INL/MIS-24-81718-Revision-0

Cyber Informed Engineering (CIE) Curriculum Guide

November 2024

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

Idaho National Laboratory

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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed 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. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-81718-Revision-0

Cyber Informed Engineering (CIE) Curriculum Guide

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

November 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

Cyber-Informed Engineering

CIE Curriculum Guide

Version 1.0

September 2024

INL/MIS-24-81718-Rev000

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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. government nor any agency thereof, nor any of their employees, makes any warranty, expressed 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. References 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 U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. government or any agency thereof.

Contents

Acknowledgments

CIE Curriculum Guide Version 1.0 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, the universities listed below shared their direct experiences integrating CIE into engineering programs.

Curriculum Guide Development Team:

Benjamin Lampe
Idaho National Laboratory

Edward Huang
Auburn University

Daniel Cole
University of Pittsburgh

Shane McFly
National Renewable Energy Laboratory &
Colorado School of Mines

Matt Luallen
University of Illinois at Urbana-Champaign

Casey O'Brien
University of Illinois at Urbana-Champaign

Dominic Saebeler
University of Illinois at Urbana-Champaign

Sin Ming Loo
Boise State University

Saman Zonouz
Georgia Tech

Animesh Chhotaray
Georgia Tech

Krystel Castillo
University of Texas at San Antonio

Gonzalo Martinez Medina
University of Texas at San Antonio

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. A key goal of this guide is to help institutions deliver CIE-focused education to produce future engineers and technicians who meet the nation's infrastructure needs. To accommodate a broad range of educational goals and approaches, this guide outlines several practical integration strategies, links to resources that can accelerate CIE adoption, and offers perspectives from partner academic institutions on the various implementation strategies.

CIE is a framework for engineers and technicians to integrate engineering controls that reduce or mitigate the impact of cyber attacks into any physical system, used in critical energy infrastructure or in other industries**.** 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 supports that strategic objective by helping institutions integrate CIE into educational programs. It offers a variety of integration strategies, 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 cyber sabotage, exploitation, theft, and misuse within the system.

THE IMPORTANCE OF EDUCATING CYBER-INFORMED ENGINEERS

The U.S. faces ever-evolving cybersecurity threats. 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 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]

[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.

[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.

Now, as this OT environment increases in cyber-physical[4] solutions, the design, configuration, and management of devices and machines is a shared experience between cyber professionals and engineers. Thus, we must build in security through both traditional cybersecurity practices as well as engineering practices. To achieve this, especially from an engineering perspective, engineers do not need to become cybersecurity professionals. 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 life cycle of cyber-physical assets.

At present, engineering that is cyber-informed is not the norm in engineering education. To address this gap, engineering schools must update their curricula to include digital modernization in the curriculum. As the technologies used and deployed in engineering disciplines become increasingly digitized—allowing for possible cyber manipulation—engineers must address this new "failure mode" within their engineering discipline and practices. CIE calls on engineers to include cybersecurity consequence considerations as a foundational element of engineering risk management for any function aided by digital technology.

This guide helps engineering education and training programs to increase focus on the strategic intersection between cybersecurity and engineering, addressing gaps in how we train engineers and technicians, and providing them with the means to build in security 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.

2. Goals and Outcomes

The goal of this Curriculum Guide is to provide guidance, a framework, and resources for incorporating cyber-informed engineering (CIE) into engineering programs and related educational activities.

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

1. **Develop curricula:** Develop CIE curricula that support your institution's specific goals, approaches, and needs. This guide offers practical strategies for integrating CIE at several different levels, and includes examples and insights from university partners.
2. **Plan courses:** Plan courses 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[5] are being addressed.
3. **Design educational activities:** Design educational activities such as assignments, projects, or labs that reinforce CIE concepts.

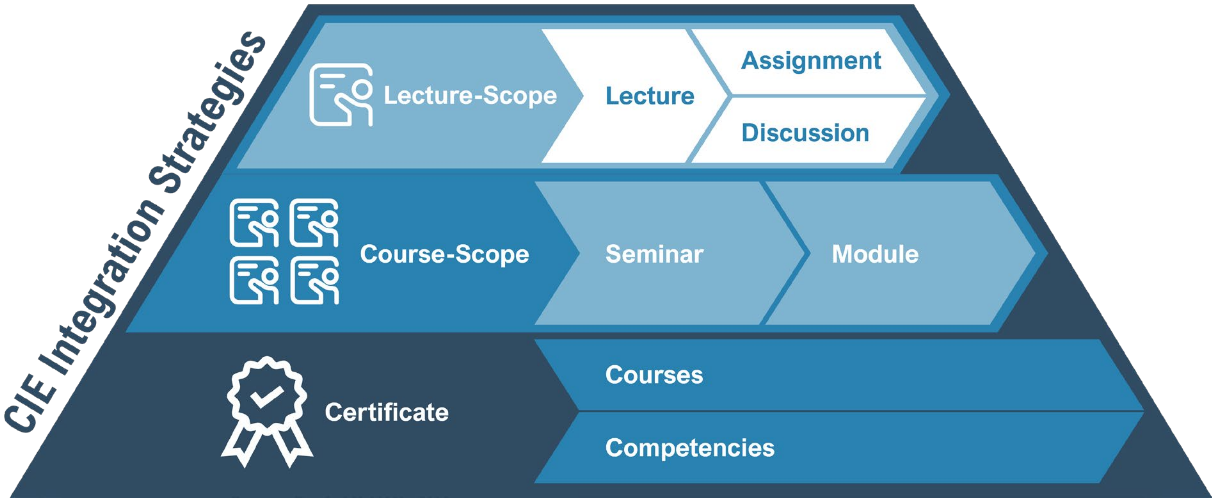
[4] Cyber-physical systems (CPS) are "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components." (Definition derived from the U.S. National Science Foundation.)

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

3. CIE Integration Strategies

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

Figure 1. CIE Integration Strategies



The three strategies allow for a tiered approach within each discipline of practice:

- **Lecture-Scope Strategy:** These options integrate CIE concepts within the context of a class lecture, an assignment, or a class discussion, and are meant for about a one- to four-hour interaction with CIE.
- **Course-Scope Strategy:** These options operate within the context of a single course and are meant for about a 4- to 20-hour interaction with CIE.
- **Certificate Strategy:** These options 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 strategies, a set of learning objective examples are provided in Appendix A. These learning objectives cover the 12 CIE principles 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.

3.1. Strategy 1: Lecture-Scope

The first integration strategy is to incorporate CIE into lecture activities. These activities can include, but are not limited to, the **class lecture** itself, **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.

STRATEGY 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, one option is to survey the twelve principles and describe what each of the principles is.

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

It is important to provide situational examples that you may have encountered in your career 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 lecture if needed.

Focused Case Study of the 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, you are encouraged to use this model, or replace it with your own sector example. If you create your own example, consider sharing with cie@inl.gov as that can also be made available as a curriculum resource to other institutions. For this focused case study, spending five minutes on each principle fills the hour. For a longer class (up to 2-4 hours), participants can spend more time discussing each of the twelve principles and providing a discussion, see Class Discussion section below for a resource. Longer exploration of this case study represents an opportunity for a seminar (or module), see respective section below.

Principle Tagging in Existing Lectures:
Another opportunity exists when considering the breadth that engineering programs cover for engineering students. Because CIE provides a worldview lens by which to interpret the implementation of engineering practices, if faculty recognizes a topic in their course of lecturing that involves the use of digital technologies in calculating engineered outcomes, relating to the use of a related CIE principle is available in that lecture. Consider including a reference to the CIE Implementation Guide and the respective principle page to provide additional context for students to further explore.

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 introduced in general engineering design courses before students progress to specialized engineering design courses. In these general 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 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, such as semiconductor factory design, power grids, anti-UAV defense systems, and airport baggage handling systems, showcasing the application of CIE principles.

Boise State University - The concept of CIE is introduced in various courses (e.g. engineering junior communication course, introduction to engineering course, etc.) 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 Information Trust Institute researchers offer to share the presented material and collaborate on incorporating CIE as a regular course element. They also provide access to the INL CIE site and additional background materials for faculty to review at their convenience. Students are then assigned to rethink design approaches, incorporating security elements early in the engineering process.

STRATEGY 1B: ASSIGNMENT

Assignments or project assignments play a crucial role in integrating CIE into engineering design classes. Each CIE principle can be incorporated into assignments, for example, challenging students to consider both the "As-Is" design and the "To-Be" design while integrating CIE principles. This approach not only assesses students' comprehension of CIE principles but also evaluates their ability to implement them and identify associated benefits.

Often in combination with the class lecture section, these activities are used to check for understanding (at a minimum), but more advanced activities could check for higher levels of learning (e.g., analysis or evaluation). For those lectures, seminars, or modules that focus on surveying the CIE principles, the following are examples that can be used to assess for a level of learning:

CIE Workbooks:

The following set of curriculum resources provides workbooks that are used to engage participants to systematically think through an engineering project considering the CIE principles. This activity, when used within the lecture, seminar, or module format, can provide different uses. For example, when used in a lecture, you may be able to remove specific items 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, you may be able to accomplish the activity through class discussion and participation. Finally, when used as part of a module in a course, the workbook can be 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

It is encouraged that the pattern used in these workbooks provide a model for adopting a sequential approach to walking through the CIE principles in each use case. If you make your own workbook, consider sharing it with CIE@inl.gov so your curriculum resource can be made available to other institutions around the nation and included in future updates.

Specific Principle(s) Activity:

Each principle, or a combination of principles, can be combined as an assignment for students to evaluate and incorporate into the system they are designing. It can also be added as part of a requirement for students to think through and reflect on what they have done as part of the engineering design process. A great place for this type of addition is the capstone design course. The capstone design is a culminating activity that usually involves an industry sponsored project where students can consider the CIE principles and how they use CIE engineering solutions to reduce cyber impacts.

When considering each principle, the following example activities could be used to improve CIE competency of the student:

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.

If you were to combine a set of principles into an activity, you can consider an activity such as:

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 down 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.

Example Perspectives:

Auburn University – In the digital systems engineering design course at Auburn University, CIE principles are assessed through weekly assignments and a semester-long project in a flipped classroom setting. Students analyze the current system, identify cybersecurity issues, incorporate CIE principles, propose a "to-be" system, develop logical and physical architectures, and validate and verify their designs. These topics are evaluated through both the weekly assignments and the project to ensure that students can apply CIE concepts and principles throughout the systems engineering lifecycle. Each week, students develop a part of the "to-be" system, brainstorm approaches to incorporate CIE concepts, and refine their designs with their teammates.

STRATEGY 1C: CLASS DISCUSSION

In both in-person and flipped classrooms, class discussions serve as valuable activities for integrating Cyber-Informed Engineering (CIE) into engineering design classes. These discussions can take the form of team or class dialogues, exploring various methods to integrate CIE into existing designs. Furthermore, students or instructors can act as third-party evaluators, ensuring that CIE principles are incorporated into the design artifacts.

Principle-Specific Discussions

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

The CIE Implementation Guide, is focused on the questions someone may ask when given an engineering project across any point of the system lifecycle. An opportunity exists that when an engineering project, failure mode analysis topic, or an engineering problem is discussed, certain questions from this guide from one of the principle(s) and lifecycle phases can be used as the basis of a discussion. Such a discussion may include consequence, active defense, and technical engineering controls. For example, students need to think through (in a group to capture different thought processes) what the intended and unintended features and uses are for the provided engineering problem. Consequence is an outcome. If the unintended use occurred, what is the unintended outcome? 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.

Once again, while this resource focuses on a Water sector example, you are encouraged to use this model, or replace it with your own sector example. If you create your own example, consider sharing with cie@inl.gov so that it can be made available as a curriculum resource to other institutions around the nation. 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.

3.2. Strategy 2: Course-Scope

The second integration strategy involves creating courses to integrate CIE principles into engineering curricula. These courses would 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 and safe functionalities.

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

STRATEGY 2A: SEMINAR

In short one- to two-hour-long seminars, CIE principles can be motivated using invited talks on attacks and defenses against cyber-physical systems. 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. For example, the previously discussed Water Booster Pump Station case study can be used to explain the twelve principles in a more detailed fashion.

Example Perspectives:

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

Boise State University - In a one-hour seminar, we present hacks involving hardware, software, and industrial control systems, such as Stuxnet, Jeep Uconnect, and the Ukrainian power grid. We discuss why engineering students should learn cyber-informed engineering and how future engineers can apply cyber-informed engineering. Then we spent a little time highlighting the principles of cyber-informed engineering.

STRATEGY 2B: MODULE

Course modules offer another avenue to explain CIE principles in a more detailed way, like long seminars. 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 few CIE principles in a more detailed way. For example, CIE principles such as Active Defense and Planned Resilience can be explained by discussing defense/safety mechanisms against attacks/risks that were not accounted for in the original modeling of the design of a system.

CIE Module:

A module is usually more than one lecture. It can range from a week's worth of content to several weeks. To cover CIE as a module, the Implementation Guide can be used. An overview of CIE is provided. How many principles can be covered depends on the length of the module. The principles can be combined into 3 sets of 4 principles each, or 4 sets of 3 principles each. At times, based on what engineering disciplines are being applied, cover them as a lecture, then in-class actives to further the learning can be more productive. An example of a mock 4-week CIE Module is as follows:

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

Example Perspectives:

Auburn University – The principles of Cyber-Informed Engineering are integrated into general systems engineering design courses. The course comprises 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 - With a module, which could be a week or several weeks, we took the same approach as a seminar. With the availability of the implementation guide, it gives it more structure. If it is a one-week module, we use the implementation guide. If it is more than a week, we have students work on a project that goes through all the phases of design 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 the new material seamlessly integrates with the course's focus.

Georgia Tech – At Georgia Tech, we offer three CIE-informed courses: *Introduction to Cyber-Physical Systems Security, Critical Infrastructures Security and Resilience, and Cybersecurity of Drones*, which satisfy several CIE principles. In these three courses, we 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 cyber-physical systems (CPS) and critical infrastructures, but also understand the importance of resilience and proactive defense measures. Additionally, we promote students to independently learn about the state-of-the-art research in making different cyber-physical systems resilient to failures as well as cyber attacks by including graded paper-presentations as part of the courses.

More specifically, in the *Introduction to Cyber-Physical Systems Security* course, we focus on the fundamentals of CPS security by using Industrial Control Systems (ICS) as the target CPS. In this course, we teach students the complex integration of sensors, actuators, control systems, engineering workstations, human machine interaction (HMI) devices, data historians in an ICS. We emphasize the need to account for the interdependencies between these various components of an ICS while designing defenses again adversarial attacks. This course module satisfies the *Interdependency Evaluation* CIE principle as it emphasizes the need of security-specific design decisions to take into account the interaction between various components of an ICS. In order to protect ICS from cyber attacks, we use our "Hacking ICS" module to teach the critical functions in an ICS and the several consequences that can result from malfunctioning of these functions. For example, a malware that infects an ICS and has arbitrary control over the control systems has the ability to cause a wide range of damage (e.g., damaging the actuators) to the system and also remain stealthy by masking incorrect sensor data. This module satisfies the *Consequence Focused Design* CIE 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?" We also teach students the *Secure Information Architecture* CIE 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 as well as network security measures can be used to protect critical data in the individual security zones as well as the data flowing between zones.

In our more advanced course *Cybersecurity of Drones,* we teach students topics such as *physics-aware malware, actuator control channel attacks* in our "Attacks against Drones" module to allow students to learn about complex and sophisticated adversarial techniques. In order to defend against such adversaries, we also incorporate topics such as firmware reverse-engineering, AI-enabled perception and control to emphasize the importance of CIE principles: *Active Defenses* and *Planned Resilience* against attacks that were not accounted for in the threat modeling of the design of a drone. While *Active Defenses* allows a drone to potentially thwart new attacks, *Planned Resilience* allows for the drone to fail safely if/when the defenses are not able to prevent any attack.

3.3. Strategy 3: Certificate

The third strategy for integrating CIE into curricula is to offer it as a **certificate**. The certificate has courses that are part of the degree requirements, making it available to all STEM students, not just engineering students. This means that STEM graduates will be aware of cyber issues that impact the security of the programs, systems, codes, or algorithms they design.

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 as non-credit; the latter is usually done through a Workforce Development/Continuing Education department or college (e.g., College of Engineering) 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. Lastly, certificates can also be stacked on top of each other, providing a pathway toward more advanced study and other certificates.

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 (the most popular)
- 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, cyber-informed engineering frameworks, and ethics. Students can choose the other nine credit hours from a list of courses for various certificates.

These certifications attempt to help our engineering students to be cyber literate so that they can competently navigate their domain space when addressing cyber challenges. This means that STEM graduates will be aware of cyber issues that impact the security of the programs, systems, codes, or algorithms they design.

Auburn University – To teach students cyber-informed engineering (CIE), we offer a CIE-enabled Systems Engineering Program designed for students from all engineering disciplines at Auburn University. This program is open to students in Aerospace Engineering, Biosystems Engineering, Chemical Engineering, Civil Engineering, Computer Science, Electrical and Computer Engineering, Industrial and Systems Engineering, and Mechanical Engineering. It equips them to apply CIE principles throughout the entire lifecycle of design and management processes. The program includes four key courses. The first two courses 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 courses 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

Given enough courses, one could logically make a degree program rather than a certificate. his concept does not align with the core of CIE implementation guidance. CIE represents a worldview framework intended to shape the interpretation and practice of engineering, rather than serve as 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, we anticipate 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, we integrate CIE principles into our existing undergraduate programs, in-person master's/PhD programs, and the online Master of Engineering Management 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 life cycle. 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 our cybersecurity program, for subsequent courses. This approach affords students the opportunity to cultivate both breadth and depth of knowledge in applying CIE principles to real-world scenarios.

Boise State University - The computer systems engineering degree balances skills from both computer science and electrical engineering, with a focus on designing systems with cybersecurity in mind. This newest undergraduate degree in computer systems engineering includes two cyber courses. The first course is the introductory course mentioned above. The second course is Cyber-Informed Engineering. This course aims at designing systems in the cyber age. Designing reliable and resilient systems for cyber applications, viewed as a step-by-step process through the system life cycle, from design through development, production, and management, with cyber as part of the design specifications.

For our students in the asynchronous online cyber operations degree, we also offer a one-credit hour cyber-informed engineering course. Cyber touches every aspect of our lives, and more and more systems have some level of connectivity to the Internet. These systems could be mission-critical systems, life-saving and life-supporting systems, mechanical autonomous systems, industrial control systems, critical infrastructure, and so on.

4. Conclusion

This Curriculum Guide is a tool for bridging the current gap in engineering education by embedding cyber-informed engineering (CIE) principles into academic programs through various options. 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 cybersecurity 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 cyber risk management in engineering education, we empower future engineers to innately prioritize security in the digital age, 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 curriculum ready for a CIE review or in need of expert CIE guidance, please do not hesitate to contact us. Support is available in ensuring that your materials meet the principles of CIE. For document review or any inquiries you might have, 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 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 question. 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.

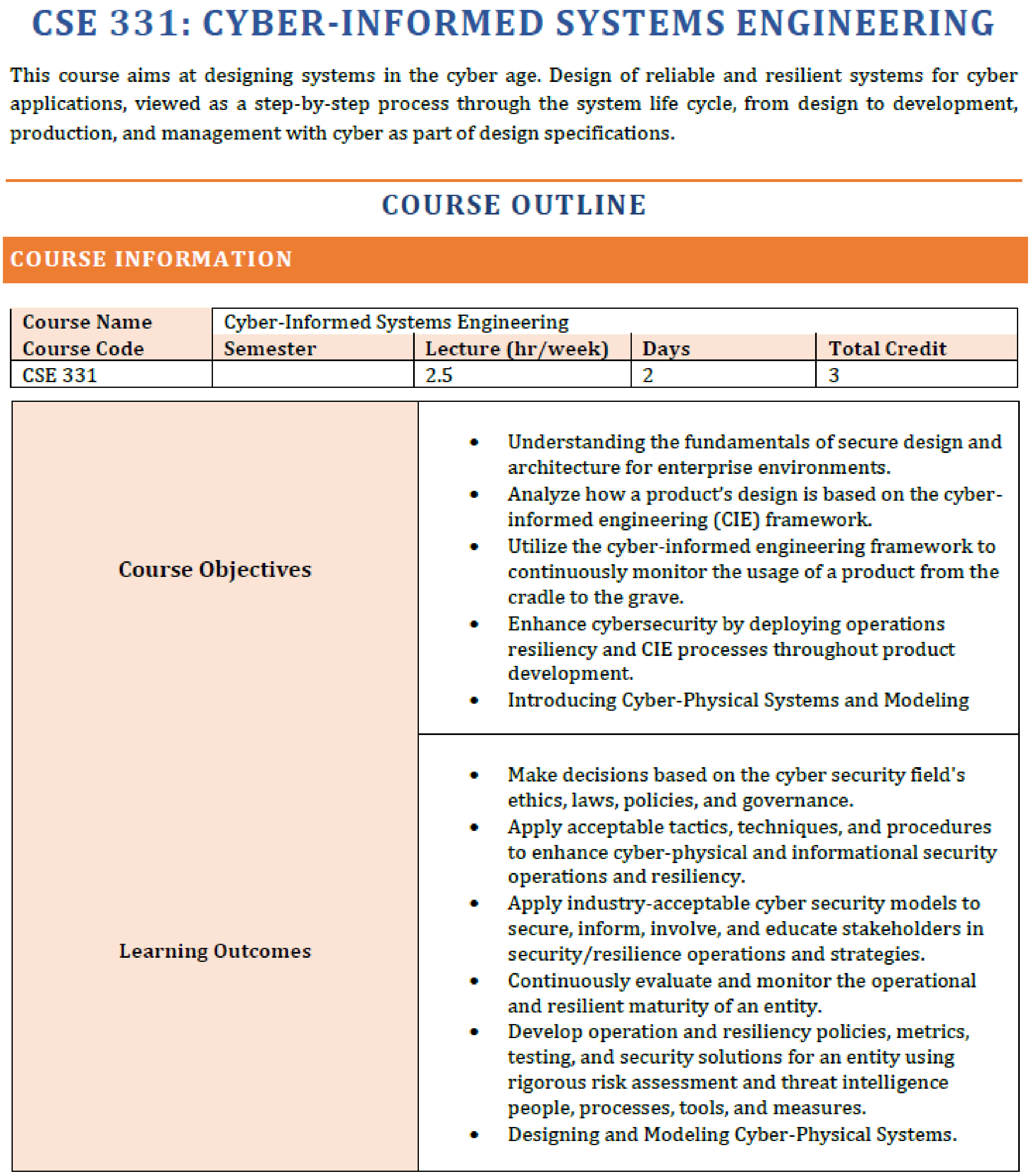
	Principle	Key Question	Key Learning Objective
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?	Identify a digital asset within a system.
			Contrast where digital assets are present and where 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 the 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 we provide alternate countermeasures 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 might these results be communicated to cybersecurity team members.

The result of this type 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[6] 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.

[6] 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 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.

Cyber-Informed Engineering