INL/CON-23-71008-Revision-0

Cyber-Informed Engineering GuidanceImplementing CIE in Early Systems Engineering Lifecycle Stages

June 2023

Shannon Leigh Eggers, Katya L Le Blanc, Robert S Anderson, Virginia L Wright

Changing the World's Energy Future

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

INL/CON-23-71008-Revision-0

Cyber-Informed Engineering GuidanceImplementing CIE in Early Systems Engineering Lifecycle Stages

Shannon Leigh Eggers, Katya L Le Blanc, Robert S Anderson, Virginia L Wright

June 2023

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 Guidance—Implementing CIE in Early Systems Engineering Lifecycle Stages

U.S.A.

Shannon L. Eggers[1], Robert S. Anderson[2], Virginia L. Wright[3], Katya L. Le Blanc[4]

Idaho National Laboratory

[1]Shannon.Eggers@inl.gov, [2]Robert.Anderson@inl.gov, [3]virginia.wright@inl.gov, [4]Katya.Leblanc@inl.gov

Abstract

Traditionally, cybersecurity is not considered in the design process. Design engineers typically focus on building safety and reliability into their products and applications. Security against malicious cyber incidents is often an afterthought, resulting in deployment of security solutions during installation or operation. Unfortunately, waiting to consider cybersecurity until later in the systems engineering lifecycle often results in less effective and more expense security. Idaho National Laboratory (INL) developed the concept of Cyber-Informed Engineering (CIE) in 2015 to provide a framework that enables cybersecurity to be built into systems beginning at the conceptual design stage. In addition to ongoing research by INL, the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response has recently developed a National CIE Strategy document for incorporating CIE into the design and operation of infrastructure systems reliant on digital monitoring or controls. This paper provides a brief review of this National CIE Strategy as well as a roadmap to historical, current, and future CIE research by INL through the U.S. DOE Office of Nuclear Energy (NE) Cybersecurity Crosscutting Technology Development Program. A near-term focus of the DOE-NE's research and development is to extend the foundational CIE work into detailed guidance for implementation during initial systems engineering stages in nuclear digital instrumentation and control projects and to demonstrate use of the guidance in an integrated energy systems project.

1. Introduction

The U.S. Department of Energy Office (DOE) of Cybersecurity, Energy Security, and Emergency Response (CESER) released a National Cyber-Informed Engineering (CIE) Strategy document in June 2022 to further increase security, reliability, and resilience in the energy sector. This strategy document builds on foundational work developed at Idaho National Laboratory (INL) that began in 2015 [1]. CIE is a multidisciplinary approach advocating the use of a set of principles throughout the systems engineering lifecycle to ensure that cybersecurity is considered in every aspect of design, testing, implementation, operation, maintenance, and disposal (or decommissioning). Fundamentally, CIE is a cyber risk management tool that complements existing cybersecurity practices by incorporating engineering solutions, information and communications technology solutions, and operational technology solutions to minimize risks from malicious and unintentional cyber incidents. Even though the scope of digital engineering modifications at nuclear facilities may vary, incorporating CIE methodologies can provide enhanced capabilities for protection from, detection of, and response to consequences resulting from compromise or failure. Designed-in solutions typically provide more secure solutions at lower cost than solutions bolted-on during deployment or operation. The goal of this paper is to provide an overview of

the U.S.'s new National CIE Strategy and to provide a roadmap of historical, current, and future CIE research.

2. U.S. National Cyber-Informed Engineering Strategy

Current engineering design practices often focus on safety and reliability of a device or system, neglecting to consider cybersecurity risks from intelligent, capable, and persistent adversaries. The consequence of this decision is that treatment of cyber risk is delayed until implementation and operation, resulting in bolted-on rather than built-in cybersecurity. The U.S. DOE-CESER released a National CIE Strategy report in June, 2022, [2] with a goal to incorporate the principles of CIE into the design and operation of infrastructure systems that rely on digital assets. As illustrated in Figure 1, the five strategy pillars aim to provide awareness of CIE, embed CIE into education, develop the body of knowledge for CIE, apply CIE to current infrastructure, and continue research and development (R&D) for future infrastructure.

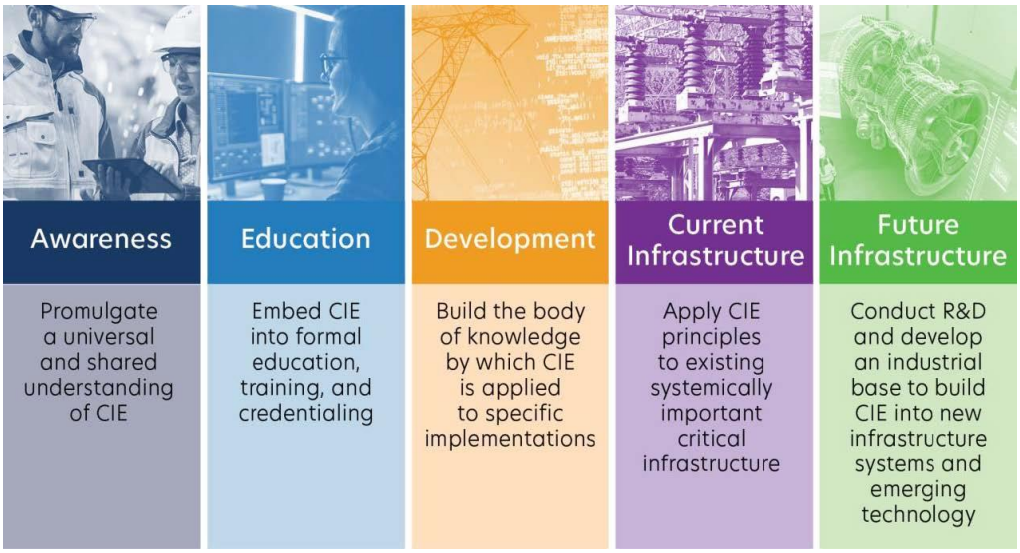

Figure 1. The five pillars in the U.S. DOE-CESER National Strategy to incorporate CIE as common practice across the energy sector [2].

CIE incorporates design and organizational principals to engineer out some cyber risk throughout the systems engineering lifecycle, beginning with earliest stages. Table 1 provides a set of principles established by the National Strategy to consider when designing a new digital device or solution.

Table 1. The U.S. DOE-CESER CIE National Strategy principles [2].

Design & Operational Principles	Organizational Principles
Consequence-focused design	Interdependency evaluation
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Resilient layered defenses	Planned resiliency with no assumed security
Design simplification	Engineering information control
Active defense	Cybersecurity culture

3. Review of Past Research by the U.S. DOE-NE Cybersecurity Program

One recommendation in the "development" pillar of the strategic plan is to leverage U.S. DOE National Laboratories, academia, government partners, and industry to continually improve and expand upon the

applicability of CIE [2]. CIE is a focus area of the U.S. DOE Office of Nuclear Energy (NE) Cybersecurity Crosscutting Technology Development Program. The research, development, and demonstration of CIE in the nuclear domain by National Laboratories participating in the DOE-NE Cybersecurity Program will help build the body of knowledge and formalize CIE best practices, thereby adding to the open-source library of CIE tools, case studies, and lessons learned.

While the concept for CIE began in 2015, the initial CIE framework was developed in 2017 by Idaho National Laboratory (INL) under the DOE-NE Cybersecurity Program [3]. This framework provides a foundation for CIE principles and describes how they can be implemented and integrated into a nuclear facility with the stated goal to deepen "the involvement of engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threats [3]." This 2017 report also provides preliminary application aids to use through the systems engineering lifecycle.

In 2021, researchers at INL evaluated use of the CIE framework developed by Anderson et al. [3] in the high-level design stage of a hydrogen generation project in which heat and electricity are provided by a nuclear power plant [4]. In this research, a hazard and operability (HAZOP) study was conducted to identify the consequences of cyber incidents on digital instrumentation and control (I&C) components. This cyber risk analysis discovered several vulnerabilities in the design that ultimately resulted in simplification and redesign of the digital I&C system [4]. This research project also highlighted the importance of a multidisciplinary approach that provided opportunities for each team member to learn more about the interconnections between engineering, safety, risk, and cybersecurity [4].

Further insight into the use of CIE for nuclear reactor digital I&C can be found in [5]. This publication provides a brief primer on nuclear reactor I&C and their associated cyber risks while also outlining how CIE might be used in current and future reactor designs and applications [5]. Figure 2 shows a notional usage of CIE principles throughout the entire systems engineering lifecycle.

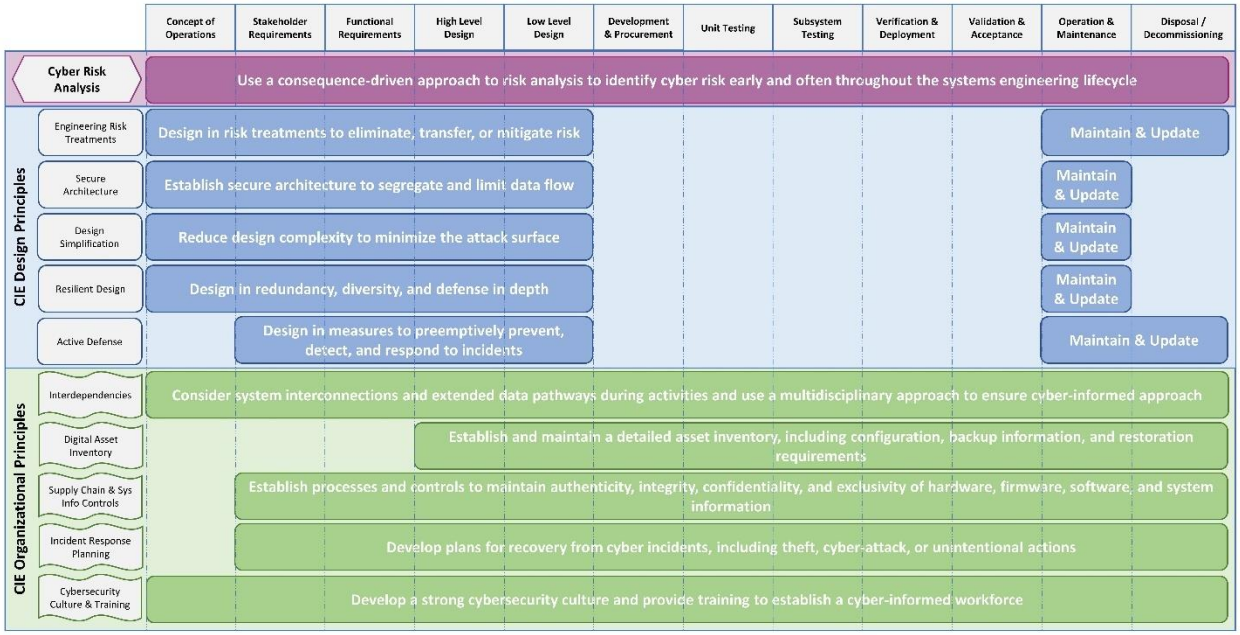

Figure 2. Notional usage of CIE principles throughout the systems engineering lifecycle [5].

4. Current and Future Work

INL is currently developing guidance on use of CIE during the early stages of the systems engineering lifecycle for nuclear digital I&C projects, including development of new reactor technologies and advanced reactors. The objective of this guidance is to provide detailed suggestions and application aides for how to consider and implement CIE activities. An example of the workflow for the stakeholder requirements stage is shown in Figure 3. Similar to the Systems Engineering Guidebook for Intelligent Transportation Systems [6], the guidance will provide the objective, description, and context for each lifecycle stage. The context includes inputs, constraints, enablers, activities, and outputs for incorporating cybersecurity into the project. Examples of each context will be provided, with detailed recommendations where possible.

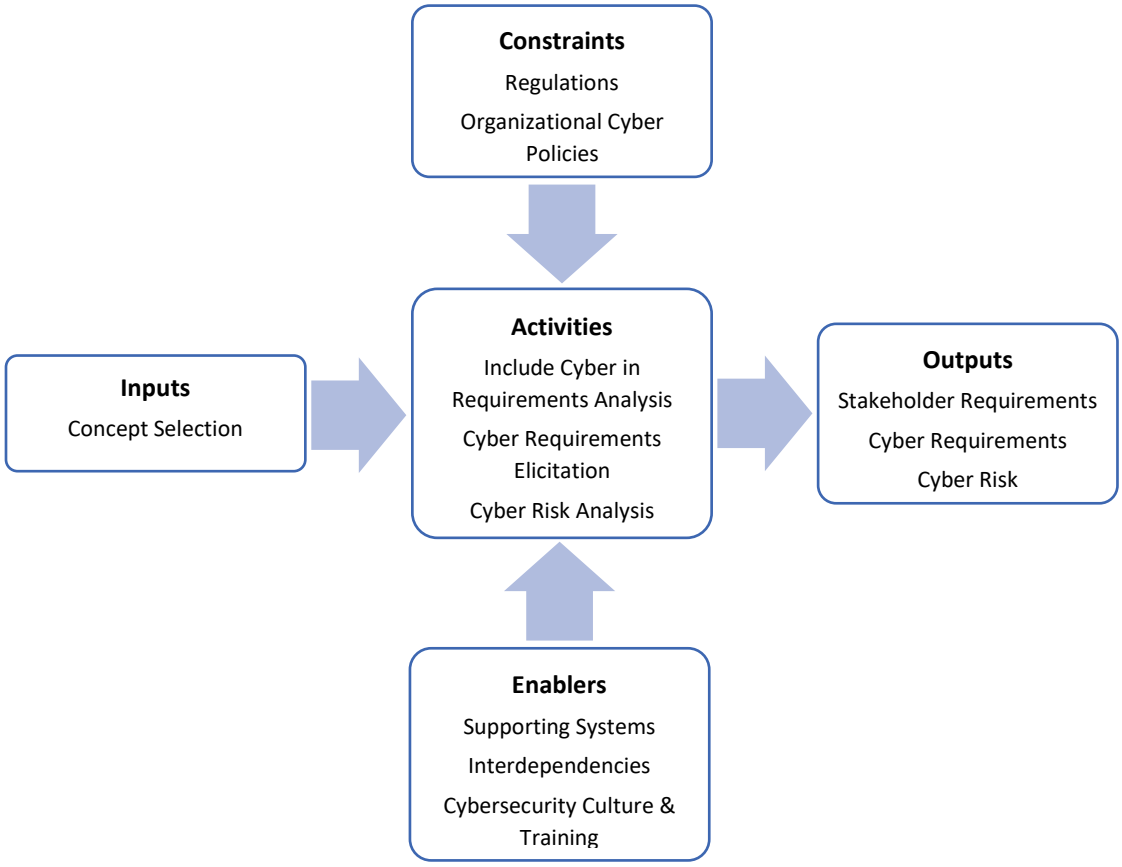

Figure 3. Notional context example for the stakeholder requirements stage.

After this initial guidance is developed for the early stages of nuclear I&C projects, including feasibility, concept of operations, stakeholder requirements, system requirements, and high-level design, the DOE-NE Cybersecurity Program will perform case studies to demonstrate its use and to identify improvement opportunities. It is anticipated that an initial case study will include an integrated energy system interconnected with a small modular reactor. Other case studies have been defined but not yet established. Collaboration with industry organizations and nuclear facilities is anticipated and desired, with the end goal of building the CIE body of knowledge and expanding the CIE open-source repository with concrete examples for incorporating CIE into academia and industry.

Supporting this work, DOE-CESER is building awareness of CIE through engagement with asset owners and operators, universities, vendors, and CIE practitioners through a broad community of practice. They are working with multiple universities to build CIE into engineering curriculum to build the awareness of cyber risks which might affect engineered systems and the potential to leverage engineering design mitigations to reduce the likelihood or impact of such events. CESER is also developing a library of resources which can be leveraged by CIE practitioners to guide their work.

Conclusion

The broader adoption of CIE will enable cyber risk reduction throughout critical infrastructure, including nuclear facilities. The CIE National Strategy is a transformational approach to cybersecurity to further increase the security, reliability, and resilience in the energy sector. The CIE framework requires engineers to build cybersecurity into the design by promoting both secure-by-design and organizational concepts. The DOE-NE Cybersecurity Program and INL researchers plan to continue researching the CIE framework to develop detailed, actionable guidance that nuclear projects can use to ensure cybersecurity is introduced early and often throughout the systems engineering lifecycle.

Acknowledgments

This work was supported by the U.S. DOE Office of Nuclear Energy Cybersecurity Crosscutting Technology Development Program and the U.S. DOE National Nuclear Security Administration Office of International Nuclear Security under the DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

References

[1] Anderson, R. and J. Price, "Cyber Informed Engineering: The need for a new risk informed and design methodology," Idaho National Laboratory, INL/CON-15-34244, June 2015, Available: https://inldigitallibrary.inl.gov/sites/sti/sti/6618307.pdf.

[2] DOE, "National Cyber-Informed Engineering Strategy from the U.S. Department of Energy," U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, 2022, Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

[3] Anderson, R.S., J. Benjamin, V.L. Wright, L. Quinones, and J. Paz, "Cyber-Informed Engineering," Idaho National Laboratory, 2017.

[4] Eggers, S. *et al.*, "Cyber-Informed Engineering case study of an integrated hydrogen generation plant," in *ANS 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT)*, Online Virtual Meeting, 2021: American Nuclear Society.

[5] Eggers, S. and R. Anderson, "Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control," in *Nuclear Reactors*, Chad Pope, Ed. London, UK: IntechOpen, 2022.

[6] DoT, "Systems engineering guidebook for Intelligent Transportation Systems, Version 3.0," U.S. Department of Transportation, 2009.