ABB

Middle East oil refinery chooses ABB Cyber Security Fingerprint to strengthen cyber security defenses

—
01 ABB experts help improve process performance.

Even though the petroleum refinery's comprehensive security included military guards and advanced cyber security measures, plant operators wanted to ensure the same level of comprehensive cyber security policies and procedures were applied across all of its process control systems.

—
ABB Ltd.
579 Executive Campus Drive
Westerville, OH 43082

abb.com/cybersecurity

Customer need
• Review existing cyber security measures
• Identify security gaps
• Make improvements

ABB's response
To ensure the facility's existing cyber security measures took their process control systems into account, the refinery chose the ABB Cyber Security Fingerprint service to identify areas of improvement in the plant's automation systems.

ABB Cyber Security Fingerprint starts by gathering data on the current state of cyber-readiness from all computers associated with the systems and from key personnel. It then runs that data through ABB's proprietary software-based analysis tool and compares the results to cybersecurity best practices. The resulting report provides detailed recommendations to reduce cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for the control systems going forward.

Results
Even though extensive security measures were already in place, the ABB Cyber Security Fingerprint found opportunities for improvement. Outdated and unnecessary software was identified for updating or removal. Security patches for several software versions were missing and also needed to be updated.

The report spurred the company's management to action. This included fixing the identified problems as well as scheduling periodic ABB Cyber Security Fingerprint audits to ensure the company's cybersecurity policies and procedures were always up-to-date.

Customer Benefits
• Comprehensive overview of the plant's cyber security readiness and effectiveness
• Improved risk mitigation
• Enhanced control system security
• Revamped and improved security policies and procedures