CERIAS Tech Report 2012-14

A Curriculum Model for Industrial Control Systems Cyber-Security with Sample Modules

by J. Chris Foreman, James H. Graham, Jeffrey L. Hieb, Rammohan K. Ragade
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

A Curriculum Model for Industrial Control Systems Cyber-Security with Sample Modules

Dr. J. Chris Foreman and
Dr. James H. Graham
Dept. of Electrical and Computer Engineering
J. B. Speed School of Engineering
University of Louisville
Louisville, KY 40292 USA
jchrisf@louisville.edu

Dr. Jeffrey L. Hieb
Dept. of Engineering Fundamentals
Dr. Rammohan K. Ragade
Dept. of Computer Engineering and Computer Science
J. B. Speed School of Engineering
University of Louisville
Louisville, KY 40292 USA

Abstract

Cyber-security has been a topic of interest for several decades, and much work has been done in this area. Historically, industrial control systems (ICS) have been an island, both figuratively and literally, as they have utilized closed, proprietary systems air-gapped from the outside world. As these systems are now being incorporated into the corporate Wide Area Network (WAN) and subsequently exposed to the Internet at large, they are now at risk for cyber attack. The educational arena is still considerably lacking in producing new professionals or training existing ones to combat this new threat. As ICS are often in control of critical infrastructure, they are increasingly becoming targets of terroristic cyber attacks. A discussion of the educational deficits and a proposed solution is presented with sample modules and a class evaluation.

1 INTRODUCTION

Cyber-security has been an area of substantial interest and research for a number of years, especially now with the widespread penetration of the World Wide Web (WWW), which brought the general public into mainstream computing. Because of this, there has been much development in curricula to train new students and existing professionals in cyber-security. However, this development has typically been focused in the Information Technology (IT) sector and training has been introduced primarily to computer science and computer engineering students. Industrial Control Systems (ICS) have typically been the venue of electrical, mechanical, and chemical engineers who utilize such systems to control industrial processes. As such, curricula in cyber-security for ICS students and professionals have been deficient. In the last few years, there have been efforts to address this need in academia. [1] Commercial and governmental laboratory efforts, including guidelines and research, have been also done. [2][3] Many of these efforts have been in the form of short courses on how to use Commercial Off-The-Shelf solutions (COTS). Some of these efforts have begun to introduce theoretical and advanced topics in cyber-security for ICS but there is still much development to be done to achieve the level of detail needed for these systems.

1.1 History of Industrial Control Systems

Historically, ICS were built on closed, proprietary systems and air-gapped from the outside world. In the last several years, ICS have begun using COTS solutions from IT. These systems have subsequently become networked into the corporate WAN and as a result, exposed to the Internet at large. Most of these ICS still incorporate legacy systems and incorporate little to no cyber-security capabilities. This leaves these systems open to cyber attack. [4]

Existing professionals in ICS have come from an engineering background that typically did not include principles of cyber-security. As such, they are ill prepared to incorporate these principles after the fact. The large presence of legacy systems, due to long lifetimes in ICS, has resulted in systems incapable of support cyber-security as well. There is reluctance to accept this need among management as cyber-security can often pose expensive ICS upgrades where the payback is not well defined. Cyber attacks on ICS have only started surfacing. [5] Other misperceptions exist as a result of the separation between the goals of IT and ICS professionals. For example, in IT, information access and confidentiality are the key properties to protect. In contrast with ICS, the cyber information is only of secondary importance. The primary concern is that of the industrial process being controlled. These are some of the reasons that ICS cyber-security has lagged historically.

1.2 ICS in Critical Infrastructure

ICS are often utilized for the control of critical infrastructure such as: water treatment and delivery; power generation and distribution; telecommunication and Internet; and others. These infrastructure are also interdependent, which compounds the risk when one or more of these are attacked. [6]

1.3 Development of ICS Cyber-Security Modules

To address the lack of understanding and expertise in ICS cyber-security, a model of a comprehensive curriculum and two sample modules were developed for students in an academic setting. By education new students thoroughly in both principles of cyber-security and ICS technology, such students will be able to effectively apply existing solutions and develop new solutions to replace legacy system in use. These two modules were presented to a university class of students and evaluated with a 25-question test and survey of the students' perceptions.

2 CURRENT EDUCATIONAL LANDSCAPE

In order to better analyze the topic of ICS cyber-security education, it is important to understand the types of students, institutions, and curricula present in this field.

2.1 Students

Students are categorized into one of three backgrounds based on their pre-existing skill sets and motivation for seeking ICS cyber-security training.

- Academic – These students are typically new to both industrial process control and cyber-security and typically have no professional experience in industry. They typically seek and receive a largely theoretical approach.
- Professional – These students are experienced professionals using ICS in industrial settings. They typically seek practical application with brief exposure to some theoretical components.
- Managerial – These students are non-technical professionals, such as plant supervisors or managers, working in ICS or IT fields that need to understand policies and strategies for corporate integration of ICS cyber-security. They may also be non-engineering end users of ICS.

2.2 Institutions

There are traditional academic institutions, such as colleges and universities, which are an important source for the production of new technical professionals. Professional organizations, government laboratories, and ICS vendors also perform practical training of existing professionals.

- Academic – It is important to introduce ICS cyber-security concepts at the undergraduate level. The graduate level instruction should be reserved for advanced topics in ICS cyber-security. Several academic institutions have incorporated computer and network security into their curriculum but very few have implemented ICS cyber-security; perhaps viewing this as either too specialized for a dedicated course or as too low perceived demand by students and industry. Cyber-security courses also tend to be taught to computer students (CS, CE, CSE) rather than general engineering students (EE, ME, ChemE), which are more likely to work with ICS in industrial process environments. Therefore, with respect to ICS cyber-security instructional needs, cyber-security education is either insufficient or presented to the wrong group of students.
- Professional – These include private companies that educate professionals for profit, trade organizations that educate professional members, and ICS vendor companies. This type of educational training is designed for working professionals and as such, the format consists of a short, intensive class schedule ranging from less than one day to a few consecutive full-time days. This training may span many specialized topics in ICS cyber-security and achieve quick exposure for working professionals yet; they are not reinforced over a sufficiently long time frame or in a multiple course curriculum. Therefore, it may be difficult for the student to gain a true understanding of core principles from such courses.
- Government laboratories – These have recently taken a research and development role in ICS cyber-security working with academic and corporate partners on cyber-security solutions. Short courses and workshops have also resulted from these efforts.

2.3 Curricula

The educational content of courses designed for ICS cyber-security generally follows two main themes. A complete program in ICS cyber-security requires development of both themes.

- Theoretical – Includes principles of cyber-security as applied to ICS; techniques for threat detection, analysis, and prevention; principles of network design; protocol analysis; policy development; and others.
- Application – Supports the direct implementation of ICS cyber-security solutions; training on specific ICS cyber-security products and configuration support; and the establishment of site-specific ICS cyber-security policies. The unique aspects of the process being controlled should also be discussed with respect to a specific site or class of sites.

3 COMPREHENSIVE CURRICULA MODEL

The creation of a comprehensive curriculum model was necessary to form a plan course development and a

basis of comparison to existing programs. The goal was to develop a model, and subsequent educational modules, such that they could be incorporated into existing academic curricula.

3.1 A Comprehensive Model

In Section 1, it was discussed that one of the key problems in ICS cyber-security education is that students are typically educated along two paths being either industrial control systems technology or cyber-security technology. In the interests of quick graduation and lack of historical precedence, there has been very little overlap between these. A comprehensive curriculum should require coursework along both of these paths, which in turn, requires multiple courses. In figure 3.1, these two paths of ICS and cyber-security are illustrated. If a student already has expertise in one of these areas, they are directed to coursework along the other path as indicated in the notes to the side. These two paths then merge into one common path, which includes the integration of ICS and cyber-security and concepts of policy management.

The format is compatible with traditional academic institutions as these serve as the primary educational path for new professionals. Professional organizations, as discussed previously, are good resources to fill in the gaps for working professionals who are deficient in a few areas.

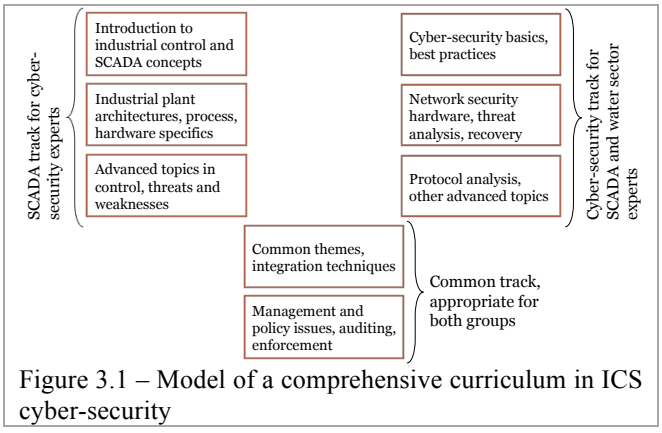

Figure 3.1 – Model of a comprehensive curriculum in ICS cyber-security

3.2 The Two Modules

The modules were developed as two 50-minute sessions. The target audience was senior and graduate level students in computer engineering and computer science with some experience in cyber-security, and little to no experience in ICS technology. This was considered the most beneficial development path and target audience to achieve the goal of enhancing an existing program with a drop in module. While students of ICS technology would be lacking in skills of cyber-security, there are a greater number of training programs and resources on this topic in addition to COTS solutions.

Development followed a straightforward path of collecting information from commercial and industrial sources on ICS technology and typical application scenarios in order to introduce students to methods and terms common in industrial practice. Some topics were explored in more detail, such as protocols, in which the students had general knowledge but no exposure to ICS specific technologies. This allowed them to expand their understanding of new information using skills they had previously developed. In the second module, specific cyber-attacks on ICS installations were investigated to define the problem of ICS cyber-security vulnerabilities in an interesting manner. Solutions were then presented in the form of authentication, protocol security, and intrusion detection that were specific to ICS applications, yet again building on the students' previous knowledge of cyber-security in general. Policy and educational issues finished the module presentation. Figures 3.2 and 3.3 illustrate a representative slide from each of the developed modules.

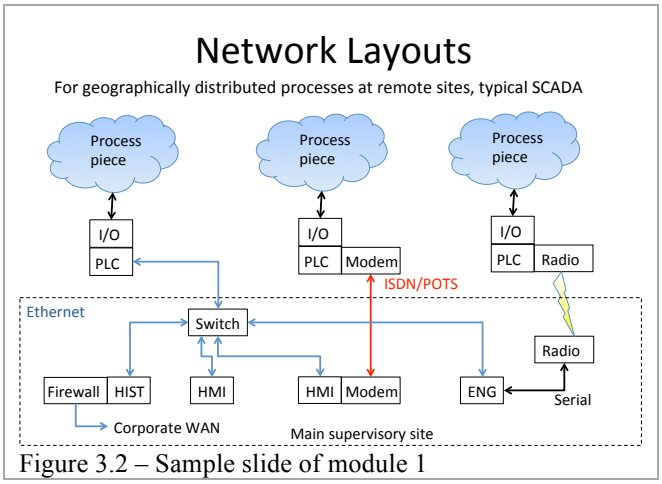

Figure 3.2 – Sample slide of module 1

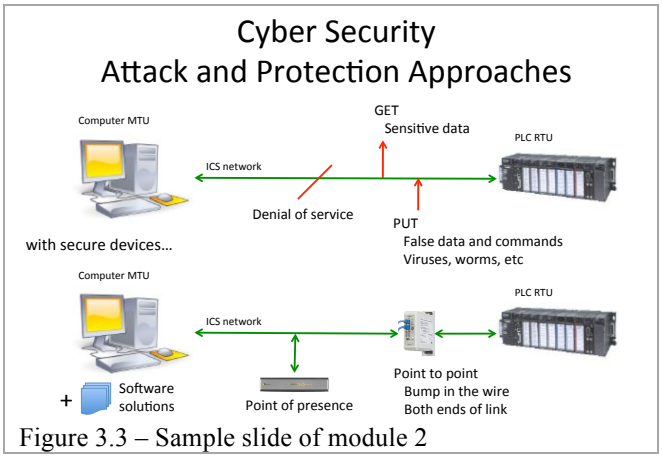

Figure 3.3 – Sample slide of module 2

4 CLASS EVALUATION

The modules were presented to senior and graduate level students in the Computer Science and Computer Engineering department as a supplement to the course "Information Security" at the University of Louisville. These students were familiar with the principles of cyber-security in IT environments, yet had no significant exposure to ICS or industrial environments.

4.1 Evaluative Test

A 25-question test was administered to evaluate the students' understanding and retention of the module presentation. In figure 4.1, the frequency distribution of final test scores out of a possible 25 is illustrated. The plot indicates the typical bell curve distribution with very few students achieving a low score below 15 and several receiving a good score above 20. Individual questions were evaluated by the percentage of correct responses. Most questions were answered correctly by at least 60% of the students and several were answered correctly by over 80% of the students, indicating that the material was largely understood. A few questions were answered correctly by less than 20% of the students. In these cases, the contrasts between ICS vs. IT cyber-security needed to be explored in more detail.

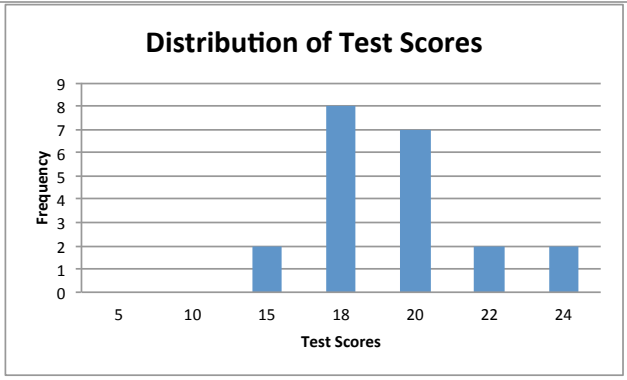

Figure 4.1 – Distribution of test scores

4.2 Evaluative Survey

An anonymous survey of 10 statements was developed to gauge the students' subjective opinion of the educational modules with respect to ease of understanding, appropriate level of detail, prior knowledge, perceived knowledge gained, and potential interest in pursuing further ICS cyber-security training. Students were asked to rate their degree of agreement or disagreement with the survey statements using a likert scale response.

Many students agreed that they were unaware of ICS cyber-security issues, but a significant number claimed to have some media exposure regarding recent security breaches. The first three statements were related to the clarity and effectiveness of the presentation materials, and most students agreed that materials were clear and the presentation was effective. Statements evaluating knowledge gained and technical detail were also overwhelmingly positive. A few students indicated that too much material was covered, which was interpreted to mean that the principles of ICS need more time to be developed than afforded in short courses. A few students indicated that they might consider altering their career path based on the modules presented.

5 CONCLUSIONS

It was found that students are rarely exposed to both areas of ICS technology and IT cyber-security. It was also found that IT information security was more developed in traditional academic settings versus ICS technology, which often is relegated to vocational and technical institutions. These two themes need to be integrated to achieve a comprehensive ICS cyber-security education. As a result of their separation, students and professionals often have insufficient skills, i.e. a focus along only one theme. Some relevant efforts were found, though there is still a low penetration of ICS cyber-security skills throughout both the student population and the installed workforce working in ICS.

As the problem of ICS cyber-security becomes recognized through education, industry acceptance, and cyber-attacks themselves, the perceived importance of obtaining skills in this area will grow. The prototype educational modules from this project, in addition to existing curricular efforts, can serve as a platform for future course development and research.

7.1 Recommendations

Future work in ICS cyber-security education should include the following additional steps:

1. Cyber-security modules should be developed and presented in ICS technology courses to expose students to these new concepts.
2. Follow up modules from those discussed in Section 3.2 should be developed to explore these topics in more detail.
3. Introduce graduate student research topics to provide students with a path to developing solutions in ICS cyber-security.
4. Create modules that are appropriate for professional students and incorporate them into existing or new short courses.

ACKNOWLEDGEMENTS

This research was funded by the Department of Homeland Security through the National Institute of Hometown Security.

REFERENCES

[1] Jill Slay and Elena Sitnikova, "Developing SCADA Systems Security Course within a Systems Engineering Program," *Proceedings of the 12th Colloquium for Information Systems Security Education*, pp. 101-108, University of Texas, Dallas, TX June 2-4, 2008.

[2] Keith Stouffer, Joe Falco, and Karen Scarfone,"NIST Guide to Industrial Control Systems Security Publication 800-82," found at http://csrc.nist.gov / publications / drafts / 800-82 / draft_sp800-82-fpd.pdf, September 2008.

[3] Jared Verba and Michael Milvich, "Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)," *IEEE Conference on Technologies for Homeland Security*, pp. 469-473, 2008.

[4] Ning Cai, Jidong Wang, and Xinghuo Yu, "SCADA System Security: Complexity, History and New Developments," *IEEE International Conference on Industrial Informatics*, Daejeon Korea, pp. 569-574, July 2008.

[5] Eric Chien, "W32.Stuxnet Dossier," Symantec, found at http://www.symantec.com / connect / blogs / w32stuxnet-dossier, February 2011.

[6] Jerry Gillette, Ronald Fisher, James Peerenboom, Ronald Whitfield, "Analyzing Water/Wastewater Infrastructure Interdependencies," *Infrastructure Assurance Center Argonne National Laboratory*, 2008.

BIOGRAPHIES

J. Chris Foreman (Ph.D. Computer Science and Engineering degree, University of Louisville, 2008) is a senior member of IEEE, the Power and Energy Society, and also holds both B.S. (1990) and M.Eng. (1996) degrees in Electrical Engineering from the University of Louisville. He is a postdoctoral associate at the University of Louisville in Louisville, KY. He teaches and performs research in industrial control systems and cyber-security, renewable energy systems, and intelligent power grids. He has worked primarily in the power generation industry as well as other process industries since 1993 for companies such as Westinghouse Process Control Division, Cinergy, and Alcoa Inc.

James H. Graham (Ph.D. degree, Purdue University, 1980) is the Henry Vogt Professor and the Chair of Electrical and Computer Engineering at the University of Louisville in Louisville, KY. He also received his Bachelor's degree in Electrical Engineering from the Rose-Hulman Institute of Technology and the M.S. degree from Purdue University in 1978. He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and a registered professional engineer. He has over thirty years of experience in the computer engineering and electrical engineering fields. Prof. Graham has served as a faculty member at Rensselaer Polytechnic Institute and as a product engineer with General Motors Corporation. His research interests involve information security, algorithms for computational science, intelligent systems, distributed computing, computer simulation, and intelligent energy systems.

Jeffrey L. Hieb is currently an Assistant Professor in the Department of Engineering Fundamentals at the University of Louisville. His research interests include the use of technology in engineering education; secure operating systems and cyber-security for industrial control systems.

Rammohan K. Ragade (Ph.D., I. I. T. Kanpur, India (1968)) is a Professor of Computer Engineering and Computer Science at the University of Louisville. He holds a B.E. degree in Electrical Power Engineering from I. I. Sc. Bangalore, India (1964). He served as the Coordinator for the Ph.D. Program in Computer Science and Engineering from 1999-2005. He has written well over 100 papers, including journal articles, refereed conference papers, chapter contributions to books and is the co-editor of four books. He is a senior member of IEEE. He is a member of the ACM. He has taught graduate courses in Software Engineering and Advanced Software Engineering, Software Design, Computer Security, Knowledge Engineering, Computer Architecture, and Simulation Modeling. His research interests include agent technologies, object oriented methodologies, real-time modeling, human computer interaction, knowledge engineering and rule-based expert systems, and system simulation. He has held and participated in several funded research grants and contracts.