INL/MIS-23-71129-Revision-0

Engineering-In Cybersecurity

March 2023

Virginia L Wright, Marc Sachs

Changing the World's Energy Future

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

INL/MIS-23-71129-Revision-0

Engineering-In Cybersecurity

Virginia L Wright, Marc Sachs

March 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

Engineering-In Cybersecurity

Cyber-Informed Engineering is a framework which allows engineers to build resiliency to the impacts of cyber attack into engineered systems starting in the early design phases. This article introduces the framework and provides a description of some of its principles and resources for learning more.

On February 1, 2023, leaders of the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) released an article, "Stop Passing the Buck on Cybersecurity"[i], describing the United States dependency on technology vulnerable to adversary intrusions as "less a cyber problem than a broader technology and culture problem." They described that as technology has become prevalent in our lives, we have come to accept that it is also vulnerable and indefensible by design. Users of technology have assumed the burden of defending ourselves from the impacts of these flaws.

This is equally true for engineers. Digital technology in the systems we design makes them faster, more capable and less expensive to operate than their analog counterparts and digital tools aiding our systems design process allow us to render better designs faster and to support more complex systems than ever before. However, from ransomware to advanced adversaries, these technologies are vulnerable to digital failure and attack and in engineered systems, the consequences of such failures can be catastrophic. Though we work with our information technology counterparts to secure these systems, these protections often occur at the end of our system-design process leveraging bolt-on technology. The CISA article calls for a different approach, where problems are fixed at the earliest possible stage, in design, rather than in operations.

The Department of Energy's National Laboratories have developed just such an approach, tailored to the needs of the engineers building the nation's critical infrastructure systems. This emerging framework, called Cyber-Informed Engineering (CIE), allows engineers to understand the potential consequences of digital failure or exploitation in their projects, beginning in the concept stage, and develop engineering-driven mitigations which can either eliminate or lessen the impact of such consequences. Especially beginning in the design phases, engineers can leverage a far wider range of consequence mitigations than cybersecurity solutions provide, including manual, process, or procedural controls. Engineers are trained and experienced in identifying, tracking, and diminishing fundamental engineering risks and CIE allows cybersecurity to be treated in the same way.

CIE considers twelve fundamental principles for understanding and reducing risk stemming from digital failure or exploit. Two of these are described below, and the remainder can be found in the National Strategy for Cyber-Informed Engineering[ii].

DESIGN AND OPERATIONS	ORGANIZATIONAL
Consequence-focused design	Interdependency evaluation
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Design simplification	Planned resilience
Resilient layered defenses	Engineering information control
Active defense	Cybersecurity culture

Figure 1 - Cyber-Informed Engineering Principles

Consequence-focused design allows the engineering team to focus, first, on identifying the functions performed by the system or process where the consequences of failure or malfunction are most catastrophic. For those critical functions, the team considers where digital technology might allow an unprotected action to initiate a high-consequence event. These could include unauthorized system actions, invalid data which would drive an automated action, or interdiction of a digitally-governed control. The team then considers design changes which could either remove the possibility for the unprotected action or mitigate the consequences. These changes, if enacted would act in addition to traditional cybersecurity protections to reduce the possibility or impact of undesired digital events to result in catastrophic consequences.

The **Engineered Controls** principle leverages ideas from the traditional safety Hierarchy of Controls[iii] (right) to help a team consider the potential security "value" of mitigative solutions. In cybersecurity, as in safety, *Elimination* of the possibility that an undesired digital event could happen, either by removing the digital dependency or the functions which enable the event is the most effective mitigation but is rarely possible. *Substitution* of the dependency or function with a capability which has less potential to allow the undesired event is a more likely possibility than outright elimination, but may introduce new consequences or dependencies which must be examined. An *engineered control*, such as a manual override, may be put in place to prevent the digital event from driving the consequence however, the team must ensure that the control does not also depend upon a digital mechanism. An *administrative* solution, such as a policy or procedure may provide guidance to prevent or enable quick recovery from the undesired event, and such solutions are usually low-cost, but are also less effective than other options discussed. Finally, some sort of *protective* mechanism (referred to as Personal Protective Equipment in our controls hierarchy) would provide protection from the consequences of the event without mitigating or preventing them. In CIE, we seek to eliminate, substitute, or build engineered controls where we can.

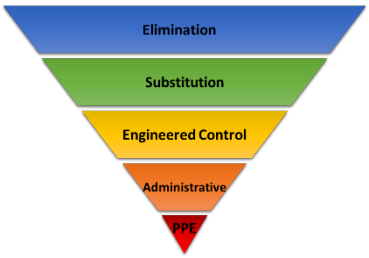

Figure 2 - Hierarchy of Controls

CIE's 12 principles were drawn from decades of system assessment and evaluation by the Idaho National Laboratory and incorporate lessons learned across a range of infrastructure sectors and system complexities. These principles allow an engineering team to design engineered systems which are resilient to cyber-attack well before they procure and implement the technologies which enable them. The mitigation strategies built into the design not only compliment operational cybersecurity solutions,

which should still be applied to selected technologies, but due to the understanding of critical functions and high-impact consequences, can inform the selection and design of operational cybersecurity to provide protections in the most important areas of the systems. They build a culture of cybersecurity on engineering projects with roles and responsibilities not just for the IT members of the team, but for everyone who participates in the design, build, operation and maintenance of the engineered system, including both those who are directly employed and those who provide contracted services. It elevates the discussion of cybersecurity risk so that it can be quantified and mitigated similarly to other engineering risks.

The National Strategy for Cyber-Informed Engineering was developed by a team of advisors assembled by the Department of Energy at the direction of Congress. Experts from energy sector asset owners and operators, vendors/manufacturers, standards organizations, research and academic institutions, National Laboratories, and government agencies developed a strategy which, across five pillars of action, contains strategic recommendations for building awareness of CIE, incorporating CIE into formal education, training and credentialing, building the body of knowledge by which CIE is implemented, applying CIE to current systemically important infrastructure and applying CIE in federally funded research which will build future energy infrastructure and technology.

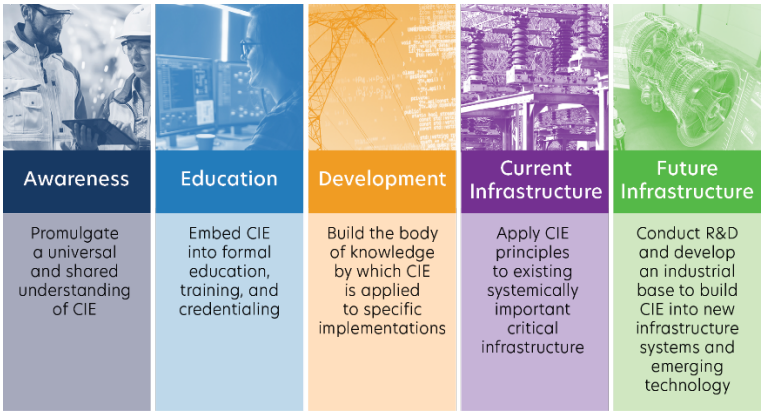

Figure 3 - National Cyber-Informed Engineering Strategic Pillars

Implementation of the National CIE Strategy is underway. Multiple universities, including Auburn University, the University of Texas at San Antonio, Boise State University and Idaho State University are building CIE into engineering curricula and degree programs to ensure that future engineers and technicians can employ these principles. The National Laboratories, including Idaho National Laboratory and the National Renewable Energy Laboratory are collaborating to create the body of knowledge and tools for applying CIE. A Community of Practice has been established to allow CIE practitioners to share success stories and to learn from others.

Though developed initially for energy applications, Cyber-Informed Engineering is a model which can apply to any sector practicing engineering design. CIE principles have been deployed in advanced nuclear reactor technology design, to eliminate potential sources of digital frailty from the design. Additionally, consulting firms in the water sector are using CIE to design-in security for water processing and distribution systems. If you are interested in knowing more about CIE or joining the Community of Practice, please contact the CIE team at CIE@inl.gov.

[i] Goldstein and Easterly. “Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products.” Foreign Affairs, February 1, 2023. https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity.

[ii] Caddy, et al. “National Strategy for Cyber-Informed Engineering.” DEPARTMENT of ENERGY. June 20, 2022. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

[iii] National Institute for Occupational Safety and Health. “Hierarchy of Controls”. CDC. (n.d.), https://www.cdc.gov/niosh/topics/hierarchy/default.html