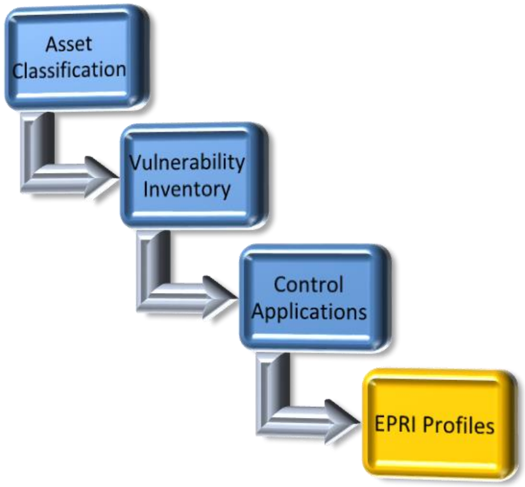
# Getting to Know Your “Attack Surface”

***EPRI is developing cyber security assessment profiles for devices with a range of attack surfaces to help evaluate cyber vulnerabilities and implement appropriate protective measures.***

“Attack surface” is a term that has gained traction in the world of cyber security. It refers to the various points or vectors through which an unauthorized user can try to enter data to or extract data from an environment. For example, a valve actuator at a nuclear plant has a relatively small attack surface, while a digital control system has a more complex attack surface and likely would require additional levels of security and protection.

In response to emerging technical and regulatory requirements, EPRI is developing a graded approach to cyber security for nuclear plants that will help assess what protective measures are needed for a given cyber asset (computer, network, programmable logic controller) to mitigate a specific cyber security vulnerability. The research will develop and validate a cyber asset classification scheme based on common vulnerabilities and attack surface profiles within a nuclear plant environment. The assessment profiles and device attack surface criteria developed through this effort will enable users to reduce the time and effort required to conduct controls assessments, provide consistent assessments across similar devices, and enable the sharing and reuse of completed assessment data for identical devices to drive efficiencies in the cyber security assessment process.

Phase I will address devices with small attack surfaces that do not have general purpose network interfaces, removable media, or advanced serial interfaces. Candidate devices include instrument transmitters, valve actuators and controllers (positioners), digital chart recorders, and single loop controllers.



Results will consist of attack surface criteria and security control methods to mitigate that small attack surface profile. These profiles can then be used to consistently identify and protect assets that match the attack surface criteria. The profiles also will be expressed in Excel formatted files for easy import into a plant’s security assessment tool. The Phase I technical report (3002004999) is planned for completion in fall 2015.

Phase II and later phases will address equipment with progressively more complex attack surfaces, such as network interfaces and programmable logic. EPRI also plans to develop an attack surface methodology enabling users to evaluate assets too complex for the common profiles.

For more information, contact Matt Gibson at 704.595.295 or mgibson@epri.com.

© 2015 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc.