Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

Novel Techniques in Cyber and Risk Assessments

Nathanial Evans, PhD
Argonne National Laboratory

Amanda Joyce
Argonne National Laboratory

Abstract

The evolution of assessments away from maturity-based assessment towards comparative methodologies has been happening for the past few years as organizations begin to understand the benefits of comparative analysis. Applying a comparative methodology assessment to nuclear facilities presents many challenges but also creates many benefits as demonstrated in critical infrastructure as a whole. These benefits include improving the sector as a whole by identifying high, low and average performers thus allowing low performers the ability to see where their largest weakness is. In turn, when facilities are reassessed, high performers may no longer be high performers, thus having them work to better their posture. We identify this as "friendly competition". While no facilities are being explicitly called out, there is an internal want to be the higher performer versus the lower performer.

Overall comparability creates an easier conversation and graphic that can be used to highlight changes needed and can be understood by non-cyber speaking experts. This creates an easier buy in to allow for changes to occur and where there are limited options, a prioritization of which ones will have the largest impacts.

It appears comparability has not been fully explored for nuclear energy and security domains and is a viable approach to complement traditional maturity-based models.

Introduction

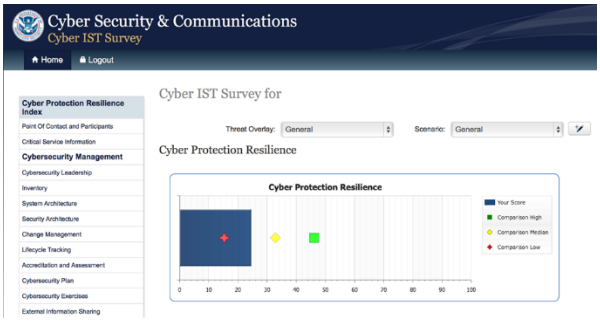
Today's critical infrastructure is highly interconnected. This interconnectedness allows owners and operators the ability to remotely operate, monitor, patch, and alter their infrastructure without being physically located near the system. This increase in accessibility adds security concerns to the infrastructure. Specifically, the power grid known for being the "largest interconnected machine" is a vastly large complex system that is critical to life and well-being in the United States. The power grid consists of millions of miles of transmission and distribution lines and thousands of power plants and substations.

Not only is the overall power grid connected internally, but also it is largely the most relied upon system among all critical infrastructure sectors. This interconnected nexus of energy and critical infrastructure lends to a large attack vector when an attacker sees the potential damage that can be caused by an attack on the power grid as shown in the Ukraine 2015 attack, which left over 200,000 customers without power for several hours. The complexity in which this smart system communicates could also lead to catastrophic consequences if a breach to the security of the system occurred.

While the Energy Sector is one of the most heavily regulated sectors within the 16 Critical Infrastructure Sectors, the release of the National Institute of Standards and Technology Cybersecurity Framework provides for improved voluntary guidelines that may not be included

in regulations. There is a need to begin evaluating the current cybersecurity posture of infrastructure utilized within the power grid to ensure properly implemented Energy Sector and Department of Energy safeguards and procedures.

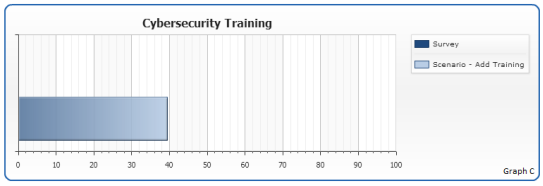
Argonne National Laboratory, leveraging prior experience on assessment methodology, looks to assist in developing an energy-focused cyber assessment utilizing the Energy Sector Cybersecurity Framework Implementation Guide that allows for both the Department of Energy and the owner/operator of the cyber system to review where they stand within the framework and the regulations provided.



Comparison based methodology

A comparison based methodology is based on multi-attribute decision analysis that takes a weighted linear aggregation of assessment data and compares them against similar peers. This approach as evidenced through the Department of Homeland Security Cyber and Infrastructure Security Agency Cyber Infrastructure Survey (DHS CISA CIS) has shown itself to be an effective way to encourage change across an industry. The CIS tool provides uses with a set of assessment questions setup with multiple tiers. The end result of the tool provides a graphical display of where the facility falls in comparison to others that have completed the survey. This display has been shown to provide valuable information for facilities because it: 1) identifies the where the low performers are, 2) allows for marketing of a high performer and 3) allows for prioritization of changes.

Comparability allows for performers to prioritize change in a way to get them the most impact for the littlest dollar while still trimming the lowest hanging issues as detailed in the low performer paragraph.



Being a low performer creates a sense of improvement and a comparative method allows the organization to see what the most effective improvement would be. This reduction in the low performers raises the entire industry steadily as it creates a new round of low performers who don't want that status. We are calling this feedback loop "performance encouragement" and has shown to be an effective approach to raising a sector as a whole.

High performers like to celebrate being a high performer. This allows them to celebrate that while still maintaining peer autonomy. Additionally, in a continually changing assessment framework or tool, this may be a limited status which encourages continued investment and assessment.

Nuclear facilities need to be cyber robust

According to Gary Johnson in the Cyber Robust Systems: The Vulnerability of the Current Approach to Cyber Security Chapter a cyber robust nuclear power plant system needs to provide a "truly independent level of defense in depth against a cyber-attack." This is done in a two-step approach: first identifying cyber hazards and then designing a robust system to address the hazard. Offline mechanisms should be heavily considered in this process as sort of a reverse side channel defensive approach. This could be done by looking at analog solutions in a digital world, inserting mechanical systems in place and taking advantage of approaches that use physics to limit the consequence.

Another approach is to take a similar approach to a cyber hazard as would be done in a safety system approach. This would include requiring certain levels of accuracy and trustworthiness in assessments. This is then followed with designing layers of administrative and technical systems to ensure multiple layers of safety are in place for any specific safety hazard.

Recommendations

Understanding that regulations are the minimal requirements and not necessary the best requirements for the industry specifically for cybersecurity is key to understanding that additional security measures are needed. But understanding where to implement security measures within one's own organization may not always be relevantly clear. Utilizing a comparative methodology such as the one suggested above, allows users to see directly various scenarios where an increase in their security and resilience score would provide them the most security and resilience overall or within the sub-categories. Thus ideally, removing the uncertainty of where to provide the best investment for future growth.

This needs to be explored more to understand specific requirements that the nuclear energy sector has in place but it provides many benefits that make the adoption a viable option for consideration.

Acknowledgements
Argonne National Laboratory's work was supported by the U.S. Department of Energy, Office of Science, under contract DE-AC02-06CH11357.

References
Yastrebenetsky & Kharchenko. Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. Various chapters. IGI Global. 2020.

Joyce, Petit, Phillips, Nowak, & Evans. Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program. ANL/GSS-17/2.
Argonne National Laboratory. 2017. https://publications.anl.gov/anlpubs/2018/03/140164.pdf