# 3.7.

# Industrial Control Systems Management

Service de l'eau
Service des technologies de l'information

March 7, 2022
**2021 ANNUAL REPORT**
Auditor General of the Ville de Montréal

# 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.*

## List of Acronyms

| | |
|---|---|
| **AD** | Active Directory |
| **DEP** | Direction de l'eau potable |
| **DMZ** | Demilitarized Zone |
| **ICS** | Industrial Control Systems |
| **IDS/IPS** | Intrusion detection system/Intrusion prevention system |
| **IT** | Information technology |
| **OT** | Operational technology |
| **PI** | Plant Information |
| **RACI** | Responsible, Accountable, Consulted, Informed |
| **SCADA** | Supervisory Control and Data Acquisition System |
| **SE** | Service de l'eau |
| **STI** | Service des technologies de l'information |
| **the City** | Ville de Montréal |

# Table of Contents

# 1. Background

Created in 2005, the Service de l'eau (SE) stems from a formal desire on the part of the Ville de Montréal (the City) to structure water management activities: production, distribution and treatment. This department includes, among other things, 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. The Direction de l'eau potable (DEP) of the SE is responsible for managing all its plants.

Each drinking water plant centrally controls its equipment through the Supervisory Control and Data Acquisition System (SCADA).

The 2021 budget[1] includes $456M in investments for water infrastructure and $274M for the operation of the SE.

The Service des technologies de l'information (STI) supports the DEP in matters related to developing, technological infrastructure and IT security.

More than ever, cities are facing emerging threats in the form of cyberattacks aimed at damaging, destroying or taking control of the 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 as well as industrial and technological controls are in place at the City to reduce the risks associated with these threats.

[1] 2021–2030 TCW–Ville de Montréal.

## 2. Purpose and Scope of the Audit

Pursuant to the provisions of the *Cities and Towns Act*, we conducted a performance audit of the Industrial Control Systems Management used by the DEP. We carried out this mission in accordance with the *Canadian Standard on Assurance Engagement* (CSAE) 3001 of the *CPA Canada Handbook – Assurance*.

The purpose of this audit was to determine whether the mechanisms put in place by the City ensure the sound management and high degree of accessibility of the ICS and Information technology (IT) used by the DEP.

The role of the Auditor General of the Ville de Montréal is to provide a conclusion regarding the purpose of the audit. To that end, we gathered sufficient and appropriate relevant evidence on which to base our conclusion and obtain a reasonable level of assurance. Our assessment is based on criteria we deemed valid for the purposes of this audit. These criteria are presented in Appendix 5.1.

The Auditor General of the Ville de Montréal applies the *Canadian Standard on Quality Control* (CSQC) 1 of the *CPA Canada Handbook – Assurance* and, accordingly, maintains a comprehensive quality control system that includes documented policies and procedures with respect to compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. The Auditor General also complies with the independence and other ethical requirements of the *Code of ethics of chartered professional accountants*, which are based on the fundamental principles of integrity, professional competence and due diligence, confidentiality and professional conduct.

Our audit work covered the period from May 2021 to December 2021. Our work consisted of interviewing staff, examining various documents and conducting the surveys we deemed appropriate to obtain the necessary evidence. We also took into account information that was sent to us up to March 7, 2022.

Our work focused on the following plants and systems:

- Lachine plant: Treats drinking water for the citizens of the Lachine borough;
- Charles-J.-Des Baillets plant: Jointly with the Atwater plant, treats drinking water for the citizens of the central and eastern boroughs of Montréal;
- Supervisory Control and Data Acquisition System (SCADA): Allows for the supervision of the SE’s industrial processes, data acquisition (including measurements, alarms, level, and pressure) and remote control of the various industrial components;
- Plant information (PI)/Historian System: Allows quick access to historical, current and forecasting data from various data sources;
- CT-Logic System: Continually assesses the level of compliance of the treated drinking water with the various regulatory requirements governing the City.

These systems also include network equipment, IT servers, operating systems and databases.

At the end of our work, a draft audit report was presented for discussion to the relevant managers in the audited business units. The final report was then forwarded to the management of the business units concerned, as well as to the City's Direction Générale.

# 3. Audit Results

## 3.1. Management Frameworks and Governance

Managing the systems used by the DEP requires a vast range of expertise from, among others, Operational and Information technology (OT/IT) specialists, automation engineers, electronics technicians and operators. Most of this expertise comes from the DEP, but some is found in the STI, especially in matters dealing with computer security, the operation of IT systems, technological support, architecture, and the development of IT business solutions.

It is important, therefore, to ensure that the stakeholders involved in managing the systems have adequate documentation adapted to the reality of industrial environments.

### 3.1.1. Management Frameworks for the Systems of the Direction de l'eau potable

In general, the DEP's industrial controls are documented by automation engineers in the form of multiple directives, processes and procedures. However, there is no formal process for the periodic review of this documentation, and we noted that it is not systematically updated.

Updates are usually made at the time of a project, i.e., following major changes. It is possible, therefore, that some information contained in these documents does not reflect the current situation.

In addition, the STI has developed various IT management frameworks in the form of standards, directives and guides. These management frameworks are distributed on the City's Intranet and must be applied by all the City's departments.

However, we believe that some management frameworks should be specifically developed to meet the reality of the DEP's industrial environments. These management frameworks should cover the following processes:

- Logical access (applications and networks) management;
- All changes management;
- Systems monitoring;

- Information asset management;
- ICS updates management;
- Firewall configuration management.

In the absence of such management frameworks adapted to the reality of the DEP's industrial environments, the IT security and control measures included in the current management frameworks produced by the STI may be unable to address the DEP's issues. This would increase the risk of a cyberattack that could take control of the ICS and disrupt the treatment and delivery of drinking water to the population.

### 3.1.1.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau put in place formal management frameworks for the periodic review of industrial control documentation and ensure that it is systematically updated.

### 3.1.1.B. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau and the Service des technologies de l'information jointly put in place management frameworks adapted to the reality of the industrial environments of the Direction de l'eau potable regarding:

- Logical access (applications and networks) management;
- All changes management;
- Systems monitoring;
- Information asset management;
- Industrial Control System updates management;
- Firewall configuration management.

### 3.1.2. Roles and Responsibilities

To ensure sound governance and management of the ICS and IT used by the DEP, it is important to have formal, clear and detailed documentation regarding the roles and responsibilities of the various stakeholders involved. Such documentation could take the form of a matrix of roles and responsibilities (e.g., a RACI, "Responsible, Accountable, Consulted, and Informed") that is approved and distributed to the stakeholders, and with which they comply.

In 2019, a document regarding the high-level sharing of roles and responsibilities between the SE (including the DEP) and the STI was produced jointly by the managers of these two sectors. The table below summarizes the main elements of this sharing.

TABLE 1

## High-Level Sharing of Roles and Responsibilities

| | Roadmap | Design | Operation | Supplier management |
|---|---|---|---|---|
| Group 1 (Operational technology assets/Industrial Control Systems) | Service de l'eau | Service de l'eau | Service de l'eau | Service de l'eau |
| Group 2 (Information technology assets linked to Operational technology) | Service de l'eau /Service des technologies de l'information | Service des technologies de l'information /Service de l'eau | Service de l'eau /Service des technologies de l'information | Service des technologies de l'information /Service de l'eau |
| Group 3 (Information technology assets /business systems) | Service des technologies de l'information | Service des technologies de l'information | Service des technologies de l'information | Service des technologies de l'information |

We found that:

- Assets connected with Group 1 are those associated with the OT and ICS and fall completely under the responsibility of the SE. These assets include the SCADA, automatons[2] and telemetry systems[3];
- Assets connected with Group 2 include the IT systems used by the SE to efficiently manage its industrial environments. The design and operation of these systems are highly contextualized regarding the SE's industrial environments. These systems are partly designed, operated, supported and maintained by the SE and the STI. The assets include servers, switches, firewalls and networks;
- Assets connected with Group 3 consist of systems that are entirely managed by the STI. They include servers and applications located in the City's corporate environments. Among these are payroll processing, change management, as well as backup and email systems.

Nevertheless, this document does not provide details of how roles and responsibilities are shared between the DEP and the STI.

[2] Automaton: Programmable digital electronic device for controlling industrial processes using sequential processing.

[3] Telemetry system: Enables data acquisition using various antennas, sensors or modems installed in several different locations.

In addition, there is no formal document (e.g., a RACI) that clearly defines the roles and responsibilities of the following key stakeholders:

- The DEP's resources that perform various **industrial controls** on the ICS (e.g., developing and implementing changes, monitoring and/or running SCADA applications);
- The resources from the DEP and/or STI that perform various **IT controls** related to the DEP's computer systems (e.g., monitoring networks and servers, managing databases, updating operation systems).

The absence of such documentation increases the risk of major activities being omitted, carried out by inappropriate stakeholders or performed inadequately. The materialization of these risks could ultimately lead to water treatment errors, undetected cyberattacks and/or disruption in the distribution of drinking water to citizens.

### 3.1.2.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau and the Service des technologies de l'information jointly:

- Create a formal document that clearly defines in detail:
  - the sharing of roles and responsibilities between the Direction de l'eau potable and the Service des technologies de l'information;
  - the roles and responsibilities of the resources of the Direction de l'eau potable and of the Service des technologies de l'information that perform various Information technology controls related to the computer systems of the Direction de l'eau potable.
- Ensure the distribution, clear understanding and application of these roles and responsibilities by the stakeholders.

### 3.1.2.B. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau:

- Formally document the roles and responsibilities of the stakeholders that perform various industrial controls on the Industrial Control Systems of the Direction de l'eau potable;
- Ensure the distribution, clear understanding and application of these roles and responsibilities by the stakeholders.

## 3.2. Sufficiency and Adequacy of Resources

Maintaining sufficient qualified and experienced human resources is essential to enable the DEP to achieve its objectives and ensure that the treatment of drinking water for citizens always meets the various regulatory requirements.

During our audit, we found the following:

### The DEP's Automation Resources

The current resources (e.g., automation engineers, electronics technicians and operators) are sufficient to meet needs. We did not detect any significant issue based on the information we consulted.

### The DEP's IT Resources

The DEP has four IT positions to manage and operate the systems (comprising, in particular, servers, applications, operating systems and databases), networks and telecommunications components under its responsibility.

We observed that two of these four positions are currently vacant. Considering that the two people who recently left the DEP occupied senior positions and that the two remaining resources are more junior, this situation has resulted in a significant loss of expertise for the DEP, as well as a considerable increase in the tasks to be accomplished by the existing resources.

In addition, the DEP resources that are responsible for the ICS and/or IT systems do not have a formal training plan. Such a plan would contribute to regularly updating and upgrading their knowledge.

### STI's IT Resources

Within the STI is the Division Gestion de l'eau, which reports to the Direction Gestion du territoire. This team consists of 10 programmers/analysts (the position of division head is currently vacant but has been filled on an interim basis) and is responsible for the development and support of business solutions for the SE (e.g., scheduling application and chemical products management application). There was no significant issue observed.

The STI allocates the equivalent of one full-time resource to the SE for tasks related to computer security and another for activities related to the technological architecture. However, these are not dedicated resources with the necessary experience or expertise in OT specific to the SE's industrial environments.

During our audit, we identified the following issues:

1. Lack of resources with specific expertise related to the computer security of the DEP's industrial environments;
2. Absence of formal management frameworks specific to the DEP's industrial environments related to IT security and control (e.g., change management, logical access management, configuration of firewalls);
3. Lack of an awareness program about cybersecurity threats to industrial environments. This program should be regularly updated and distributed to the DEP's resources;
4. No evidence that the STI manages the IT security of the three groups (i.e., OT/ICS, IT linked to the OT, and business systems), as indicated in the document regarding the high-level sharing of roles and responsibilities between the SE and the STI (see Table 1 in Section 3.1.2. Roles and Responsibilities).

These issues lead us to conclude that the STI lacks sufficient qualified and experienced resources in the industrial environment field to properly support the DEP in the development and maintenance of a technological environment that meets sound security and control practices for industrial environments. Detailing the roles and responsibilities shared between the DEP and the STI, as mentioned in recommendations 3.1.2.A. and 3.1.2.B., is essential to be able to conduct a quantitative and qualitative evaluation of this lack of resources.

The lack of IT resources, both at the DEP and at the STI, could have a negative impact on the DEP's ICS and IT management and security activities. Failure to carry out these activities could lead to water treatment errors, undetected cyberattacks and/or a disruption in the distribution of drinking water to citizens.

### 3.2.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau:

- Ensure that it has the necessary Information technology resources to effectively carry out the detailed activities provided in the sharing of roles and responsibilities between the stakeholders (see recommendations 3.1.2.A. and 3.1.2.B.);
- Implement a formal training plan for the resources of the Direction de l'eau potable responsible for the Industrial Control Systems and/or Information technology systems.

### 3.2.B. Recommendation

We recommend that the Service des technologies de l'information:

- Ensure that it has the necessary Information technology resources to effectively carry out the detailed activities provided in the sharing of roles and responsibilities between the stakeholders (see recommendation 3.1.2.A.);
- Develop and distribute a systematic awareness program for the Direction de l'eau potable that tracks changes in cybersecurity threats to industrial environments.

## 3.3. Logical Access Management

Managing logical access is of paramount importance for IT security. It ensures that only authorized persons can access an organization's systems and that this access is limited to the specific needs of these individuals.

It is important, therefore, to ensure that access to the SCADA, PI/Historian and CT-Logic systems and to the Active Directory (AD) of the industrial environments meets sound logical access management practices, including the following:

- Access should be granted only to those authorized persons whose functions require such access, especially in the case of high-level access;
- Access codes should identify each user (i.e., not be generic) to ensure accountability and access traceability;
- Security parameters should ensure the robustness of the passwords, thereby contributing to reducing the risk of access by an unauthorized person.

Based on our audit, we found the following issues:

- There are no formal management frameworks adapted to the reality of the DEP governing logical access, including the granting, deletion, modification as well as review of access and remote access. This issue was raised in Section 3.1. of this report and is the subject of recommendation 3.1.1.B.;
- Three automation engineers who are users of the PI/Historian application also have administrator rights.[4] This dual access (i.e.; user and administrator) does not meet sound practices for the separation of duties;
- These same three engineers also have domain administrator rights on the AD of the industrial environment. Such rights should not be granted to them since they are not necessary for the performance of their functions.

These deviations from sound practices could increase the risk of unauthorized access and inappropriate use of these systems, which could have a negative impact on the proper functioning of the DEP's systems.

### 3.3.A. Recommendation

**We recommend that the Direction de l'eau potable of the Service de l'eau ensure that management frameworks (see recommendation 3.1.1.B.) for logical access include the following:**

- **Granting, deleting, modifying and reviewing access, along with managing remote access;**
- **Security parameters of passwords for the Supervisory Control and Data Acquisition, Plant Information/Historian and CT-Logic systems, and the industrial environment's Active Directory;**
- **Use of nominatives accounts for access to the systems;**
- **Management of administrator rights to the Plant Information/Historian systems and the industrial environment's Active Directory.**

[4] Administrator rights: Access that allows a user to perform administrative functions (e.g., adding, deleting or changing the access rights of other users).

## 3.4. Network Safety

The DEP's networks are made up of equipment (e.g., automatons, servers, firewalls, routers, switches) linked through connections (cable, wireless, radio) and communication protocols that enable the exchange of information.

Network safety consists of implementing a process to protect this equipment's components from unauthorized intrusions, changes or inappropriate disclosure (leaks) to maintain the smooth operation of these networks.

### 3.4.1. Network Architecture

A schematic representation of the network architecture is provided in the form of several documents. Some of these documents were produced in 2020, and others in 2021. They are relatively up to date. They were also approved by an authorized person. However, these documents are incomplete since they do not cover industrial field equipment (e.g., receivers, sensors, valves and pumps). This situation increases the risk of an imperfect view of the architecture's components leading to errors and/or poor decisions.

In addition, we observed the following positive elements:

- The DEP's network is properly segmented through virtual networks which are isolated from the corporate network and the Internet. This segmentation follows sound network security practices;
- The firewalls, as well as the Demilitarized Zone (DMZ),[5] are properly configured to protect the network equipment and application servers;
- The servers (i.e., SCADA, PI/Historian, CT-Logic and AD) can neither access the Internet nor be accessed from it.

#### 3.4.1.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau formally study the possibility of describing the industrial field equipment (e.g., receivers, sensors, valves and pumps) in the current documentation of the network architecture of the Direction de l'eau potable.

### 3.4.2. IT Asset Management

Managing information assets is an important part of IT security. The purpose is to ensure, among other things, that an organization's assets are accounted for, deployed and maintained. This enables organizations to systematically assess the state of each of these assets in relation to obsolescence, performance and updating of their systems.

[5] DMZ: A subsystem separated from the industrial network and isolated from the Internet by a firewall.

The IT project titled "Démarche de gestion des actifs," included in the "SE's IT Infrastructure" program, is aimed at updating the management of the SE's information assets. The project consists of the following five steps:

1. Inventory;
2. Assets and characteristics;
3. Criticality;
4. Templates;
5. Ranges.

The DEP currently uses the tool Maximo to help manage its IT assets. The level of criticality of these assets is classified based on a risk matrix focused primarily on the continuity of operations.

Based on our audit, we found the following:

- The IT project titled "Démarche de gestion des actifs" is under way. The step involving the inventory of assets has not yet been completed;
- There are no formal management frameworks for updating the ICS. This issue was raised in Section 3.1. of this report and is the subject of recommendation 3.1.1.B.

These gaps in the IT assets management could increase the risk of cyberattacks that, in turn, could lead to disruptions in the treatment and/or distribution of drinking water to citizens.

### 3.4.2.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau complete the Information technology project titled "Démarche de gestion des actifs" and ensure that it is applied by the stakeholders.

## 3.5. Systems Monitoring

Monitoring is an IT activity that makes it possible to continually supervise an IT systems' infrastructure. This monitoring is usually done using specialized software that enables administrators to supervise their systems and constantly measure the systems' availability and performance, among other things.

We found that there are no formal management frameworks for monitoring the DEP's systems. This issue was raised in Section 3.1. of this report and is the subject of recommendation 3.1.1.B.

A tool is used to monitor the availability of the systems and to issue alerts to the appropriate persons. However, this tool does not cover all the systems.

The absence of proper systems monitoring could increase the risk of outages or unauthorized intrusion attempts going undetected and corrected in a timely manner, which could affect the quality of the treatment and distribution of drinking water to the population.

### 3.5.A. Recommendation

We recommend that the Direction de l'eau potable of the Service de l'eau ensure that all its assets are automatically monitored.

## 3.6. Change Management

Managing changes to the DEP's ICS and IT is a basic element of this sector's risk control process. The objective is to ensure that any change to a production environment is recorded, evaluated, authorized, prioritized, planned, tested and implemented in a controlled way by following management frameworks that are formally documented, approved, updated and distributed and that the stakeholders comply with.

During our audit, we found the following:

- No change management frameworks exist. This issue was raised in Section 3.1. of this report and is the subject of recommendation 3.1.1.B.;
- Major changes made during projects are usually documented in Maximo (the tool used to document DEP changes). However, in the absence of formal management frameworks, it is impossible to assess the level of completeness of this documentation;
- Minor changes are not formally documented.

In addition, we conducted an efficiency test to verify to what extent the changes documented in Maximo met sound practices. To do this, we:

- Used the Maximo tool to retrieve changes (for the years 2020 and 2021) made at the Charles-J.-Des Baillets and Lachine plants involving applications included within our scope (e.g., SCADA, PI/Historian and CT-Logic);
- Sampled a change at the Lachine plant and two changes at the Charles-J.-Des Baillets plant.

After analyzing these three changes, we concluded that they failed to follow sound change management practices (e.g., absence of analysis, approval, testing, description of the solutions developed, or evidence of authorization to implement them).

Gaps in change management could increase the risk of unauthorized and undesirable changes being released, which could have major negative consequences on the integrity and availability of ICS.

Since recommendation 3.1.1.B. already covers the elements to be improved, we will not issue a new recommendation.

# 4. Conclusion

The Ville de Montréal (the City) has put in place mechanisms to ensure the sound management and high degree of accessibility of the Industrial Control Systems (ICS) used by the Direction de l'eau potable (DEP):

- The DEP's industrial controls are properly documented;
- The high-level sharing of roles and responsibilities between the stakeholders is documented;
- The DEP's automation resources are sufficient to meet needs;
- A schematic representation of the technological architecture shows adequate segmentation of the networks;
- Network safety equipment is properly configured;
- A technological tool is used to monitor the availability of the systems and to issue alerts to the appropriate persons;
- Major changes are usually documented in a technological tool.

However, several elements—that have no significant impact on the availability of the DEP's ICS and Information technology (IT)—require improvements. Below are the details based on specific evaluation criteria:

### Evaluation criterion – Management Frameworks and Governance

The ICS management frameworks have not been systematically reviewed using a formal procedure. Furthermore, there are no formal management frameworks adapted to the reality of the DEP in terms of IT controls. Such a situation could ultimately lead to inappropriate actions and interfere with the smooth operation of the DEP's systems.

The absence of a formal document detailing the roles and responsibilities of the stakeholders in managing the DEP's systems increases the risk of major activities being omitted, carried out by inappropriate stakeholders or performed inadequately.

### Evaluation criterion – Sufficiency and Adequacy of Resources

There is a lack of experienced IT resources in the industrial field at both the DEP and the Service des technologies de l'information (STI). In addition, there is no formal training plan or awareness plan to deal with cybersecurity issues in the industrial field. This could result in a negative impact on the performance of major activities related to the management and computer security of the DEP's ICS and IT.

### Evaluation criterion – Logical Access Management

There are no formal frameworks related to the management of the DEP's ICS logical access. This gap increases the risk of unauthorized access and inappropriate use of these systems.

### Evaluation criterion – Network Security

The documentation of the DEP's network architecture is incomplete.

There are no formal management frameworks related to updating the ICS. This increases the risk of cyberattacks.

### Evaluation criterion – Systems Monitoring

The tool used for automatic monitoring does not cover all the DEP's systems. As well, no formal documentation exists to provide a framework for this monitoring. This increases the risk of outages or unauthorized intrusion attempts not being detected and corrected in a timely manner.

### Evaluation criterion – Change Management

There are no formal frameworks for the management of changes to the DEP's ICS. In addition, change requests are not systematically documented. As well, the information contained in the documented changes is often incomplete or absent. These elements increase the risk of unauthorized and undesirable changes being released.

In general, the materialization of these risks could have a negative impact on the DEP's systems and, consequently, disrupt the treatment and distribution of drinking water to the citizens.

# 5. Appendix

## 5.1. Objective and Evaluation Criteria

### Objective

Determine to what extent the mechanisms put in place by the Ville de Montréal ensure the sound management of the industrial and Information technology controls of the systems used by the Direction de l'eau potable (DEP). This includes in particular aspects of governance, management frameworks, security of industrial and technological environments, training, and awareness of the risks of cyberattacks.

### Evaluation Criteria

**1. Evaluation criterion – Management Frameworks and Governance**
Management frameworks related to the Industrial Control Systems (ICS) and Information technology (IT) controls of the IT environments used by the DEP are properly documented. These documents are complete, up to date, formally approved and distributed to the stakeholders, who apply them.

The roles and responsibilities of the stakeholders involved in the ICS and IT controls of the IT environments used by the DEP are documented, complete, up to date, formally distributed to the stakeholders and applied by them.

**2. Evaluation criterion – Sufficiency and Adequacy of Resources**
There are sufficient and adequate resources in place to design and apply sound practices for the security of the ICS and IT used by the DEP.

The staff responsible for designing, operating, maintaining, supporting and securing the DEP's systems (industrial and technological) have a continuous training plan and are regularly made aware of the security rules that must be followed and the new threats that could affect the DEP's systems.

### 3. Evaluation criterion–Logical Access Management

The management of identifiers and logical access for all main ICS and IT used by the DEP follows sound practices.

### 4. Evaluation criterion–Network Security

The architecture and configuration of the networks used by the DEP follow sound practices regarding the security of the ICS.

### 5. Evaluation criterion–Systems Monitoring

The DEP's systems are subject to continual monitoring to detect various threats in a timely manner that could affect the treatment or distribution of drinking water to the population.

### 6. Evaluation criterion–Change Management

The process for managing changes to the DEP's systems follows sound practices and is systematically applied.