Industrial Control Systems Management

Background

The Direction de l'eau potable (DEP) of the Service de l'eau (SE) of the Ville de Montréal (the City) manages six drinking water production plants located on the territory of the Island of Montréal. Their total production capacity is close to three million cubic metres of drinking water per day, serving some two million citizens.

Each drinking water plant centrally controls its equipment through the Supervisory Control and Data Acquisition System (SCADA). Various other computer systems are also used for the planning, management, monitoring and control of this equipment.

More than ever, cities are facing emerging threats in the form of cyberattacks aimed at damaging, destroying or taking control of Industrial Control Systems (ICS), which could disrupt the supply of drinking water or render it unavailable and lead to several million dollars in random demands.

It is important to ensure that safety measures and industrial and technological controls are in place at the City to reduce the risks associated with these threats.

Purpose of the Audit

To determine whether the mechanisms put in place by the City ensure the sound management and high degree of availability of the Industrial Control Systems used by the DEP.

Results

We concluded that, in general, the City has put in place mechanisms to ensure the sound management and high degree of accessibility of the ICS and Information technology (IT) for the production of drinking water.

However, several elements require improvement, especially the management frameworks, the sufficiency of specialized industrial IT resources, and the management of information assets.

Nevertheless, given the presence of several compensating controls, these elements have no significant impact on the availability of the DEP's ICS and IT.

Main Findings

Management Framework and Governance

- The DEP's industrial controls are properly documented, but there is no systematic review. In addition, there are no formal IT management frameworks adapted to the reality of the DEP's environment. A document exists regarding the sharing of high-level roles and responsibilities, but it does not detail the roles and responsibilities of stakeholders in managing the DEP's ICS.

Sufficiency of Resources

- The DEP's automation resources are sufficient to meet demand. However, there is a lack of experienced industrial IT resources, both at the DEP and at the Service des technologies de l'information.

Logical Access Management

- There are no formal logical access management frameworks to manage the DEP's ICS.

Network Security

- A schematic representation of the technological architecture shows adequate network segmentation. Network security equipment is properly configured. Nevertheless, there are no formal management frameworks for ICS updates.

Systems Monitoring

- A technological tool is used to monitor the availability of the systems and to issue alerts to stakeholders. However, this tool does not cover all the systems. This monitoring is not subject to formal management frameworks.

Change Management

- Major changes are generally documented in a technological tool. However, there are no formal change management frameworks, and requests for changes are not systematically documented.

In addition to these results, we have made various recommendations to the business units, which are presented in the following pages. These business units were given the opportunity to agree to the recommendations.