INL/MIS-23-75451-Revision-0

Securing the Clean Energy Transition with Cyber-Informed Engineering

February 2024

Samuel Douglas Chanoski, Emma Mary Stewart, Virginia L Wright

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-75451-Revision-0

Securing the Clean Energy Transition with Cyber-Informed Engineering

Samuel Douglas Chanoski, Emma Mary Stewart, Virginia L Wright

February 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Securing the Clean Energy Transition with Cyber-Informed Engineering
Emma Stewart, Virginia Wright and Sam Chanoski, INL

The Bipartisan Infrastructure Law kick-started a surge in clean energy investments in the United States. Amid the clean energy transition and the novel systems it introduces, such as renewable generation and controllable loads, we must recognize that the foundation of our electric grid's reliability and efficiency lies in the protection and coordination of these systems through increasingly automated connected devices.

These devices must now adapt to more and more variable inputs previously unconsidered, as the fundamental behaviors of the grid grow more complex with the evolving resource mix. The automation and data exchange required to enable advanced control schemes and adaptive protection increases the attack surface by which protection systems could be affected by digital sabotage. Securing these devices and their supporting infrastructure from the outset is imperative, starting from the conceptual design and continuing through the entire engineering lifecycle.

The Department of Energy[1] developed the Cyber-Informed Engineering (CIE) methodology to support incorporation of cyber defenses as a part of the engineering development processes. This approach focuses engineers on the identification of the most critical consequences which could be realized via cyber attack and helps them develop, where possible, engineering-based controls to either deny avenues of attack or mitigate the consequences of exploitation. Traditional cybersecurity techniques are also leveraged, but with defenses aligned to and prioritized for the most catastrophic impacts of attack.

CIE is an ideal approach to seamlessly integrate the necessary advanced control capabilities and adaptive protection systems, especially considering the trend towards cloud-based infrastructure and process controls. As automation assumes a critical role, we must integrate human-in-the-loop design processes with consequence-based approaches for these critical technologies. By focusing on both the initial design and the lifecycle aspects, we can optimize for functionality and cost while simultaneously incorporating intelligent cybersecure decisions along the way. For instance, ensuring the security of the data feed used for automatic actions may require integrating measurements from less secure or non-compliant locations, such as renewable resource forecasting, into a comprehensive security framework. Identifying these interlinked components and securing them appropriately would be a key contribution of CIE incorporated into an existing design and implementation process.

The Department of Energy published an implementation guide[2] in July, 2023, full of considerations for applying CIE at every stage of the systems engineering lifecycle. This guide contains critical questions for the design team to consider as well as a case study showing how the approach could be applied to a real-world situation. DOE is working with universities and standards bodies to incorporate this methodology into the education and guidance for engineering critical infrastructure. To learn more about CIE, visit https://inl.gov/cie/ or email us at CIE@inl.gov.

[1] https://www.energy.gov/ceser/articles/cyber-informed-engineering-bridge-between-cyber-and-critical-infrastructure-securing

[2] https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf