CERIAS

The Center for Education and Research in Information Assurance and Security

Curriculum Guidance for Industrial Control System Security

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

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 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

Figure 1: ICS Concept Map

Program Structure for ICSS

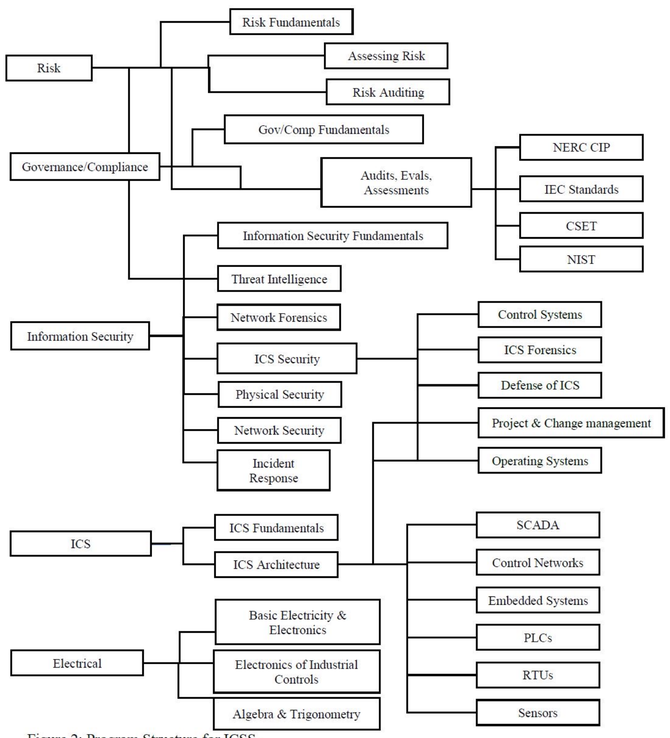

Figure 2: Program Structure for ICSS

CSS 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

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

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
Workforce/Soft skills	Technical Writing	
	Project Management	
	Organizational Communication	

Table 4: Major Topics in ICSS

For additional information regarding this research, please contact Douglas Rapp at rapp1@purdue.edu

PURDUE UNIVERSITY Discovery Park

CERIAS