ROVISYS®
Automation & Information Solutions

CASE STUDY

NERC-CIP ASSESSMENT: POWERING UP CYBERSECURITY

To meet the NERC-CIPv5 requirements, this electric utility turned to RoviSys to perform the critical analysis of its facilities' cybersecurity status.

ROVISYS

With a unique set of capabilities and expertise in the utilities industry plus a deep understanding of process controls, information technology and management, and cybersecurity, RoviSys was the clear choice to take on this project.

As the reach of the Industrial Internet of Things grows, so does the risk of cyberattacks, malware, and data theft. For critical pieces of the country's infrastructure like power generation, any such risk is unacceptable.

THE PROBLEM

To help mitigate the cybersecurity risk to the bulk power system, NERC issued the fifth version of its critical infrastructure protection cybersecurity standards (CIPv5). The sweeping set of regulations required a full, top-to-bottom analysis of the utility's generating facilities to determine what procedures, policies, or systems required remediation to meet the requirements.

THE SOLUTION

RoviSys began with the Department of Homeland Security's Cyber Security Evaluation Tool (CSET), interviews with key stakeholders at the utility, and all the utility's existing cyber security policies and procedures. The CSET tool provides a systematic and repeatable approach to assessing the cybersecurity posture of cyber systems and networks with high-level and detailed questions related to all industrial control and information technology systems.

Based on CSET, RoviSys compiled a list of questions that would need to be answered to gather the information to do the assessment. It then met with IT personnel and plant personnel, working closely with them to answer the questions. For those questions that could not be answered immediately, RoviSys worked with the utility to determine what needed to be done to obtain the answers.

As a part of the assessment, RoviSys conducted a physical and logical review of the utility's facility as well as a detailed review of all documented policies and procedures that were provided by the utility.

RoviSys then compiled all the information obtained from the questionnaire, from the site survey, and from the review of the policies and procedures and organized the information into categories for review against NERC-CIP compliance requirements. The information was arranged into the following categories:

Using CSET, RoviSys compiled variance statistics for the compliance categories and ranked the primary deficiencies of the facility systems based on greatest vulnerability exposure.

THE RESULTS

The analysis results followed a three-level track:

First, and most important, was identification of deficiencies that required immediate remediation for facility compliance by April 1, 2017.

The second level of analysis found deficient items requiring remediation for compliance by September 1, 2018 (compliance dates mandated by NERC-CIP for low-impact facilities).

Finally, analysis was conducted on vulnerabilities that place the utility at high risk based on NERC CIPv5.

The conclusions created a roadmap for the utility to pursue a successful, low-impact facility audit after remediation of the non-compliance issues and greatly improve the plant's overall cyber security. With this analysis in hand, the utility had a clear course of action in place to make the IT, OT, and physical security changes necessary to meet the cybersecurity requirements of the NERC-CIP standards.

Training	System Protection	System Integrity
System and Services Acquisition	Software	Risk Management and Assessment
Remote Access Control	Procedures	Portable/Mobile/Wireless
Policies and Procedures – General	Policies	Plans
Physical Security	Personnel	Organizational
Monitoring and Malware	Maintenance	Info and Document Management
Info Protection	Incident Response	Environmental Security
Continuity	Configuration Management	Communication Protection
Audit and Accountability	Account Management	Access Control