Use of Cyber-Informed Engineering for digital risk mitigation

Wm. Arthur Conklin, University of Houston, Texas,
waconklin@uh.edu

CIE Curriculum Guide

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

https://www.osti.gov/servlets/purl/3006953

Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
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?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn "what ifs" into "even ifs"?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

Appendix A: Learning Objective Examples

Appendix A of the Curriculum guide provides sample learning objectives that focus on the CIE principles using the key questions.

Additional Resources can be found in the **CIE Implementation Guide**

The CIE Implementation Guide describes the principles of CIE and outlines questions that engineering teams should consider during each phase of a system's lifecycle to effectively employ these principles.

https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

CIE – Engineered Controls Database

Cyber-Informed Engineering (CIE) addresses the reality that cyber attacks on engineered systems can have consequences far beyond data loss or disruption of digital networks. When control systems are compromised, safety, reliability, and performance of the physical process itself may be threatened.

https://github.com/idaholab/CIE_EC_Database

Definition of Engineered Controls

Engineered controls are design features embedded in engineered systems that remove avenues of cyber attack or limit the consequences of such attacks. They function as resilient-by-design mechanisms, ensuring that even if digital protections fail, the system remains safe, reliable, and capable of recovery.

These controls are fundamentally different from information security tools such as firewalls, intrusion detection systems, encryption, or patching. Those tools protect data, access, and networks. Engineered controls, by contrast, protect the engineered process itself. They represent the point where engineering practice intersects with cyber resilience, and they are evaluated not for confidentiality, integrity, or availability of information, but for their ability to safeguard safety, reliability, and performance.

The use of Engineered Controls expands the toolbox of cybersecurity professionals. These non-digital methods are used to protect the engineered process itself. While traditional cybersecurity controls protect data, access, and networks, the restriction of the effect to the CIA triad does not support protecting the SRP triad which is critical in the engineered system.

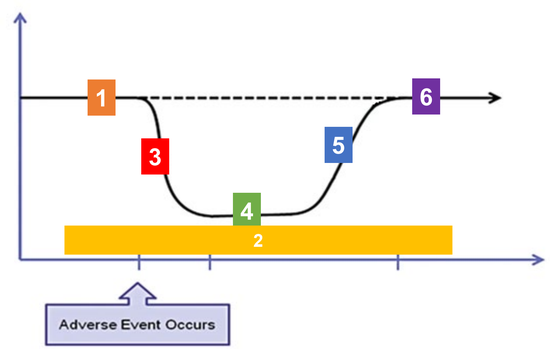
Engineered controls are design features embedded in engineered systems that remove avenues of cyber attack or limit the consequences of such attacks. They function as resilient-by-design mechanisms, ensuring that even if digital protections fail, the system remains safe, reliable, and capable of recovery.

Categories of Engineered Controls

1. Physical Logic Mechanisms
2. Redundant Designs
3. Physical Constraint and Material Properties
4. Digital Engineered Controls
5. Passive Physical Dynamics
6. One-way Enforcement and Irreversible Actions
7. Fail-Safe Defaults

Relationship of Engineered Controls to System Resilience

Six Families to Characterize the Application of Engineering Controls



1. **Restrict (Prevention) –** Remove the avenue for attack | incident
2. **Recognize (Indication) –** Monitor for an incident occurrence / detection for changes in performance.
3. **Resist (Resistance) –** Methods to resist or limit the incident's ability to degrade performance.
4. **Redirect (Respond) –** Taking corrective actions to redirect performance towards acceptable/optimal levels or preventing further degradation and impacts
5. **Restore (Recover) –** Focusing on reducing recovery time to return to acceptable/optimal performance. Inverse of Resist for its characteristics.
6. **Reconfigure (Adapt) –** Ensure that systems learn from the adverse event and adjust its approach to harden and reduce future impact from similar events.

Cyber-Informed Engineering

CIE Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and performed by Idaho National Laboratory and the National Laboratory of the Rockies.