Contribution ID: **546** Type: **Paper**

A Proven Approach for Effective Computer Security Self-Assessments at Nuclear Facilities

A proven method for conducting cyber security self-assessments at nuclear power plants is now available for international use. This method was originally developed by Pacific Northwest National Laboratory (PNNL) under contract by the United States Nuclear Regulatory Commission (USNRC) for use by U.S. nuclear power plant licensees. The "Method", described in NUREG/CR-6847 "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants", was originally a limited release document that was withheld from public disclosure. The USNRC rescinded the document's classification and it is now publicly available. The Method provides a systematic, phased, and risk-informed approach to help decision makers and security specialists understand their relative cyber security posture. The Method goes into more detail on how to make risk-informed decisions using information obtained during the self-assessment guidance than does the IAEA's 2016 publication, Conducting Computer Security Assessments at Nuclear Facilities. However, the two approaches are compatible, with the Method fitting neatly into the framework provided by the IAEA's assessment guidance.

While the focus of the Method concentrates on systems associated with safety, security and emergency preparedness, it can also be extended to other systems within a nuclear facility (e.g. operational control systems associated with secondary or balance-of-plant operation, traditional IT systems related to business functions). Completed assessments may be used to support or validate the selection of computer security controls to mitigate cyber threats as well as demonstrate compliance with regulations or statutes enacted by Competent Authorities.

The Method assesses the cyber security posture of key systems at a nuclear facility with a focus on the protection of design base functions. It considers both physical and digital elements of system vulnerabilities and the resulting potential consequences from exploitation. It is well-suited for addressing blended cyber-attacks. A semi-quantitative analytical approach is used in the evaluation of potential vulnerabilities, consequences, and risks. The Method's risk assessment provides a technical basis for the selection of security controls to mitigate cyber-attacks.

The Method consists of six stages that fit within the steps outlined in IAEA assessment guidance. These stages are:
1. Examination of plant-wide cyber security practices. The team gathers information on the facility's cyber security policies, procedures, and practices. Information is also gathered on resources that can play a role in the cyber security of critical systems.
2. Identification of Critical Systems and Critical Digital Assets (CDAs) to be assessed. Systems associated with safety, security and emergency preparedness are identified. These systems are analyzed to identify and understand the digital assets that perform the design base function of the system. An initial consequence analysis for each identified CDA is used to estimate the potential consequences to the system and facility from a successful cyber-attack.
3. Conduct tabletop reviews and validation testing of the CDAs and their connected digital assets. Conduct tabletop reviews with plant personnel responsible for the design, operation, and maintenance of the identified critical systems and CDAs. Validation involves physical inspections (walk-downs) and a configuration review of critical systems. Where appropriate, an option exists to conduct scanning of CDAs and connected digital assets.
4. Conduct assessments of susceptibility. Results from the tabletop reviews and validation testing are used to assess the susceptibility to cyber exploitation of each CDA. Pathway analysis is used to understand the various vectors of attack that may exist for the system. Both direct and indirect pathways of compromise are considered. The product of this stage is an estimate of the overall susceptibility level for each CDA.
5. Conduct risk assessment activities. The initial consequence analyses that was performed in Stage 2 is reassessed using the additional information gathered in Stages 3 and 4. These results are used in conjunction with the results of susceptibility assessments to estimate the risks of cyber exploitation for each identified CDA.
6. Conduct risk management activities. Identify and characterize potential new security controls that could be implemented to enhance cyber security. A cost-benefit analysis is performed to identify those security controls that maximize effective protection and minimize risks to operation. Effective risk management options and recommendations are prepared for senior plant management approval and implementation.

The Method's application at U.S. nuclear power plants has been very encouraging. The only nuclear plant in the U.S. that did not have any adverse finding during its initial NRC computer security inspection prepared for its NRC inspection through the diligent application of this self-assessment method and the implementation

of the recommendations that came out of that self-assessment. Nuclear facilities around the world might find application of the Method extremely helpful for making cost-effective, risk-based decisions regarding computer security and for preparing them to pass computer security inspections by their competent authorities. This paper will summarize the Method and report on its successful application.

State

United States

Gender

Author: LANDINE, Guy (Pacific Northwest National Laboratory)

Co-authors: GLANTZ, Clifford (Pacific Northwest National Laboratory); COLES, Garill (Pacific Northwest National Laboratory)

Presenter: LANDINE, Guy (Pacific Northwest National Laboratory)

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