2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023
The Harbor of Engineering Education for 130 Years
ASEE
Paper ID #38918

Board 251: Developing Micro-Credentials to Infuse Cybersecurity into Technician Education

Dr. Evelyn C. Brown, North Carolina State University, Raleigh

Dr. Brown is Director of Extension Research and Development at North Carolina State University. She works for Industry Expansion Solutions, the industrial extension arm of the NC State College of Engineering. She has expertise in the area of grant evaluation, serving as external evaluator for numerous federally-funded grants. She currently serves as PI on an NSF ATE grant titled "The Robotics/Automation and Cybersecurity Knowledge Sharing Coordination Network", or TRACKS-CN.

Zackary Tyler Hubbard

Developing Micro-credentials to Infuse Cybersecurity into Technician Education

Evelyn Brown, North Carolina State University
Zackary Hubbard, Rowan-Cabarrus Community College

Abstract

With manufacturing facilities across the country becoming more connected, it is critical that safeguards are in place to protect against threats to facilities' cyber-physical systems. Technicians with training in robotics/automation/mechatronics are well positioned to help provide a first line of defense to such threats. This work, funded through a National Science Foundation (NSF) Advanced Technological Education (ATE) grant, seeks to enhance technician cybersecurity awareness through education and training. The paper provides details on the process the project team utilized to develop an initial micro-credential in the area of cybersecurity for robotics/automation/mechatronics. The paper focuses on the badge creation process and outlines how the badge modules developed can be shared to help raise cyber awareness in other fields, such as semiconductors, solar power, and electric vehicles. The badge leverages the work of other NSF ATE projects, providing a no-cost avenue for automation technicians to expand their background by earning a digital badge that enhances their resume.

Background

Today's manufacturing involves cyber-physical systems that connect automation devices to each other and to the Internet. As a result, technicians working in manufacturing need to possess an awareness of potential cybersecurity threats to their equipment and systems. The Robotics/ Automation and Cybersecurity Knowledge Sharing Coordination Network (TRACKS-CN) is an NSF-funded ATE project that seeks to enhance technician education and training at the convergence of automation/robotics and cybersecurity. The coordination network originated with six community colleges, one community college system office, four Manufacturing Extension Partnerships (MEPs), two Manufacturing USA Institutes, and the National Initiative for Cybersecurity Education (NICE). It has expanded to now include five additional community colleges and four more MEPs. While the development of a digital badge was not one of the proposed deliverables of the TRACKS-CN grant, working collaboratively, network members developed a micro-credential to help meet the goals of the ATE project.

According to Hunt et al. [1] , micro-credentials offer a number of benefits, including: flexibility (can be earned at the learners pace), cost efficiency (lower cost and fewer barriers to participate), competency (learners develop and demonstrate competence in a skill or knowledge area), and collaboration (micro-credentials allow content to be easily shared among educators). While micro-credentials have become accepted in some fields, such as Information Technology [2] and in some sectors, such as the gig economy [3], their recognition as a valid method for current or potential employees to demonstrate capabilities is still lagging in manufacturing, particularly among smaller-sized manufacturers (P. Mintz, personal communication, February 12, 2023). The project team is currently developing a plan to utilize MEP members from TRACKS-CN to help educate small and medium-sized manufacturers about the benefits of micro-credentials. In

an effort to begin to develop best practices for sharing the benefits of micro-credentials with MEP clients, the PI has initiated conversations with regional managers who support the North Carolina Manufacturing Extension Partnership.

Objectives

As previously mentioned, the goal of the ATE project is to enhance technician education and training at the convergence of robotics/automation and cybersecurity. The project team's initial plan included the development of a web portal to house information on these topics. However, attempts to locate training materials at the convergence of these topics yielded little in the area of Operational Technology (OT), with most of the available content focusing solely on Information Technology (IT). The coordination network membership includes numerous community college faculty with expertise in the areas of robotics/automation/mechatronics and cybersecurity, so the decision was made to utilize that expertise to develop a micro-credential focused on these topics. The objective of the initial digital badge is to provide cybersecurity awareness training to technicians with a background in robotics/automation/mechatronics.

Program Description

To begin the digital badge development, the project's co-PIs, one with expertise in mechatronics and one with expertise in cybersecurity, reviewed the 54 NICE competencies [4] to determine which ones had direct ties to Advanced Manufacturing. Then, a subcommittee referred to as the Badge Team was formed, and its membership consisted of a subset of the TRACKS-CN members. The Badge Team discussed the competencies and came to agreement on 11 NICE competencies to include in the initial awareness badge (see Figure 1, below). They also developed a framework for the badge modules, which included the use of scenarios based upon real-life cybersecurity examples from industry. Working with a qualitative researcher from a nearby four-year institution, one of the co-PIs developed an interview protocol to enable quicker, more directed conversations with manufacturers. The goal was to minimize the time needed to capture the relevant information from which to create a scenario for each competency. To keep things anonymous, when scenarios were created, letters of the Greek alphabet were used as the names of the companies. Also, each scenario was reviewed and approved by the company prior to inclusion in the published badge content.

The Badge Team determined that the badge should consist of 11 modules, one per competency. While the type of content for each module is not identical, each module concludes with a scenario-based assessment. Currently, the assessment is the same for all badge earners. During 2023, the final year of project funding, the project team plans to develop additional assessment questions that can be included on a rotating basis, in order to reduce the chance that a solution key could be developed and circulated online.

The badge is named Cyber4RAM, where RAM is robotics/automation/mechatronics. Most of the content for the modules was pulled together and/or developed by a faculty member from one of the TRACKS-CN member institutions. This faculty member created the 11 modules using the standards from the Quality Matters Higher Education Rubric [5]. Each module begins with an overview and then moves into explaining a topic that aligns with the chosen competency, using a variety of materials. Each module ends with a quiz, which is used to measure the student's

learning and includes a scenario from a manufacturing company that has some type of cybersecurity concern or issue. As explained above, the scenarios are based on interviews conducted with actual companies, but company names and details were anonymized to protect their identities and to keep the details of their cybersecurity issue confidential. Additionally, since one of the creators of e-Mates [6] is also a member of TRACKS-CN, the badge incorporates e-Mates in some of its modules. Also, the National Center for Supply Chain Automation granted the project team permission to include content from their e-book [7].

Another key aspect of this work is the badge development process created. The eight steps of this process are provided in Figure 2, below. As noted above, the process began with reviewing the existing list of published NICE competencies and selecting the ones tied to the topic area (Advanced Manufacturing). After developing an interview protocol and speaking with industry, scenarios and assessments for each competency were developed, allowing the content developer to "back into" the content creation step. While some existing content on the competency topics was located, the amount of existing training materials focused on building cyber awareness among technicians working in robotics/automation/mechatronics was limited. Canvas Instructure, which is available to users at no cost, was the Learning Management System (LMS) utilized. Credly is the badge issuer for the Cyber4RAM badge. Credly was selected due to its reputation and due to a pre-existing relationship between the PIs institution and Credly.

The project team believes that as micro-credentials become more prevalent, the methodology employed in this project may be useful for others. The hope is that by sharing this methodology, the time it takes others to develop a new digital badge can be reduced. Additionally, because Cyber4RAM badge content is in modular form, some or all of the content can be easily shared with others who are developing related badges, such as Cyber4Semi (semiconductors) or Cyber4EV (electric vehicles). The Cyber4RAM badge was created to offer an alternative to traditional coursework, as often there is not room in a curriculum to require automation technicians to complete separate cybersecurity courses. If an educator wishes to incorporate the Cyber4RAM content into their course offering, the project team can share a SCORM package that can be utilized via their institution's LMS.

NICE Competencies for Badge

1. Asset and Inventory Mgmt.
2. Computer Languages
3. Data Privacy
4. Data Security
5. Digital Forensics
6. Identity Management
7. Incident Management
8. Infrastructure Design
9. Physical Device Security
10. Systems Integration
11. Vulnerabilities Assessment

Figure 1: Badge Competencies

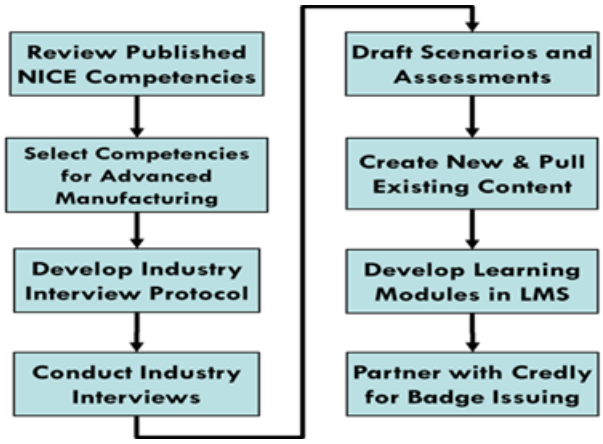

Figure 2: Badge Development Process

The Cyber4RAM badge was piloted in fall 2022, using TRACKS-CN members, as well as other individuals connected to the project. Feedback from beta testers was incorporated, though there were only a few minor adjustments and edits needed. On November 1, 2022, a soft launch of the badge was implemented. Community college faculty affiliated with TRACKS-CN provided badge registration information to their students, many of whom completed the badge. A full launch took place February 1, 2023, accompanied by a press release and a social media campaign about the badge.

Results/Evaluation

Since July 2022, the PI and co-PIs have shared information about the Cyber4RAM badge and the badge development process with a number of organizations. Those organizations include: Northwest State Community College (OH), National Coalition of Advanced Technology Centers; Fayetteville Technical Community College (NC); Texas A&M Cybersecurity Center (TX); Clemson University Center for Workforce Development (SC); Florida Advanced Technology Education Center (FLATE); North Carolina Partnership for Cybersecurity Education (NC-PaCE); Cyber for Manufacturing Innovation Institute (TX); Micro Nano Technology Education Center; Dakota State University (SD); and American Association of Community Colleges.

In addition, the PI has disseminated material about the Cyber4RAM badge and its development with individuals from academia, industry, and economic development organizations at events such as: High Impact Technology Exchange Conference (UT); Workforce Conversation (VA); MEP Best Practices Conference (IL); North Carolina Community College System Conference; ATE PI Conference (DC); and the NC-PaCE Cybersecurity Symposium. In April 2022, the co-PI provided an overview of the badge for the monthly NICE Community Coordinating Council Meeting. Also, the PI and co-PI were invited by the Center for Occupational Research and Development (CORD) to provide a webinar for the North Carolina Network for Excellence in Teaching (NC-NET). The webinar was delivered in January 2023.

As a result of the dissemination efforts, 33 learners have earned the badge (as of 2/10/23). Also, some of the individuals with whom the PI has connected, such as the Director of FLATE, have shared the badge within their networks, which has led to additional badge earners. Other contacts have asked for a copy of a recent press release to share within their networks, in order to further promote the Cyber4RAM badge.

While evaluation of the badge, in terms of outcomes and impacts, is beyond the scope of work for the external evaluator contracted to evaluate the TRACKS-CN grant, the coordination network's inclusion of 11 community colleges offers and avenue through which evaluation can occur. As community college faculty who are members of TRACKS-CN share the badge link with their students, they can share a link to an anonymous Qualtrics survey that measures learners' perceived gains in confidence in the module competency areas and gathers input on learners' anticipated benefits of completing the badge.

The PI is currently the evaluator for several NSF ATE projects, and has experience developing participant perception surveys. The PI would need to secure proper IRB approval from her

institution prior to delivering the survey or disseminating its results. A link to the participant perception survey can be added to the TRACKS-CN website to enable feedback to be obtained from badge earners who are not current community college students or who are not students at an educational institution in the coordination network.

Conclusions

Infusing cybersecurity into technician education and training is critical for the continued success of US manufacturing. As automation and technology advances lead to manufacturers incorporating more cyber-physical systems, the threat of cyber-attacks increases. Technicians who are on the front lines, working in the areas of robotics, automation, and mechatronics, can help protect their company and its assets by becoming more aware of key cybersecurity competencies. The Cyber4RAM badge provides cyber awareness for technicians working in advanced manufacturing.

Future Plans

Other critical industries, such as semiconductor technology, electric vehicles, solar technology, and others, may find value in adapting the Cyber4RAM badge to fit their needs. The modular design of the Cyber4RAM badge makes it easy to share some or all of the modules with educators and those seeking to train technicians. The project team plans to continue to disseminate information about the badge and its development process, and will share the badge development process and badge modules with educators and others with an interest in helping technicians develop cyber awareness. The project team is also considering ways to share the badge development process with some or all of the eight federal agencies that lead skilled technical workforce development programs [8].

This work is part of a project funded by the Advanced Technological Education Program of the National Science Foundation DUE #2000867. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References Cited:

[1] T. Hunt, R. Carter, L. Zhang, and S. Yang, "Micro-credentials: the potential of personalized professional development," *Development and Learning in Organizations: An International Journal*, vol. 34, no. 2, pp. 33-35, 2020.

[2] B. Hoanca, B. and B. Craig,. "Invited Paper: Building a K-16-Industry Partnership to Train IT Professionals," *Journal of Information Systems Education*, vol. 30, no. 4, pp. 232–241, 2019.

[3] L. Wheelahan and G. Moodie, "Gig Qualifications for the Gig Economy: Micro-Credentials and the 'Hungry Mile'," *Higher Education: The International Journal of Higher Education Research*, vol. 83, no. 6, pp. 1279–1295, 2022.

[4] NIST Computer Security Resource Center. *Nice Framework Competencies: Assessing Learners for Cybersecurity Work (2nd Draft)*. National Institute of Standards and Technology https://csrc.nist.gov/publications/detail/nistir/8355/draft (accessed December 5, 2021).

[5] "Quality Matters Higher Education Rubric" https://www.qualitymatters.org/qa-resources/rubric-standards/higher-ed-rubric (accessed July 12, 2022)

[6] M. Qaissaunee, and J. Sands, myEMATES: http://e-mate2.s3-website-us-east-1.amazonaws.com/ (accessed August 16, 2022).

[7] National Center for Supply Chain Automation, *Introduction to the Automated Warehouse*, 2nd ed. 2022. [E-book] Available: https://supplychainautomation.com/resources/etextbook/

[8] A. Reamer, "Federal Agencies with Skilled Technical Workforce (STW) Development Programs" in *Prepared under NSF Contract 49100421C0020-Administrative Datasets on Non-Degree Credentials: Creating and Analyzing a Repository.* April 21, 2022.