Industry Advisory Board View on Industry 4.0 Cybersecurity and Other Topics

Sidney Martin, St. Petersburg College; Marilyn Barger, FLATE; Catherine M. Davis, St. Petersburg College

Abstract

The purpose of this investigation is to have industry members (members 88, responses n=36) in West Central Florida answer the following questions about participating on the engineering technology advisory board:

1. Employer expectations of the cybersecurity skills needed for engineering technology graduates.
2. Determine the hiring needs of the local engineering technology companies in the Tampa Bay Region.
3. Explain the benefits to the manufacturing or engineering organization participating in an advisory committee.
4. Determine the local need for engineering technology students to understand electrified vehicles or semiconductor manufacturing.
5. What is the view of employers regarding the requirements for students to continue their education in Lean Six Sigma?

This paper is a qualitative review of the talent needs of manufacturers in Pinellas County, Florida, located on the West Coast of Central Florida. Manufacturing in Pinellas County (and extended into Tampa Bay includes electronics, defense, medical devices, aviation, and aerospace.

This paper investigates the hiring needs of local employers for engineering technicians in the region. The local employers may participate with St. Petersburg College on an advisory board, and the benefits of the advisory committees and their program recommendations are explored. Survey results suggest that there is a need for electrified vehicles, semiconductors, and quality-understanding engineering technicians. These employer needs are reviewed, and recommended solutions will be presented.

Introduction

Industry 4.0 outlines requirements for the future of manufacturing. There are areas of interest to engineering technology programs in that the graduates can perform functions to support the implementation and provide ongoing support to manufacturing organizations. There is a need to determine what skills are needed for an engineering technologist. This research intends to determine the needs of a skilled engineering technician and to what extent the manufacturers require the engineering technician to know about cybersecurity.

As Industry 4.0 expands, cybersecurity is expected to be an integral part of manufacturing floor operational technicians' responsibilities and part of the security team to protect equipment on the manufacturing floor [1]. Cisco [2] reports that 54% of companies surveyed have experienced a cybersecurity incident in the last 12 months. Cisco identifies applications as an added layer of complexity as malicious actors look at applications as a way to infiltrate a company's infrastructure to do damage. Cybersecurity will protect manufacturers' production floors and equipment from hackers and malicious actors.

This paper asked organizations in the Tampa Bay area on the West Coast of Florida to participate in a collaborative lab session. Pinellas County is the third largest county in the state for the manufacturing employee base and the second largest in the number of manufacturing organizations. Pinellas County is in the center of the eight-county Tampa Bay region. Pinellas County has significant industry clusters, including manufacturing, aviation, aerospace, defense, and life sciences. The country and the general Tampa Bay area need a talent pipeline in STEM careers. There is a need for training and education to close skills gaps for early career employees and an additional need for upskilling. The differentiation of the West Coast is offered as the East Coast of Florida focuses on space and related activities. The advisory committee members were surveyed to obtain their views regarding the need for technologies to be included in engineering technician programs. The input received from the organizations is provided and analyzed to develop an understanding of what understanding an engineering technician should have.

Literature Review

The need for engineering technicians is essential to the growth of industry in the United States. As the industry expands, the lack of manufacturing organizations are seeking to implement Industry 4.0. Skills needed for mechatronics technicians to work in the Industry 4.0 manufacturing community were reported by Acerbi and Rossi [3] to include the following:

- Knowledge about process speed and programming
- Expert interdisciplinary with various knowledge about instruments and components in manufacturing. The knowledge should include information about mechanical systems, robots, actuators, sensors, computer systems, and embedded systems
- Programming languages to use the above devices
- Ability to process data from sensors embedded in these systems
- Cyber-physical systems, which are systems that include networking, computation, and integration of sensors and other devices

Li [4] identifies a need for engineering technicians to understand virtual reality, cyber-physical systems, and the Internet of Things to participate in the workspace of future growth.

Material and Methods

Two approaches were taken to determine the required skills for regional technicians. The first approach consisted of a survey sent to 88 advisory board members (n=36 for responses) of 82 local representatives to gather input on their organizations' needs of graduates from the St. Petersburg College's Engineering Technician Department. A meeting in the college's collaborative laboratories was held to determine the skill needs for the engineering technician positions. St. Peterburg College' Workforce Division coordinated the meeting.

Stakeholders from local manufacturing companies, workforce support organizations, and St. Petersburg College gathered at SPC's collaborative labs to discuss an electromechanical workforce training program. The manufacturing representatives were presented with industry statistics for hiring, which included a discussion regarding that there are multiple titles for engineering technicians that conflict with the government classifications. For some companies at the meeting, a maintenance technician is highly skilled, and others regard the position as entry-level and needing a high school degree or equivalent.

The first meeting resulted in the attendees asking these questions:

- How do you capture and transfer subject matter expert knowledge from industry to the workforce?
- There is a force multiplier of joining forces between the manufacturers to fill gaps in industry needs.
- Equipment donations from the industry could be made to accelerate learning.
- There is a need to define soft skills and the needed technical skills.
- There has to be a combined emphasis on recruitment by the college and the employers. If you don't have people coming in, it does not matter what the curriculum is.
- Expanding the company's university model, the company provides education to the employees throughout their employment, replacing the need for college.
- Core competencies must be learned, and this takes time.
- The timeline for any education or training must be less than one year and could be delivered such that learning is done for a while and on-the-job training can be alternated.
- There is a need for swift training programs that get candidates working quickly.

The manufacturing industry participants then deployed into manufacturing and workforce support teams to discuss their engineering technology workforce needs and how they address them. During team report-outs, employers discussed having different job titles for similar positions, which can confuse their industry, HR managers, and candidates looking for employment. They also discussed apprenticeship programs; many were unsure if they would benefit their organizations.

The group discussed creating a standard engineering technician curriculum that could be an entry point for new employees. The employers listed the skills they would like to be taught in this curriculum and identified the top outcomes of standardizing a curriculum.

The top three desired outcomes determined by polling the attendees at the collaboration lab session are

- Basic electronics background, basic troubleshooting, including safety (understanding low and high voltage [480 v+], being able to follow schematics, understanding when you need to go to more experienced personnel for help and when to do that. reading a multimeter. have sub-classes for different specialties (vacuum, optics, mechatronics, project management)
- Schematic reading and understanding. Be able to review a schematic, have error detection skills, and understand how feedback works in a system
- Mathematics skills, including dimensional measuring in general (understanding tolerances

The manufacturers discussed forming an ad hoc, provisional Electromechanical Workforce Advisory Committee to support getting this program off the ground. They brainstormed which key stakeholder groups should be included and how this advisory committee would address regional talent needs. The manufacturers present felt the benefits of joining together through virtual meetings to guide by providing industry needs. The committee could obtain valuable input regarding specific skills needed and will grow the talent pipeline. This group will help create unified training and industry language and address gaps in skills required in the future.

The manufacturers attending the sessions requested the following for sessions to be developed in the following topics suggested. They asked for a course on how to work in the manufacturing engineering field. This feedback included soft skills such as writing a resume, calling in when you will be out from work, and how to schedule a vacation. A course would follow this course in soldering. All the companies in attendance thought the soldering skills were critical. They would allow the individual to have permanent employment at the company and be able to attend technician training. Some employers were requesting soldering compliance to the J-STD-001. This training would include an introduction to safety. The soldering skills had to be at a level that could work with small components. The attendees of the course would also be taught schematic reading. The students must also learn to use Word and Excel in this course. The students should also know die packaging and flip chip attach processes. The die preparation would be done using a microscope. Mechanical hands-on work needs to be done.

There is a need for the technicians to be able to do assembly work and entry-level work, which includes electronics, basic math calculations, radio frequency knowledge, reading schematics, and being able to match work instructions to schematics, controllers, and motors. The technician must have an understanding of electrostatic discharge and be able to follow procedures every single time. The technician must also know how to program a programable logic controller and understand lockout tagout requirements. The engineering technician must have many skills. The manufacturing organizations are requesting that these students be prepared in a term much shorter than the two years for the student to acquire an associate degree.

Questions

The questions to be investigated by this paper are as follows:

1. Employer expectations of the cybersecurity skills needed for engineering technology graduates.
2. Determine the hiring needs of the local engineering technology companies in the Tampa Bay Region.
3. Determine the local need for engineering technology students to understand electrified vehicles or semiconductor manufacturing.
4. What is the view of employers regarding the requirements for students to continue their education in Lean Six Sigma?

These questions will provide a basic understanding of the educational needs of the engineering technician. Question 1 is to investigate an area of education that is new for engineering technicians. Question 4 is an area that has been included in engineering education that may have become integrated into the manufacturing processes and no longer need to be included in academic engineering technician programs.

Data

A survey was sent to 88 members of the advisory committees supporting the engineering, manufacturing, and building arts programs at St. Petersburg College. Emails were sent to all 88 members, and 36 responded for a 41% response rate.

Total responses: 33 (plus three who stated not responding)

The advisory committee membership has reported the following functions for those who are part of the committee.

Vice president/director	28
CEO/president	23
Engineering	18
Marketing/sales	7
Human resources	6
Production/manufacturing	6
	88

Responses to cybersecurity skills needed by engineering technician graduates (more than one could be provided):

Not applicable	18
Cybersecurity (foundational)	6
No answer	4
Unknown	4
CMMC requirements	1
FedRamp	1
Medical device security	1

Network Segmentation	1
Computer literacy	1
Database	1
	38

CMMC is the Cybersecurity Maturity Model Certification
FedRamp standardizes the security requirements of cybersecurity cloud services.

Hiring needs:

Need but undefined	13
No needs	4
BioMed Technician	2
No answer	2
Mechatronics (4-6)/design (2-3)	1
Construction Management	1
Architectural drafting	1
30 technicians	1

Need for engineering technicians in semiconductor or electrified vehicles:

Yes	10
No	19
No answer	4
	33

Need for Lean Six Sigma knowledge:

Yes	18
No	11
No answer	4
	33

Results

The manufacturers report a need for engineering technicians, with one manufacturer reporting that they need 30. Most manufacturers report needing between one and four technicians if they are hiring. The manufacturers are not supporting specialized skills in cybersecurity, with 26 of the 33 responses not identifying any specific skills needed. Approximately one-third of the respondents feel that semiconductor or electrified vehicle skilled technicians will be required. Fifty-five percent of the respondents indicate that formal training is still needed for Lean Six Sigma.

Discussion

In this region, technicians need to be created in increased numbers. The current graduation rate for technicians is too low to support the growth needs in manufacturing. It was unexpected to find that cybersecurity needs for technicians were not well supported. In the responses, some construction field members may not believe that cybersecurity issues could affect their job sites.

Seven individuals identify with marketing and sales. These individuals may not think about the requirements of the manufacturing or production floors at their organizations. The 38 responses are higher than the number of participants as the questions allow two answers. Twenty-six individuals felt there were no answers to be provided. This lack of response indicates that those responding to this survey have not considered the impact of cybersecurity issues on the manufacturing floor and that awareness of this need must be heightened. Six individuals did respond with informed responses, indicating that 18% are aware of the need for engineering technicians on the manufacturing floor to be aware of cybersecurity issues.

The convening of meetings with the local manufacturing community revealed that they need technicians who can develop their skills in less than two calendar years. There is a need for the reported skills to be generated in the short term, which could be as little as eight weeks. There is an expectation that this training should take no longer than fourteen months. The skills listed in some instances exceed those taught in a two-year engineering program and would have to have the learning scaffolded so these specific areas could be taught and understood by the participants in the class.

The advisory boards suggested a strong need for engineering technicians in the region. The growth for some will be significant, requiring large numbers of technicians. Being aware of electrified vehicles, semiconductors, and Lean Six Sigma is essential to hire engineering technicians successfully.

Conclusion

The manufacturing community in the West Central Florida region needs engineering technicians. The manufacturing community has not yet identified cybersecurity as a strong need for engineering technicians. The manufacturing organizations anticipate the need for engineering technicians who understand soldering, electrified vehicles, and Lean Six Sigma.

References

[1] L. Marianna, L. Mariangela, and A Corallo. *Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework.* Science Direct. Available https://www.sciencedirect.com/science/article/abs/pii/S0166361518303658

[2] Cisco Cybersecurity Readiness Index, *Cisco Systems, 2023* *https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-market-snapshot-usa.pdf*

[3] Acerbi F, Rossi M and Terzi S (2022). Identifying and assessing the required I4.0 skills for manufacturing companies' workforce. *Frontiers in Manufacturing Technology, (2):*921445. Doi: 10.3389/fmtec.2022.921445

[4] Li, L. Reskilling and Upskilling the Future-ready. Workforce for Industry 4.0 and Beyond. *Inf Syst Front* (2022). https://doi.org/10.1007/s10796-022-10308-y

Biographies

MARILYN BARGER is the senior education advisor for FLATE part of the FloridaMakes Network, a Manufacturing Extension Partnership Center. She was the PI and executive director of FLATE, an ATE Center focused on manufacturing technology education in Florida for over 18 years. Today FLATE is part of the FloridaMakes Network (www.floridamakes.com), the NIST Manufacturing Extension Partnership Center in Florida which is continuing its NSF mission supporting manufacturing technician education. Dr. Barger serves on several national and regional workforce education boards and has developed award-winning curricula for STEM programs at all educational levels. She taught Environmental Engineering at Hofstra and FAMU-FSU College of Engineering, authored many engineering education papers, is a registered professional engineer in Florida, and a fellow of both the American Society of Engineering Education and the American Institute of Medical and Biochemical Engineers.

SIDNEY MARTIN holds BS and MS in electrical engineering from the University of Massachusetts, Dartmouth. He holds a Doctorate in Education from Murray State University, focusing on STEM. Dr. Martin has led manufacturing many high-reliability power electronic components used in space and military applications. His area of research is in the retention of underrepresented students in engineering. He is a licensed professional engineer (Manufacturing), a project management professional, a Lean Six Sigma Master Black Belt, and a Scrum Master. Dr. Martin enjoys teaching electrical and electronic courses. Electrical engineering is fascinating, and he is always willing to share his successes and failures. Dr. Martin was on the *Today* show (2008), demonstrating a waterproofed smartphone, radio, and other commercial items that did not need waterproofing at that time. Dr. Martin holds various patents on waterproofing electronics. Information about this waterproofing company can be found at www.hzo.com. Dr. Martin is an active Institute of Electrical and Electronic Engineering member and researches in the area of retention of underrepresented minorities in engineering. Recently, he has been researching advanced power electronics for the electrification of autonomous vehicles.

CATHERINE DAVIS is retired military and current adjunct for Saint Petersburg College. She has over 20 years background in systems administration, hardware and software troubleshooting, and network management for the federal government and more than 8 years as an adjunct. She received her bachelor's degree in Management Information Systems from the University of South Florida and her master's degree from Troy University also in Management Information Systems. Her expertise and courses taught include computer and information technology concepts, ethical hacking, network security foundations, introduction to computer programming (Python) and fundamentals of Linux/Unix operating environment.

APPENDIX I

The following is a cyber checklist that will assist in determining what frameworks are involved for risk assessments in identifying, assessing, and mitigating some of the cybersecurity threats. The framework addresses various aspects of cybersecurity, from hardware and software security to incident response planning. We should note that adopting these simple principles and multiple strategies can bolster the cybersecurity posture and effectively safeguard against the digital footprint left behind against any cyber intrusion.

A. Identify and Assess Cybersecurity Threats:

1. Hardware:

- Regularly assessing and updating firmware and software on all hardware devices can be crucial to preventing potential vulnerabilities.

2. Public Facing Application:

- This ensures the security of public-facing applications and regular assessments, including vulnerability scanning and security patches. This assessment process is imperative to the success of any cyber threats.

3. Internet Accessible Devices:

- Apply a zero-trust model approach to all internet-accessible devices enhances cyber threats.

- Defining access controls and restrictions further mitigates risks involved

4. Zero Trust Model:

- Implementing a zero-trust model involves distrusting entities and devices by default.

- Managing user access, enforcing strict device and network access control, and applying granular security policies are essential components of this approach.

B. Protect Assets from Cyber Intrusions:

1. Accounts:

- Enforcing robust authentication methods and regularly reviewing user accounts and permissions are essential for safeguarding.

2. Passwords:

- Strengthening password complexity and multifactor authentication (MFA) for critical accounts significantly enhances account security.

3. Security Approaches: Defense in Depth:

- Deploying edge firewalls, utilizing wireless security protocols, employing intrusion detection systems, host intrusion prevention systems, and web application firewalls are critical to any layer of defense.

4. Data:

- Classifying data based on sensitivity and implementing encryption for data at rest and in transit ensures data security

C. Detect Compromises:

1. Tools and Practices:

- Using various tools like Kali Linux for penetration testing, Burp Suite for web application security testing, deploying intrusion systems, and implementing Multifactor Authentication (MFA) aids in detecting unauthorized access. Applying Snort helps define any malicious network activity.

D. Plan for Compromise Response:

1. Prepare:

- Developing an incident response plan (IRP) and establishing an incident response team are foundational and practical responses to compromises.

2. Detect:

- Monitoring for signs of compromise using intrusion detection systems and real-time log monitoring helps in the early detection of incidents.

3. Analysis:

- Investigating and analyzing the nature and scope of a compromise enables informed decision-making during incident response.

4. Containment:

- Isolating affected systems to prevent further spread of the compromise is a crucial step in limiting network damage.

E. Recover and Implement Recovery Plan:

1. Risk Mitigation:

- Defining clear risk mitigation goals and strategies and assessing potential risks and their impacts aids in effective recovery planning.

2. Recovery:

- Developing and implementing a recovery plan, including data restoration from backups and data integrity verification, ensures a systematic recovery process.

We live in a quickly changing technology world and an era of escalating cyber threats. We need to have a robust cybersecurity framework to combat these changes. Organizations need to safeguard their digital assets. By identifying, preventing, detecting, and responding to cyber intrusions through the comprehensive strategies outlined in this paper, organizations can significantly enhance their cybersecurity posture and minimize the potential impacts of cyber threats.