INL/MIS-23-71831-Revision-0

A National Secure-by-Design Strategy

April 2023

Virginia L Wright, Andrew A Bochman, Andrew Ohrt

Changing the World's Energy Future

Idaho National Laboratory

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

INL/MIS-23-71831-Revision-0

A National Secure-by-Design Strategy

Virginia L Wright, Andrew A Bochman, Andrew Ohrt

April 2023

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

"A National Secure-by-Design Strategy"

by

Virginia Wright, INL
Andrew Ohrt, West Yost
Andy Bochman, INL

The U.S. National Cybersecurity Strategy published March 2, 2023, signals that Washington is calling for major changes in how the country prioritizes the security of software systems used in critical infrastructure. It acknowledges that the de facto approach, until now essentially "let the buyer beware," leaves entities who are least able to assess or defend vulnerable software responsible for the impacts of designed-in weaknesses while the makers of the technology bear no liability. The strategy recommends a security-by-design approach that includes holding software vendors liable for upholding a "duty of care" to consumers and for systems to be designed to "fail safely and recover quickly." For energy infrastructure, the strategy calls out the need to implement the National Cyber-Informed Engineering Strategy[1] to achieve markedly more effective cyber security protections.

The engineers who construct our complex infrastructure systems leverage strict standards and procedures to ensure high levels of safety and reliability. However, most of these procedures were developed well before the advent of modern cybersecurity and do not yet guide engineers to consider cyber threats, let alone to design-in cyber security defenses. Through Cyber-Informed Engineering, the Department of Energy and its National Laboratories seek to educate engineers to remove avenues for and mitigate impacts of cyber-attack on the systems they design. Early in the design lifecycle, engineers can identify the critical functions of the system they are creating and engineer the system to limit the impacts of digital disruption or misuse. Combined with a robust IT security strategy, cyber-informed engineering offers the opportunity to achieve robust protections not available through cybersecurity alone.

The Idaho National Laboratory pioneered the development of Cyber-Informed Engineering concepts and is working with DOE to educate others in industry, academia, and government on how to apply these concepts to real-world challenges. In this article, we'll outline some of the basic principles of Cyber-Informed Engineering and offer examples, using a water sector scenario, of how they're being put into successful practice.

Consequence-Focused Design

[1] https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document

The most important task in any organization is assuring that its most critical functions are never disrupted. Engineers are trained to design resilient systems, using specific techniques for identifying traditional failure modes and preventing them. However, an intelligently directed cyber-attack doesn't work like a traditional system failure. It may even mirror normal system operations, while triggering actions that are out of the normal sequence or occur to a greater or lesser degree than normal. Adversaries often take advantage of the innate functionality of a system to cause undesirable operations, such as overflowing a tank, or repeatedly turning power on or off to damage critical assets and disrupt operations.

In the practice of Cyber-Informed Engineering, the first step engineers must take is identifying the functions and related subsystems with the potential to result in catastrophic consequences if misused by an intelligent adversary. Then, as described below, they can identify methods to prevent an attack, stop the negative consequences or limit their impact. Identifying areas of potential misuse with the most negative impact helps an engineering team prioritize and lead risk management approaches for these consequences through system design, development, and operations.

> *Imagine that a municipal water utility is considering a new cloud-based service to enable monitoring and control of a critical, remote pump station. The control capability includes the remote manual start and stop of drinking-water pumps. Cloud technology would make operations far more efficient and would save significant labor. As part of a cyber-informed design review, the asset owner was asked to imagine the worst consequences of an attack. The design team identified a scenario where an attacker could penetrate the cloud service and use it to remotely control pumps, possibly affecting the reliability of flow or the safety of the water supply. The asset owner deemed this to be too high a risk and so delayed acquisition of Cloud capabilities unless and until the team could establish a way to reduce this risk to near-zero.*

Engineered Controls

When high impact consequences of cyber-attack are identified in the design phase, engineers have the power to adjust physical system parameters in response. They can select technologies with features that present less risk if misused. They can change how processes function or adjust capacities, and tolerances to reduce the harm that negative consequences can cause. They can also introduce additional validations and controls to ensure expected results. Because these protections may incorporate physical barriers or other elements in an industrial process, they provide an additional barrier to cyber-attack when used with traditional cyber defense technologies. We can and should leverage cybersecurity tools for the protection and detection of threat conditions, but by incorporating design changes from engineers, we can build in protections that thwart avenues for and limit the consequences of attack.

> *Members of the municipal utility's design team reviewed the features of the water pumps available to an attacker through the cloud service. They identified that the worst*

consequence would result from an attacker remotely starting and stopping pumps too quickly. They determined that installing a $50 analog time-delay relay in the controller of the pump would prevent the cloud-based attacker from harming the system even if they were able to gain remote access. The utility elected to incorporate this protection and proceeded with procurement of the cost-saving cloud technology.

Active Defense

When an infrastructure system is attacked by an adversary, system operators and information technology specialists must work together to ensure continued operation of critical system functions and, at the same time, defend the system from said attack. Unless these actions are planned, documented, and practiced, this process can be at best inefficient or at worst, entirely ineffective. Using Cyber-Informed Engineering, engineers plan response approaches which allow continued, if possibly degraded system function even when critical systems or features are not present. They incorporate information technology specialists in the development of response strategies from design and development into operations. They regularly conduct exercises to practice the documented response procedures and measure their effectiveness. Rather than being passive in the event of a cyber-attack, engineers and operators become an active part of the response team.

Most municipal water utilities rely on an automated Supervisory Control and Data Acquisition (SCADA) system to control their operational functions. This system has programming that maximizes the efficiency and effectiveness of the water system and oversees system operations far better than any human could. When trained in core Cyber-Informed Engineering concepts, engineering and operations teams develop procedures to follow in the event of attacks on their SCADA systems and conduct regular exercises with their IT, engineering, and operations teams, simulating scenarios where automation is either unavailable or unreliable. Regular exercises allow the operations staff to develop requisite skills and demonstrate the ability to operate their water systems and maintain safe and reliable service to customers.

Owners of energy, water, and other critical infrastructure systems must be continuously ready to weather cyberattacks that breach their external electronic defenses. Adding engineering-led defensive measures, as described above, enhances their ability to withstand and prevent catastrophic consequences of cyber-attack. The National Strategy for Cyber-Informed Engineering, called out in the National Cybersecurity Strategy, provides the means to educate engineers, develop tools and apply these cyber defense methods to current and future infrastructures. By identifying catastrophic consequences before they occur, and eliminating the ability of cyber adversaries to achieve the negative outcomes they seek we can markedly improve cyber defense of the infrastructures that support and assure some of the nation’s most critical functions.