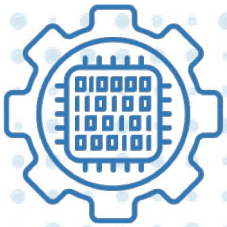
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.



Cyber-Informed Engineering

CIE Curriculum Guide

Version 2.0

May 2025

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 Laboratory of the Rockies.

INL/RPT-25-88269

Contents

List of Figures

Acknowledgments

CIE Curriculum Guide Version 2.0 development was led by Idaho National Laboratory (INL) with significant support from members of the CIE Community of Practice (COP) Education Working Group. Inputs to this guide were reviewed and informed by stakeholders from a diverse set of academic institutions. In particular, faculty members from universities listed below shared their direct experiences integrating CIE into engineering programs.

Curriculum Guide Development Team:

Benjamin Lampe Idaho National Laboratory	**William Lyons** Norwich University	**Saman Zonouz** Georgia Tech
Wm. Arthur Conklin University of Houston Missouri S&T	**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 Laboratory of the Rockies & Colorado School of Mines	**Sin Ming Loo** Boise State University	**Gonzalo Martinez Medina** University of Texas at San Antonio
Edward Huang Auburn University	**Dominic Forte** University of Florida	**Mirza Ahmed** Norwich University

1. Introduction

The Cyber-Informed Engineering (CIE) Curriculum Guide provides a framework, guidance, and resources for incorporating CIE into university-level engineering programs and related educational activities. CIE keeps the consequences of digital risk from impacting the safety, reliability, and performance of our critical infrastructure.

A key goal of this guide is to help educators adopt cyber-informed engineering into their delivery of engineering education and provide examples of CIE-focused education. CIE-focused education is necessary to produce future engineers and technicians who understand digital risk in modern engineered systems to meet the nation's infrastructure resilience needs. To accommodate a broad range of educational goals and approaches across any number of institutions, this guide outlines several practical integration examples, links to resources that can accelerate this CIE adoption, and offers perspectives from partner academic institutions on the various implementation strategies.

CIE is a framework for engineers and technicians to integrate engineered controls that reduce or mitigate the impact of cyber-attacks into any cyber-physical system used in critical energy infrastructure or in other sectors. The U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) developed a Congressionally directed National Cyber-Informed Engineering Strategy (July 2022) to build CIE into U.S. energy infrastructure.[1]

Learn More about CIE
Visit DOE CESER's CIE Program page and find more resources throughout this guide.

Embedding CIE into formal education, training, and credentialing is one of the five key pillars of the National CIE Strategy. This Curriculum Guide continues to support this strategic objective by helping institutions integrate CIE into educational programs. It offers a variety of examples of integration, including class activities, implementing new courses, or offering CIE instruction as a certificate. Integrating CIE concepts into engineering programs ensures our engineers-in-training will be better able to consider and mitigate the potential for cyber impact throughout the engineering design life cycle, leveraging engineering solutions to limit the pathways for or impact of cyber sabotage, exploitation, theft, or misuse within the system.

THE IMPORTANCE OF EDUCATING CYBER-INFORMED ENGINEERS

The U.S. faces ever-evolving cybersecurity threats in our engineered systems. Our adversaries maintain capabilities to launch cyber-attacks that could disrupt critical infrastructure, endangering the health and safety of the public. Historically, cybersecurity has been the purview of information technology (IT)[2] professionals, while industrial control system (ICS) technologies

[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.

[2] Information technology (IT) is any system that is used for the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information.

have been the purview of engineering professionals. Now, as use of digital technology increases in industrial contexts, an increasingly complex world of ICS has emerged that blends both IT and operational technology (OT).[3]

As the OT environment increasingly incorporates cyber-physical[4] solutions, the design, configuration, and management of devices and machines necessarily become a shared responsibility between cyber professionals and engineers. Thus, we must build in security through both traditional cybersecurity practices (i.e. information security controls) and engineering practices (i.e., engineered controls). This shift necessitates a new approach: Cyber-Informed Engineering. CIE is crucial because it addresses critical gaps in how physical systems with digital components are designed and protected against impacts from evolving cyber risks. Engineers do not need to become cybersecurity professionals to achieve this. Rather, they must be "cyber-informed" in their engineering approaches. This means being aware of cyber impacts, understanding the implications of incorporating digital assets, and being prepared to offer engineering standards of care throughout the lifecycle of cyber-physical assets.

At present, engineering that is cyber-informed is not the expected norm in engineering education. To prove this point, consider ABET's criteria for accrediting Engineering Programs[5] and their required student outcomes. The application of engineering design only maintains consideration of public health, safety, and welfare, and global, cultural, social, environmental, and economic factors and contexts. The expectation of digital risk is absent, representing a key gap in risks of modern engineered system solutions.

To address this gap, engineering schools must update their curricula to include digital modernization in the curriculum. As engineering disciplines increasingly rely on digital technologies, creating new opportunities for cyber manipulation, engineers must recognize and address this emerging "failure mode" throughout the entire system lifecycle. CIE calls on engineers to include digital risk consequence considerations as a foundational element of engineering risk management for any function aided by digital technology.

Engineering modern systems is a complex process involving balancing multiple objectives including safety, risk, resilience, performance, and cost. The key to managing any of these is to involve each from the outset, not bolt them on at the end. CIE empowers engineers with the knowledge to include engineering our cyber risk elements across the entire system lifecycle, beginning from the earliest phases of conceptual design and requirements development. CIE provides a framework for engineers and technicians to integrate engineering controls that reduce or mitigate the impact of digital risks into any physical system. CIE uses design decisions and engineering controls to mitigate the consequences when a cyber-enabled risk is manifested

[3] Operational technology (OT) is any system that interacts with the physical environment, detecting or causing a direct change through the monitoring and control of devices, processes, and events.
[4] Cyber-physical systems (CPS) are "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components." (Definition derived from the U.S. National Science Foundation.)
[5] "Criteria for Accrediting Engineering Programs, 2025 - 2026," ABET, February 28, 2025, https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2025-2026/.

or even eliminate avenues for these risks. CIE further allows engineers to advise the approaches used by specialized IT and OT cybersecurity experts, aligning cybersecurity mitigations with the most critical consequences identified by engineers.

ABET accreditation requires engineering programs to demonstrate that graduates can apply knowledge of safety principles in their engineering work. This has resulted in safety being infused throughout the curriculum. Including cyber/digital risk in the list of essential safety elements of student outcomes will enable them to produce professional outcomes that include considerations of digital risk and digital risk reduction as part of the engineering design process.

This guide helps engineering faculty take the journey into addressing the strategic intersection between digital risk and engineering through the adoption of CIE into engineering education. This approach addresses gaps in how we train engineers and technicians and provides them with the means to build in resilience from the ground up. The resulting cyber-informed workforce will be instrumental in designing, managing, and safeguarding the cyber-physical systems that are vital to our national security and public welfare. By embedding CIE into formal education, training, and credentialing, institutions can help produce future engineers and technicians who are better able to consider and mitigate the potential for cyber impact throughout the engineering design lifecycle, resulting in more secure critical infrastructures.

2. Goals and Outcomes

The long-term objective of incorporating CIE into education is to create a working awareness of its principles and practices, engraining them into the engineer's toolbox so they become a natural part of the design and analysis process used in normal practice. Ultimately, this will be the result of the native infusion of CIE principles and practices into the entirety of the education curriculum, much like safety principles.

This guide details the many mechanisms that can be employed by educational institutions as they transit the journey to complete incorporation of CIE principles and practices into their programs. All accredited engineering programs have a continuous improvement process associated with the drive to increase student success. This guide provides the details needed to make CIE inclusion part of that process over time. CIE is not unique or specific to any engineering domain. The concepts are domain agnostic and can be incorporated in all the domains' contexts and exercises.

Conversations with stakeholders have emphasized inclusion of CIE into the Professional Engineering (PE) certificate as an essential long-term goal. Although this guide does not address the complete path to that goal, it does define the critical first step. The only way to include CIE in engineering exams, at any level, is to integrate it in university curricula.

Full adoption of 'digital risk' as a necessary addition into ABET's student outcomes 2[6] and 4[7] as new factors and contexts, starts with the educators adopting the mindset in their delivery of materials. As such, the goal of this Curriculum Guide is to provide guidance, a framework, and resources for incorporating CIE into engineering programs and related educational activities as recognition of digital risk continues to formalize in academic institutions and professional engineering societies.

Using this guide, educators should be able to do the following:

1. **Develop curricula:** Develop CIE curricula that support an institution's specific goals, approaches, and needs. This guide offers practical examples for integrating CIE at several different levels and includes insights from university partners.
2. **Plan courses, lectures, and learning outcomes:** Plan courses, lectures, and learning outcomes that focus on or include CIE concepts. This guide outlines several learning objectives for CIE that can be used to construct a syllabus, plan lessons, and ensure all levels of Bloom's Taxonomy[8] are being addressed.
3. **Design educational activities:** Design educational activities such as assignments, projects, or labs that reinforce CIE concepts. This guide outlines CIE laboratory activities to bring analysis and application of CIE principles into a few classes across a course.

Achieving complete integration of CIE principles into any education program will be the product of a continuous journey in curriculum development. As faculty improve classes over time, they will determine appropriate injection points to include CIE. This guide includes examples of how several institutions have explored introductory applications of CIE. This stepped inclusion of CIE's principles and practices into existing educational approaches will take time, trial, and error, but—in alignment with ABET's requirement for meaningful, data-driven program improvement—allows the addition of CIE information over time and with appropriate review and revision to establish meaningful context and details for proper inclusion.

This guide seeks to provide the necessary information to facilitate this inclusion, whether it be in a certificate, a class, or as parts of projects. Each program and discipline can adopt these elements in a sequenced basis that maps to their own timeline of curriculum improvement, with differing levels of initial and continuous improvement. The pathway to success is simple; start small, and continually make small adjustments until CIE is infused throughout a program as part of context-based learning objectives.

---

[6] "an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors" in "Criteria for Accrediting Engineering Programs, 2025 - 2026," ABET, February 28, 2025, https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2025-2026/#GC2.

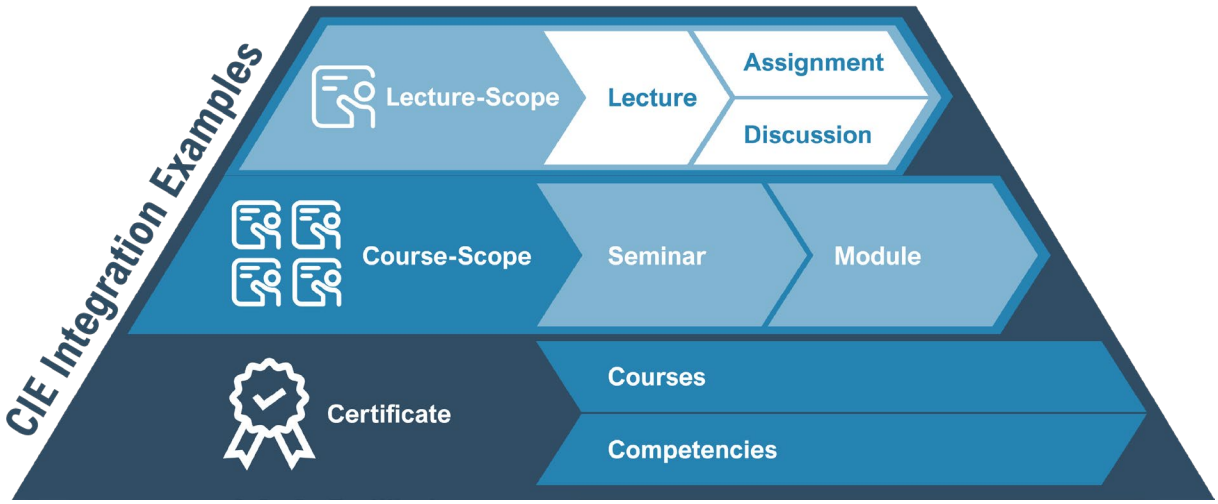
[7] "an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts" in "Criteria for Accrediting Engineering Programs, 2025 - 2026," ABET, February 28, 2025, https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2025-2026/#GC2.

[8] Armstrong, Patricia. "Bloom's Taxonomy." Vanderbilt University Center for Teaching, 2010. https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/.

3. CIE Integration Examples

This guide outlines a set of integration examples built on the Lecture, Course, and Certificate (LCC) pathways (see Figure 1). This approach allows flexibility for each academic institution to determine which strategies to implement within their current environment. Each strategy is accompanied by CIE integration examples to help illustrate how these strategies have already been successfully adopted by CIE academic partners.

Figure 1. CIE Integration Strategies



These examples allow for a targeted approach within each discipline of practice:

- **Lecture-Scope Examples:** These use cases integrate CIE concepts within the context of a class lecture, assignment, or class discussion in an existing course model, and are meant for about a one- to four-hour interaction with CIE.
- **Course-Scope Examples:** These use cases operate within the context of a single, dedicated course and are meant for about a 4- to 20-hour interaction with CIE.
- **Certificate Example:** These uses cases operate within the context of a series of classes or courses and are meant for a recurring and comprehensive (20+-hour) interaction with CIE. A certificate is a combination of courses, usually 9 to 20 credit hours.

To support these integration examples, a set of learning objective examples are provided in Appendix A. These learning objectives cover the 12 CIE principles (see Figure 2) and follow Bloom's Taxonomy for levels of learning. Consider using the learning objective examples in combination with the three integration strategies to incorporate CIE into the curriculum.

Figure 2. CIE Principles and Key Questions.

	PRINCIPLE	KEY QUESTION
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5	**Layered Defenses**	How do I create the best compilation of system defenses?
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12	**Organizational Culture**	How do I ensure that everyone’s behavior and decisions align with our security goals?

3.1. Lecture-Scope

Lecture-scope activities can include, but are not limited to, the **class lecture**, **assignments** or project assignments, and **class discussions**. The course delivery methods may vary, spanning traditional in-person formats, synchronous or asynchronous online models, flipped classrooms, or hybrid approaches. Instructors are strongly encouraged to integrate these activities in alignment with their specific course modality.

TOTAL INTEGRATION STRATEGY

CIE can be included in lectures in many ways as stand-alone lectures, assignments, or discussions. Separating out the addition of CIE principles allows a clear discussion of the elements and can be bolted into virtually any level of curriculum. As a first step, this is an easy way to get started, but over time, the CIE elements are best learned within the context of the engineering process—fully integrated into the entire curriculum.

The key is to include CIE principles as part of the existing materials, making the materials presented more comprehensive and complete. The context of the existing lecture should be leveraged as an environment where the addition of the CIE principles can bring enhanced clarity to specific educational elements. Just as safety would not be ignored at an obvious juncture in a lecture, the issues associated with digital risk can be handled via CIE principles.

Total integration is the long-term goal of including CIE into an engineering curriculum. The strategies that follow are methods of moving towards this goal in an organized manner.

EXAMPLE 1A: CLASS LECTURE

Depending on the course topics, some courses may focus more on the general engineering design process, while others may delve into specific systems engineering designs. Regardless, all courses can integrate a dedicated lecture on the concepts and principles of CIE. This lecture serves to establish a foundational understanding of CIE within the engineering design process and lifecycle.

In design-focused lectures, employing CIE case studies enhances the learning experience by actively engaging learners and encouraging immediate application of newly acquired CIE skills.

CIE Implementation Guide
The 12 principles of CIE, outlined on page 9 of the CIE Implementation Guide, can be incorporated into specific courses through examples or case studies. For instance, the CIE principle of design simplification can be introduced in a hardware design course, prompting students to consider CIE from the outset of their design process.

The following are examples that can be used to support a lecture presentation on the CIE principles when given the opportunity to talk about the topics of introduction to engineering, engineering in the modern age, or secure engineering practices.

General Presentation of the Principles:

When minimal time is available to introduce CIE as a worldview for engineers, it may be appropriate to survey and describe the twelve principles.

CIE Lecture Slides

The example CIE lecture slides provide a presentation that surveys the twelve CIE principles.

Presenters may consider providing situational examples encountered in their careers to further emphasize the point of the principle for the students.

Recorded CIE Webinar Presentation

If subject matter expertise is minimal, consider the use of a guest lecture or watching this recorded webinar presentation of the CIE lecture slides to increase your familiarity with the basics of CIE in preparation for facilitating this lecture-scope.

Reach out to CIE@inl.gov for additional support in identifying a guest lecturer if needed.

Focused Case Study of the Principles:

If slightly more time or expertise is available in the context of a course, or for students focused on a specific sector, a focused case study may be a powerful way to introduce the twelve CIE principles.

Water Booster Pump Station Case Study Lecture Slides

This focused case study presentation introduces the 12 CIE principles and applies them to a specific engineered system: a water booster pump station.

While this resource focuses on a water sector example, faculty are encouraged to use this model or replace it with another sector example. Please consider sharing new examples with CIE@inl.gov to be made available as a curriculum resource to other institutions. For this focused case study, spending five minutes on each principle will fill the hour. For a longer class (up to 2-4 hours), participants can spend more time discussing each of the twelve principles. See Class Discussion below for a resource. Longer exploration of this case study represents an opportunity for a seminar (or module), as described in the respective section below.

Principle Tagging in Existing Lectures:

CIE provides a worldview lens by which to interpret the implementation of engineering practices. As faculty consider the breadth of engineering considerations in their course, they may recognize a topic in their lectures that could involve the use of digital technologies in calculating engineered outcomes. Here, related CIE principles may be flagged and discussed in that lecture. Consider using the questions from Figure 2 or the list of potential Learning Objectives in Appendix A.

If the connection to the principle needs exploration and discussion to confirm its relationship, consider connecting with CIE@inl.gov to provide more specific CIE background and content to support the framing intended for that lecture topic.

CIE Wordmark
Consider integrating the CIE wordmark in lecture slides to call out connections to CIE concepts.

Cyber-Informed Engineering

Example Perspectives:

Auburn University - The concepts and principles of CIE are first introduced in general systems engineering design courses, laying a foundation before students advance to more specialized engineering design courses. In these foundational courses, students learn each phase of the systems engineering lifecycle—from concept definition, system definition, and realization, to production, support, utilization, and retirement—integrating CIE principles at every stage. These courses, including *Systems Engineering 1*, *System Lifecycle Requirements*, *Digital Systems Engineering Design*, and *Model-Based Systems Engineering*, are integral to Auburn's digital engineering curriculum. Here, students not only master the engineering design process through the lens of CIE but also create corresponding digital design artifacts. Additionally, class lectures provide examples of digital design artifacts across various engineering domains, including applications like a water booster pump station, showcasing the application of CIE principles.

Boise State University - The concept of CIE is introduced in various courses (e.g., *Engineering Junior Communication*, *Introduction to Engineering*) through a one-hour lecture. The lecture starts by highlighting the implications of interconnected systems and major hacking events. It also engages students to think through exercises as future engineers, including what they can do to make systems more secure and less hackable and what they can do for systems to maintain basic functionality.

University of Illinois Urbana-Champaign (UIUC) - A guest lecture provides an opportunity to showcase the synergy between CIE and the course content without requiring professors to develop new material independently. After the guest lecture, UIUC's Information Trust Institute researchers share the presented material, INL's CIE site, and additional background materials for faculty to review at their convenience. Following the lecture, students are assigned to rethink design approaches, incorporating security elements early in the engineering process.

Georgia Tech: CIE concepts are introduced through a dedicated lecture within the engineering curriculum. This lecture features a guest presentation by Sam Chanoski (Idaho National Laboratory), who provides students with an overview of foundational CIE principles, their national relevance, and their application to cyber-physical systems (CPS). By engaging directly with a practitioner at the forefront of CIE, students gain exposure to both theoretical concepts and real-world applications. The lecture emphasizes how CIE

informs system design and risk management for CPS, equipping students with a broader understanding of how engineering decisions intersect with cybersecurity concerns.

University of Florida: CIE principles are introduced in the graduate course, *Advanced Hardware Security and Trust,* and reinforced across six modules covering state-of-the-art hardware security challenges. Lectures incorporate case studies on side-channel and fault injection attacks, counterfeit electronics, hardware Trojans, supply chain threats, and intellectual property protection, helping students connect theory to practical system design. Planned expansions for the next academic year will integrate CIE lectures into *Intro to ECE*[9] and both *ECE Design I & II* courses, ensuring undergraduate exposure.

University of Texas at San Antonio: CIE is taught primarily through laboratory-based lectures and demonstrations using the Amatrol Mechatronics Learning System. Instructors present CIE principles such as consequence-focused design, engineered controls, and layered defenses in the context of smart manufacturing. Lectures highlight vulnerabilities like Programmable Logic Controller (PLC) manipulation, sensor spoofing, and synchronization faults, linking them directly to cyber-physical consequences.

Norwich University: CIE lectures have been developed for introduction into classes during the 2025-2026 academic year, including *Introduction and CIE Background* and *Consequence-Focused Design*, which provides an in-depth look at CIE Principle 1, Consequence-Focused Design. CIE lectures are expected to be taught in *Introduction to Electrical and Computer Engineering/Mechanical Engineering/Civil Engineering Lab* (EE121/ME121/CE121), *Introduction to Transportation Engineering* (CE336), *Fluid Mechanics* (EG303), and *Heating, Ventilation and A/C* (ME 492).

EXAMPLE 1B: ASSIGNMENT

Assignments can play a crucial role in building on lectures to integrate CIE into engineering design classes. CIE principles can be incorporated into planned assignments (e.g., an assignment that challenges students to consider “as-is” design and “to-be” design). This approach assesses students' comprehension of CIE principles and evaluates their ability to implement them and identify associated benefits. More advanced activities can assess higher levels of learning such as analysis or evaluation. The following examples can be paired with lectures, seminars, or modules that focus on surveying the CIE principles, to assess the level of learning.

CIE Workbooks:

The following set of workbooks challenge participants to systematically think through an engineering project considering the CIE principles. These can be used in custom applications, as needed. When used in a lecture, specific items can be removed from the answer guide to see if students can fill in the blank given the limited exposure to the CIE principles discussed in the lecture. Or, when used in a seminar, the activity may be accomplished through class discussion and participation. Finally, when used as part of a module in a course, the workbook can be

[9] ECE stands for Electrical and Computer Engineering.

broken up by principle so that as each principle is covered, the student is able to accomplish the activity for each principle each time.

Workbook for a Water Sector Upgrade: https://www.osti.gov/biblio/2371031

Workbook for an Advanced Distribution Management System Update: https://www.osti.gov/biblio/1986517

Workbook for a Microgrid Deployment: https://www.osti.gov/biblio/2315001

The workbooks follow a recommended sequential approach to walk through CIE principles for each use case. Please consider sharing with CIE@inl.gov to be made available as a curriculum resource to other institutions.

Specific Principle(s) Activity:

Each principle, or combination of principles, can be leveraged into an assignment for students to evaluate and incorporate into system design. A reflection activity could also focus on a specific principle, encouraging students to self-assess their work in an engineering design process. These activities may be especially valuable in a capstone design course, or similar culminating activity involving an industry-sponsored project or other comprehensive design that could use engineering solutions to reduce cyber impacts. This is an ideal opportunity to assess students' comprehension of CIE principles and evaluate their ability to implement them and identify associated benefits as part of a comprehensive design process. For principle-specific activity examples, please see Appendix D.

Example Perspectives:

Auburn University – In Auburn University's *Digital Systems Engineering Design* course, students apply CIE principles through weekly assignments and a semester-long project in a flipped classroom setting. Each week, students develop components of a proposed "to-be" system, analyze cybersecurity vulnerabilities in the current system, and collaborate to incorporate CIE concepts into their designs. They create logical and physical architectures and conduct validation and verification activities. Both the weekly assignments and final project assess students' ability to integrate CIE principles throughout the system's engineering lifecycle.

Boise State University: Assignments in Boise State's CIE-related courses include problem sets and projects that require students to evaluate vulnerabilities in hardware, firmware, and industrial control systems. Students use CIE principles to propose secure design strategies and analyze trade-offs in resilience and performance. Graduate-level assignments in *CORe 514* emphasize applying the CIE framework to design or evaluate complex systems, with students producing structured analyses or system redesigns.

Georgia Tech - In Georgia Tech's drone systems courses, students apply CIE principles through four mini-projects and a culminating final project. In the mini-projects, teams of undergraduate and graduate students address CIE-based missions that require applying engineered controls, consequence-focused design, and fallback planning to simulate drone scenarios, including sensor spoofing, command injection, and swarm instability. These assignments expose students to a variety of attacks, defenses, and safety measures in a controlled environment. The final project builds on these experiences, requiring students to secure a physical drone against a selected class of cyber-physical attacks and to demonstrate CIE-informed defensive mechanisms during live flight missions. Both the mini-projects and the final project assess students' ability to integrate CIE concepts into the design, defense, and operation of cyber-physical systems.

University of Florida: Assignments emphasize real-world application, with exam problems and project tasks requiring students to apply CIE principles to analyze vulnerabilities in systems such as traffic lights, sprinkler systems, and embedded controllers. In design courses, students will be required to incorporate at least one CIE principle into their project specifications, demonstrations, and final reports.

University of Texas at San Antonio: Assignments are embedded into lab exercises, requiring students to simulate disruptions (e.g., misaligned assembly, corrupted logic, altered thresholds), record observed system consequences, and propose mitigation strategies. Reports must include fault trees, failure chain diagrams, or attacks graphs, with each solution explicitly mapped to CIE principles. Students also produce redesign proposals that incorporate resilience practices and engineered safeguards.

EXAMPLE 1C: CLASS DISCUSSION

In both traditional and flipped classrooms, class discussions serve as valuable activities to integrate CIE principles into engineering design learning. These discussions can take the form of team or class dialogues, exploring various methods to integrate CIE into existing designs. This approach may improve student ability to comprehend, implement, and identify the benefits of CIE principles. Further, students or instructors can act as third-party evaluators, ensuring that CIE principles are incorporated appropriately into design artifacts.

Principle-Specific Discussions

CIE Implementation Guide:
https://www.osti.gov/biblio/1995796

The CIE Implementation Guide outlines questions an engineering professional could ask in order to consider CIE at any point in the system lifecycle of an engineering project. When an engineering project, failure mode analysis topic, or an engineering problem is discussed in class, questions from this guide can be used as the basis of a discussion. Such a discussion may include Consequence-Focused Design, Active Defense, and Engineering Controls. For example, a group of students is tasked to think through the intended and unintended features and uses of an engineering application. They may discuss the following:

- If the unintended use occurred, what is the unintended outcome, or consequence?
- What engineering controls or design features can be added to prevent unintended outcomes?
- What kind of real-time monitoring can be designed for early detection as an active defense feature?

Use-Case Discussions:

Water Booster Pump Station Case Study Lecture Slides
The case study lecture slides provides a presentation that introduces the twelve CIE principles and how they are addressed by a specific engineered system, a Water Booster Pump Station, and leaves how it is addressed open so as to promote student participation in a discussion format.

A use-case discussion allows students to assess comprehend, implement, and identify the benefits of CIE principles in a real-world, application-specific context. While the resource above focuses on a water sector example, it can be used as a model to develop a more relevant sector-specific example. Please consider sharing new examples with CIE@inl.gov to be made available as a curriculum resource to other institutions. For this focused case study, spending 5-10 minutes introducing the principle, and another 5-10 minutes promoting student discussion on each principle fills multiple hours (up to 2-4 hours).

Example Perspectives:

Auburn University - In the *Model-Based Systems Engineering* course at Auburn University, class discussions are conducted in an open forum where students can share their design concepts and ideas for incorporating CIE into their existing designs. The semester-long project benefits from input and evaluation by domain and cybersecurity experts throughout the semester. Students have access to course-level forums open to all classmates and domain experts, project-level forums that support video calls and project collaboration and help forums for technical and CIE idea support.

Colorado School of Mines – The graduate level *Cyber Physical System Security* course is online and fully asynchronous. As part of the course, weekly discussions center around current events and topics within the field. This course is an introduction to the domain for most of the graduate students enrolled, as their focus areas span the breadth of computer science and engineering. A week-long discussion board is introduced about CIE principles through the use case of a medical device. The students consider engineering design decisions related to the security posture of an artificial pancreas system for diabetics which consists of a continuous glucose monitor, control software, and an insulin pump which are connected wirelessly. The students are asked to discuss some of the CIE principles relevant to the design of this cyber-physical system.

University of Florida: Class discussions during lectures and project phases provide opportunities for students to compare attack surfaces and debate the effectiveness of CIE-aligned defenses. Faculty guide conversations around Engineered Controls, Active

Defenses, and supply chain safeguards. Within the University of Florida's Talent Pipeline program, student cohorts also hold structured discussions on national security challenges, including risks tied to AI integration into critical infrastructure, further embedding CIE into experiential learning.

University of Texas at San Antonio: Students participate in instructor-guided discussions before and after lab simulations to analyze how cyber faults propagate across interconnected stations. These discussions emphasize the importance of consequence modeling, interdependency analysis, and layered defense strategies. Students reflect on the effectiveness of proposed solutions and debate trade-offs between complexity, performance, and resilience.

3.2. Course-Scope

The second set of examples demonstrate courses created to integrate CIE principles into engineering curricula. These courses aim to provide students with foundational knowledge and practical skills to address cybersecurity challenges in modern cyber physical systems (CPS) through the practice of engineering. Additionally, the objectives of these courses should focus on educating students about the complexities of securing CPS and critical infrastructures, fostering interdisciplinary collaboration, and promoting proactive defensive strategies. A combination of course **seminars** and **modules** can be used to teach students how to design, analyze, and maintain resilient cyber-physical systems (CPS) and infrastructures. These educational components will equip students to deal with ongoing malicious or accidental disruptions and to automatically restore their core safe functionalities.

Appendix B includes an example of a Course Syllabus from Boise State Universities' CSE 331: Cyber-Informed Systems Engineering course.

EXAMPLE 2A: SEMINAR

Short one- to two-hour-long seminars on attacks on and defenses in cyber-physical systems can introduce practical application of CIE principles. Longer, multi-hour seminars can be used to introduce CIE principles in a holistic sense and elicit participation in a discussion. Consider using guidance from the Lecture-Scope above when integrating specific CIE lectures into this seminar option.

Example Perspectives:

Auburn University - The invited speaker presents the current system design for an anti-UAV defense system in a one-hour seminar. This presentation covers the hardware, software, and corresponding digital design artifacts. The seminar then discusses the application of CIE to their existing design and proposes possible improvements to the design artifacts.

Boise State University - In a one-hour seminar, a speaker presents hacks involving hardware, software, and industrial control systems—such as Stuxnet, Jeep Uconnect, and the Ukrainian power grid. This seminar discusses why engineering students should learn Cyber-Informed Engineering and how future engineers can apply it. Finally, speakers close by highlighting specific CIE principles.

EXAMPLE 2B: MODULE

Course modules offer another avenue to explain CIE principles in more detail, extending beyond what a seminar may offer. Case studies like the water booster pump station can be used as an introductory module to introduce all 12 CIE principles. Additionally, dedicated modules can be used to explain specific CIE principles in greater detail. For example, CIE principles such as Active Defense and Planned Resilience can be explained through discussion on defense and safety mechanisms for attacks or risks that were not accounted for in the original system design modeling.

CIE Module:

A module generally consists of multiple lectures, and can consist of one or several weeks' worth of content. The Implementation Guide can be used as a foundation for a CIE module. The format may begin with an overview of CIE, then progress to focus on some or all principles, depending on the length of the module. The principles can be combined into 3 sets of 4 principles, or 4 sets of 3 principles. Depending on the applied engineering disciplines, a lecture followed by in-class activities to further learning may be more productive. The example below demonstrates a mock 4-week CIE Module:

Cyber-Informed Engineering	Week 1	• Introduction to CIE and Digital Modernization in Engineering Practices (Modern day risk management for Engineers) • Principles 1 and 2
	Week 2	• Principles 3, 4, 5, and 6
	Week 3	• Principles 7, 8, 9, and 10
	Week 4	• Principles 11 and 12 • CIE Project Activity Presentations

Example Perspectives:

Auburn University – The principles of CIE are integrated into systems engineering design courses. These courses comprise twelve modules, each aligned with the phases of the systems engineering lifecycle. Consequently, CIE principles can be incorporated into each module according to its respective lifecycle phase. Each module includes a combination of theoretical instruction, practical exercises, hands-on weekly homework assignments, and participation in a design project within a flipped classroom setting.

Boise State University – This module takes the same approach as a seminar, but spanning one to several weeks, with the Implementation Guide providing increased structure. In a one-week module, educators primarily use the Implementation Guide, whereas a multi-week module requires students to work on a project following all design phases using the Implementation Guide.

University of Illinois Urbana-Champaign - At the University of Illinois Urbana-Champaign (UIUC), Information Trust Institute (ITI) researchers have successfully integrated CIE concepts into existing engineering and cybersecurity coursework by leveraging ITI's established relationships with faculty involved in previous security research programs. This approach begins with a discussion on how CIE aligns with the existing curriculum, followed by a brief overview of CIE. ITI researchers then offer to present a single module during a class session, ensuring new material seamlessly integrates with the course's focus.

Georgia Tech – Georgia Tech, offers three CIE-informed course modules: *Introduction to Cyber-Physical Systems Security, Critical Infrastructures Security and Resilience, and Cybersecurity of Drones*, which satisfy several CIE principles. These three courses use a combination of theoretical instruction, practical exercises, and hands-on projects to help students not only get comprehensive insights into the vulnerabilities and interdependencies inherent in CPS and critical infrastructures but also understand the importance of resilience and proactive defense measures. Additionally, students are encouraged to independently learn about the state-of-the-art research in making different cyber-physical systems resilient to failures and cyber attacks by including graded paper-presentations as part of the courses.

Specifically, the *Introduction to Cyber-Physical Systems Security* course, focuses on the fundamentals of CPS security, using Industrial Control Systems (ICS) as the target CPS. In this course, students learn the complex integration of sensors, actuators, control systems, engineering workstations, human machine interaction (HMI) devices, and data historians in an ICS, emphasizing the need to account for the interdependencies between these components of an ICS while designing defenses against adversarial attacks. This course module satisfies the Interdependency Evaluation principle as it emphasizes the need for security-specific design decisions to account for the interaction between components.

Further, the *Hacking ICS* module teaches the critical functions in an ICS and the consequences that can result from malfunction. This module satisfies the Consequence Focused Design principle as it answers the key question: “How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?” Students learn the Secure Information Architecture principle by teaching them the concept of “Security Zones” (defined using a group of assets at a particular site with similar security requirements) and how different access control policies, data monitoring solutions, and network security measures can be used to protect critical data in the individual security zones and data flows between zones.

In the “Attacks Against Drones” module of the more advanced *Cybersecurity of Drones* course*,* students learn about physics-aware malware and actuator control channel attacks to understand how the CIE principles Active Defenses and Planned Resilience can defend against complex and sophisticated adversarial techniques—specifically those that were not accounted for in the design’s threat modeling. While Active Defense allows a drone to potentially thwart new attacks, Planned Resilience allows for the drone to fail safely if and/or when the defenses are not able to prevent any attack.

University of Florida: The University of Florida (UF) is piloting CIE in the graduate course *EEE 6742: Advanced Hardware Security and Trust* in Fall 2025. Planned undergraduate integration includes *EEL 3000: Intro to ECE*, *EEL 3923C: Design I*, and *EEL 4924C: Design II* during the 2025–26 academic year. UF also intends to expand CIE integration to other ECE courses (Power Systems, Communications, Control Systems, Machine Learning, Robotics) and to cross-disciplinary programs like Integrated Product & Process Design (IPPD) and the Engineering Leadership Institute.

University of Texas at San Antonio: CIE content is integrated into undergraduate engineering courses through the Amatrol proof-of-concept testbed. Modular stations (MS1–MS9) simulate smart manufacturing processes including feeding, gauging, assembly, and testing. Planned expansions include incorporating CIE labs and exercises into broader engineering coursework within the Department of Mechanical Engineering and related disciplines, aligning with DOE CESER's national priorities in cybersecurity and smart manufacturing.

3.3. Certificate

The third example for integrating CIE into curricula is to offer it as a **certificate**. A certificate is a credential that designates requisite knowledge and skills of an occupation, profession, or academic program. In academia, certificates can be offered for-credit or not-for-credit. The latter is usually done through a Workforce Development or Continuing Education department or college within the higher education institution. They are designed to be completed in a short period of time (e.g., one year). In the case of for-credit certificates, learners can apply their course credits to an undergraduate degree later, should they choose that route. Certificates can also be stacked on top of each other, providing a pathway toward more advanced study and other certificates.

The CIE certificate can be made available to all STEM students—not just engineering—with included courses that are part of the core degree requirements. This ensures STEM graduates gain awareness of cyber issues that impact safety, reliability, and performance of cyber-physical systems and the associated relationship to the security of the programs, systems, codes, or algorithms they design.

Example Perspectives:

Boise State University – BSU's Security in Cyber Physical Systems Certificates are four different 12-credit-hour certificates for students in multiple engineering programs (and are especially popular for electrical engineering students):

- *Security in Cyber Physical Systems Software Focus*
- *Security in Cyber Physical Systems Hardware Firmware Focus*
- *Security in Cyber Physical Systems Power Systems Focus*[10]
- *Security in Cyber Physical Systems Industrial Processes Focus*

All certificates have a common course with introductory cybersecurity topics. The 3-credit-hour introductory course includes cybersecurity, security engineering and frameworks, cryptography, IT vs. OT, pen testing, risk assessment, open-source intelligence, CIE frameworks, and ethics. Students can choose the other nine credit hours from a list of courses for various certificates.

These certifications attempt to help engineering students become cyber literate in to 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.

Auburn University – To teach students CIE, Auburn offers a CIE-enabled Systems Engineering Program designed for students from all engineering disciplines. This program is open to students in Aerospace Engineering, Biosystems Engineering, Chemical Engineering, Civil Engineering, Computer Science, Electrical and Computer Engineering,

[10] This is the most popular certificate.

Industrial and Systems Engineering, and Mechanical Engineering. It equips students to apply CIE principles throughout the entire design lifecycle and management processes.

The program includes four key courses. The first two are academically equivalent to the International Council on Systems Engineering (INCOSE) Associate Systems Engineering Professional (ASEP) certificate, ensuring students gain both systems engineering knowledge and CIE competencies. The third and fourth focus on engineering modeling and design skills within the context of model-based systems engineering, emphasizing the integration of CIE principles into the systems engineering design process and framework.

STRATEGIC NOTE

Although a full CIE program could logically be designed, given enough courses, this concept does not align with the core CIE implementation guidance goals and outcomes. CIE represents a holistic framework intended to shape the interpretation and practice of engineering, rather than a standalone academic program. The focus should be on integrating CIE principles into existing engineering curricula, allowing these principles to enhance and inform traditional engineering education. Given that the current body of knowledge within CIE is still maturing, it is premature to consider developing a distinct degree program in any shape beyond the use of certificates. As the guidelines for CIE evolve, the CIE program anticipates further enriching the content of certificates and augmenting the scope of existing engineering degree programs.

Example Perspectives:

Auburn University – In collaboration with the Thomas Walter Center at Auburn University, Auburn integrates CIE principles into existing undergraduate programs, in-person master's and PhD programs, and the online Master of Engineering Management (MEM) program. CIE concepts 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 lifecycle. By infusing CIE principles into the core curriculum of the systems engineering program, students will establish a solid foundation in CIE before branching out into various engineering disciplines, including the 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.

Boise State University – Boise State's Computer Systems Engineering undergraduate degree program blends computer science and electrical engineering, with an emphasis on secure system design. Within the curriculum, students take two cyber-focused courses: an introductory cybersecurity course, which is also shared with certificate programs, and a Cyber-Informed Engineering course that emphasizes designing reliable and resilient systems for cyber-physical applications. The CIE course guides students through the system lifecycle—from design through development to production and management—embedding cybersecurity as a core design specification. In addition, Boise State's Cyber Operations and Resilience program extends access to CIE through a one-credit asynchronous online course, enabling students outside traditional engineering disciplines to engage with CIE principles.

4. Lessons Learned

Integrating CIE into curricula is not a one-sized-fits-all process. The CIE Program has partnered with several U.S. universities to embed CIE into coursework. Each institution has taken its own approach, but all have encountered challenges along the way. Lessons learned from their experiences are outlined below.

4.1. Auburn University

Auburn University's experience integrating CIE into systems engineering education has highlighted the value of embedding cybersecurity principles directly into the design process:

- **Integrated Approach over Standalone Course**: Auburn chose to incorporate CIE principles into existing systems engineering courses rather than creating a dedicated CIE course. Students internalize cybersecurity as an essential part of engineering design, fostering a mindset that naturally considers security from the outset.
- **Real-World Scenarios Enhance Learning**: Using challenges like the water treatment plant design gives students opportunities to apply CIE principles in practical, relatable contexts. These examples make abstract concepts more accessible, increase engagement and highlight the relevance of cybersecurity in engineering decisions.
- **Complementary Disciplines**: Systems engineering and CIE both adopt a life cycle approach—one focused on design rigor, the other on proactive cybersecurity. Their integration enhances both disciplines, equipping students to create systems that are both technically sound and cyber-resilient across their full life span.

4.2. Boise State University

Boise State's long-standing integration of CIE into its programs underscores several key insights:

- **Value for Graduates:** Alumni—particularly electrical and computer engineering graduates—report that CIE training has been instrumental in their careers. This is particularly important for those working in critical infrastructure industries sectors, such as power and energy.
- **Importance of Curriculum Flexibility:** Offering both in-person and asynchronous online CIE courses broadens access and allows students outside traditional engineering disciplines to develop cyber-aware design skills.
- **Applied Leaning Strengthens Outcomes:** Case studies and hands-on projects provide tangible opportunities for students to see how cyber risks influence engineering decisions, reinforcing the need for secure and resilient system design.

4.3. Georgia Tech

Georgia Tech's integration of CIE into engineering coursework highlights several strategies and lesson learned that can help institutions strengthen student understanding and application of CIE principles

- **CIE Principle Clustering Can Enable Targeted Learning:** Grouping the 12 CIE principles into clusters—active attack prevention, system understanding, attack-impact minimization, and limiting information leakage—can help students better grasp how to apply them in practice.
    - *CIE Principles for Active Attack Prevention*. These principles (Secure Information Architecture, Engineered Controls, Active Defense) focus on preventing cyber attacks before they can cause harm.
    - *CIE Principles for System Understanding*. These principles (Interdependency Evaluation, Consequence-Focused Design, Digital Asset Awareness, Design Simplification) help engineers deeply understand how cyber and physical components interact, so they can design more secure systems.
    - *CIE Principles for Attack-Impact Minimization*. These principles (Consequence-Focused Design, Engineered Controls, Planned Resilience, Layered Defense) help ensure the system continues to function safely even when under attack.
- **Cyber risks and physical impacts need to be tightly coupled while teaching CIE:** To effectively teach CIE, it is important to tightly couple cyber risks with their physical impacts. Students must not only understand how cyber attacks occur, but also what real-world harm they could cause—especially in safety-critical systems.
- **CIE in curriculum as an experiment:** Integrating CIE into the curriculum is still an evolving process. While resources are available, they are not sufficient on their own to foster deep understanding. Many students initially struggled to distinguish CIE from general cybersecurity frameworks like confidentiality, integrity, and availability (CIA) or even control-theoretic approaches like control invariance. This confusion highlighted the need for more structured guidance, framing, and examples that clearly demonstrate what makes CIE distinct: engineering-first thinking, consequence-driven design, and system-level integration of security.
- **Longer CIE exposure helps in internalizing the benefits of CIE and will likely improve adoption:** While a single assignment or lecture can introduce students to CIE principles, brief exposure may not be enough for them to confidently apply the concepts in engineering design. Students became more comfortable with CIE ideas after encountering them in multiple assignments. Gradual, repeated engagement seems to help students better connect CIE principles to real-world system design, especially in complex cyber-physical domains like drones.

4.4. University of Illinois Urbana-Champaign (UIUC)

At UIUC, faculty and staff promoting CIE concepts face common challenges when introducing a new framework into an already packed engineering curriculum. Their efforts highlight practical approaches to embedding CIE into existing programs.

- **Embed CIE into existing courses**: Most majors have extensive required coursework and electives, leaving little room for additional content. Despite these challenges, ITI, ECE, Civil Engineering, and other departments are exploring ways to embed CIE principles into existing courses. ITI staff view this as the most effective approach for building awareness, generating interest, and fostering collaboration with faculty who recognize the value of CIE integration.
- **Utilize guest lecturers**: While the creation of entirely new CIE-focused courses in the near term is unlikely outside ITI and ECE, a planned course launch in 2026 could provide a model for adoption across other engineering departments in future years. In the meantime, guest lectures - particularly in lab-based or project-focused courses - offer the most practical pathway for integrating CIE concepts into Illinois' curriculum.

4.5. University of Texas at San Antonio (UTSA)

From UTSA's experience implementing CIE highlights several lessons for effectively integrating the framework into hands-on engineering education.

- **Modularity**: The modular nature of the Amatrol stations enables flexible exploration of fault propagation and CIE interventions.
- **Create practical exercises**: Embedding CIE principles in concrete lab tasks (e.g., validation logic, attack graph construction) increases comprehension.
- **Consistency is key**: Ensuring consistent instructor guidance is crucial to prevent lab deviations or misinterpretations of cybersecurity scenarios.
- **Consider available resources**: Hardware constraints may limit the scope of some failure simulations.

5. Recommendations for Other Institutions

Institutions that have begun the task of implementing CIE into their curricula have kindly offered their recommendations to other institutions that wish to do the same.

5.1. Auburn University

Auburn University encourages other institutions to integrate CIE principles into existing engineering courses.

- **Embedding CIE within the curriculum** ensures cybersecurity is treated as a core aspect of engineering design.
- Using **real-world scenarios**, such as critical infrastructure challenges, helps students apply these principles in practical contexts. Emphasizing the full system life cycle further reinforces the connection between secure design and long-term resilience.
- **Cross-disciplinary collaboration** among faculty and investment in instructor development are essential for effective delivery. Aligning educational efforts with national and industry needs ensures graduates are prepared to support the cybersecurity of critical systems.

5.2. Boise State University

Boise State recommends that institutions integrate CIE principles into existing engineering and STEM curricula rather than treating CIE as a standalone specialty. Key considerations include the following:

- **Develop entry-level CIE courses with minimal prerequisites** so students across engineering and related disciplines can participate.
- **Use real-world critical infrastructure examples** to help students connect theory to practice.
- **Embed CIE concepts throughout the engineering lifecycle**, reinforcing that cybersecurity is a core design consideration
- **Foster faculty collaboration across departments** to ensure CIE is taught consistently and aligned with industry and national security needs. A CIE course with minimal prerequisites, in which students from all engineering or STEM disciplines can enroll to learn.

5.3. Georgia Tech

Through the addition of CIE into Georgia Tech's curricula, it has the following recommendations to offer:

- When designing assignments, instructors **should maintain a clear separation between cyber and physical components** in the problem statement, such as identifying which subsystem is vulnerable and what physical outcome might result from an exploit. However, in the solution, students must connect the two domains and work through the full lifecycle: attack prevention, detection, and mitigation.
- Assignments should **explicitly ask students to protect both the system and its "mission".** This means addressing system continuity and not just stopping the attack. Framing challenges this way reinforces the core CIE mindset: securing engineered systems to be resilient by design, with both safety and security in mind.
- **Be aware of the differences in thinking between cyber and engineering students:** Cybersecurity students will naturally gravitate toward principles under active attack prevention[11] to design technical countermeasures tailored to specific threat models. On the other hand, engineering students will find value in system understanding and attack-impact minimization principles[12] that will help them evaluate how physical systems respond under attack and plan resilient responses that prioritize mission continuity and safety. This separation will allow students

[11] Outlined by Georgia Tech, these include Secure Information Architecture, Engineered Controls, and Active Defense.
[12] Outlined by Georgia Tech, these include Consequence-Focused Design, Engineered Controls, Planned Resilience, and Layered Defense.

5.4. University of Illinois Urbana-Champaign

The University of Illinois Urbana-Champaign offers the following advice to institutions seeking to integrate CIE into their curricula:

- Begin by **leveraging existing courses**, particularly lab-based or project-focused offerings, to build awareness and demonstrate relevance without overhauling curricula.
- **Guest lectures and modular content can serve as effective entry points**, while early engagement with faculty is critical to highlight the alignment of CIE with their teaching objectives, research interests, and professional priorities.
- Because CIE is relevant across multiple disciplines, programs should **encourage participation from civil, computer, industrial, biomedical, and other engineering fields**, as well as related areas such as computer science and education.
- **Incorporating CIE principles into research initiatives and engaging industrial partners can further support adoption** by demonstrating real-world application and value. Over time, institutions may consider piloting an introductory CIE course that can serve as a framework for broader curriculum development.
- **Viewing CIE integration as an incremental process** - focused initially on socialization, proof-of-concept opportunities, and faculty collaboration - can help ensure sustained adoption and long-term impact.

5.5. University of Texas at San Antonio (UTSA)

When initiating the implementation of CIE into an institution for the first time, UTSA recommends:

- **Start with Consequences**: Focus student attention on the real-world outcomes of cyber disruptions rather than abstract technical exploits.
- **Utilize Modular Testbeds**: Platforms like Amatrol offer a scalable, controlled environment for introducing cyber-physical interactions.
- **Map CIE Principles Explicitly**: Link each activity or mitigation to a specific CIE principle so students internalize the framework.
- **Leverage Attack Graphs**: These help students visualize cascading effects and identify where controls should be placed.
- **Simplify Design**: Encourage minimal viable automation logic to teach how overcomplexity can increase vulnerability.

6. Conclusion

This Curriculum Guide is a tool for bridging the current gap in engineering education by embedding CIE principles into academic programs. By incorporating the guidance, framework, and resources provided, educational institutions can prepare a new generation of engineers and technicians who are not only proficient in their traditional disciplines but are also equipped with the knowledge and mindset to integrate digital risk consequence considerations into all phases of engineering practice. This principled answer to digital modernization in curricula is critical, considering the increasingly sophisticated cyber threats targeting the Nation's infrastructure. By

ensuring that CIE is a core element of digital risk management in engineering education, future engineers are empowered to innately prioritize resilience, thereby reinforcing the resilience of our infrastructure against the evolving landscape of cyber threats.

Additional Curriculum Resources are in active development and may not be captured in this current iteration of the curriculum guide.

Visit the resources below to stay up to date with CIE and CIE Curriculum Resources.

CIE Website:
Visit DOE CESER's CIE Program page

CIE Resources Library:
inl.gov/cie-resource-library/

CIE Community of Practice (COP)
Email CIE@inl.gov to join the CIE COP and its three monthly Working Groups: Standards, Education, and Implementation.

Should you find yourself with curricula ready for a CIE review or in need of expert CIE guidance, please do not hesitate to contact us. Support is available to ensure that your materials meet the principles of CIE. For document review or any additional inquiries send an email to CIE@inl.gov, and we will be glad to assist you.

Additional curriculum resources are available through the CIE Community of Practice Education Working Group. To join, send an email requesting membership to CIE@inl.gov.

The Education Working Group meets on the third Wednesday of every month at 9 am MT / 11 am ET. Its purpose is to develop curricula and materials that integrate CIE principles into engineering degree programs. Members will also be added to the Quarterly CIE COP (which meets on the second Wednesday of January, April, July, and October at 11 am MT / 1 pm ET) to stay informed about CIE development across all three COP Working Groups: Standards, Education, and Implementation.

Appendix A: Learning Objective Examples

To ensure the effectiveness of CIE assignments, courses, and programs, it is essential to establish clear learning objectives and develop robust assessment methods. The following learning objectives focus on the CIE principles and their key questions. These are presented as examples and are not meant to be seen as comprehensive.

Additional Resource: CIE Implementation Guide
Consider using the CIE Implementation Guide to further refine or expand learning objectives that better fit your specific CIE focus.

Principle		Key Question	Key Learning Objective
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?	Define what is a critical function considering undesired consequences.
			Identify a critical function within a collection of system functions.
			Implement an industry-provided classification method for identifying critical functions.
			Compare and contrast the system functions considering consequences to enumerate the critical functions.
			Determine critical functions of a system and evaluate whether it prevents undesired consequences.
			Develop a critical function and consequence classification method.

Principle		Key Question	Key Learning Objective
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?	Define what an engineered control is.
			Identify engineered controls in a system.
			Given a list of system controls, select and implement engineered controls in a system.
			Given a list of system controls, distinguish between the engineered controls and the digital controls.
			Judge the effect of an engineered control in its ability to reduce the avenue for attack or the damage that could result.
			Design an engineered control that reduces the avenue for attack or the damage that could result.
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?	List the important data points in a system for a given function.
			Locate the path for an important data in a system for a provided function.
			Sketch the path and transformations that an important data undertakes in a system for a provided function.
			Question whether the path used by an important data in a system for a provided function can be improved.
			Defend that the path selected for important data is the most optimal from a cybersecurity standpoint.
			Construct a secure data path for an important data tag in a system for a provided function.

Principle		Key Question	Key Learning Objective
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?	List an example of an unnecessary feature in relation to a system function.
			Explain what an unnecessary feature looks like and how its removal does not impact the critical functions of the system.
			Distinguish between features of a system that are not absolutely necessary and those that are necessary to achieve critical functions of a system.
			Illustrate the difference between necessary and unnecessary features and how those that are unnecessary do not impact the critical function.
			Convince someone else that a certain function is unnecessary to the successful operation of a critical function of the system.
			Modify a system by successfully removing a previously implemented function and confirming its success operation.
5	**Layered Defenses**	How do I create the best compilation of system defenses?	Define defense in depth as a principle for securing a system.
			Discuss how multiple layers provide redundancy of defenses.
			Determine a set of system defenses that are completely independent from one another.
			Categorize a set of system defenses into cyber-vulnerable and not cyber-vulnerable.
			Defend whether a set of system defenses provide completely independent protections against cyber threats.
			Create a compilation of independent system defenses.

Principle		Key Question	Key Learning Objective
6	Active Defense	How do I proactively prepare to defend my system from any threat?	Outline the role of active defense.
			Discuss the use of active defense in system response to threats.
			Model the roles and responsibilities of active defense in an organization.
			Diagram the actions and triggers for an active defense implementation.
			Grade the effectiveness of an active defense implementation.
			Develop an active defense plan for a list of anomalies, system conditions, and circumstances that could bring about adverse consequences.
7	Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?	Define what an interdependence is and what it is not.
			Give an example of an interdependence in a system with another system.
			Determine where a system can impact others or be impacted by others.
			Analyze a system for its set of interdependencies.
			Evaluate the strength of interdependency for each of the interdependencies for a system.
			Formulate a method for evaluating the level of interdependency that is in a system or system of systems.

Principle		Key Question	Key Learning Objective
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?	Identify a digital asset within a system.
			Contrast where digital assets are present and where they are not present in a system.
			Illustrate where digital assets are used in a system.
			Break down what functions are provided by digital assets in a system.
			Evaluate what a function in a digital asset is capable of in a system.
			Formulate the assumptions about how a function works in a digital asset within a system
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?	List out examples of supply chain requirements for sharing information about cyber incidents, vulnerabilities, bills of materials and vendor development processes.
			Summarize the purpose of procurement language and contract requirements as it pertains to security.
			Predict how an example of procurement/contract requirement language can provide security to the system.
			Analyze how an example of procurement/contract requirement language can be verified.
			Grade the level of success in protecting the supply chain of the system given a set of procurement language or contract requirements.
			Formulate the behaviors, assumptions, and core security features that a vendor could practice when providing components or services into a system.

Principle		Key Question	Key Learning Objective
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?	List a set of digital-compromised (i.e. digital failure or cyber attack) failure modes in a system.
			Discuss different system failure modes, including how to operate through them, even if it is at a lower level of performance or reliability.
			Model a set of known diminished operating modes for a system.
			Classify diminished operating modes with its system operations (i.e. operating when the team is uncertain of the validity of the data emerging from the system, when automation logic is not dependable, or support services are not available).
			Judge between a set of diminished operating modes which is more optimal.
			Create a system condition for safe failure or continued operations under a cyber incident.
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?	List common engineering documents (i.e. PI&D, design specs, bill of materials, engineer job postings, etc.).
			Discuss the level of understanding of a system given a set of engineering documents.
			Predict the consequence to a system if an adversary acquired an engineering document.
			Associate consequences to the uncontrolled release of various engineering documents.
			Evaluate the effect of loss of engineer documents.
			Create a list of identifiable information that could be misused and a framework to securely contain and exchange the information.

Principle		Key Question	Key Learning Objective
12	**Organizational Culture**	How do I ensure that everyone's behavior and decisions align with our security goals?	List the roles in an organization that participate in a system's lifecycle.
			Describe culture in an organization.
			Model a discussion about how and why cybersecurity is incorporated into a system.
			Analyze a behavior, practice, or choice and its effect on organization's values and priorities.
			Evaluate a job role's contribution to the cybersecurity of a system.
			Create a training that demonstrates alignment of a job role's behavior to an organizational security goal.

Appendix B: Example Course Syllabus

The following syllabus is provided as an example of a CIE Course offered from Boise State University and their adoption of CIE into their institution offerings for engineering students. This course is focused on engineering and cybersecurity and incorporates Cyber-Informed Engineering ideas.

CSE 331: CYBER-INFORMED SYSTEMS ENGINEERING

This course aims at designing systems in the cyber age. Design of reliable and resilient systems for cyber applications, viewed as a step-by-step process through the system life cycle, from design to development, production, and management with cyber as part of design specifications.

COURSE OUTLINE

COURSE INFORMATION

Course Name	Cyber-Informed Systems Engineering			
Course Code	Semester	Lecture (hr/week)	Days	Total Credit
CSE 331		2.5	2	3

Course Objectives	• Understanding the fundamentals of secure design and architecture for enterprise environments. • Analyze how a product's design is based on the cyber-informed engineering (CIE) framework. • Utilize the cyber-informed engineering framework to continuously monitor the usage of a product from the cradle to the grave. • Enhance cybersecurity by deploying operations resiliency and CIE processes throughout product development. • Introducing Cyber-Physical Systems and Modeling
Learning Outcomes	• Make decisions based on the cyber security field's ethics, laws, policies, and governance. • Apply acceptable tactics, techniques, and procedures to enhance cyber-physical and informational security operations and resiliency. • Apply industry-acceptable cyber security models to secure, inform, involve, and educate stakeholders in security/resilience operations and strategies. • Continuously evaluate and monitor the operational and resilient maturity of an entity. • Develop operation and resiliency policies, metrics, testing, and security solutions for an entity using rigorous risk assessment and threat intelligence people, processes, tools, and measures. • Designing and Modeling Cyber-Physical Systems.

COURSE TOPICS & STUDY MATERIALS

	Topic	Description
Week s~5	Introduction to Secure Design and Architecture Fundamentals for Enterprise Environment	• Security Concepts for the Enterprise • Cloud Computing and Virtualization. • Summarize App Development, Deployment, and Automation. • Authentication and Authorization Design Concepts and Controls. • Cybersecurity Resilience. • Security for Embedded and Specialized Systems and Controls. • Cryptography Fundamentals and PKI • Secure Network Architecture Services and Practices. • Security Infrastructure Design • Secure Software Integration • Data Security Techniques • Enterprise Security Emerging Technologies.
Weeks ~4	Implementation of Cyber-Informed Engineering (CIE) Principles	• Purpose of CIE • CIE Principles • Systems Engineering Lifecycle Model for CIE
Weeks ~6	Cyber-Physical Systems: Modeling and Simulation	• Basic Modeling Concepts • Modeling Cyber Components • Modeling Interfaces for Cyber-Physical Systems

Suggested Textbook	• Anderson, R. (2020), "Security Engineering: a guide to building dependable distributed systems." Wiley. ISBN: 978-1-119-64278-7 (ebook available) • Rajeev Alur, "Principles of Cyber-Physical Systems" The MIT Press (optional)

EVALUATION SYSTEM

Semester Requirement	Percentage
Attendance and Class Activities	20
Quizzes	20
Assignment	30
Semester Project	30
Total	**100**

Appendix C: CIE Laboratory Design Guide

A common educational activity in engineering programs is the lab experience. In the context of an engineering program, a "lab" is a controlled environment designed for the purpose of scientific research, experimentation, and analysis. Labs in engineering programs are equipped with specific tools, equipment, and instruments that enable students and researchers to apply the physics and theoretical knowledge practically, conduct experiments, simulate scenarios, and test hypotheses. These lab activities provide hands-on experience that is essential for understanding complex concepts and preparing students for real-world engineering challenges.

This CIE Lab Design Guide complements the CIE Curriculum Guide by offering discussion, insights, and practical examples of a CIE lab experience. This is important for engineering program labs to consider because the tools, equipment, and instruments used by students to analyze and experiment with when applying theoretical knowledge are increasingly being digitized. Even more so, the processes and scenarios that simulate engineering knowledge are being controlled and monitored by equipment and instruments that are increasingly being digitized. Furthermore, the engineering tools used to design equipment and tools to solve an engineering problem are increasingly being achieved through programmed functions and deployed via digital means. With this increase in reliance on digital solutions to apply engineering knowledge, it is necessary to include CIE principles in the lab experience to ensure students consider the ability for the tools, equipment, and instruments to be susceptible to cyber attack and its impact to the physics or theoretical knowledge, experiments, scenarios, or hypotheses. These cyber attacks are problematic considering the impacts that result within these engineering processes. Students in engineering programs shaped with a CIE worldview are trained to question and consider the implication of the digital failure mode as part of their engineering decision making for this modern digital age.

To achieve this, especially from an engineering perspective, engineers do not need to become cybersecurity professionals. Rather, they must be “cyber-informed” at a minimum. This means being aware of cyber impacts that come from manipulating some of the variables in the engineering process, understanding the implications of incorporating digital assets, and being prepared to offer engineering standards of care throughout the life cycle of engineered solutions.

C.1 Discussion

In university engineering labs, the use of digital tools and equipment is crucial for teaching students about real-world applications of their theoretical knowledge. For example, in electrical engineering and mechanical engineering programs where students explore the concepts of control theory with a lab experience. In these labs, they may feature programmable logic controllers (PLCs) that use Proportional, Integral, Derivative (PID) control algorithms. Through computer interfaces and digital equipment, students experiment with and adjust the control parameters of these systems, directly observing the effects of their changes.

When students manipulate the PID settings, they can see how the system behaves under non-standard conditions, including failure modes. This direct interaction with these digital functions

provides a concrete understanding of how delicate the balance of control system parameters is and what happens when that balance is disrupted.

The lab exercise, from a CIE principle perspective, provides opportunity to introduce the concept of adversarial manipulation, pushing students to consider system security. They can be tasked with thinking about what might happen if someone with malicious intent were to alter the PID values, which values have greater impact, and how might alternate countermeasures be provided separate from the PLC to maintain stability in the scenario. This encourages students to think about how to mitigate impacts in such scenarios, possibly by designing fail-safes, incorporating safety and security measures, or how to communicate these results to cybersecurity team members.

The result of these types of CIE enhancements in engineering lab activities is the creation of a group of students who are not just knowledgeable in engineering principles but are also aware of and prepared to address impacts that arise from cyber compromises. They learn to anticipate potential threats and to design systems that are resilient against both accidental failures and intentional attacks. This practical understanding of both system dynamics and security thinking is essential in the modern digital world, where technology and threats to it are constantly evolving.

C.2 Insights

It is recognized that current engineering programs at universities offer a vast landscape of lab experiences. These labs are also equipped with a large diversity of digitalized tools, equipment, and instruments integral to the activities and experiments in which students undertake. In such a digitalized environment, students are not just engaging with the physical aspects of engineering but also with the software, control systems, and digital interfaces that drive modern engineering solutions.

The introduction of CIE into these lab experiences brings an additional layer of opportunity to these current lab activities and experiments. When students interact with digitalized engineering tools, they can consider not only how these tools function, which occurs now, but the consequence if their variables are manipulated in a strategic manner. CIE-focused questions provided during these lab activities can prompt students to think about the implications of this digital manipulation.

The CIE Implementation Guide[13] serves as a resource to accomplish this educational process. It offers a body of questions for educators to probe students and address the intersection of cyber impacts and engineering. By using questions from the guide against a laboratory-scale system design, educators can encourage students to examine the use of digital systems, the potential impacts of cyber threats, and how to countermeasure these impacts. Students then foster a questioning attitude as it pertains to the resilience of their engineered solutions and consider how an adversary might exploit digital characteristics.

[13] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. *CIE Implementation Guide*. September 2023. https://www.osti.gov/biblio/1995796.

Incorporating CIE principles into lab experiences challenges the current thinking and traditional approaches to engineering solutions. It compels students to integrate cybersecurity considerations into the design and operational phases. Ultimately, by blending the current depth of lab experiences with these insights from CIE principles, students are better prepared to design, analyze, and protect the complex engineering systems that are foundational to critical infrastructure.

C.3 Lab Use Case Examples

The following three use cases, developed jointly by the Cybersecurity Manufacturing Innovation Institute (CyManII) and the University of Texas at San Antonio (UTSA), guide an audience of engineering students through a manufacturing scenario to analyze and apply a combination of CIE principles and traditional cybersecurity practices.

Access More Resources by Joining the CIE Community of Practice Education Working Group
Complete use cases and additional educational resources are available to members of the CIE Community of Practice (COP) Education Working Group. Email CIE@inl.gov to join.

SEMICONDUCTOR MANUFACTURING PROCESS:

The case study examines the application of cyber-informed engineering (CIE) principles to the photolithography process in semiconductor manufacturing. It focuses on a simulated smart manufacturing environment that replicates key aspects of a semiconductor fabrication facility. The study explores the implementation of CIE principles such as consequence-focused design, engineered controls, secure information architecture, and resilient layered defenses within the context of photolithography. Utilizing a combination of physical hardware and simulation tools, including industrial control system software, networked workstations, and programmable logic controllers, the case study provides hands-on experience in identifying and mitigating cybersecurity risks specific to semiconductor production. Students are challenged to consider the complex interdependencies of semiconductor manufacturing systems, the critical nature of maintaining cleanroom environments, and the potential consequences of cyber attacks on product quality and production efficiency.

ATTACK GRAPH IN A SEMICONDUCTOR WAFER FABRICATION PROCESS:

The case study explores the application of attack graph-based stochastic modeling and cyber-informed engineering (CIE) principles to enhance cybersecurity in semiconductor wafer fabrication. Focusing on a simulated semiconductor manufacturing environment, the study demonstrates how attack graphs can be utilized to visualize potential vulnerabilities and attack paths within the facility's network infrastructure. The case study examines the implementation of key CIE principles, including consequence-focused design, engineered controls, and resilient layered defenses, within the context of semiconductor production. Using a combination of network equipment, Raspberry Pi devices, and simulation software, students engage in hands-on activities to identify critical nodes, assess potential cyber risks, and develop targeted defense

strategies. By integrating attack graph analysis with CIE principles, this comprehensive approach aims to equip students with the skills to protect advanced manufacturing processes.

CNC MACHINE IN A SMART MANUFACTURING FACILITY:

The case study examines the implementation of cyber-informed engineering (CIE) principles in a smart manufacturing facility, focusing on a Tormach 1100MX CNC machine. The case explores key CIE principles, including consequence-focused design, engineered controls, secure information architecture, and cybersecurity culture. It emphasizes the importance of continuous monitoring using design integrity metrics, profile monitoring, and operational metrics to maintain system security and efficiency. The case study highlights the integration of advanced technologies such as 3D scanners and energy sensors to enhance security measures and operational effectiveness. Students are encouraged to consider the interdependencies between systems, the management of digital assets, and the development of resilient defense strategies.

Appendix D: Principle-Specific Activities

The following example activities demonstrate how to consider individual principles to improve a student's CIE competency.

Principle 1 Consequence-Focused Design

Given access to a system, its documentation, and its business context, describe what physical events cannot be allowed to occur.

- Create a list of impacts to the critical function that must not be allowed to occur.
- Characterize the impacts.

Principle 2 Engineered Controls

Given a scenario, such as:

- An adversary has successfully breached cybersecurity defenses and compromised the digital control systems of a boiler system. The worker, with a comprehensive understanding of both the digital and mechanical components of the boiler system, needs to respond to this threat.
    - The student identifies the pressure release valve as an engineered control designed to prevent physical damage to the boiler in the event of digital system manipulation.
- An HVAC system is presented to the worker, detailing all digital and mechanical components. Upon examination, it is evident that no fuses are installed to protect the variable frequency drive components.
    - The student identifies the absence of fuses as a vulnerability that could lead to physical damage to the motor drives in the event of a cyber attack.
- A backup mechanical breaker is installed in line with a digital relay in a substation, and the breaker is set to trip when it detects conditions that exceed preset mechanical thresholds.
    - The student recognizes the mechanical breaker as an engineered control necessary to prevent system damage in the event the digital relay is compromised.
    - The student includes inspection and testing of the breaker as part of their maintenance routine.
- A manufacturing plant relies on an automated control system to manage its production line. The plant's operations include high-precision CNC machines for cutting and shaping metal parts. These CNC machines have hardware interlocks that trigger an emergency stop if overheating is detected.
    - The student recognizes the hardware interlocks as an engineered control to prevent catastrophic damage in the event the SCADA system is compromised by a cyber attack.
- The student includes inspection and testing of the hardware interlocks as part of their maintenance routine.

Principle 3 Secure Information Architecture

A scenario where the student is asked to replace the analog pressure gauges with digital pressure gauges so that they can be remotely monitored and reduce workforce labor and other business drivers.

- Identify the requirements for the digital meter.
- Do market research to find and identify options based on requirements.
- Address the pros/cons of the new digital meter.
- Make a recommendation based on the above.
- Explaining how the meter contributes to the system's critical functionality.

-or-

Given an existing system architecture, explain how a change to the architecture will enable the compromise of the control of data in the system.

- Identify the critical data within a system architecture.
- Identify the life cycle of the data within the system.
- List potential desired and undesired access and manipulation of critical system data.
- Show how a change in the path creates critical data insecurity.

Principle 4 Design Simplification

The company utilizes programmable logic controllers (PLC's) for critical field functions.

- Identifies that a digital PLC leveraged for a critical function has the potential to be targeted for adversary attack and recommends the disablement of unnecessary functions.
- Provide written documentation for hand off to either the IT or Cyber organization.

Principle 5 Layered Defenses

Student provided design documentation must identify the defenses protecting a critical function from cyber attack to advise if additional defenses are required, providing a fresh perspective to the design team.

- Identify each layer that provides defensive protection to the function and identify additional protection opportunities.

Principle 6 Active Defense

Engineering is asked to provide input to a cyber incident response plan for which they are a stakeholder.

- Student is able to identify necessary linkages to operations team roles and responsibilities and describe engineering and operations-based tasks in active defense of a process system.

Principle 7	Interdependency Evaluation

Given a scenario, such as:

- A critical function of the entity is processing data in a computer center which requires that cooling be available at all times.
    - Student identifies that the HVAC system and the connected water system are upstream dependencies and notifies the system owners about the degree of dependency which exists.
- A company has obtained a UPS and backup generator to support critical functions.
- Student identifies and documents the change in dependency, alerting other stakeholders including new dependencies and recommends reevaluation of response and resiliency plans.

Principle 8	Digital Asset Awareness

Provided with a Piping & Instrumentation Diagram of a System in question:

- Identifies the extent of digital signals being communicated to the Controller.
- Analyzes for the paths in the process system that have digital influence and the implications of that digital influence (i.e. monitoring only, control function present, etc.)

Principle 9	Cyber-Secure Supply Chain

A work ticket is provided to the learner requesting that they perform a set of unit tests on the critical component within a control system and provide the results as part of closing out the ticket.

- Identification of the correct component to perform the unit test on.
- Identification of variances in the expected outcome and the outcome provided by the test.
- Provide documentation of validation and recommendations to consider moving forward after executing the unit tests on the critical components.

Principle 10 Planned Resilience

During a cyber attack on a utility company, the decision is made to sever all external network communications to critical substations and operate manually. Given a detailed description of a system and its incident response plan, the student is tasked with identifying the critical functions of the substation and outlining the procedures for operating these functions manually, without relying on network communication.

- Identify the critical functions.
- Identify the steps to perform manual operation of critical functions.
- Recognize the restoration prioritization.

Principle 11 Engineering Information Control

Given access to a variety of engineering information, identify what details are sensitive and should not be disclosed.

- Recognize engineering information.
- Recognize sensitive details.
- Describe the reasons why details are sensitive.

Principle 12 Organization Culture

Given a policy or standard operating procedure that lacks cybersecurity provisions/considerations, explain to the plant manager why you think an updated policy (that includes security/cybersecurity provisions) is necessary.

- Review an existing policy/procedure.
- Identify cybersecurity weaknesses within the policy/procedure.
- Describe why an improvement is necessary.
- Discuss the implications of the improvement options.
- Propose an improvement.

The following example activity demonstrates how to consider a set of principles in combination to improve a student's CIE competency.

Principle 9	and	**Principle 10**
Cyber-Secure Supply Chain		**Planned Resilience**

Choose an industry of your liking and identify the critical functions. Based on your critical functions and components, implement the 9th (Cyber-Secure Supply Chain Controls) or 10th (Planned Resilience) CIE principle on the systems engineering lifecycle. Your assignment should have the following information:

- Compile a comprehensive report that addresses each principle and system lifecycle's questions accurately.
- List your enterprise's critical functions.
- Use diagrams, examples, and references where necessary to support your points.
- Include a bibliography with references to configuration management literature or related resources.
- If using a generative AI tool (e.g., ChatGPT), write the prompt and the date you have used it in the reference.
- The assignment page should not exceed 5 pages.

Cyber-Informed
Engineering