Towards Standards-Based Industrial Control Systems Security Education in The United States

Sean McBride

Jill Slay

La Trobe University

June 2020

Abstract

In light of evolving threats, we are concerned that the professionals who design, build, operate and maintain industrial control systems (ICS) within the United States are unprepared to protect and defend them. This paper succinctly describes three key concerns for national and institutional educational leadership seeking to prepare such a capable workforce. Firstly, foundational information security concepts were created without consideration for the unique needs of industrial control environments. Secondly, existing U.S. educational standards for ICS security lack thorough development. Thirdly, current standards do not account for the career paths of industrial professionals. Given these concerns, we provide near- and long-term suggestions aimed to produce standards-based programs that meet this national imperative.

Keywords

Industrial control systems, critical infrastructure, industrial cybersecurity, education, training, standards

Evolving Threats to Industrial Environments Require Organized Workforce Development

Since the early 2000s, researchers and a variety of adversaries, ranging from cyber criminals to nation-states, have turned their attention to discovering and exploiting vulnerabilities in industrial control systems (ICS), which control infrastructures ranging from electricity grids to manufacturing facilities.

McBride (2016) reports that researchers disclosed more than 1,500 ICS-specific vulnerabilities between the year 2000 and 2015, with an increasing rate of disclosure after 2010.

Examples of nation-state cyber-attacks resulting in physical consequence include the Stuxnet worm that targeted centrifuges at Iran's Natanz uranium enrichment facility (Langner, 2013), the Western Ukraine power outage of 2015 (Whitehead, Owens, Gammel, and Smith, 2017), the Kyiv outage in 2016 (Greenberg, 2017), and the Triton malware that triggered a plant shut down by targeting the safety system at an undisclosed facility in the Middle East 2017 (Johnson, Caban, Krotofil, Scali, Brubaker, and Glyer, 2017).

Examples of incidents that were not directed at industrial control systems, but caused them significant harm include the Wannacry ransomware, which halted manufacturing at a Honda plant in June 2017 (Tajitsu, 2017), and the NotPetya ransomware, which stopped pharmaceutical production at a Merck facility the same month (O'neill, 2017). Merck informed its investors that the attack cost the company an estimated $310 million.

In light of these developments in the threat environment, we are concerned that the professionals who design, build, operate and maintain industrial control systems are unprepared to protect and defend them – and that existing cyber security education standards do not meet the need:

- Firstly, foundational information security concepts and standards were created without consideration for the unique needs of industrial control systems.
- Secondly, existing educational standards for ICS security standards lack thorough development.
- Thirdly, current standards do not account for the career paths of industrial professionals.

Foundational Information Security Educational Concepts Were Not Intended to Address ICS

The key difference between an industrial control system and an information system is that the latter exist to control information, while the former exist to control the real, physical world. Information systems are concerned with national secrets, trade secrets, intellectual property, personally identifiable information, and financial details. Industrial control systems are concerned with speeds, temperatures, pressures and positions of machinery that provides electricity, gasoline, and drinking water. Each type of system requires its own expertise, and carries its own consequences.

Foundational education and training concepts for information assurance disciplines (which encompass computer security and information security) established in notable publications such as *Information Security: A Comprehensive Model* (McCumber, 1991), and *A Model for Information Assurance: An Integrated Model* (Maconachy, Schou, Ragsdale, Welch, 2001), include integrity, confidentiality, availability, authenticity and non-repudiation. We note that the authors created these materials for information assurance not for industrial control assurance. A review of the foundational documents provides no clues that their authors considered their application to industrial control systems.

When Richard Morely invented the first programmable logic controller (which forms the backbone of industrial control systems) in 1968, he and his team intentionally avoided any terminology that could equate their industrial control device with a "computer" – used to store and process business information. The unreliability of, and the moving parts of, contemporary computers were dangers from which plant operators needed protection (Dunn, 2008). Hence, from the inception, the fathers of industrial control systems sought to separate their field from that of mainstream computing. We assert that personnel designing, building, operating and maintaining industrial control systems should concern themselves with concepts of safety, reliability, and controllability much more than integrity, confidentially, and availability.

Over the ensuing decades, industrial control systems came to rely on very similar technologies as traditional information systems. This reliance has increased the need to apply security concepts largely developed with traditional information systems in mind. Nevertheless, we assert that the specialized

knowledge required to safely, reliably, and controllably operate industrial processes exceeds the intended scope of the information assurance models underpinning the traditional information systems.

In particular, we find arguments that one can merely re-prioritize the security services – such as confidentially, integrity, and availability – named in these models to overcome a deficiency in the models' raison d'être- both fanciful and ill-advised (see Neitzel and Huba, 2014; and Smith, 2016 for examples of the re-prioritization approach). These arguments are fanciful because they ignore the key differences between the two types of system. They are ill-advised because they ignore historical and practical context.

Current National Standards for ICS Security Lack Thorough Development

In this section, we examine national ICS security educational standards advanced by 1) the National Security Agency (NSA), and 2) the National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology

In 2017, the National Institute of Standards and Technology (NIST), working with the Department of Homeland Security (DHS), published its National Initiative for Cybersecurity Education (NICE). This framework, codified in NIST Special Publication 800-181, represents a significant and time-consuming undertaking to classify responsibilities of the US cyber security workforce. The document includes 7 workforce categories, 34 specialty areas, and 52 work roles. Each work role includes tasks as well as knowledge, skills and abilities (KSAs [Newhouse, Keith, Scribner, and White 2017]).

A review of the document shows that the authors paid almost no attention to industrial control systems: First, the NICE framework never mentions the term "industrial control system". Instead, it uses the term "SCADA", which is a particular application of industrial control. This usage may demonstrate ignorance of appropriate terminology, or at least careless attention to detail.

Second, the term "SCADA" appears only at the KSA level, rather than as a specialty area or work role. This treatment tends to indicate that the National Institute of Standards and Technology (NIST) and

Department of Homeland Security (DHS) find industrial control systems only tangentially related to developing the US Cybersecurity Workforce.

Finally, of the three occurrences of term "SCADA" two are in parenthetical references, underscoring again the unimportance of the concept:

- *Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access* (Newhouse 2017 p. 44)
- *Knowledge of the range of existing networks* (e.g., PBX, LANs, WANs, WIFI, SCADA) (Newhouse, 2017 p. 63)

The third occurrence is a single broad swipe

> *Knowledge of general Supervisory control and data acquisition (SCADA) system components* (Newhouse, 2017 p. 71)

These KSAs are mapped to the Specialist, Target Developer, and Threat/Warning Analyst work roles. None of these correspond to individuals assigned to actually protect or defend operational industrial control systems that ultimately provide critical services such as electricity or drinking water.

To address the objection that SP 800-181 was created to serve the needs of US government employees, and the US government does not need such professionals because it does own industrial control systems: we note that military bases, naval ships, and Bureau of Reclamation hydroelectric stations are important examples of federal government facilities that operate these systems.

National Security Agency

Since 1999, the US National Security Agency (NSA) has required schools participating in its "Centers of Academic Excellence in Information Assurance" program to demonstrate adherence to NSA's educational standards (Bishop and Taylor 2009).

In 2014, the NSA shifted to a Knowledge Units approach for schools to demonstrate their compliance (Conklin, 2014). Under this shift, the NSA created a Knowledge Unit for Industrial Control Systems (ICS). This unit is optional, meaning that schools are not required to include its content unless

they desire to specialize in this field. The 2020 Knowledge Unit includes nine topics and five outcomes (National Centers of Academic Excellence, 2020). Our review of the Unit found several deficiencies, which indicate insufficient participation of subject matter experts in its creation:

- Inaccurate terminology. The first topic listed in the Unit is "SCADA firewall". This term is a misapplication of the term "SCADA", which is a specific way a human operator interacts with an industrial control system. The second topic listed in the Unit is "hardware components". The term is ambiguous and could be better rendered as "sensors and actuators" for example.
- No mention of consequence assessment. As mentioned previously, consequence is a key distinguishing characteristic between industrial control systems and information systems.
- No discussion of roles and responsibilities that exist within the plant environment. A student expected to secure industrial environments should reasonably know the titles and qualifications of the individuals with which he or she would interact.
- No discussion of lifecycle attack vectors. Vendors and the popular press have propagated the myth of an air gap between the industrial control system and the business network. Students who do not recognize ways that an adversary could access industrial control systems across their lifecycle are unprepared to defend them.

Current U.S. Workforce Standards Do Not Account for the Career Path of Industrial Professionals

Finally, we are aware that the instrumentation and control technicians that configure sensors, program PLCs, and troubleshoot control loops, often come from specialized two-year technical career programs.

One prominent case is Marty Edwards, who served as Director of the US Department of Homeland Security (DHS) Industrial Control Systems Computer Emergency Response Team (ICS-CERT) from 2011 to 2017. Edwards is a graduate of the British Columbia Institute of Technology where

he studied electrical and electronics engineering, earning a two-year diploma (Edwards, 2017). This hands-on experience prepared and qualified him for a career as an automation technician and enabled him to make sense of the security details affecting industrial environments.

It is practical to recognize that the individuals who will cause, notice, and respond to cyber incidents in industrial environments are the people who work there every day – that is the control technicians and engineers who design, program, install, commission, operate, and maintain these systems. In order to successfully defend critical infrastructure, educational standards must apply to institutions and programs that produce these professionals.

As of April 2018 the National Security Agency has designated more than 200 institutions as Centers of Academic Excellence in Information Assurance. Only two qualify under the Industrial Control Systems focus area (NSA, 2018). Only one – Idaho State University – encompasses a two-year hands-on program producing instrumentation technicians.

The Way Forward

In order to advance standards that meet the national imperative for qualified professionals to defend critical industrial control systems, we recommend:

- Engage qualified ICS security professionals to fully develop educational standards that improve the NSA Knowledge Unit, and expand the NICE framework. This engagement should involve a reasonable number of participants and perspectives to represent a consensus. It should document the qualifications of the participants. It should rely on methods to ensure applicability to the problem space and associated workforce needs.
- Review international ICS security training and education standards efforts. This will ensure that the resulting standards incorporate key observations and lessons learned from previous efforts outside the United States.
- Engage with key international and global organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), Association of Computing Machinery (ACM), and

International Society of Automation (ISA) to promote adoption through alignment with existing cybersecurity education and training standards.

Potential Roadblocks

As we envision a future of standards-based education for industrial cybersecurity, we find the following roadblocks of greatest concern:

1. The need for industrial cybersecurity education and training is not well understood. Speaking empirically, cybersecurity policy leaders, educators and practitioners alike seem to view industrial cybersecurity as a specialization in the field rather than an area meriting a foundational level of attention. As the list of significant challenges in traditional cybersecurity continues to grow, this perception is unlikely to change. Efforts to create industrial cybersecurity educational standards will be of limited value if policy leaders at the national and institutional levels remain unwilling to incentivize and support programs that implement those standards.
2. Practitioners and academics are often separated by a significant gulf. Based on our experience, academics frequently excel because they are removed from the realities of daily IT and ICS systems operations. Failure to involve the right parties in standards development efforts, and later curriculum design and delivery, may significantly hamper the effectiveness of the standards and the resulting workforce. National educational policy makers and leadership of educational institutions must ensure practitioner-heavy involvement.
3. Instructional expertise in the field of industrial cybersecurity is hard to come by. Industrial cybersecurity is an emerging educational field. Professionals who understand industrial cybersecurity command salaries with which educational institutions cannot compete. Academically qualified (PhDs) in the field generally do not exist. National policy makers and institutional leadership can foster relationships with potential qualified instructors through unique approaches and incentives not available in the commercial world such as part-time fellowships, interaction with academic circles, bestowal of certain faculty benefits, and honorariums.

4. Due to its cyber-physical nature, an industrial cybersecurity educational program carries costs which schools may not be prepared to assume. It is unreasonable for us to prepare students to defend critical industrial systems when they have never seen or touched the core components of those systems. Controllers, human machine interface (HMI) panels, transmitters, motors, pumps, valves, and common industrial processes such as heat exchange, flow control, and motion control require hands-on experience to fully appreciate. National policy makers and institutional leadership can fund capital expenditures and maintenance of educational ICS security laboratories, given that these programs adhere to the appropriate national educational standards. National policy makers and institutional leadership should seek opportunities to partner with ICS equipment suppliers and local industry partners who normally own and operate this equipment to achieve an appropriate balance of virtual, simulated, and hands-on learning experiences.

References

Bishop, M. and Talyor, C. (2009) *A Critical Analysis of the Centers of Academic Excellence Program*, Proceedings of the 13th Colloquium for Information Systems Security Education. Retrieved from https://cisse.info/resources/archives/category/12-papers?download=125:s01p04-2009

Conklin W., Cline, R., and Roosa T. (2014). *Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors*, 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2014, pp. 2006-2014. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6758852&isnumber=6758592

Dunn, A. (2008). *The father of invention: Dick Morley looks back on the 40th anniversary of the PLC*. Retrieved from https://www.automationmag.com/features/the-father-of-invention-dick-morley-looks-back-on-the-40th-anniversary-of-the-plc.html.

Edwards, M. (2018). Linkedin profile. Reterieved from https://www.linkedin.com/in/marty-edwards-738aa313b/.

Geenberg, A. (2017). *'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID*. Wired. Retrieved from: https://www.wired.com/story/crash-override-malware/

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., and Glyer, C. (2017). *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. Retrieved from: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Langner, R. (2013). *To Kill a Centrifuge*. Retrieved from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lingafelt, S. (2017). *The History and Development of a "Cyber Security" Program Criteria*. Retrieved from http://www.abet.org/blog/news/the-history-and-development-of-a-cyber-security-program-criteria/.

Maconachy, V., Schou, C., Ragsdale, D. and Welch, D. (2001). *A Model for Information Assurance: An Integrated Approach*. Retrieved from http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf

McCumber, J. (1991). *Information Systems Security: A Comprehensive Model.* Retreived from: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-NCSC-proceedings-vol-1.pdf.

National Security Agency (2014). *Knowledge Units*. Retrieved from: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf

Neitzel, L., and Huba, B. (2014). *Top ten differences between ICS and IT cybersecurity*. Retrieved from https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/.

Newhouse, W., Keith, S., Scribner, B., White, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, Washington, DC. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NSA (2018). *CAE Designated Institutions*. Retrieved from: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

O'neill, P. (2017). *NotPetya ransomware cost Merck more than $310 million.* Retrieved from https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/

Smith, R. (2016). *Introduction to ICS Security - Pt. 2 - IT versus ICS Security*. Retrieved from: http://www.exida.com/Blog/introduction-to-ics-security-pt.-2-it-versus-ics-security.

Tajitsu, N., (2017). *Honda halts Japan car plant after WannaCry virus hits computer network*. Retrieved from https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI

Whitehead, D., Owens, K. Gammel, D., and Smith J. (2017). *Ukraine cyber-induced power outage: Analysis and practical mitigation strategies*. 2017 70th Annual Conference for Protective Relay

Engineers (CPRE), College Station, TX, pp. 1-8. Retrieved from:

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8090056&isnumber=8089819