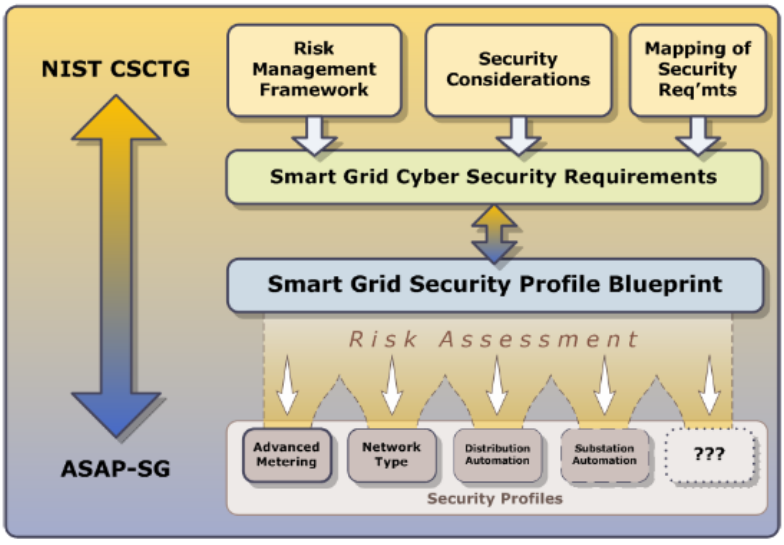
WIZNUCLEUS SMARTGRID CYBER SECURITY RISK MANAGEMENT PLATFORM – WizSG™

Wiznucleus WizSmartGrid (WizSG™)

Wiznucleus, a leading provider or Cyber Security Risk management Software Solutions has developed WizSG™ for SmartGrid by leveraging its strong cyber security risk management and compliance technology platform and its experience and successful track record of deploying cyber security risk assessment software in nuclear power plants and the utilities.

While the implementation of Advanced Metering Infrastructure (AMI), Distribution Automation, Transmission Automation, and Distributed Generation brings significant benefits to society, these new smart grid functions will leverage an Information Technology infrastructure in order to deliver these new capabilities. Automation within the grid will require the development of new applications and technologies designed deliver the benefits of a smarter grid. Automation is inherently vulnerable to cyber security risks, which if unmanaged provide a significant risk to the modern grid. The risk lies in the fact that applications and technologies will be used to control physical grid elements, in order to provide automated responses to conditions on the power system. As such these responses represent real activities, which if improperly operated could result in; loss of personally identifiable information, instability in the sustainability of the grid, and the ability to operate the system in safe reliable manner. WizSG™ has monitored the development of standards and best practice development, and understands the method and direction that has been established.

Figure 1: Security Architecture Methodology



Source: EPRI, Electric Power Research Institute

WIZNUCLEUS SMARTGRID CYBER SECURITY RISK MANAGEMENT PLATFORM – WizSG™

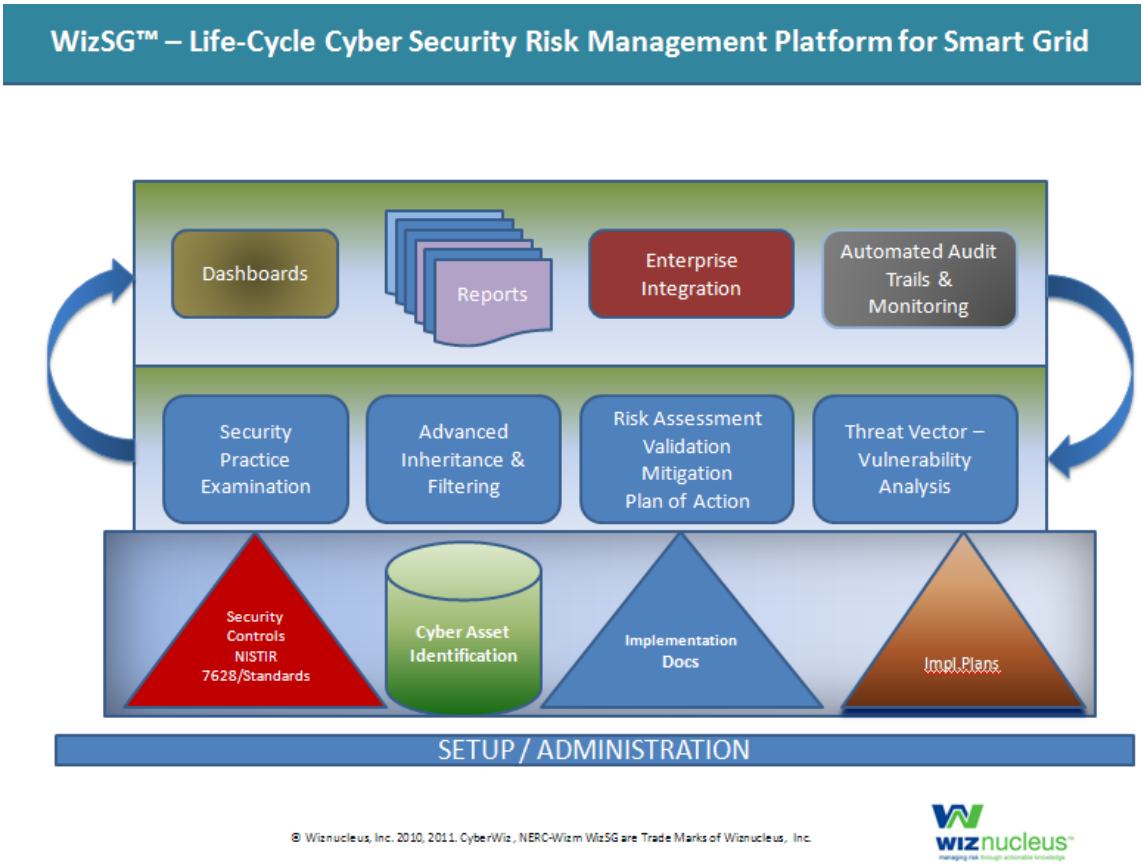
WizSG™ is designed to identify cyber security weaknesses in the various parts of the smart grid infrastructure, delivering the ability to monitor cyber security posture across multiple smart grid elements. This is done by leveraging frameworks, security considerations, and requirements that have been used to put together an overall best practice architecture as desgined by the NIST CSCTG and ASAP-SG. The product leverages technical standards from protocols such as IEC 61850, ANSI C12.XX, and others, which provides utilities with the ability to view risks to their Smart Grid components, based on variances. In addition to this, the tool takes into account guidance from NISTIR 7628 and NERC CIP, which illustrate best practices associated with the proper security management of a Smart Grid infrastructure. WizSG™ maintains the ability to interface with systems within the four key modern grid areas; AMI, Distribution Automation, Transmission Automation and Distributed Generation. WizSG™ identifies cyber security weaknesses in each of these architectures through the assessment and validation of the existing security control infrastructure. Where controls are not present, WizSG™ evaluates the lack of controls, to determine if any compensating controls exist to mitigate risk. This is done through the incorporation of our key risk indicator model, which is used to measure key risk to the infrastructure given the nature of the system. These risk indicators are rolled up to a centralized dashboard, which provides utilities with a mechanism to view enterprise smart grid risk.

WizSG™ accomplishes the following three processes:

- ***WizSG™ Risk ID*** – *Used to identify risks to components within each element of Smart Grid.*
- ***WizSG™ Risk Control*** – *Used to quantify risks identified in the WizSG™ Risk ID application.*
- ***WizSG™ Risk Monitor*** – *Used to illustrate overall risk for each Smart Grid element.*

WIZNUCLEUS SMARTGRID CYBER SECURITY RISK MANAGEMENT PLATFORM – WizSG™

Figure 2: WizSG Architecture



WizSG ™ also provides risk mitigation recommendations, based on the risks identified. For example, if no protection against malicious code is available for components within one of the Smart Grid architectures, such as may be the case in Smart Meters, the tool will identify that deficiency as a risk. It will then provide a risk mitigation recommendation to implement a solution such as an Intrusion Detection System (IDS), to be implemented in a manner that monitor the networks that support Smart Meter's for malicious payloads. The tool is also able to baseline protocols and normal usage, in order to support the integration of application white listing tools. Risk mitigation is used to reduce the overall risk to the Smart Grid architecture and Wiznucleus understands that risk can never be eliminated. As a result the WizSG tool is programmed to recommend solutions to reduce risk to an level that is acceptable to the organization that uses it. This provides the organization with a sliding scale of risk that adjusts as the infrastructure changes. When new technology and functionality are implemented, the tool takes those factors into account, identifies risk and remediation options for the risks that are identified.

WIZNUCLEUS SMARTGRID CYBER SECURITY RISK MANAGEMENT PLATFORM – WizSG™

WizSG™ - Risk ID

WizSG™ - Risk ID is used to help utilities to identify risk for each smart grid element. Within each element of smart grid, there are various components. Each component leverages an architecture that can be assessed for cyber security posture. These are multiple components to an AMI system, for example;

- *Home Area Network*
- *Residential Smart Meter*
- *Neighborhood Area Network*
- *Smart Collector*
- *Wide Area Network*
- *Utility Back Office*

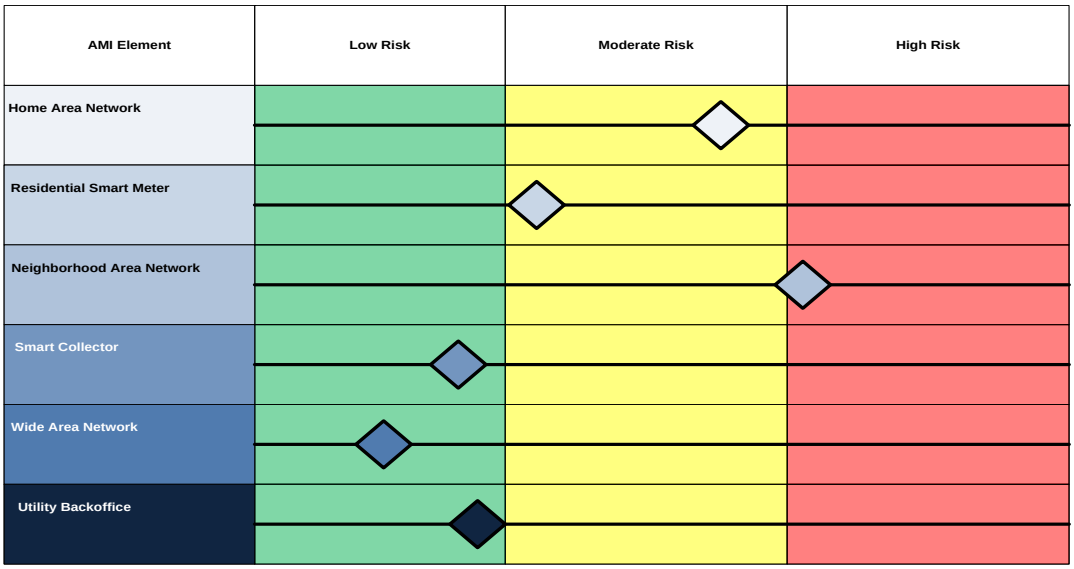
WizSG™ can identify risk in each of the components through a series of risk indicators. Risk indicators are identified based on the set of common controls which should be implemented based on the threats that exist. For example, there is a threat to Residential Smart Meters, that is, there is generally no physical protection for them. The primary key risk indicator, given this threat, is to determine the number of access vectors for the smart meter. A smart meter may have multiple access vectors-- radio communications access point in the smart meter, an optical port on the smart meter for physical access and perhaps a port which connects the meter to the home area network. Each interface is evaluated for cyber security posture, whether or not there are controls to prevent access to the smart meter from the optical port, radio communications interface or home area network interface. No control on one or more of these interfaces would represent a key risk indicator that would trigger further evaluation of the ability to access a smart meter. This process is repeated for each component within the AMI Smart Grid element, as well as in all Smart Grid elements that WizSG™ is used for.

WizSG™ - Risk Control

WizSG™ has been preprogrammed with a set of key risk indicators in each element of this architecture. The component of the tool is known as WizSG™ Risk Control. As the risk increases, the key risk indicator scale moves in the direction upward identifying the fact that more risk is present on the specific element being monitored. These risk factors are then correlated to other risks within the AMI architecture to deliver an overall total risk scoring. This allows utilities to address issues within the specific elements of AMI in order to reduce the risks. The following figure illustrates how the dashboard within WizSG™ shows cyber security risk at each layer of the AMI model;

WIZNUCLEUS SMARTGRID CYBER SECURITY RISK MANAGEMENT PLATFORM – WizSG™

Figure 1: WizSG™ Risk Control



WizSG™ assigns a risk score to each AMI element. These elements are then evaluated for cyber security posture based on whether or not they have the standard cyber security controls that should be implemented in any architecture. Where the controls are not present, a risk is noted. Where risks are noted, WizSG™ is associates them to compensating controls. A risk score is then established based on the overall posture of the element, which is represented by each of the diamonds on the risk matrix. Wiznucleus realizes that the impact and risk in each of these areas is different and therefore has taken an approach to ensure that this potential is taken into account. The utility back office for example maintains most of the standard cyber security controls in existence, because it is essentially representative of applications on servers behind firewalls with monitoring controls. The impact of compromise in such an environment would be very high; however the probability of occurrence is low given the controls in place. This may be different for the home area network, where the impact is low, but the probability high, depending on what is implemented.

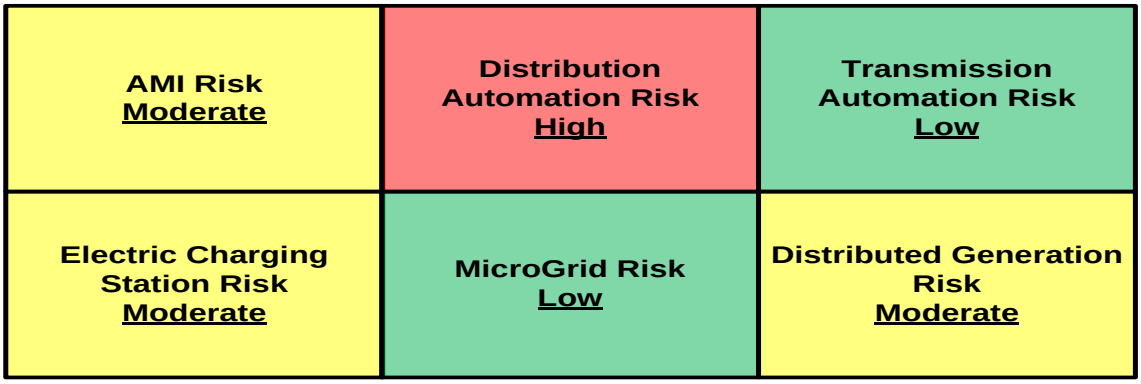
WizSG™ - Risk Monitor

WizSG™ takes this approach in identifying, managing and monitoring cyber risk in other areas of Smart Grid. The key to the product is in its breakdown of smart grid into logical components, where risk can be measured. Furthermore the risk scoring is represented as being fair because the impact is quantified into the risk factor at the system level. This makes it easy to roll up an overall risk score, which gives the utility with a snapshot view

of their current cyber security posture associated with their smart grid deployment. Using the example from the figure above, using WizSG™s risk calculator, the overall risk to this AMI deployment is low to moderate, given

the risk levels that were identified. The utility might then get an overall view of their smart grid deployments in the same manner. The following figure represents WizSG™s overall view of risk for a utility smart grid deployment.

Figure 2: WizSG™ Risk Monitor



The dashboard provides the utility with a view of risk within each smart grid area. Selecting an area will take the utility to the lower level view of risk for that specific smart grid element. The utility can then drill down further to see which controls are missing, why the risk exists, etc. WizSG™ has developed a risk module for each smart grid element, allowing utilities to implement the tool only for the smart grid elements that they maintain, and add additional modules as they implement new smart grid elements.

ABOUT WIZNUCLEUS

Wiznucleus, a privately owned MBE, provides advanced automation software and expertise required for life-cycle management of cyber security assessment software solutions. Wiznucleus solutions were built from the ground up to address key cyber security requirements as it pertains to critical infrastructure. Wiznucleus cyber security assessment and risk management software is currently in operation in nuclear power plants and utilities. The software platform provides advanced functionality utilizing the highly scalable and flexible technology architecture with integrated management reporting and threat vector analysis. Wiznucleus leverages its deep understanding of cyber security risk assessment and threat management in nuclear power plants, utilities and smart grid sectors. Current customers of Wiznucleus include some of the leading nuclear power plants, utilities, and regulatory agencies. Wiznucleus is headquartered in New York City, New York.