INL/RPT-24-82020-Revision-0



# Cyber-Informed Engineering Adoption in University Engineering Programs

September 2024

Benjamin Ruhlig Lampe, Edward Huang, Daniel Cole , Shane McFly, Matt Luallen, Casey O'Brien, Dominic Saebeler, Sin Ming Loo, Saman Zonouz, Animesh Chhotaray, Krystel Castillo , Gonzalo Martinez Medina

Changing the World's Energy Future


*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

INL/RPT-24-82020-Revision-0

# Cyber-Informed Engineering Adoption in University Engineering Programs

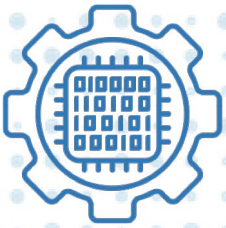
**Benjamin Ruhlig Lampe, Edward Huang, Daniel Cole , Shane McFly, Matt Luallen, Casey O'Brien, Dominic Saebeler, Sin Ming Loo, Saman Zonouz, Animesh Chhotaray, Krystel Castillo , Gonzalo Martinez Medina**

**September 2024**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**



Cyber-Informed Engineering

# CIE Adoption in University Engineering Programs

## An Overview of CIE Integration Successes at Nine U.S. Educational Institutions

September 2024

INL/RPT-24-82020-Rev000

Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

# Contents



# Acknowledgments


Report development was led by Idaho National Laboratory (INL) with significant support from university partners and members of the CIE Community of Practice (COP) Education Working Group. In particular, the universities listed below shared their direct experiences integrating CIE into engineering programs.

Report Development Team:

**Benjamin Lampe**
Idaho National Laboratory

**Matt Luallen**
University of Illinois at Urbana-Champaign

**Saman Zonouz**
Georgia Tech

**Edward Huang**
Auburn University

**Casey O'Brien**
University of Illinois at Urbana-Champaign

**Animesh Chhotaray**
Georgia Tech

**Daniel Cole**
University of Pittsburgh

**Dominic Saebeler**
University of Illinois at Urbana-Champaign

**Krystel Castillo**
University of Texas at San Antonio

**Shane McFly**
National Renewable Energy Laboratory &
Colorado School of Mines

**Sin Ming Loo**
Boise State University

**Gonzalo Martinez Medina**
University of Texas at San Antonio

# 1. CIE Adoption Overview

This report examines the adoption of Cyber-Informed Engineering (CIE) in university engineering programs, driven by the need to protect critical energy infrastructure from adversarial threats. CIE equips current and future engineers and technicians with the necessary mindset, skills, and competencies to enhance the resilience of engineered systems against cyber attacks. **This report highlights nine academic partners who are incorporating CIE into their curricula through various approaches, including lectures, courses, and certificates**.

CIE is a framework for engineers and technicians to integrate engineering controls that reduce or mitigate the impact of cyber attacks into any cyber-physical system, used in critical energy infrastructure or in other industries.

**Learn More about CIE**
Visit DOE CESER's CIE Program page to find CIE background and resources.

Embedding CIE into formal education, training, and credentialing is one of the five key pillars of the National CIE Strategy.[1] This report highlights the CIE adoption strategies of leading academic institutions, representing a critical first step to prepare the next generation of system designers, operators, and users to build and maintain a more secure and resilient cyber-physical environment. CIE coursework not only builds understanding of secure engineering practices in this modern digital age but also how to implement them effectively to ensure resilient behavior over time.

**This report is a companion to the Cyber-Informed Engineering (CIE) Curriculum Guide**, Version 1.0, which provides strategies and guidance for integrating CIE into engineering programs and educational activities. That Guide offers several strategies for adopting CIE topics and material into accredited programs, and includes detailed examples and insights from the university partners highlighted in this Adoption Report.

This companion report compiles and showcases active efforts by universities to integrate CIE into their programs. The goal is to teach engineering students to naturally consider cyber risk in their work, which can lead to a reduction in cybersecurity impacts in engineered systems. These approaches are merely examples and do not represent the full range of options for CIE integration into academic curricula.

## GET INVOLVED

For institutions considering the adoption of CIE or those that have already started, this report is an invitation to engage and share knowledge. The Department of Energy encourages institutions to reach out for help in developing CIE courses and to share their experiences in implementing CIE. This exchange of information is crucial for refining CIE educational materials and practices. Institutions that have integrated CIE into their curricula are encouraged to collaborate by sharing

[1] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. *National CIE Strategy*. June 2022. https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document.

how they have approached this task. Email CIE@inl.gov to request support, share resources, or to join the CIE Community of Practice and its Education Working Group.

# 2. Academic Partnerships

This section provides a snapshot of the academic institutions that have begun incorporating Cyber-Informed Engineering (CIE) into their programs for the recent or upcoming academic years. On the following pages, each institution outlines its approach to CIE adoption.

**Figure 1. Educational Institutions Implementing CIE in Engineering Programs**


It should be recognized that these examples are part of an emerging trend, as many more universities are currently in discussions with the Department of Energy's CIE Program to determine their plans for integrating CIE in future academic years. This report focuses on the immediate steps taken by these academic partners, setting the stage for the anticipated expansion of CIE integration in engineering education.

BOISE STATE UNIVERSITY

## Boise State University

Cybersecurity education at Boise State ranges from cybersecurity awareness to technical tracks in various cybersecurity topics. The technical tracks include courses, certificates, and degrees that support learning in cyber-informed engineering.

## CURRICULUM

### Courses

The computer systems engineering degree balances skills from both computer science and electrical engineering, with a focus on designing systems with cybersecurity in mind. This newest undergraduate degree in computer systems engineering includes two cyber courses. The first is a 3-credit hour introductory course that includes why cybersecurity, security engineering and frameworks, cryptography, IT vs. OT, pen testing, risk assessment, open-source intelligence, cyber-informed engineering frameworks, and ethics. The second course is Cyber-Informed Engineering. This course aims at designing systems in the cyber age. Designing reliable and resilient systems for cyber applications, viewed as a step-by-step process through the system life cycle, from design through development, production, and management, with cyber as part of the design specifications.

For our students in the asynchronous online cyber operations track, we also offer a one-credit hour cyber-informed engineering course. The goal of this course is to help students understand the nuances of designing and developing systems that are cyber-informed. Cyber touches every aspect of our lives, and more and more systems have some level of connectivity to the Internet. This exposes these systems to the risks associated with the Internet, as these systems could become targets for cyber attacks. These systems could be mission-critical systems, lifesaving and life-supporting systems, mechanical autonomous systems, industrial control systems, critical infrastructure, and so on.

## Certificate Programs

We also need our engineering students to be cyber literate so that they can competently navigate their domain space when addressing cyber challenges. This means that STEM graduates will be aware of cyber issues that impact the security of the programs, systems, codes, or algorithms they design. This is a 12-credit hour certificate for students in multiple engineering programs (very popular for electrical engineering students). All certificates have a common course of introductory cybersecurity topics, mentioned above. Students can choose the other nine credit hours from a list of courses for various certificates.

Our four certificate programs include:

1. Security in Cyber Physical Systems Software Focus
2. Security in Cyber Physical Systems Hardware Firmware Focus
3. Security in Cyber Physical Systems Power Systems Focus (the most popular)
4. Security in Cyber Physical Systems Industrial Processes Focus

## Auburn University

To educate our future engineers with the CIE mindset throughout the entire engineering lifecycle, Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security develops diverse educational activities. These initiatives include curriculum design, course offerings, and seminars hosted by student organizations at Auburn University.

Cybersecurity challenges are inherently complex and require an interdisciplinary approach to protect the diverse range of systems and sectors that require safeguarding. Instead of solely concentrating on identifying and rectifying vulnerabilities, the principles of Cyber-Informed Engineering (CIE) integrate cybersecurity considerations right from the inception of system design, long before the inclusion of software and security controls. This proactive approach empowers engineers to address security concerns well ahead of integrating software and security controls, ensuring a more resilient and robust system from its inception.

Focusing on systems engineering and digital engineering across various engineering disciplines, Auburn's CIE activities aim not only to foster cybersecurity specialists but also to equip traditional engineers with the mindset needed to tackle the risks posed by cyber systems in critical infrastructure systems. Auburn University is one of only ten universities in the Nation to hold all three Centers of Academic Excellence (CAE) designations in Cyber Operations (CAE-CO), Cyber Defense (CAE-CD), and Research (CAE-R) from the National Security Agency (NSA) and Department of Homeland Security (DHS).

## CURRICULUM

### Classes and Lectures

In the upcoming semesters, we will utilize single classes to explore the benefits of implementing CIE. Qualitative discussions on the advantages of CIE will be incorporated into lectures within the Digital Systems Engineering course, while the benefits will be quantitatively measured in the Model-Based Systems Engineering course. By dedicating specific lectures or segments thereof to this topic, students will gain insights into both the qualitative and quantitative aspects of CIE's impact on engineering practices.

### Courses

For our curriculum design, in collaboration with the Thomas Walter Center at Auburn University, we will integrate CIE principles into our existing undergraduate programs, in-person master's/PhD programs, and the online Master of Engineering Management program. CIE concepts will infuse the core courses of product design and systems engineering. These efforts will empower students across various levels—undergraduate, master's, and PhD—as well as diverse disciplines such as business, engineering, and education, to cultivate CIE mindsets from product inception through development, manufacturing, operations, and retirement across the entire life cycle.

Examples of courses that are or are planning to include introductory CIE modules include:

- INSY 4970/7970 (offered every Fall): Systems Engineering
- INSY 7710 (offered every Spring): Life Cycle Engineering
- INSY 4970/7970 (offered every Fall): Digital Systems Engineering Design
- INSY 4970/7970 (offered every spring): Model-Based Systems Engineering

All four of these courses constitute the core curriculum for our emerging Auburn University Systems Engineering Program, designed to accommodate students from all engineering disciplines at Auburn University. Engineering students across various fields—such as Aerospace Engineering, Biosystems Engineering, Chemical Engineering, Civil Engineering, Computer Science, Electrical and Computer Engineering, Industrial and Systems Engineering, and Mechanical Engineering—are eligible to enroll in this program, equipping them to learn CIE for designing and managing entire life cycles. Moreover, the first two courses will be academically equivalent to the International Council on Systems Engineering (INCOSE) Associate Systems Engineering Professional (ASEP) certificate, ensuring students acquire both systems engineering knowledge and CIE competencies. The third and fourth courses will impart engineering modeling and design skills within the context of model-based systems engineering, emphasizing not only technical capabilities but also the seamless integration of CIE principles into the systems engineering design process and framework.

By infusing CIE principles into the core curriculum of the systems engineering program at Auburn University, students will establish a solid foundation in CIE before branching out into various engineering disciplines, including our cybersecurity program, for subsequent courses. This approach affords students the opportunity to cultivate both breadth and depth of knowledge in applying CIE principles to real-world scenarios.

In addition to our course offerings, our Auburn University team will develop CIE implementation examples. Within the Digital Systems Engineering Design course, students will engage in semester-long projects aimed at applying model-based systems engineering techniques to design systems from concept inception through to testing, verification, and validation. We will select diverse applications from various domains to demonstrate CIE implementation across the entire life cycle. These examples will serve as reference models to assist future students in integrating CIE with the systems engineering process.

## STUDENT ENGAGEMENT

Auburn University supports several student organizations including the Auburn University Ethical Hacking Club (AUEHC), American Institute of Aeronautics and Astronautics (AIAA) Design Build Fly club, the American Society of Mechanical Engineers (ASME), INCOSE, the Institute of Industrial and Systems Engineers (IISE), and the American Society of Safety Professionals (ASSP). The CIE principles will be promoted in these student organizations.

**For more information** on Auburn University's approach to incorporating CIE into the Systems Engineering program, please contact cie@auburn.edu.

## Georgia Tech

Georgia Tech has adopted CIE principles through multiple avenues – innovative research, education, and interdisciplinary collaboration– to strengthen the security and resilience of critical infrastructure sectors.

Georgia Tech's adoption of CIE can be illustrated through our Security of Engineered Systems (SES) Vision. The SES initiative, led by Saman Zonouz, addresses cross-sector security challenges and resilience issues by developing engineering platforms with built-in security principles. SES aims to create a holistic security strategy integrating research, education, and technological innovation to develop solutions such as vulnerability discovery, risk assessment, and incident response. Enabled by CIE principles, the initiative also focuses on education and workforce development by establishing comprehensive curricula for students and professionals in cybersecurity for critical infrastructures. Additionally, SES, in coordination with Georgia Tech Research Institute, is developing multi-sector testbed facilities to support experimentation, technology transfer, and entrepreneurship, thus advancing secure and resilient critical infrastructures.

### CURRICULUM

#### Courses

At Georgia Tech, several courses have been designed to align with CIE principles and prepare students to tackle cybersecurity challenges in critical infrastructures. Our "Cybersecurity of Drones" course offers a hands-on in-depth exploration of resilience issues in unmanned aerial vehicles, teaching students to secure drone systems from cyber threats through hands-on techniques and research projects. The "Introduction to Cyber-Physical Systems Security" course introduces students to the fundamental security concepts specific to cyber-physical systems (CPS), enabling them to understand the complexities involved in securing interconnected digital and physical systems. Furthermore, the "Critical Infrastructures Security and Resilience" course provides a comprehensive examination of security challenges in modern critical infrastructures, covering concepts such as safety, reliability, and recovery. These courses are informed by CIE principles such as Secure Information Architecture, Planned Resilience, and Interdependency Evaluation, ensuring that students gain the necessary skills and knowledge to address the unique cybersecurity challenges of critical infrastructures.

#### Degree Programs

Georgia Tech's Online Masters of Cybersecurity Program, directed by Saman Zonouz, offers a Cyber-Physical Systems (CPS) track designed to train professionals to design, analyze, and maintain resilient systems capable of withstanding both accidental disruptions and sophisticated cyber attacks. Influenced by CIE principles, the recently revised program curriculum includes courses from multiple schools and departments, providing a broad education in CPS security monitoring, attack detection, risk analysis, and intrusion response. Some of the courses that are offered as part of the CPS track are Introduction to Cyber-Physical Systems Security,

Introduction to Cyber-Physical Electrical Energy Systems, Power Systems Protection, Advanced Topics in Malware Analysis, and Advanced Hardware Oriented Security & Trust.

## RESEARCH AND COLLABORATION

### Research Projects

The Vertically Integrated Projects Program (VIP) fosters interdisciplinary collaboration by engaging undergraduate and graduate students in long-term, large-scale projects led by faculty members. Through these projects, students gain practical experience in addressing complex, interconnected engineering challenges, which is key to achieving CIE principles. By working in multidisciplinary teams, students learn to evaluate interdependencies and design holistic solutions that enhance critical infrastructure security and resilience.

If you have any questions on any of these avenues of adopting CIE, please reach out to us at cie@groups.gatech.edu.

## University of Pittsburgh

The University of Pittsburgh's (Pitt) long-term goal is to integrate cyber-informed engineering (CIE) into the undergraduate and graduate curriculum at Pitt and develop educational content with hands-on experiences on cyber-informed engineering.

### CURRICULUM

#### Certificate Programs

The Swanson School of Engineering recently announced the creation of a new "Cybersecurity in Emerging Engineering Systems" undergraduate certificate with plans to bundle courses on cybersecurity, engineering systems, and artificial intelligence. This new certificate allows all majors to participate if desired.

### RESEARCH AND COLLABORATION

#### Research Centers

Pitt faculty have created a Cyber Energy Center with Department of Energy funding. The Cyber Energy Center will develop a graduate program in cybersecurity with a focus on cyber-informed engineering.

In the summer of 2023, Pitt worked with Idaho National Lab (INL) to develop industry-relevant cyber-informed engineering solutions, while also training eight undergraduate honors students. Forming two teams of four diverse students and using the mission model canvas as their main tool, the teams investigated two problems. The first problem focused on strategies for convincing executives in energy-related companies to invest in cyber-informed engineering. The second problem, under the assumption that the company invested into cyber-informed engineering, investigated implementation hurdles, both technical and social, for personnel within the company.

In 2024, we built on the findings of the 2023 cohort, describing how a training workshop in cyber-informed engineering should be adopted and communicated to energy companies and on INL's goals. In collaboration with INL staff, we focused on cybersecurity educational modules. The focus was for students to design and develop curriculum that can be used in university courses and for company training or seminars. We are increasing the size of the program to 16 students to enable us to have four teams of four develop a more complete curriculum.

We focused on defining use cases emphasizing the integration of IT (information technology, which includes networking, data processing and exchange) and OT (operational technology, which includes physical processes, control, and machinery) in electric power applications. We are adopting the Lean Innovation approach to find the use cases and rank/filter them based on consequence-driven principles in CIE design. After defining the use cases, students described

how to implement cyber-informed engineering during IT-OT integration. Students then created videos describing the use cases and the potential approaches for CIE design in each use case. These videos will be used as supporting material for introducing CIE design examples in university courses, industry training, etc. In addition, students worked on hands-on experiments to emulate different threats based on the use cases identified. Each experiment will emphasize some cybersecurity principles and mitigation approaches.

## University of Illinois Urbana-Champaign

Cybersecurity problems are inherently complex and multifaceted due to the diverse systems and sectors that require protective measures. Under the leadership of the Information Trust Institute (ITI) within the Grainger College of Engineering at the University of Illinois Urbana-Champaign (UIUC), we are implementing a proactive security approach from the outset of the engineering life cycle, or what is known as cyber-informed engineering. This approach is reflected in a variety of educational offerings, including credit courses for undergraduate and graduate students, as well as non-credit options for workforce development and reskilling across multiple colleges - business, education, and engineering.

## CURRICULUM

### Courses

In partnership with faculty across the Grainger College of Engineering, ITI has introduced the concept of CIE, which is being gradually introduced (or there are plans to introduce) modules within existing courses beginning with the 2023/2024 academic year. These courses will initially be in computer science (CS), electrical/computer engineering (ECE), civil engineering and industrial and systems engineering.

Examples of courses that are or will include introductory CIE modules include:

- Computer Science/Electrical and Computer Engineering: CS 460/ECE 419: Security Lab
- Computer Science/Electrical and Computer Engineering: CS 461/ECE 422: Computer Security 1
- Electrical and Computer Engineering: ECE 391: Computer Systems Engineering
- Electrical and Computer Engineering: ECE 498DN: Trustworthy Critical Infrastructures
- General Engineering: ENG 198: Introduction to Cybersecurity (Undergraduate Seminar course)
- General Engineering: ENG 298: Foundational Technical and Organizational Concepts in Cybersecurity
- Civil Engineering: CEE 598: Integrated Urban Water Infrastructure (IUW)
- Civil Engineering: CEE 453: Urban Hydrology and Hydraulics (Senior Design Course)
- Systems Engineering: SE290: Undergraduate Seminar

## RESEARCH AND COLLABORATION

### Research Projects

The University is also renowned for its leading-edge research at the intersection of IT and cyber-physical systems. ITI has been infusing CIE concepts into existing and proposed research projects to cement this concept into the mindset of those exploring designs for future solutions.

Collaboration extends to working with students and organizations at UIUC's Research Park and engaging in the National Science Foundation (NSF)-funded Scholarship for Service (SFS) program, which offers scholarships for cybersecurity education in return for government service after graduation.

## STUDENT ENGAGEMENT

UIUC supports student-driven initiatives like the SIGPwny competition club and conducts various industry-focused exercises, such as tabletop and purple-teaming drills.

A recognized leader in cybersecurity education, UIUC was designated by the National Security Agency (NSA) and Department of Homeland Security (DHS) as a National Center of Academic Excellence in Cyber Defense (CAE-CD) and Research (CAE-R) since 2000 and 2008, respectively. Through these efforts, UIUC's educators, researchers, and students are at the forefront of developing secure and reliable critical infrastructure systems.

## Idaho State University

Since 2016, Idaho State University's (ISU) Industrial Cybersecurity Engineering Technology (ICET) program has prepared technical professionals to safeguard critical systems from accidental and intentional cybersecurity related events. ISU is mapping its ICET program to CIE principles and found that 42 separate hands-on learning activities over the final year of the ICET program directly addressed CIE principles within the context of critical functions and industrial control systems.

## CURRICULUM

### Classes and Lectures

A recent mapping exercise found that 42 separate hands-on learning activities over the final year of the ICET program directly addressed Cyber-Informed Engineering (CIE) principles within the context of critical functions and industrial control systems. Eleven of these activities deal with the first two CIE principles: Consequence-Focused Design and Engineered Controls. These represent the apex of CIE because 1) they require significant knowledge and skill scaffolding to reach adequate performance; and 2) they are more applicable to critical infrastructure industrial control systems environments than the other 10 principles.

### Courses

ISU has designed hands-on training stations core to the students' learning objectives in the ICET program. For instance, in the following courses demonstrate the adoption of CIE principles:

- CYBR 4481 – Critical Infrastructure Defense: students are given a flow control station and must identify possible high consequence events and then modify PLC logic to cause the event. Students are then expected to propose Engineered Controls and conduct a feasibility analysis of those engineered controls.
- CYBR 3383 – Security Design for Cyber-Physical Systems: students are given a heat exchange station and must describe the security uses of model. Students are then expected to populate a model of the station and recursively improve and populate the model.
- CYBR 3384 – Risk Management in Cyber-Physical Systems: students tour industrial control systems (ICS) and review ICS designs. Students are then expected to identify Planned Resilience characteristics and opportunities for Design Simplification of the ICS system designs.

Upcoming courses planned at Idaho State University that cover the application of CIE principles include a new PLC security course which focuses on PLC code quality, writing secure PLC code, hardening of a PLC, and implementing secure protocols.

Students from the ICET program have found employment at some of the country's leading organizations, including Idaho National Laboratory, National Renewable Energy Laboratory, Idaho Environmental Coalition, Naval Nuclear Laboratory, West Yost Associates, Accenture, Savannah River Nuclear Site, 1898 & Co., and HDR Engineering.

The University of Texas at San Antonio™

## University of Texas at San Antonio

The University of Texas at San Antonio (UTSA) has been at the forefront of Cyber-Informed Engineering (CIE) education and research since the inception of the national strategy in 2022. UTSA's approach to CIE integration is multifaceted, encompassing curriculum enhancement, certificate development, laboratory and use case designs.

### CURRICULUM

#### Classes and Lectures

UTSA has been conducting extensive research to develop case studies to demonstrate the practical application of CIE principles, along with lab design considerations. All case studies include laboratory equipment overview as well as a lab activity that strengthens the applicable CIE principles. Three case studies have been developed, each focusing on different aspects of CIE implementation in critical infrastructure and manufacturing settings:

1. Smart Manufacturing Facility (CNC Machine) Case Study: This study examines the application of CIE principles to a Tormach 1100MX CNC machine in a smart manufacturing facility. The case study demonstrates how CIE can enhance the security and efficiency of precision engineering processes, in this case subtractive manufacturing. The study highlights the importance of considering cyber-informed engineering tools in every aspect of the automated process, from machine operation to data protection and supply chain security.
2. Semiconductors Case Study: Focusing on the photolithography process in semiconductor manufacturing, this case study illustrates the critical need for CIE in critical processes for the nation. It addresses the unique cybersecurity challenges faced in semiconductor fabrication and demonstrates how CIE principles can be applied to protect intellectual property, ensure product quality, and maintain operational continuity after a cyber attack.
3. Attack Graph-Based Defense in Wafer Fabrication Case Study: This case study explores the use of attack graph-based stochastic modeling approaches to enhance cybersecurity in fabrication processes. It demonstrates how CIE principles can be applied to identify vulnerabilities, prioritize defense measures, and optimize resource allocation for cybersecurity. This use case is extensible to other domains as it presents a generic methodology to achieve cyber-informed engineering systems. The case study underscores the importance of a systematic, risk-based approach to cybersecurity in complex manufacturing environments.

These case studies serve multiple purposes in CIE education efforts:

a) They provide concrete examples of how CIE principles can be applied in real-world scenarios, helping students bridge the gap between theory and practice in a safe laboratory/test bed environment.
b) They serve as valuable teaching tools, allowing instructors to illustrate complex CIE concepts through relatable, industry-relevant examples.
c) They demonstrate urgency to address cybersecurity challenges in critical infrastructure and advanced manufacturing sectors.
d) They contribute to the broader body of knowledge in CIE, potentially influencing industry practices and future research directions.

### Certificate Programs

UTSA is actively developing a Cyber-Informed Engineering Certificate program for undergraduates, with plans to launch as early as spring/summer 2025. This program aims to equip students with the skills and knowledge necessary to meet national infrastructure needs in the context of cybersecurity. The curriculum design process has involved drafting core courses and electives, identifying experienced cyber-physical professionals to serve as instructors, and engaging with students to gauge interest and expectations. The certificate program will offer a comprehensive understanding of CIE principles and their practical applications in various engineering disciplines.

## RESEARCH AND COLLABORATION

### Research Centers

UTSA's commitment to CIE extends beyond the classroom. Through the Cybersecurity Manufacturing Innovation Institute (CyManII), funded by Department of Energy, UTSA leads the way on cybersecurity to protect critical manufacturing processes and the energy transition with two university-industry hubs: Cybersecurity for Manufacturing (C4M) and Cybersecurity for Energy Transition (C4ET).

Housed at C4M, a prototype CIE design laboratory has been deployed, providing students with hands-on experience and exposure to industry-standard equipment and processes. The C4M facility serves as a bridge between academic research and practical implementation, allowing UTSA to refine its CIE curriculum based on current industry needs and technological advancements.

To ensure alignment with industry standards, UTSA has conducted a literature review on standards (specifically ISA/IEC 62443) with CIE principles and developed a matrix that maps out the CIE principles against key concepts in IEC 62443.

Looking to the future, UTSA plans to continue expanding its CIE initiatives. This includes further development of the CIE design laboratory, ongoing refinement of the certificate program curriculum, and exploration of additional case studies and research projects. The university is also considering strategies for integrating CIE principles across a broader range of engineering courses, potentially leading to fully integrated curricula that incorporate CIE concepts throughout the engineering education experience.

# Lamar University

Lamar University is located in Southeast Texas, a region rich in energy infrastructure, including major refineries, petrochemical facilities, ports, and oil and gas transportation and storage facilities. The university offers cybersecurity education across multiple disciplines.

## CURRICULUM

### Classes and Lectures

Industrial cybersecurity (ICS) is critical for ensuring the security of the U.S. energy infrastructure. To support the workforce needs of critical energy and chemical infrastructure, Chemical Engineering, Computer Science, and Criminal Justice faculty at Lamar University (LU) are integrating the contents of industrial cybersecurity into the chemical engineering curriculum and examining their efficacy. This approach has been well received by students.

### Courses

Within the College of Engineering, the Electrical and Computer Engineering Department delivers a series of courses focused on computer network cybersecurity. The College of Business, through its Department of Management Information Systems, provides coursework addressing cybersecurity-related issues.

Finally, the Department of Sociology, Social Work, Criminal Justice, and Anthropology offers courses in cybersecurity and digital forensics.

### Degree Programs

The Department of Computer Science in the College of Arts and Sciences provides a Bachelor of Science degree in cybersecurity.

## RESEARCH AND COLLABORATION

### Research Centers

Lamar University is establishing a Center for Data Analytics and Cybersecurity to advance digital capacity and enhance cybersecurity and resiliency for industrial operations. This center will foster multidisciplinary collaboration in research and education to support the workforce needs of critical energy and chemical infrastructure. We are planning to integrate CIE principles into the curriculum in the future.

## Colorado School of Mines

Colorado School of Mines Computer Science Department hosts the Center for Cyber Security and Privacy (CCSP), whose mission is to support and promote cybersecurity and privacy education and research at Colorado School of Mines (Mines) and the region. Mines has coordinated with the National Renewable Energy Laboratory and Idaho National Laboratory to develop a seminar introducing Cyber Informed Engineering (CIE) to its students.

CCSP fulfills its mission by

1. Leveraging the unique strengths of Mines in engineering and applied science education and research
2. Promoting high-quality and high-impact cybersecurity and privacy research
3. Bolstering cybersecurity and privacy education and training
4. Fostering cross-discipline and cross-institution collaboration, knowledge sharing, and resource sharing engaging the local communities and the region.

The education and research activities at CCSP are closely aligned with the Federal Cybersecurity R&D Strategic Plan, and with the National Centers of Academic Excellence in Cyber Defense (CD) Education (CAE-CDE) program requirements. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated Colorado School of Mines as a National Center of Academic Excellence in Cyber Defense Education since 2016. Mines students who complete the corresponding Cyber Defense Education requirements receive an official Cyber Defense Education Certificate authorized by NSA and DHS.

## CURRICULUM

### Classes and Lectures

In alignment with the CCSP mission, Colorado School of Mines is the first university in the region to offer Cyber Physical Systems Security courses at both the undergraduate and graduate levels. Through these cross-discipline engineering courses, Mines has coordinated with the National Renewable Energy Laboratory and Idaho National Laboratory to develop a seminar introducing Cyber Informed Engineering (CIE) to its students. The seminar includes an hour-long lecture which walks the students through some of the principles of CIE through the use case of a cyber physical medical system. The seminar also includes a week-long online discussion forum encouraging students to apply the CIE approach to design decisions which could be made during the development of such a device. This seminar was introduced in the summer of 2024 and was very well received by the class. It will continue to be presented during upcoming semesters while broader CIE adoption is discussed.

Cyber-Informed Engineering

INL/RPT-24-82020-Rev000