CIE and CCE: Changing the Engineering Mindset for a More Secure Future

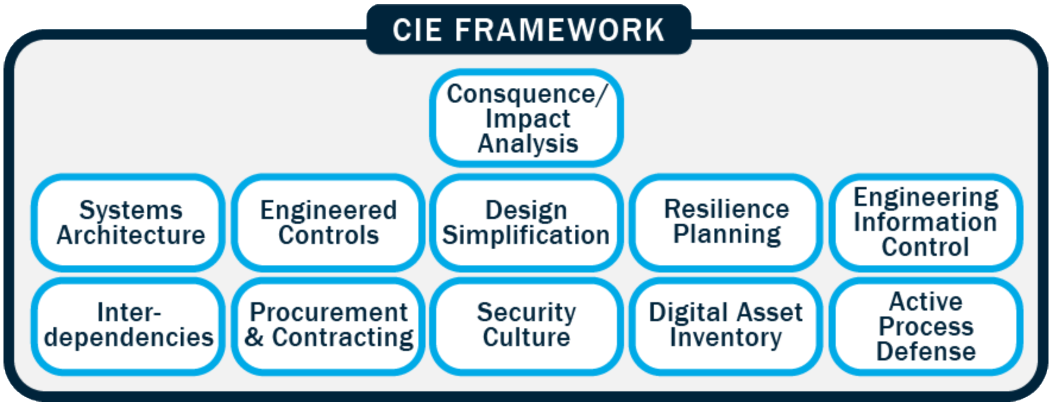
Systems innovation and technological integration have expanded control systems' connections to corporate networks, integrators, vendors, and the internet for speed of monitoring and the convenience of remote maintenance. Adversaries have taken notice—and advantage. The ever-increasing rate and severity of cybersecurity events effecting control systems demonstrates an imperative need for a change in philosophy and engineering practices; to proactively secure existing digital infrastructure and build new systems bolstered against a modern and future cyber-adversary.

Idaho National Laboratory (INL), in partnership with the Department of Energy (DOE), has developed a framework to shape cybersecurity efforts in engineering and a rigorous process of application. The **Cyber-Informed Engineering (CIE)** framework and body of knowledge drives the inclusion of cyber security as a foundational element of risk management for engineering of functions aided by digital technology.[i] **Consequence-driven Cyber-informed Engineering (CCE)** is a rigorous process for applying CIE's core principles to a specific organization, facility, or mission by identifying their most critical functions, methods and means an adversary would likely use to manipulate or compromise them, and determining the most effective means of removing or mitigating those risks.[ii]

CIE

By including cybersecurity as a core element of engineering risk management, CIE ensures that inherent risks of digital technology (which manifest through failure, malign disruption, or compromise) are considered and mitigated in the earliest possible stages of the design lifecycle.[iii] CIE is applied within each lifecycle step for engineered systems, from early concept to implementation. CIE facilitates a mindset and culture for designing engineered systems through which all parties involved in critical functions (particularly engineering personnel) consider how cyber risk could be mitigated through purposeful design. Adversarial considerations and the engineering process combine to improve existing functions or build a system that has drastically reduced possibility of critical failure or compromise via cyber means. CIE emphasizes "engineering out" potential risk in key areas, as well as ensuring resiliency and response maturity within the design of the engineered system.

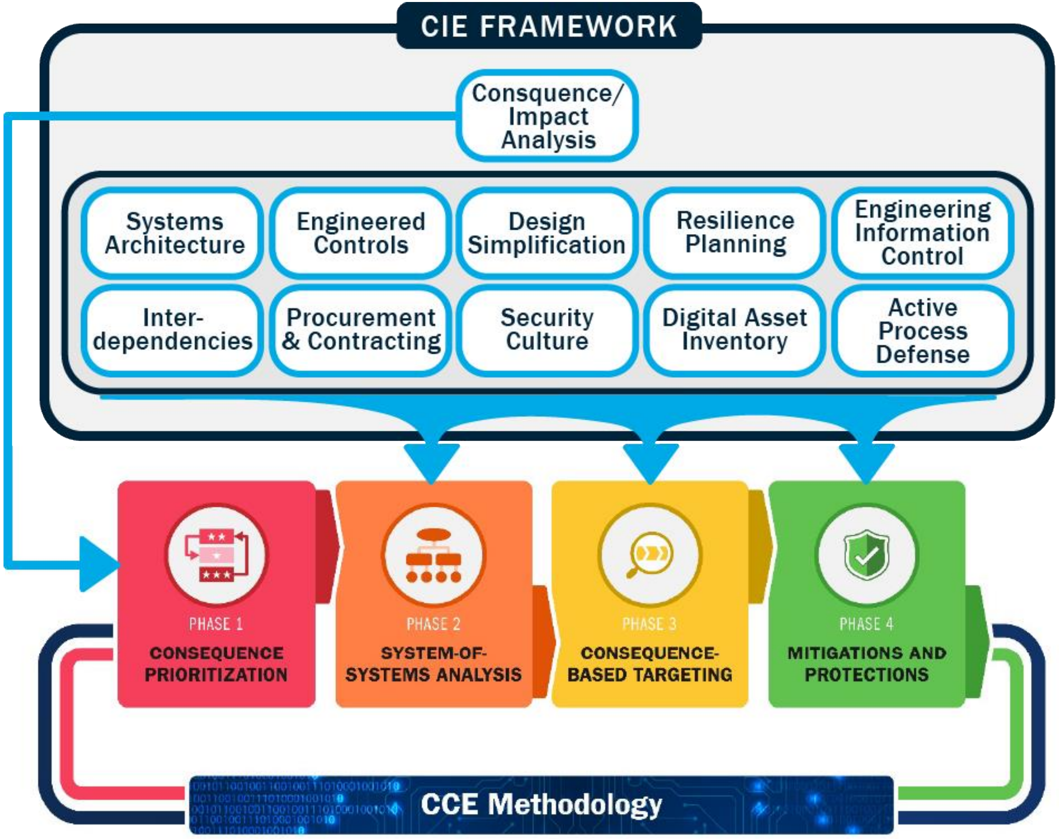
CIE is arranged into 11 areas of focus:



CCE

CCE puts CIE's cybersecurity in engineering concepts into practice at an organization by considering their most critical functions from an adversarial perspective.[iv] CCE begins with an assumption that a sophisticated and determined adversary *will* compromise an organization, but that it *is* possible to determine which functions could cause critical impact if manipulated and plan high-impact defensive measures against an adversary's interference.

INL walks an organization through core components of CIE in CCE's 4-phase process to evaluate and remove or mitigate weaknesses in their critical functions:[v]



To organizations deemed critical to US national security, INL and DOE offer training, valuable expertise, and support throughout the rigorous process of a CCE engagement. Any critical infrastructure organization may request and apply a self-driven version of the process known as Accelerate. A 16-hour preparatory training and workshop is available to support Accelerate initiatives.[vi]

CIE and CCE Roadmaps

DOE has experienced CCE successes with multiple organizations thus far in both the private and public sectors, ranging from electric, nuclear, natural gas, military, and more.[vii] Other organizations are currently in process of receiving Accelerate training, undergoing a CCE engagement, or are committed to participating in one or the other in the future. Thanks to congressional support, CCE is also in the process of being introduced at university engineering programs to create a generation of cyber-aware engineers.

CIE is an emerging paradigm to guide engineering design for cybersecurity in critical infrastructure applications. It was incorporated into the Wind Energy Technology Office Roadmap for Wind Cybersecurity as a design recommendation for reducing cyber risk in the Wind industry[viii]. In addition, a national strategy is under development to foster Cyber-Informed Engineering principles into engineering education and into practice across projects from research to industry.[ix] As the national strategy results in information sharing and a Center of Excellence for Cyber Informed Engineering, the application of these principles will be realized across infrastructure sectors.

[i] *Engineering Out the Cyber-Risk to Protect What Matters Most.* Andrew Bochman, Virginia Wright. RSA. YouTube, May 16, 2019. https://www.youtube.com/watch?v=R5o-t33nWoA.

[ii] “Consequence-Driven Cyber-Informed Engineering (CCE).” Idaho National Laboratory. April 21, 2021. https://inl.gov/cce/.

[iii] *Cyber-Informed Engineering Defined.* Robert Anderson, Julio Rodriguez, Chris Spirito, Virginia Wright. 2017. International Atomic Energy Agency (IAEA): IAEA.

[iv] “Consequence-Driven Cyber-Informed Engineering.” INL.gov. Idaho National Laboratory. Accessed April 29, 2021. https://factsheets.inl.gov/FactSheets/Consequence-driven%20Cyber-informed%20Engineering.pdf.

[v] “Consequence-Driven Cyber-Informed Engineering (CCE).” Idaho National Laboratory. April 21, 2021. https://inl.gov/cce/.

[vi] “TIER 1 VS. TIER 2 ENGAGEMENTS AND TRAINING.” INL.gov. Idaho National Laboratory. Accessed April 29, 2021. https://inl.gov/wp-content/uploads/2021/01/CCE_FactSheets_Tier1vsTier2_1.18.21.pdf.

[vii] *CCE-Consequence-Driven Cyber-Informed Engineering.* Idaho National Lab. YouTube, 2020. https://www.youtube.com/watch?v=rxGJJ_iT_N4&amp;t=285s.

[viii] “Roadmap for Wind Cybersecurity.” DOE.gov. Department of Energy, Wind Energy Technology Office. Accessed May 5, 2021. https://www.energy.gov/sites/prod/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf

[ix] “National Defense Authorization Act for Fiscal Year 2020”, Section 5726, 116th Congress, Congress.gov December 9, 2019, https://www.congress.gov/116/crpt/hrpt333/CRPT-116hrpt333.pdf,