrial control systems; importance of securing ICS systems; understand how control system assets interact with industrial control systems; familiarity in retrieval and research methods in ICS.
Potential Assessment Methods: Multiple choice exams; lab evaluation.

Prerequisites: Modern Control Theory; SCADA Risk Management and Auditing; SCADA Security Awareness and Standards.

NICE Mapping: Skills in PR and AN

Lab: Computers available to teach students application of ICS software and how it can be secured.

Justification: This course would be a capstone class in cybersecurity in an ICS environment; all the previous courses would build up to this one.

Course: Electrical Circuits and Mechanics

Delivery Methods: Distance (virtual) vs in person: in person.

Credit Hours: 3

Description: Fundamental concepts, units and laws for DC and AC circuits with applications. Network theorems, network simplification, and mesh analysis.

Topics: AC circuits; DC circuits; basic digital and linear circuitry; timer circuits; logic gates; circuitry interfacing; semiconductors; I/O control.

Potential Assessment Methods: Multiple choice exams, circuitry lab practical.

Prerequisites: N/A

NICE Mapping: N/A

Lab: Application of circuitry labs

Justification: This course provides the fundamental understanding of circuitry; all following classes would build off the skills used in this course.

Course: Individual Project/Independent Study

Delivery Methods: Distance (virtual) vs in person: TBD

Credit Hours: 6

Description: TBD

Topics: TBD

Potential Assessment Methods: TBD

Prerequisites: TBD

NICE Mapping: N/A

Lab: TBD

Justification: TBD

(i) Regional Specialties

While none of the institutions in FEMA Region 5 have an existing ICSS program, various colleges and universities have different expertise that could be leveraged to support a Hub and Spoke program in ICSS. Almost all the institutions have basic courses in Algebra and Trigonometry. Several of the institutions have Associate's (A), Bachelor's (B), Master's (M), or PhD (P) programs. A few only have one or two classes (C):

University	OT	Cybersecurity	ICSS
Chicago State University	B	M	N
Eastern Illinois University	B	M	N
Governors State University	N	M	N
Illinois State University	C	M	C
University of Illinois at Chicago	B, M, P	M, P	N
University of Illinois at Springfield	N	B	N
University of Illinois at Urbana-Champaign	B, M, P	C	N
Northeastern Illinois University	N	M	N
Northern Illinois University	B, M, P	N	N
Southern Illinois University Carbondale	B, M, P	M	N
Southern Illinois University Edwardsville	B, M, P	B	N
Western Illinois University - Macomb	B	B	N
Bemidji State University	N	N	N
Metropolitan State University	N	M	N
Minnesota State University, Mankato	B, M	C	N
Minnesota State University Moorhead	N	B	N
Southwest Minnesota State University	N	C	N
St. Cloud State University	B	B	N
University of Minnesota - Crookston	N	B	N
University of Minnesota - Morris	N	N	N
University of Minnesota - Twin Cities	B, M, P	M	N
University of Minnesota - Duluth	B, M	C	N
Winona State University	B	C	N
University of Wisconsin - Madison	B, M, P	N	N
University of Wisconsin - Milwaukee	B, M, P	C	N
University of Wisconsin - Eau Claire	N	N	N
University of Wisconsin - Green Bay	B	B	N
University of Wisconsin - La Crosse	N	M	N
University of Wisconsin - Oshkosh	B	M	N
University of Wisconsin - Parkside	B	M	N
University of Wisconsin - Platteville	B, M	M	N
University of Wisconsin - River Falls	C	M	N
University of Wisconsin - Stevens Point	C	B	N
University of Wisconsin - Stout	B	C	N
University of Wisconsin - Superior	N	M	N
University of Wisconsin - Whitewater	B, M	C	N

Ball State University	N	C	C
Indiana State University	B, M	A, B	BS
Indiana University Bloomington	C	A, B, M, P	N
Indiana University East	N	N	N
Indiana University Kokomo	N	N	N
Indiana University Northwest	N	N	N
Indiana University Bloomington Indianapolis	B, M	B, M	N
Indiana University South Bend	N	N	N
Indiana University Southeast	N	N	N
Ivy Tech Community College of Indiana	A	A	N
Purdue University	B, M, P	B, M, P	C
Purdue University Fort Wayne	A, B	C	N
Purdue University Northwest	B, M	B	N
University of Southern Indiana	B	C	N
Vincennes University	A	C, B	N
Central Michigan University	B, MS	C, M	N
Eastern Michigan University	B	B, M	N
Ferris State University	B, MS	A, B, M	N
Grand Valley State University	B	C, B, M	N
Lake Superior State University	A, B	N	N
Michigan State University	B, M, P	C	N
Michigan Technological University	B, M, P	C, B, M	C
Northern Michigan University	A, B	C, A, B, M	N
Oakland University	B , MS	A, B, M	C
Saginaw Valley State University	C, B	C, M	C
University of Michigan	B, M, P	C	P
University of Michigan	B	C	N
University of Michigan	C	B	N
Wayne State University	B, M, P	N	P
Western Michigan University	B, M, P	B, M, C	N
Bowling Green State University	B, M	B, M	N
Central State University	C	N	N
Cleveland State University	B	B, M	N
Kent State University	A, B	C, A, B	C
Miami University	B	N	N
Northeast Ohio Medical University (NEOMED)	N	N	N
Ohio University	B, M, P	N	N
The Ohio State University	B, M, P	C	N

Shawnee State University	N	A, B	N
The University of Akron	A, B	N	N
The University of Toledo	B, M	M	N
Wright State University	C, B, M, P	C, B, M	N
Youngstown State University	C, M	N	N

Table 12: FEMA Region 5 School Programs

(ii) Available Curricula

There are a few samples of existing curricula in ICSS that may be leveraged as a basis to build on other criteria. There are existing examples of curricula that may be used as a basis to support some of these courses. These include[1]:

No.	Type of Resource	Resource Description	Link
1	Seed Security Labs	This is an open-source project that provides a set of labs and training that can be used to supplement ICSS learning.	https://seedsecuritylabs.org/labs.html
2	CLARK Digital Library	This is an online repository of expert reviewed learning materials ranging from modules to full courses. It contains courses and modules such as: Cybersecurity of ICS ICS Fundamentals and Security Security in Cyber-Physical Systems Introduction to ICS Industrial Network Protocols Securing Industrial Networks Introduction to ICS Overview of ICS Components and Processes Attacks on Industrial Control Networks Mentoring Industrial Control Networks Industrial Malware and Attack Cases Introduction to SCADA Secure Management of Control Systems	https://www.clark.center/home

[1] Our thanks to the ICSCOP Educational Materials and Resources Working Group, especially Sean McBride, for the provision of this resource list.

		SCADA Control System Networking	
3	Industrial Cybersecurity Community of Practice ICSCOP	This is a national group that brings together professionals from government, industry, and academia focused on ICSS and ICSS education. There are several working groups including one devoted to developing standards in ICSS and another developing a repository of ICSS educational materials and resources.	https://inl.gov/icscop/
4	Electronic Documents	a. Cyber-Physical Systems Security Knowledge Area document. b. A collection of Resources for Getting Started in ICS/SCADA Cybersecurity	a. https://www.cybok.org/media/downloads/Cyber-Physical_Systems_Security_issue_1.0.pdf b. https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/
5	ICS and ICSS Textbooks	a. Securing SCADA Systems b. RIoT Control: Understanding and Managing Risks and the IoT c. Cybersecurity for ICS: SCADA, DCS, PLC, HMI, SIS d. Blue Team Handbook: SOC, SIEM and Threat Hunting	a. https://www.amazon.com/Securing-SCADA-Systems-Ronald-Krutz/dp/0764597876 b. https://www.amazon.com/RIoT-Control-Understanding-Managing-Internet-ebook/dp/B01M1SBMDE c. https://www.amazon.com/Cybersecurity-Industrial-Control-Systems-SCADA-ebook/dp/B0071ART60/ref=sr_1_3?dchild=1&keywords=cybersecurity+for+industrial+control+systems&qid=1616797021&s=digital-text&sr=1-3

			d. https://www.amazon.com/Blue-Team-Handbook-Condensed-Operations/dp/1091493898/ref=sr_1_1?dchild=1&qid=1617118498&refinements=p_27%3ADon+Murdoch+GSE&s=books&sr=1-1&text=Don+Murdoch+GSE
6	SANS Industrial Control Systems Library	The SANS Industrial Control Systems Library is a central resource for all ICS Brochures detailing our courses, Posters, Surveys, Whitepapers, and our Defense Use Case papers	https://www.sans.org/blog/industrial-control-systems-library/
7	ICS and ICSS videos	S4 ICS Security Event.	https://www.youtube.com/channel/UC5MdLu7ji_eyGiTfigk75lQ
8	Fortiphy	Basic training bundles for ICS related materials.	a. https://fortiphyd.talentlms.com/catalog/index
9	International Society of Automation Courses	a. Using ISA/IEC Standards to Secure Your Control Systems b. IACS Cybersecurity Design and Implementation c. IACS Cybersecurity Operations and Maintenance	a. https://www.isa.org/products/using-the-isa-iec-62443-standards-to-secure-your-c b. https://www.isa.org/products/iacs-cybersecurity-design-implementation-ic34 c. https://www.isa.org/products/iacs-cybersecurity-operations-maintenance-ic37
10	ISC^2 Courses	a. Exploring Cybersecurity in Industrial Control Systems b. Exploring Cybersecurity in Industrial Control Systems	a. https://www.isc2.org/Development/Immersive-Courses/Exploring-Cybersecurity-in-

			Industrial-Control-Systems# b. https://www.isc2.org/Development/Immersive-Courses/Exploring-Cybersecurity-in-Industrial-Control-Systems
11	Cybersecurity and Infrastructure Security Agency	A series of training courses in ICS	https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT
12	ISACA Training and Certifications	a. ICS 410:ICS/SCADA Security Essentials b. ICS 515: ICS Active Defense and Incident Response c. ICS 612: ICS Cybersecurity In-Depth	a. https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/ b. https://www.sans.org/cyber-security-courses/industrial-control-system-active-defense-and-incident-response/ c. https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth/
13	Idaho State University Industrial Cybersecurity Engineering Technology Program		https://www.isu.edu/industrialcybersecurity/
14	BSI Group Certified Lead SCADA Security Professional Training Course		https://www.bsigroup.com/en-US/our-services/cybersecurity-information-resilience/training-courses/certified-lead-scada-security-

			professional-training-course/
15	FireEye Fundamentals of ICS Security		https://www.fireeye.com/services/training/courses/fundamentals-ics-security.html
16	Secura ICS Security Training		https://www.secura.com/services/people/training-courses/industrial-control-systems-security-training
17	Honeywell Red Team/Blue Team ICS Cybersecurity Training		https://www.honeywellprocess.com/en-US/explore/services/industrial-it-solutions/Pages/Red-Team--Blue-Team-ICS-CYBERSECURITY-TRAINING.aspx
18	INFOSEC SCADA/ICS Security Training Bootcamp		https://www.infosecinstitute.com/courses/scada-security-boot-camp/
19	GIAC Certifications	a. Global Industrial Security Professional b. GIAC Response and Industrial Defense c. GCIP GIAC Critical Infrastructure Protection	a. https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp?msc=giac-focus-area b. https://www.giac.org/certification/response-industrial-defense-grid?msc=giac-focus-area c. https://www.giac.org/certification/critical-infrastructure-protection-gcip?msc=giac-focus-area

20	University of Houston Accelerated Control Systems/SCADA Security Class		https://uh.edu/technology/departments/ilt/certificates_old/scada/
21	NYU security Architectures for Industrial Control Systems		https://engineering.nyu.edu/sites/default/files/2020-11/ECE_GY_9463_S21.pdf
22	Technology and Management Training Courses and Seminars (TONEX) SCADA Security Training		https://www.tonex.com/training-courses/scada-security-training/
23	Industrial Control Systems Cyber Security Institute	a. Fundamentals of IT and OT Systems b. Conducting Asset Inventories for US DoD Facility Related Control Systems using the Army Methodology c. Fundamentals of Industrial and Facility Related Control System Cybersecurity	https://icscsi.org/curriculum-introics.html a. https://icscsi.org/curriculum-itotfundamentals.html b. https://icscsi.org/curriculum-dodrmfinventory.html c. https://icscsi.org/curriculum-assessingics.html
24	Udemy Courses	ICS/SCADA Cybersecurity	https://www.udemy.com/course/ics-scada-cyber-security/
25	Cybrary Courses	ICS/SCADA Fundamentals	https://www.cybrary.it/course/ics-scada-fundamentals/
26	SecuriCIP	a. Industrial Cybersecurity Essentials b. Industrial Cybersecurity Technical Professional	a. https://www.securicip.com/course/online-securicip-icse-industrial-cyber-security-essentials-apr-2021/

			b. https://www.securicip.com/course/online-securicip-industrial-cyber-security-technical-professional-may-2021/
27	Information Assurance Certification Review Board Certified SCADA Security Architect		https://www.iacertification.org/cssa_certified_scada_security_architect.html
28	Wilmington University Graduate Certificate in SCADA Security		https://www.wilmu.edu/technology/scada-cyber-security-curriculum.aspx
29	E-Council ICS/SCADA Cybersecurity		https://iclass.eccouncil.org/our-courses/ics-scada/
30	PECB Lead SCADA Security Manager Training		https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager
31	Dragos ICS Cybersecurity Training		https://www.dragos.com/training/
32	Exida Academy Training Cybersecurity for Industrial Automation Control Systems for Employees and Contractors		https://www.exida.com/Training/Course/IEC-62443-cybersecurity-for-industrial-automation-control-systems-iacs
33	Naval Postgraduate School Industrial Control System Security		https://nps.edu/web/c3o/labtainer-lab-summary1#Industrial%20Control%20Systems

Table 13: Sampling of ICSS Curricular Resources

In addition to building off curricula and projects such as these, these resources can be used to disseminate curricula to participating schools in the Hub and Spoke network. For example, CLARK could be used to house curricula developed at one institution for access and use by other institutions.

(iii)Process to Create Hands-On Curriculum

Hands-on curriculum could be created with reference to existing elements of the NICE Framework. However, this Framework is limited in its applicability to ICSS. A recommendation for the design of curriculum is Backwards Design championed by Wiggins and McTighe. This approach focuses on student outcomes, specifically student understanding and abilities rather than memorization or coverage of course content. Therefore, backwards design begins with the identification of desired student outcomes. These outcomes are in the form of what students should know or be able to do. These will be drawn from various sources including the NICE Framework (NIST SP 800-181), the NSA NCAE-C Knowledge Units, and the Association for Computing Machinery (ACM)/IEEE Computer Society (IEEE CS)/Association for Information Systems Special Interest Group on Security (AIS SIGSEC)/International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) Joint Task Force Cybersecurity Curriculum Guidance Document. The learning outcomes outlined in the Section 2. b. are recommended.

The next step is to determine acceptable evidence that demonstrates that the content has been mastered. Section 2. i. iv. next discusses the forms this evidence could take.

Next, is to plan the learning experiences. These will align with the outcomes and pedagogical methods. These should also be informed by input from partners, and refined by the availability of technical resources (e.g., lab equipment). This will differ from Hub to Hub, and will evolve over time.

The final step is the review to ensure the alignment among the outcomes, content, assessments, and pedagogy.

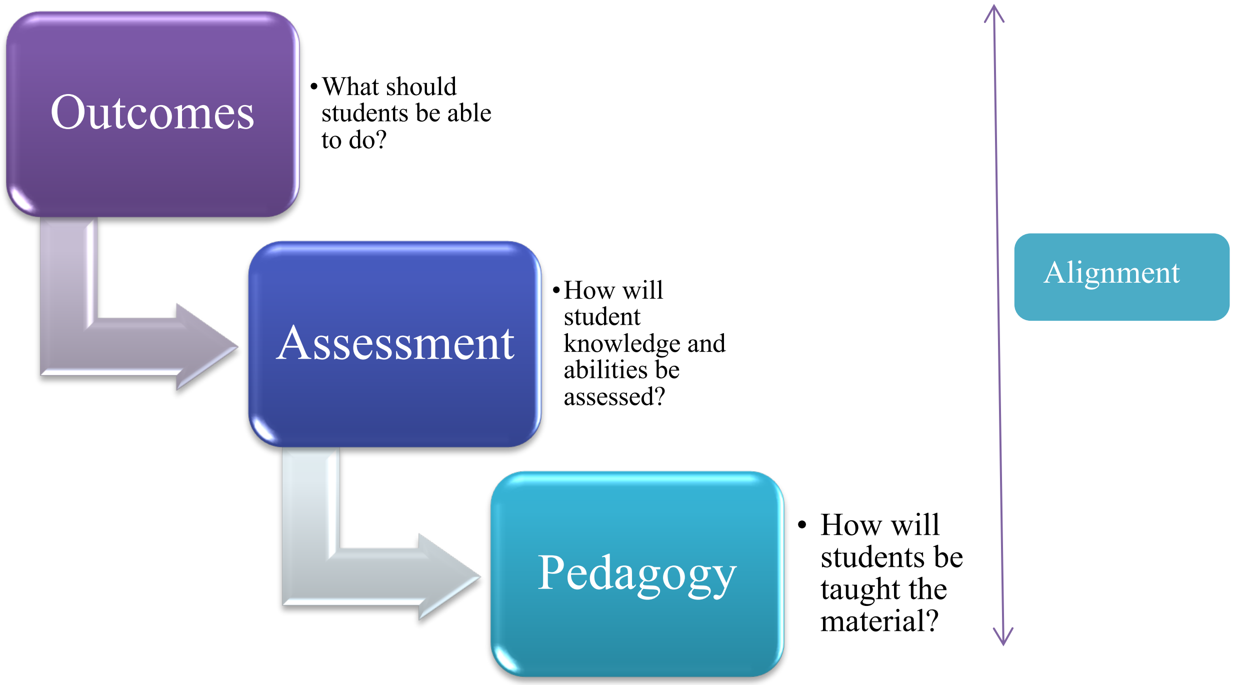

Outcomes
• What should students be able to do?
Assessment
• How will student knowledge and abilities be assessed?
Pedagogy
• How will students be taught the material?
Alignment

Figure 4: Process in Creating Hands-On Curriculum

(iv) Assessment Plan

The plan for assessment includes a range from small individual assessments to larger cross-program assessments:

- *Formative/Summative*: Assessment should be ongoing and serve a dual purpose. Formative assessment is intended to gather information to help the instructor improve the ongoing learning process by demonstrating where the students are. Summative evaluation is intended to judge the success of the learning process for the students. Formative assessment happens regularly throughout the learning process while summative assessment happens at the end of learning experiences (e.g., at the completion of a course or program). Formative assessment is low stakes and helps identify where students are struggling. It could take the form of pair discussions, proposals, concept maps, short quizzes, discussion, jigsaws, etc. Summative assessment would include exams, tests, proposals, projects, presentations.
- *Knowledge/Skill*: The assessment of knowledge vs. the assessment of skill is another element that should be carefully considered as different methods are appropriate for each.

Some suggestions for assessments are:

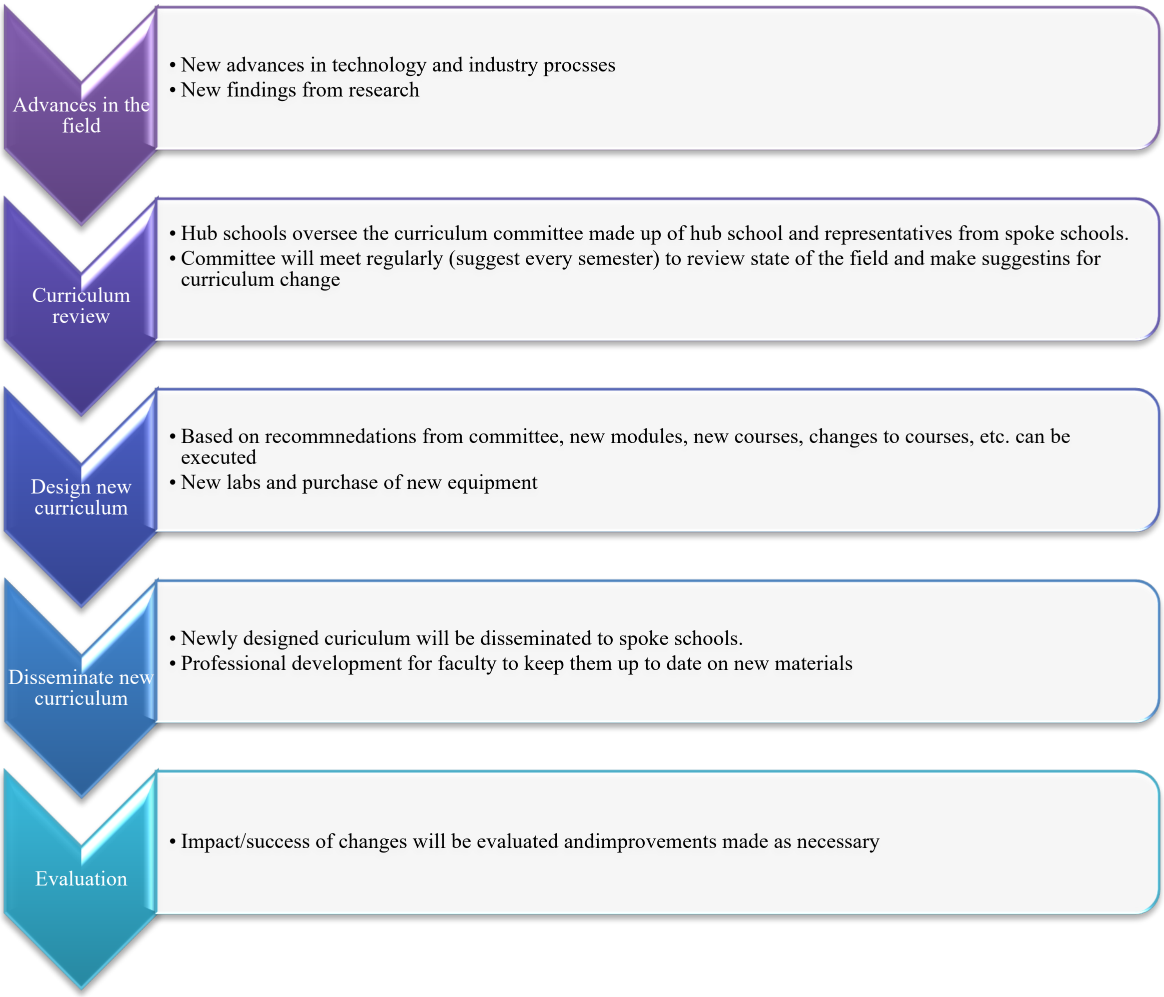
Learning Outcomes	Notes on assessments
Maintain ICS devices and attendant networks	Projects, exams
Identify and mitigate evolving ICS security threats	Proposal, exams
Assess evolving risks to ICS systems	Report, exams

Learning Outcomes	Notes on assessments
Maintain high standards of safety in ICS environments	Projects, reports
Implement and maintain ICSS software	Project, exams
Communicate with OT and IT personnel	Report, exams

Table 14: Assessment Suggestions

(v) Update Curriculum

There are a few steps to updating the curriculum. As described in figure 5 below, this process comprises of: advances in the field, curriculum review, designing a new curriculum, disseminating a new curriculum, and evaluation. Advances in the field consist of incorporating updated research findings that provide an overview of current knowledge, allowing opportunities to identify gaps in existing research, implementing newer technologies, and revising industry methodologies. The curriculum review involves a representative from both hub and spoke schools to meet regularly with hub schools to examine the curriculum and suggest any changes or propose improvements. Based on the discussions from this meeting, any changes to the curriculum (adding new modules, requiring resources such as equipment, changing courses, etc.) can be added and executed. After agreeing to the new curriculum design, it is disseminated to spoke schools to keep faculty members up to date on the changes. Lastly, any curriculum modifications may be evaluated, and improvements can be made as necessary.



Advances in the field

- New advances in technology and industry procsses
- New findings from research

Curriculum review

- Hub schools oversee the curriculum committee made up of hub school and representatives from spoke schools.
- Committee will meet regularly (suggest every semester) to review state of the field and make suggestins for curriculum change

Design new curriculum

- Based on recommnedations from committee, new modules, new courses, changes to courses, etc. can be executed
- New labs and purchase of new equipment

Disseminate new curriculum

- Newly designed curiculum will be disseminated to spoke schools.
- Professional development for faculty to keep them up to date on new materials

Evaluation

- Impact/success of changes will be evaluated andimprovements made as necessary

Figure 5: Process for curriculum updates

(vi)Creating a Path for Students

Once the Hub and Spoke network is implemented, the next step is to create a path for students. Section 2 above provides exemplars of the courses that should be considered for inclusion in an ICSS curriculum. Anywhere from 1/3 to 1/2 of the program should cover general education courses (e.g., sciences, ethics, written and oral communication, social sciences, humanities) that are necessary for a well-rounded education. The rest of the courses will be technical. The nature of ICSS means that these technical courses may span several academic units (OT and IT). For most institutions, these courses may be found in Computer Science, IT, Computer Engineering, Industrial Engineering, departments, to name a few. It is therefore likely an interdepartmental or interdisciplinary program will need to be created. There are several considerations when considering a student path:

- The number of credits students need to take to complete a degree. How many of those credits are reserved for certain courses or course types?
- Where expertise in the various technical courses is to be found at the various institutions. Based on this, a decision needs to be made as to which academic unit will administer the degree. Either one existing academic unit is to be selected with classes recognized from other units, or a new unit is to be created.

- Consideration for which courses already exist, which courses can be reasonably modified, and which courses need to be created from scratch.
- Once the courses, credits, and degree administration are decided, the student path through the program can then be mapped out.

Hands-on experience is a valuable component of the educational program we have described and dedicated educational experiences of this kind need to be built into the curriculum. This requires identifying appropriate departments to manage such experiences, faculty to supervise them, and mechanisms for appropriate placement and evaluation of the students. Most higher education schools have programs for work-study/internship already in place. These would need to be appropriately adapted for the ICSS program, including identifying appropriate partners.

3. Hub and Spoke Implementation Strategy for Industrial Control Systems Curriculum

a. Exemplar Hub and Spoke Models for Education and Training

Currently, ICSS education is rare. As previously mentioned, there are only a few institutions with the combination of laboratories, instructional materials, and instructors needed to offer a useful curriculum that also includes the broader base of skills employers need. This is one reason why there are many training and certification programs: the expectation is that base education will be gained in a previous degree and then on-the-job, with an additional set of skills to be taught and tested in the certification programs and tutorials. This results in disconnected and disparate programs and knowledge.

There is considerable potential for a Hub and Spoke system to have centralized resources at the Hub available to help the Spoke schools develop courses. ICS labs can be shared virtually among collaborating schools. Instructors can develop and share instructional materials. Furthermore, the collection of schools can work together to develop ancillary materials (i.e., textbooks, lab manuals) and standardized curriculum). Industry partners in each region can also provide resources and feedback on a scale larger than might be available to singleton schools. As these programs grow in expertise and experience, standardization will occur.

An alternative (that may also be executed in parallel) is to build a set of self-contained labs with accompanying textbooks based on singleton programs. Those can then be deployed to participating schools to spread the teaching according to the same plan. If this is designed to fit into the joint ACM/IEEE/IFIP curriculum, it will be simpler for schools to adopt into their curriculum.

There are several approaches that can be taken to constructing this Hub and Spoke structure:

- *Standard*: Structured as a set of Hub schools, each with 5-10 attendant Spoke schools. In this structure the institutions are administratively independent, and students largely complete their education at one institution. The institutions share resources, such as curricula, expertise, funding, etc. largely flowing from the Hubs to the Spokes (although some Spokes will contribute materials to the Hubs and/or Spokes). This has the advantage of leveraging the expertise and prestige of a Hub school to bolster education for students at the Spoke schools.
- *Placement*: This is structured as a set of complementary programs with some shared administration. In this model, each Hub and its attendant Spokes together constitute a complete program. The Hub is responsible for core programs and primary administration and the Spoke schools have expertise in various areas. The students start at the Hub school and are then placed and attend classes at various institutions within the system depending on their desired expertise. This structure has the advantage of exposing students to different environments and integrating students into the community. Placement is driven by learning objectives, which allows for more flexible and tailored learning environments. This method has the disadvantage of being administratively challenging; schools that are differently-resourced may provide different qualities of education. This method may work best in university systems with multiple campuses across a state.
- *Centralized*: In this model, students enroll at a Hub or Spoke institution and spend their entire educational career there. However, learning is centralized at the Hub school. The Hub school designs and administers the ICSS-specific course work, primarily online, and all students at the Spoke school attend that set of classes. Therefore, while they are physically at the Spoke

schools, their primary ICSS education is from the Hub; their general education can be what is provided at the local institution. This has the benefits of standardizing the ICSS learning experience, easing transitions into and out of work integrated learning, and as Hub schools with a proven track record, provide students at Spoke schools with a quality academic experience. This model has the disadvantage of being administratively challenging and placing a great deal of pressure on the resources of the Hub school.

- *Clinical*: In this model, the Hub is responsible for developing and administering the curriculum. Students then attend a Spoke school for their hands-on practice or clinical education. This model works best when work placements are geographically adjacent to Spoke schools so students can attend a Spoke school while completing work placement.

b. Logistics of Hub and Spoke Models in FEMA Region 5

The hub and spoke model for education in industrial control system security will work particularly well in FEMA Region 5. With the establishment of the foundational education at the hub school, the educational content can be easily distributed to the spoke schools in an electronic format through university systems and/or file sharing services. The recent pandemic has forced the distribution of educational material and content delivery online with colleges and universities gaining widespread expertise. Additionally, both faculty and staff have gained valuable experience with adapting content to a wide variety of Learning Management Systems (LMS). Distribution of content and incorporation into university LMS should be logistically simple.

With the foundational content established, spoke schools can and should engage the ecosystems in which they exist (industry, infrastructure, military) to add additional content that creates the skills required by ICS security stakeholders. As industrial control systems will vary by manufacturer and industry, the ability to add relevant educational content for a particular industry or industry cluster (for example: automotive manufacturing, pharmaceutical production, energy production, military operations, etc.) will be paramount to serve the security needs of the region.

In order to support the educational requirements of the foundational education content, a comprehensive inventory and evaluation of the following assets should be conducted:

- Industrial Control System Cybersecurity Ranges. (A range being a sophisticated virtualized education platform that uses industry standard virtual networks and security tools to teach comprehensive threat scenarios. Example: Cyberbit)
- ICS Cybersecurity virtual lab exercises. (Unlike the ICS cybersecurity range, these virtual labs provide a virtual approach to teaching short, foundational concepts. Example: SCADSUDO)
- Physical ICSS Labs with industry standard equipment. (This provides a unique opportunity for spoke schools to collaborate with both industry and government to fund, design, and build labs that are relevant to the region. Example: Endress & Houser IIoT Labs in Greenwood, IN)

Finally, an evaluation criterion to determine the efficacy of the initiative should be established with a criterion that not only includes program success rates but also industry partnerships and placement rates. Content and success should be reviewed annually at a conference of participating schools and partners with workshops aim at continuous initiative improvement.

c. Common Core Functions for Spoke Schools

The true benefit of hub and spoke schools is that the spoke schools do not need to reinvent the wheel and can utilize the benefits of an established curriculum without administrative overhead and of collaboration with more experienced faculty, a larger institution, and a more varied environment. Keeping this in mind, following suggestions are made for the functions of spoke schools:

- Appoint affiliate program director responsible for implementation of the program at the Spoke school who shall be responsible and accountable for ensuring that the program satisfies standards provided by the hub school and shall ensure that quality education occurs at all training sites and for all students.
- Provide appropriate resources to support the education program (e.g., space, administrative, equipment)
- Educating and training students.
- Provide for staff salary (at appropriate levels; students and instructors), benefits, and professional development funds

d. Inclusion Strategies for Diverse Learner Constituencies

An important core value for all programs should be to ensure that diverse learner constituencies are recruited and retained. Some strategies to ensure this include:

- Learners need to be part of the discussion and guide the curriculum development process, whether from an instructor standpoint, or a student one. This allows for a more diversified curriculum that adapts and supports all students from different backgrounds and identities (minorities, underrepresented groups, veterans, tribal populations)
- Engage with diverse learners and encourage them to share their experiences, opinions, and allow them to express their perspectives on how inclusion has an impact on their educational journey. This helps guide curriculum and program developments.
- Provide webcasts or videos that provide a glimpse of intercultural experiences students can experience on campus and what the campus has to offer for diverse learners. This helps learners feel included and have a sense of belonging.
- Identify barriers that students from underrepresented groups face when reaching their educational goals. Identifying barriers (barriers faced by people from an underrepresented group) to inclusive learning helps in any future decisions and meet the needs of these learners.
- Networking with alumni to stay connected and engaged and discuss any specific concerns. This keeps learners up to date and allows communication and collaboration between learners.
- Require diverse members of committees/boards to ensure inclusivity in recruitment and retention.
- Increase inclusive programs/activities/courses that are crafted to teach all students, such as including examples, case scenarios of different cultures/backgrounds.
- Marketing for recruitment and retention should not target a particular population. Website and social media pages are the face of any company/school/organization. Having a group of diverse learners as the front page of an educational institution gives the idea that all students are welcome and encouraged to learn.

- Anonymous surveys/questionnaires related to diversity and inclusion should be sent out to all students, faculty, and staff. This gives learners an opportunity to share any suggestions or issues related to inclusion and diversity.
- Provide scholarships/grants for diverse learners to increase recruitment from their populations. Allowing learners an opportunity to grow and get an education is an excellent way to increase targeted recruitment incentives.
- Include students in the faculty hiring process and curriculum development meetings. This allows students to get an insight in the hiring process of educators.
- Utilize technology-enriched instruction to facilitate student learning through active engagement.
- Consider using a multi-sensory approach to aid teaching, particularly when catering to learners with disabilities. This approach may be more useful in case of children with multiple disabilities as they need repetition through different modalities for reinforcement.

e. Common Core Functions for Hub Schools

The ideal goal of the Hub school is to enable a mass customization of the governance in their partner networks. After doing a survey of existing Hub and Spoke models of education (e.g., Centers of Academic Excellence), the following suggestions are made for what could be some of the common core responsibilities for hub schools:

- Development of the program curriculum.
- Working with affiliates to obtain as well as maintain accreditation.
- Program administration, which include coordinating advisory committee, evaluations, overseeing compliance with training requirements.
- Find reasonable balance between efficiently coordinating the network and satisfying singular Spoke schools.
- Develop positive, open relationships with school leaders, empathy to their specific needs and challenges, demonstrate confidentiality and openness while addressing school curriculum priorities.
- Help colleagues strengthen teaching and learning practices, create mentoring opportunities, share resources, build capacity for growth, and bring colleagues together.
- Encourage collective team cohesiveness and team-based methodology.
- At the commencement of each semester, coordinate meetings with school leaders and learning designers to discuss upcoming school priorities and initiatives to define a ‘Scope of Project’ summary. ‘Scope of Project’ summary should include aspects of student engagement, curriculum (i.e., assessment, feedback strategies and online learning environments), and/or targeted academic professional learning. The team should develop a strategic approach that best utilizes varied skill sets (i.e., from all members of the team) that align with meeting goal objectives efficiently and effectively.

In the Hub and Spoke model we are suggesting, the Hub school will manage curricula development, resource allocation, and host an advisory board. The Hub schools would be tasked with recommending curricula required for classes in an ICSS major. The Hub schools will build their curricula based on the recommendations and required skillsets of industry professionals. The Hub school will also be tasked with serving as an advisor for its Spoke schools - the advisory role serves to provide Spoke schools with any additional resources and mentoring to provide them with adequate information for them to succeed.

The Hub schools will be determined based on several different factors: Hub schools should have existing Science, Technology, Engineering and Math (STEM) programs, including electrical and industrial engineering, cybersecurity, and mathematics - these three fields were identified as precursors to ICSS. Hub schools must also have existing relationships with industry professionals across the region, allowing the school to keep in touch with what skillsets and experiences are required for a newly graduated student to enter the industry. In addition, a school with faculty or funding to hire new faculty in ICSS would be preferred. A Hub school is also preferred to have ABET accreditation, or equivalent engineering teaching accreditation. By these standards, a Hub school will most likely be a larger school in a region or the main campus in an expansive university system (e.g., University of Wisconsin at Madison; Purdue University West Lafayette campus). Each hub is recommended to have between four to eight Spoke schools, and these Spoke schools will be assigned to Hubs based on geographical distance from the Hub. As experience and resources are obtained, more Spokes might be added to some Hubs, but careful oversight must be exercised to prevent over-extension.

It is important to have clear criteria for selection of the Hub schools. One might be tempted to use CAE designations or ABET accreditation as required characteristics. However, those designations are not held by all universities that might be appropriate: both CAE and ABET are viewed by some faculties as overly-prescriptive and confining. ABET, in particular, is not widely sought by CS departments homed outside of schools of engineering. Given that ICSS is relatively rarely taught (as we have noted above) it is vital that universities be selected with a history of innovation, with appropriate and enthusiastic faculty, and with a solid foundation of education in core computing, security, and engineering.

f. Strategies for Curriculum Sharing

ICSS requires hands on training, experimentation, and application. It is beneficial to learners to have access to online and virtual resources to help them learn the knowledge and skills required in the field. It is suggested that each Hub manages a level of interoperability across its various Spoke schools. One way to do this is to implement a common Learning Management System (LMS) across all participating schools in the hub and Spoke network. An example of this is present within the University of Wisconsin academic system; in 2012 the university system implemented the LMS Canvas across all thirteen of its campuses across the state. Another example is Purdue University, which standardized its four campuses and online education to the Brightspace LMS in 2020.

An LMS should contain a centralized portal for all learning modules, lectures, manuals, homework assignments, assessments (e.g., quizzes, exams), feedback, and all other resources needed for students to be successful in their classes. It is recommended that the role of the Hub school is to define loose requirements for the type and extent of curricula that is made available in an online/virtualized setting. In response to the Hub school's role, the individual Spoke schools have the freedom to apply the recommended curricula from the Hub school as it is desired. In a centralized learning management software setting, curricula could easily be shared across Hub and Spoke institutions.

Several programs in ICSS were identified nationwide. These programs provide an opportunity to share curriculum resources and leverage efficiencies:

- *Non-credit offerings:* Most professional certifications are based on a for-profit model. However, these certifications could potentially be offered through multiple institutions as both online and in-person courses. These could offer opportunities to upskill, especially for those already holding expertise in cybersecurity or OT. They also offer opportunities as entryways into ICSS for those transitioning from one career to another. This creates potential within the Hub and Spoke network to serve incumbent workers by offering courses that are not for credit.

- *Transitioning to advanced degrees*: The one-year and two-year degrees offer opportunities to partner with four-year degree granting institutions. These partnerships could offer a simplified pipeline from the Associate's degree into a Bachelor's degree program.
- *Sharing hands-on resources:* smaller schools or schools with shorter programs may not be able to afford or may not wish to incur the cost of the hands-on resources necessary for an in-depth ICSS program. Partnering with larger institutions could offer opportunities for students at the smaller institutions to access lab facilities and resources (e.g., hardware) where they could receive hands-on education.
- *Sharing curriculum:* A survey of existing programs reveals a variety of courses offered at each institution. A Hub and Spoke model with a centralized curriculum repository offers an opportunity for faculty at the various institutions to access course materials that do not exist at their institutions. It also offers the opportunity for online courses that could be accessed by students at multiple institutions.
- *Research testbeds:* Partnerships among institutions also offers the opportunity to test various pedagogical structures and delivery.

g. Strategies for Instructor Professional Development

The quality of the education learners receive is largely based on instructor expertise. To ensure instructors are well trained and up to date with the latest advances:

- Host conferences that focus on faculty professional development to provide them an opportunity to learn from their peers, experience various engagements (e.g., effective practices, inclusion and diversity, teaching in an online environment, designing courses, and implementing curriculum, etc.). Instructors can have an opportunity to learn about new technologies they can use in their classroom to improve teaching strategies as well as learn new skills.
- Present a webcast for Spoke schools, hosted by Hub schools. These can be held every couple of months. Topics can be presented by Spoke schools. Discussions may include strategies to boost student engagement and participation. They can be recorded and re-used in future workshops.
- Provide Spoke school educators the necessary funding and support to obtain professional certifications and/or further their education for continuous learning and growth.
- Weekly discussions through online forums/chat groups. Participants can pose questions/issues they'd like to get answered/discuss. Instructors need to have a platform they feel comfortable in when sharing or reflecting their own professional/academic growth.
- Suggest yearly research publications related to ICS curriculum and curriculum developments. This allows instructors to be directly involved in the curriculum process and increase their engagement in learning changes and/or improvements. Additional research areas can include diverse learning, inclusion, acceptance, understanding different paces of learning, promoting students to enter STEM fields, incorporating various styles for learning in the classroom, etc.
-
- Collaboration between different Spoke schools (e.g., visitations or workshops across the schools).

- Instructor participation in curriculum development and enhancements from Spoke schools.
- Annual or semiannual workshops and training sessions for faculty from all Hub and Spoke schools, with participation by experts from industry, government, and other academic institutions.

h. Resources for Schools to Participate

For a Spoke school to participate in this network, they need existing electrical and industrial engineering, cybersecurity, and mathematics program. Students need a dedicated space to learn the fundamentals of electrical engineering, preferably a lab that has electrical equipment, including circuitry, electric sensors, and mock grid systems to help students learn through simulation. The dedicated lab space would be required to have some sort of access control (e.g., student ID card to access the lab rooms) that is limited to only students that are involved with the course and related ICSS program. The lab rooms may also be required to be open 24x7, as students often work after school hours on their assignments in labs. Students would also need to learn the basics of control systems with specific tools used in the industry (e.g., PLCs, Human Machine Interfaces (HMI's), monitor-control systems, switches, pneumatics, and other input/output devices). Cybersecurity courses would require computer and network laboratories, with networking hardware (e.g., switches, routers, network adaptors, centralized servers, virtual machines running various operating systems). Software licenses could include various Microsoft office and virtualization software, packet analyzing software, verification keys for Microsoft operating systems, etc. Mathematics courses may require the use of online learning resources (e.g., Piazza, Matlab).

i. Progress and Evaluation Metrics

Measures of Success:

The success of a program depends on maintaining standards and continuous improvement. To ensure the quality of the program, various evaluation metrics must be gathered. These include:

- Establish program goals and objectives (the purpose of the program). These objectives and goals will determine what is to be measured.
- Document the level of success in accomplishing the identified program goals and objectives. Use this information to determine the level of success to identify the needs for areas that need additional attention.
- Comparing academic progress and changes over time.
- Periodic reports describing the effectiveness of the program.
- Use information from various evaluations and check to see if requirements have been met.
- Feedback and surveys from alumni and employers to compare the success of the program against industry standards.

Potential Risks in Establishing these Programs:

In establishing these programs, a few potential risks may cause the program to fail to meet the program goals. The ability to identify risks is a crucial part of strategic program developments and planning. These identified potential risks include complexity, costs estimate, lack of resources, and lack of planning. Establishing this program may develop areas of complexity, which is likely due to using new or different methodologies, procedures, or practices. Unexpected cost risks are common and most likely to occur due to the lack of pre-planning. Lack of resources and lack of planning are potential risks that may be overlooked and may cause significant delays and shortages. Below are ways to mitigate these risks.

Ways to Mitigate the Risks:

- To avoid areas of complexity, offering training for instructors and interpersonal collaboration to provide a clear understanding of the roles and responsibilities of every individual in the school system (i.e., instructors, department chairs, dean). Any areas of misunderstanding, confusion, or suggestions for change needs to be addressed immediately.
- Strong, continuous planning ahead of time is the best way to budget time and cost estimates. The detail of this documentation should depend on the program segments and its corresponding cost estimates to avoid underbudgeting.
- To avoid resource shortages, it is important that we manage the resource availability and identify and prioritize the nature of the resource. This helps determine the factors that may simulate the risk and the effect it has on the success of the program.
- Preplanning necessary strategies for assessment, program and course objectives, and clearly identifying what's, when's, and how's of the program curriculum.

Appendix A4-1: A Sampling of ICS Programs

Program	Program Type	Description
GIAC Global Industrial Cybersecurity Professional	Certification	Designed to assess base level knowledge across professions that engineer or support ICS or ICSS
GIAC Response Industrial Defense	Certification	Active Defense strategies specific to and appropriate for an ICS network and system. Must demonstrate an understanding of the Active Defense approach, and how to mitigate threats from ICS-specific attacks. Must show understanding of strategies and fundamental techniques specific to core subjects with an ICS-focus, such as network security monitoring (NSM) and digital forensics IR (GRID).
GIAC Critical Infrastructure Protection	Certification	Understanding of the cruciality of the grid, or the bulk electric system in infrastructure, and the demanding that the personnel is charged with supporting it, understanding the impact of their actions/inactions regarding system reliability, safety, and security. Course helps validate the professionals who access, support, and maintain the critical systems that keep the grid running understand the regulatory requirements and practical implementation strategies to achieve regulatory compliance & CSEC objectives (GCIP).
ISC^2 Cybersecurity in ICS	Certification	explores the fundamental concepts around security concerns within industrial control systems (ICS) helping you understand how ICS supports critical infrastructure and the global need for ICS security, as it proliferates in various industries.

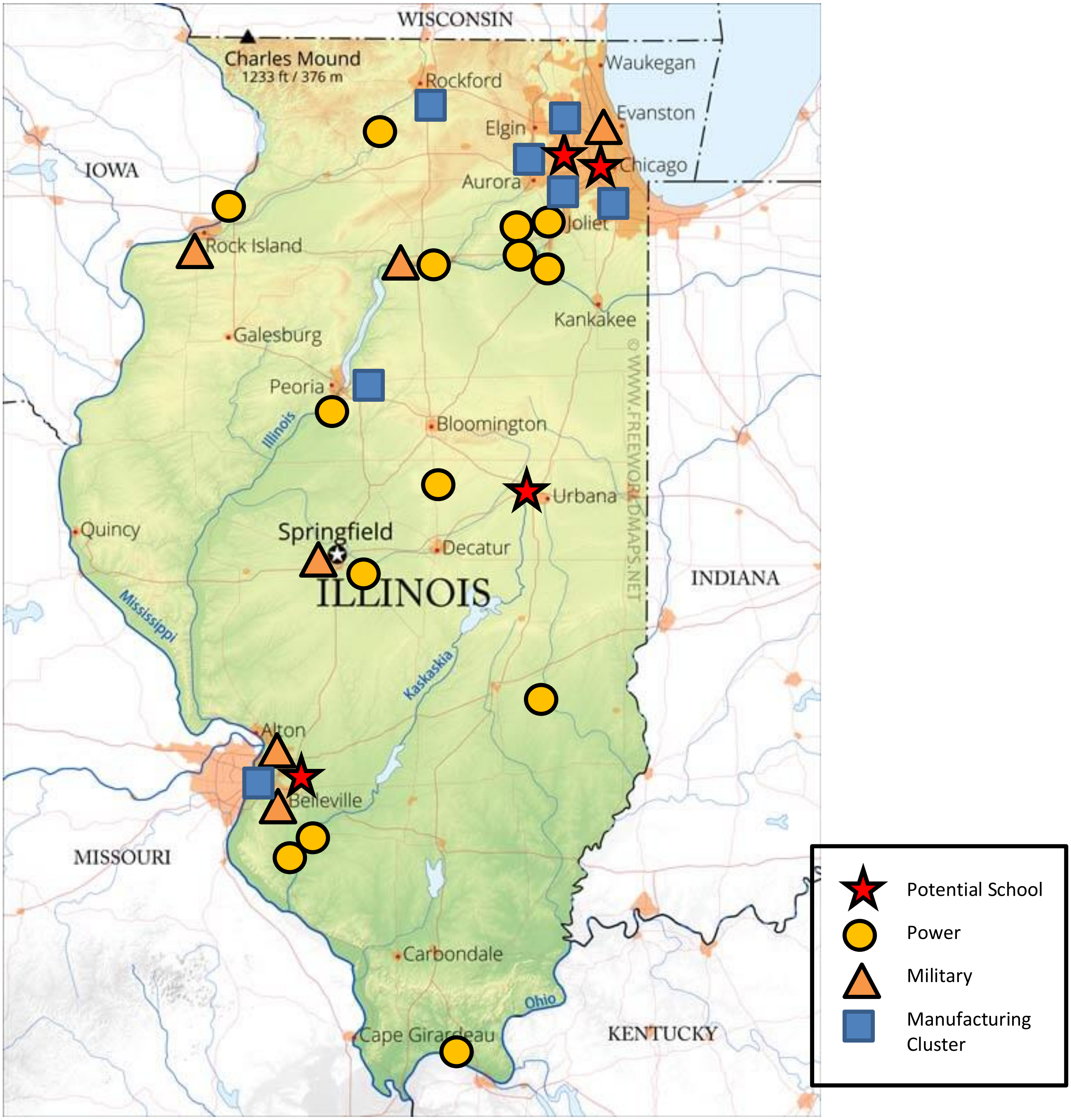
Tonex SCADA Security Training	Certification	Principles of SCADA and Industrial network security; (2.) Securing infrastructure networks for smart grid; (3.) SCADA system components; (4.) Architecture protocol; (5.) Cybersecurity; (6.) Provisioning; (7.) Regulatory requirements; (8.) Theory of operations; (9.) How to evaluate potential SCADA benefits.
Tonex ICS Cybersecurity Training	Certification	Introduces students to the fundamentals of ICS, recognize security architecture for ICS, identify different vulnerabilities in ICS network, remote devices, software, control servers, learn active defense and IR for ICS, essentials for NERC critical infrastructure protection (CIP) and list its strategies, apply risk management techniques for ICS, techniques for defending ICS, audit risks for ICS, apply IEC standard to network and system security of ICS, implement security program step by step, understand different ICS servers and their vulnerabilities to attacks, apply cybersecurity standards based on NIST SP 800-82.
SANS Graduate Certificate in Industrial Control Systems Security	Certification	A highly technical, hands-on program focused on teaching the applied technologies used to defend and secure industrial control systems, operations technology, and cyber-physical systems. Topics covered include networked industrial control system environment, monitoring it for threats, performing incident response against identified threats, and using knowledge gained from interactions with the adversary to enhance network security and maintain the safety and reliability of operations.

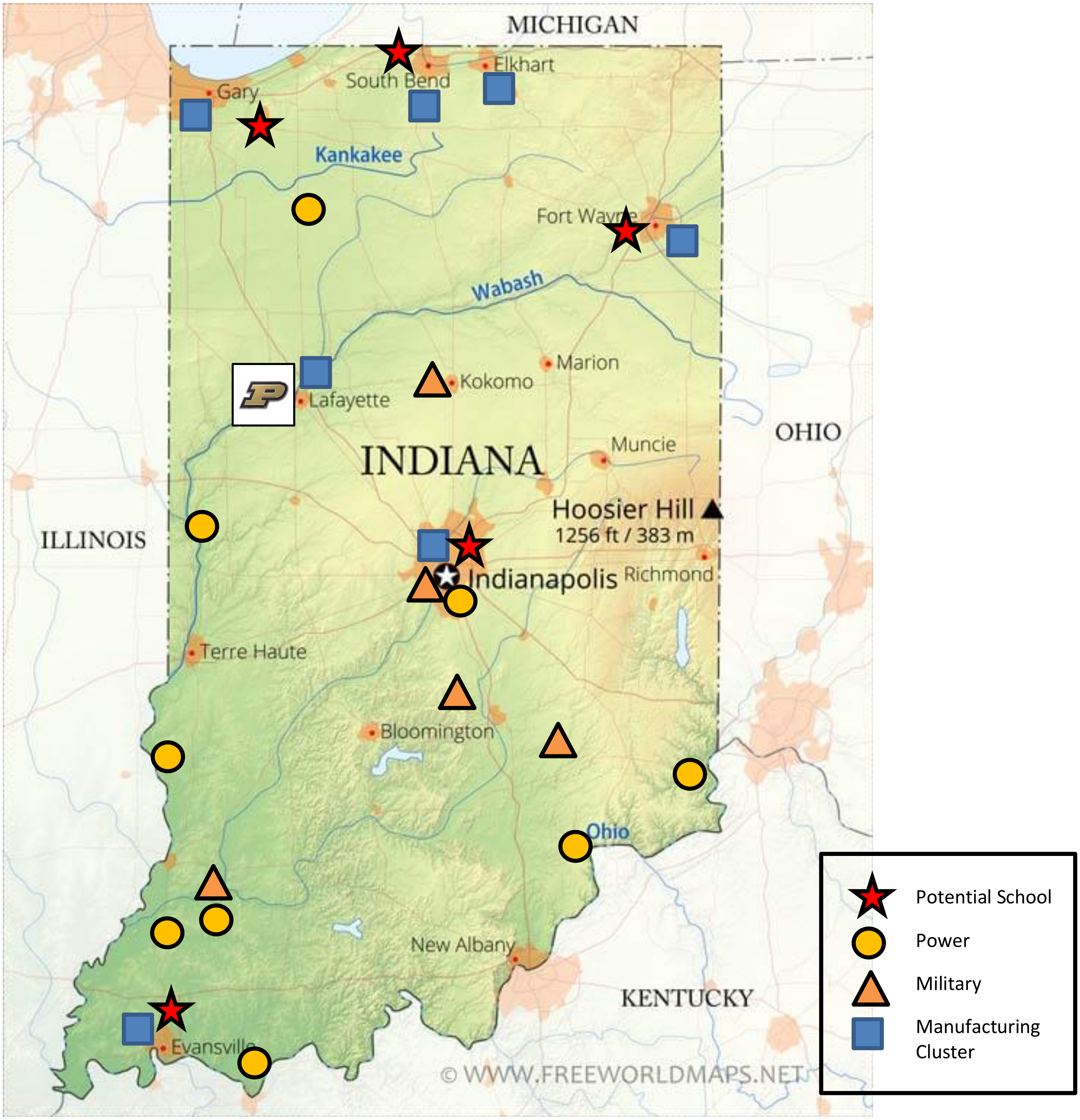
CISA Introduction to Control Systems Cybersecurity	Certification	introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain
CISA Intermediate Cybersecurity for ICS	Certification	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyberattacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks.
CISA ICS Cybersecurity	Certification	This course explores the fundamental concepts around security concerns within industrial control systems (ICS) helping students understand how ICS supports critical infrastructure and the global need for ICS security, as it proliferates in various industries. This course takes students through scenarios in these industry sectors: Oil and gas, food processing and healthcare.
CISA Operational Security for Control Systems	Certification	
CISA Differences in Deployment of ICS	Certification	
CISA Common IT Components on ICS CISA Cybersecurity within ICS & IT Domains	Certification	
CISA Attack Methodologies in IT & ICS	Certification	
CISA Mapping IT Defense-in-Depth Security Solutions to ICS	Certification	
CISA Industrial Control Systems Cybersecurity Landscape for Managers	Certification	

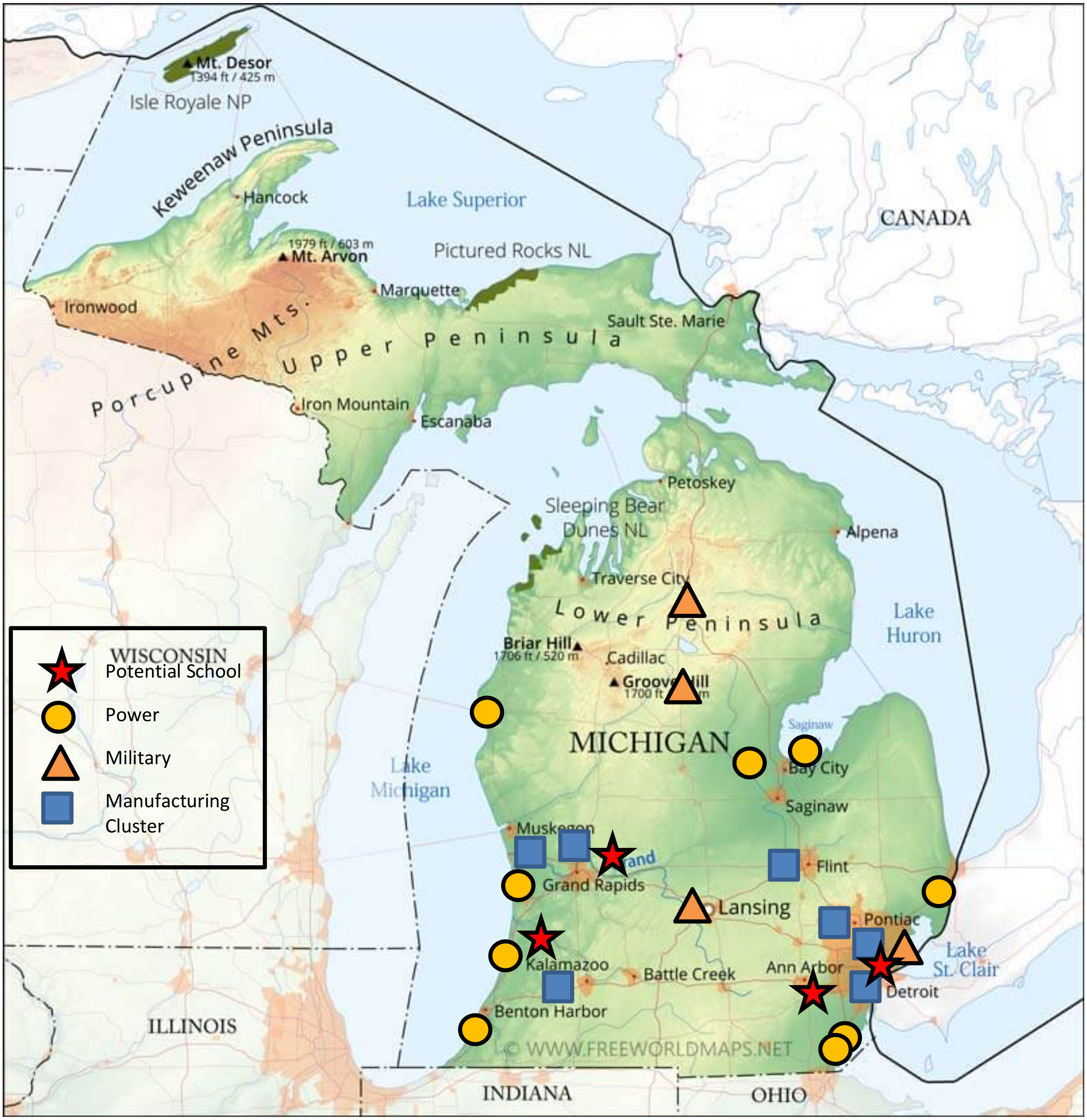
ISA Cybersecurity Fundamentals Specialist	Certification	This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.
ISA Cybersecurity Risk Assessment Specialist	Certification	This course gives students the tools they need to assess the cybersecurity of new or existing IACS and to develop a cybersecurity requirements specification that can be used to document the cybersecurity requirements of the project.
ISA Cybersecurity Design Specialist	Certification	This course will provide students with the information and skills to select and implement cybersecurity countermeasures for a new or existing IACS to achieve the target security level assigned to each IACS zone or conduit. Additionally, students will learn how to develop and execute test plans to verify that the cybersecurity of an IACS solution has properly satisfied the objectives in the cybersecurity requirements specification.
ISA Cybersecurity Maintenance Specialist	Certification	This course focuses on the ongoing operations and maintenance of IACS cybersecurity, which involves activities such as network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures.
Industrial Control System Cybersecurity Institute	Certification	This course introduces students to ICS cyber security,

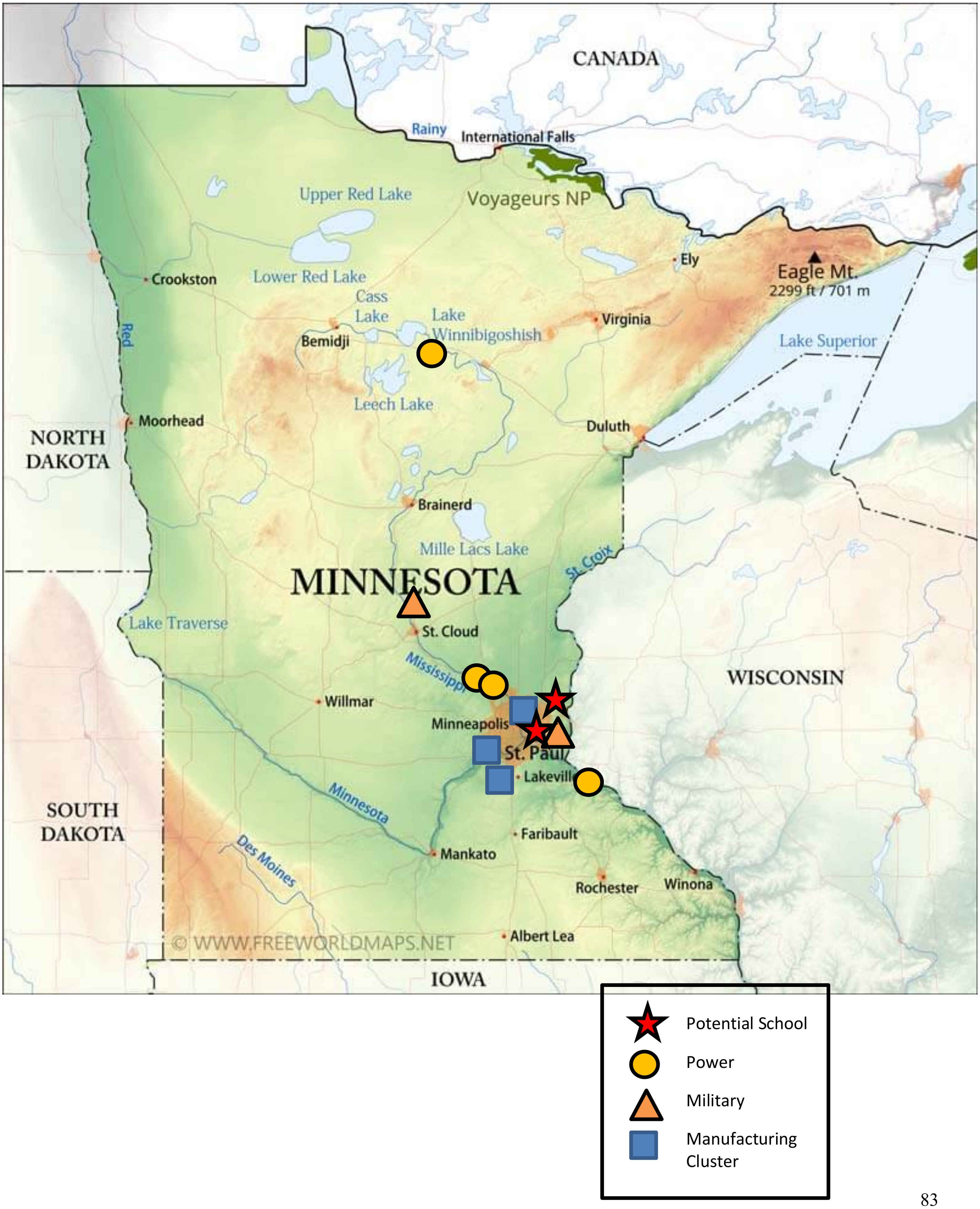
		fundamentals of IT and OT systems, conducting asset inventories for DoD facility-related control systems using the army methodology, and fundamentals of industrial and facility-related control system cyber security.
Wilmington University SCADA Cybersecurity Certificate	Certification	Students learn to monitor and respond to attacks within SCADA systems. The certification curriculum familiarizes students with knowledge of SCADA architecture, risk management and auditing, and security awareness and standards.
Idaho State University Industrial Cybersecurity Engineering Technology	Degree	Students learn to communicate with both industrial operations and IT personnel, ensure safety while performing work orders, maintain ICS device inventory, track evolving risks affecting ICS, aid in conducting cyber security assessments, and update ICS software and firmware.

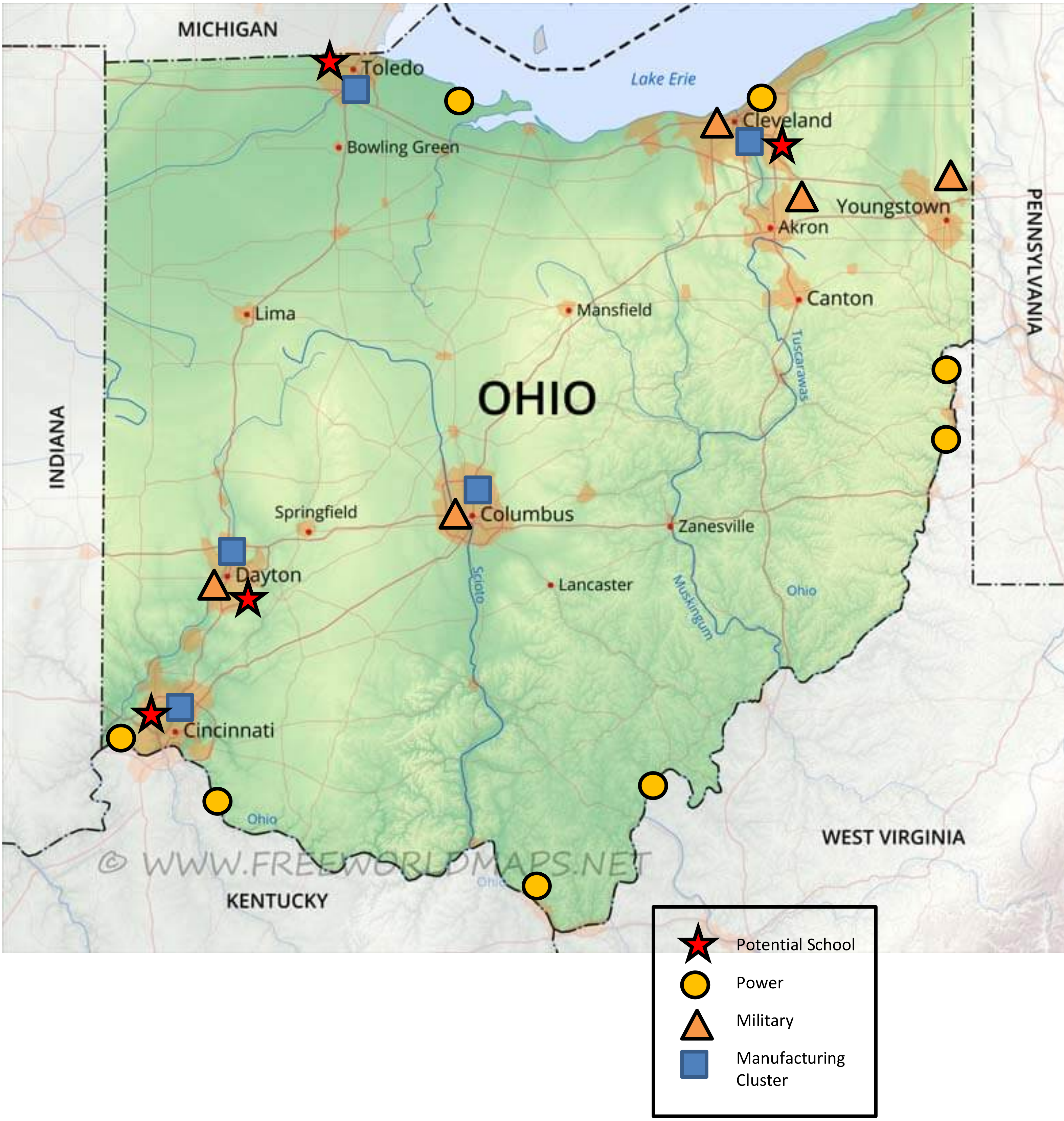
Appendix A4-2: Potential Hub and Spoke Locations in FEMA Region 5

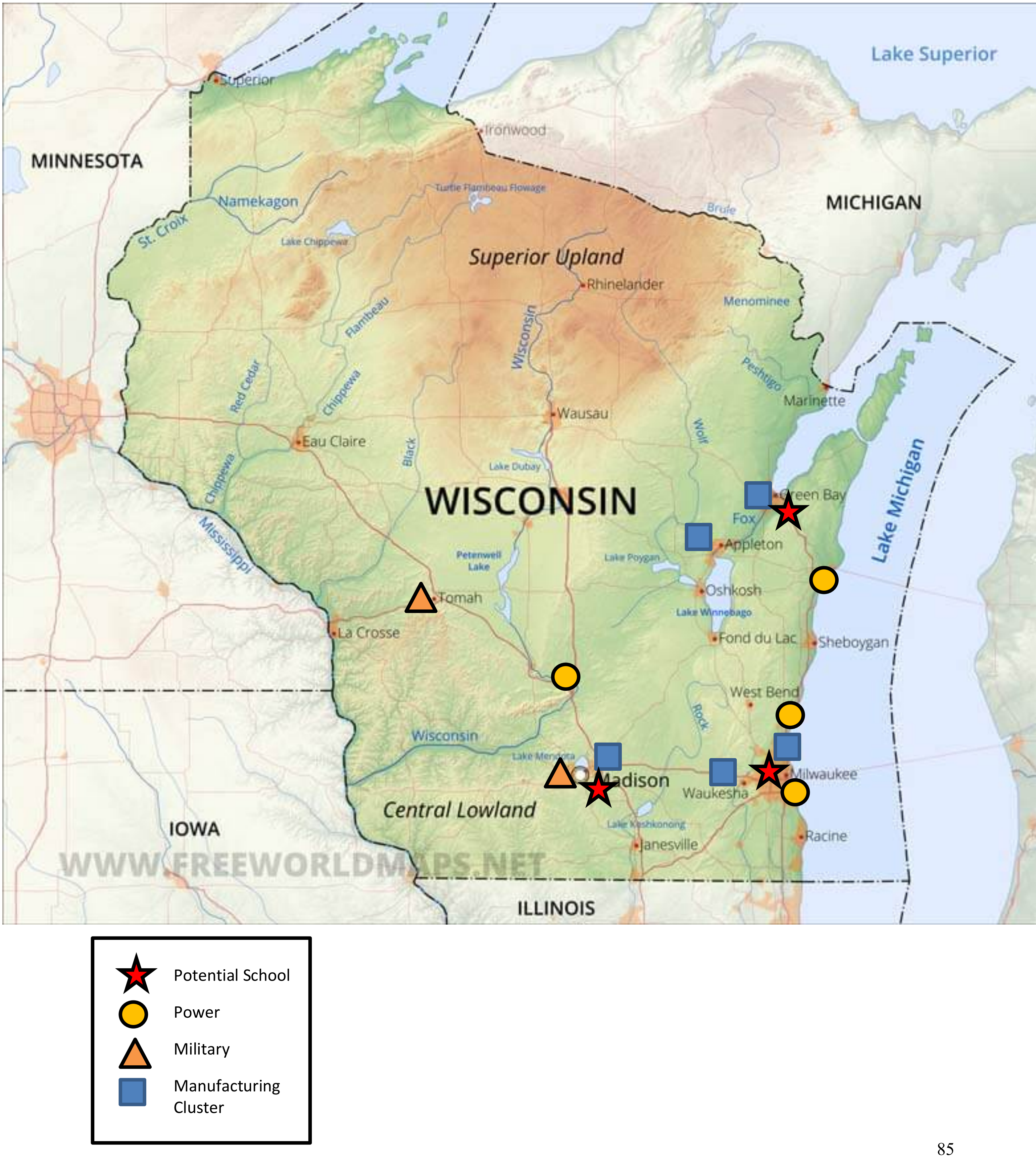



MICHIGAN
South Bend
Elkhart
Gary
Kankakee
Fort Wayne
Wabash
Marion
Kokomo
Lafayette
OHIO
INDIANA
Muncie
Hoosier Hill
1256 ft / 383 m
ILLINOIS
Indianapolis
Richmond
Terre Haute
Bloomington
Ohio
New Albany
KENTUCKY
Evansville
© WWW.FREEWORLDMAPS.NET
Potential School
Power
Military
Manufacturing Cluster


Potential School
Power
Military
Manufacturing Cluster
Mt. Desor
1394 ft / 425 m
Isle Royale NP
Keweenaw Peninsula
Hancock
Lake Superior
CANADA
1979 ft / 603 m
Mt. Arvon
Pictured Rocks NL
Marquette
Ironwood
Porcupine Mts.
Upper Peninsula
Sault Ste. Marie
Iron Mountain
Escanaba
Petoskey
Sleeping Bear Dunes NL
Alpena
Traverse City
Lower Peninsula
Lake Huron
Briar Hill
1706 ft / 520 m
Cadillac
Grooved Hill
1700 ft
WISCONSIN
MICHIGAN
Saginaw
Bay City
Saginaw
Lake Michigan
Muskegon
Grand
Flint
Grand Rapids
Lansing
Pontiac
Lake St. Clair
Kalamazoo
Battle Creek
Ann Arbor
Detroit
Benton Harbor
ILLINOIS
© WWW.FREEWORLDMAPS.NET
INDIANA
OHIO


CANADA
Rainy
International Falls
Upper Red Lake
Voyageurs NP
Ely
Eagle Mt.
2299 ft / 701 m
Crookston
Lower Red Lake
Cass Lake
Lake Winnibigoshish
Virginia
Lake Superior
Bemidji
Red
Leech Lake
Moorhead
Duluth
NORTH DAKOTA
Brainerd
Mille Lacs Lake
St. Croix
MINNESOTA
Lake Traverse
St. Cloud
Mississippi
WISCONSIN
Willmar
Minneapolis
St. Paul
Lakeville
SOUTH DAKOTA
Minnesota
Faribault
Des Moines
Mankato
Rochester
Winona
© WWW.FREEWORLDMAPS.NET
Albert Lea
IOWA
Potential School
Power
Military
Manufacturing Cluster


MICHIGAN
Toledo
Lake Erie
Bowling Green
Cleveland
Youngstown
Akron
Canton
PENNSYLVANIA
Lima
Mansfield
OHIO
Tuscarawas
INDIANA
Springfield
Columbus
Zanesville
Dayton
Lancaster
Scioto
Muskingum
Ohio
Cincinnati
Ohio
WEST VIRGINIA
© WWW.FREEWORLDMAPS.NET
Ohio
KENTUCKY
Potential School
Power
Military
Manufacturing Cluster


Lake Superior
Superior
Ironwood
MINNESOTA
MICHIGAN
Namekagon
St. Croix
Turtle Flambeau Flowage
Lake Chippewa
Brule
Superior Upland
Rhinelander
Menominee
Flambeau
Wisconsin
Red Cedar
Chippewa
Peshtigo
Marinette
Wausau
Wolf
Eau Claire
Black
Lake Dubay
Lake Michigan
WISCONSIN
Green Bay
Fox
Appleton
Chippewa
Mississippi
Petenwell Lake
Lake Poygan
Oshkosh
Tomah
Lake Winnebago
La Crosse
Fond du Lac
Sheboygan
West Bend
Rock
Wisconsin
Lake Mendota
Madison
Milwaukee
Waukesha
Central Lowland
IOWA
Lake Koshkonong
Racine
Janesville
WWW.FREEWORLDMAPS.NET
ILLINOIS
★ Potential School
● Power
▲ Military
■ Manufacturing Cluster

State	Critical Infrastructure* (Electric)**	Military***	Potential Spokes
Illinois	Braidwood Nuclear Generating Station, Braidwood, IL	Scott Air Force Base in St Clair, IL	Illinois Institute of Technology
	Byron Nuclear Generating Station, Ogle County, IL	Rock Island Arsenal Army Base in Arsenal Island, IL	University of Illinois Champaign - Urbana
	Clinton Nuclear Generating Station, Clinton, IL	Camp Price Support Center Army Base in Granite City, IL	University of Chicago
	Dresden Nuclear Power Plant, Morris, IL	Great Lakes Training Center Navy Base North Chicago, IL	Southwestern Illinois University Edwardsville
	LaSalle County Nuclear Generating Station, LaSalle County, IL	Joint Force Headquarters Illinois (IL NG), Springfield, Illinois	
	Quad Cities Nuclear Generating Station, Cordova, IL	Marseilles Training Center, Marseilles, Illinois	
	Baldwin Generating Center, Baldwin, IL		
	Joppa Steam Plant, Joppa, IL		
	Kincaid Generation, Christian County, IL		
	Newton Power Plant, Jasper County, IL		
	Powerton Station, Pekin, IL		
	Prairie State Energy Campus, Marissa		
	Joliet Station, Joliet, IN		

	Kendall County Generation Facility, Minooka, IL		
Indiana	Cayuga, Cayuga, IN	Camp Atterbury Army Base in Edinburgh, IN	University of Notre Dame - SouthBend
	Clifty Creek, Madison, IN	NSWC Crane Division Navy Base in Martin County, IN	Indiana State University - Evansville
	Gibson, Gibson County, IN	Grissom Air Reserve Base Air Force in Kokomo, IN	Valparaiso University - Valparaiso
	Harding St, Indianapolis, IN	Muscatatuck Urban Training Center, Butlerville, IN	University of Southern Indiana - Evansville
	Merom, Merom, IN	Joint Forces Headquarters Indiana, Indianapolis, IN	Indiana University - Purdue University Indianapolis
	Petersburg, Petersburg, IN		Purdue University - Fort Wayne
	Rockport, Rockport, IN		
	R.M. Schafer, Wheatfield, IN		
	Tanner's Creek, Lawrenceburg, IN		
Michigan	Enrico Fermi Nuclear Generating Station, Monroe, MI	Selfridge ANGB Air Force Base in Harrison, MI	University of Michigan - Ann Arbor
	Donald C. Cook Nuclear Power Plant, Bridgman, MI	Detroit Arsenal Army Base in Warren, MI	Michigan State University - Leslie
	Belle River Power Plant, St. Claire, MI	Joint Forces Headquarters Michigan, Lansing, MI	Wayne State - Detroit
	J.H. Campbell Power Plant, Port Sheldon Township, MI	Camp Grayling Joint Maneuver Training Center, Grayling, MI	Grand Rapids Community College
	Monroe Power Plant, Monroe, IN		
	Midland Cogeneration Venture, Midland, MI		
	New Covert Generating Facility, Covert, MI		

	Dan E. Karn 3 & 4, Essexville, MI		
	Ludington Pumped Storage Power Plant, Ludington, MI		
Minnesota	Monticello Nuclear Generating Plant, Monticello, Minnesota	Joint Forces Headquarters Minnesota, Cottage Grove, MN	University of Minnesota Twin Cities
	Prairie Island Nuclear Power Plant, Red Wing, Minnesota	Camp Ripley, Little Falls, MN	Dunwoody College of Technology
	Clay Boswell Energy Center, Cohasset, Minnesota		
	Sherburne County Generating Station, Becker, Minnesota		
Ohio	Davis-Besse Nuclear Plant, Oak Harbor, OH	Wright Patterson Air Force Base in Montgomery, OH	Case Western - Cleveland
	Perry Nuclear Plant, Cleveland OH	Youngstown–Warren Air Reserve Station in Vienna, OH	University of Dayton
	Hanging Rock Energy Facility, Hanging Rock	ISC Cleveland Coast Guard Base in Cleveland, OH	University of Cincinnati
	Cardinal Power Plant, Brilliant, OH	Camp James A. Garfield Joint Military Training Center, Ravenna, OH	University of Toledo
	Gavin Power Plant, Cheshire, OH	Joint Forces Headquarters Ohio, Columbus, OH	
	Kyger Creek Power Plant, Chesire, OH		
	Miami Fort Power Station, North Bend, OH		
	W. H. Sammis Power Plant, Stratton, OH		
	William H. Zimmer Power Station, Moscow, OH		
Wisconsin	Columbia Energy Center, Portage, Wisconsin	Fort Mccoy Army Base, Tomah, WI	University of Wisconsin - Milwaukee

	Elm Road Generating Station, Oak Creek, Wisconsin	Joint Forces Headquarters Wisconsin (WI NG), Madison, WI	Northeast Technical College - Green Bay
	Oak Creek Power Plant, Oak Creek, Wisconsin		Madison Area Technical College - Madison (has a certificate in Cyber Security in an Industrial Control Environment (IoT))
	Port Washington Generating Station, Port Washington, Wisconsin		
	Point Beach Nuclear Plant, Two Rivers, Wisconsin		

*Water treatment/supply was not used as a criteria and this utility is inconsistently regulated and there are hundreds of both public and private water supply assets in each state.

** Electricity over 1000MW Nameplate Capacity.

*** Active duty bases, State NG Headquarters, major NG training installations

Appendix A4-3: Sample Descriptions of Work Roles and Their Mapping

Job Title	Job Description	Requirements	Competencies
OT/ICS Cybersecurity Manager	Directs and oversees the work of industrial cybersecurity for all phases of the plant, product, and system life cycles. The manager interfaces continuously with operations, IT, and cybersecurity personnel.	• Knowledge in: PLC, RTU, DCS, SIS, MES, Historians, HMI, SCADA systems • Knowledge of Windows/UNIX platforms and IT/OT network communication protocols, I.e., TCP/IP, UDP, DNP3, Modbus, IEC 61850, OPC, OPC UA, HART, Foundation Fieldbus, PROFINET • Knowledge in industrial control regulations – NIST SP 800-82, IEC 62443, NERC CIP • Knowledge in leading end-to-end solutions – strategy, design, development, testing, training, implementation • Knowledge in deploying/supporting a variety of cybersecurity practices and technologies, I.e., risk assessments, compliance assessments, vulnerability assessments, antivirus software, firewalls, IDS/IPS, deep packet inspection, SIEM, centralized alert logging/monitoring in ICS environments • Tasks include prioritizing efforts, understanding requirements per effort, obtaining and managing budget, building the team, and running and improving the program.	Written Communication, Workforce Management, Web Technologies, Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Third Party Oversight/Acquisition Management, Technology Awareness, Teaching Others, Systems Testing and Evaluation, Systems Integration, Strategic Planning, Software Testing and Evaluation, Software Development, Risk Management, Project Management, Problem Solving, Presenting Effectively, Policy Management, Organizational Awareness, Interpersonal Skills, Computer Languages, Critical Thinking

		• Organizational and communication skills (written, verbal, presentation, facilitation) • Technical writing; writing progress reports, final deliverable reports, etc. • Knowledge in maintaining and managing NERC CIP compliance requirements, global and regional OT policies, standards, and procedures.	
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	• Master of Science in Electrical, Mechanical, or Computer Engineering • Knowledge of industrial automation, information technology, and cybersecurity. • Knowledge of industrial safety and cybersecurity events including detailed root-cause analysis • Tasks include creation of industrial systems inventory and model for cybersecurity purposes, design physical failsafe’s to counteract potential cyber sabotage, 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, optimize industrial system designs for security effectiveness and efficiency) • Certifications: information systems security, industrial automation	Written Communication, Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Computer Forensics, Computer Languages, Computer Network Defense, Critical Thinking, Data Analysis, Data Privacy and Protection, Interpersonal Skills, Knowledge Management, Mathematical Reasoning, Operating Systems, Organizational Awareness, Presenting Effectively, Problem Solving, Requirement Analysis, Risk Management, Software Development, Software Testing and Evaluation, Strategic

			Planning, System Integration, Technology Awareness, Threat Analysis
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	• Certifications: control systems technician, industrial cybersecurity, basic networking, basic security. • Tasks include 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. • Knowledge of OT terminology and cultures • Knowledge of common security weaknesses in OT environments	Written Communication, Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Computer Network Defense, Critical Thinking, Data Privacy and Protection, External Awareness, Incident Management, Mathematical Reasoning, Operating Systems, Organizational Awareness, Interpersonal Skills, Software Testing and Evaluation, Systems Testing and Evaluation
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,	• Tasks include 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.	Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Mathematical

	options, and recommendations. The analyst works with industrial operations personnel to gain perspective and vet practicality of possible courses of action	• Knowledge in tech-related compliance and risk management frameworks; RMF, NIST 800-53, ISA/IEC 62443, UL CAP, ISO 27001, GDPR, CSL, SOC 2 or other comparable • Technical project management skills using agile methodologies • Problem solving skills • Maintain a library of standardized security and privacy responses to common inquiries, audits, and questions from external sources. • Maintain a current and up-to-date knowledge of security and privacy regulations • Knowledge in cybersecurity risk and technology assessments • Ability to communicate security and privacy requirements and trends to stakeholders/layman people • Technical writing for both internal and external use (different levels of confidentiality) • Monitoring and understanding meaningful technical metrics for compliance	Reasoning, Organizational Awareness, Interpersonal Skills, Software Testing and Evaluation, Systems Testing and Evaluation, Web Technologies, Written Communication, Strategic Planning
Industrial Automation and Control Systems Cybersecurity Specialist/ Senior Associate IT/OT Cybersecurity	Works among enterprise cybersecurity personnel to contextualize and synthesize threats, vulnerabilities, and consequences relevant to industrial environments to provide strategic, tactical, and operational decision	• Knowledge in performing requirements of management or security audits/assessments • Knowledge in and familiarity with information and network security standards • Knowledge in engineering and OT • Knowledge in security control frameworks such as IEC-62443, IACS Cybersecurity standard, NIST CSF, 20 Critical Controls,	Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology

	makers with perspective, options, and recommendations. The analyst works with industrial operations personnel to gain perspective and vet practicality of possible courses of action.	or ISO 27002, or other policies and standards to industrial networking and security • Knowledge in troubleshooting system integration issues and working with security, network, and ICS technologies to implement secure solutions • Understand of security standards of OT/ICS/SCADA system protocols; Knowledge in PLC, HMI, VFD, OT network hardware • PLC and HMI programming software: Siemens Step7, RSlogix 500, Factory Talk, Panel View • Application of NIST 800-82 or others industry standards to ensure proper protections for technical and physician control systems. • Knowledge in developing/implementing a disaster recovery plan • Knowledge in collecting, analyzing, and escalation of security events and knowing what response, if any, is needed (e.g., when critical systems, sensitive data/information is compromised) • Understanding of policies, processes, and controls standardized by cybersecurity regulatory institutions and frameworks, such as the Center for Internet Security (CIS), NIST, etc. where applicable.	Awareness, Mathematical Reasoning, Organizational Awareness, Interpersonal Skills, Software Testing and Evaluation, Systems Testing and Evaluation, Critical Thinking, Computer Language, Web Technologies, Written Communication, Strategic Planning

		• Knowledge in cyber vulnerability assessments, such as pen-testing, real activations, or tabletop IR plan exercises • Communication skills, ability to speak and present information effectively to groups of varying sizes • Interpersonal skills • System admin and support skills in an ICS environment (servers/SCADAs, HMIs, OS, patching systems, disaster recovery, etc.) • Knowledge with Windows, active directory, group policy, DNS, encryption, patch management, anti-virus software, system configuration management • Knowledge in networking constructs, such as LAN, WAN, VPN, routers, firewalls, servers, IDS/IPS, SIEM, DLP, TCP/IP • Knowledge in a variety of OS; Windows server, varying Windows editions, Linux, etc. • Knowledge in Cyber Kill Chain, Diamond Model of Intrusion Analysis • Tasks include ensuring compliance with corporate security standards, providing recommendations to manage risks, act as Subject Matter Expert on ICS/SCADA security related issues, design, implement, monitor, and maintain security controls, ensure security compliance with regulations. • Knowledge of security audits/assessments, information and network security standards,	

		technical skills in engineering and OT, security frameworks such as NIST 800-53 NIST 800-171, NIST 800-82, ISO 2700x, IEC/ISA 62443, and 20 Critical Controls, knowledge in troubleshooting system integration issues, working with security, network, and ICS technologies to implement secure solutions. • Assessing gaps in cybersecurity systems, designs, and implementations • Knowledge in planning, designing, and implementing cyber security controls in an IT/OT system, and having it meet industry standards and guidelines • Knowledge in developing policy and policy recommendations for networks of IT/OT and systems cyber security and compliance controls • Technical writing skills. Developing content rich reports of deliverables with results of subject matter to experts • Knowledge in current cybersecurity/IT/OT technologies, products, and trends • Interpersonal, communication, and verbal skills • Knowledge in types of security architectures and cloud virtualizations. • Knowledge in different OT environments to include cyber defenses across PCN, ICS, and SCADA systems • Solid understanding of cyber security attack surfaces and vectors, method types and their	

		usage in targeted attacks such as phishing, malware implantation, perimeter vulnerabilities, application vulnerabilities, lateral movement, etc. • **IACS:** knowledge in IACS communication protocols, like Siemens, Modbus, Rockwell	
ICS Network Security Engineer/ Senior Industrial Control System Security Engineer		● Knowledge in cybersecurity and/or information security. Designing, configuring, standardizing and, implementing cybersecurity compensating controls OT devices and applications such as RTUs, PLCs, and SCADA. ● Knowledge in control system cyber security certification or training from SANS, CISA, ISA, Infosec, etc. desirable ● Knowledge in one or more of the following: NERC CIP, NIST 800-82, ISA/IEC 62443, NIST Cybersecurity Framework, and FedRAMP. ● Strong troubleshooting and problem-solving skills. ● Excellent interpersonal skills and the ability to work within all levels of the organization. ● Solid Knowledge in networking concepts and project management skills. ● Knowledge in Microsoft-based, complex systems in the security engineering role using the security features of Windows 2008/2012 Server products, Windows 7/10, and SQL Server products.	Interpersonal Skills, Critical Thinking, Systems Testing and Evaluation, Infrastructure Design, Computer Network Defense

		● Knowledge in Tenable Security Center, Forcepoint/Websense DLP, Cisco ASA, Sourcefire, Symantec SEP, Nessus, NMAP, Snort, Burp Suite, or similar products. ● Knowledge of ICS/SCADA design, implementation, and engineering experience ● Knowledge in ISC/SCADA security control architecture, research, development, design, testing and implementation ● Knowledge in networking with a strong understanding of network communication protocols (IPv4, IPv6, Modbus, BACnet, etc.)	
SCADA Cybersecurity Solutions Architect	Development of secure architecture and design patterns for industrial control systems, SCADA, and other grid/operational technology environments.	● Knowledge in designing and implementing complex solutions in an enterprise network, according to specific requirements. ● Knowledge in network security, industrial control system security, cloud-based security. ● Communication (verbal, facilitative) and interpersonal skills with solutions/systems architect ● Knowledge in security control frameworks; Critical Security Controls, OWASP, NIST Cybersecurity Framework, NIST 800 series ● Knowledge with operational support for networks, systems, applications, databases. ● Knowledge in Identity and Access Management Systems, applied cryptography, and firewalls.	Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Problem Solving, Critical Thinking, Computer Languages, Computer Forensics, Computer Network Defense, Conflict Management, Data Privacy and Protection, Information Systems/Network Security, Information Technology Assessment, Intelligence Analysis, Interpersonal Skills, Strategic Planning, Organizational Awareness, Software Testing

		● Vulnerability analyses, including pen-testing of networks and web applications, and understanding of red team experiences. ● Knowledge in utilizing cyber tools to perform cybersecurity controls assessments of IT/OT solutions. ● Programming proficiency, ideally in languages like C, C++, Java, JavaScript, & Python	and Evaluation, Software Development, Operating systems, Problem Solving, Software Testing and Evaluation, Teaching Others, Technology Awareness, Telecommunications, Threat Analysis, Web Technology, Written Communication
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.	● Understanding of Distributed control systems (DCS) and supervisory control & data ● Tasks include Describes and characterizes systems, designs and conducts tests, discovers vulnerabilities, develops adversarial perspective, recommends mitigations, documents and reports findings	Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Written Communication Web Technology, Threat Analysis, Telecommunications, Teaching Others, Project Management, Operating Systems, Oral Communication, Organizational Awareness, Problem Solving, Interpersonal Skills, Presenting Effectively, Critical Thinking, Computers and Electronics, Computer Languages, Computer Network Defense, Software Testing and Evaluation, Systems

			Testing and Evaluation, Requirements Analysis
ICS/OT Consultant	Helps clients assess and strengthen ICS/OT security capability and work to continually improve assessment methodologies	● Ability to manage multiple projects at once, most likely under different companies with different contexts ● Project management skills to plan, track, and report on progress ● Technical writing: comprehensive and accurate reports for both technical and executive audiences. ● Understanding of IT/OT network communication protocols; TCP/IP, UDP, DNP3, Modbus, IEC 61850, OPC, OPC UA, PROFINET, etc. ● Understanding of operational technologies, like Program Logic Controllers, SCADA software, Distributed control systems ● Understanding of processes regarding security event analysis, IR, computer forensics, malware analysis, misc. security operations ● Understanding of cybersecurity operations, event monitoring, SIEM tools ● Familiarity of UNIX/Windows OS and administrative tools ● Familiarity of security controls for common platforms and devices (Windows, UNIX, Linux, PLCs, controllers, network equipment)	Project Management, Software Development, Risk Management, Strategic Planning, System Testing and Evaluation, Technology Awareness, Infrastructure Design, Risk Management, Legal, Government, and Jurisprudence, Information Systems/Network Security, Vulnerabilities Assessment, Computer Languages, Oral Communication, Technology Awareness, Asset/Inventory Management, Business Continuity, Collection Operations, Computer Languages, Computer Network Defense, Computers and Electronics, Conflict Management, Critical Thinking Data Analysis, Data Management, Database Management Systems, Data Administration, Incident Management, Identity Management, Incident Management, Information Systems/Network Security,

			Information Technology Assessment, Knowledge Management, Interpersonal Skills, Mathematical Reasoning, Network Management, Operating Systems, Operations Support, Operations Support, Oral Communication, Organizational Awareness, Policy Management, Problem Solving, Written Communication, Vulnerabilities Assessment, Threat Analysis

Appendix A4-4: References

The following documents were consulted in the preparation of this report.

(ISC)^2. (2020) *Exploring Cybersecurity in Industrial Control Systems*. ISC2. https://www.isc2.org/Development/Immersive-Courses/Exploring-Cybersecurity-in-Industrial-Control-Systems.

(ISC)^2. (2020). *Cybersecurity Professionals Stand Up to a Pandemic (ISC)2 CYBERSECURITY WORKFORCE STUDY*. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

Accenture. (2020). *Lessons from leaders to master cybersecurity execution*. https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

AGA. (2006). *AGA-12 Cryptographic Protection of SCADA Communications*. http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/AGA%20-%20Cryptographic%20Protection%20of%20SCADA%20Communications%20-%2012%20Part1.pdf

API. (2009). *API STD 1164: Pipeline SCADA Security*. https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%201164&item_s_key=00451686

APTA. (2010). *Securing Control and Communications Systems in Transit Environments*. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-001-10.pdf

Ausherman, N. (2019). *Five steps to Reduce Cyber Risks* [Text]. NIST. https://www.nist.gov/mep/cybersecurity-resources-manufacturers/where-start

Bossier Parish Community College. (n.d). *Industrial Control Systems, CTS*. BPCC. http://catalog.bpcc.edu/preview_program.php?catoid=4&poid=470&returnto=221.

Brunner, C. (2008). *IEC 61850 for power system commun... Preview & related info | Mendeley*. https://www.mendeley.com/catalogue/21092a74-bb1b-3dde-a4b8-9e41a8461f51/?utm_source=desktop&utm_medium=1.19.4&utm_campaign=open_catalog&userDocumentId=%7B330cfebd-92d8-3a2f-a6da-aaf8a73dc144%7D

Chenoweth, J., Green, J., Shaw, T., Shinn, M., & Simonds, G. (2014). *The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power React*. NRC Web. Retrieved February 3, 2021, from https://nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7141/index.html

CISA. (2007). *Chemical Facility Anti-Terrorism Standards | CISA*. https://www.cisa.gov/chemical-facility-anti-terrorism-standards

CISA. (2009). *Risk-Based Performance Standards (RBPS) | CISA*. https://www.cisa.gov/risk-based-performance-standards

Clark State. (n.d). *Supervisory Control and Data Acquisition (SCADA) Departmental Certificate*. ClarkState. (n.d). https://www.clarkstate.edu/academics/degrees-and-certificates/engineering-manufacturing-and-mechanical-services/supervisory-control-and-data-acquisition-scada-departmental-certificate/.

CloudPassage (2016). "CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education," https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

Conway, T., Gutierrez, T., & Sims, S. *ICS456: Essentials for NERC Critical Infrastructure Protection*. SANS. https://www.sans.org/cyber-security-courses/essentials-for-nerc-critical-infrastructure-protection/.

Crumpler, W. C., & Lewis, J. L. (2019). *The Cybersecurity Workforce Gap*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

CSC. (2020). *Cyberspace Solarium Commission—Report*. Solarium.Gov. https://www.solarium.gov/report

CSIS (2016) *Hacking the Skills Shortage.* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.

Cybersecurity & Infrastructure Security Agency. (n.d). *Training Available Through CISA*. CISA. https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT.

Cybersecurity Ventures & Herjavec Group. (2019). *The 2019/2020 Official Annual Cybersecurity Jobs Report*. Cybersecurity Ventures. https://www.herjavecgroup.com/wp-content/uploads/2019/10/HG-CV-2019-Cybersecurity-Jobs-Report.pdf

Cybersecurity Ventures. (2020). *Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021*. Steve Morgan. https://cybersecurityventures.com/annual-cybercrime-report-2020/

Cyberseek (2021). Cybersecurity Supply/Demand Heat Map. https://www.cyberseek.org/heatmap.html

DHS/TSA. (2018). *Pipeline Security Guidelines [March 2018]* [Article]. United States. Transportation Security Administration. Homeland Security Digital Library; United States. Transportation Security Administration. https://www.hsdl.org/?abstract&did=

Dolezilek, D. (2006). IEC 61850: What You Need to Know About Functionality and Practical Implementation. *2006 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, 1–17. https://doi.org/10.1109/PSAMP.2006.285368

Dunwoody College of Technology. (n.d). *Industrial Controls (ICOT), Certificate*. Dunwoody. https://catalog.dunwoody.edu/catalog-student-handbook/academic-programs/robotics-manufacturing/industrial-controls-robotics-icon-certificate/.

Dunwoody College of Technology. (n.d). *Industrial Controls & Robotics (ICON), AAS*. Dunwoody. https://catalog.dunwoody.edu/catalog-student-handbook/academic-programs/robotics-manufacturing/industrial-controls-robotics-icon-aas/.

Evans and Reeder (2016). A Human Capital Crisis in Cybersecurity. *Technical Proficiency Matters*. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency

EWE. (2010). *Process Control Domain—Security Requirements for Vendors*. http://osgug.ucaiug.org/conformity/security/Shared%20Documents/WIB%20M2784%20PCS%20VendorSecurity%20v2.pdf

GAO. (2020). *Passenger Rail Security*. https://www.gao.gov/assets/710/705684.pdf

GIAC Certifications. (n.d). *Cyber Security Certification: GRID* . GIAC. https://www.giac.org/certification/response-industrial-defense-grid?msc=giac-focus-area.

GIAC Certifications. (n.d). *GIAC Critical Infrastructure Protection (GCIP)*. GIAC. https://www.giac.org/certification/critical-infrastructure-protection-gcip?msc=giac-focus-area.

GIAC Certifications. (n.d). *Global Industrial Cyber Security Professional (GICSP)*. GIAC. https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp?msc=giac-focus-area.

Hernández, E., Whitesell, T., & Wyszczelski, K. (2020). *A Practical Guide to Substation T... Preview & related info | Mendeley*. https://www.mendeley.com/catalogue/560be3c0-9f5f-3ba8-89cfc9ff5106b214/?utm_source=desktop&utm_medium=1.19.4&utm_campaign=open_catalog&userDocumentId=%7Bb12f1d50-76a0-3900-a9cb-67e6a29f7739%7D

IBM Security. (2020). *X-Force Threat Intelligence Index*. https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf

Idaho National Laboratory. (2004). *A Comparison of Oil and Gas Segment Cyber Security Standards*. 27.

IEEE, S. A. (2014). *IEEE 1686-2013—IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*. https://standards.ieee.org/standard/1686-2013.html

IEEE, S. A. (2017). *P1686—Standard for Intelligent Electronic Devices Cyber Security Capabilities*. https://standards.ieee.org/project/1686.html

Indiana State University. (n.d). *Automation and Control Engineering Technology (ACET)*. IndState. https://www.indstate.edu/technology/acet.

International Society of Automation. (n.d). *Control Systems Engineer (CSE) Licensure Preparation*. ISA. https://www.isa.org/training-and-certification/isa-certification/cse-licensure-preparation.

International Society of Automation. (n.d). *Control Systems Training*. ISA. https://www.isa.org/training-and-certification/isa-training/control-systems-training.

International Society of Automation. (n.d). *ISA Certified Automation Professional® (CAP®) Certification Program*. ISA. https://www.isa.org/training-and-certification/isa-certification/cap.

International Society of Automation. (n.d). *ISA Certified Control Systems Technician® (CCST®)*. ISA. https://www.isa.org/training-and-certification/isa-certification/ccst.

ISA. (2016, December). *ISA99, Industrial Automation&Control Sys Security- ISA*. Isa.Org. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

ISACA, "State of Cybersecurity (2018) Part 1: Workforce Development," http://www.isaca.org/Knowledge-Center/ Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF?regnum=458196.

ISO. (2005, June). *ISO/IEC 17799:2005 Information technology—Security techniques—Code of practice for information security management*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/96/39612.html

ISO. (2013, October). *ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls*. Iso.Org. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54533.html

ISO/IEC 27002 code of practice. (n.d.). Retrieved February 3, 2021, from https://www.iso27001security.com/html/27002.html

ITI Technical College. (n.d). *Instrument & Control Systems Technology (AOS)*. ITICollege. https://www.iticollege.edu/our-programs/instrument-control-systems-technology/.

Kaspersky Industrial CyberSecurity. (2018). *The State of Industrial Cybersecurity 2018 | Kaspersky Industrial CyberSecurity*. Kaspersky Industrial CyberSecurity | Holistic Approach to Industrial Cybersecurity. https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/

Lee College. *Industrial Systems Technician*. (n.d). Lee. https://www.lee.edu/programs/industrial-systems/.

Lee, R. M. (n.d). *ICS515: ICS Active Defense and Incident Response*. SANS. https://www.sans.org/cyber-security-courses/industrial-control-system-active-defense-and-incident-response/.

Louisiana Tech University. (n.d). *Instrumentation and Control Systems Engineering Technology*. LATech. https://coes.latech.edu/undergraduate-programs/instrumentation-and-control-systems-engineering-technology/.

Mallory, P. (2019). *NIST CSF: Risk Management Framework—Infosec Resources*. https://resources.infosecinstitute.com/topic/nist-csf-risk-management-framework/

Markets and Markets. (2020). *Industrial Control Systems (ICS) Security Market*. https://cdn.livechat-files.com/api/file/lc/att/11766279/6eafd432601317445b2e183e308e9e2d/B&S%20-%20ICS%20Security%20Market%20-%20Global%20Forecast%20to%202025.pdf

Mid-State Technical College. (n.d). *Industrial Automation & Controls Engineering Technology*. MSTC. https://www.mstc.edu/programs/industrial-automation-controls-engineering-technology.

Millersville University. (n.d). *Robotics & Control Systems Technology Degree Requirements*. Millersville. https://www.millersville.edu/aest/degrees/more/rcs-req.php.

National Council of Examiners for Engineering and Surveying. (n.d). *PE Control Systems Engineering exam*. NCEES. https://ncees.org/engineering/pe/control-systems/.

National Initiative for Cybersecurity Education. (2017) "Workshop on Cybersecurity Workforce Development: Notes from Panel Discussions." https://www.nist.gov/sites/default/files/documents/2017/09/28/chicago_workshop_summary_notes.pdf

NEI. (2010). *NEI 08-09 [Rev. 6] Cyber Security Plan for Nuclear Power Reactors*.

NERC. (2010). *CIP-002-4*. https://www.nerc.com/pa/Stand/Pages/CIP0024RI.aspx

NERC. (2010). *CIP-005-4a*. https://www.nerc.com/pa/Stand/Pages/CIP0054aRI.aspx

NERC. (2011). *CIP-003-4*. https://www.nerc.com/pa/Stand/Pages/CIP0034RI.aspx

NERC. (2011). *CIP-004-4*. https://www.nerc.com/pa/Stand/Pages/CIP0044RI.aspx

NERC. (2011). *CIP-006-4c*. https://www.nerc.com/pa/Stand/Pages/CIP0064cRI.aspx

NERC. (2011). *CIP-007-4b*. https://www.nerc.com/pa/Stand/Pages/CIP0074bRI.aspx

NERC. (2011). *CIP-008-4*. https://www.nerc.com/pa/Stand/Pages/CIP0084RI.aspx

NERC. (2011). *CIP-008-4*. https://www.nerc.com/pa/Stand/Pages/CIP0084RI.aspx

NERC. (n.d.). *CIP Standards* [Nerc.com]. Retrieved February 3, 2021, from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Nguyen, C. T., Gopstein, A. M., Byrnett, D. S., Worthington, K., & Villarreal, C. (2020). *Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report*. https://www.nist.gov/publications/framework-and-roadmap-smart-grid-interoperability-standards-regional-roundtables

NIS, S. N. S. W. (2012). *Considerations for The Incorporation of Cyber Security in Development of Industry Standards*.

NIST, I. T. L. (2006). *Minimum Security Requirements for Federal Information and Information Systems* (Federal Information Processing Standard (FIPS) 200). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.200

NIST, I. T. L. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Standards NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

NIST. (2013). *Cybersecurity Framework*. NIST. https://www.nist.gov/cyberframework

NIST. (2019, November 5). *OSCAL*. Https://Pages.Nist.Gov/OSCAL/. https://pages.nist.gov/OSCAL/

North Iowa Area Community College. (n.d). *Industrial Systems Technology, A.A.S.* NIACC. http://catalog.niacc.edu/preview_program.php?catoid=8&poid=1330.

NSA, C. S. S. (n.d.). *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)*. NSA/IAD. Retrieved February 3, 2021, from https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/a-framework-for-assessing-and-improving-the-security-posture.cfm

O.T. and ICS Security. (2020). *The Next Big Challenge*. Balbix. https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge/

Parsons. (2018). *Critical Infrastructure Risk Assessment*. Industrial Control Systems Cybersecurity: Survey of Engineering and Operational Technology Professionals. Parsons.Com. https://www.parsons.com/cipsurvey/

RISSB. (2018). *Rail Cyber Security*. https://scadahacker.com/library/Documents/Standards/Au-RISSB%20-%20AS-7770%20-%20Rail%20Cyber%20Security%20v2.0.pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST Special Publication (SP) 800-171 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r2

Savannah Technical College. (n.d). *Industrial Maintenance Systems Technology Degree*. SavannahTech. https://www.savannahtech.edu/programs/industrial-systems-associate-degree/.

Scarfone, K., Tibbs, C., & Sexton, M. (2010). *Guide to Securing WiMAX Wireless Communications* (NIST Special Publication (SP) 800-127 (Withdrawn)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-127

Searle, J. (n.d). *ICS410: ICS/SCADA Security Essentials*. SANS. https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/.

Steve Sharkey, Drew Morin, and John Hunter. (2017) "*Comments of T-Mobile USA, Inc.*", https://www.nist.gov/sites/default/files/documents/2017/08/04/t-mobile.pdf

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. https://www.nist.gov/publications/risk-management-guide-information-technology-systems

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. https://www.nist.gov/publications/risk-management-guide-information-technology-systems

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication (SP) 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

The Business Research Company. (2020, December). *Cybersecurity Services Market Opportunities and Strategies*. https://www.thebusinessresearchcompany.com/report/cybersecurity-services-market

Tonex Technology and Management Training Courses and Seminars. (n.d). *SCADA Training | SCADA Course*. Tonex. https://www.tonex.com/training-courses/scada-training/.

Tripwire. (2019). *Tripwire State of Industrial Cybersecurity Report*. https://www.tripwire.com//media/tripwiredotcom/files/research/dimensional-research-ics-security-report-survey-201910-d4.pdf?rev=b68fd7ada923479488396bf6ab51c37d

Turk, Robert J., (2005) *Cyber Incidents Involving Control Systems*. United States. https://doi.org/10.2172/911775

U.S. Government Publishing Office (2017). *Reviewing Federal I.T. Workforce Challenges and Possible Solutions. https://www.govinfo.gov/content/pkg/CHRG-115hhrg25717/html/CHRG-115hhrg25717.htm*

University of Wisconsin Platteville. (n.d). *Industrial Control Systems Technology Minor*. UWPlatt. https://catalog.uwplatt.edu/undergraduate/business-industry-life-science-agriculture/industrial-studies/industrial-control-systems-technology-minor/.

Waketech Technical Community College. (n.d). *Electronics Engineering Technology Certificates*. Waketech. https://www.waketech.edu/programs-courses/credit/electronics-engineering-technology/degrees-programs/certificates.

Whatcom Community College. (n.d). *Degree & Certificates*. Whatcom. https://www.whatcom.edu/academics/degrees-certificates/bachelor-of-applied-science-it-networking-cybersecurity/degree-certificates#CertP - industrial control systems.

Wichita State. (n.d). *Details: Cyber Physical Systems, Undergraduate Certificate*. Wichita.

Wilmington University. *Graduate Certificate in SCADA Cybersecurity*. Wilmu. https://www.wilmu.edu/technology/scada-cyber-security.aspx.