Guide des systèmes de surveillance vidéo

GSMGC-011 (2024)

Préparé par :
La Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
73, promenade Leikin Ottawa (Ontario) K1A 0R2
Publication publiée : 2024-05-15
Mise à jour :

Avant-propos

Guide des systèmes de surveillance vidéo (CCTV) est une publication NON CLASSIFIÉE, publiée sous l'autorité du Principal Organisme Responsable de la Sécurité Matérielle (POSM) de la GRC.

Il s'agit d'une publication du gouvernement du Canada qui servira de guide pour la conception et la mise en œuvre d'un système de CCTV pour les ministères, les organismes et les employés du gouvernement du Canada (GC).

Les suggestions de modifications et d'autres renseignements peuvent être envoyés au principal organisme de la sécurité matérielle de la GRC RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur du Guide des systèmes de surveillance vidéo GSMGC-011 est 2024-05-15.

Registre des modifications

Amendement no.	Date	Entrée par	Résumé de la modification

Remarque : Le pouvoir de modification ou de dérogation est conféré au principal organisme responsable de la sécurité matérielle de la GRC (POSM de la GRC).

Contenu

1. Introduction

La GRC, Principal Organisme Responsable de la Sécurité Matérielle (POSM) pour le gouvernement du Canada, est chargée de fournir des conseils et des directives sur toutes les questions liées à la sécurité matérielle. Cela comprend les lignes directrices pour les systèmes de surveillance vidéo (CCTV) dans les immeubles et les installations du GC.

Remarque : Ci-après, l'utilisation du CCTV dans le présent guide s'appliquera aux systèmes de surveillance vidéo.

1.1. But

Le présent guide vise à fournir aux professionnels de la sécurité du GC des renseignements sur la conception, la sélection et l'approvisionnement appropriés des systèmes et des composants de CCTV dans le cadre de la posture de sécurité globale d'une installation, y compris la gestion et la protection de l'accès, processus de détection, d'intervention et de rétablissement.

Le guide contient à la fois les mesures de contrôle de sécurité requises, indiquées par l'utilisation du mot « doit », et les mesures de contrôle de sécurité ou les lignes directrices recommandées, indiquées par l'utilisation du mot « devrait ». L'utilisation du mot « doit » indique une référence à une politique ou à une norme établie du gouvernement du Canada, tandis que l'utilisation du mot « devrait » renvoie à des conseils, à des directives ou à une pratique exemplaire.

Les mesures de sécurité physiques de base sont conçues pour assurer une protection contre les types courants de menaces auxquelles les ministères et organismes peuvent être confrontés. Certains ministères et organismes ou activités opérationnelles peuvent faire face à des menaces différentes en raison de la nature de leurs activités, de leur emplacement ou de l'attrait de leurs actifs. Par exemple, les établissements policiers ou militaires, les services de santé, les laboratoires, les installations de recherche de nature délicate, les musées, les comptoirs de services, les bureaux dans les zones à criminalité élevée et les installations situées à l'extérieur du Canada.

1.2. Applicabilité

Le présent guide s'applique aux employés et aux entrepreneurs du GC qui ont des responsabilités en matière de sécurité et de gestion immobilière des installations du GC. Cela comprend le personnel qui participe à la conception des systèmes de surveillance des installations, les dirigeants principaux de la sécurité et les gestionnaires délégués de la sécurité et de la gestion des installations, ainsi que les praticiens de la sécurité responsables de l'évaluation des menaces et des risques (EMR) et mettre en œuvre des mesures d'atténuation.

Les ministères et organismes du GC sont responsables de déterminer leurs exigences en matière de sécurité pour la sélection des sites et l'aménagement des installations, ainsi que les mesures de sécurité jugées nécessaires pour protéger les installations en fonction d'une évaluation des menaces et des risques (EMR). Cette responsabilité comprend les mesures de

sécurité (portes extérieures, CCTV et éclairage de sécurité), les systèmes de l'immeuble (systèmes mécaniques et électriques) et la sécurité des personnes (escaliers de sortie, alarmes d'incendie et gicleurs). Les exigences en matière de vidéosurveillance relèvent de cette responsabilité.

1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle

Tous les employés du gouvernement du Canada (GC) ont la responsabilité de protéger les personnes, les renseignements et les biens du GC. Il est important que les politiques et les pratiques en matière de sécurité ne servent pas d'obstacles à l'inclusion, mais soutiennent et respectent plutôt tout le personnel du GC tout en veillant à ce que les mesures de sécurité appropriées soient maintenues pour protéger le personnel, les biens et l'information du GC.

Les initiatives visant à promouvoir l'égalité et l'inclusion entre les diverses communautés et patrimoines au sein du GC devraient être respectées dans le développement et la maintenance des systèmes de sécurité matérielle. Les ministères et organismes devraient respecter toutes les lois, politiques et directives du GC sur l'équité, la diversité et l'inclusion (EDI) dans la promotion d'un milieu de travail juste et équitable pour toutes les personnes, tout en s'assurant qu'elles s'acquittent de leurs responsabilités en matière de sécurité.

Les ministères et organismes devraient mener un exercice de gestion des risques pour veiller à ce que, même si la dignité de tous est respectée, la protection des renseignements, des biens et du personnel du GC soit maintenue. Toutes les questions sur les politiques et les directives de l'EDI doivent d'abord être adressées à l'autorité ministérielle responsable.

1.4. Considérations aux technologies de l'information

Suite aux menaces qui évoluent constamment et l'intégration de la sécurité matérielle et de la technologie de l'information (TI), il est essentiel d'évaluer le risque de toute application et/ou de tout logiciel connecté à un réseau pour faire fonctionner et soutenir l'équipement dans les bâtiments contrôlés par le gouvernement du Canada.

Avant de mettre en œuvre des applications et/ou des logiciels qui contrôleront et/ou automatiseront certaines fonctions de l'immeuble, votre service de sécurité ministériel exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de s'assurer que l'intégrité et la disponibilité des composants que les applications et/ou logiciels contrôlent sont maintenues et que tout risque mis en évidence sera atténué. Il est fortement recommandé de commencer le processus SA&A tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus SA&A, veuillez consulter votre service de sécurité ministériel.

2. Coordonnées

Pour plus d'informations, contacter:

Gendarmerie royale du Canada
Principale organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

Acronyme	Signifiant
ASI	Alimentation sans interruption. Interchangeable avec UPS
CCTV	Systèmes de surveillance vidéo. Interchangeable avec CCVE
DEI	Détection électronique d'intrusion
DEL	Diode électroluminescente aussi appelée LED
DGS	Directive sur la gestion de la sécurité
DVR	Enregistreur vidéo numérique
EMR	Évaluation de la menace et des risques
GSMGC	Guide de sécurité matérielle du gouvernement du Canada
IP	Protocole Internet
ONVIF	Open Network Video Interface Forum
POSM	GRC Principal Organisme Responsable de la Sécurité Matérielle
PSG	Politique sur la sécurité du gouvernement
PSIA	Physical Security Interopérabilité Alliance
PTZ	Caméra à zoom panoramique
SA&A	Évaluation et autorisation de sécurité
SCT	Secrétariat du Conseil du Trésor du Canada

4. Glossaire

Terme	Définition
Détection électronique d'intrusion	Un système composé de capteurs qui détecte un changement d'état (mouvement, courant électrique, chaleur, codes d'accès), transmet des messages à un programme de surveillance électronique ou à un équipement de notification (sonnerie d'alarme, tableau de distribution, logiciel d'accès à distance) et permet l'analyse du changement d'état signalé (alarme sonore, Centre des opérations de sécurité, arbre d'appels/avis électronique).
Évaluation des menaces et des risques	Processus d'évaluation des biens d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques.

Interférence des signaux collatéraux	Toute perturbation involontaire des signaux de communication sans fil par d'autres signaux de fréquence présents dans la zone d'exploitation.
Multiplicateur de force	Toute action, formation, ressource ou outil qui augmente l'effet ou l'efficacité d'une action, d'un processus ou d'un système.
Open Network Video Interface Forum (anglaise seulement)	Un forum de l'industrie facilitant le développement et l'utilisation d'une norme ouverte mondiale pour l'interface des produits de sécurité physiques basés sur IP et pour la façon dont les produits IP dans la vidéosurveillance et d'autres domaines de sécurité physique peuvent communiquer entre eux.
Physical Security Interoperability Alliance (anglaise seulement)	Un groupe mondial de fabricants et d'intégrateurs de systèmes de sécurité physique promouvant l'interopérabilité des dispositifs et systèmes de sécurité IP dans le domaine de la sécurité physique et promouvant et développant des spécifications ouvertes, pertinentes pour la technologie de sécurité physique en réseau, dans tous les segments de l'industrie, y compris la vidéo, le stockage, l'analyse, l'intrusion et le contrôle d'accès.
Vidéosurveillance	Tout composant d'un système de surveillance électronique comprenant des caméras, des moniteurs, du matériel d'enregistrement et d'autres technologies pour surveiller n'importe quel espace. Interchangeable avec CCTV et CCVE.

5. Introduction aux systèmes de surveillance vidéo

La capacité de détecter et d'intervenir en cas d'urgence ou d'incident de sécurité dépend en grande partie de la capacité de surveiller continuellement une zone ou un espace. De plus, la capacité de coordonner une intervention pour contrer toute activité qui menace la sécurité des personnes ou des biens dépend de renseignements fiables, clairs et opportuns. L'utilisation de la surveillance exclusivement humaine, bien qu'efficace et hautement adaptable si elle est correctement formée, est coûteuse en termes de ressources financières et de surveillance. De plus, la surveillance humaine peut être entachée de perceptions personnelles, de préjugés, de lacunes en matière de formation et d'influence externe. Les méthodes de surveillance électronique se sont avérées plus efficaces pour fournir un enregistrement visuel impartial des événements pour le personnel de sécurité ou les premiers intervenants.

Conçue à l'origine comme un réseau de caméras reliées à un ou plusieurs moniteurs de télévision pour fournir une capacité de surveillance à distance en temps réel, la vidéosurveillance a évolué avec les progrès technologiques en matière de qualité audiovisuelle, de signaux câblés et sans-fil, d'imagerie numérique et de stockage. Aujourd'hui, les produits de vidéosurveillance à distance sont disponibles dans une grande variété d'applications et de capacités, résulter en une grande variété de terminologie. Pour faciliter la compréhension, en plus de la note de la section 1, le terme CCTV doit être utilisé dans le présent guide pour décrire tout système de surveillance électronique composé de caméras, de moniteurs, d'équipement d'enregistrement et d'autres technologies pour surveiller tout espace. Les ministères et organismes peuvent utiliser une terminologie qui répond à

leurs besoins uniques, bien que l'acronyme CCTV soit très reconnaissable et interchangeable avec de nombreux produits modernes et systèmes de surveillance vidéo.

5.1. Protection, Détection, Réponse, et Récupération

Il est important de noter que le CCTV n'empêche pas les intrusions, les activités criminelles, l'espionnage parrainé par l'État ou des entreprises, ou les incidents violents de se produire dans ou près des installations du GC. Les systèmes de CCTV ne devraient pas être utilisés dans le but de surveiller le rendement ou l'assiduité des employés, car cette pratique serait contraire aux dispositions de la Loi sur la protection des renseignements personnels qui avisent les enregistrements vidéo et les images contenant des renseignements personnels et la divulgation des enregistrements de CCTV pour une l'objet administratif exigerait le consentement de la personne. Les ministères et organismes devraient utiliser la CCTV comme technologie habilitante dans la gestion de l'accès et leurs efforts de protection, de détection, de réponse, et de récupération. Le CCTV devrait être utilisé en coopération avec des mesures et procédures de sécurité supplémentaires.

5.1.1. Protection

Un système CCTV bien conçu et bien entretenu est un multiplicateur de force qui permet aux ministères et aux organismes de surveiller en permanence les zones qui ne seraient pas possibles uniquement par une force de sécurité. La présence de caméras CCTV peut constituer une barrière psychologique ou un moyen de dissuasion contre l'intrusion.

5.1.2. Détection

Les systèmes CCTV permettent au personnel de sécurité de surveiller les zones dépourvues de personnel, les emplacements de gestion des accès, d'établir des schémas de base de mouvement à l'intérieur et à l'extérieur d'une zone ou d'une installation, d'identifier une tentative d'intrusion et d'initier une intervention. Les limites des systèmes CCTV dans la détection des intrusions sont généralement causées par une mauvaise ou une couverture insuffisante de l'espace (« angles morts »), un nombre insuffisant d'employés pour surveiller efficacement toutes les caméras ou un manque de formation sur l'équipement fourni. Par conséquent, il est important de maintenir un bon système de gestion des accès.

5.1.3. Réponse

L'utilisation d'images CCTV en direct pour coordonner une intervention par le personnel de sécurité ou d'application de la loi est une méthode efficace pour limiter les répercussions ou les dommages sur le personnel, les biens, l'information ou la réputation publique du GC. Idéalement, le système de CCTV devrait être surveillé et contrôlé à l'intérieur ou à proximité immédiate d'un centre des opérations de sécurité et soutenu par un système de communication fiable. Cela devrait permettre la surveillance en direct et l'enregistrement d'un événement actif sans interférer avec la visualisation continue d'autres caméras en direct.

5.1.4. Récupération

Afin de permettre un retour rapide aux opérations normales ou à la prestation de services, le personnel du centre des opérations de sécurité peut utiliser la vidéo CCTV en direct pour coordonner les efforts de récupération jusqu'à ce que du personnel supplémentaire soit disponible. On peut obtenir plus de renseignements sur les interventions en cas d'urgence auprès de Sécurité publique Canada.

6. Considérations de Conception

La conception de tout système CCTV devrait être fondée sur une évaluation des menaces et des risques (EMR) correctement effectuée afin de déterminer les exigences propres au site, les vulnérabilités dans les mesures de sécurité physique actuelles et les besoins ou les plans futurs de l'installation. Des considérations supplémentaires pour les ministères, les organismes et les installations à locataires multiples qui ont la garde seront déterminées dans le processus d'EMR. Des représentants des équipes de la Sécurité, de la Sûreté, de la Sécurité, de la Gestion immobilière, de l'Entretien, de la Technologie de l'information (IT) et des Ressources humaines devraient être consultés pendant la phase de conception avant la sélection d'un système CCTV. Il serait très utile d'engager les services d'un architecte / cabinet de conception CCTV professionnel pendant la phase de conception de tout projet.

6.1. Établir les Exigences

Lors de l'établissement des exigences en matière de CCTV, en fonction des vulnérabilités en matière de sûreté et de sécurité identifiées dans l'EMR, les principaux domaines de préoccupation peuvent inclure:

- **Quels domaines nécessitent une observation 24/7?** Les zones peuvent comprendre des installations de stationnement, des limites de périmètre de la propriété, des entrées et des sorties des bâtiments de l'installation et des aires d'accueil. Les renseignements de nature délicate sont-ils protégés de la vue ou de l'enregistrement du CCTV;
- **Pourquoi le CCTV est-il nécessaire ou préférable pour les zones identifiées?** Antécédents d'activités criminelles ou préoccupations en matière de sécurité, zone trop grande pour assurer une surveillance complète en utilisant uniquement le personnel de sécurité, ou d'autres raisons identifiées dans l'EMR;
- **Comment utiliser le système CCTV?** Y a-t-il des considérations opérationnelles ou juridiques qui exigent une surveillance continue ou un enregistrement de l'environnement? Une évaluation des facteurs relatifs à la vie privée (EFVP) a-t-elle été effectuée ou est-elle nécessaire;
- **Y a-t-il des exigences légales?** L'affichage de la signalisation pour informer les systèmes de vidéosurveillance est une exigence. Chaque emplacement a des exigences uniques, en vertu de la loi, et l'autorité compétente établit ce qui est requis pour la signalisation; et
- **Où et par qui le système CCTV doit-il être surveillé, contrôlé et entretenu?** Surveillance sur place ou à distance de l'imagerie CCTV, utilisation d'un centre des opérations de sécurité ou d'un service de sécurité sous contrat, ou intégration à un système de gestion des accès ou à des dispositifs d'alarme contre les intrusions?

6.2. Déterminer les contraintes et les limites

En plus des exigences en matière de CCTV établies pour contrer ou gérer les vulnérabilités relevées au cours du processus d'EMR, les ministères et organismes devraient également tenir compte des limites existantes dans la conception d'un système de CCTV.

6.2.1. Éclairage

Les ministères et organismes devraient avoir un éclairage de sécurité conforme au GSMGC-004 (2020) Guide sur les considérations relatives à l'éclairage de sécurité, car cela aidera la plupart des systèmes CCTV à capturer correctement les images pour les visualiser. S'assurer que les zones de couverture sont évaluées dans des conditions de faible luminosité et de nuit pour déterminer si un éclairage supplémentaire est nécessaire ou si le choix de caméras capables de visualiser et d'analyser les images dans ces conditions est nécessaire. Par exemple, les zones d'accès situées du côté sont ou ouest d'une installation qui auront des considérations spéciales pour le lever et le coucher du soleil; comme les caméras faisant face au soleil levant ou couchant auront des images obscurcies causées par une lumière vive, des ombres et des changements d'humidité à l'intérieur du boîtier de la caméra (buée ou glace). Un autre emplacement ou un autre angle de la caméra peut être nécessaire pour éviter ce type de vue obstruée si la caméra n'est pas équipée de la technologie pour s'adapter à ces conditions.

6.2.2. Infrastructure

Le système CCTV est-il une nouvelle installation ou le remplacement d'un système existant? Les ministères et organismes devraient évaluer le CCTV existant par rapport aux exigences établies afin de s'assurer qu'une conception inadéquate n'est pas copiée ou réutilisée pour maintenir les coûts à un faible niveau; la vulnérabilité existera toujours avec le nouvel équipement ou la nouvelle architecture. De même, il en va de même pour les systèmes de contrôle CCTV d'un centre des opérations de sécurité.

6.2.3. Environnement

Le climat du Canada varie considérablement au cours de l'année. Les systèmes CCTV doivent être efficaces dans la plage extrême de températures et de conditions météorologiques de l'emplacement employé. Par exemple, les boîtiers de caméra doivent être très résistants à l'humidité qui pénètre et cause de la glace ou de la buée qui nuirait à l'efficacité de l'objectif de la caméra. Les vents violents, la pluie et les tempêtes de neige peuvent désactiver les communications sans fil si les antennes ne sont pas conçues pour ce facteur environnemental. Les arbres et autres végétaux peuvent nuire à la vue de la caméra au moment de l'installation ou plus tard au fur et à mesure de leur croissance. Un soin particulier doit être apporté à la sélection des composants CCTV qui peuvent survivre et fonctionner correctement dans le climat de l'emplacement afin d'éviter la perte de couverture et les réparations et remplacements fréquents ou inutiles.

6.2.4. Alimentation électrique

Les composants CCTV doivent être compatibles avec l'alimentation électrique de l'emplacement. Les composants provenant de l'extérieur du pays peuvent ne pas avoir la

même tension d'entrée que l'alimentation électrique du site. La meilleure pratique consiste à vérifier que tous les composants du système sont conformes aux normes locales, telles que, 100 – 240 V. D'autres considérations relatives à l'alimentation électrique peuvent comprendre l'alimentation de secours, comme les générateurs ou l'alimentation sans interruption (ASI), ou l'utilisation de sources d'énergie de remplacement, y compris l'énergie solaire avec batterie de secours vers le haut, comme options potentielles d'alimentation électrique pour de nouveaux projets ou rénovations.

6.2.5. Capacité d'expansion

Les exigences de CCTV peuvent changer au fil du temps. Lors de la conception d'un système CCTV, il convient d'envisager l'utilisation d'une plate-forme technologique compatible avec les composants de plusieurs fabricants et capable d'expansion ou de modification future. Le fait d'avoir un système CCTV de conception modulaire qui peut être modifié plus facilement pour s'adapter à de nouvelles configurations peut réduire les vulnérabilités et les coûts futurs.

6.2.6. Facilité d'entretien

La disponibilité des pièces de rechange et des techniciens autorisés à entretenir le système devrait être une considération lors du choix d'un système CCTV et d'un contrat de maintenance. Tout retard dans la réparation d'un composant CCTV non fonctionnel augmente la vulnérabilité et le risque d'exploitation.

6.3. Interopérabilité

Les systèmes de sécurité physique sont conçus pour fonctionner de façon complémentaire afin de fournir une atténuation robuste des risques de sécurité auxquels font face les ministères et organismes. Qu'il s'agisse d'étendre un système CCTV existant ou d'en concevoir un nouveau, la capacité des composants CCTV sélectionnés à s'intégrer à d'autres technologies et processus doit être prise en compte.

6.3.1. Détection électronique d'intrusion

L'intégration du CCTV au système de détection d'intrusion d'une installation peut faciliter une évaluation rapide de toute alarme et aider le personnel intervenant à coordonner son enquête. Par exemple, les systèmes CCTV utilisant des caméras à zoom panoramique (PTZ) pourraient être déclenchés par des capteurs (détecteur de mouvement, contacts de fenêtre ou de porte, bouton de panique) diriger immédiatement une ou plusieurs caméras vers le capteur déclenché pour un examen visuel rapide de la zone d'alarme, à condition qu'il y ait une couverture redondante de la ou des zone(s) de la zone(s) PTZ vue avant l'alarme.

6.3.2. Systèmes de gestion d'accès

À l'instar d'un système intégré de CCTV et de détection électronique des intrusions, l'utilisation de CCTV pour soutenir les systèmes de gestion de l'accès serait un avantage si une installation présente un risque identifié de brèches de périmètre ou d'effraction dans une EMR. La capacité d'identifier et de suivre des personnes ou des objets avant qu'ils n'aient franchi une clôture périphérique ou n'entrent dans une installation pourrait

permettre au personnel de sécurité de coordonner les activités pour perturber ou intercepter l'intrus potentiel.

6.3.3. Systèmes et infrastructure de gestion des immeubles

L'automatisation des bâtiments et l'intégration des CCTV peuvent optimiser la surveillance des infrastructures essentielles, comme les systèmes de chauffage, de ventilation et de refroidissement (CVC), l'équipement de production d'électricité, les aires d'entreposage de matières dangereuses ou d'autres endroits où la présence humaine n'est pas constante. Si la catégorisation de sécurité de la zone surveillée le permet, la surveillance à distance de ces systèmes peut être possible dans le centre des opérations de sécurité d'une installation, le centre de commandement des CCTV, ou via un réseau de protocole Internet ou un logiciel.

6.3.4. Normes pour l'interopérabilité des technologies de protocole Internet

Les systèmes basés sur le protocole Internet, ou IP, ont la capacité de fournir des vidéos haute performance de manière rentable. En raison de la popularité de cette technologie, il est essentiel que les composants IP, au sein d'un système CCTV, soient capables de fonctionner avec l'ensemble du réseau. Les normes pour cette interopérabilité comprennent:

- Open Network Video Interface Forum (ONVIF - site Web en anglais seulement), une norme établie pour la communication de la vidéosurveillance entre les produits IP; et
- Physical Security Interoperability Alliance (PSIA - site Web en anglais seulement), une norme établie de spécifications pour les dispositifs et systèmes de sécurité IP, y compris la vidéo, le stockage, l'analyse, la détection d'intrusion et la gestion des accès.

Comme il est indiqué à la section 6.2.5, la capacité d'étendre un système CCTV existant ou futur dépend en grande partie de l'interopérabilité des composants du système. Les ministères et organismes devraient vérifier que leurs systèmes CCTV ont cette capacité d'expansion ou devraient tenir compte de l'évolutivité et de l'interopérabilité des composants dans la conception du nouveau système CCTV.

7. Composants d'un système CCTV

Les systèmes CCTV sont un réseau connecté d'équipements conçus pour capturer, transmettre, afficher et stocker des données d'imagerie. Les systèmes de vidéosurveillance varient en complexité, allant d'une seule caméra connectée à un moniteur, affichant les images vidéo, à des systèmes en réseau capables de surveiller et de contrôler des centaines de caméras connectées localement, à distance et dans le monde. Voir l'annexe A – Considérations Technologiques pour voir une comparaison des progrès technologiques dans les composants CCTV. Les composantes courantes d'un système CCTV sont les suivantes:

7.1. Caméras

Composant le plus reconnaissable et le plus visible d'un système CCTV, les caméras sont les capteurs qui convertissent la scène visible formée par l'objectif en un signal électrique ou binaire adapté à la transmission à un appareil distant. Il est extrêmement important de sélectionner la caméra appropriée pour l'environnement, l'application et l'infrastructure disponibles. En raison de l'avancement rapide de la technologie, les ministères et les organismes devraient être conscients de la compatibilité et de la fonctionnalité futures lors de la sélection des caméras CCTV.

7.1.1. Types de caméras

Voir l'annexe A – Considérations Technologiques pour voir une comparaison des technologies analogiques, numériques et technologie IP numérique lors de l'évaluation du ou des types de caméras nécessaires pour le CCTV d'un emplacement. Classés par fonction, mais souvent conçus avec des capacités de chevauchement, les types de caméras disponibles pour les ministères et organismes comprennent:

- **Caméra fixe:** Ces caméras sont montées en position fixe dans le but de se concentrer sur un champ de vision principal ou une zone d'intérêt. Situé à l'intérieur et à l'extérieur, ouvertement ou secrètement, et varient en taille et durabilité. Couramment utilisé pour la surveillance 24 heures sur 24, 7 jours sur 7 des clôtures de périmètre et des espaces ouverts; toutefois, ces caméras sont limitées pour fournir une « image complète » si les autres caméras ne fournissent pas un champ de vision qui se chevauche pour prévenir les « angles morts ». Ces caméras peuvent être intégrées aux systèmes de détection d'intrusion avec le logiciel approprié et/ou l'étiquetage approprié de la vue de la caméra sur le moniteur connecté;
- **Caméra à zoom panoramique (PTZ):** Les caméras PTZ permettent de déplacer l'appareil photo à distance, via un contrôleur, vers la gauche ou la droite (panoramique), vers le haut et vers le bas (inclinaison), et permettent à l'objectif de zoomer et de zoomer. Ces caméras sont mieux utilisées par le personnel de sécurité qui utilise le système CCTV dans une salle de contrôle ou un centre des opérations de sécurité. Les caméras PTZ ont l'avantage de permettre à l'opérateur de suivre une personne en mouvement ou de localiser un objet suspect pour observation à distance. Des procédures opérationnelles normalisées devraient être établies, après tout changement de vue, pour s'assurer qu'une caméra PTZ est retournée au champ de vision d'origine si elle est utilisée principalement pour une observation statique. Les caméras PTZ peuvent également avoir une fonction de « patrouille » pour « balayer » les zones au lieu de rester en position statique;
- **Caméra dôme:** Peut fonctionner comme une caméra fixe ou PTZ dissimulée dans le boîtier en forme de dôme. Le boîtier extérieur du boîtier de la caméra rend difficile pour les spectateurs d'identifier la direction de la caméra et peut fournir une certaine dissuasion contre les activités indésirables ou criminelles. Le boîtier des caméras de dôme peut également inclure des caractéristiques anti-vandalisme. Les caméras de dôme sont utilisées pour la surveillance intérieure et extérieure et sont bien adaptées aux entrées, aux escaliers, aux halls d'accueil et aux zones de contrôle de sécurité;

- **Caméra bullet:** Une version plus robuste de la caméra fixe, les caméras bullet sont cylindriques, sont fabriquées dans une variété de longueurs et sont idéales pour une utilisation en extérieur. Installées dans des boîtiers de protection, les caméras sont protégées de la poussière, de la saleté et d'autres éléments naturels. Ils sont équipés d'objectifs différents en fonction des exigences de l'application, y compris certaines caméras bullet qui ont de petites lumières DEL (diode électroluminescente aussi appelée LED) entourant l'objectif pour détecter les chiffres en mouvement dans des conditions de faible luminosité ou de nuit;
- **Caméra de vision nocturne et diurne:** Capable de fonctionner dans des environnements mal éclairés ou des emplacements extérieurs. Ces caméras sont équipées d'une puce d'imagerie très sensible qui permet d'obtenir automatiquement une image viable dans des conditions changeantes, de faible luminosité à brillante;
- **Caméra infrarouge/de vision nocturne:** Comme les caméras de vision nocturne et diurne, les caméras à vision infrarouge/nocturne peuvent être fixes ou PTZ et sont équipées pour capturer des images dans des conditions de faible luminosité à nocturne. L'efficacité de ces caméras dépendra de la capacité de l'objectif installé et des capteurs d'imagerie. Ce type de caméra est avantageux pour la surveillance 24/7 de l'infrastructure vitale, comme les aéroports, les ports maritimes, les installations de production d'électricité, d'autres infrastructures essentielles et les installations diplomatiques ou de défense à l'étranger; et
- **Caméra d'imagerie thermique:** Une caméra thermique capture et crée une image d'un objet en utilisant un rayonnement infrarouge, ou chaleur, émis par l'objet qui est invisible à l'œil humain. Les caméras thermiques sont capables de détecter la chaleur ou les signatures infrarouges sur de longues distances avec des émetteurs infrarouges spécialisés; cependant, les caméras thermiques ne sont pas efficaces pour détecter à travers le verre ou l'eau. La capacité de fournir une image à travers la fumée ou le brouillard à faible densité est limitée, mais les capteurs thermiques peuvent se dégrader avec le temps et nécessiter un entretien ou un remplacement plus fréquent.

7.2. Objectifs

Un objectif de caméra est un morceau de verre ou de plastique conçu pour contrôler et mettre au point la quantité de lumière du monde extérieur sur le capteur d'imagerie dans l'appareil photo; créer une image claire de la scène à l'exposition correcte. Il existe trois types d'objectifs de base pour les caméras CCTV : fixe, varifocal et zoom, et ceux-ci peuvent inclure des options de conception pour les conditions de faible luminosité.

7.2.1. Types d'objectifs

Chaque type d'objectif présente des caractéristiques différentes des autres, en fonction de l'application prévue, et fournit la meilleure image et les meilleurs détails possibles pour la zone surveillée. Ces caractéristiques comprennent:

- **Objectif fixe:** Les objectifs fixes ont une distance focale et un champ de vision horizontal définis qui nécessitent que la caméra soit physiquement rapprochée ou

éloignée de la zone surveillée pour modifier la quantité de détails pouvant être visualisée. Les lentilles fixes fonctionnent bien dans une application d'observation générale en surveillant une petite zone, comme un hall d'accueil ou une porte d'entrée;

- **Objectif à Focale variable:** Les objectifs à focale variable offrent généralement plus de flexibilité avec les positions d'installation en raison de la plage de focales dans l'objectif qui fournit différents champs de vision. Les objectifs à focale variable nécessitent toujours un réglage manuel pour modifier le champ de vision;
- **Objectif Zoom/Téléobjectif:** Semblables à la capacité des objectifs à focale variable de changer le champ de vision d'un appareil photo, les objectifs zoom permettent de modifier à distance le point focal, mais avec une plus grande portée du champ de vision que les autres types d'objectifs. Les objectifs à zoom motorisé, ou téléobjectifs ont l'avantage de recentrer le champ de vision lorsque l'objectif est ajusté par un opérateur; et
- **Objectif asphérique ou Iris automatique:** Une considération supplémentaire dans le choix des lentilles peut inclure les conditions d'éclairage de l'environnement sous vue. Dans un objectif à iris automatique, la caméra contrôle l'ouverture et la fermeture de l'iris dans l'objectif, en fonction de la quantité de lumière nécessaire pour produire une image. Les lentilles asphériques sont conçues avec une forme plus convexe qu'une lentille normale pour recueillir plus de lumière et permettre une meilleure image dans des conditions de lumière incohérentes. Ces lentilles sont disponibles dans une variété de formes et peuvent corriger la mise au point de la lumière à différents points, appelés aberration sphérique, lorsque la lumière traverse l'objectif. Cela peut aider à produire une meilleure image dans les applications à faible luminosité.

7.3. Boîtier et Supports de Caméra

Les caméras CCTV peuvent être des pièces d'équipement délicates qui nécessitent une protection contre les interférences physiques et les conditions environnementales. Le choix du boîtier de protection et du matériel de montage approprié diffère pour les caméras extérieures et intérieures dans un système CCTV. Il est important de tenir compte des conditions environnementales pour les caméras situées à l'extérieur. La chaleur et le froid extrêmes peuvent endommager les appareils électriques tout comme les climats humides et secs ou poussiéreux. S'assurer que le boîtier de caméra et le matériel de montage approprié sont utilisés aidera à protéger les caméras CCTV et permettra des conditions optimales pour la collecte d'images.

7.3.1. Boîtier de Camera

La coque ou le boîtier de protection d'une caméra CCTV doit être adapté au type et à la fonction de la caméra et à l'environnement dans lequel elle se trouve. Il faut porter attention à la capacité du boîtier à résister à l'humidité, aux changements de température importants, à l'impact physique et aux particules étrangères qui interfèrent avec l'appareil photo ou les images capturées. Exemples de boîtiers de caméra:

- **Boîtiers étanche:** conçu pour empêcher la contamination (eau, poussière, vapeurs chimiques) de l'environnement extérieur d'endommager les composants électriques de la caméra;
- **Boîtiers résistants aux chocs:** construit avec des matériaux robustes, ce type de logement est conçu pour résister aux interférences physiques du vandalisme et des délinquants violents;
- **Boîtiers inviolables:** Similaires aux modèles résistants aux chocs, ils sont construits avec des coques extérieures durcies, mais permettent d'accéder à la caméra via un port verrouillable. Ces modèles sont conçus pour résister à l'entrée forcée;
- **Boîtiers de dôme:** Fréquemment utilisés avec les caméras PTZ, ces « dômes » cachent la direction vers laquelle la caméra est orientée et sont moins évidents pour les observateurs extérieurs. De plus, le profil bas du dôme limite les interférences des conditions environnementales (vent, pluie, neige) qui peuvent provoquer des vibrations; et
- **Boîtiers résistant aux balles ou aux explosions:** construit avec des matériaux hautement résistants aux chocs pour limiter l'effet de l'impact violent de l'explosion ou des armes à feu. Ce type de logement serait normalement limité aux installations militaires et diplomatiques dans des environnements hostiles.

7.3.2. Supports de Caméra

Les caméras CCTV peuvent être montées sur une grande variété de surfaces lors de la conception de la disposition des caméras d'un système CCTV. Comme pour le boîtier de la caméra, le matériel de montage dépend des fonctions de la caméra, de l'utilisation prévue et de l'environnement dans lequel elle se trouve. Peu importe si la caméra est destinée à être cachée ou ouverte, ou située dans un environnement intérieur ou extérieur, les considérations courantes sont les suivantes:

- **Taille et poids de l'appareil:** la quincaillerie et le matériel d'ancrage du support, du boîtier et de la caméra doivent pouvoir résister au poids combiné;
- **Durabilité du matériel:** la robustesse du matériel de montage et du boîtier de la caméra doit être suffisante pour protéger la caméra dans l'environnement prévu;
- **Champ de vision:** la caméra doit être installée à un endroit capable de capturer/visualiser l'espace entier prévu, si une caméra supplémentaire ne fournit pas un champ de vision qui se chevauche pour observer tout l'espace; et
- **Vulnérabilité à l'altération ou aux dommages:** La plupart des emplacements de caméras CCTV doivent être hors de portée du grand public. Le montage de caméras CCTV dans les coins du plafond, sur les structures du bâtiment ou sur les poteaux d'éclairage de sécurité limitera les possibilités d'endommager ou de falsifier les caméras.

7.4. Moniteurs

Destinés à l'affichage d'images capturées par le réseau de caméras, les moniteurs CCTV varient en qualité d'image, en taille et en connectivité avec d'autres appareils. Le choix du moniteur à utiliser dans un système de vidéosurveillance devrait inclure des considérations sur la qualité de l'image que le moniteur peut produire, la durabilité de l'écran du moniteur à un

fonctionnement continu ou prolongé (image gravée dans l'écran), la consommation d'énergie / chaleur générée, la durée de vie du moniteur ou la compatibilité technologique (analogique vs numérique/numérique IP) et le type de transmission réseau (filaire ou sans fil). Les types de moniteurs disponibles pour les systèmes de vidéosurveillance peuvent inclure:

- Télévisions: standard, haute définition (HDTV) ou ultra haute définition (UHD). Ceux-ci peuvent avoir un double objectif et sont devenus courants dans de nombreuses applications, mais peuvent être susceptibles d'endommager l'écran en cas d'utilisation prolongée ou continue;
- Moniteurs d'ordinateur: Normalement connecté à des dispositifs de gestion et de stockage CCTV (enregistreur vidéo numérique / DVR), ce style de moniteur fonctionne bien dans une configuration de poste de travail dans une salle de contrôle CCTV ou un centre des opérations de sécurité;
- Moniteurs LCD/OLED: Les moniteurs à cristaux liquides (LCD) et à diodes électroluminescentes organiques (OLED) sont devenus des options viables, comme les moniteurs CCTV, en raison de la disponibilité accrue et des progrès de la technologie d'imagerie. Ceux-ci viennent dans une variété de tailles, sont relativement légers (montage mural), et nécessitent moins d'électricité que les technologies précédentes; et
- Mûr vidéo: une collection en réseau de moniteurs muraux et de murs vidéo qui fonctionnent bien dans un centre des opérations de sécurité et qui sont capables d'afficher un large éventail d'images de vidéosurveillance et d'autres écrans vidéo pour l'aménagement des installations et les cartes; alarmes, journaux d'événements et autres applications utiles dans une situation nécessitant une coordination ou une intervention de sécurité.

Les anciens systèmes CCTV utilisant plus de caméras que les moniteurs devront utiliser des dispositifs (tels que des commutateurs ou des multiplexeurs) pour permettre à la vue affichée sur le moniteur de passer d'un flux de caméra à un autre. Les systèmes de réseau IP numériques et numériques n'ont pas besoin de ce matériel supplémentaire pour modifier l'affichage du moniteur.

7.5. Moyen de Transmission

La méthode de transmission des signaux vidéo de la ou des caméra(s) au dispositif de traitement du système, comme le DVR ou les moniteurs, est aussi importante que la sélection et la qualité de la caméra, de l'objectif et du dispositif de traitement. L'assurance d'un signal vidéo fort sur l'ensemble du réseau permettra une image supérieure qui est disponible pour le personnel qui regarde le moniteur. Les supports de transmission peuvent être divisés en systèmes filaires et sans fil. Voir l'annexe A – Considérations Technologiques pour une comparaison de ces supports de transmission vidéo dans les technologies existantes.

7.5.1. Câblé

La méthode traditionnelle de transmission des signaux vidéo de la caméra au moniteur, la technologie de câblage CCTV a considérablement évolué. Les types couramment disponibles pour les systèmes CCTV sont les câbles coaxiaux et à fibre optique. Des options de câblage plus spécialisées sont disponibles. Les ministères et organismes devraient

consulter conjointement un concepteur de système de vidéosurveillance et l'autorité ministérielle en matière de sécurité au cas par cas si des besoins spécialisés sont cernés dans l'EMR.

Les **câbles coaxiaux** sont la connexion courante dans les systèmes CCTV depuis des décennies. Un câble multicouche, un câble coaxial doit avoir un noyau en cuivre pour transmettre correctement le signal électrique de la caméra au moniteur et un blindage en cuivre tressé à 95% ou une couche de maille pour limiter les interférences externes. Si la longueur du câble est grande, les ministères et les organismes devraient utiliser des amplificateurs pour assurer un signal fort dans tout le réseau. En tant que moyen de transmission électrique, assurez-vous que les câbles coaxiaux sont correctement mis à la terre pour éviter toute perturbation du signal.

Les **câbles à fibres optiques** sont composés de fibres de verre ou de plastique enveloppées dans une couche protectrice. Contrairement aux câbles coaxiaux, les câbles à fibre optique transmettent des impulsions lumineuses au lieu de signaux électriques. Cela nécessite l'utilisation de convertisseurs sur les deux extrémités des câbles à fibre optique pour convertir l'électricité en impulsions lumineuses et revenir à des signaux électriques. Bien que le câble à fibre optique soit plus fragile et nécessite un traitement supplémentaire que le câble coaxial, il n'est pas affecté par la radiofréquence ni les interférences électromagnétiques et peut transmettre sur des distances beaucoup plus longues sans dégrader le signal.

7.5.2. Sans Fil

Les systèmes sans fil CCTV sont très populaires dans les zones résidentielles et les petites entreprises. La capacité d'établir et de gérer un système CCTV complet, sans l'infrastructure nécessaire pour un système câblé, peut fournir beaucoup de mobilité et de flexibilité. Malheureusement, l'obtention d'une fréquence dédiée pour les transmissions peut être difficile à certains endroits.

Les systèmes sans fil sont plus vulnérables aux interférences et aux interruptions intentionnelles ou collatérales des signaux que les systèmes câblés. L'augmentation du nombre de cas de cyberingérence et de surveillance secrète peut être problématique pour le GC. Les ministères et organismes devraient tenir compte de ces considérations lorsqu'ils effectuent une EMR avant d'installer des composants sans fil dans le système CCTV.

7.6. Stockage des images

Les enregistrements CCTV peuvent être essentiels à la collecte de preuves lors d'enquêtes sur des actes criminels ou des incidents critiques. Le stockage d'images a beaucoup évolué, passant des disques durs sur bande aux disques durs numériques et aux systèmes infonuagiques sur Internet. Les ministères et organismes devraient évaluer leurs besoins en matière de stockage d'images, dans le cadre d'une EMR, lorsqu'ils conçoivent ou mettent à niveau un système CCTV. L'utilisation de l'entreposage « à l'intérieur de la caméra/à bord » devrait être évitée en raison du risque d'altération ou d'accès non autorisé, en particulier pour

les caméras situées à l'extérieur d'une zone contrôlée.

Les **enregistreurs vidéo numériques (DVR)** peuvent offrir une personnalisation de la façon dont les images sont enregistrées, des informations incluses dans l'affichage des images et des caméras enregistrées. Les options permettant l'enregistrement continu d'images, avec un paramètre d'écrasement (enregistrement sur des séquences plus anciennes), peuvent économiser de l'espace sur un disque dur. De nombreux systèmes DVR sont évolutifs et permettent à de nombreux disques durs de travailler en collaboration pour fournir des mois à des années d'enregistrements si cette capacité est justifiée. Une caractéristique supplémentaire des disques durs amovibles est qu'ils offrent une flexibilité dans la préservation des enregistrements originaux pour une utilisation ultérieure ou comme preuve si nécessaire.

Les **enregistreurs vidéo réseau (NVR)** sont un système IP qui stocke les données vidéo et les images transmises via un réseau Internet. Ces systèmes d'enregistrement transfèrent les images et les données vers un lecteur ou un dispositif de stockage (portable ou de stockage de masse) ou vers un stockage « en nuage » dans un serveur réseau distant. Cette option de stockage peut réduire le besoin de stockage physique dans la salle de contrôle des CCTV ou le centre des opérations de sécurité, mais les images et les données doivent être stockées dans un serveur ministériel du GC ou dans un endroit adéquatement contrôlé et protégé au Canada seulement. Voir 7.8.1. Considérations relatives à la cybersécurité pour en savoir plus.

Les images enregistrées doivent être protégées de la même manière que les autres renseignements du GC. Si la diffusion non autorisée d'images enregistrées peut être préjudiciable, ces images auront un niveau de catégorisation égal au niveau de blessure potentielle. Consulter le DSM, Annexe J : Norme sur la catégorisation de la sécurité et le document GCPSG-007 (2022) Transport, transmission et entreposage du matériel protégé et classifié pour en savoir plus.

7.7. Gestion de système

Les systèmes CCTV sont souvent complexes et présentent une vaste gamme de configurations potentielles pour répondre aux besoins d'une EMR. Les ministères et les organismes peuvent tirer profit de la mise au point de systèmes CCTV qui sont intégrés à du matériel, des logiciels, une infrastructure et des dispositifs de communication compatibles qui favorisent l'interopérabilité et la compréhension et la maintenance communes du système.

7.8. Systèmes de réseau à protocole Internet

Les systèmes CCTV basés sur Internet remplacent régulièrement les anciens systèmes analogiques en grande partie grâce à l'avantage supplémentaire de l'interopérabilité avec des appareils ou des ordinateurs en réseau partout dans le monde. Avec la technologie Power over Ethernet (PoE), les appareils en réseau reçoivent l'alimentation électrique et transmettent des données via le même câble, ce qui réduit le nombre de composants nécessaires et augmente l'efficacité de la conception. La capacité d'interagir avec plusieurs applications dans un système ministériel de gestion de l'accès ou un centre des opérations de sécurité augmente l'efficacité du personnel de sécurité et permet l'expansion future d'un réseau de CCTV.

7.8.1. Considérations relatives à la Cybersécurité

Comme pour toutes les applications Internet, les systèmes IP CCTV sont vulnérables aux cyberattaques et à la surveillance secrète si des mesures appropriées ne sont pas prises. La protection des images CCTV devrait être considérée de la même façon que les autres renseignements de nature délicate pour le GC. Les ministères et organismes devraient envisager d'utiliser un réseau privé pour les systèmes IP CCTV. Cela fournirait une protection supplémentaire contre l'accès non autorisé au système CCTV via un ordinateur sur le réseau de bureau régulier. Pour de plus amples renseignements ou des consultations sur les risques de cybersécurité, veuillez communiquer avec le Centre canadien pour la cybersécurité.

8. Considérations relatives au cycle de vie

La maintenance régulière programmée peut permettre au matériel et aux logiciels CCTV de fonctionner efficacement, de prolonger la durée de vie de l'équipement et d'identifier les problèmes avant qu'une panne ne se produise. Les tâches de maintenance préventive peuvent inclure:

- Inspection visuelle de l'équipement pour détecter les dommages, la décoloration, les fuites, l'humidité (buée) ou la corrosion;
- Vérifier s'il y a des signes d'ouverture ou d'altération non autorisée des composants du système (des scellés inviolables peuvent être appropriés s'il s'agit d'une menace identifiée pour l'emplacement);
- Nettoyage des caméras, des objectifs et des boîtiers. Les caméras extérieures peuvent nécessiter des vérifications et un nettoyage supplémentaires lorsqu'elles sont touchées par les conditions météorologiques;
- Effectuer les tests diagnostiques recommandés par le ou les fabricants; et
- Utilisation et test de tous les composants, fonctionnalités logicielles et qualité d'enregistrement du système CCTV.

Comme un système CCTV, ou tout élément clé du système, approche de la fin de la durée de vie utile prévue, les ministères et organismes devraient évaluer la faisabilité de la réparation ou du remplacement par rapport à l'efficacité à long terme de l'ensemble du système CCTV. Un système CCTV dans un état de délabrement ou de quasi-effondrement constant est une vulnérabilité accrue qui aggrave les risques identifiés dans une EMR. Les ministères et les organismes devraient envisager de remplacer les composantes désuètes ou disjointes de la CCTV par un système de CCTV complet ou compatible qui est conçu pour répondre aux besoins et aux besoins futurs potentiels cernés dans une EMR.

Les ententes de service et les contrats d'entretien peuvent comprendre des « appels d'urgence » (temps de réponse définis), des soins 24 heures sur 24 et des réparations sous garantie et hors garantie. Les ministères et organismes peuvent évaluer la nécessité de conserver sur place des composants et de l'équipement de CCTV de remplacement afin d'éviter des retards prolongés dans la restauration complète du système.

9. Références et documents connexes

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Loi sur la protection des renseignements personnels (justice.gc.ca)
- Centre de la sécurité des télécommunications (cse-cst.gc.ca)
- Centre canadien pour la cybersécurité
- Sécurité publique Canada - Accueil (securitepublique.gc.ca)
- Surveillance - Commissariat à la protection de la vie privée du Canada
- Un guide en langage clair et simple sur les exceptions et exclusions prévues par la Loi sur la protection des renseignements personnels - Canada.ca
- CCTV Technology Handbook, July 2013, US Department of Homeland Security (en anglais seulement)
- CCTV, March 2022, UK National Protective Security Authority (en anglais seulement)
- Directive sur l'obligation de prendre des mesures d'adaptation
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale
- Guide à l'intention des employés deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale
- Open Network Video Interface Forum (en anglais seulement)
- Physical Security Interoperability Alliance (en anglais seulement)
- Guide des considérations relatives à la conception d'un centre des opérations de sécurité (rcmp-grc.gc.ca)
- Guide sur les considérations liées à l'éclairage de sécurité (rcmp-grc.gc.ca)
- gcpsg-gsmgc-006-2024-fra.pdf (rcmp-grc.gc.ca)
- gcpsg-gsmgc-007-2022-fra.pdf (rcmp-grc.gc.ca)
- gcpsg-gsmgc-019-2023-fra.pdf (rcmp-grc.gc.ca)
- Guide d'évaluation des menaces et des risques

Annexe A - Considérations Technologiques

Spécifications	Analogique	Numérique	Numérique IP
Qualité vidéo	Bon en basse lumière, mais images pauvres ou dégradées / graining lors de l'expansion pour les fonctionnalités de zoom	Qualité supérieure à l'analogique avec une meilleure polyvalence de zoom / imagerie	Haute définition numérique avec des détails vidéo supérieurs et une plus grande portée de vue. Champ de vision plus large et plus de détails disponibles dans les fonctions de zoom
Résolution	720 x 480 pixels	1280 x 720 pixels à 8 mégapixels (3840 x 2160)	Jusqu'à 8K UHD (7680 x 4320) de transmissions compressées et codées.
Alimentation électrique	Les caméras nécessitent une source d'alimentation / un fil électrique séparé pour fonctionner	Les caméras nécessitent une source d'alimentation / un fil électrique séparée pour fonctionner	Alimentation par Ethernet. Élimine le besoin de fil électrique séparé pour alimenter les caméras.
Moyen de Transmission	câble ou câble coaxial (dois être en cuivre)	Câble coaxial (fil de cuivre) ou fibre optique	Ethernet et Sans Fil
Câblé /Sans Fil	Câblé	Câblé	Les deux. Solution pratique dans des domaines difficiles ou coûteux à faire fonctionner le câble; comme dans les bâtiments historiques. La sécurité des émissions devrait être prise en compte dans le processus décisionnel. Communiquez avec le CST pour obtenir des conseils sur la sécurité des émissions des signaux.
Distance de transmission du signal	Peut transmettre un signal vidéo jusqu'à environ 1,5 km via un câble câblé à paire torsadée traditionnel ou 600 mètres via un câble coaxial.	Peut transmettre le signal vidéo environ 600 mètres par câble coaxial ou 950-1000 mètres par câble à fibre optique.	Les caméras IP peuvent envoyer de la vidéo numérique à 100 mètres sur un câble Ethernet à paires torsadées et à des distances illimitées sur des réseaux IP. Les

			images conservent une clarté de 100 % sur de longues distances et lorsque le signal est converti entre différents formats.
Sécurité de la transmission des signaux	Nécessite un accès très étroit ou physique aux images de brèche ou d'interception ou aux signaux électriques émis. Impossible d'y accéder à distance, car il n'est pas connecté à Internet.	Câble coaxial identique à l'analogique. La fibre optique est moins vulnérable aux radiofréquences et aux interférences électromagnétiques, mais elle est fragile par rapport au câble coaxial.	Signal transmis sous forme de données Internet; câblé et sans fil. Mêmes préoccupations en matière de sécurité que les signaux de données Internet et mobiles.
Fiabilité	Vulnérable aux radiofréquences et aux interférences électromagnétiques.	Câble coaxial identique à l'analogique. La fibre optique est moins vulnérable aux radiofréquences et aux interférences électromagnétiques, mais elle est fragile par rapport au câble coaxial.	Vulnérabilité liée au réseau Internet et aux interférences externes (piratage, rançongiciel, système d'exploitation). La compatibilité des logiciels est une préoccupation.
Capacité d'étendre le système	L'expansion nécessite une infrastructure supplémentaire pour accueillir le câblage.	L'expansion nécessite une infrastructure supplémentaire pour accueillir le câblage.	L'extension s'intègre facilement dans le réseau existant avec des licences supplémentaires pour les logiciels.
Facilité d'installation	Nécessite une infrastructure standard (conduit) pour alimenter et relier le réseau). Les grands réseaux ont besoin de plus de soutien.	Nécessite une infrastructure standard (conduit) pour alimenter et relier le réseau). Les grands réseaux ont besoin de plus de soutien.	Moins d'infrastructure nécessaire que les systèmes non IP.

10. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné et recommande par la présente, GSMGC-011 (2024) Guide des systèmes de surveillance vidéo pour approbation.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.05.16 08:11:11 -04'00'

Shawn Nattress,
Gestionnaire
Principale Organisme Responsable de la Sécurité Matérielle, GRC

Date

Approuvé

J'approuve par la présente GSMGC-011 (2024) Guide des systèmes de surveillance vidéo.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.05.23 12:06:22 -04'00'

André St-Pierre,
Directeur, Sécurité Matérielle
Gendarmerie royale du Canada

Date