

Energy—IT Security for Industrial Control Systems in Alberta’s Electrical Industry

SUMMARY

Industrial control systems¹ help control industrial processes. ICS devices are widely used in Alberta’s electrical industry and are generally controlled by instructions received from information technology devices.

The electrical industry uses ICS to control and monitor critical components such as turbines and circuit breakers in power generation and distribution. These control systems help to ensure electricity reaches Albertans and other markets efficiently, safely and securely. Therefore, IT security² must be carefully considered when designing and using ICS.

We decided to audit ICS because we believe Albertans may be at risk if ICS are unsecured or do not meet minimum IT security standards.

The Alberta Utilities Commission is a provincial agency that provides independent, adjudicative functions. The AUC is accountable to the Legislature through the Minister of Energy, who is designated the responsible minister.³ The Government of Alberta has given the AUC a regulatory mandate over the utilities sector, and natural gas and electricity markets to protect the social, economic and environmental interests of Alberta where competitive market forces do not. The AUC also establishes mandatory requirements and standards of practice for the retail electric markets through the use of a rule-making procedure involving a consultative process with stakeholders and interested parties.

On September 15, 2015 the AUC approved mandatory IT security standards for ICS in the electrical industry. Although some electrical operators may have already implemented IT security standards for ICS, they do not have to comply with these new standards until October 2017.

What we examined

We examined the Alberta Utilities Commission’s role in:

- assessing risks and developing, implementing and communicating adequate IT security standards for ICS to mitigate those risks
- monitoring operators in the electrical industry for compliance with IT security standards for ICS and enforce compliance with the standards

¹ These systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) and other types of control systems.

² IT security is the protection of information technology systems against unauthorized access or modification of data in storage, processing, or transit, and the hardware on which the data resides.

³ <http://finance.alberta.ca/publications/budget/budget2015/energy.pdf>

Overall conclusion

The AUC fulfilled its role and followed its processes, as required by regulation, to adjudicate⁴ and approve the IT security standards recommended by the Alberta Electric System Operator (AESO). However, Alberta's electrical operators do not have to comply with the newly-approved IT security standards until October 2017.

What we found

The AUC and AESO have clear roles and responsibilities for developing and approving IT security standards for ICS used by Alberta's electricity operators. The AESO's role is to develop and recommend the standards. The AUC's role is to approve the recommended standards. If there are objections to the standards from electrical industry operators or Albertans, the AUC is required to assess the objections before deciding whether to approve the recommended standards.

Why this is important to Albertans

Electricity is essential to modern life. Disruption or loss of electricity from accidental or targeted disruption to Alberta's electricity grid could harm the safety of Albertans or the environment.

AUDIT OBJECTIVE AND SCOPE

Our audit objective was to determine what the AUC's role is with respect to objections and complaints filed in connection with the approval of the Alberta Reliability Standards - IT security standards for ICS, and if there are effective AUC processes to carry out that role.

We conducted our field work between January and July 2015. We substantially completed our audit on September 18, 2015. Our audit was conducted in accordance with the *Auditor General Act* and the standards for assurance engagements set out in the CPA Canada Handbook—Assurance.

FINDINGS

The AUC followed its processes to approve IT security standards

Background

Alberta's electrical industry relies on critical infrastructure to safely and efficiently generate and deliver electricity to Albertans and to other national and international markets. ICS are a critical part of electrical operators' efforts to monitor and ensure safe and reliable operations. If the ICS devices are not secure, they could be misused to cause damage to critical infrastructure (e.g., electrical generation stations, high voltage power lines), resulting in harm to Albertans or the environment.

The electrical industry uses ICS to control and monitor critical components such as turbines and circuit breakers in power generation and distribution. IT security for ICS is a critical part of decisions about the design of these controls and their use in operations. In essence, these ICS help ensure electricity reaches all Albertans efficiently, safely and securely.

For the safety of Albertans, Alberta's environment and its economy, it is important to regularly assess IT security risks in the electrical industry and implement IT security standards to mitigate the identified risks.

⁴ That is, to make a formal judgment or decision about a problem or disputed matter.

The *Transmission Regulation*⁵ under the *Electric Utilities Act*⁶ gives the AESO the authority to develop reliability standards for Alberta’s electrical industry based on the North American Electric Reliability Council’s (NERC) standards.⁷ NERC implemented IT security standards in 2008 and the AESO started a process to adopt those standards in 2012.

The *Transmission Regulation* under the *Electric Utilities Act* also:

- requires the AESO to submit proposed reliability standards to the AUC with its recommendation to approve or reject them
- requires the AUC to follow the AESO’s recommendation unless a third party can show that the standards are technically deficient or they are not in the public interest

Criteria: the standards for our audit

The AUC should have effective processes to assess objections to Alberta Reliability Standards dealing with ICS IT security standards for Alberta’s critical electrical infrastructure.

Our findings

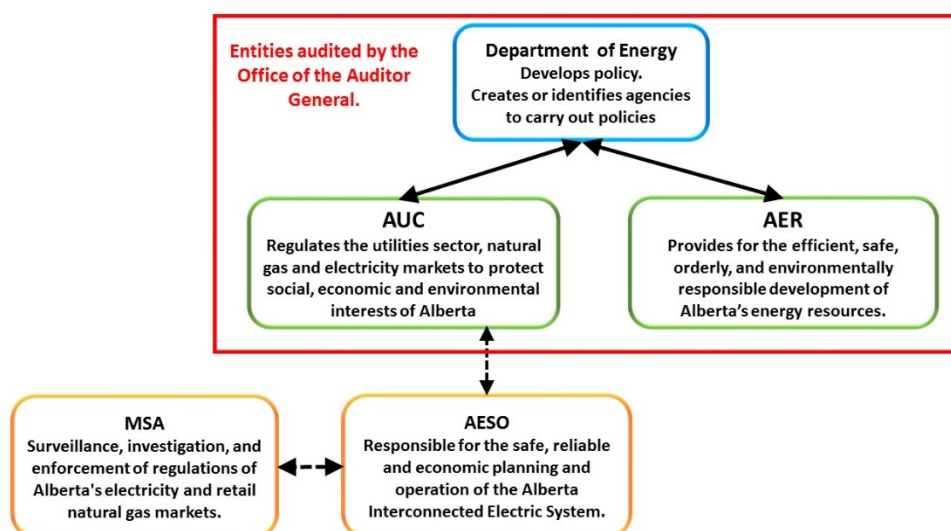
KEY FINDINGS

- The AUC followed its processes to assess the IT security standards recommended by the AESO and to adjudicate the objections from the electrical industry.
- The AUC approved the recommended IT security standards for ICS. Alberta’s electrical operators must comply with the standards by October 2017.

The AUC reviewed and approved the security standards

The AESO developed NERC-based IT security standards to protect Alberta’s electrical infrastructure. In September 2014 the AESO put forward the IT security standards to the AUC with a recommendation to approve the standards. However, electrical operators objected to implementation costs and the effective dates of the standards.

We are not the auditor of the AESO or the Market Surveillance Administrator.⁸ We did, however, talk to the AESO about its process to develop the Alberta Reliability Standards for IT security. The AESO provided us with versions of the standards they sent to the AUC.



⁵ *Transmission Regulation*—Alberta Regulation 86/2007

⁶ *Electric Utilities Act*—Statutes of Alberta, 2003, Chapter E-5.1

⁷ <http://www.nerc.com/pa/stand/Pages/default.aspx>

⁸ The *Electric Utilities Act* states the AESO and Market Surveillance Administrator are not provincial corporations for the purposes of the *Financial Administration Act* or the *Auditor General Act*.

We reviewed, but did not audit or assess, the AESO's processes to develop, or to monitor and enforce IT security standards for Alberta's electrical industry. Our review of the documentation did not identify anything to suggest the AESO cannot develop a reasonable set of ICS IT security standards based on electrical industry best practices.

The AUC has defined its processes to assess objections to proposed standards before making a decision to approve or reject the standards.

The AUC followed its adjudicative processes to assess the electrical operators' objections and decide whether to approve or reject the AESO's reliability standards for IT security. The AUC approved the IT security standards after its review on September 15, 2015.

The standards are now approved. The *Transmission Regulation* gives the AESO and Market Surveillance Administrator the authority to monitor and enforce the industry's compliance with the reliability standards. However, Alberta's electrical operators do not have to comply with the standards until October 2017.