Case Study

U.S. Power Company Works with Industrial IT Solutions to Perform a SCADA Cyber Security Vulnerability Assessment

“We needed access to cyber security experts with process control systems knowledge. Honeywell’s team of experts was just what we needed to assess our SCADA system.”
- Audit Team Lead, U.S. Power Company

Background
Power companies have developed a safety culture that is ingrained into everyday activities. Physical security of power company installations is a part of that safety culture. As cyber-attacks have come to the forefront of just about any business that utilizes electronic communications, power companies are finding that cyber security requires the same level of focus and commitment as safety.

A growing number of consulting firms are offering cyber security services, and it is a challenge to determine the experience level of the service engineers and the depth of knowledge in standard and best practices as they apply to control systems.

Benefits
Honeywell’s Industrial IT Solutions team provide a suite of solutions for process control systems that are vendor-neutral and address the increasing risk level of today’s contemporary systems.

The Industrial IT Solutions team offers:
• 12+ years’ experience providing industrial-strength security solutions
• 400+ projects combining IT best practices and complex process control environments
• Experience with over 70 control systems

The Cyber Security Vulnerability Assessment (CSVA) focuses on protecting a site’s assets by evaluating the current situation against industry standard, regulatory requirements, and best practices.

The CSVA enables customers to:
• Minimize vulnerability to cyber events
• Reduce impact and shorten recovery time of an incident
• Improve system performance
• Reduce resource load from automated solutions
• Interface with a single source supplier for turnkey security solutions
• Avoid large fines, shutdowns, and additional staffing

Challenge
A forward-thinking U.S. power company employed regularly-recurring audits of various controls, systems and programs. However, when it came to a SCADA-based cyber security vulnerability assessment, the in-house audit team did not possess the specific combination of process control experience and IT security risks. They realized they required a third-party expert with a unique combination of knowledge of the two worlds.
Finding a cyber security consulting firm with this expertise was not easy, however. The power company contacted several consulting firms, none of which were familiar with SCADA or other process control systems.

**Solution**

After contacting a number of these IT consulting firms, the power company chose Honeywell’s Industrial IT Solutions.

The Industrial IT Solutions team possessed the experience and background that the power company required to review their SCADA system.

The power company and Industrial IT Solutions embarked on a collaborative review of the power company’s process control systems and SCADA risk-assessment policies and procedures. During the risk assessment process, high-level risks were identified. This information was used to estimate, prioritize and coordinate ongoing risk-mitigation activities.

**Results**

Based on the Industrial IT Solutions team knowledge of control systems and process control environments, the power company contracted with them to supplement the existing IT risk assessment process.

The power company received a high-quality, expert assessment with specific risk rankings to outline specific areas for remediation. Industrial IT Solutions provided a unique combination of cyber security and SCADA control system experience that enabled the power company to:

- assess their true risk
- abide by corporate standard of audit and review
- prioritize the tasks they needed to execute

---

**About CSVA and the Process**

Many control system organizations today lack the manpower and skillset to assess the vulnerabilities and risks associated with Industrial IT. Working with Honeywell Industrial IT professionals can help close the gap and facilitate the implementation of a phased on-going approach to security your critical infrastructure.

Assessing your assets and vulnerabilities is a first and repeated phase in the lifecycle (see above diagram).

Based on the results of the CSVA, recommendations can be implemented and the next phase of the life cycle addressed.

For more information on how Honeywell’s Industrial IT Solutions can help your site reduce risk and address vulnerabilities, contact your Honeywell Account Manager.