Chapter 19
Securing SaskEnergy's SCADA System

1.0 Main Points

The people and economy of Saskatchewan require safe, uninterrupted, and effective distribution of natural gas. Natural gas is used to heat buildings, power appliances, and is used by many Saskatchewan industries.

SaskEnergy delivers natural gas to 358,000 customers throughout Saskatchewan. Natural gas is transported to customers using a pipeline distribution system that covers 92% of Saskatchewan communities. SaskEnergy relies on both physical and information technology assets to distribute natural gas. Physical assets include compressor stations and pipelines. Information technology assets like supervisory control and data acquisition (SCADA) systems are used to monitor and control the physical transportation of natural gas through pipelines.

This chapter describes our audit of SaskEnergy's SCADA system. The objective of our work was to assess whether SaskEnergy had effective processes to secure its SCADA system. For the period of September 1, 2012 to February 28, 2013, our audit found that SaskEnergy did not have effective processes to secure its SCADA system. SaskEnergy needs to improve its processes in the following areas:

- Prepare a complete threat and risk assessment for its SCADA system
- Implement complete policies and procedures to protect the confidentiality, integrity, and availability of its SCADA system
- Properly configure its SCADA system to protect against security threats
- Protect its facilities from unauthorized access
- Protect its SCADA system from unauthorized access
- Monitor SCADA system security
- Test its SCADA system continuity plan

We make seven recommendations in this chapter to help SaskEnergy protect the confidentiality, integrity, and availability of its SCADA system, and associated data.

Although we have made process recommendations, we recognize that SaskEnergy has been able to provide safe and reliable operations for many years and has not experienced a major outage resulting from its SCADA system.

2.0 INTRODUCTION

SaskEnergy Incorporated (SaskEnergy) is a provincial Crown corporation created under *The SaskEnergy Act*. SaskEnergy owns and operates a natural gas utility which has the exclusive legislated franchise to distribute natural gas within Saskatchewan.

SaskEnergy delivers natural gas to more than 358,000 residential, farm, commercial, and industrial customers throughout Saskatchewan. Natural gas is transported to customers through an 83,000-kilometer pipeline system that covers 92% of Saskatchewan communities. Natural gas heats homes, hotels, hospitals, schools, and recreational centres throughout the province. It powers appliances (e.g., water heaters, fireplaces, barbeques) used by the people of Saskatchewan every day, and is also used by many Saskatchewan industries such as steel, pulp and paper, potash, petrochemical, electrical generation, and fertilizer production.

3.0 CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure means physical and information technology assets that are essential for the functioning of society and the economy. Critical infrastructure is used for electricity generation, gas and oil distribution, telecommunications, water supply, and transportation systems. Physical assets that are part of critical infrastructure include facilities and equipment needed to provide essential services. Information technology assets that are part of critical infrastructure include industrial control systems like SCADA systems that are used to monitor and control critical infrastructure facilities. SaskEnergy uses a SCADA system to monitor and control the physical transportation of natural gas through pipelines.

Critical infrastructure needs to be available at all times. Continuous availability requires strong security processes to protect against risks associated with unintentional actions by staff or actions with malicious intent. In fall 2012, the Office of the Auditor General of Canada reported on the importance of protecting Canadian critical infrastructure, including infrastructure managed by provinces, against cyberattacks.[1] The report highlights that cyberattacks on critical infrastructure of many nations, including Canada, have been reported. The report also indicates that the frequency and severity of cyber threats are increasing.

The people of Saskatchewan rely on the availability of critical infrastructure every day. Various utility providers use critical infrastructure to provide their services to the residents of Saskatchewan. For example, SaskPower provides electricity generation and transmission, SaskWater monitors water provision to communities, Water Security Agency of Saskatchewan monitors water levels and controls flows from dams, and SaskEnergy distributes natural gas to consumers.

[1] Cyberattacks include the unintentional or unauthorized access, use, manipulation or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf (11 April 2013).

4.0 Importance of Protecting SaskEnergy's Critical Infrastructure

The Saskatchewan people and the economy require safe, uninterrupted, and effective distribution of natural gas.

SaskEnergy has maintained a reliable system of distribution of natural gas for the past 25 years. While some localized outages have occurred, the province has never been without natural gas for an extended period of time.

A worst-case failure would likely require multiple and concurrent adverse events. The consequences of a worst-case failure could have a major impact on the province. If natural gas distribution failed in the middle of the winter, homes, government buildings (e.g., hospitals, schools), and businesses would be without heat. It is not clear whether the electric grid would be capable of supporting the increased power demand that would result if gas distribution failed or for how long. Without power or heat, everything from telecommunications service to water delivery could be at risk.

5.0 SaskEnergy's Critical Infrastructure

SaskEnergy has 26 natural gas facilities (e.g., compressor stations) within the province. A compressor station works by pressurizing natural gas transported in transmission pipelines. The pressure pushes the natural gas through the pipeline to end consumers. Without sufficient pressure, natural gas would not flow to consumers. Excess pressure could create unsafe conditions at a compressor station or in a pipeline.

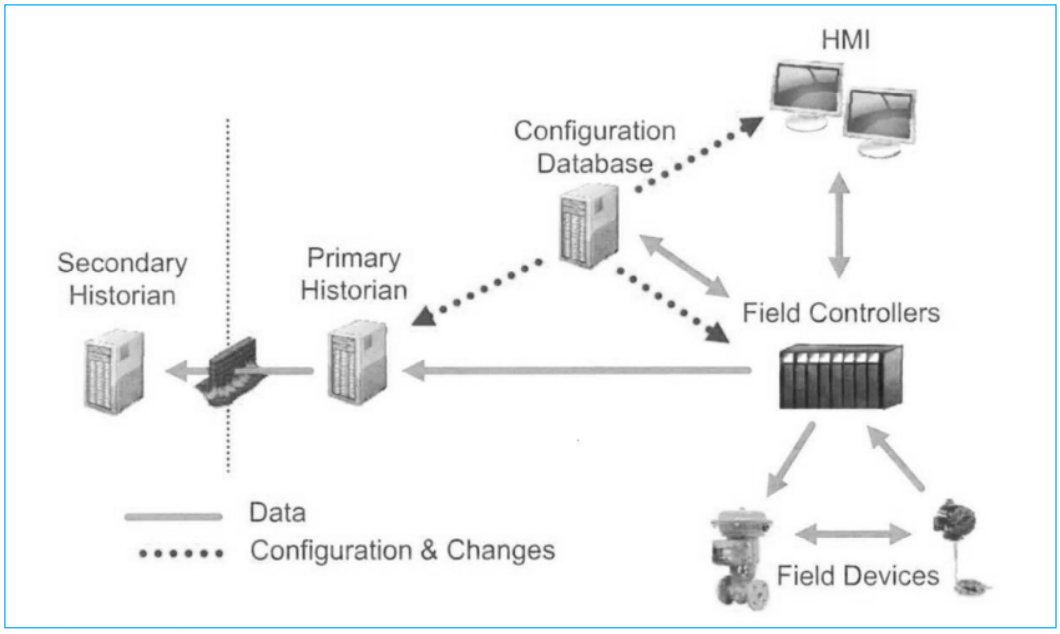
SaskEnergy monitors its compressor stations, pipelines, and all related equipment using data collected by its SCADA system. Field devices continuously read data from compressor stations, pipelines, and related equipment. For example, the data may include the natural gas flow rate through the pipeline, pipeline pressure, and temperature readings. The information obtained by field devices is conveyed in real time via a telecommunications system (i.e., SaskTel) to a central computer system. The central computer system includes a console that is monitored by operators. The console is referenced as HMI in **Figure 1** below. Monitoring enables operators to take timely actions for equipment malfunctions, leaks, or other unusual activity. SaskEnergy's SCADA system allows operators to remotely operate equipment by sending requests back to field devices. Operators are to monitor data at all times.

Field devices are programmed to perform specific functions at specified intervals. The security of the field devices is important. Inappropriate or unauthorized changes could halt or alter the information sent to operators or alter how critical equipment functions.

All data received by the SCADA system is stored in computers known as historians. The historian allows for trending and other analytical auditing.

Figure 1 shows the flow of data and changes in a typical SCADA system.

Figure 1—Flow of Data and Changes in a Typical SCADA System



Source: Intermediate Cybersecurity for Industrial Control Systems, Homeland Security, p.12

6.0 Interdependency of Saskatchewan's Major Utility Providers

There are critical relationships among the province's utility providers (i.e., SaskTel, SaskPower, and SaskEnergy). These providers are interdependent, such that a failure to provide services by one of the providers could lead to the failure of services provided by the others.

SaskPower is a key user of natural gas delivered by SaskEnergy. SaskPower operates six natural gas power plants that supply about 32% of the province's electricity.[2] The sudden loss of a source of power generation can have a significant impact on the reliability of interconnected electric systems. For example, if SaskEnergy experienced a significant disruption affecting natural gas flow to SaskPower, SaskPower could experience a reduction in power supply to its customers.

SaskEnergy relies on communication lines provided by SaskTel to receive and send data from/to natural gas facilities. SaskTel relies on SaskPower to provide electrical services.

In addition, SaskWater shares certain SCADA system infrastructure with SaskEnergy. SaskWater uses a SCADA system to monitor the quality of water provided to its customers. Therefore, a failure of SaskEnergy's SCADA system could lead to a failure of SaskWater's SCADA system.

[2] www.saskpower.com/our-power-future/power-education (13 April 2013).

7.0 AUDIT OBJECTIVE, SCOPE, CRITERIA, AND CONCLUSION

The objective of this audit was to assess whether SaskEnergy had effective processes to secure its supervisory control and data acquisition (SCADA) system used to control and monitor distribution of natural gas for the period of September 1, 2012 to February 28, 2013. Security includes the processes needed to protect the availability, integrity, and confidentiality of SaskEnergy's SCADA system and associated data.

To conduct this audit, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook - Assurance*. To evaluate the effectiveness of SaskEnergy's processes to secure its SCADA system, we examined SaskEnergy's manuals, reports, and policies and procedures. We reviewed its internal auditor's reports on SCADA system security and supporting working papers. We also visited selected sites to examine SCADA system computers and field devices.

The audit criteria are based on our related work, reviews of literature including reports of other auditors, and consultations with management. **Section 10.0** includes key sources for these criteria. SaskEnergy's management agreed with the criteria in **Figure 2**.

Figure 2—Audit Criteria

To have effective processes to secure its supervisory control and data acquisition (SCADA) system, SaskEnergy should:

1. **Maintain a security framework for SCADA system**
   - 1.1 Clearly define responsibilities for managing and securing the system
   - 1.2 Approved security policies and procedures exist and are followed
   - 1.3 Monitor and address security risks
2. **Protect SCADA system from unauthorized access**
   - 2.1 Configurations protect the system from unauthorized access
   - 2.2 User access controls protect the system from unauthorized access
   - 2.3 Physical security controls protect the system from unauthorized access
3. **Make SCADA system available for operation**
   - 3.1 System and data backups occur and are tested
   - 3.2 Disaster recovery plans are in place and tested
4. **Maintain SCADA system integrity**
   - 4.1 Monitor the system to determine if operating as planned
   - 4.2 Change management processes exist and are followed

We concluded that SaskEnergy did not have effective processes to secure its supervisory control and data acquisition (SCADA) system used to control and monitor distribution of natural gas for the period of September 1, 2012 to February 28, 2013. SaskEnergy needs to improve its processes in the following areas:

- **Prepare a complete threat and risk assessment for its SCADA system**
- **Implement complete policies and procedures to protect the confidentiality, integrity, and availability of its SCADA system**
- **Properly configure its SCADA system to protect against security threats**
- **Protect its facilities from unauthorized access**
- **Protect its SCADA system from unauthorized access**

- **Monitor SCADA system security**
- **Test its SCADA system continuity plan**

Although we have made process recommendations, we recognize that SaskEnergy has been able to provide safe and reliable operations for many years and has not experienced a major outage resulting from its SCADA system.

8.0 Key Findings and Recommendations

In this section, we set out our key findings and recommendations related to the audit criteria in **Figure 2**.

8.1 Need to Improve Security Framework

SaskEnergy is responsible for the operations of all critical SaskEnergy infrastructure including the SCADA system, overseeing natural gas distribution, and managing compressor stations. SaskEnergy has qualified employees assigned to monitor its SCADA system. Hiring policies include a review of credentials, reference checks, and criminal record checks.

SaskEnergy has identified key organizational risks. However, it has not completed a formal assessment of the threats and risks related to its SCADA system. Threat and risk assessment processes would allow SaskEnergy to assess, identify, and mitigate the overall level of risk to which they are exposed. Threat and risk assessment processes can assist SaskEnergy in prioritizing and allocating resources. The threat and risk assessment should be completed and senior management and the Board should review and approve the assessment. Exposure to unidentified or unmitigated risks could lead to a failure to meet business objectives including the loss of availability of the SCADA system and related critical infrastructure.

1. **We recommend that SaskEnergy Incorporated complete a threat and risk assessment of its supervisory control and data acquisition system.**

SaskEnergy has some corporate information technology policies and procedures. While many of its corporate policies apply to information technology systems in general, high security and availability requirements result in specific needs for SCADA systems. SaskEnergy does not have complete policies and procedures for its SCADA system. For example, SaskEnergy has policies and procedures for user access and antivirus updates but does not have complete and approved policies and procedures for monitoring and making changes to security equipment (e.g., firewalls), physically securing field devices and computer equipment at compressor stations, and managing incidents. Further policies may be needed once a threat and risk assessment is complete. Without complete policies and procedures, SaskEnergy's SCADA system is at risk of unauthorized alteration or loss of availability.

2. **We recommend that SaskEnergy Incorporated implement complete policies to protect the confidentiality, integrity, and availability of its supervisory control and data acquisition system based on a threat and risk assessment.**

Periodically, the Board and senior management have received reports about the security of the SCADA system. For example, SaskEnergy's internal auditor reported its audit findings on SCADA system security to the Board and management in 2010 and 2012. Management also advised the Board about a security incident that impacted SaskEnergy's SCADA system in 2011. The Board periodically monitors management's progress towards addressing the internal auditor's findings on SCADA system security.

As described above, SaskEnergy has not prepared a threat and risk assessment or implemented effective policies and procedures to protect its SCADA system. As a result, the Board did not receive complete risk assessment results or periodic reports on compliance with SCADA system policies and procedures.

8.2 Need to Protect SCADA System From Unauthorized Access

SaskEnergy did not securely configure its SCADA system. The SCADA system should be protected from other networks including SaskEnergy's corporate network.

The SCADA system should also have effective controls to detect unauthorized changes or other potentially malicious activity. Network security equipment should log security alerts, errors, and warning messages. SaskEnergy needs to improve its processes to monitor security logs.

Effective security configuration and timely review of security logs can prevent and detect potential cyberattacks before a breach occurs.

3. **We recommend that SaskEnergy Incorporated configure its supervisory control and data acquisition system network to protect it from security threats.**

4. **We recommend that SaskEnergy Incorporated monitor the security of its supervisory control and data acquisition system.**

Management is working to implement stronger security controls to protect the SCADA system network, computers, and related equipment.

SaskEnergy has policies and procedures for granting and removing user access to its SCADA system. SaskEnergy uses a standard form to document user access approvals.

Existing staff who no longer require SCADA system access and past employees were removed on a timely basis. Management also reviews user access lists for the SCADA system on a periodic basis.

The primary SCADA system, including physical access to the HMI and other SCADA system components, is appropriately physically secured. Staff are physically present 24 hours a day. Key card access is required.

SaskEnergy needs to improve its policies and procedures for controlling physical access to some of its facilities. The facilities are surrounded by wire fences that are locked at night. However, we found SaskEnergy needs to better protect SCADA computer equipment in use at its facilities.

5. **We recommend that SaskEnergy Incorporated effectively restrict physical access to its facilities.**

6. **We recommend that SaskEnergy Incorporated effectively restrict access to its supervisory control and data acquisition system.**

8.3 Business Continuity Plan Not Tested

SaskEnergy has policies and processes for SCADA system backups. Backup data was sent to a contingency site on a daily basis. The contingency site includes a fully operational SCADA system with up-to-date data. During the audit period, SaskEnergy successfully tested the processes to make its contingency site available for use.

SaskEnergy prepared a business continuity plan for the business unit that manages its SCADA system. The business continuity plan sets out some scenario assumptions such as the loss of its SCADA system. The plan also sets out general strategies and steps needed for assessing situations and taking action. SaskEnergy's current business continuity plan was prepared in September 2012 and has not yet been tested.

Testing a business continuity plan that allows for various interruption scenarios that would allow SaskEnergy to determine if its business continuity plan can effectively address varying risks. In addition, given the interdependencies between provincial utility providers, SaskEnergy may want to consider planning and testing for scenarios that involve interruption of services from other utility providers.

SaskEnergy should consider interdependency risks as part of the threat and risk assessment we described earlier in this chapter. SaskEnergy may need to update its business continuity processes based on the results of a threat and risk assessment.

7. **We recommend that SaskEnergy Incorporated test its business continuity plan for its supervisory control and data acquisition system to verify its effectiveness.**

8.4 Processes to Maintain System Integrity Needed

SaskEnergy uses operators to monitor whether the SCADA system is operating as planned. Operators monitor the SCADA system at all times. Operator actions (e.g., open/close a pipeline valve) are monitored. SaskEnergy reviews actions taken by junior operators.

SaskEnergy does not have complete incident management policies and procedures for its SCADA system. Procedures help guide employee responses to reduce risk to the organization and ensure that proper communications or protocols are followed in emergencies. Procedures also help to ensure proper documentation and debriefing following an incident to help the organization improve and reduce future risk from similar incidents. We report the need for SaskEnergy to implement complete policies and procedures for its SCADA system earlier in **Section 8.1**.

SaskEnergy's SCADA system needs to be updated for known security risks on a timely basis. Effective August 2, 2012, SaskEnergy contracted with its SCADA system vendor to provide change management services for all SCADA system computers. The vendor is required to update all SCADA system computers every six months, plus one ad hoc update per year at SaskEnergy's request. SaskEnergy's threat and risk assessment should consider whether the update frequency is sufficient to effectively protect its SCADA system computers.

At March 31, 2013, the SCADA system computers managed by the vendor were up to date. However, the vendor is not responsible for updating other equipment (e.g., firewalls) required to operate the SCADA system network. SaskEnergy does not have policies and procedures for updating equipment that is not managed by its vendor. We include this weakness as part of the policy and procedure weakness reported in **Section 8.1** and the security configuration weakness reported in **Section 8.2**.

9.0 Glossary

Backup—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Business Continuity Plan—A plan for an organization to carry on providing key programs and services after a serious disruption or emergency. The part of a business continuity plan that relates to restoring IT systems and data is often called a disaster recovery plan.

Change management—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

Configure—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

Firewall—Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

Intrusion detection system—Software and/or hardware intended to detect malicious activity or policy violations on a network or computer.

Network—A group of computers that communicate with each other.

Physical access controls—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Server—A computer that hosts systems or data for use by other computers on a network.

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

10.0 Selected References

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants. (2009). *Trust Services Principles, Criteria, and Illustrations*. Toronto: Author.

Government of Canada. (2010). *Canada's Cyber Security Strategy*. Canada: Author.

Idaho National Laboratory. (2006). *Control Systems Cyber Security: Defence in Depth Strategies*. Idaho: U.S. Department of Homeland Security.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management*; 2nd Edition. Geneva: Author.

Office of the Auditor General of Canada. (Fall 2012). Protecting Canadian Critical Infrastructure Against Cyber Threats. Retrieved from http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf (11 April 2013).

Stamp, Jason, et al. (2003). *Sustainable Security for Infrastructure SCADA*. New Mexico: Sandia Corporation.

Tenable Network Security, Inc. (2008). *Protecting Critical Infrastructure – SCADA Network Security Monitoring* (Revision 6). Author.

The Information Systems Audit and Control Foundation. (2007). *CoBiT4.1*. Rolling Meadows, IL: Author.

Transportation of Natural Gas. (2011). Retrieved from http://www.naturalgas.org/naturalgas/transport.asp (11 April 2013).

U.S. Department of Homeland Security. (Not dated). *Intermediate Cybersecurity for Industrial Control Systems* [Presentation]. Washington, D.C.: Author.

U.S. Department of Homeland Security. (Not dated). *Introduction to Control Systems Cybersecurity*. Washington, D.C.: Author.