CRITICAL FUNCTION ASSURANCE (CFA)

OPTIMIZING SECURITY ACTIVITIES TO ASSURE CRITICAL FUNCTIONS

Critical Function Assurance (CFA) is a foundational approach to identifying, prioritizing, and mitigating the risk that is inherent in the delivery of critical functions that depend on digital technology. It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. This focus enables effective application of scarce security resources to the most vital areas of a business, mission or organization and provides the foundation for optimizing greater security strategy and policy efforts.

- Modern life – enabled by a complex and interdependent web of critical functions
- Functions made available 24/7 through outsourcing and automation using unique and intentional deployments of microprocessors, software, and firmware
- Cyber-enabled sabotage events that target the technology we depend on to deliver critical functions disrupts traditional risk management - determining the probability of such events becomes nearly impossible, and at best highly speculative.

To truly determine which events have the highest impact on a critical function teams must first understand critical function delivery. CFA provides the analytic basis and focus to answer questions such as:

- What in our business is most important to protect from cyber-enabled sabotage?
- Where should we focus our general security efforts and resources?
- Where should we engage in cyber-informed engineering efforts of devices or engineered solutions?
- Where should we pen test, and what are we looking for?
- Where should we conduct tailored monitoring and detection activities?

CFA is about protecting the reason an operation or organization exists, and it is foundational for meaningful ICS security and policy improvement and adaptability.

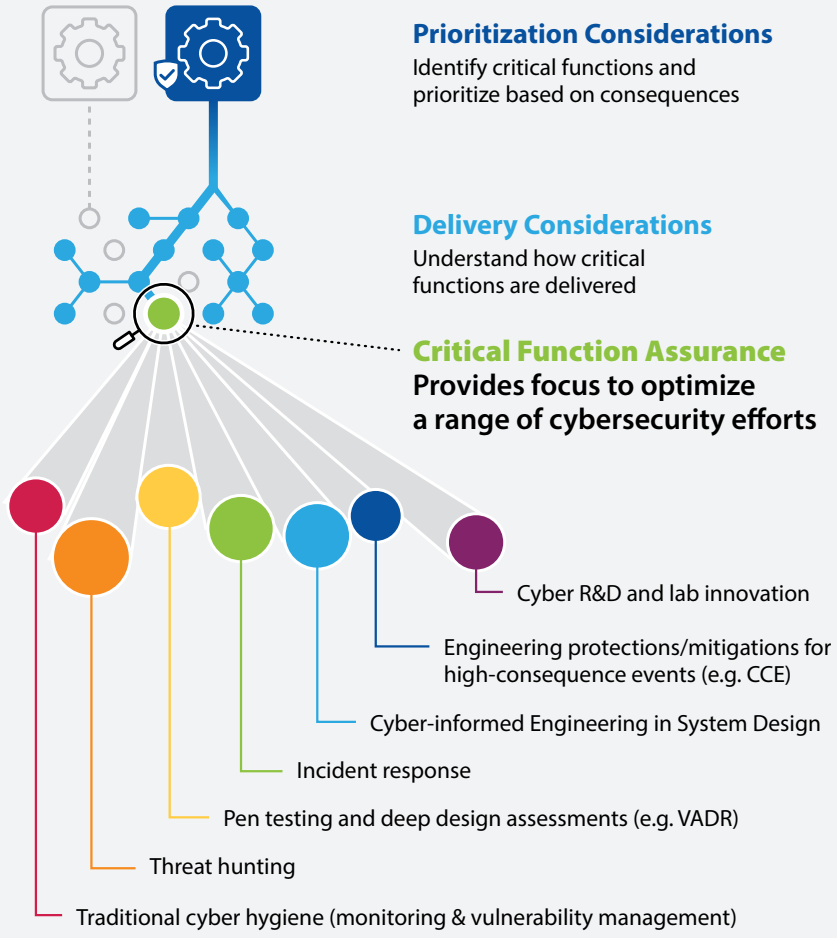


Figure. CFA-Focus and Optimatization of Security Efforts

Understanding the Relationship Between CFA, CIE and CCE

For over 20 years, Idaho National Laboratory has focused on Critical Function Assurance (CFA) and specifically the role that industrial control systems and operational technology play in assuring critical functions and missions in the digital age. INL championed the concept of Cyber-informed Engineering (CIE) and created a robust and repeatable methodology to apply CIE principles, prioritized based on functional impact and operational understanding through Consequence-driven Cyber-informed Engineering (CCE).

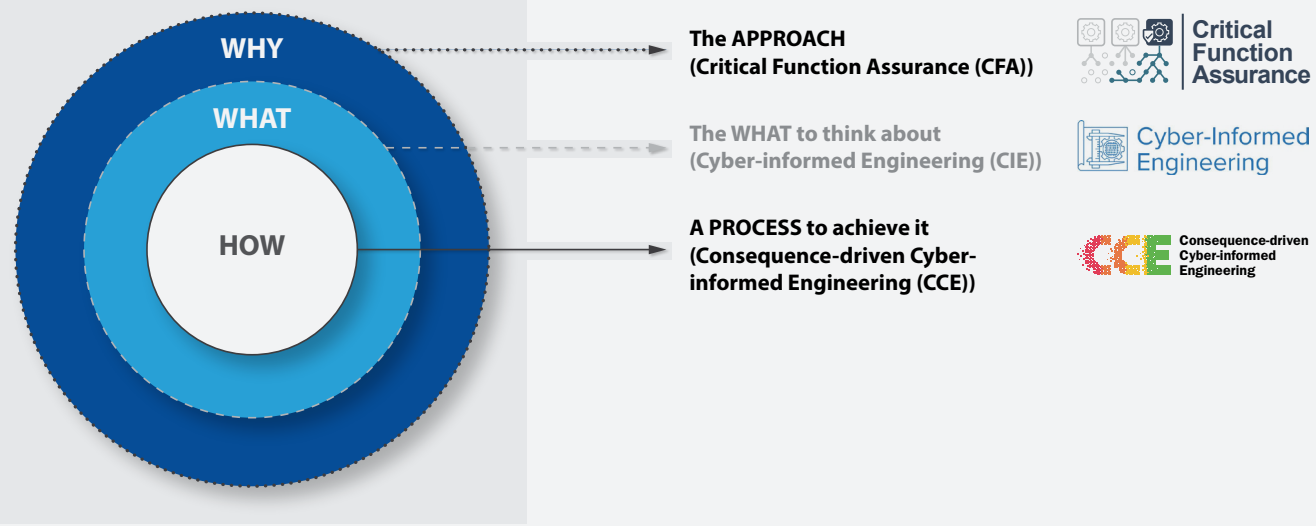
Critical Function Assurance is an approach to prioritize and address risk based on impact. It is rooted in a holistic understanding of how critical functions are delivered. It provides rapid focus to what matters most and illuminates elements and areas of risk that are often overlooked. This focus enables effective application of available security resources to the most vital areas of a business/mission/entity and provides the foundation for optimizing security strategy and policy efforts.

Cyber-informed Engineering (CIE) is a series of principles focused on integrating cybersecurity considerations into the conception, design, development and operation of any physical system that has digital connectivity, monitoring or control related to the delivery of a critical function.

Consequence-driven Cyber-informed Engineering (CCE) is the repeatable process/methodology to merge the essence of CFA, by prioritizing and addressing risk based on impact and functional delivery knowledge (the Consequence-driven piece), with the application of CIE principles (the Cyber-informed Engineering piece). It provides a holistic process to achieve the desired result of assuring what matters most in a structured, time-proven and repeatable way.

In essence, the relationship can be simplified by thinking of CFA as the 'WHY,' or the objective, and CIE as 'WHAT' principles to think about in achieving the objective. CCE can be thought of as a repeatable process to apply elements of CFA and CIE to achieve assurance of critical functions.

FOR MORE INFORMATION, VISIT OR CONTACT:
https://inl.gov/cce/ • cce@inl.gov
https://inl.gov/cie/ • cie@inl.gov



Idaho National Laboratory

23-50859_R1