Honeywell
THE POWER OF CONNECTED | Connected Industrial

Total Improves Cyber Security with Managed Security Services

Case Study

"Honeywell provided the cyber security knowledge base required to protect our refinery's control system. We have 24/7 coverage regardless of what is happening in the plant."

– Lanny Gibson, Process Control Supervisor

Total Port Arthur Refinery

Background

Like other large energy firms, Total S.A. requires industrial cyber security solutions that allow the company to address today's rising security threats while allowing the staff to focus on their industrial process. Headquartered in La Defense, France, the company operates in the upstream, refining & chemicals, and marketing & services segments of the Oil & Gas industry.

Total Petrochemicals & Refining USA, Inc. (TPRI) is part of the Refining-Petrochemicals Americas Segment of Total S.A. and a major producer of polypropylene, polystyrene, styrene, base chemicals and polyethylene.

Total's Port Arthur refinery partnered with Honeywell to achieve an enhanced cyber security posture.

Total's Port Arthur Refinery has a capacity of 169,000 barrels per day of transportation fuels. It processes crudes with conversion capabilities centering on coking, Fluid Catalytic Cracking Unit (FCCU) and reforming technologies.

Challenge

Industrial control systems have been increasingly targeted by bad actors since the discovery of Stuxnet in 2010. In the face of increased discovery of industrial exploits, even common practices like the use of USB drives to maintain industrial control systems can be used to propagate malware.

For industrial sites, specific cyber security vulnerabilities can include:

- Lack of security policies and procedures
- Undocumented or undiscovered ways to gain access to the industrial process network from the public internet
- Access points that span the business Local Area Network (LAN) to the Process Control Network (PCN)
- Out of date anti-virus software

Protecting plant operations requires not only robust firewalls, but also additional security measures and defenses. Detailed reporting is equally important to provide the information needed to manage and respond to malicious attacks.

.

About Honeywell's Managed Industrial Cyber Security Services

Around the world, industrial firms and critical infrastructure operators partner with Honeywell to address the unique requirements of cyber security in process control environments. Honeywell's broad expertise encompasses automation assets and their integrated communication networks —a distinct advantage in control system security.

- Obsolete firmware and operating systems that cannot be maintained with security updates and security patches
- PCN architectures implemented without network segmentation and other security design considerations
- Incomplete or infrequent backup process.

As part of the lifecycle management of the control system, Total's engineering staff consulted with Honeywell's cyber security experts to perform a complete site audit to identify security vulnerabilities and develop a strategy to mitigate threats. Total corporate representatives met with Honeywell to define and implement an approach to updates, patching and other cyber security activities that allowed the plant to improve site security while being able to focus on their core refining processes.

Key to implementing an effective cyber security program was supporting the small in-house automation department at Port Arthur, which was responsible for overseeing a relatively large PCN consisting of approximately 120 servers and workstations.

Solution

Honeywell's Managed Industrial Cyber Security Services helped to reduce the risk of security breaches and manage the security posture of process control infrastructure. Honeywell's Managed Industrial Cyber Security Services provided skilled industrial security engineers to support the ongoing maintenance and monitoring of the site's industrial cyber security.

The first effort of its kind within Total Petrochemicals & Refining USA, Managed Cyber Security Services for the Port Arthur Refinery include:

- Honeywell Secure Connection featuring encrypted communication to protect data even through the site's corporate network
- Automated Patching and Anti-Malware services to ensure all computers are continuously updated with the latest security protections
- Continuous Monitoring and Alerting services to monitor the performance and health condition of the PCN, including controllers, servers, and workstations
- Intelligence Reporting Services to transform system statistics into actionable trends.

When a facility like the Port Arthur Refinery launches Honeywell's Secure Connection, an authenticated, encrypted Virtual Private Network (VPN) is established. Various Honeywell and customer entities can connect to this network to help the refinery address security issues or general maintenance issues. Having a secure means of remote connection and maintenance can also help reduce downtime and troubleshooting related to any issues.

A dedicated Honeywell site support specialist supports Total's services agreement. This provides assistance with patch and anti-virus automation, security and performance monitoring, activity and trend reporting, advanced monitoring and co-management, and secure access.

Benefits

With Honeywell's Managed Industrial Cyber Security Services, the Port Arthur Refinery has greater visibility into the cyber security and system conditions of its PCN architecture.

From Total's perspective, partnering with a recognized cyber security specialist made good business sense. Refinery personnel are very knowledgeable in plant processes, but often do not have the resources and skills to maintain the ongoing security posture of the process control network.

Future plans include expanding the scope of Honeywell's services to cover additional assets such as analyzer networks and safety systems. Total also wants to provide global users on its business network with safe and secure access to cyber security information when needed.

Summary

Honeywell's suite of technology infrastructure services has helped Total secure the various aspects of its DCS. This includes an array of security defenses integrated to protect the network, workstations, applications, and process equipment.

This approach results in enhanced operating system security, stability and reliability, ultimately contributing to improved production and safety for complex industrial plant domains.

For More Information

Learn more about how Honeywell's Managed Industrial Cyber Security Services can protect plant operations, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

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

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Park, Pudong Shanghai, China 201203

www.honeywellprocess.com

SS-17-11-ENG
July 2017

Honeywell