Chapter 47
SaskEnergy—SCADA System Security

1.0 Main Points

By August 2017, SaskEnergy implemented our remaining two recommendations related to its processes to secure SCADA. It configured and monitored its SCADA system to protect it from security threats.

SaskEnergy delivers natural gas to the people of Saskatchewan. To help it do so, it uses its IT-based supervisory control and data acquisition (SCADA) system to control and monitor the physical transportation of natural gas through pipelines. Strong security processes are key to protecting its SCADA system against risks associated with unintentional actions by staff or actions with malicious intent.

2.0 Introduction

In 2013, we assessed SaskEnergy's processes to secure its SCADA system. Our *2013 Report – Volume 1*, Chapter 19 concluded that SaskEnergy did not have effective processes to secure its SCADA system used to control and monitor distribution of natural gas for the period of September 1, 2012 to February 28, 2013.[1] We made seven recommendations. As reported in our *2015 Report – Volume 1*, Chapter 30, by March 20, 2015, SaskEnergy had implemented five of the seven recommendations.

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance* (including CSAE 3001). To evaluate SaskEnergy's progress towards meeting our recommendations, we used the relevant criteria from the original audit. SaskEnergy's management agreed with the criteria in the original audit.

To perform our follow-up of the recommendations, we discussed actions taken with management and reviewed relevant evidence (e.g., SCADA network architecture changes, monitoring reports, incident reports).

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Crown and Central Agencies agreed to the recommendation, the status of the recommendation at August 31, 2017, and SaskEnergy's actions up to that date. We found that SaskEnergy implemented the two remaining recommendations.

[1] The original report regarding these recommendations can be found at www.auditor.sk.ca under the "Publications" tab, Public Reports.

3.1 SCADA Configured to Protect SaskEnergy from Security Threats

We recommended that SaskEnergy Incorporated configure its supervisory control and data acquisition system network to protect it from security threats. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy strengthened the configuration of its SCADA system network to protect it from security threats.

In 2015, we reported that SaskEnergy had developed a plan to configure the SCADA system network based on a threat and risk assessment. The planned configuration was largely consistent with industry recommendations for SCADA systems. For example, the plan required firewalls to separate the SCADA system from other networks, zones within the network to help isolate incidents if they occur, and systems to identify unauthorized changes to the network. SaskEnergy had begun to make these changes.

By August 31, 2017, SaskEnergy had made the most significant configuration changes required by its plan. It scheduled the two remaining changes for October 2017 to reduce interruptions to its natural gas systems. In addition, SaskEnergy had adequate processes to maintain the network configuration by updating network devices for new security threats and risks.

3.2 SCADA Security Monitored

We recommended that SaskEnergy Incorporated monitor the security of its supervisory control and data acquisition system. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy uses real-time reporting to monitor the security of its SCADA system.

In 2015, SaskEnergy configured devices in its SCADA system network to provide continuous monitoring of security information (e.g., user log-ons, changes to devices). In addition, it contracted with a service provider to analyze the information and provide reports and real time alerts for suspicious activity. The service provider monitors 24 hours a day, 365 days a year.

We found SaskEnergy employees follow documented processes to respond to alerts received from the service provider. Processes included tracking reported incidents, assessing risk, investigating, and escalating if required.

All incidents reported by the service provider from August 2016 to June 2017 were low risk.