perspecta LABS

A new approach to smart grid security assessment

A white paper on the challenges of traditional security assessments and the advantages of a 4-Quadrant™ approach

Shedding light on hidden security risks

Smart grid challenges

Today, an electric utility uses many different technologies and networks to meet its varied needs for communications – some legacy, some still evolving. Accelerated smart grid deployments have dramatically increased the presence and role of intelligent endpoints, controls and sensors in the electrical system. Most noteworthy are utility advanced metering infrastructure, distribution automation and substation, and automation programs. This distributed intelligence requires secure and reliable field network communications and devices, which necessitates the rethinking of traditional utility operations technology security.

Critical enhancements to traditional security capabilities include:

- New methods, techniques and tools to identify intelligent device vulnerabilities
- New tools to provide visibility into wireless network traffic
- New means to monitor and detect anomalous behavior and potential signs of intrusion
- New capabilities to support forensics and diagnostics

IT network and vulnerability scans are not adequate

The challenges of security assessments and risk management for smart grid systems differ from traditional IP-based computer networks; both in scope and technique. Field network infrastructure consists of a large number of embedded intelligent devices typically in the form of dual-band wireless nodes, signal repeaters, smart meters, supervisory control and data acquisition remote terminal units, line sensors and various monitors. While powerful, these embedded mini-computing systems are much less capable than their enterprise counterparts and their security controls are typically much less mature. Many of these intelligent endpoints cannot be physically protected, therefore are susceptible to both physical and cyberattacks.

Wireless field networks are heterogeneous and may consist of three or more different radio systems, such as 3G/4G/LTE technologies (usually for backhaul), proprietary access radios, and short range ZigBee home area networks (HAN). Communication is usually carried over a mix of standards-based and proprietary protocols and network technologies.

This not only makes visibility into the network difficult, but renders traditional IT security assessment methods and tools unusable as well.

Field networks further employ a variety of security controls including public-key infrastructure, mixed asymmetric and symmetric cryptography, new secure broadcast protocols and proprietary secure-session approaches with many options. Depending on what security features a utility has chosen to deploy and how those features are configured, each utility may be susceptible to different, yet related types of attacks.

Once a vulnerability is identified, mitigation is an even greater challenge as utilities cannot layer on their own security, but instead must rely on vendor-specific solutions. These challenges require a different approach to better understand the attack modalities applicable to each utility's field network and its intelligent field devices, as well as, technology to monitor and detect the presence of such attacks, especially if mitigating controls are not yet available.

Perspecta Labs' proven 4-Quadrant Security Assessment Methodology

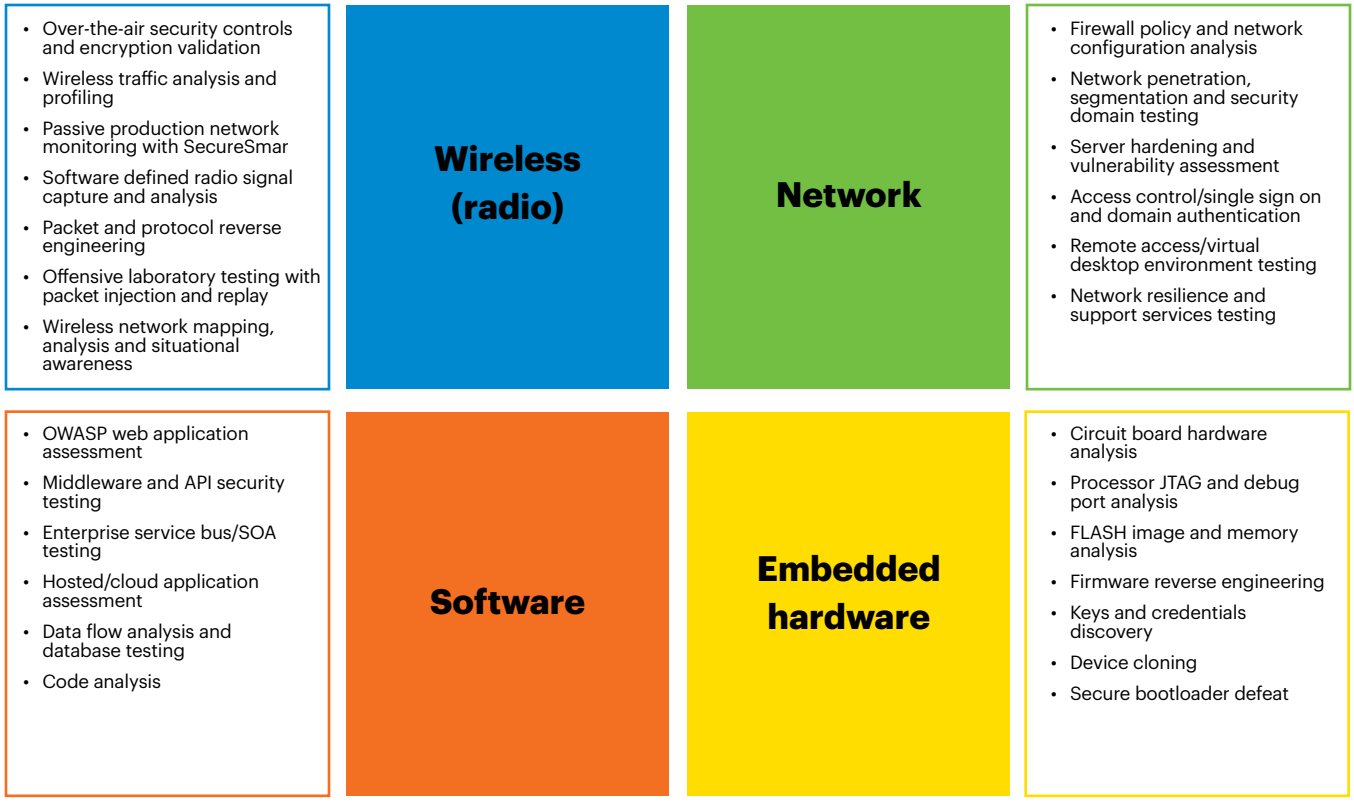
Perspecta Labs' 4-Quadrant Security Assessment Methodology, a component of its Secure**Smart™** critical infrastructure solution line combines traditional penetration testing techniques for networks, computer systems, and applications, with a detailed embedded hardware security and unique radio communications analysis capability. The 4-Quadrant Security Assessment Methodology focuses on four areas: wireless (radio), network, software and embedded hardware/firmware.

Perspecta Labs uses its proven 4-Quardrant Security Assessment Methodology to perform vulnerability assessments and penetration testing across enterprise networks, communications systems, utility and smart energy systems, industrial control systems, IPTV and protected content systems.

This methodology takes into account the embedded systems nature and deployment of intelligent electronic devices (sometimes over a wide geographical area), extended traditional IT vulnerability assessment and penetration testing beyond application, operating system and networking vulnerabilities for physically secure, IP-based and web infrastructures.

Our 4-Quadrant methodology seeks to validate whether the security controls claimed by the system vendor, operator and owner actually exist and are operational. It then focuses on the discovery and means to exploit design, implementation and configuration weaknesses. This methodology is designed to emulate real attacks against target systems to determine the potential for malicious actors to perform the same attacks in a production environment.

Our 4-Quadrant methodology covers the four quadrants of the vulnerability assessment space for these systems, addressing application and management software, wireless communications, back-end and tiered transportation network access controls, and embedded hardware and firmware. While the results from each quadrant individually provide deep insight, Perspecta Labs goes further by linking the testing efforts and findings across each quadrant to evaluate cross-quadrant vulnerabilities. Linking vulnerabilities together from different quadrants into a larger operational exploit exposes the true risk and potential for damage that is sometimes not apparent when looking at only one category.



Wireless (radio) communication security assessment

A specialized capability that seeks to uncover low-level vulnerabilities in wireless communications beginning with modulation scheme and coding, media access control, link level properties, network synchronization, routing, and transport security up through application layer communication exchanges in wireless field networks, home area networks, ZigBee networks and other wireless systems. This portion of the 4-Quadrant assessment requires skills and competencies in wireless modulation techniques and protocol reverse engineering.

Network security assessment

Seeks to uncover vulnerabilities in the back-end network(s) that typically interconnect wireless field networks with enterprise, management and control applications. This focuses on perimeter and compartment defenses, edge routers and gateways, and means to access backend compartments from field networks, internal corporate data networks and remote access. This portion of the 4-Quardrant assessment requires skills and competency with IPv4/IPv6 networks, equipment configuration and firewall policies, and fixed and wireless networks and transport systems.

Application and management software security assessment

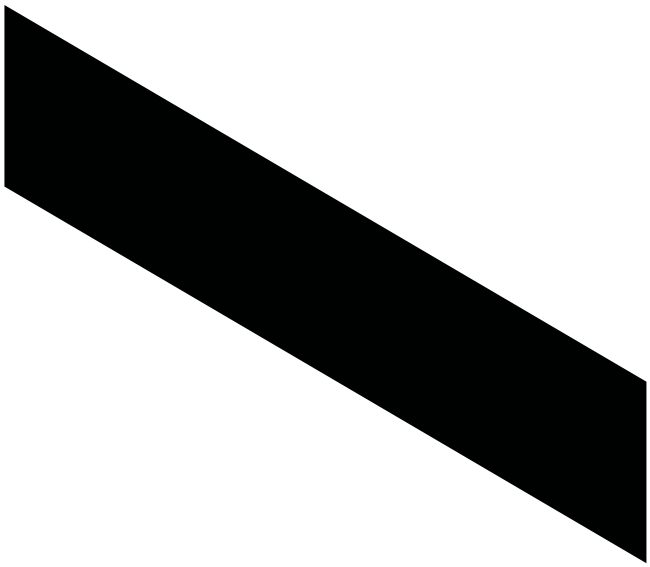
Seeks to uncover weaknesses and vulnerabilities in head-end management server applications, customer care, customer portal and business support systems. Activities include testing for Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks in web-based systems, enterprise service oriented architectures, and web services interfaces in support components such as databases, authentication services, crypto services, name services and time services. This portion of the 4-Quadrant assessment requires skills and competency in enterprise service architectures, web technologies, computer programming and security vulnerability testing.

Embedded hardware and firmware security assessment

A specialized capability that seeks to uncover weaknesses and vulnerabilities related in the embedded system circuitry, hardware interfaces, on-chip debugging functions, bootloaders and firmware. This portion of the 4-Quadrant assessment requires skills and competency in electrical engineering, embedded systems, software vulnerabilities and reverse engineering.

The Perspecta Labs advantage

There is always a risk when introducing new equipment and/or new manufacturers into network infrastructure. For this reason utilities need a comprehensive approach to assessing vulnerabilities and mitigating them both before deployment decisions are made and throughout the product's lifecycle. We provide utilities with comprehensive, holistic and insightful vulnerability assessment and penetration testing in all four quadrants. The Perspecta Labs' 4-Quadrant Security Assessment Methodology is an industry-leading approach that can effectively identify vulnerabilities and develop mitigation plans to prevent malefactors from exploiting these vulnerabilities.



Learn more at perspectalabs.com

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920