Consequence-driven
Cyber-informed
Engineering

TIER 1 ENGAGEMENT EXPECTATIONS

CCE is a structured method that outlines an attacker's approach to cyber-enabled sabotage and delivers specific engineering solutions—not just cyber controls—to design-out cyber risk from critical operations.

WHAT A CCE EFFORT DELIVERS:

NATIONAL SECURITY IMPACTS

Idaho National Laboratory (INL) conducts Tier 1 CCE engagements with companies or organizations that deliver functions or services deemed highly critical to national security—making them prime targets for cyber sabotage. INL is working with the U.S. Departments of Energy, Homeland Security, and Defense to conduct CCE engagements with potential high-value targets, delivering mitigations that support national security.

Not a Traditional Cybersecurity Assessment

CCE is not a cybersecurity audit, penetration test, or technology vulnerability assessment. It shifts cyber risk assessment from individual technologies to entire operations and processes.

Structured Evaluation to Deliver Specific Mitigations

CCE is a structured process to identify how cyber-enabled sabotage could result in events that threaten national security and business viability, then identify the engineering changes or operational controls that eliminate or significantly block those events.

Guided by INL, Performed by You

A CCE engagement is an intensive, iterative, guided analysis effort. The effort is co-led by an INL team of CCE experts and a company-designated team of engineering, operations, process, and cyber experts.

An Aggressor Approach that Assumes Compromise

CCE results in engineering changes and process controls—not just cyber solutions—to limit the damage an attacker can do once inside. Traditional cybersecurity approaches correctly focus on building strong, layered perimeter defenses to keep attackers out. For national security functions, CCE takes defense a step further—assuming that an advanced, targeted attack campaign can find a way in.

Consequence-driven
Cyber-informed
Engineering

TIER 1 ENGAGEMENT EXPECTATIONS

CCE TEAM EXPECTATIONS

The organization should dedicate a core team of knowledgeable personnel, with a heavy focus on engineering, operations, process, and cyber experts. The organization's team, with the support of INL, will deeply examine the people, processes, and technologies that deliver the organization's most critical functions.

- This requires the right mix of personnel and disciplines, drawn from multiple business units.
- Despite the cyber focus, a CCE Tier 1 engagement cannot be conducted with cybersecurity or IT/OT staff alone.

Past CCE teams have included the organizations:

- System engineers • Operations managers • Primary system process SMEs
- Cyber and information security experts • Business unit managers • Risk managers
- As needed representatives from: procurement, contracting, finance, system maintenance, network architecture, calibration, prognostics/diagnostics, etc.

An INL-led team of targeters, control system cybersecurity analysts, process and technology SMEs, and facilitators will provide guidance, support, analysis, and expertise throughout the engagement.

ESTIMATED TIME AND RESOURCE COMMITMENT

C-suite buy-in and commitment of management staff is critical to success

Resource requirement:
Motivated team of 6-12 engineering, operations, cyber and process staff, totaling ~1-2 full-time equivalent (FTE) personnel

9- to 12-month engagement

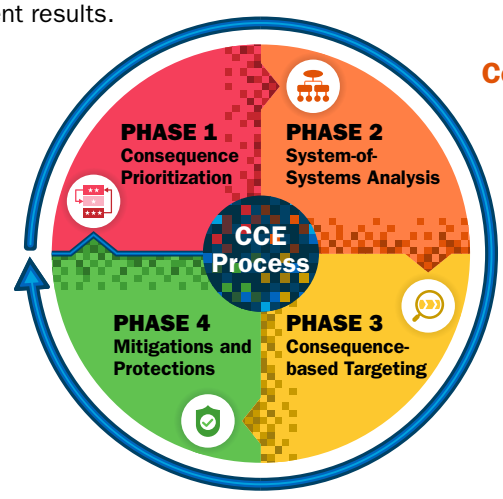
- 8-12 video teleconferences, 1-2 hours each
- ~4-6 onsite meetings, 2-3 days each (alternate video teleconference option when onsite meetings are not possible)

CCE PROCESS STEPS

INL's Execution Team will lead your organization through a structured four-phase evaluation process. The Execution Team will meet with the organization's motivated CCE team throughout each phase, using brief video-teleconferences and more intensive multi-day work sessions conducted at your facility (when possible). The organization will have access to a custom-built CCE Tool Belt to support analysis and securely organize and document results.

Determine critical areas of focus:
Define High Consequence Events (HCEs) that use cyber means to achieve catastrophic disruptions to critical functions

Design-out the cyber-risk:
Identify engineering/operation controls to remove or mitigate risk and threat tripwires to identify adversary activity



Conduct a detailed system breakdown:
Thoroughly examine and collect data on the operations of cyber-physical systems that deliver critical functions

Map Requirements for Cyber Sabotage:
Identify the information, access, and actions required to cause identified HCEs

Idaho National Laboratory INL