Contribution ID: **216** Type: **Interactive Content Presentation**

Consequence-driven Cyber-Informed Engineering

Cyber Informed Engineering (CIE) was defined in IAEA CN-244-520 as the inclusion of the cyber-attack and defense perspective (cyber security aspects) into the engineering process. It is the process by which engineering personnel are made aware of how their current actions impact the processes by which they architect and design systems. Decisions do not always take into consideration the attack tactics, techniques and procedures currently in use by capable cyber-adversaries. Consequence analysis and associated engineering mitigations are some of the most important elements within the CIE framework. Ensuring the most critical functions are available to perform as designed, when called upon, is vital. Idaho National Laboratory (INL) has created an operational process for performing cyber-informed consequence analysis and engineering mitigations. Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the highest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments. The CCE process helps nuclear asset owners to: identify high-impact / high-consequence events that could result in interruption of critical functions, analyze the infrastructure which could be subverted to enable those events, and develop specific mitigations to avoid, or engineer out, these consequences. An operational approach to CCE is provided.

Gender

Male

State

United States

Authors: ANDERSON, Robert (Idaho National Laboratory); SMITH, Robert (Idaho National Laboratory)

Presenter: ANDERSON, Robert (Idaho National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security