3.7.

Gestion des systèmes de contrôle industriels

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

Le 7 mars 2022

RAPPORT ANNUEL 2021
Bureau du vérificateur général de la Ville de Montréal

Gestion des systèmes de contrôle industriels

Mise en contexte

La Direction de l'eau potable (DEP) du Service de l'eau (SE) de la Ville de Montréal (la Ville) gère notamment 6 usines de production d'eau potable situées sur le territoire de l'île de Montréal. Elles totalisent une capacité de production de près de 3 millions de mètres cubes d'eau potable par jour, et ce, afin de desservir ses quelques 2 millions de citoyens.

Chaque usine d'eau potable contrôle de manière centralisée leurs équipements par un système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA). De plus, divers autres systèmes informatiques sont utilisés pour la planification, la gestion, le suivi et le contrôle de ces équipements.

Plus que jamais, les villes sont confrontées à des menaces émergentes sous la forme de cyberattaques qui ont pour objectifs de prendre le contrôle, d'endommager ou de détruire des Systèmes de contrôle industriels (SCI), ce qui pourrait perturber ou rendre indisponible l'approvisionnement de l'eau potable et mener à des demandes de rançon de plusieurs millions de dollars.

Il est important de s'assurer que des mesures de sécurité ainsi que des contrôles industriels et technologiques sont en place à la Ville afin de réduire les risques associés à ces menaces.

Objectif de l'audit

Déterminer si les mécanismes mis en place à la Ville permettent une saine gestion ainsi qu'une haute disponibilité des Systèmes de contrôle industriels utilisés par la DEP.

Résultats

De façon globale, nous concluons que la Ville a mis en place des mécanismes permettant une saine gestion et une haute disponibilité des SCI et des technologies de l'information (TI) pour la production d'eau potable.

Cependant, plusieurs éléments nécessitent des améliorations notamment au niveau des encadrements, de la suffisance des ressources TI spécialisées dans le domaine industriel ainsi que de la gestion des actifs informationnels.

Toutefois, compte tenu de la présence de plusieurs contrôles compensatoires, ces derniers éléments n'ont pas d'impacts significatifs sur la disponibilité des SCI et TI de la DEP.

Principaux constats

Encadrement et gouvernance

- Les contrôles industriels de la DEP sont adéquatement documentés, mais il n'y a pas de révision systématique. De plus, il n'y a pas d'encadrements formels TI adaptés à la réalité de l'environnement de la DEP. Il existe un document de partage à haut niveau des rôles et des responsabilités, mais il ne présente pas les rôles et les responsabilités détaillés des parties prenantes dans la gestion des SCI de la DEP.

Suffisance des ressources

- Les ressources en automatisation de la DEP sont suffisantes afin de répondre aux besoins. Toutefois, il y a un manque de ressources TI expérimentées dans le domaine industriel tant au niveau de la DEP que du Service des technologies de l'information.

Gestion des accès logiques

- Il n'existe pas d'encadrements formels de gestion des accès logiques des SCI de la DEP.

Sécurité des réseaux

- Une architecture technologique a été schématisée avec une segmentation adéquate des réseaux. Les équipements de sécurité réseau sont adéquatement configurés. Néanmoins, il n'y a pas d'encadrements formels de gestion des mises à jour des SCI.

Surveillance des systèmes

- Un outil technologique est utilisé afin de surveiller la disponibilité de systèmes et envoyer des alertes aux parties prenantes. Toutefois, cet outil ne couvre pas l'ensemble de ces systèmes. Cette surveillance ne fait pas l'objet d'encadrements formels.

Gestion des changements

- Les changements importants sont généralement documentés dans un outil technologique. Cependant, il n'y a pas d'encadrements formels de gestion des changements et les demandes de changements ne sont pas systématiquement documentées.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées dans les pages suivantes. Ces unités d'affaires ont eu l'opportunité de donner leur accord relativement aux recommandations.

Liste des sigles

AD	*« Active directory »*
DEP	Direction de l'eau potable
DMZ	*« Demilitarized zone »*
IDS/IPS	*« Intrusion detection system/ Intrusion prevention system »*
la VILLE	Ville de Montréal
PI	*« Plant information »*
RACI	Réalisateur, Approbateur, Consulté, Informé
SCADA	Système de contrôle et d'acquisition de données *« Supervisory Control and Data Acquisition »*
SCI	Systèmes de contrôle industriels
SE	Service de l'eau
STI	Service des technologies de l'information
TI	Technologies de l'information
TO	Technologies opérationnelles

Table des matières

1. Contexte

Le Service de l'eau (SE), créé en 2005, est issu d'une volonté formelle de la Ville de Montréal (la Ville) de structurer les activités liées à la gestion de l'eau : la production, la distribution et l'assainissement. Ce Service comprend, entre autres, six usines de production d'eau potable situées sur le territoire de l'île de Montréal. Elles totalisent une capacité de production de près de trois millions de mètres cubes d'eau par jour afin de desservir ses quelques deux millions de citoyens. La Direction de l'eau potable (DEP) du SE est responsable de la gestion de l'ensemble de ses usines.

Chaque usine d'eau potable contrôle de manière centralisée leurs équipements par un système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA).

Le budget de 2021[1] prévoit des investissements totalisant 456 M$ dans les infrastructures de l'eau et 274 M$ pour le fonctionnement du SE.

Le Service des technologies de l'information (STI) soutient la DEP concernant notamment les aspects liés au développement, aux infrastructures technologiques et à la sécurité informatique.

Plus que jamais, les villes sont confrontées à des menaces émergentes sous la forme de cyberattaques qui ont pour but de prendre le contrôle, d'endommager ou de détruire les Systèmes de contrôle industriels (SCI), ce qui pourrait perturber ou rendre indisponible l'approvisionnement de l'eau potable et mener à des demandes de rançon de plusieurs millions de dollars.

Il est important de s'assurer que des mesures de sécurité ainsi que des contrôles industriels et technologiques sont en place à la Ville afin de réduire les risques associés à ces menaces.

1 PDI 2021-2030 – Ville de Montréal.

2. Objectif de l'audit et portée des travaux

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de performance portant sur la Gestion des Systèmes de contrôle industriels utilisés par la DEP. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001 du *Manuel de CPA Canada – Certification.*

Cet audit avait pour objectif de déterminer si les mécanismes mis en place à la Ville permettent une saine gestion ainsi qu'une haute disponibilité des SCI et des technologies de l'information (TI) utilisés par la DEP.

La responsabilité du vérificateur général de la Ville consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, nous avons recueilli des éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés à l'annexe 5.1.

Le vérificateur général de la Ville applique la *Norme canadienne de contrôle qualité* (NCCQ 1), du *Manuel de CPA Canada – Certification* et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Nos travaux d'audit ont porté sur la période de mai 2021 à décembre 2021. Ils ont consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'au 7 mars 2022.

Nos travaux ont porté sur les usines et les systèmes suivants :

- Usine Lachine : Assure le traitement de l'eau potable pour les citoyens de l'arrondissement de Lachine;
- Usine Charles-J.-Des Baillets : Assure, conjointement avec l'usine Atwater, le traitement de l'eau potable pour les citoyens des arrondissements du centre et de l'est de Montréal;
- Système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA) : Permet de superviser les processus industriels du SE, de réaliser des acquisitions de données (mesures, alarmes, niveau, pression, etc.) et de contrôler à distance diverses composantes industrielles;

- Système « *Plant information* » (PI)/Historian : Facilite l'accès rapide à des données historiques, actuelles et prédictives, à partir de diverses sources de données;
- Système CT-Logic : Évalue de façon continue le niveau de conformité de l'eau potable traitée par rapport aux différentes exigences réglementaires auxquelles la Ville est assujettie.

Ces systèmes incluent également des équipements de réseau, des serveurs informatiques, des systèmes d'exploitation ainsi que des bases de données.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein des unités d'affaires auditées. Par la suite, le rapport final a été transmis à la direction des unités d'affaires concernées ainsi qu'à la Direction générale de la Ville.

3. Résultats de l'audit

3.1. Encadrements et gouvernance

La gestion des systèmes utilisés par la DEP requiert une vaste gamme d'expertises provenant, entre autres, de spécialistes en technologies opérationnelles (TO) et en TI, d'ingénieurs en automatisation, d'électrotechniciens et d'opérateurs. La plupart de ces expertises proviennent de la DEP, mais certaines se retrouvent au STI, notamment en ce qui a trait à la sécurité informatique, à l'exploitation de systèmes TI, au soutien technologique, à l'architecture, ainsi que du développement de solutions d'affaires liées aux TI.

Ainsi, il est important de s'assurer que les parties prenantes à cette gestion possèdent une documentation adéquate et adaptée à la réalité des environnements industriels.

3.1.1. Encadrements liés aux systèmes de la Direction de l'eau potable

De façon générale, les contrôles industriels de la DEP sont documentés par des ingénieurs en automatisation, sous la forme de multiples directives, processus et procédures. Cependant, il n'existe pas de processus formel de révision périodique de cette documentation. Ainsi, nous constatons que cette dernière n'est pas systématiquement mise à jour.

En effet, les mises à jour se font généralement lors de projets, donc à la suite de changements importants. Ainsi, il est possible que certaines informations contenues dans ces documents ne reflètent pas la réalité actuelle.

Par ailleurs, le STI a développé divers encadrements sous la forme de standards, directives et guides en lien avec la gestion des TI. Ces encadrements sont diffusés sur l'intranet de la Ville et ils doivent être appliqués par tous les services de la Ville.

Cependant, nous sommes d'avis que certains encadrements devraient être développés spécifiquement afin de répondre à la réalité des environnements industriels de la DEP. Ces encadrements devraient couvrir les processus suivants :

- La gestion des accès logiques (applicatifs et réseaux);
- La gestion de l'ensemble des changements;
- La surveillance des systèmes;
- La gestion des actifs informationnels;
- La gestion des mises à jour des SCI;
- La gestion de la configuration des pare-feux.

En l'absence de tels encadrements adaptés à la réalité des environnements industriels de la DEP, il serait possible que les mesures de sécurité et de contrôles en technologies de l'information inclus dans les encadrements actuels produits par le STI ne répondent pas aux enjeux de la DEP. Ceci augmenterait le risque d'une cyberattaque qui prendrait le contrôle des SCI et perturberait le traitement ainsi que la livraison d'eau potable à la population.

3.1.1.A. Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de mettre en place des encadrements formels concernant la révision périodique de la documentation des contrôles industriels et de s'assurer que cette dernière est systématiquement mise à jour.

3.1.1.B. Recommandation

Nous recommandons conjointement à la Direction de l'eau potable du Service de l'eau et au Service des technologies de l'information de mettre en place des encadrements adaptés à la réalité des environnements industriels de la Direction de l'eau potable en ce qui concerne la :

- gestion des accès logiques (applicatifs et réseaux);
- gestion de l'ensemble des changements;
- surveillance des systèmes;
- gestion des actifs informationnels;
- gestion des mises à jour des Systèmes de contrôle industriels;
- gestion de la configuration des pare-feux.

3.1.2. Rôles et responsabilités

Afin d'assurer une saine gouvernance et gestion des SCI et TI utilisés par la DEP, il est important d'avoir une documentation formelle, claire et détaillée des rôles et des responsabilités des différentes parties prenantes impliquées. Une telle documentation pourrait prendre la forme d'une matrice des rôles et des responsabilités (p. ex. un RACI « Réalisateur, Approbateur, Consulté, Informé ») approuvée, diffusée et respectée par les parties prenantes.

En 2019, un document de partage à haut niveau des rôles et des responsabilités entre le SE (incluant la DEP) et le STI a été produit conjointement par des gestionnaires de ces deux secteurs. Le tableau ci-dessous résume les principaux éléments de ce partage.

TABLEAU 1

Partage à haut niveau des rôles et des responsabilités

	Feuille de route	Conception	Exploitation	Gestion des fournisseurs
Groupe 1 (actifs technologies opérationnelles / Systèmes de contrôle industriels)	Service de l'eau	Service de l'eau	Service de l'eau	Service de l'eau
Groupe 2 (actifs technologies de l'information imbriqués dans les technologies opérationnelles)	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
Groupe 3 (actifs technologies de l'information / systèmes entreprises)	Service des technologies de l'information	Service des technologies de l'information	Service des technologies de l'information	Service des technologies de l'information

Ainsi, nous observons que les :

- actifs liés au groupe 1, soient ceux associés aux TO ainsi qu'aux SCI sont entièrement sous la responsabilité du SE. Ces actifs incluent notamment les SCADA, les automates[2] et les systèmes de télémétrie[3];
- actifs liés au groupe 2 incluent les systèmes TI utilisés par le SE afin de gérer efficacement ses environnements industriels. La conception et l'exploitation de ces systèmes sont fortement contextualisées aux environnements industriels du SE. Ces systèmes sont en partie conçus, exploités, soutenuset entretenus par le SE et le STI. Ces actifs incluent notamment des serveurs, des commutateurs, des pare-feux ainsi que des réseaux;
- actifs liés au groupe 3 se composent de systèmes entièrement gérés par le STI. Ils incluent notamment des serveurs et des applications localisés dans les environnements corporatifs de la Ville. Nous y retrouvons, entre autres, les systèmes pour le traitement de la paie, la gestion des changements, ainsi que les systèmes de sauvegardes et de courriels.

Toutefois, ce document ne représente pas de façon détaillée le partage des rôles et des responsabilités entre la DEP et le STI.

De plus, il n'existe pas de document formel (p. ex. un RACI) qui définit clairement les rôles et des responsabilités des principaux intervenants suivants :

- Les ressources de la DEP qui réalisent divers **contrôles industriels** sur les SCI (p. ex. le développement et la mise en production des changements, la surveillance et/ou l'exploitation d'applications SCADA);
- Les ressources provenant de la DEP et/ou du STI qui réalisent divers **contrôles TI** en lien avec les systèmes informatiques de la DEP (p. ex. la surveillance des réseaux et des serveurs, la gestion des bases de données, les mises à jour des systèmes d'exploitation).

L'absence d'une telle documentation augmente le risque que des activités importantes soient omises, effectuées par des intervenants inappropriés ou exécutées de façon inadéquate. La matérialisation de ces risques pourrait ultimement mener à des erreurs dans le traitement de l'eau, à des cyberattaques non détectées et/ou à une perturbation de la distribution d'eau potable aux citoyens.

2 Automate : Dispositif électronique numérique programmable destiné à la commande de processus industriels par un traitement séquentiel.

3 Système de télémétrie : Permet d'effectuer l'acquisition de données à partir de différentes antennes, capteurs ou modems installés à plusieurs endroits différents.

3.1.2.A. Recommandation

Nous recommandons conjointement à la Direction de l'eau potable du Service de l'eau et au Service des technologies de l'information de :

- créer un document formel qui représente clairement et de façon détaillée :
- le partage des rôles et des responsabilités entre la Direction de l'eau potable et le Service des technologies de l'information;
- les rôles et les responsabilités des ressources de la Direction de l'eau potable et du Service des technologies de l'information qui réalisent divers contrôles en technologies de l'information en lien avec les systèmes informatiques de la Direction de l'eau potable.
- s'assurer de la diffusion, de la bonne compréhension et de la mise en application de ces rôles et ces responsabilités auprès des parties prenantes.

3.1.2.B. Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de :

- documenter formellement les rôles et les responsabilités des parties prenantes qui réalisent divers contrôles industriels sur les Systèmes de contrôle industriels de la Direction de l'eau potable;
- s'assurer de la diffusion, de la bonne compréhension et de la mise en application de ces rôles et ces responsabilités auprès des parties prenantes.

3.2. Suffisance et adéquation des ressources

Le maintien de ressources humaines qualifiées, expérimentées et en nombre suffisant est essentiel afin de permettre à la DEP d'atteindre ses objectifs et d'assurer aux citoyens le traitement d'eau potable qui répond en tout temps aux différentes exigences réglementaires.

Lors de nos travaux, nous avons constaté les éléments suivants :

Ressources en automatisation de la DEP

Les ressources en place (p. ex. les ingénieurs en automatisation, les électrotechniciens, les opérateurs) sont suffisantes pour répondre aux besoins. En effet, aucun élément d'information ne nous permet de détecter d'enjeu significatif à ce niveau.

Ressources TI de la DEP

La DEP dispose de quatre postes en TI, afin de gérer et d'exploiter les systèmes (incluant notamment, les serveurs, les applications, les systèmes d'exploitation, les bases de données), les réseaux, ainsi que les composantes de télécommunication sous sa responsabilité.

Nous observons que deux de ces quatre postes sont actuellement vacants. Considérant que les deux personnes qui ont récemment quitté la DEP occupaient des fonctions séniors et que les deux ressources restantes sont plus juniors, cette situation occasionne une perte d'expertise significative pour la DEP, ainsi qu'un accroissement considérable des tâches à réaliser auprès des ressources en place.

De plus, les ressources de la DEP ayant des responsabilités sur les SCI et / ou sur les systèmes TI ne disposent pas de plan de formation formel. Un tel plan permettrait de contribuer à l'actualisation et au rehaussement régulier de leurs connaissances.

Ressources TI du STI

Au sein du STI, nous retrouvons la Division Gestion de l'eau qui relève de la Direction Gestion du territoire. Cette équipe est composée de 10 programmeurs/analystes (le poste de chef de division est actuellement vacant, mais est assuré par intérim) et elle est responsable du développement, ainsi que du support de solutions d'affaires pour le SE (p. ex. l'application pour la gestion des horaires ainsi que pour la gestion des produits chimiques). Aucun enjeu significatif n'a été observé à cet effet.

Le STI alloue au SE l'équivalent d'une ressource à temps plein pour les tâches liées à la sécurité informatique et une autre pour les activités liées à l'architecture technologique. Toutefois, il ne s'agit pas de ressources dédiées qui possèdent nécessairement l'expérience ainsi que l'expertise en TO spécifiques aux environnements industriels du SE.

Lors de nos travaux d'audit, nous avons soulevé les enjeux suivants :

1. Le manque de ressources ayant une expertise spécifique liée à la sécurité informatique des environnements industriels de la DEP;
2. L'absence d'encadrements formels spécifiques aux environnements industriels de la DEP en matière de sécurité et contrôle informatiques (p. ex. la gestion des changements, la gestion des accès logiques, la configuration des pare-feux);
3. Pas de programme de sensibilisation face aux menaces en cybersécurité des environnements industriels. Ce programme devrait être diffusé et actualisé régulièrement auprès des ressources de la DEP;
4. Aucune évidence que le STI gère la sécurité informatique des trois groupes (c.-à-d. TO/SCI, TI imbriqués dans TO et systèmes d'entreprises), comme indiqué dans le document de partage à haut niveau des rôles et des responsabilités entre le SE et le STI (voir le tableau 1 à la section 3.1.2. Rôles et responsabilités).

Ces enjeux nous permettent de conclure que le STI ne possède pas suffisamment de ressources qualifiées et expérimentées dans le domaine des environnements industriels, et ce, afin de soutenir adéquatement la DEP dans l'évolution et le maintien d'un environnement technologique qui répond aux saines pratiques en matière de sécurité et de contrôles des environnements industriels.Afin de contribuer à l'évaluation quantitative et qualitative de ce manque de ressources, il sera essentiel de détailler les rôles et les responsabilités entre la DEP et le STI comme mentionnés dans les recommandations 3.1.2.A. et 3.1.2.B.

Le manque de ressources TI, tant à la DEP qu'au STI, pourrait avoir un impact négatif sur les activités liées à la gestion et à la sécurité informatique des SCI et TI de la DEP. La réalisation inadéquate de ces activités pourrait mener à des erreurs dans le traitement de l'eau, à des cyberattaques non détectées et/ou à une perturbation de la distribution d'eau potable aux citoyens.

3.2.A. Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de :

- s'assurer d'avoir les ressources en technologies de l'information nécessaires afin de réaliser efficacement les activités détaillées prévues dans le partage des rôles et des responsabilités entre les parties prenantes (voir les recommandations 3.1.2.A. et 3.1.2.B.);
- mettre en place un plan formel de formation pour les ressources de la Direction de l'eau potable ayant des responsabilités sur les Systèmes de contrôle industriels et/ou sur les systèmes TI.

3.2.B. Recommandation

Nous recommandons au Service des technologies de l'information de :

- s'assurer d'avoir les ressources en technologies de l'information nécessaires afin de réaliser efficacement les activités détaillées prévues dans le partage des rôles et des responsabilités entre les parties prenantes (voir la recommandation 3.1.2.A.);
- développer et de diffuser auprès de la Direction de l'eau potable un programme de sensibilisation systématique qui suit l'évolution des menaces en cybersécurité des environnements industriels.

3.3. Gestion des accès logiques

La gestion des accès logiques est un contrôle de première importance en matière de sécurité de l'information. Elle permet notamment de s'assurer que seules les personnes autorisées accèdent aux systèmes d'une organisation et que ces accès se limitent aux besoins spécifiques de ces derniers.

Donc, il est important de s'assurer que l'accès aux systèmes SCADA, PI/Historian, CT-Logic ainsi que l'« *Active directory* » (AD) de l'environnement industriels répond aux saines pratiques en matière de gestion des accès logiques, incluant notamment les éléments suivants :

- Les accès ne devraient être alloués qu'aux personnes autorisées et dont les fonctions requièrent de tels accès, particulièrement en ce qui a trait aux accès à hauts privilèges;
- Les codes d'accès devraient permettre d'identifier chaque utilisateur (c.-à-d. ne pas être générique), afin d'assurer une imputabilité et une traçabilité des accès;
- Les paramètres de sécurité devraient permettre d'assurer une robustesse des mots de passe et ainsi contribuer à réduire le risque d'accès par une personne non autorisée.

À la suite de nos travaux d'audit, nous avons constaté les enjeux suivants :

- Il n'existe pas d'encadrements formels liés à la gestion des accès logiques adaptés à la réalité de la DEP, incluant l'octroi, la suppression, la modification, la révision des accès et l'accès à distance. Cet enjeu a été soulevé dans la section 3.1. de ce rapport et fait l'objet de la recommandation 3.1.1.B.;
- Trois ingénieurs en automatisation qui sont des utilisateurs de l'application PI/Historian possèdent également des droits d'administrateur[4]. Ce double accès (c.-à-d. les utilisateurs et les administrateurs) ne répond pas aux saines pratiques en matière de séparation des tâches;
- Ces mêmes trois ingénieurs possèdent également des droits d'administrateur de domaine à l'AD de l'environnement industriel. De tels droits ne devraient pas leur être alloués, car ils ne sont pas nécessaires à la réalisation de leurs fonctions.

Ces écarts face aux saines pratiques pourraient augmenter le risque d'accès non autorisés et d'une utilisation inappropriée de ces systèmes, ce qui pourrait avoir des impacts négatifs sur le bon fonctionnement des systèmes de la DEP.

4 Droits d'administrateur : Un accès qui permet à un utilisateur d'exécuter des fonctions d'administration (p. ex. l'ajout, la suppression et la modification des droits d'accès des autres utilisateurs).

3.3.A. Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de s'assurer que les encadrements liés à la gestion des accès logiques (voir la recommandation 3.1.1.B.) incluent notamment les éléments suivants :

- L'octroi, la suppression, la modification et la révision d'accès, ainsi que la gestion des accès à distance;
- Les paramètres de sécurité des mots de passe pour les Systèmes de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* », « *Plant information* » / Historian, CT-Logic ainsi qu'à l'« *Active directory* » de l'environnement industriel;
- L'utilisation des comptes nominatifs pour l'accès aux systèmes;
- La gestion des droits d'administrateurs aux systèmes « *Plant information* » / Historian et à l'« *Active directory* » de l'environnement industriel.

3.4. Sécurité des réseaux

Les réseaux de la DEP sont composés d'équipements (p. ex. les automates, les serveurs, les pare-feux, les routeurs, les commutateurs) reliés entre eux par le biais de connexions (filaire, sans-fil, radio) et de protocoles de communication afin de permettre l'échange d'informations.

La sécurité des réseaux consiste à mettre en place un processus afin de protéger les composants de ces derniers contre les intrusions non autorisées, les modifications ou les divulgations inappropriées, et ce, afin de maintenir le bon fonctionnement de ces réseaux.

3.4.1. Architecture réseau

Une architecture réseau a été schématisée sous la forme de plusieurs documents. Certains de ces documents ont été produits en 2020 et d'autres en 2021. Donc, ils sont relativement à jour. De plus, ils ont été approuvés par une personne autorisée. Cependant, ces documents sont incomplets, car ils ne couvrent pas les équipements terrain industriels (p. ex. les capteurs, les senseurs, les valves et les pompes). Cette situation augmente le risque qu'une vue imparfaite des composantes d'architecture mène à des erreurs et / ou à de mauvaises décisions.

Par ailleurs, nous avons observé les éléments positifs suivants :

- Le réseau de la DEP est adéquatement segmenté via des réseaux virtuels. De plus, ces derniers sont isolés du réseau corporatif et d'Internet. Cette segmentation suit les saines pratiques en matière de sécurité des réseaux;

- Les pare-feux ainsi que la zone « *Demilitarized zone* » (DMZ)[5] sont adéquatement configurés pour protéger les équipements réseau et les serveurs applicatifs;
- Les serveurs (c.-à-d. SCADA, PI/Historian, CT-Logic et AD) ne sont pas accessibles à partir d'Internet et ils ne peuvent également pas atteindre ce dernier.

3.4.1.A Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau d'évaluer formellement la possibilité de schématiser les équipements terrain industriels (p. ex. les capteurs, les senseurs, les valves et les pompes) dans la documentation actuelle de l'architecture réseau de la Direction de l'eau potable.

3.4.2. Gestion des actifs informationnels

La gestion des actifs informationnels est un élément important de la sécurité de l'information. Ce processus a pour objectif d'assurer, entre autres, que les actifs d'une organisation sont comptabilisés, déployés et entretenus. Ce qui permet aux organisations d'évaluer systématiquement l'état de chacun de ces actifs concernant notamment la désuétude, la performance ainsi que la mise à jour de leurs systèmes.

Le projet TI « Démarche de gestion des actifs » inclus dans le programme « Infrastructure TI du SE » a pour objectif d'actualiser la gestion des actifs informationnels du SE. Ce projet se compose des cinq étapes suivantes :

1. Inventaire;
2. Actifs et attributs;
3. Criticité;
4. Gabarits;
5. Gammes.

Actuellement, la DEP utilise l'outil Maximo afin de l'appuyer dans sa gestion des actifs informationnels. La classification du niveau de criticité de ces actifs se fait selon une matrice de risques orientés principalement sur la continuité des opérations.

5 DMZ : Un sous-réseau séparé du réseau industriel et isolé de l'Internet par un pare-feu.

À la suite de nos travaux, nous avons observé les éléments suivants :

- Le projet TI « Démarche de gestion des actifs » est en cours de réalisation. En effet, l'étape liée à l'inventaire des actifs n'est pas complétée;
- Il n'existe pas d'encadrements formels liés à la gestion des mises à jour des SCI. Cet enjeu a été soulevé dans la section 3.1. de ce rapport et fait l'objet de la recommandation 3.1.1.B.

Ces lacunes dans la gestion des actifs informationnels pourraient augmenter le risque de cyberattaques, ce qui pourrait mener à des perturbations dans le traitement et/ou la distribution de l'eau potable aux citoyens.

3.4.2.A Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de compléter le projet en technologies de l'information « Démarche de gestion des actifs » et s'assurer de sa mise en application par les parties prenantes.

3.5. Surveillance des systèmes

La surveillance est une activité informatique qui permet la supervision continue d'une infrastructure des systèmes informatiques. Cette surveillance se fait généralement par des logiciels spécialisés qui permettent aux administrateurs de superviser leurs systèmes et de mesurer continuellement, entre autres, la disponibilité et la performance de ces derniers.

Nous avons constaté qu'il n'existe pas d'encadrements formels liés à la gestion de la surveillance des systèmes de la DEP. Cet enjeu a été soulevé dans la section 3.1. de ce rapport et fait l'objet de la recommandation 3.1.1.B.

Un outil est utilisé afin de surveiller la disponibilité des systèmes et d'envoyer des alertes aux personnes appropriées. Toutefois, cet outil ne couvre pas l'ensemble de ces systèmes.

L'absence d'une surveillance adéquate des systèmes pourrait augmenter le risque que des pannes ou des tentatives d'intrusions non autorisées ne soient pas détectées et corrigées en temps opportun, ce qui pourrait affecter la qualité du traitement de l'eau potable ainsi que sa distribution à la population.

3.5.A Recommandation

Nous recommandons à la Direction de l'eau potable du Service de l'eau de s'assurer que l'ensemble de ses actifs font l'objet d'une surveillance automatique.

3.6. Gestion des changements

La gestion des changements liée aux SCI et TI de la DEP constitue un élément fondamental du processus de contrôle des risques de ce secteur. Cette gestion a pour objectif de s'assurer que toute modification dans un environnement de production est enregistrée, évaluée, autorisée, priorisée, planifiée, testée et mise en œuvre de manière contrôlée en suivant des encadrements formellement documentés, approuvés, à jour, diffusés et respectés par les parties prenantes.

Lors de nos travaux, nous avons constaté les enjeux suivants :

- Il n'existe pas d'encadrements de gestion des changements. Cet enjeu a été soulevé dans la section 3.1. de ce rapport et fait l'objet de la recommandation 3.1.1.B.;
- Les changements importants qui se font dans le cadre de projets sont généralement documentés dans Maximo (outil utilisé notamment pour documenter les changements de la DEP). Cependant, en l'absence d'encadrements formels en place, il n'est pas possible d'en évaluer le niveau d'exhaustivité;
- Les changements mineurs ne sont pas formellement documentés.

De plus, nous avons effectué un test d'efficacité afin de vérifier dans quelle mesure les changements documentés dans Maximo respectent les saines pratiques et pour cela, nous avons :

- à partir de l'outil Maximo, extrait les changements (pour les années 2020 et 2021) liés aux usines Charles-J.-Des Baillets et Lachine qui touchent les applications incluses dans notre portée (c.-à-d. SCADA, PI/Historian et CT-Logic);
- défini un échantillon d'un changement pour l'usine de Lachine et de deux changements de Charles-J.-Des Baillets.

Après avoir analysé les trois changements retenus, nous avons constaté qu'ils ne suivent pas les saines pratiques de gestion des changements (p. ex. l'absence d'analyse, d'approbation, de tests, de description de la solution développée, d'évidence d'autorisations de mise en production).

Les lacunes dans la gestion des changements pourraient augmenter les risques de mises en production de changements non autorisés et indésirables qui pourraient avoir des conséquences négatives importantes sur l'intégrité et la disponibilité des SCI.

Nous n'émettrons pas une nouvelle recommandation puisque la recommandation 3.1.1.B. couvre déjà les éléments à améliorer.

4. Conclusion

La Ville de Montréal (la Ville) a mis en place des mécanismes permettant une saine gestion et une haute disponibilité des Systèmes de contrôle industriels (SCI) utilisés par la Direction de l'eau potable (DEP). En effet :

- les contrôles industriels de la DEP sont adéquatement documentés;
- il existe un document de partage à haut niveau des rôles et des responsabilités entre les parties prenantes;
- les ressources en automatisation de la DEP sont suffisantes afin de répondre aux besoins;
- une architecture technologique a été schématisée avec une segmentation adéquate des réseaux;
- les équipements de sécurité réseau sont adéquatement configurés;
- un outil technologique est utilisé afin de surveiller la disponibilité des systèmes et envoyer des alertes aux personnes appropriées;
- les changements importants sont généralement documentés dans un outil technologique.

Cependant, plusieurs éléments – n'ayant pas d'impacts significatifs sur la disponibilité des SCI et technologies de l'information (TI) de la DEP – nécessitent des améliorations. Plus précisément, voici les détails selon les critères d'évaluation suivants :

Critère d'évaluation – Encadrements et gouvernance

Les encadrements des SCI ne sont pas révisés systématiquement selon une procédure formelle. D'autre part, concernant les contrôles en TI, il n'existe pas d'encadrements formels adaptés à la réalité de la DEP. Une telle situation pourrait ultimement mener à des actions inappropriées et nuire au bon fonctionnement des systèmes de la DEP.

L'absence d'un document formel qui présente les rôles et les responsabilités détaillés des parties prenantes dans la gestion des systèmes de la DEP augmente le risque que des activités importantes soient omises, effectuées par des intervenants inappropriés ou exécutées de façon inadéquate.

Critère d'évaluation – Suffisance et adéquation des ressources

Il y a un manque de ressources TI expérimentées dans le domaine industriel, et ce, tant au niveau de la DEP que du Service des technologies de l'information (STI). De plus, il n'y a aucun plan de formation formel ni plan de sensibilisation face aux enjeux de cybersécurité dans le domaine industriel. Cela pourrait mener à un impact négatif sur la réalisation de certaines activités importantes liées à la gestion et à la sécurité informatique des SCI et TI de la DEP.

Critère d'évaluation – Gestion des accès logiques

Il n'existe pas d'encadrements formels liés à la gestion des accès logiques des SCI de la DEP. Ces lacunes augmentent le risque d'accès non autorisé et d'une utilisation inappropriée de ces systèmes.

Critère d'évaluation – Sécurité des réseaux

La documentation de l'architecture réseau de la DEP n'est pas complète.

Il n'existe pas d'encadrements formels liés à la gestion des mises à jour des SCI. Cela augmente le risque de cyberattaques.

Critère d'évaluation – Surveillance des systèmes

L'outil utilisé pour la surveillance automatique ne couvre pas l'ensemble des systèmes de la DEP. Également, Il n'existe pas de documentation formelle afin d'encadrer cette surveillance. Cela augmente le risque que des pannes ou des tentatives d'intrusion non autorisées ne soient pas détectées et corrigées en temps opportun.

Critère d'évaluation – Gestion des changements

Il n'existe pas d'encadrements formels liés à la gestion des changements des SCI de la DEP. De plus, les demandes de changements ne sont pas systématiquement documentées. Également, les informations contenues dans les changements documentés étaient souvent incomplètes ou absentes. Ces éléments augmentent le risque de mises en production de changements non autorisés et indésirables.

De façon globale, la matérialisation de ces risques pourrait avoir un impact négatif sur les systèmes de la DEP et, par conséquent, perturber le traitement ainsi que la distribution de l'eau potable auprès des citoyens.

5. Annexe

5.1. Objectif et critères d'évaluation

Objectif

Déterminer dans quelle mesure les mécanismes mis en place à la Ville de Montréal permettent une saine gestion des contrôles industriels et technologies de l'information (TI) des systèmes utilisés par la Direction de l'eau potable (DEP). Ceci inclut notamment les aspects de gouvernance, d'encadrements, de sécurité des environnements industriels et technologiques, de formation et de sensibilisation face aux risques de cyberattaques.

Critères d'évaluation

Critère 1 : Encadrements et gouvernance

Des encadrements liés aux Systèmes de contrôle industriels (SCI) ainsi qu'aux contrôles TI des environnements informatiques utilisés par la DEP sont adéquatement documentés. Ces documents sont complets, à jour, formellement approuvés et diffusés auprès des parties prenantes et mis en application par ces dernières.

Les rôles et les responsabilités des parties prenantes impliquées dans les SCI ainsi que dans les contrôles TI des environnements informatiques utilisés par la DEP sont documentés, complets, à jour, formellement diffusés auprès des parties prenantes et mis en application par ces dernières.

Critère 2 : Suffisance et adéquation des ressources

Des ressources suffisantes et adéquates sont présentes afin de concevoir et de mettre en application les saines pratiques en matière de sécurité des SCI et informatiques utilisés par la DEP.

Le personnel responsable de concevoir, exploiter, maintenir, soutenir et sécuriser les systèmes (industriels et technologiques) de la DEP possède un plan de formation continue et il est régulièrement sensibilisé aux règles de sécurité à respecter et aux nouvelles menaces pouvant affecter les systèmes de la DEP.

Critère 3 : Gestion des accès logiques
La gestion des identifiants et des accès logiques liés aux principaux SCI et informatiques utilisés par la DEP respecte les saines pratiques.

Critère 4 : Sécurité des réseaux
L'architecture et la configuration des réseaux utilisés par la DEP respectent les saines pratiques en matière de sécurité des SCI.

Critère 5 : Surveillance des systèmes
Les systèmes de la DEP font l'objet d'une surveillance continue afin de détecter en temps opportun diverses menaces pouvant affecter le traitement ou la distribution de l'eau potable à la population.

Critère 6 : Gestion des changements
Le processus de gestion des changements des systèmes de la DEP respecte les saines pratiques et il est systématiquement mis en application.