SCADA Cybersecurity Education
from a Curriculum and Instruction Perspective

R. T. Albert

1Professional Management Division, University of Maine at Fort Kent, Fort Kent, ME, USA

Abstract – Concerns over the cybersecurity risks associated with Supervisory Control and Data Acquisition (SCADA) components used to manage significant utility infrastructures have continued to rise. Educational institutions have been called upon to prepare a workforce that is sensitive to such concerns and able to effectively address them. Recognition of the absence of a consistent approach by such institutions to provide such education served as the impetus for this study. The aim of this study was to elucidate the role of SCADA in curriculum standards relating to cybersecurity, provide examples of SCADA instructional approaches, and offer recommendations as to which may work best in a typical public undergraduate university setting. The purpose of this paper is to share approaches and recommendations for addressing SCADA cybersecurity education from a curriculum and instruction perspective.

Keywords: SCADA, Cybersecurity, Education, Information Security Education, Curriculum

1 Introduction

Concerns over the cybersecurity risks associated with Supervisory Control and Data Acquisition (SCADA) components used to manage significant utility infrastructures have been widely reported [1-4]. The vulnerability to attack exhibited by SCADA components is due in large part to the lack of authentication and confidentiality controls in the SCADA protocols themselves. Physical security of SCADA remote terminal units (RTUs) further aggravates the situation. Cybersecurity risks continue to mount with each report of the potential for loss of a critical infrastructure.

A recent confidential power-flow analysis by the Federal Energy Regulatory Commission was reported as revealing the United States could suffer a coast-to-coast blackout if just nine of the country’s 55,000 electric-transmission substations were knocked out in a coordinated attack. The possibility for a nation-wide blackout lasting for weeks or months has also been reported. The analysis triggered increased interest in tightening physical security through imposition of security standards. Efforts to squelch public disclosure of such reports are increasing in frequency as various agencies [5, 6] and companies [7] fall back to “security through obscurity” in an attempt to sure up weak SCADA cybersecurity. Concomitantly, the need to raise awareness, knowledge and skills of those charged with the cybersecurity of SCADA systems has become increasingly pronounced.

Educational institutions have been called upon to prepare a workforce that is sensitive to the cybersecurity risks associated with SCADA components and able to effectively address them. One of the great impediments to progress in this regard has been the absence of a consistent approach by such institutions to provide such education. Several factors have contributed to the exacerbation of the problem. Absence of a consistent approach by such institutions to provide such education served as the impetus for this study.

The aim of this study is to elucidate the role of SCADA in curriculum standards relating to cybersecurity, provide examples of SCADA instructional approaches, and offer recommendations as to which may work best in a typical public undergraduate university setting.

The aim of this study is to elucidate the role of SCADA in curriculum standards relating to cybersecurity, provide examples of SCADA instructional approaches, and offer recommendations as to which may work best in a typical public undergraduate university setting. The purpose of this paper is to share approaches and recommendations for addressing SCADA cybersecurity education from a curriculum and instruction perspective in hopes of furthering a more consistent and effective approach to addressing SCADA cybersecurity education.

2 The Role of SCADA in Curriculum Standards

The current ambiguous state of SCADA cybersecurity in curriculum standards is due to many factors. For example, differences continue to exist in the opinions and interpretations of cybersecurity as a concept. Another example is the ongoing development of control system security standards by many professional organizations. Some of these organizations have made great strides. In a similar sense, the emergence of Information Security and Assurance as an academic entity and, concomitantly, the identification of a suitable accrediting body, remain in flux. Still other factors have slowed the advancement of SCADA cybersecurity education, not least of which is formation of a consensus on the best placement of the broader cybersecurity curriculum within established academic programs.

Rowe [8] argues that Information Technology programs are “uniquely best-suited to an advanced cybersecurity curriculum” (p. 115) since the core “pillars” serve as pre-requisites for cybersecurity. Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS) has made substantial contributions to the broader discussion of the role of security education within computing programs but the wide-spread adoption of their
recommendations relating to the use of a layered approach to cybersecurity, remains to be realized. This is likely due in part to the inherent cross-disciplinary nature of cybersecurity concepts.

The cross-disciplinary nature of SCADA cybersecurity education, falling between curriculum standards, as it were, has limited full recognition and adoption in any single domain. For example, SCADA systems coverage has been addressed in numerous ways in undergraduate mechanical engineering and mechatronics education programs, as cited by Senk [9]. In some instances, SCADA cybersecurity has been identified for inclusion in curriculum to better meet new competencies demanded by the workplace market [10]. In other instances, only partial coverage, such as the “availability” of system functions aspects of SCADA cybersecurity are promoted, according to Papa [11]. More often than not, the focus of such coverage has not been on cybersecurity aspects of SCADA systems. Collectively, such factors can retard the advancement of SCADA cybersecurity education. Nevertheless, progress continues and SCADA is becoming more pronounced in curriculum standards.

Government and societal norms, economic, political, technological, environmental, and audience diversity are among the numerous factors that should be considered when shaping curricula. Each curriculum standard/guideline development entity also takes into account its own particular audience needs (e.g., professional certification requirements).

2.1 SCADA and ACM/IEEE Curriculum Standards

The most recent 2013 Association of Computing Machinery (ACM)/Institute of Electronic and Electrical Engineers Computer Society (IEEE) Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (2013) [12] are a reflection of the evolution of the field over many decades. The guiding principles followed in its development are similar to those followed by other curriculum development entities. Included among these principles are:

- “Computer science curricula should be designed to provide students the flexibility to work across many disciplines.” (p. 20)
- “Computer science curricula should be designed to prepare graduates for a variety of professions, attracting the full range of talent to the field.” (p. 21)
- Curricular guidelines “must be relevant to a variety of institutions”(p. 21)
- Curricular guidelines “should provide the greatest flexibility in organizing topics into courses and curricula.” (p. 21)

A three-tiered classification of a “Body of Knowledge Units” was identified (Core Tier 1 – Essential topics, Core Tier 2 – Important topics, Electives). A very similar classification approach has most recently been used by the National Security Agency (NSA)/Department of Homeland Security (DHS) in its establishment of criteria for recognition of Centers of Academic Excellent in Information Assurance/Cyber Defense (CAE-IA/CD) [13]. In addition, three levels are identified for depth of coverage in a topic (Knowledge, Application and Evaluation).

For the first time, Information Assurance and Security (IAS) are recognized as a knowledge area and have been added to the body of knowledge “in recognition of the world’s reliance on information technology and its critical role in computer science education.” (p. 97). IAS is identified as unique among the set of knowledge areas “given the manner in which the topics are pervasive throughout other knowledge areas.” (p. 97). IAS concepts are classified in all three tiers and are widely dispersed. Over 30 hours of coverage are associated with each of Core Tier 1 and Core Tier 2. Cross-core coverage supports the potential value of a modular instructional approach.

No specific reference to SCADA cybersecurity exists in the ACM/IEEE Computer Science (CS) Curriculum Guidelines, however, the concepts essential to developing knowledge and skills in SCADA cybersecurity are present. This suggests that SCADA cybersecurity education might best be addressed within computer science programs through use of an “exemplar” approach in which topics/outcomes are presented/achieved through exploration of their value in the context of SCADA cybersecurity design and operations.

Information Technology (IT) is the newest computing discipline covered by the ACM/IEEE computing curricula recommendations [14]. These recommendations are also evolving and are presented in a separate volume. Nevertheless, information assurance and security is identified as overarching the IT pillars including programming, networking, human-computer interaction, databases, and web systems. One of the guiding principles used in the development of the IT curriculum guidelines is “The curriculum must reflect those aspects that set Information Technology apart from other computing disciplines” (p. 22). By earlier recognition and inclusion of IAS in its curriculum guidelines, it could be argued that IAS is more aligned with IT than CS. This would be a mistake given the ever-evolving nature of these curricular guidelines and the apparent influence this earlier inclusion has had on the more recent CS curriculum guidelines.

2.2 Critical Infrastructure and Control Systems Security Curriculum

The model proposed in the Critical Infrastructure and Control Systems Security Curriculum [15] is very comprehensive. The model is presented as a collection of
modules that tend to emphasize policy aspects of the management of critical infrastructure and control systems. Nevertheless, its modularity aids the adoption of components that are well suited to a variety of educational contexts, particularly those at the masters degree level. “The curriculum focuses primarily on the role of control systems in energy, cyber, and other infrastructures [and] provides materials from which instructors can design a specific syllabus to meet the needs and requirements of their particular circumstances.” (p. 1) [15]

2.3 SCADA and NSA/DHS CAE-IA/CD Recognition Guidelines

The NSA/DHS have established criteria for recognition of Centers of Academic Excellent in Information Assurance/Cyber Defense (CAE-IA/CD). These criteria have evolved substantially over the past few years and currently include “Industrial Control Systems/SCADA Security” as a “specialty area” that educational institutions may optionally be assessed against in their application for NSA/DHS recognition [13].

On one hand, inclusion of SCADA security among the criteria may be viewed as beneficial to the cause. On the other hand, however, relegating it to the status of an optional specialization area may be viewed as detrimental.

Collectively, these curriculum standards, particularly the inclusion of SCADA as an identified component, aid in directing the evolution of academic program curricula and instructional practices. The evolution of the curriculum standards themselves is driven by industry and societal needs. As these needs become more pronounced, the rate of evolutionary advancement will likely increase. In the interim, identification of demonstrably effective instructional approaches is left to those instructional staff engaged in the scholarship of teaching and learning.

Based on the legacy work of Ernest Boyer's Scholarship Reconsidered [16], the scholarship of teaching and learning has been variously defined as promoting “teaching as a scholarly endeavor and a worthy subject for research, producing a public body of knowledge open to critique and evaluation. Its intent is not only to improve teaching but also to create a community of ‘scholarly teachers’ who add to the body of knowledge about teaching and learning as well as benefiting from the SoTL research of others” [17].

3 SCADA Instructional Approaches

SCADA instructional approaches exist in many forms. Variability due to differences in student learning objectives and student characteristics is to be expected. So too is variability due to experimentation with various instructional approaches. Those instructors engaged in the scholarship of teaching and learning may best exemplify such active experimentation. Variability then is expected, natural and demonstrative of the potential for instructional advancement.

Consistency in the application of instructional approaches demonstrated to be effective is essential to adequate preparation of the cybersecurity workforce. It is also essential to addressing the concerns over cybersecurity risks associated with SCADA components used to manage significant utility infrastructures. Until such time the role of SCADA cybersecurity becomes precisely and prominently defined in curriculum standards, consistency of adoption of demonstrably effective instructional strategies will remain an elusive goal. Sheen has argued the extent to which SCADA system security is currently incorporated into computing disciplines varies from little to none [18]. To date, different SCADA cybersecurity instructional strategies have, nevertheless, shown promise.

Note the following sample of instructional approaches represents a variety of approaches that have been studied. These approaches are not mutually exclusive but often complementary when appropriately adopted and implemented.

3.1 Modular Approach

Guillermo [19] reported on a modular approach to incorporation of SCADA cybersecurity education that is intended to “… augment an existing course on critical infrastructure with slightly advanced technological and information security-related materials without overwhelming non-computer science students” (p. 55). The modules and course learning outcomes focus on critical infrastructure and control systems (CICS) security. Four modules are presented for consideration.

- CICS Technology
- Exploration of Prominent CICS Security Standards and Vulnerability Assessment
- CICS Risk Assessment and Mitigation Techniques
- CICS Security Policies

The value and role of supportive laboratories and lab activities are also addressed as is the ongoing work with development of a Critical Infrastructure Security and Assessment Laboratory (CISAL). The introduction of laboratory activities into the curriculum is identified a major challenge [19].

Perhaps the greatest promise to the value of this approach lies in the potential to adopt modules as supplements to other courses pertaining to information security, risk management, and emergency preparedness. Recognition of the multi-disciplinary nature of SCADA cybersecurity is a key to advancement.
3.2 Hands-On Toolkit/Laboratory Testbed Approach

Experiential methods of teaching are widely known to be appropriate and effective. Such methods are perhaps most effective with learners who learn best through application of knowledge and skills. No SCADA cybersecurity instructional approach exhibits more variety than those focused on the provision of hands-on laboratories and laboratory exercises. Numerous approaches have been explored and reported, some of which are included here as exemplars.

Guillermo [20] discusses the design and implementation of a Critical Infrastructure Security and Assessment Laboratory (CISAL) as an approach to augment the National SCADA Test Bed (NSTB) at the Idaho National Laboratory. The intent behind establishment of the CISAL facility was to “… simulate research and education in the STEM disciplines by providing a facility that is openly accessible to the academic community.” (p. 74). The value of such openly accessible facilities to SCADA cybersecurity education rests in the quantity and quality of the laboratory exercises that are supported and effectively linked to an overarching curriculum. The challenge, according to Guillermo, is in the “continual development” and revision of such laboratory activities and “introduction of novel practices that will leverage the availability of state-of-the-art equipment and system tools” (p. 76).

Later contributions by Guillermo [21] included the specification of SCADA security toolkits as a cost-effective means of equipping educators with the SCADA components essential to supporting hands-on components of SCADA cybersecurity education. Security instructional modules based on these tool-kits are also presented to reinforce the concepts of “wireless communication, information security, control protocols such as Modbus/TCP and DNP3, HMI design and implementation, automation programming and circuit design” (p. 270).

In attempting to “bridge the cultural thinking gap” between control system engineers (responsibly for designing and maintaining critical infrastructure) and information technology professionals (responsible for protecting systems these systems from cyber attacks), Foo [22] suggest a postgraduate curriculum aimed at providing theoretical and practical exercises to raise awareness and preparedness of both groups. A key component of this curriculum is the availability of a number of SCADA system simulators (e.g., Water Reservoir, Smart Meter). Of particular import is the implementation of the simulators from SCADA components commonly used in the field and the utilization of virtual machines to simulate networking components and RTU’s. Similarity between the equipment used in the laboratory with that used in the field can favorably influence instructional effectiveness. Simulators can be more affordable and therefore more accessible in educational contexts.

Instructional methods are often limited by available resources. Virtualized environments show promise in bridging gaps (e.g., financial). This author would be remiss without referring to at least one example of an approach that exemplifies this concern directly. Sahin [23], alludes to the financial challenges associated with availing students laboratory experiments based on industrial components. The use of LabVIEW software to virtualize a SCADA environment and instrumentation and the positive effect on student learning is reported. Favorable outcomes suggest that, even with limited resources, SCADA cybersecurity education is attainable.

3.2.1 Web-based Virtual Hands-On Laboratory Testbed Approach

The value and benefits of remotely accessible web-based laboratory resources to increased instructional effectiveness in online, blended, and hybrid delivery modalities have been widely reported, as has recognition of the trend to share such resource between institutions [24, 25]. Such approaches do have limitations (e.g., the requirement for qualified staff members who can effectively configure and maintain a variety of configuration profiles in support of differing research and instructional initiatives) and these should be carefully considered. Much work remains to determine the best approach to making such resources more suitable to widespread adoption.

3.3 Case-Study/Group Work Approach

Rowe [8] identifies several advantages associated with the adoption of a case-study instructional approach including availing students opportunities to discuss and develop deeper insight into the “motives, targets, threats, risk, and incident response in the real world.” (p. 118). By engaging in critical analysis of the effectiveness of current practices and formulation of recommendations that will improve effectiveness, students are engaged at higher levels of thought and reasoning.

Collectively, the above instructional approaches to SCADA cybersecurity education exemplify the variability that exists among institutions as they continue to explore and seek out those that are most effective. Instructional staff are encouraged to explore these, as well as other novel approaches for effectiveness in their own setting. Thus, the concerns over cybersecurity risks associated with SCADA, may best be addressed through broader engagement in the scholarship of teaching and learning.

4 Recommendations

The outcomes of this study illustrate that several instructional approaches have and continue to be explored. Each approach is targeted to addressing the need to educate students about one or more aspects of SCADA cybersecurity. Each emphasizes a particular cognitive domain (e.g.,
comprehension, application, evaluation) and delivery modality (e.g., online, face-to-face).

SCADA cybersecurity education can perhaps best be viewed as a microcosm within the larger cybersecurity education domain. As such, recommendations pertaining to the positioning, design, and implementation of SCADA cybersecurity curriculum and instructional approaches should be informed by adoption of demonstrably effective approaches to cybersecurity education.

One particularly promising approach proposed by Rowe [8] provides an adaptable framework named “Prepare, Defend, Act” (p. 113). When viewed as categories, the three elements can be contextualized, according to the authors, through the following questions:

1. “What cyber-threats are there and how can we prepare for, and minimize potential attacks? (Preparing)
2. How to design and maintain secure systems? (Defending)
3. What should be done in the event of a cyber-attack and how can one place attribution? (Acting)” (p. 117)

The approach is readily adaptable and focusable on SCADA cybersecurity education. In a similar vein, the instructional methods identified by Rowe [8], including “hands-on exposure”, “collaboration”, and “case studies” have also been demonstrated to be effective as discussed above. All approaches should be designed and implemented to support the broadest range of delivery modalities.

The continuing efforts to refine professional and curriculum standards and engage more deeply in the scholarship of teaching and learning will undoubtedly lead to more effective instructional approaches. These in turn, will be more widely adopted with increased consistency of application and overall effectiveness.

Ultimately, each educational institution must take into account its own unique mission, educational programs, and student learning objectives when deciding which SCADA instructional approach(es) to adopt, modify and implement. This process should be informed through the findings reported by those educators engaged in the scholarship of teaching and learning of SCADA cybersecurity. Greater engagement will speed discovery of the most effective SCADA cybersecurity instructional approaches.

5 Conclusion

The concerns over risks associated with SCADA cybersecurity are clearly warranted as vulnerabilities continue to be identified. Preparation of a knowledgeable and skilled cybersecurity workforce is one of the great challenges facing education institutions today. Factors including evolving professional and curriculum standards have contributed to inconsistent application of effective instructional strategies. Instructional approaches continue to be explored with each targeting specific cognitive domains and delivery formats of SCADA cybersecurity. Each institution must take into account its own mission, educational programs, and student learning outcomes when deciding which SCADA instructional approach(es) to utilize. Simultaneously, educators are urged to engage more deeply in the scholarship of teaching and learning of SCADA cybersecurity. Through a collective approach, we may best prepare a future workforce sensitive to such concerns and able to effectively address them.

6 References


