Management of the Metro's Industrial Control Systems

Société de transport de Montréal

3.6.

January 31, 2023

2022 Annual Report
Auditor General of
the Ville de Montréal

Management of Industrial Control Systems

Background

The Société de transport de Montréal (STM) provides the population of the Island of Montréal with public transit services, including metro, bus and paratransit.

The metro network consists of 4 lines serving 68 stations over 71 kilometres. This represents a service offer of 85.3 million kilometres travelled annually. The metro is centrally controlled by a Supervisory Control and Data Acquisition (SCADA) System, which monitors and manages the metro's operations. This management requires the use of industrial control systems (ICS) consisting of operational technology (OT) and information technology (IT).

Like all traditional information systems, the ICS can face emerging threats in the form of cyberattacks that cause damage, theft of information, and destruction or alteration of the proper functioning of the metro's ICS.

This report discusses our findings which are public in nature. A separate detailed report has been released internally only due to the highly sensitive and confidential information it contains.

Purpose of the audit

To determine whether the mechanisms in place at the STM ensure the sound management and high degree of availability of the ICS used by the metro.

Results

We conclude that management of the ICS by the STM needs improvements to ensure that it is more effectively managed and to reduce the risks of loss of availability of the metro.

Inadequate management of logical access to the ICS increases the risk of unauthorized access, which could damage the functioning of the metro. In addition, the absence of a formal IT recovery plan carries the risk of loss of availability of the ICS.

Several other elements require improvements, in particular in the areas of:

- Formalizing roles and responsibilities;
- The absence of an awareness program specific to the metro's ICS;
- Systems monitoring; and
- The comprehensiveness of the change management process.

Nonetheless, the STM has the following adequate control mechanisms:

- The Division Livraison des services technologiques métro's human resources are adequate;
- The IT/OT architecture is documented, with adequate segmentation of the networks;
- The firewalls are regularly updated.

Main Findings

Roles and responsabilities

- There is no formal document detailing the sharing of roles and responsibilities for the metro's Industrial Control Systems.

Sufficiency and Suitability of Human Resources

- The human resources in place at the Division Livraison des services technologiques métro are sufficient to meet its needs.
- There is no awareness program specific to the metro's ICS for the resources of the Division Livraison des services technologiques métro.

Management of Logical Access

- Logical access control frameworks are not adapted to the metro's ICS, nor systematically applied.

Security of the Industrial Environment Networks

- The technology architecture is documented and consists of an adequate segmentation of the networks.
- The firewalls are regularly updated.
- There is no formal assessment mechanism or procedure for installing updates on the ICS server.

Systems Monitoring

- A monitoring and security incident warning tool is in place. However, there is no monitoring framework for the metro's ICS.

Change Management

- A formal change management process is applied. However, it is incomplete according to sound industry practices.

IT Recovery of Systems

- There is no formal recovery plan for the computer systems.

In addition to these results, we formulated various recommendations to the business units, which are presented on the following pages.

List of Acronyms

ICS
Industrial control systems

IT
Information technology

OT
Operational technology

RACI
Responsible, Accountable, Consulted, Informed

SCADA
Supervisory Control and Data Acquisition System

SOC
Security Operations Centre

Table of Contents

1. Background

The Société de transport de Montréal (STM) provides the population of the Island of Montréal with public transit services, including metro, bus and paratransit.

The metro network consists of four lines serving 68 stations over 71 kilometres of underground tunnels. This represents a service offer of 85.3 million kilometres travelled annually. In 2022, a budget of $338M was allocated to the metro service.

The metro is centrally controlled by a Supervisory Control and Data Acquisition (SCADA) System that monitors and manages the metro's operations. This management requires the use of industrial control systems (ICS), consisting of operational technology (OT) and information technology (IT), to:

- Automate the processes, thereby reducing the risk of the ICS becoming unavailable and the possibility for human error;
- Accelerate responses to incidents (e.g., equipment breakdowns, computer failure) by having real-time information and adequate monitoring tools;
- Increase customer satisfaction by quickly making improvements to infrastructure and applications.

Two stakeholders are involved in managing the ICS. They report to the STM's Direction exécutive des technologies de l'information et de l'innovation:

- The Division Livraison des services technologiques métro is responsible for development, operations, change management and technology infrastructure;
- The Direction Sécurité des actifs informationnels is responsible for cybersecurity, which also includes monitoring and managing incidents, as well as staff awareness.

The threats that can affect the availability of the service provided to users come mainly from:

- Human error or equipment breakdown making metro service unavailable;
- Cyberattacks (e.g., ransomware) causing damage, the theft of information, or the destruction of or damage to the proper functioning of the metro's ICS.

Currently, every type of ICS (e.g., public transit, drinking water processing, electrical distribution) is potentially subject to these threats. It is important, therefore, to ensure that ICS monitoring measures are in place to reduce these risks

2. Purpose and Scope of the Audit and Evaluation Criteria

2.1. Purpose of the Audit

Pursuant to the provisions of the *Cities and Towns Act*, we conducted a performance audit of the management of the metro's Industrial Control Systems. We carried out this mission in accordance with the *Canadian Standard on Assurance Engagement* (CSAE) C3001 of the *CPA Canada Handbook – Assurance.*

The objective of this audit was to determine whether the mechanisms in place at the STM ensure the sound management and high degree of accessibility of the industrial control systems used by the metro.

2.2. Evaluation Criteria

Our evaluation was based on the following criteria, which we deemed to be valid under the circumstances:

1. Roles and responsabilities

The roles and responsibilities of the stakeholders involved with the industrial control systems used by the STM for the metro are formally documented, complete and up to date, and they are disseminated to them and applied by them.

2. Sufficiency and Suitability of Human Resources

The human resources available to design and apply sound practices regarding the development, operation and security of the ICS used by the STM for the metro are sufficient and suitable.

3. Logical Access Management

Logical access management of the main ICS used by the metro adheres to sound practices.

4. Security of the Industrial Environment Networks

The architecture and configuration of the networks used for the ICS adhere to sound security practices.

5. Systems Monitoring

The metro's main ICS are continually monitored to detect various threats in a timely manner that could compromise service to metro customers.

6. Change Management

The change management process for the metro's ICS (equipment and software) adheres to

sound practices and is applied systematically.

7. IT Recovery of Systems

The recovery procedure for the metro's ICS is documented and tested regularly and provides solutions in the event of a major incident (e.g., a disaster, such as a fire, forcing the evacuation of a building).

The City's Auditor General is responsible for providing a conclusion on the objective of the audit. To this end, we collected sufficient and appropriate evidence to arrive at our conclusion with a reasonable degree of assurance.

At the end of our work, an audit report was presented to the managers of the audited business units for the purpose of discussion. The final report was then forwarded to the management of the business units involved, as well as to the STM's management.

The City's Auditor General applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements.* This standard requires the City's Auditor General to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. In addition, it complies with the independence and other ethical requirements of the Code of ethics of chartered professional accountants, which are founded on fundamental principles of integrity, professional competence and due diligence, confidentiality and professional conduct.

Our audit covered the period from September 2021 to November 2022. The work consisted of interviewing staff, examining various documents and conducting surveys that we deemed appropriate to obtain the necessary evidence. We also took into consideration information that we received up to January 31, 2023.

2.3. Scope of the Audit

Our work dealt with the SCADA and the IT systems used for planning, managing, monitoring and controlling of the metro's ICS.

These systems also include network equipment, computer servers and operating systems.

This report discusses our findings which are public in nature. A separate detailed report has been released internally only due to the highly sensitive and confidential information it contains.

3. Audit Results

3.1. Roles and Responsibilities

Having formal, clear and detailed documentation of the roles and responsibilities of the various stakeholders involved is important to ensure sound governance and management of the ICS used by the metro. Such documentation can take the form of an approved roles and responsibilities matrix (e.g., RACI [Responsible, Accountable, Consulted, Informed]), disseminated to the stakeholders.

Two sectors within the Direction exécutive des technologies de l'information et de l'innovation at the STM are stakeholders on the metro's ICS:

- The Division Livraison des services technologiques metro, which is responsible for operating the ICS, such as SCADA, owned by the division;
- The Direction Sécurité des actifs informationnels, which is responsible for cybersecurity, including monitoring and managing cybersecurity, managing incidents and building awareness.

While the roles seem to be known to all, there is no formal document (e.g., a RACI matrix) detailing the sharing of roles and responsibilities for the metro's ICS for the STM.

Some documents exist detailing roles and responsibilities within the Division Livraison des services technologiques métro, especially for the automation, integration, monitoring and control sectors, as well as traffic and communications. However, these documents contain only descriptions of tasks and responsibilities and do not represent a formal RACI matrix per se.

As for the Direction Sécurité des actifs informationnels, it underwent a reorganization during the first quarter of 2022. The STM's total cybersecurity resources tripled, and a new manager was hired at the Direction. Given these recent changes, no RACI matrix has yet been documented.

The absence of such documentation increases the risk that major activities will be omitted, executed inadequately, or performed by the wrong people. The materialization of these risks could ultimately lead to a loss of effective metro operations.

RECOMMENDATION 3.1.A.

We recommend that the Division Livraison des services technologiques métro and the Direction Sécurité des actifs informationnels:

- Create a formal document detailing the sharing of roles and responsibilities between the Division Livraison des services technologiques métro and the Direction Sécurité des actifs informationnels;
- Ensure that these roles and responsibilities are disseminated to, well understood by and implemented by the stakeholders.

3.2. Sufficiency and Suitability of Human Resources

Maintaining qualified and experienced human resources in sufficient number is vital to the STM's success in achieving its objectives for metro operations.

During our audit, we found the following elements in the business units that are stakeholders in managing the metro's industrial control systems:

- **Resources of the Division Livraison des services technologiques métro**

  According to the capacity management documents provided to us, the current resources (e.g., automation engineers, network architects, operators) are sufficient to meet the operational and project needs of the metro's ICS. We did not detect any significant issues at this level based on the information provided.

- **Resources of the Direction Sécurité des actifs informationnels**

  We found that the resources of the Division Livraison des services technologiques métro lacked an awareness program specific to the ICS. As a result, the staff's knowledge may not be up to date regarding the threats that could affect the ICS.

RECOMMENDATION 3.2.A.

We recommend that the Direction Sécurité des actifs informationnels develop and implement an awareness plan for the resources of the Division Livraison des services technologiques métro specific to the industrial control systems.

3.3. Logical Access Management

Logical access management is a crucial information security control. It ensures that only authorized persons can access an organization's systems, with that access limited to what is required to perform their work.

Upon completion of our audit, we found the following shortcomings:

- While frameworks exist for logical access management at the STM, none is adapted to the reality of the metro's ICS (including granting, deleting, modifying and reviewing access and remote access);
- Contrary to the STM's procedure, access requests are not formal for one of the metro's systems;
- We were unable to obtain access review documents for access to the metro's server room. Accordingly, we are unsure whether such verification is done.

Frameworks that are not adapted and applied systematically could increase the risk of unauthorized access to the ICS.

RECOMMENDATION 3.3.A.

We recommend that the Division Livraison des services technologiques métro adapt the STM's frameworks for logical access management to the reality of the metro's industrial control systems.

RECOMMENDATION 3.3.B.

We recommend that the Division Livraison des services technologiques métro implement a recurring process to review access to the metro's server room and keep the related documents.

3.4. Security of Industrial Environment Networks

The metro's networks are composed of equipment (e.g., automatons,[1] servers, firewalls[2]) linked through cable, wireless and radio connections and communication protocols that enable the exchange of information. Networks security consists of implementing a process to maintain them in good working order by protecting their components against unauthorized intrusions, modifications or inappropriate disclosure.

During our audit, we uncovered the following positive elements:

- A network architecture was graphically depicted in the form of several documents. The documents were duly approved;
- The metro's network is adequately segmented by virtual networks. In addition, these networks are isolated from the corporate network and the Internet. This segmentation adheres to sound network security practices;
- The firewalls are regularly updated to protect network equipment and application servers;
- The servers are not accessible from the Internet, nor can they connect with the Internet.

We noted, however, that there is no formal assessment mechanism or procedure to install updates on the ICS servers. This increases the risk that important updates are not installed, which could impact the availability of the metro's ICS.

RECOMMENDATION 3.4.A.

We recommend that the Division Livraison des services technologiques métro implement a formal assessment mechanism and a procedure to install updates.

---

1 Automaton: Machine that performs tasks automatically, without human intervention.

2 Firewall: Security system designed to filter data flow between networks.

3.5. Systems Monitoring

Monitoring is a computer activity that allows for continuous surveillance of computer systems. This monitoring is generally done using specialized software that enables administrators to surveil their systems and continuously measure unauthorized access and intrusion attempts, among other things.

We found the following:

- A security incident surveillance tool was implemented in April 2022;
- A resource is dedicated to analyzing these security incidents;
- In the event that an incident occurs, an alert is sent to an on-duty resource of the STM's Security Operations Centre's (SOC) team.

However, we discovered that no formal framework exists to monitor the metro's ICS. This increases the risk that related activities will not be performed efficiently and consistently.

RECOMMENDATION 3.5.A.

We recommend that the Direction Sécurité des actifs informationnels, in collaboration with the Division Livraison des services technologiques métro, develop and implement the formal frameworks needed for sound governance of the monitoring of the metro's industrial control systems.

3.6. Change Management

The objective of change management is to ensure that all changes to a production environment[3] are recorded, evaluated, authorized, prioritized, planned, tested and implemented in a controlled manner by following formally documented, approved and updated frameworks that are disseminated to the stakeholders, who then adhere to them. This is a basic element of ICS risk management.

During our audit, we found that a formal change management process for the metro's ICS was documented, updated and known to the stakeholders. However, this process is incomplete in terms of sound industry practices.

The quality assurance team is aware of all changes to be made to the control environment. Weekly follow-up meetings are held at which changes are presented.

Our analysis of the documentation for four changes led us to conclude that there is compliance with the requirements of the STM's change management process.

With an incomplete change management process, the STM could be exposing itself to risks that impact the availability of the metro's ICS and the integrity and confidentiality of their data.

---

3 Production environment is a term used to describe the framework in which software is actually put into service for its intended end uses.

RECOMMENDATION 3.6.A.

We recommend that the Division Livraison des services technologiques métro, in collaboration with the Direction Sécurité des actifs informationnels, complete the change management process to comply with sound industry practices.

3.7. IT Recovery of Systems

Metro operations rely heavily on the ICS. It is critical, therefore, for the STM to prepare itself for any potential disaster that could disrupt or interrupt the functioning of these ICS. Threats can come from outside, such as a cyberattack, or from inside, e.g., equipment sabotage, major technical failure or equipment breakdown. The process consists, among other things, of a testing program over several years that includes recovery exercises and testing procedures, as well as solutions in the event of an incident.

While recovery tests have been conducted on all of the metro's ICS, they have not been performed regularly since 2019. We also found that there is no formal recovery plan.

The absence of a formal IT recovery plan prevents the STM from being sufficiently prepared in the event of a disaster, which could lead to interruption of metro service and increase the time required to resume operations.

RECOMMENDATION 3.7.A.

We recommend that the Direction Sécurité des actifs informationnels implement a formal IT recovery plan for the metro's industrial control systems.

4. Conclusion

The management of the metro's industrial control systems (ICS) by the Société de transport de Montréal (STM) requires improvements to ensure that these systems are managed more effectively to reduce potential risks of loss of availability of the metro.

Inadequate management of logical access to the ICS increases the risk of unauthorized access. In addition, the lack of a formal IT recovery plan carries the risk of loss of availability of the ICS.

Several other elements require improvements in the following areas:

- Formalizing roles and responsibilities;
- The absence of an awareness program specific to the metro's ICS;
- Systems monitoring;
- The comprehensiveness of the change management process.

Nonetheless, the STM has the following adequate control mechanisms:

- The human resources in place at the Division Livraison des services technologiques métro are sufficient to meet its needs;
- The technology architecture is documented and includes adequate segmentation of the networks;
- The firewalls are regularly updated;
- A technological surveillance and warning tool is used;
- There is a formal change management process that is applied and followed up.

The details below are based on the following evaluation criteria:

Roles and Responsibilities

While roles and responsibilities are known to all, the absence of a formal document that lists the stakeholders responsible for managing the metro's ICS increases the risk that major activities will be omitted, performed by the wrong people or executed inadequately. The materialization of these risks could ultimately lead to a decrease in efficiency of the metro's operations.

Sufficiency and Suitability of Human Resources

The Division Livraison des services technologiques métro has sufficient human resources. However, there is no awareness program specific to the metro's ICS for these resources. As a result, the staff's knowledge may not be up to date regarding threats that could affect the ICS.

Logical Access Management

Logical access management frameworks are not adapted to the metro's ICS, nor systematically applied. This could increase the risk of unauthorized access to the metro's ICS.

Security of the Industrial Environment Systems

The technology architecture is documented, and the metro's network is adequately segmented by virtual networks and isolated from the corporate network and the Internet. On the other hand, there is no formal assessment mechanism or procedure for installing updates on the ICS servers. This increases the risk that important updates are not installed, which could impact the availability of the metro's ICS.

Systems Monitoring

A security incident monitoring tool is in place. However, there is no formal framework for monitoring all the metro's ICS, which increases the risk that related activities will not be performed efficiently and consistently.

Change Management

A formal change management process is applied. However, it is incomplete according to sound industry practices, which could expose the STM to risks that impact the availability of the metro's ICS and the integrity and confidentiality of their data.

IT Recovery of Systems

There is no formal IT recovery plan, which prevents the STM from being sufficiently prepared in the event of a disaster. This could lead to interruption of metro service and increase the time required to resume operations.