Energy—IT Security for Industrial Control Systems in Alberta's Oil and Gas Industry

SUMMARY

Industrial control systems[1] help control industrial processes. ICS are widely used in Alberta's oil and gas industry and are generally controlled by instructions received from information technology devices.

ICS devices are part of the critical infrastructure the oil and gas industry uses to produce and safely deliver energy products to provincial, national and international markets. The industry uses ICS to control pumps and valves and to detect leaks in pipeline operations, for example. These control systems help to ensure oil and gas reaches Albertans, refineries and other markets efficiently, safely and securely. Therefore, IT security[2] 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. Oil and gas operators with inter-provincial or international operations may already follow international ICS IT security standards. However, the Alberta government does not currently require provincially regulated oil and gas operators to meet ICS IT security standards.

What we examined

We examined the roles the Department of Energy, Alberta Energy Regulator and the Department of Justice and Solicitor General have to:

- assess risks[3] to Alberta caused by possibly unsecured ICS used in provincially regulated oil and gas infrastructure
- assess whether provincially regulated oil and gas operators have adequate IT security standards for their ICS

Overall conclusion

The Department of Justice and Solicitor General has assessed the threat of attack on Alberta's oil and gas industry through ICS and concluded that it is low. However, no Alberta government entity has assessed the impact of an attack if one were to occur.

What we found

The Department of Energy manages Alberta's non-renewable resources and protects the interests of Albertans. The department has not assessed IT security risks to ICS in Alberta's oil and gas infrastructure.

[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 protection of the hardware on which the data resides.
[3] A risk assessment identifies threats and the risks and impact if those threats are carried out.

The Alberta Energy Regulator is the provincial agency that carries out oil and gas regulatory functions for which the Minister of Energy is accountable.[4] The Alberta government has given the AER a mandate to ensure Alberta's energy resource policies and regulations are efficient and effectively support public safety and environment management.[5] However, the AER has not assessed IT security risks to ICS in Alberta's oil and gas infrastructure.

The Department of Justice and Solicitor General gathers intelligence to identify security threats to Alberta's critical infrastructure. It has assessed the threat of attacks on Alberta's oil and gas industry as low, but it has not assessed what the risks or impact might be if there was a successful attack on Alberta's oil and gas infrastructure.

Ultimately, the oil and gas operators are responsible for the security of the ICS devices they use and the results of any unauthorized use or attack on their infrastructure.

What needs to be done

The Department of Energy and Alberta Energy Regulator need to decide if they should assess IT security risks to ICS in Alberta's provincially regulated oil and gas industries.

Why this is important to Albertans

The Department of Energy and the Alberta Energy Regulator should understand the risks and impact to Albertans from unsecured ICS.

AUDIT OBJECTIVE AND SCOPE

Our audit objective was to determine if the Department of Energy and Alberta Energy Regulator understand the risks from unsecured ICS, and what, if any, role they should play in ensuring those risks are adequately mitigated.

We conducted our field work between January and July 2015. We substantially completed our audit on November 9, 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 AND RECOMMENDATIONS

Unsecured ICS and risk

Background

Alberta's oil and gas industry relies on critical infrastructure to extract, refine and transport its products and safely deliver those products to provincial, national and international markets. Industrial control systems are a key component of energy operators' efforts to monitor and ensure safe and reliable operations. For example, pipeline operators use ICS to control pumps and valves and to detect leaks or other problems. If the ICS are not secure, they can be misused to cause damage to critical infrastructure (e.g., oil wells, pipelines and refineries), resulting in harm to Albertans or the environment.

[4] http://finance.alberta.ca/publications/budget/budget2015/energy.pdf
[5] http://www.aer.ca/about-aer/what-we-do

In 2010 the world learned that a virus, called Stuxnet, successfully attacked the ICS used in Iranian nuclear facilities. The Stuxnet virus attacked programmable logic controllers, a type of ICS. Recently, a German steel mill's ICS were attacked by manipulating and disrupting ICS so that a blast furnace could not be shut down, which resulted in "massive physical damage."[6]

Alberta is not immune to security risks from ICS. For example, there was a sophisticated cyber attack against a Calgary-based company's systems.[7] The company supplies ICS remote administration and monitoring tools and services to the energy sector in Alberta. Attacks on industry exploiting unsecured ICS are not common and may not be an immediate risk to Alberta's oil and gas industry. However, if those who want to harm Alberta's oil and gas industry obtain the skills needed to do so, the risks to Alberta increase.

We spoke with oil and gas operators in Alberta, with national and international operations, about their ICS controls. The operators we talked to had, or were implementing, IT security standards to comply with national and international standards. But provincially regulated oil and gas companies do not have to comply with minimum IT security standards for ICS. ICS devices that are not configured to a minimum IT security standard are at a higher risk of cyber exploitation or attack.

Similar to home computers, ICS used in Alberta's oil and gas industry need to be regularly updated and secured to protect them against unauthorized access and malicious use. Most ICS began as proprietary, stand-alone collections of hardware and software that were walled off from the rest of the world and isolated from most external threats. Today, widely available software applications, internet-enabled devices and other non-proprietary IT offerings have been integrated into most such systems. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems.[8] When ICS are not updated or maintained to a minimum security level, they are at increased risk of cyber attacks that could disrupt Alberta's energy industry and harm Albertans and the environment.

RECOMMENDATION 2: FURTHER ASSESS PROVINCIALLY REGULATED INDUSTRIAL CONTROL SYSTEMS

We recommend that the Department of Energy and Alberta Energy Regulator work together to determine whether a further assessment of threats, risks and impacts to industrial control systems used in provincially regulated oil and gas infrastructure would benefit Alberta.

[6] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
[7] http://www.securityweek.com/telvent-hit-sophisticated-cyber attack-scada-admin-tool-compromised
[8] http://www.nist.gov/el/isd/201506_ics_security.cfm

Criteria: the standards for our audit

The Department of Energy and Alberta Energy Regulator should understand whether there are threats, risks and impacts to Albertans because of unsecured ICS.

Our findings

KEY FINDINGS

- The AER asserted it does not currently have a role in assessing risks with ICS or IT security standards for Alberta's oil and gas industry.
- The Department of Energy does not believe it is responsible for determining whether ICS risks to provincially regulated oil and gas infrastructure should be assessed.
- No Alberta government entity has assessed the risks or impact to Alberta's provincially regulated oil and gas infrastructure if successfully attacked through unsecured ICS.

No one has assessed all the threats, risks and potential impact with ICS

Through meetings and discussions with the AER, we confirmed that AER has not assessed the risks to provincially regulated oil and gas infrastructure from unsecured ICS.

Through meetings and discussions with the Department of Energy we confirmed it had not determined whether risks of unsecured ICS used in provincially regulated oil and gas infrastructure require a risk assessment.

The Department of Justice and Solicitor General gathers intelligence to identify threats to Alberta's critical infrastructure. It then distributes this threat information to interested stakeholders in the oil and gas industry. But it does this only for the small percentage of provincially regulated oil and gas infrastructure identified as critical.[9] The Department of Justice and Solicitor General also works with the AER and the oil and gas operators to communicate threats it identifies.

In a recent report the Department of Justice and Solicitor General found there is currently a high threat of exploitation[10] but a low threat of cyber attack[11] to Alberta's oil and gas industry. The report also suggests that a more detailed threat and risk assessment should be conducted to better understand the threats and possible impact of an attack on Alberta's oil and gas industry. Further, the department's processes to assess and report threats would not raise its "low threat" of cyber attack until there was evidence an attack had occurred (see Figure 1 on next page).

The Department of Justice and Solicitor General used the example of a dam to better illustrate its role in assessing threats to critical infrastructure. The department assesses whether there are threats to attack the dam, then communicates with those responsible for the safety of the dam about those threats. It does not, however, assess if the control systems ensuring the safe release of water are secured from malicious use or if the dam was built to required standards. It also does not assess what the impact would be to people living downstream if there was a breach and all the water in the dam was released at once.

[9] The Department of Justice and Solicitor General has identified fewer than 50 oil and gas industry sites in Alberta as being critical.
[10] Exploitation—where bad actors gain unauthorized entry into ICS or IT systems to steal information.
[11] Cyber attack—where bad actors gain unauthorized entry into ICS or IT systems to cause physical damage to infrastructure, Albertans or the environment.

Figure 1—More information on the difference between a threat and a risk

Threat Vs Risk. **A** + **T** + **V** = **R**
Asset + Threat + Vulnerability = Risk.

An asset is what you want to protect—e.g., provincially regulated oil and gas infrastructure.

A threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage or destroy an asset.
A threat is what we're trying to protect against.

A vulnerability is a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset.
A vulnerability is a weakness or gap in our protection efforts.

The risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
Risk is the intersection of assets, threats and vulnerabilities.

We were unable to obtain any documentation from any provincial government entity to show that an assessment of the possible risks and impacts from an attack on unsecured ICS was completed.

Implications and risks if not implemented

If the Department of Energy and Alberta Energy Regulator are unaware of the possible risks and impacts from unsecured ICS, they cannot ensure that oil and gas operators are properly mitigating those risks to protect Albertans.