Process Solutlons

Honeywell

Success Story

U.S. Power Company Works with Honeywell 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.

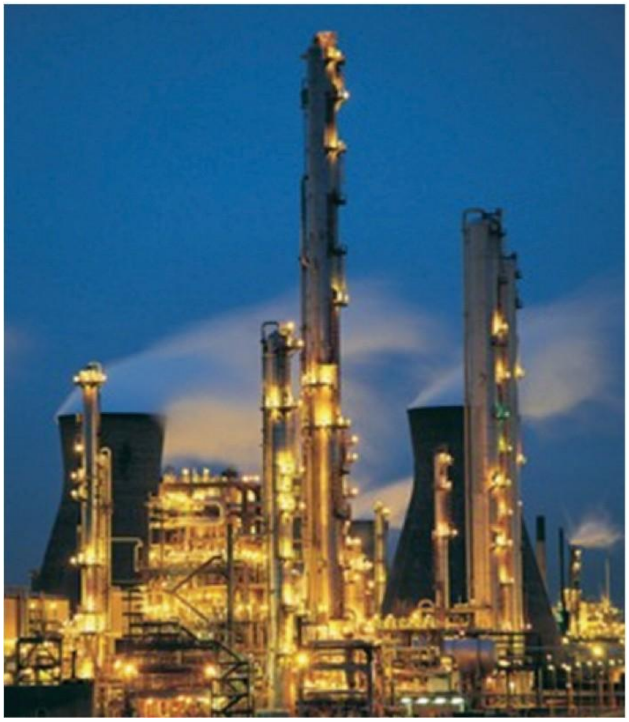
Benefits

Honeywell’s Industrial Cyber Security team provides a suite of solutions for process control systems that are vendor-neutral and address the increasing risk level of today’s contemporary 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 cyber 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 consulting firms, the power company chose cyber security solutions from Honeywell.

The Honeywell Cyber Security team possessed the experience and expertise that the power company required to review their SCADA system.

The power company and Honeywell 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

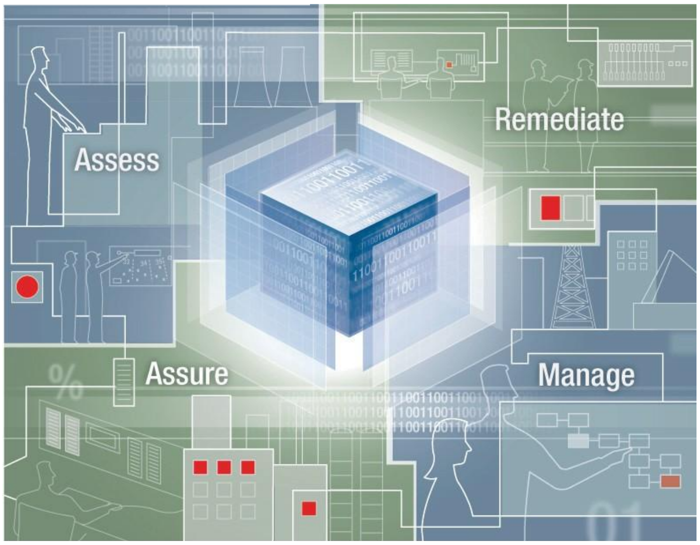
Based on Honeywell's knowledge of control systems, process control environments and cyber security, the power company contracted with them to supplement the existing risk assessment process.

The power company received a high-quality, expert assessment with specific risk rankings. Areas were highlighted for remediation 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

Assess your assets and vulnerabilities against industry standards and best practices

Remediate your network with a custom-designed security program



Assure your security program is functioning as designed

Manage your network security investment with support and training

About CSVA and the Process

Many control system organizations today lack the manpower and skill set to assess the vulnerabilities and risks associated with Industrial Cyber Security-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 Cyber Security Solutions can help your site reduce risk and address vulnerabilities, contact your Honeywell Account Manager.

For More Information

Learn more about how Honeywell's Industrial Cyber Security Solutions can help improve cyber security at your facility, visit our website www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

SS-13-02-ENG
November 2014