CYBERCORE integration center

Providing assistance after a compromise is imperative to developing and sharing actionable information, but preventing a high-consequence attack is an even greater opportunity.

Consequence-driven Cyber-informed Engineering

Consequence-driven Cyber-informed Engineering (CCE) is a new methodology focused on securing the nation's critical infrastructure systems. Developed at Idaho National Laboratory, CCE starts with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted network can and will be penetrated. This think like the adversary approach provides critical infrastructure owners, operators, vendors and manufacturers with a disciplined methodology to:

- Evaluate complex systems.
- Determine what must be fully safeguarded.
- Apply proven engineering strategies to isolate and protect an industry's most critical assets.

CCE Concepts

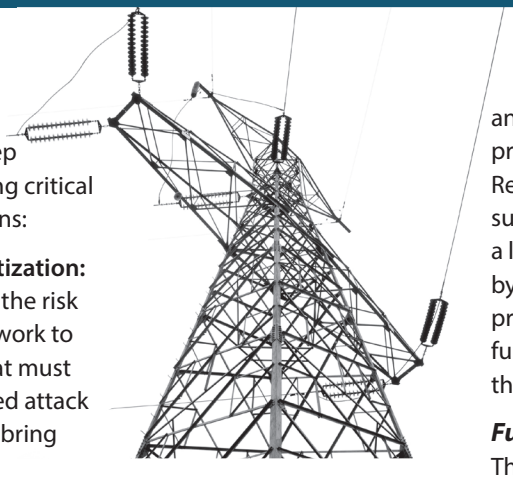
Consequence-driven – INL leads executives and operational experts through a series of exercises to identify the most critical functions essential to fulfilling their organization's mission and determine the potential consequences of a cyberattack against these functions.

Cyber-informed – Using the CCE methodology, INL guides system operators to identify key points within a critical system vulnerable to a cyberattack.

Engineering – INL then fully leverages an organization's operational expertise, system understanding and process knowledge to engineer out cybersecurity risks.

Changing the World's Energy Future

INL Idaho National Laboratory



Methodology Steps

CCE provides a four-step process for safeguarding critical infrastructure operations:

1. **Consequence Prioritization:** Sets a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.
2. **System of Systems Analysis:** Gathers information and identifies the systematic interdependencies between critical processes, defense systems, and enabling or dependent components.
3. **Consequence-Based Targeting:** Determines the adversary's path to achieve the highest impact effects, where they need to be to conduct the attack and what information is required to achieve those goals.
4. **Mitigations and Protections:** Removes or disrupts the digital attack paths as fully as possible.

Securing Operational Technology

As organizations integrate new technology solutions into their operational processes, their risk exposure also increases. Consequence-driven Cyber-informed Engineering moves beyond the traditional focus areas of security by looking at an organization's entire operation, securing the most essential operations and processes while simultaneously securing the technology. These frameworks expand on traditional assessments so that vulnerabilities are assessed not only in the context of a specific technology, but also how an exploited vulnerability may impact the operations and processes of the entire organization.

Highlighted Successes

Working and collaborating across critical infrastructure sectors to identify the highest consequence operational systems provides a practical strategy for industry and government to invest and prioritize risks to critical functions. Recently, INL completed a successful CCE pilot project with a large utility. As acknowledged by the utility's own engineers, the process shifted their perspectives, fundamentally changing how they approach risk decisions.

Future Expansion

Threats to national critical functions come from many sources, and the job of defending these vital infrastructures, including the electric power grid, natural gas pipelines, chemical plants and many more, is a challenging task for any single organization. That's why INL is working alongside the Departments of Energy, Defense, and Homeland Security to form strategic partnerships with industry and academia to expand and evolve the CCE methodology. Expert training programs are currently being developed that will help us better secure the most critical infrastructures in the United States and around the world.

CCE combines cyber risk assessments and engineering principles to safeguard critical infrastructure operations.

For more information

Cybercore Director

Scott Cramer
208-526-2757
scott.cramer@inl.gov

Deputy Director for Programs

Rob Helton
208-526-6266
robert.helton@inl.gov

CCE Program Manager

Rob Smith
208-526-3881
robert.smith@inl.gov

CCE Technical Advisor

Curtis St. Michel
208-526-7064
curtis.stmichel@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory