Engineering Educators Bringing the World Together

2025 ASEE Annual Conference & Exposition

Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE

Paper ID #47058

Cyber-Informed Engineering Course Syllabus for Undergraduate Engineering Programs

Catalina Aranzazu-Suescun, Embry-Riddle Aeronautical University - Prescott

Dr. Catalina Aranzazu-Suescun is an assistant professor at Embry-Riddle Aeronautical University in the department of Cyber Intelligence and Security. She has a Ph.D. in Electrical Engineering from Florida Atlantic University. Her research interests are Wireless Sensor Networks and Security in IoT.

Ing. Luis Felipe Zapata-Rivera, Embry-Riddle Aeronautical University

Dr. Luis Felipe Zapata-Rivera is an Assistant Professor at Embry-Riddle Aeronautical University. He earned a Ph.D. in Computer Engineering at Florida Atlantic University, in the past worked as an assistant researcher in the group of educational Technologies at Eafit University in Medellin, Colombia. His research area is the online Laboratories

Cyber-Informed Engineering Course Syllabus for Undergraduate Engineering Programs

Abstract

Cybersecurity is a broad field that encompasses the development of mechanisms to prevent, detect, and recover from cyber and physical attacks. These security mechanisms should cover the security of a company's assets, the security of information (such as personally identifiable information (PII), know-how, and software), and the security of network components and devices. When a system has vulnerabilities in its software or hardware, it becomes an easy target for attacks. The motivation behind these attacks can include stealing information, gaining unauthorized access to data and networks, making a system unavailable, or damaging a company's reputation. Therefore, understanding how to minimize vulnerabilities in systems is crucial for reducing the likelihood of an attack.

Currently, few undergraduate engineering programs offer a minor in cybersecurity that provides the minimum knowledge an engineer should have to create secure engineering solutions. Moreover, only a few universities offer a Cybersecurity Engineering program. In this program, students learn to identify threats and vulnerabilities in hardware systems and software and apply these concepts in developing engineering solutions that are prepared for both physical and cyberattacks.

Cyber-Informed Engineering (CIE) is an emerging concept that integrates cybersecurity considerations into engineering projects, especially those involving the development of physical objects and machinery, such as cyber-physical systems. Without cybersecurity knowledge, the solutions engineers create can open doors for hackers to manipulate systems, machinery, or objects for their benefit. This creates a need to design and integrate CIE content into engineering undergraduate programs.

This paper presents a preliminary course syllabus design that can serve as a foundation for creating an undergraduate engineering curriculum tailored to different engineering programs. The proposed content can also be used to define a sequence of courses for a minor in Cyber-Informed Engineering, applicable to various engineering fields. As previously mentioned, the focus will be on undergraduate engineering fields that deal with software or physical machinery, such as software, computer, electrical, mechanical, and aerospace engineering, among others.

Introduction

With advances in technology and the increasing integration of the Internet into more aspects of our daily lives, cybersecurity has become an important topic that should be taught in every career, regardless of the field of work. Attackers are constantly searching for vulnerabilities in systems and networks to insert malware or launch attacks aimed at extracting or modifying sensitive information from users. However, not only are systems, networks, software, and hardware exposed to various threats, but individuals themselves can also become targets of several attacks due to misinformation and improper use of security measures. Techniques like social engineering are used to deceive people into providing information or performing actions that undermine the security of the institutions where they study or work. This situation has led to the understanding that people are the weakest link in the security chain.

In engineering fields that directly interact with technology, the Internet, machinery, cyber-physical systems, networks, and software, it is imperative to raise awareness among future professionals about the risks, threats, and vulnerabilities that any system can pose.

This paper proposes a cybersecurity course syllabus that will serve as the foundation for courses in a minor in Cyber-Informed Engineering. The rest of the paper is organized as follows: Section ”Literature Review” presents the state of the art in defining cybersecurity courses for engineering. Section ”Curriculum Proposed” outlines the preliminary curriculum proposed in this work. Section ”Discussion” explores potential challenges and future work. Finally, the conclusions are presented.

Literature Review

This literature review section explores the foundational concepts, frameworks, and research advancements in Cyber-Informed Engineering (CIE), highlighting key contributors who have shaped the field. It examines the integration of cybersecurity into engineering curricula, the development of industry standards, and the practical applications of CIE in critical sectors like cyber-physical systems, energy, transportation, and communications.

The need for cybersecurity awareness across various engineering fields has existed for over a decade. In 2015, George Mason University’s Volgenau School of Engineering introduced a new undergraduate program focused on producing engineers who can design and implement cybersecurity mechanisms in various industries, including infrastructure, healthcare, transportation, energy, and defense. This degree was called Cybersecurity Engineering[1]. Similarly, the Melbourne Institute of Technology (MIT) began offering a major in cybersecurity for both its bachelor’s and master’s programs in networking. This major enables students to acquire basic skills in the use of security tools, mitigation mechanisms, and business contingency planning for companies[2]. Professors from the University of Miami and the University of North Carolina Wilmington defined best practices for including cybersecurity courses in Computer Science, Information Science, and Engineering programs. The goal is to help institutions seeking designation by the National Security Agency (NSA) as a Center of Academic Excellence (CAE) in Cyber Operations (CO). Some of these best practices include incorporating hands-on learning activities, staying up to date with industry trends, using interdisciplinary approaches, and teaching secure software practices throughout the software development lifecycle[3]. Professors from Saint George University of Beirut and Applied Science Private University developed a framework for academia focused on cybersecurity awareness across various academic fields. The framework outlines required cybersecurity topics, best practices at the institutional level, and the use of learning management systems (LMS) to organize and deploy training modules for students[4]. Similarly, professors at the University of Helsinki designed guidelines for creating a cybersecurity curriculum for university-level programs, focusing on developing courses that align with workforce needs[5].

Beyond course inclusion and degree design, some researchers have developed strategies to enhance cybersecurity competencies among students from various engineering fields. Professors at the Universidad Politécnica de Madrid have been working on defining short educational videos and incorporating techniques like flipped classrooms to increase student engagement and help them learn fundamental cybersecurity skills[6]. Professors at Florida Gulf Coast University and Florida International University conducted a study in the Software Engineering program, where they assessed students' cybersecurity knowledge, their ability to identify project issues, and how they evaluated existing code. The case study involved pre- and post-tests designed to assess knowledge and skills before and after students completed various activities[7].

The Office of Cybersecurity, Energy Security, and Emergency Response, part of the U.S. Department of Energy, has been working on strategies to promote the concept of Cyber-Informed Engineering (CIE). They define CIE as an evolving approach that integrates cybersecurity principles throughout the entire lifecycle of physical systems—whether in energy, transportation, or other sectors—aimed at reducing or preventing vulnerabilities to cyberattacks. From this perspective, CIE emphasizes the incorporation of cybersecurity into the design, development, and operation of these systems, using engineering decisions and controls to minimize the potential impact of cyber threats on critical infrastructure and asset owners. The goal is to strengthen defenses against the most severe consequences of cyberattacks[8].

Recently, the IEEE Standards Association approved a PAR titled ”Guide for Cyber-Informed Engineering Curricula,” where a new working group will define competencies and learning outcomes for CIE education. This group will provide a framework for higher education institutions to design and deliver courses, certificates, and badges. This standard will guide institutions in incorporating CIE principles into existing engineering programs or developing standalone courses, ensuring that graduates acquire the skills needed to strengthen the resilience and security of cyber-physical systems[9].

The Idaho National Laboratory (INL) is developing CIE to incorporate cybersecurity into engineering practices for critical infrastructure. INL focuses on developing tools, standards, and educational resources that prioritize cybersecurity in the design and operation of infrastructure systems. INL also promotes a 200-member CIE Community of Practice that fosters collaboration and knowledge sharing. INL is working on a CIE Implementation Guide and Resource Library to support the adoption of CIE practices and generate strategic partnerships with academia and industry to integrate CIE principles into engineering programs and infrastructure projects. Through these efforts, INL ensures that infrastructure is designed with built-in cyber defenses, improving the resilience of energy systems against potential cyber threats[10].

Course Proposed

Course Definition

This course is designed to provide engineers with a comprehensive understanding of cybersecurity principles and practices essential for securing critical infrastructure and systems. It covers key topics such as threat detection, security assessment, methodologies for securing systems, and incident response. Engineers will gain hands-on experience in identifying vulnerabilities, implementing security measures, and integrating cybersecurity into the lifecycle of engineering projects. By the end of the course, students will have the skills necessary to proactively defend against cyber threats, ensuring the resilience and security of both cyber-physical systems and the broader engineering infrastructure they create and support.

Figure 1 presents the recommended placement of the CIE course within the flowchart of an engineering program. The junior/senior year is suggested for the inclusion of the CIE course due to the level of knowledge students have in their engineering field. In their senior year, they can apply cybersecurity concepts to their final projects or capstones. However, the cybersecurity content does not require any prior knowledge or prerequisite courses in the cybersecurity field.

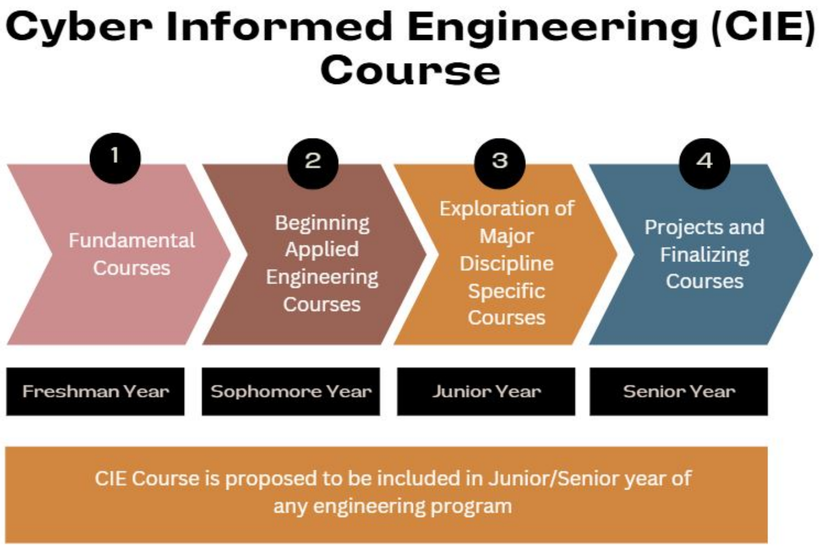
Cyber Informed Engineering (CIE) Course
1
Fundamental Courses
2
Beginning Applied Engineering Courses
3
Exploration of Major Discipline Specific Courses
4
Projects and Finalizing Courses
Freshman Year
Sophomore Year
Junior Year
Senior Year
CIE Course is proposed to be included in Junior/Senior year of any engineering program

Figure 1: Recommended Placement of the CIE Course within the Flowchart

To better tailor the course to the various engineering disciplines, several considerations must be taken into account. First, the core course content should remain consistent across all programs. Second, examples, practical problems, activities, and projects should be specifically designed to align with and reflect the unique challenges and principles of each discipline, ensuring their relevance and applicability. In this line, professors teaching the course should customize the activities to align more closely with the particular engineering specialties of their students.

For example, in an industrial engineering program, physical security topics should be explored through challenges related to access control of people to production plants. In contrast, in a computer engineering program, the same topics should be presented in the context of securing access to data center facilities.

Another example is for chemical engineers in the topic of incident response, laboratories should have well-defined policies to prevent accidents, along with mechanisms to detect incidents when they occur. Additionally, there should be action plans in place to respond effectively to such incidents. In contrast, for software engineers, the focus should be on preventing vulnerabilities in their code, such as hardcoded credentials and misconfigured services. Systems should be capable of analyzing software products to identify these issues during testing phases. Additionally, companies and institutions should have a structured response plan for handling software-related incidents.

Learning Outcomes and Assessments Instruments

Table presents the proposed learning outcomes for the course and the possible assessment instruments to evaluate the performance of these learning outcomes. The proposed assessment instruments can be modified or adjusted depending on:

- Particular aspects of the class
- Engineering discipline of the students
- Evolution of the course over multiple semesters
- Preferences of the faculty member

Table 1: Learning Outcomes and Proposed Assessment Instruments for the course

Learning Outcome	**Proposed Assessment Instruments**
Students will be able to assess potential cybersecurity threats and vulnerabilities within engineering systems, performing risk assessments to prioritize and mitigate risks to critical infrastructure	Homework and in-class activities on the topic of security assessment and risk management
Students will be able to apply principles of secure system design to engineering projects, integrating cybersecurity measures at every stage of the system lifecycle: design, implementation, deployment, and maintenance	Course final project
Students will develop the ability to implement security controls, such as encryption and access control, and deploy effective threat detection and response mechanisms to secure systems from cyber-attacks	Homeworks and quizzes in the topics of cryptography, access control, and incident response
Students will demonstrate the ability to integrate cybersecurity principles into their engineering workflows, ensuring that all aspects of critical infrastructure projects are designed, developed, and operated with security as an essential component	Course final project
Students will demonstrate knowledge of, and facility with, cyber resources available to make decisions regarding risk and trade-offs based on value	Quizzes and in-class activities during the course

Course Topics

Table 2 presents key topics that serve as the foundation for cybersecurity proficiency among professionals, particularly engineers. These topics are critical for developing a strong cybersecurity understanding in the context of engineering practice. Each topic is carefully selected with a rationale for its inclusion, explaining its relevance to engineering roles. Additionally, the table cites sources that recognize these topics as essential for cyber-aware professionals, highlighting their integration into existing courses, cybersecurity textbooks, and relevant literature reviews.

The topics presented in the table are commonly covered in introductory cybersecurity courses within both cybersecurity and engineering programs, forming the core knowledge base for professionals entering the field.

Table 2: Topics Proposed

Topic	Detailed Subtopics	Description	Justification	Presented in Source
Malware	Main Categories: Infecting and Hiding. Types: Virus, worms, trojan horses, rootkits, spyware, adware, botnets.	Malware, or malicious software, is a program designed to perform attacks such as stealing information, modifying or deleting data, and providing remote access and control to an attacker. There are two main categories of malware: infecting and hiding. ”Infecting” spreads the malware to adjacent network devices, while ”hiding” seeks to conceal its traces and avoid detection.	Engineers often work on projects that require collaboration with teams distributed across different locations. In this context, having a fundamental awareness of cybersecurity threats and the skills to identify malicious applications or code is crucial. These capabilities help prevent data breaches and unauthorized access, safeguarding sensitive information from potential theft and cyberattacks.	[1] [4] [10] [11] [12] [14]
Cyber-attacks	Types of Attacks: Physical or Cyber. Types of Physical Attacks: Hardware attack, tailgating, surveillance. Types of Cyberattacks: Active (password attacks, man-in-the-middle, spoofing, replay attacks, Denial of Service) and Passive (reconnaissance, sniffing).	Cyberattacks are malicious assaults on computers, systems, or networks. They can be classified as active attacks, which involve modifying data or attempting to gain unauthorized access to locations, or passive attacks, which do not alter the system but are carried out to monitor traffic, data, or people.	Having a clear understanding of the different types of cyberattacks and their methods reduces the likelihood of engineers becoming targets of cyber threats. Knowing how to prevent and detect attacks is essential in every project development.	[4] [10] [11] [12]

Continued on next page

Table 2 – continued from previous page

Topic	Detailed Subtopics	Description	Justification	Presented in Source
Social Engineering	Types: Pretexting, phishing, vishing, smishing, baiting, piggybacking, quid pro quo.	Social engineering is a type of attack where authorized individuals are manipulated to carry out actions for attackers, such as providing confidential or sensitive information or accessing restricted areas.	Engineers working on collaborative projects are often unaware of the identities and authorization levels of other individuals. Developing an understanding of social engineering attacks significantly reduces the risk of engineers becoming targets. By recognizing that attacks can originate not only from software but also through human interaction, engineers can better protect themselves and their work.	[4] [11]
Network Security	Network Vulnerabilities and Attacks: Methodologies to Secure Networks.	Network security involves various methodologies used to prevent attacks by unauthorized individuals on a network. To effectively apply these methodologies, it is essential to understand the vulnerabilities and potential attacks that a network can face.	Understanding network vulnerabilities and attacks is crucial for engineers, as it helps them develop strategies and practices designed to prevent unauthorized access, data breaches, and other cyber threats commonly reported on computer networks. Engineers can implement targeted measures, prioritize resources, and adapt security protocols to evolving threats.	[1] [2] [5] [10] [11] [13] [14]
Cryptography	Types of Cryptography: Symmetric (Stream ciphers and block ciphers) and Asymmetric (Digital signatures, exchange of symmetric keys, and certificates). Hashing.	Cryptography involves the study of techniques used to convert plaintext into ciphertext. This ensures that only authorized individuals can use, modify, and delete the information, while also providing non-repudiation.	Engineers should be able to protect their information and use techniques to ensure its integrity. This includes designs, processes, and procedures, as well as input datasets and output result data.	[1] [3] [5] [10] [11] [12] [13] [14]
Access Control	Types of Access Control: Physical and Logical. Four Steps of Access Control: Identification, Authentication, Authorization, and Accountability.	Access control is the process of protecting a network, system, file, application, or location to ensure that it is used only by authorized individuals, preventing unauthorized use of these resources.	Engineers should understand the importance of granting proper permissions for accessing project resources only to authorized users. This helps in identifying legitimate users, understanding the mechanisms used to validate their identities, defining security policies, and documenting interactions for accountability.	[1] [5] [10] [11] [13]

Continued on next page

Table 2 – continued from previous page

Topic	Detailed Subtopics	Description	Justification	Presented in Source
Security Assessment	Definition and Main Differences Between Vulnerability Assessments and Penetration Testing	Security Assessments are periodic exercises that test an organization's security preparedness. They can be conducted using automated tools to find vulnerabilities in the system or by performing simulated attacks on the network, a practice commonly known as penetration testing.	Security assessments are important because they allow engineers to proactively identify potential threats and vulnerabilities in their systems. This enables them to develop preventive measures and mitigation strategies, ultimately minimizing the impact of potential cyberattacks.	[11] [13]
Risk Management	Definition and Steps for the Risk Management Process	The risk management process, or risk assessment, involves identifying, analyzing, evaluating, and treating risks that could occur in an institution, typically to prevent them. Risks are identified not only in cybersecurity but also in financial, environmental, legal, and other areas.	Engineers across various industries must possess the knowledge and skills to perform risk management, enabling them to identify potential threats in different areas. This proactive approach allows them to prevent incidents before they occur, not just from a security perspective, but across a range of other fields as well.	[3] [5] [10] [11]
Incident Response	Definition. Configuration of Defenders (Firewalls, Intrusion Detection Systems, and Intrusion Prevention Systems). Incident Response Methodologies: Digital Forensics, and Network Forensics	Incident Response is a methodology used to search for and monitor networks, systems, software, and computers to detect malicious actions that may have eluded security measures. The incident response process begins with the detection of abnormal activity in the network. Next, evidence is gathered and analyzed, followed by the presentation of a report with the findings.	Engineers must be equipped with the ability to respond effectively during a cyberattack. Establishing a clear and comprehensive set of procedures for both immediate response and post-incident actions is crucial. This ensures that cybersecurity experts can efficiently carry out mitigation and corrective measures on affected systems, minimizing damage and facilitating a smooth recovery.	[1] [2] [3] [5] [10] [13]

Source[11] is used as the required textbook for the CI120 Introduction to Cybersecurity course. Source[12] was developed by the Massachusetts Institute of Technology in 2021. Source[13] presents the topics for the Cybersecurity bachelor's degree at Purdue University.

Discussion

The proposed cybersecurity course for engineers serves as a foundational step in promoting consensus and sparking discussions that will lead to the development of a tailored curriculum suitable for various engineering programs. The course aims to equip engineers with the knowledge necessary to work on large-scale projects without compromising their integrity due to cybersecurity lapses. Additionally, it empowers engineers to integrate cybersecurity measures into their designs and systems, ensuring the protection and resilience of both their creations and their implementations.

The topics defined for the course can also be extended to serve as in-depth courses, forming the basis for a minor in any engineering discipline. Related topics, such as security assessment and risk management, can be considered part of a cybersecurity minor.

One important aspect to highlight is that the topics proposed in our work cover the most essential aspects of cybersecurity that every engineer should know. In the literature review, these topics are not confined to a single course; rather, most are defined across multiple courses or even as part of a complete curriculum for a bachelor's degree. Another aspect to feature is that the reviewed existing cybersecurity initiatives for engineering programs are presented in the form of short modules, tests, and certificates to ensure that engineers develop awareness and implement best practices in their engineering project development. One of the goals of this work is to propose a course content that can be integrated as an elective or even as a core course in the curriculum. The goal of offering a course like this is to prepare engineering students on the fundamental topics of cybersecurity and their application in the development of specific engineering solutions.

Defining cybersecurity content for a diverse range of engineering programs presents a significant challenge. Fields such as software, electrical, systems, communications, and computer engineering often have distinct needs compared to disciplines like mechanical, civil, environmental, aerospace, materials, and chemical engineering. For instance, software engineers prioritize data management more heavily than materials engineers, whereas mechanical engineers place a greater emphasis on protecting cyber-physical systems compared to systems engineers.

Conclusions

Cybersecurity skills are essential for professionals across various fields. This work presents the definition of a course, including its objectives, learning outcomes, and the micro-curriculum of an undergraduate cybersecurity course for engineers. The course proposal highlights the critical importance of integrating cybersecurity training into the curricula of all engineering programs.

Taking this course will enhance students' awareness of the crucial importance of incorporating cybersecurity mechanisms into every engineering project. It will emphasize the need to address security challenges proactively, ensuring that projects are robust, secure, and prepared to handle potential threats.

Having a structured and standardized course definition will provide higher education and accreditation institutions with a compelling case for its inclusion as a required course in the curricula of engineering programs.

References

[1] P. Brouse. Systems engineering in a cyber security engineering program. *Incose International Symposium*, 25 (1):1403–1416, 2015. doi: 10.1002/j.2334-5837.2015.00138.x.

[2] S. Bevinakoppa, A. Alazab, and T. Jan. Design of computer networking courses with major in cyber security. *International Journal of Education and Learning Systems*, 3(2018):111–116, 2018. ISSN 2367-8933.

[3] A. Sobel and R. Vetter. Cybersecurity best practices for cise programs. *Computer*, 55(5):64–72, 2022. doi: 10.1109/MC.2021.3109841.

[4] M. Khader, M. Karam, and H. Fares. Cybersecurity awareness framework for academia. *Information*, 12(10), 2021. doi: 10.3390/info12100417.

[5] S. Ramezanian and V. Niemi. Cybersecurity education in universities: A comprehensive guide to curriculum development. *IEEE Access*, 12(2024), 2024. doi: 10.1109/ACCESS.2024.3392970.

[6] B. Bordel, T. Robles R. Alcarria, and D. Martin. Flipped classroom and educational videos to improve the cybersecurity competencies in future computer engineers. In *13th International Conference on Education and New Learning Technologies*, 2021. doi: 10.21125/edulearn.2021.0080.

[7] I. A. Buckley, J. Zalewski, and P. J. Clarke. Introducing a cybersecurity mindset into software engineering undergraduate courses. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 9(6): 111–116, 2018. doi: 10.14569/IJACSA.2018.090661.

[8] US Department of Energy. Cyber-informed engineering, 2024. URL `https://www.energy.gov/ceser/cyber-informed-engineering`.

[9] IEEE SA Standards Association. P3528 - guide for cyber informed engineering curricula, 2024. URL `https://standards.ieee.org/ieee/3528/11844/`.

[10] INL Idaho National Laboratories. Cyber-informed engineering, 2025. URL `https://inl.gov/national-security/cie/`.

[11] Testout Staff. *LabSim for Security Pro*. TestOut Corporation, USA, 2024.

[12] D. C. Wilson. *Cybersecurity*. MIT Press, USA, 2021.

[13] Purdue University. Cybersecurity, bs, 2025. URL `https://catalog.purdue.edu/preview_program.php?catoid=17&poid=31984`.