Annexe A

Énoncé des besoins

Services de coimplantation de centres de données

1 Introduction

Services partagés Canada (SPC), appelé ci-après le client, a un besoin (décrit aux présentes) qui porte sur l'acquisition de services commerciaux existants de coimplantation de centres de données à disponibilité élevée. Ces services doivent être fournis à partir d'un lieu unique dans un rayon d'au moins 10 km en ligne droite d'Angus (Ontario) (latitude et longitude : 44.313872, -79.8842912), et dans un rayon d'au plus 100 km de distance réseau de fibre optique, mesurée à partir d'Angus (Ontario) (latitude et longitude : 44.313872, -79.8842912) également.

Un service de coimplantation est un service prêté à partir d'un centre de données contrôlé et géré, où de nombreux clients installent des réseaux, des serveurs et du matériel de stockage et établissent des interconnexions avec divers fournisseurs de services de télécommunications ou de réseaux, à un coût et une complexité réduits au minimum.

Le besoin d'acquérir une capacité existante de centre de données sécurisé et hautement fiable par le recours à ce service de coimplantation sera :

a) fondé sur des normes et des critères acceptés de l'industrie, avec une conception et une exploitation respectueuses de l'environnement, et comprend des services de soutien continus et sans interruption du centre de données, pour le traitement des technologies de l'information (TI) décrites aux présentes;

b) physiquement installé de façon à permettre la reprise à haute disponibilité des sous-systèmes de traitement de TI entre les centres de données primaires et le service de coimplantation, grâce à l'utilisation des protocoles de télécommunication décrits aux présentes;

c) configuré pour satisfaire à un éventail d'exigences relatives à l'alimentation des TI allant de 250 kilovoltampères (kVA) jusqu'à 2 000 kVA, et un éventail de densités d'alimentation des armoires allant de 5 à 20 kVA, et des densités autonomes d'équipement de TI de jusqu'à 150 VA le pied carré (pi^2), comme décrit aux présentes;

L'entrepreneur doit respecter les délais de mise en œuvre suivants :

a) la date d'aménagement du client est définie comme étant la date à laquelle le service de coimplantation de l'entrepreneur est réputé avoir achevé avec succès la procédure d'essai d'acceptation de la salle des données (article 4.4.4 des présentes) et ne doit pas dépasser 70 jours civils suivant l'attribution du contrat. La date d'aménagement du client marque le commencement des activités que le client doit réaliser pour configurer le service de coimplantation de façon à ce qu'il soit prêt à accepter les charges de travail du client;

b) la date de mise en service du client est de 100 jours civils suivant l'attribution du contrat et est définie comme étant la date à laquelle l'entrepreneur commencera à facturer le client pour le service de coimplantation de base.

Tous les services décrits aux présentes sont considérés comme compris et couverts dans le coût des services de base spécifié à l'annexe B, « Tableaux d'établissement des prix ». L'entrepreneur doit fournir les services non compris dans le coût des services de base en conformité avec les prix fixés à l'annexe B.

2 Exigences techniques

2.1 Installations de l'entrepreneur

2.1.1 Disponibilité

a) L'entrepreneur doit fournir des services de coimplantation répondant aux exigences opérationnelles décrites dans le présent document, accessibles aux clients 24 heures par jour, sept jours par semaine, 365 jours par année (366 jours durant les années bissextiles), soit « en tout temps » comme on le dira aux présentes, nécessaires pour offrir une disponibilité de 100 % pendant toute la durée du contrat.

2.1.2 Entretien

a) L'entrepreneur doit s'assurer que ses installations sont convenablement entretenues de façon à assurer le niveau de disponibilité prévu en tout temps pendant toute la durée du contrat. Cet entretien doit comprendre, à tout le moins, les éléments suivants :

   i) enlèvement de la glace et de la neige dans les stationnements extérieurs et sur la chaussée, les allées piétonnes, les escaliers et les sorties de secours menant à l'intérieur et à l'extérieur des installations;

   ii) nettoyage de toutes les aires communes de sorte qu'elles sont bien rangées, libres de tout déchet et autres matériaux pouvant gêner;

   iii) enlèvement des déchets des installations et aussi souvent que nécessaire, pas moins d'une fois par jour;

   iv) nettoyage et réparations nécessaires pour garder l'équipement et les accessoires des salles de toilettes en bon état de fonctionnement;

   v) entretien paysagiste et nettoyage des fenêtres;

   vi) réparation et entretien des systèmes CVCA, des systèmes de sécurité des personnes et des ascenseurs (s'il y a lieu).

2.1.3 Plateformes de chargement

a) L'entrepreneur doit en tout temps donner accès au client à une plateforme de chargement et à une aire de réception dans ses installations.

b) L'entrepreneur doit fournir un ou plusieurs dispositifs mécaniques de levage permettant de déplacer l'équipement de TI du client entre l'aire de réception et l'aire d'entreposage temporaire sécurisée (définie dans le présent document) ou la salle des données (également définie dans le présent document).

2.1.4 Entreposage et disposition

a) L'entrepreneur doit fournir un espace de stockage temporaire d'au moins 40 m^2 (appelé dans le présent document « aire d'entreposage temporaire sécurisée ») pour l'infrastructure TI du client. L'aire d'entreposage temporaire sécurisée est gérée, contrôlée et accessible par l'entrepreneur seulement, et est mise à la disposition du client en tout temps.

b) Lorsqu'un représentant du client sera sur place ou présent à la plateforme de chargement des installations de l'entrepreneur pour recevoir de l'équipement de TI ou tout autre bien connexe du gouvernement, l'entrepreneur disposera en tout temps d'une procédure et d'un système pour répondre aux exigences suivantes :

   i) l'entrepreneur inscrira dans un registre toutes les marchandises reçues de la part du client. En aucun cas l'entrepreneur n'acceptera des marchandises au nom du client. Cette responsabilité appartiendra uniquement au responsable technique du client;

   ii) l'entrepreneur déplacera l'équipement du client vers l'aire d'entreposage temporaire sécurisée ou la salle de données du client décrits aux présentes, conformément aux indications du représentant du client.

c) Lorsqu'aucun représentant du client ne sera sur place ni présent à la plate-forme de chargement des installations de l'entrepreneur pour recevoir l'équipement de TI ou autres biens connexes du gouvernement, l'entrepreneur disposera en tout temps d'une procédure et d'un système pour répondre aux exigences suivantes :

   i) l'entrepreneur inscrira dans un registre toutes les marchandises reçues de la part des fournisseurs pour le compte du client;

   ii) l'entrepreneur déplacera l'équipement du client jusqu'à l'aire d'entreposage temporaire sécurisée.

d) À la demande du client, l'entrepreneur déplacera l'équipement du client de l'aire d'entreposage temporaire sécurisée à la salle de données du client.

e) À la demande du client, l'entrepreneur doit déballer l'équipement du client dans une aire spécialement réservée à cette tâche et disposer des caisses, des boîtes et des matériaux d'emballage de façon écologique (p. ex., en les recyclant).

f) Le déballage de l'équipement n'est en aucun cas autorisé dans la salle des ordinateurs ni la salle des données du client.

g) L'entrepreneur doit fournir un espace sécurisé et fermé d'au moins 6 m2, séparé de la salle de données du client, accessible seulement par ce dernier.

2.1.5 Aires communes de coimplantation

a) L'entrepreneur doit permettre aux clients d'accéder en tout temps aux aires communes de ses installations, notamment :

   i) aux salles de toilettes;

   ii) au coin-repas;

   iii) au local de premiers soins;

   iv) à la salle de réunion;

   v) aux postes de travail modulaires.

b) À la demande du client, l'entrepreneur doit lui donner en tout temps l'accès à une salle de réunion meublée sur place pouvant recevoir au moins 10 personnes, dotée de prises électriques actives et prêtes à être utilisées, de moyens de téléconférence actifs et prêts à être utilisés, d'un projecteur et d'un écran actifs et prêts à être utilisés et de capacités d'accès à Internet haute vitesse actives et prêtes à être utilisées.

c) L'entrepreneur doit fournir au moins 2 postes de travail modulaires meublés ayant les caractéristiques suivantes :

i) postes partagés par tous les clients de l'entrepreneur et mis à la disposition du client à la demande, moyennant un avis de 24 heures à l'entrepreneur;

ii) postes aménagés dans une salle ou un local pour bureau fermé et séparé à l'intérieur des installations, auquel seules les personnes autorisées peuvent avoir accès par des points d'accès contrôlés électroniquement;

iii) postes permettant l'accès :

1) à Internet haute vitesse actif et prêt à être utilisé;

2) à un téléphone connecté à une ligne terrestre actif et prêt à être utilisé.

2.1.6 Systèmes d'alimentation et refroidissement

a) L'entrepreneur doit assurer la disponibilité des systèmes d'alimentation et de refroidissement 100 % du temps. Aucun arrêt des systèmes d'alimentation et refroidissement qui pourrait affecter les opérations de la salle des ordinateurs pour raison de remplacement ou d'entretien de l'équipement n'est autorisé.

b) Les services de coimplantation de l'entrepreneur doivent atteindre l'objectif de rendement de niveau III de l'Uptime Institute ou son équivalent (voir l'appendice H). Les objectifs de niveau III de l'Uptime Institute définis aux présentent ne permettent pas d'éliminer par elle-même les points de défaillance uniques. C'est pourquoi l'entrepreneur doit mettre en œuvre des mesures de protection contre les points de défaillance uniques des systèmes mécaniques et électroniques.

c) La conception des systèmes de refroidissement de l'entrepreneur doit permettre l'alimentation en liquide réfrigéré des systèmes des armoires ou baies de TI à l'appui des générations à venir de plateformes informatiques à haute intensité. La mise en œuvre de cette conception dans l'avenir ne devra pas se répercuter sur le service aux clients.

d) L'entrepreneur doit prévoir des groupes électrogènes sur place pour assurer l'exploitation continue et sans interruption des services de coimplantation durant toutes les périodes où l'alimentation électrique du réseau publique n'est pas disponible. Il ne doit y avoir aucune limitation de la durée de fonctionnement des groupes électrogènes. Les groupes électrogènes de secours ne sont pas acceptables. En outre, l'installation des groupes électrogènes doit pouvoir être entretenue en parallèle sous la charge critique.

e) L'entrepreneur doit employer des groupes électrogènes d'urgence respectant ou dépassant toutes les exigences en matière de normes et d'émissions du niveau II.

Français
http ://www.ec.gc.ca/lcpe-cepa/default.asp?lang=Fr&n=D44ED61E-1

Anglais

http ://www.ec.gc.ca/lcpe-cepa/default.asp?lang=En&n=D44ED61E-1

f) L'entrepreneur doit configurer les services de coimplantation en fonction de la charge de pointe initiale, plus 10 %.

g) L'entrepreneur doit prévoir dans la configuration des services de coimplantation une barre omnibus d'alimentation conditionnée double « active-active » dans toutes les armoires du client et l'équipement de TI autonome des clients, peu importe les exigences relatives au type de circuit et des prises.

h) L'entrepreneur doit fournir des unités de distribution d'alimentation (PDU) autonomes et spécialisées pour les centres de données en réponse aux besoins en alimentation de la salle de données du client.

i) L'entrepreneur doit prévoir, durant toute la durée du contrat, une alimentation électrique double et un conditionnement environnemental pour l'ensemble de l'équipement de TI du client durant les activités de maintenance.

j) L'entrepreneur doit fournir des systèmes électriques de mise à la terre de l'équipement de TI conformes à la norme courante TIA-942.

k) L'entrepreneur doit fournir en tout temps une alimentation de secours desservant toutes les aires communes (définies dans le présent document).

2.1.7 Locaux de télécommunications des installations

a) L'entrepreneur doit, pour la durée du contrat, assurer aux fournisseurs de services de télécommunications du client l'accès aux salles de télécommunications pour que ces derniers puissent :

   i) installer, entretenir, exploiter, réparer, remplacer et retirer tout équipement de communication nécessaire pour fournir au client la connectivité de réseau avec et dans les locaux de télécommunications (décrite à l'article 2.2.2, « Exigence relatives au réseau ») sur les terrains et dans les immeubles utilisés par l'entrepreneur pour la prestation des services de coimplantation (la « propriété »);

   ii) installer, entretenir, exploiter, réparer et remplacer certains équipements de connexion (câbles, conduits, gaines intérieures, matériel de connexion et autres équipements passifs), avec le droit de tirer ces équipements de connexion à travers le « point d'entrée » de la propriété (défini comme étant le manchon par lequel ils pénètrent à travers la fondation de la propriété) et à travers d'autres « espaces de communication de la propriété » définis comme étant le chemin de télécommunications reliant les locaux de télécommunications au point d'entrée, au besoin, pour fournir des services de télécommunications au client;

   iii) accorder les droits d'entrée et de sortie aux employés, préposés et agents des entreprises de communications, ainsi que d'utilisation des ascenseurs, des halls d'entrée, des corridors, des escaliers, des voies d'accès et des aires de chargement communes à l'intérieur et près de la propriété.

2.1.8 Sécurité

a) La salle de données du client (définie ci-dessous) doit être une zone de sécurité (un secteur donc l'accès est réservé au personnel autorisé du client). Les exigences en matière de contrôle de sécurité énoncées dans le contrat seront en vigueur pour la zone de sécurité. Les modalités particulières relatives à l'établissement des zones de sécurité peuvent être trouvées à l'adresse suivante :

Français

http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-fra.htm

Anglais

http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-eng.htm

b) La zone de sécurité (définie à l'article 2.1.8 a.) ne sera accessible qu'à partir de la zone d'exploitation (un secteur auquel l'accès n'est réservé qu'au personnel autorisé à travailler dans ce secteur). Le périmètre de la zone de sécurité doit être démarqué par des murs d'une dalle à une autre selon les critères décrits dans les documents de référence suivants :

Appendice I, G13-01, *Pièces d'entreposage sécuritaire*.
Appendice I, G13-02, *Mur mitoyen sécuritaire*.

c) La zone de sécurité doit être construite afin de fournir des enceintes blindées contre les radiofréquences, tel que décrit dans le document ITSG-02 du Centre de la sécurité des télécommunications Canada, pouvant être trouvé à l'adresse suivante :

Français

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-fra.html

Anglais

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-eng.html

d) L'entrepreneur convient que tous ceux qui ont besoin d'avoir accès à la zone d'exploitation doivent détenir la cote de fiabilité minimale exigée par la Direction de la sécurité industrielle canadienne (DSIC) de TPSGC sans que cela n'entraîne de frais pour le client. Il est de la responsabilité de l'entrepreneur d'établir un processus et de négocier un coût avec la DSIC de TPSGC pour assurer ce service. Les documents de référence se trouvent à l'adresse suivante :

Français

http://ssi-iss.tpsgc-pwgsc.gc.ca/ssi-iss/personnel/enqut-scrnng-fra.html

Anglais

http://ssi-iss.tpsgc-pwgsc.gc.ca/ssi-iss/personnel/enqut-scrnng-eng.html

Si l'entrepreneur a des clients qui occupent un secteur des installations de coimplantation qui ne répond pas aux exigences de contrôle de sécurité de l'article 2.1.8 d, l'entrepreneur doit séparer ce secteur de la zone d'exploitation et de la zone de sécurité, selon le cas, par un mur résistant à la pénétration répondant aux spécifications décrites dans la section 2.1.8 b.

e) L'entrepreneur ne doit imposer au client aucun changement découlant de l'obtention, par un client actuel, d'une cote de sécurité plus élevée, par exemple la cote « Très secret ».

f) Les installations de l'entrepreneur doivent être dotées d'un système de surveillance vidéo et d'alarme en continu fonctionnant en tout temps dans les différents secteurs, y compris toutes les entrées de la propriété et des installations de l'entrepreneur, les entrées donnant accès à la salle de données du client, à la zone de sécurité, à la zone d'exploitation, aux plateformes de chargement, aux stationnements, à la toiture des immeubles et à tous les autres secteurs situés immédiatement dans le périmètre de la propriété.

g) L'entrepreneur doit enregistrer et conserver les données de surveillance vidéo pendant au moins 180 jours civils; ces enregistrements doivent être accessibles au responsable de la sécurité du client aux fins d'examen, à la demande. Les données vidéo doivent être remises au client dans les 24 heures qui suivent toute demande.

h) L'entrepreneur doit permettre au client de relier son équipement au système de surveillance vidéo en temps réel pour la surveillance vidéo de la salle de données du client même.

i) L'entrepreneur doit protéger les équipements TI du client à l'aide de systèmes multizones de surveillance, de détection et d'extinction des incendies. Le système d'extinction doit être à tout le moins un système d'extinction à réaction à double entrebarrage.

2.2 Exigences en matière de coimplantation

2.2.1 Exigences relatives à la salle de données du client

a) « Salle de données du client » renvoie au secteur du centre de données de l'entrepreneur réservé à l'infrastructure de TI du client. La salle de données du client doit comprendre le secteur primaire du client ainsi que tous les secteurs secondaires de ce dernier qui peuvent être inclus, à moins d'indication contraire.

b) L'entrepreneur doit concevoir et fournir la salle de données du client, qui doit satisfaire aux exigences suivantes :

   i) tout changement à la configuration doit être effectué de façon à ne pas causer d'interruption du service de CICD offert au client;

   ii) si le secteur primaire alloué ne peut pas être agrandi, l'entrepreneur fournira au client un secteur secondaire ou agrandira un secteur secondaire existant du client, qui pourra être connecté au secteur primaire sans entraîner de vulnérabilité pour la sécurité du réseau du client. Toutes les exigences relatives à la sécurité applicables au secteur primaire s'appliqueront également à tous les secteurs secondaires;

   iii) les points d'accès doivent être contrôlés électroniquement;

   iv) la salle de données doit être protégée contre tout accès non autorisé par le plafond ou le dessous du plancher;

   v) le contrôle physique doit aussi s'appliquer au câblage de réseau entrant dans le secteur primaire grâce à l'utilisation d'un conduit rigide et de câbles blindés;

c) Les installations de l'entrepreneur doivent être conçues pour recevoir la charge maximale admissible au sol de la salle de données du client renfermant des armoires emplis à pleine capacité et pouvant peser jusqu'à 1 000 kg.

d) L'entrepreneur doit installer et fournir une alimentation électrique double active et prête à être utilisée avec entre les unités de distribution de l'alimentation (PDU) de l'entrepreneur et

l'équipement de TI autonome et les armoires du client installés dans la salle de données de ce dernier.

e) L'entrepreneur doit fournir dans la salle de données du client des prises électriques utilitaires actives et prêtes à être utilisées pour le personnel d'entretien, conformément aux codes du bâtiment locaux.

f) L'entrepreneur doit fournir 2 prises téléphoniques de ligne terrestre actives et prêtes à être utilisées dans le secteur primaire de la salle de données du client ainsi que dans chacun de ses secteurs secondaires.

g) L'entrepreneur n'est pas autorisé à entrer dans la salle de données du client sans autorisation préalable écrite du responsable technique, sauf en cas d'urgence, par exemple un incendie. Si un tel événement se produit, l'accès par l'entrepreneur doit être signalé au client conformément aux exigences de la gestion des incidents relatives à la signalisation, de la façon décrite dans le présent document.

h) L'entrepreneur n'est pas autorisé à déplacer aucun des biens informatiques de la salle de données du client sans autorisation préalable écrite du responsable technique.

i) L'entrepreneur peut demander par écrit au responsable technique qu'une salle de données soit déplacée à l'intérieur de ses installations. Le responsable technique pourra, à son gré, soit rejeter ou accepter la demande, sous réserve de la condition minimale suivante :

   i) l'entrepreneur assumera seul tous les coûts associés au déplacement de la salle de données, y compris ses propres coûts, ainsi que les coûts d'investissement, les coûts ponctuels et les coûts opérationnels du client.

j) L'entrepreneur doit permettre au client de prendre les dispositions nécessaires pour faire nettoyer, à ses frais, l'intérieur des armoires de TI.

k) L'entrepreneur doit fournir des services de nettoyage de tous les planchers sur dalle et de tous les espaces sous les planchers surélevés au moins une fois par an, conformément à la norme ISO 14644-1, classe 8. Cette norme est accessible à l'adresse suivante :

   Français

   http ://www.iso.org/iso/fr/home.htm

   L'entrepreneur doit aviser par écrit le responsable technique au moins 90 jours civils avant le nettoyage prévu.

   Anglais

   http ://www.iso.org/iso/home.html

2.2.2 Exigences relatives au réseau

a) À tout le moins, les installations de l'entrepreneur doivent satisfaire aux exigences suivantes en matière de connectivité :

   i) fourniture de deux conduits souterrains distincts et séparés pour le câblage du réseau entre la limite de propriété de l'entrepreneur et les points d'entrée du réseau de les installations de l'entrepreneur (liens d'entrée), séparés d'au moins 10 m l'un de l'autre

pour réduire les risques de dommage ou de défaillance, au besoin, pour pouvoir assurer une disponibilité du service à 100 % en tout temps; fourniture de chemins de réseau haute vitesse multiples divers et non tributaires de l'entreprise, prêts à être utilisés, pour les divers fournisseurs de services de télécommunications qui desservent le secteur des installations de l'entrepreneur, aux frais de ce dernier;

ii) fourniture de deux salles de télécommunications distinctes, séparées par la plus grande distance possible, celle-ci ne devant pas être inférieure à 10 m, pour pouvoir assurer une disponibilité du service à 100 % en tout temps, dotées chacune d'un chemin de réseau sécurisé relié à un point d'entrée de réseau séparé des installations de l'entrepreneur (lien d'entrée), permettant d'aménager et d'incorporer des points de présence prêts à être utilisés, au besoin, pour les divers fournisseurs de services de télécommunications, non tributaires de l'entreprise, installés aux frais de l'entrepreneur;

iii) fourniture de chemins de câblage de réseau sécurisés entre chacun des locaux de télécommunications et de la salle de données du client permettant d'aménager et d'incorporer des points de présence prêts à être utilisés, au besoin, pour les divers fournisseurs de services de télécommunications, non tributaires de l'entreprise, installés aux frais de l'entrepreneur;

iv) fourniture d'un système de gestion du câblage pour l'interconnectivité du réseau dans la salle de données de l'entrepreneur. Le client se charge de l'architecture et de la conception du câblage.

b) L'entrepreneur doit sécuriser les locaux de télécommunications communs et n'y permettre l'accès qu'aux employés autorisés de l'entrepreneur et des fournisseurs de services de télécommunications.

2.2.3 Exigences relatives à l'alimentation

a) L'entrepreneur doit fournir la « réserve de puissance de base » suivante, qui ne comprend pas les tranches de puissance supplémentaires qui pourront être requises à la date d'aménagement du client :

i) 250 kVA, dont 90 % pour l'équipement des armoires et 10 % pour l'équipement autonome.

b) L'entrepreneur doit doter la salle de données du client de l'infrastructure électrique nécessaire pour satisfaire à un éventail de densités d'alimentation des armoires allant de 5 à 20 kVA et de densités d'équipement autonomes de 208 V triphasé allant jusqu'à 150 VA le pi^2, à la date d'aménagement du client.

c) La réserve de puissance de base définie à l'article 2.2.3 a) correspond à celle qui sera exigée pendant la durée du contrat.

3 Exigences relatives au soutien opérationnel

3.1 Soutien du service

3.1.1 Bureau de service

a) L'entrepreneur doit fournir un bureau de service servant de point de contact central pour l'enregistrement de l'ensemble des incidents, problèmes, demandes de service, demandes de changement, aide générale et demandes d'information liés au service de coimplantation.

b) L'entrepreneur doit fournir une description détaillée de l'organisation de son bureau de service et de ses processus au responsable technique au moins 40 jours civils après la date d'attribution du contrat.

c) L'entrepreneur doit fournir au client un numéro de téléphone local ou un numéro sans frais pour accéder au bureau de service au moins 40 jours civils après la date d'attribution du contrat.

d) Le bureau de service de l'entrepreneur doit être disponible en tout temps.

e) L'entrepreneur doit offrir en tout temps les services dans les deux langues officielles du Canada, le français et l'anglais.

3.1.2 Gestion des incidents

a) L'entrepreneur doit fournir les processus détaillés de gestion des incidents au responsable technique au moins 40 jours civils après la date d'attribution du contrat pour répondre aux exigences minimales suivantes :

   i) Barème A – Cibles d'intervention pour la gestion des incidents;

   ii) Barème B – Cibles d'intervention pour la gestion des incidents de sécurité.

b) L'entrepreneur doit fournir au client des services d'intervention selon la priorité des incidents, établie en fonction des répercussions de ces derniers sur la disponibilité du service, en conformité avec les exigences suivantes :

   i) Barème A – Cibles d'intervention pour la gestion des incidents;

   ii) Barème B – Cibles d'intervention pour la gestion des incidents de sécurité.

c) Le client passera au palier supérieur si les incidents ne sont pas résolus en conformité avec les exigences suivantes :

   i) Barème A – Cibles d'intervention pour la gestion des incidents;

   ii) Barème B – Cibles d'intervention pour la gestion des incidents de sécurité.

d) L'entrepreneur doit fournir au client un service en ligne sécurisé permettant, à tout le moins :

   i) d'ouvrir des dossiers d'incident où sont consignés les renseignements suivants :

      1) description de la demande,

      2) répercussions sur le client,

      3) priorité;

ii) de faire le suivi des dossiers d'incident actifs, y compris :

1) l'état des activités de l'entrepreneur,

2) les retards possibles dans la résolution des problèmes;

iii) d'examiner les demandes de résolution d'incident traitées ou annulées au cours des 12 derniers mois.

e) L'entrepreneur doit fournir des comptes pour le service Web de résolution des incidents à tous les employés désignés par le responsable technique, en conformité avec les exigences du Barème C – – Cibles d'intervention pour la gestion des changements.

3.1.3 Gestion des problèmes

a) L'entrepreneur doit fournir un processus détaillé de gestion des problèmes au responsable technique au moins 40 jours civils après la date d'attribution du contrat, et ce processus doit inclure les activités suivantes :

i) gestion du cycle de vie de tous les problèmes;

ii) identification de la cause des incidents;

iii) résolution des problèmes mise en œuvre par le processus de contrôle des changements;

iv) analyse des tendances des incidents.

b) L'entrepreneur doit fournir un service en ligne sécurisé pour permettre à tout le moins au client :

i) de présenter des demandes de résolution des problèmes permettant de consigner les renseignements suivants :

1) description de la demande,

2) date de résolution demandée,

3) répercussions sur le client,

4) priorité;

ii) de faire le suivi des demandes de résolutions des problèmes, y compris :

1) l'état des activités de l'entrepreneur,

2) les retards possibles dans la résolution des problèmes;

iii) d'examiner les demandes de résolution des problèmes traitées ou annulées au cours des 36 derniers mois.

c) L'entrepreneur doit fournir des comptes pour le service Web de résolution des problèmes à tous les employés désignés par le responsable technique, en conformité avec les exigences du Barème C – Cibles d'intervention pour la gestion des changements

3.1.4 Gestion des changements

a) L'entrepreneur doit fournir des processus détaillés de gestion des changements au responsable technique au moins 40 jours civils après la date d'attribution du contrat, de début

de la mise en service du client, en conformité avec le contrat et les exigences du Barème C – Cibles d'intervention pour la gestion des changements.

b) L'entrepreneur doit fournir un service en ligne sécurisé pour permettre au client, à tout le moins :

   i) de présenter des demandes de changement permettant de consigner les renseignements suivants :

      1) description de la demande,

      2) date de la demande de changement,

      3) priorité,

      4) recours aux services facultatifs,

      5) directives spéciales, visant notamment la planification, la coordination et l'installation de gros équipements de TI dans la salle de données du client;

   ii) de faire le suivi des demandes de changement, y compris :

      1) l'état des activités de l'entrepreneur,

      2) les retards possibles dans la résolution des problèmes;

   iii) d'examiner les demandes de changement traitées ou annulées au cours des 36 derniers mois;

   iv) de réactiver et de modifier une demande de changement annulée.

c) L'entrepreneur doit fournir des comptes pour le service Web de demande de changement à tous les employés désignés par le responsable technique, en conformité avec les exigences du Barème C – Cibles d'intervention pour la gestion des changements.

d) L'entrepreneur doit présenter un rapport mensuel des changements au client dans les 15 jours civils après la fin de chaque mois à compter de la date de mise en service du client. Ce rapport doit décrire les activités prévues, en conformité avec l'appendice E, « Rapport mensuel sur les changements ».

3.2 Prestation des services

3.2.1 Gestion de la planification

a) L'entrepreneur doit fournir un processus détaillé de gestion de la planification au responsable technique au moins 40 jours civils après la date d'attribution du contrat.

b) L'entrepreneur rencontrera le responsable technique chaque trimestre pour discuter des activités de planification à moyen et à long terme qui se rapportent notamment aux besoins en matière d'espace et d'alimentation électrique, pour le soutien de la croissance planifiée des installations de l'entrepreneur.

c) L'entrepreneur et le client travailleront ensemble pour minimiser les risques à l'environnement d'exploitation et à la disponibilité du matériel informatique de TI du client. Le responsable technique fournira à l'entrepreneur un calendrier des périodes d'activité critiques au moins 30 jours civils avant la date de mise en service du client précisée au contrat; ce calendrier sera mis à jour annuellement par le client et remis à l'entrepreneur au plus tard le 30 septembre de chaque année.

3.2.2 Gestion des niveaux de service

a) L'entrepreneur doit présenter un rapport mensuel sur les services au client dans les 15 jours civils après la fin de chaque mois à compte de la date de mise en service du client, en conformité avec l'appendice D, « Rapport mensuel sur les services ».

b) À compter de la date de mise en service du client et jusqu'à la première date d'anniversaire de cette mise en service, l'entrepreneur doit rencontrer le client en personne tous les mois à l'emplacement du SCN indiqué par le responsable technique afin de lui présenter le *Rapport mensuel sur les services*.

c) Après la première date d'anniversaire de la mise en service du client, l'entrepreneur doit rencontrer le client, à un endroit dans la RCN qui sera précisée par le responsable technique, tous les trois mois, soit au cours des moins suivant pendant la durée du contrat :

   i) février;

   ii) mai;

   iii) août;

   iv) novembre.

d) Après chaque réunion mensuelle et trimestrielle, l'entrepreneur doit remettre le procès-verbal provisoire de la réunion, en conformité avec l'appendice C, « Procès-verbaux des réunions », au responsable technique au plus tard que 7 jours civils après la réunion.

e) Le procès-verbal provisoire de la réunion sera examiné par le responsable technique, qui y notera les corrections à apporter s'il y a lieu et le retournera à l'entrepreneur au plus tard après 7 jours civils.

f) L'entrepreneur disposera de 7 jours civils après avoir reçu les corrections sur le procès-verbal provisoire de la réunion pour intégrer les modifications nécessaire et distribuer le procès-verbal définitif en format électronique (p. ex., PDF) par courriel au responsable technique du client et aux autres représentants ayant assisté à la réunion.

3.2.3 Gestion financière

a) L'entrepreneur doit fournir des rapports mensuels sur les dépenses au responsable technique et à l'autorité contractante, indiquant les dépenses totales courantes pour chaque catégorie indiquée dans la base de paiement du contrat. Le rapport sur les dépenses doit aussi comprendre un sommaire de toute modification apportée aux services de coimplantation, notamment toute modification ou suppression de l'un des services formant partie du contrat ou toute modification ultérieure au contrat. Les rapports doivent être fournis mensuellement, le premier d'entre eux devant être remis au plus tard que le 15 du mois suivant la date de mise en service du client et, ensuite, le 15 de chaque mois, et ils doivent porter sur le mois précédent.

3.2.4 Gestion des capacités

a) L'entrepreneur doit fournir un processus détaillé de gestion des capacités au responsable technique au moins 40 jours civils après la date d'attribution du contrat.

b) On prévoit que la consommation en électricité du client devrait augmenter pour passer de 250 kVA à 1 000 kVA d'ici le 30 avril 2015. Une puissance supplémentaire pouvant atteindre 1 000 kVA pourrait également être nécessaire en réponse à une croissance imprévue des besoins du client pendant la durée du contrat. La consommation prévue en électricité est fournie à titre indicatif seulement.

c) La capacité supplémentaire du client doit être assurée par l'entrepreneur de la façon suivante :

Tranches de puissance requise	Cible d'intervention
Entre 0 kVA et 250 kVA	90 jours civils au plus
Entre 251 kVA et 500 kVA	180 jours civils au plus
Entre 501 kVA et 1 000 kVA	À négocier avec l'entrepreneur, l'objectif étant de 365 jours civils au plus

d) Si le client prévoit une diminution nette de ses besoins en alimentation électrique pour sa salle de données, le responsable technique se réserve le droit de demander à l'entrepreneur de réduire la configuration de la salle de données du client en conséquence. Le cas échéant, l'entrepreneur et le responsable technique collaboreront pour élaborer un plan de réduction de la configuration de la salle de données du client.

e) Si le client prévoit une diminution nette de ses besoins, le responsable technique se réserve le droit de réduire sa consommation d'électricité moyenne annuelle de 25 % par année par rapport à l'année contractuelle précédente.

f) L'entrepreneur doit fournir un rapport mensuel sur la capacité de ses installations dans les 15 jours civils après la fin de chaque mois, à compter de la date de mise en service du client, comportant à tout le moins les renseignements suivants :

i) capacité électrique disponible et prévue pour les installations;

ii) capacité électrique UPS disponible et prévue;

iii) capacité de refroidissement disponible et prévue dans le bâtiment;

iv) capacité de refroidissement disponible et prévue dans la salle de données du client;

v) Indicateur d'efficacité énergétique (PUE) du centre de données sur une année, où :

$$\text{Indicateur d'efficacité énergétique (PUE)} = \frac{\text{Consommation totale des installations}}{\text{Consommation de l'équipement de TI}}$$

g) L'entrepreneur doit fournir un rapport mensuel sur la capacité du client dans les 15 jours civils suivant la fin de chaque mois, comportant à tout le moins les renseignements suivants :

i) consommation électrique du client (mesurée au PDU);

ii) capacité électrique UPS du client;

iii) utilisation du refroidissement par le client;

iv) utilisation de la superficie utile de la salle de données;

v) disponibilité de la superficie utile de la salle de données.

3.2.5 Gestion de la disponibilité

a) L'entrepreneur doit fournir une description détaillée des services et des processus de surveillance de ses installations au responsable technique au moins 40 jours civils après la date d'attribution du contrat.

b) L'entrepreneur doit surveiller en tout temps ses installations, notamment les systèmes de sécurité, les systèmes d'alimentation, les systèmes de refroidissement et les systèmes d'extinction des incendies.

c) Les systèmes de sécurité, les systèmes d'alimentation, les systèmes de refroidissement et les systèmes d'extinction des incendies doivent générer automatiquement des avis d'alerte transmis aux services de surveillance des installations de l'entrepreneur.

3.3 Sécurité

3.3.1 Gestion de la sécurité

a) L'entrepreneur doit fournir une description détaillée des processus de sécurité de ses installations au responsable technique au moins 40 jours civils après la date d'attribution du contrat.

b) Le responsable technique fournira à l'entrepreneur une liste du personnel autorisé du client au moins 14 jours civils avant la date d'aménagement précisée au contrat.

c) Le responsable technique fournira à l'entrepreneur des mises à jour de la liste du personnel autorisé du client au moins 2 jours civils avant la date à laquelle chacune des personnes identifiées dans la liste devra accéder aux installations.

d) L'entrepreneur doit avoir établi des processus de sécurité pour accorder et annuler les droits d'accès à ses installations 7 jours par semaine, 24 heures par jour, y compris l'accès en cas d'urgence. Ces processus seront examinés tous les trimestres par l'entrepreneur et le responsable technique ou l'agent de sécurité délégué du client. L'entrepreneur doit mettre en œuvre tous les changements aux processus de sécurité que le responsable technique juge nécessaires pour maintenir la conformité aux exigences de sécurité tout au long de la période du contrat, et ce, sans frais supplémentaires pour le client.

e) L'entrepreneur doit tenir un journal électronique de toutes les personnes qui sont entrées dans la salle de données et en sont sorties. Ces données doivent être conservées pendant au moins 180 jours civils. Dans un délai de deux heures après en avoir reçu la demande de la part du responsable technique, l'entrepreneur doit fournir un rapport indiquant toutes les personnes qui sont entrées dans la salle de données et en sont sorties.

f) L'entrepreneur doit permettre au client de mettre en œuvre un système de gestion des clés contrôlé par ce dernier.

g) L'entrepreneur doit permettre au client ou à un tiers sélectionné par le client d'effectuer des vérifications de sécurité périodiques de ses installations aux frais du client, avec l'aide de son propre personnel de sécurité ou d'experts-conseils qualifiés, afin de s'assurer que toutes les

exigences en matière de sécurité du service de coimplantation sont continuellement respectées. Ces vérifications de sécurité comprendront, notamment :

i) la mise en œuvre, par l'entrepreneur, des exigences relatives aux enquêtes de sécurité sur le personnel énoncées à l'article 2.1.8 d);

ii) la mise en œuvre, par l'entrepreneur, de la politique d'utilisation acceptable de l'entrepreneur, décrite à l'article 3.3.2 a);

iii) la mise en œuvre, par l'entrepreneur, de la politique de vérification de client acceptable, décrite à l'article 3.3.2 c).

L'entrepreneur coopérera pleinement et fournira une documentation justificative ou des ressources sans frais pour le client. Le rapport final sera communiqué à l'entrepreneur et indiquera les lacunes recensées pendant la vérification de sécurité. Ces lacunes doivent être gérées et corrigées en conformité avec le Barème B – Cibles d'intervention pour la gestion des incidents de sécurité ou comme contenu par écrit par l'entrepreneur et le client.

h) L'entrepreneur doit avoir établi des procédures pour satisfaire aux critères de rendement définis dans le Barème B – Cibles d'intervention pour la gestion des incidents de sécurité.

3.3.2 Clients des installations de l'entrepreneur

a) L'entrepreneur doit disposer d'une politique d'utilisation acceptable qui respecte à tout le moins les exigences énoncées à l'appendice F, « Politique d'utilisation acceptable ».

b) L'entrepreneur doit inclure dans ses contrats les exigences énoncées dans la politique d'utilisation acceptable pour tous les clients à ses installations.

c) L'entrepreneur doit disposer d'une politique de vérification de client acceptable pour les installations. Une politique de vérification de client acceptable est définie comme étant la norme minimale en vertu de laquelle l'entrepreneur peut accepter des clients aux installations afin de protéger les intérêts de tous les clients. La politique de vérification de client acceptable doit, à tout le moins, rejeter :

i) tout client ou personnel du client qui sont directement ou indirectement liés à des programmes décrits dans la liste des sanctions économique canadiennes;

ii) le client qui n'accepte pas les conditions de la politique d'utilisation acceptable énoncées à l'appendice F, « Politique d'utilisation acceptable ».

L'entrepreneur peut avoir accès à la liste à l'adresse suivante :

Français

http ://www.international.gc.ca/sanctions/index.aspx?lang=fra

Anglais

http ://www.international.gc.ca/sanctions/index.aspx?lang=eng

d) L'entrepreneur ne doit imposer au client aucun changement découlant de l'arrivée d'un nouveau client détenant une cote de sécurité plus élevée, par exemple la cote « Très secret ».

e) L'entrepreneur convient que le client a le droit de le soumettre à une vérification pour s'assurer que tous les clients dans les installations sont conformes à la politique de vérification client acceptable.

f) L'entrepreneur convient que le client a le droit de le soumettre à une vérification pour s'assurer qu'il met en application la politique d'utilisation acceptable pour tous les clients dans les installations.

g) Toute violation de la politique d'utilisation acceptable sera consignée comme un incident et assujettie à toutes les exigences énoncées à l'article 3.1.2, « Gestion des incidents ».

3.4 Exigences relative à la présentation des rapports et à la tenue des réunions

a) À moins d'indication contraire, tous les rapports présentés par l'entrepreneur au responsable technique ou à l'autorité contractante doivent être rédigés en anglais, par exemple si l'autorité contractante, le responsable technique et l'entrepreneur en ont convenu autrement.

b) À moins d'avis contraire, tous les rapports présentés par l'entrepreneur au responsable technique ou à l'autorité contractante doivent être livrés en format PDF, ainsi que dans la version du logiciel ayant servi à les produire (de préférence en format Microsoft Word ou en tout autre format convenu par l'autorité contractante, le responsable technique et l'entrepreneur).

c) À moins d'avis contraire, tous les rapports présentés par l'entrepreneur au responsable technique ou à l'autorité contractante doivent être livrés par courriel ou par tout autre moyen convenu par l'autorité contractante, le responsable technique et l'entrepreneur.

d) À moins d'indication contraire, toutes les réunions se tiendront par téléconférence.

3.5 Ressources de l'entrepreneur

3.5.1 Gardes de sécurité

a) À tout le moins, l'entrepreneur doit poster un garde de sécurité à ses installations, 24 heures par jour, 7 jours par semaine et 365 jours par année (366 pour les années bissextiles), conformément aux exigences suivantes :

i) les gardes de sécurité doivent être cautionnés et détenir des cartes d'identité certifiés par des organisations de sécurité satisfaisant à tout le moins aux exigences en matière de sécurité précisées dans le contrat;

ii) les gardes de sécurité à l'entrée principale des installations de l'entrepreneur doivent être postés dans une aire sécuritaire séparée (barrière matérielle) de l'aire dans laquelle les personnes entrent dans les installations de l'entrepreneur;

iii) Les gardes de sécurité doivent identifier et authentifier avec certitude toutes les personnes entrant dans les installations de l'entrepreneur :

1) toute personne autorisée entant dans les installations de l'entrepreneur doit avoir, à tout le moins, une carte de sécurité avec photo l'identifiant,

2) tous les visiteurs des installations de l'entrepreneur doivent fournir une carte d'identité avec photo et signer un registre des visiteurs. Tous les visiteurs entrant dans les installations de l'entrepreneur doivent être escortés en tout temps par un employé autorisé;

iv) le journal de sécurité électronique et le registre des visiteurs sur papier doivent être conservés pendant au moins 6 mois et indiquer toutes les personnes qui sont entrées dans les installations de l'entrepreneur ou en sont sorties.

3.5.2 Soutien du compte

a) L'entrepreneur doit désigner un chargé de compte qui répond aux critères suivants :

i) posséder au moins 5 ans d'expérience comme représentant de l'entrepreneur qui a le pouvoir de prendre des décisions en ce qui concerne tous les aspects de l'exécution du marché;

ii) assister en personne ou par téléconférence aux réunions mensuelles sur l'état d'avancement.

b) L'entrepreneur doit désigner un gestionnaire de compte qui répond aux critères suivants :

i) posséder au moins 5 ans d'expérience comme point de contact unique pour un ou des clients et se charger de l'administration courante du marché;

ii) assister en personne aux réunions mensuelles sur l'état d'avancement ainsi qu'à d'autres réunions à la demande de l'État.

3.5.3 Soutien technique

a) L'entrepreneur doit désigner un gestionnaire des installations qui possède au moins 5 ans d'expérience comme représentant de l'entrepreneur auprès du client en ce qui concerne tous les aspects de la prestation des services à l'intérieur des installations du centre de données.

b) L'entrepreneur doit désigner un technicien principal de service à la clientèle jouant le rôle d'expert-conseil technique pour les services de coimplantation. Ce technicien rencontrera tous les moins ou à la demande de l'État une personne-ressource désignée par le client.

c) L'entrepreneur doit désigner des techniciens affectés aux services de coimplantation pour répondre aux demandes de service décrits dans barèmes A, B et C.

3.5.4 Mise en œuvre des services

a) L'entrepreneur doit désigner un gestionnaire de projet de mise en œuvre des services, qui le représentera auprès du client pour tous les aspects de la mise en œuvre des services, en conformité avec les exigences énoncées à l'article 4.

4 Exigences relatives à la mise en œuvre des services

4.1 Plan de gestion de projet

a) L'entrepreneur doit fournir un plan de gestion de projet dans les 7 jours civils suivant la date d'attribution du contrat, en conformité avec l'appendice B, Plan de gestion de projet de mise en œuvre des services », qui fait état, à tout le moins, de son approche générale pour satisfaire aux exigences relatives à la mise en œuvre des services, du processus de suivi des étapes liées aux activités de mise en œuvre des services, ainsi que des activités de l'entrepreneur et des produits livrables rattachés aux activités de mise en œuvre des services.

4.2 Réunion de lancement

a) Une réunion de lancement, présidée par l'autorité contractante, sera tenue avec la participation de l'entrepreneur et de ses représentants ainsi que du responsable technique du client, au plus tard 10 jours civils après la date d'attribution du contrat.

b) La réunion aura lieu dans le SCN, et la date, l'heure et l'endroit seront donnés à l'entrepreneur par écrit par l'autorité contractante au plus tard 5 jours civils après la date d'attribution du contrat.

c) Le but de la réunion est d'examiner le calendrier et les produits livrables.

4.3 Rapports d'avancement et réunions

a) L'entrepreneur doit remettre un rapport d'avancement officiel au responsable technique au plus tard le vendredi de chaque mois à compter de la date d'attribution du contrat, dans le format précisé à l'appendice A, « Rapport hebdomadaire d'avancement sur la mise en œuvre des services». Ce rapport sera transmis par courriel en anglais en format PDF.

b) L'entrepreneur doit organiser une réunion hebdomadaire sur l'état d'avancement et y assister au plus tard 3 jours civils après avoir présenté le rapport d'avancement; le responsable technique du client et les représentants désignés, également présents par téléconférence, doivent y faire le point sur l'état d'avancement des activités de mise en œuvre des services définies dans le plan de gestion de projet.

c) Après la réunion hebdomadaire d'avancement, l'entrepreneur doit remettre le procès-verbal provisoire de la réunion au responsable technique au plus tard 1 jour civil après la réunion hebdomadaire, dans le format précisé à l'appendice C, « Procès-verbaux des réunions ». Le procès-verbal de la réunion doit être présenté en anglais en format PDF et transmis par courriel.

d) Le procès-verbal provisoire de la réunion sera examiné par le responsable technique. Ce dernier notera les corrections ou modifications à apporter s'il y a lieu et le retournera à l'entrepreneur au plus tard après 1 jour civil.

e) L'entrepreneur disposera de 1 jour civil pour faire les modifications demandées par le responsable technique et retourner le procès-verbal final de la réunion en anglais et en format PDF à ce dernier, par courriel.

4.4 Établissement des services de coimplantation

4.4.1 Emplacement des installations de l'entrepreneur

a) L'entrepreneur doit fournir des services de coimplantation à l'usage du client à partir d'un lieu unique dans un rayon d'au moins 10 km en ligne droite d'Angus (Ontario) (latitude et longitude : 44.313872, -79.8842912), et dans un rayon d'au plus 100 km de distance réseau de fibre optique, mesurée à partir d'Angus (Ontario) (latitude et longitude : 44.313872, -79.8842912) également. L'entrepreneur doit remplir cette condition pour répondre aux deux exigences opérationnelles essentielles suivantes du client :

   i) une distance minimale entre le centre de données existant du client situé près de la Base des Forces canadiennes (BFC) Borden, au Canada, afin de réduire les risques que le centre de données du client et les installations de l'entrepreneur soient hors service en même temps;

   ii) une distance maximale entre les installations de l'entrepreneur et le centre de données du client pour garantir une interconnectivité de télécommunications synchrone haute vitesse comme l'exigent les applications de TI, l'infrastructure de TI et les configurations de technologie réseau actuelles du client.

b) L'entrepreneur doit fournir les services de coimplantation à partir d'une source d'électricité indépendante de celle qui est utilisée à Angus, en Ontario.

c) L'entrepreneur doit fournir les services à partir d'une de ses installations, dans une zone où sont réduites au minimum les conséquences de conditions potentiellement dangereuses, notamment une plaine inondable, un chemin de fer ou une autoroute utilisée pour le transport de matières dangereuses, et autres utilisations connexes, y compris des usines et des entrepôts de produits chimiques.

4.4.2 Conditions relatives aux installations de l'entrepreneur

a) Les installations de l'entrepreneur doivent atteindre les objectifs de niveau III de l'Uptime Institute ou son équivalent pour les centres de données. Les objectifs de niveau III dont définis dans la topologie normalisée des niveaux (*Tier Standard: Topology*) de l'Uptime Institute (appendice H). La conformité des installations de l'entrepreneur avec la topologie de l'Uptime Institute sera attestée par une tierce partie accréditée par ce dernier et choisie par le Canada.

b) L'entrepreneur doit permettre au client ou à une tierce partie choisie par le client d'effectuer des vérifications périodiques de ses installations aux frais du client, qui seront menées par le personnel qualifié de ce dernier ou d'experts-conseils qualifiés afin de s'assurer que toutes les exigences en matière d'équivalence de l'Uptime Institute pour les services de coimplantation sont continuellement respectées.

c) L'entrepreneur doit fournir les services à partir d'installations indépendantes vouées exclusivement à la prestation de services de centre de données.

d) L'entrepreneur doit fournir les services à partir d'installations où on ne peut apercevoir aucune affiche, à l'extérieur comme à l'intérieur, qui pourrait divulguer la raison d'être de ses installations ou l'identité de ses clients.

e) L'entrepreneur doit obtenir toutes les approbations et licences de tierces parties nécessaires, conformément aux lois applicables afin de garantir que le site de coimplantation est jugé pleinement fonctionnel et prêt à être occupé pas plus tard que la date où l'installation sera prête à être utilisée par le client.

f) L'entrepreneur doit accorder au client le droit d'installer ou d'avoir accès à des antennes paraboliques orientables afin que la salle de données du client puisse prendre en charge les services par satellite.

g) Les installations de l'entrepreneur doivent comprendre un parc de stationnement général, dont au moins quatre places de stationnement seront réservés à l'usage du client, sans frais supplémentaire pour ce dernier.

4.4.3 Exigences relatives à la salle de données

a) Le client fournira à l'entrepreneur une description du matériel informatique du client au moins 5 jours après la date d'attribution du contrat.

b) L'entrepreneur doit entreprendre la conception de la salle de données du client, et la soumettre à ce dernier aux fins d'examen, dès que la description du matériel informatique du client lui a été remise en sorte que toutes les questions techniques puissent être traitées à fond. La conception de la salle de données du client doit prendre en charge le matériel informatique du client conformément aux exigences énoncées à l'article 2.2.3, « Exigences relatives à l'alimentation », alinéas a) et b). La conception de la salle de données doit comprendre ce qui suit :

   i) conception du plan d'étage pour les armoires de la salle de données du client;

   ii) conception de la distribution électrique;

   iii) conception des systèmes de refroidissement;

   iv) conception du câblage.

c) L'entrepreneur doit présenter au client sa conception de la salle de données approuvée dans ce dernier au moins 15 jours après la date d'attribution du contrat.

d) L'entrepreneur collaborera avec le client pour effectuer la configuration de la salle de données en fonction de la conception approuvée. La configuration de la salle de données du client doit comprendre ce qui suit :

   i) fourniture et installation des armoires, y compris des CPDU;

   ii) fourniture et installation de l'alimentation électrique des armoires et du matériel autonome du client;

   iii) fourniture et installation des systèmes de refroidissement des armoires et du matériel autonome du client;

   iv) fourniture et installation du câblage des baies et du matériel autonome du client;

   v) fourniture et installation des chemins de câbles.

e) La salle de données du client doit être prête à utiliser au moins 30 jours après la date d'attribution du contrat.

f) La salle de données et les armoires du client doivent être nettoyées et libérées de tous matériaux et débris de construction.

4.5 Exigences relatives à l'acceptation des travaux

4.5.1 Construction de la salle de données du client

a) Les officiers de la sécurité du client devront examiner les plans détaillés de la salle de données du client lorsque complété à 33%, 66% et 99% afin de s'assurer que les exigences en matière de sécurité décrites dans la section 2.1.8 ont été respectées.

b) Les officiers de la sécurité du client exécuteront des tests d'acceptation des enceintes blindées contre les radiofréquences, tel que détaillées dans le document ITSG-02 du Centre de la sécurité des télécommunications Canada, pouvant être trouvé à l'adresse suivante :

Français

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-fra.html

Anglais

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-eng.html

4.5.2 Procédure d'essai d'acceptation de la salle des données

a) Trente (30) jours civils après l'attribution du contrat, lorsqu'il déclare que la salle de données du client est prête à être utilisée, l'entrepreneur doit accorder au client 15 jours civils consécutifs pour lui permettre d'effectuer ses essais d'acceptation de la salle de données.

b) Le client fournira un plan d'essai à l'entrepreneur au plus tard 15 civils après les essais d'acception de la salle de données du client.

c) L'entrepreneur permettra alors au client de livrer un ensemble représentatif d'équipement et d'armoires de TI (selon le cas) aux installations où devront avoir lieu les essais.

d) L'entrepreneur déballera et déplacera l'équipement du client dans la salle de données du client.

e) Le client installera son équipement informatique dans les armoires et l'équipement autonome au besoin.

f) L'essai d'acceptation du client comportera notamment les étapes suivantes :

i) essai des connexions réseau;

ii) essai des bus à bloc d'alimentation double;

iii) construction de la salle de données;

iv) mécanismes d'accès à la salle des données.

g) Tous les éléments que le client ne considère pas comme conforme au contrat seront pris en note par le client. Une copie papier du document sera fournie à l'entrepreneur et à l'autorité

contractante au plus tard 5 jours civils après la fin de l'essai d'acceptation de la salle de données du client.

h) L'entrepreneur disposera de 10 jours civils pour corriger tous les éléments jugés non conformes par le client. L'entrepreneur doit fournir une preuve écrite au client que chaque élément a été corrigé. Le client peut, à son gré, faire un autre essai et effectuer l'essai d'acceptation de la salle de données du client après réception des documents envoyés par l'entrepreneur jusqu'à ce qu'il soit satisfait et considère que les exigences ont été respectées.

i) Le client fournira une copie papier du document d'acceptation de la salle de données du client à l'entrepreneur et à l'autorité contractante au plus tard 10 jours civils suivant l'essai concluant.

4.5.3 Plan de transition du client

Les activités entreprises par l'entrepreneur pour établir les services TI du client dans ses installations constituent la transition.

a) L'entrepreneur doit fournir un modèle de plan de transition au moins 40 jours civils après la date d'attribution du contrat. Le modèle de plan de transition décrit, à tout le moins, l'approche générale et les activités types de migration du matériel de TI du client depuis les locaux de ce dernier jusqu'aux installations de l'entrepreneur, notamment, la configuration et la conception, l'installation, les essais et l'exploitation initiale de la salle de données du client. Le plan de transition doit être coordonné avec le plan de migration du client.

b) L'entrepreneur doit organiser une première réunion de planification de la transition avec client pour entamer l'élaboration du plan de transition au moins 45 jours civils avant la date d'attribution du contrat.

c) L'entrepreneur travaillera en collaboration avec le client pour dresser le plan de transition immédiatement après la première réunion, le mettra à jour au besoin et produira des plans révisés suivant des cycles de 5 jours civils. Le plan de transition doit être coordonné avec le plan de migration du client jusqu'à ce que toutes les activités de migration du client soient terminées.

d) L'entrepreneur produira le plan de transition final au moins 60 jours civils après la date d'attribution du contrat. Ce plan donnera comprendra une description, dans les grandes lignes, des activités ci-dessous :

   i) activités relevant de l'entrepreneur :

      1) élaboration du calendrier de transition;

      2) élaboration de l'aménagement du matériel du client;

      3) essai des brides d'alimentation;

      4) essai des connexions réseau depuis les points de présence de télécommunications à la salle de données du client;

      5) entreposage sécuritaire et temporaire du matériel du client, au besoin;

      6) déballage du matériel du client;

      7) enlèvement des caisses d'emballage;

      8) déplacement du matériel du client vers la salle de données du client.

4.5.4 Aménagement du client

« Aménagement du client » s'entend des activités que le client mènera pour établir son infrastructure de technologie de l'information (TI) dans sa salle de données. Ce travail débutera au plus tard 70 jours après la date d'attribution du contrat :

a) activités relevant du client :

1) examen et approbation de l'aménagement du matériel par le client;
2) examen et approbation du calendrier par le client;
3) conception du réseau;
4) installation et aménagement du réseau, et connexion des armoires et du matériel autonome du client au réseau;
5) essai des connexions réseau de la salle de données du client;
6) livraison de l'équipement sur place;
7) installation du matériel informatique du client dans les armoires;
8) essai de la connectivité du matériel du client installé.

NOTA. – Les délais relatifs à la mise en œuvre des services énoncés sont la responsabilité de l'entrepreneur et du client. Tout retard attribuable au Canada entraînera un report des délais subséquents.

5 Autres services de base

Conformément aux « Tableaux d'établissement des prix », l'entrepreneur doit fournir tous les services permettant de répondre aux exigences énoncées ci-dessous.

a) L'entrepreneur doit fournir et installer des armoires et des unités de distribution de l'alimentation de centre de données (CPDU) pour accueillir le matériel informatique du client (voir les spécifications à l'article 5 b) ci-dessous). L'installation des armoires comprendra ce qui suit :

   i) l'alimentation électrique, ce qui comprend les circuits, le câblage des circuits et les prises de courant s'il y a lieu;

   ii) les systèmes de refroidissement, ce qui comprend les dispositifs de confinement d'air, les panneaux d'obturation, les dispositifs d'aération et tout autre composant nécessaire au refroidissement du matériel de TI du client, en conformité avec la solution de refroidissement proposée par l'entrepreneur.

b) Les armoires et CPDU fournies par le client doivent respecter les spécifications présentées ci-dessous.

Article	Configuration
Armoire de serveur – 42U	Comprend tous les dispositifs d'aération et de circulation d'air, des panneaux latéraux, dispositifs de gestion des câbles, chemins de câbles, attaches antisismiques, rails et portes verrouillables avec ensemble de clés uniques 30 po de largeur x 42 po de profondeur x 84 po de hauteur
Armoire de réseau – 42U	Comprend tous les dispositifs d'aération et de circulation d'air, des panneaux latéraux, dispositifs de gestion des câbles, chemins de câbles, attaches antisismiques, rails et porte verrouillables avec ensemble de clés uniques 30 po de largeur x 42 po de profondeur x 84 po de hauteur 40 po de largeur x 42 po de profondeur x 84 po de hauteur

CPDU	Peut comporter au moins 12 prises C13 et 12 prises C19 IEC : avec accès du protocole de gestion de réseau simple (SNMP) pour la réinitialisation de l'alimentation et la surveillance de la consommation d'énergie à distance

Le client se reportera aux modèles d'armoires et de CPDU mis en œuvre par l'entrepreneur pour orienter les fournisseurs concernant les critères applicables aux plateformes informatiques intégrées, configurées et montées dans des baies, en usine.

c) L'entrepreneur doit installer dans la salle de données le matériel autonome particulier du client qui ne correspond pas aux configurations d'armoire et de CPDU normalisées. L'entrepreneur devra peut-être tenir compte de facteurs particuliers concernant le refroidissement, les circuits d'alimentation spécialisés et le câblage, y compris pour l'équipement de 208 V triphasé. On prévoit que l'infrastructure de TI du client comprendra 90 % d'équipement monté dans des baies et 10 % de matériel autonome.

d) L'entrepreneur doit fournir et installer des chemins de câblage dans la salle de données du client afin que tous les câbles réseau et d'alimentation se terminent dans les armoires du client ou à l'équipement autonome.

e) L'entrepreneur doit fournir et installer le câblage réseau au point de terminaison du réseau de la salle de données du client.

f) L'entrepreneur doit fournir des services de câblage, en conformité avec l'architecture de câblage du client, soit fournir et installer le matériel requis, y compris :

i) fournir une configuration de câblage de réseau conforme à la norme la plus récente sur l'infrastructure de télécommunications TIA-942 pour les centres de données;

ii) installer des câbles à paires torsadées non blindées (UTP) et à fibres optiques;

iii) effectuer la connexion aux réseaux locaux Ethernet à l'aide de câbles UTP et à fibres optiques et du matériel;

iv) dresser des plans d'installation précis, fournissant un calendrier de mise en œuvre, une analyse des coûts et des rapports d'avancement;

v) installer et mettre à l'essai un réseau fédérateur pour réseau local sur câbles à fibres optiques et UTP, installer et mettre à l'essai la distribution horizontale et les interconnexions, et planifier les chemins des câbles et des conduits;

vi) effectuer les déplacements, ajouts et modifications – répondre aux besoins courants, ainsi que se charger des réinstallations importantes de matériel de traitement de données liées aux systèmes de câblage;

vii) effectuer les réparations – veiller au remplacement ou à la réparation des câbles endommagés et restauration de la connectivité;

viii) effectuer les mises à niveau – mettre à jour les réseaux de câbles existants conformément aux exigences opérationnelles;

ix) mettre à jour les dossiers et plan – mettre à jour les dossiers et aux plans de câblage au besoin et lorsque des changements sont apportés au système de câblage par l'entrepreneur responsable de l'installation du câblage.

g) L'entrepreneur doit mettre à l'essai les connexions réseau pour confirmer la connectivité d'un point à l'autre de la salle de télécommunications au point de terminaison du client.

h) L'entrepreneur doit fournir les services d'électricien à la demande du client, pour installer ou reconfigurer les circuits électriques en conformité avec les instructions du fabricant de pièces d'origine.

6 Services facultatifs

Conformément aux « Tableaux d'établissement des prix », l'entrepreneur doit fournir, à la demande, tous les services permettant de répondre aux exigences énoncées dans les paragraphes qui suivent.

6.1 Services de soutien du matériel

a) L'entrepreneur doit être disponible en tout temps pour fournir :

i) des services de redémarrage du serveur et du matériel de TI du client dans les 30 minutes suivant une demande du client;

ii) des services de surveillance visuelle permettant de vérifier les indicateurs lumineux du serveur dans les 30 minutes suivant une demande du client.

6.2 Gestion des espaces de coimplantation

6.2.1 Installation du matériel informatique du client

a) L'entrepreneur doit installer le matériel informatique du client dans les armoires ou en mode autonome.

b) L'entrepreneur doit vérifier le démarrage du matériel informatique du client.

6.2.2 Retrait du matériel informatique du client

a) L'entrepreneur doit fournir des services de retrait du matériel informatique du client des armoires ou en mode autonome de la salle de données et l'acheminer vers l'aire d'entreposage temporaire sécurisé ou au lieu de chargement en suivant les instructions du client.

Barème A : **Cibles d'intervention pour la gestion des incidents**

Le tableau suivant précise les exigences minimales à respecter par l'entrepreneur et le client pour l'établissement et la gestion des incidents aux installations de l'entrepreneur.

Un **incident** est défini comme étant un événement qui entraîne, ou qui risque d'entraîner, une interruption ou une diminution de la qualité du service.

Les **répercussions d'un incident** sont définies comme étant la mesure de la criticité d'un incident ou d'un problème pour l'entreprise, et l'urgence est définie comme étant la vitesse d'intervention requise.

Un **problème** est défini comme étant la cause sous-jacente inconnue d'un ou de plusieurs incidents. Un problème devient une erreur connue lorsque la cause originale est connue et qu'une solution définitive ou une solution de contournement a été identifiée.

Priorité	**Description**	**Intervention**
1 – Critique	Interruption du service pour le client • Incidents caractérisés par une défaillance réelle ou imminente dans les installations de l'entrepreneur, où le client subit (ou subira) des problèmes de défaillance de divers niveaux du matériel de TI du client	• L'entrepreneur doit aviser le bureau de dépannage du client au plus tard 15 minutes après que l'incident se soit produit. • L'entrepreneur doit régler le problème dans un délai de 2 heures après le début de l'incident. • L'entrepreneur doit fournir au responsable technique un rapport des progrès accomplis toutes les 30 minutes jusqu'à ce que le problème soit résolu. • Lorsque le problème est réglé, l'entrepreneur doit consigner par écrit l'incident et la solution, et envoyer un exemplaire du document au responsable technique dans un délai de 7 jours civils suivant la résolution du problème. • Le changement requis pour résoudre l'incident doit être inscrit comme étant un changement non prévu dans le Système de gestion des changements.

Priorité	Description	Intervention
2 – Élevée	Dégradation du service pour le client • Incidents caractérisés par une défaillance réelle ou imminente dans les installations de l'entrepreneur, où le client subit (ou subira) une perte complète de la redondance de toute composante des services de coimplantation pouvant entraîner la panne de tout matériel de TI du client	• L'entrepreneur doit aviser immédiatement le bureau de dépannage du client au plus tard 30 minutes après que l'incident se soit produit. • L'entrepreneur doit régler le problème dans un délai de 8 heures après le début de l'incident. • L'entrepreneur doit fournir au responsable technique un rapport des progrès accomplis toutes les heures à partir du moment où le problème s'est produit jusqu'à ce que le problème soit résolu. • Lorsque le problème est réglé, l'entrepreneur doit consigner l'incident et la solution, et envoyer un exemplaire du document au responsable technique dans un délai de 7 jours civils suivant la résolution du problème.
3 – Moyenne	Dégradation du service Incidents où toute entente sur les niveaux de service n'a pas été respectée et n'est pas directement liée à la salle de données du client	• L'entrepreneur doit aviser le bureau de dépannage du client au plus tard 60 minutes après que l'incident se soit produit. • L'entrepreneur doit régler le problème dans un délai de 24 heures après le début de l'incident. • L'entrepreneur doit fournir au responsable technique un rapport des progrès accomplis toutes les 6 heures jusqu'à ce que le problème soit résolu. • Lorsque le problème est réglé, l'entrepreneur doit consigner l'incident et la solution, et fournir l'information dans un rapport d'avancement mensuel.
4 – Faible	Problème • Incidents caractérisés par aucune dégradation du service et aucune répercussion sur le matériel de TI du client	• L'entrepreneur doit aviser le bureau de dépannage du client au plus tard 12 heures après que l'incident se soit produit. • L'entrepreneur doit résoudre le problème dans un délai de 7 jours civils après le début de l'incident. • L'entrepreneur doit fournir au responsable technique un rapport des progrès accomplis sur demande jusqu'à ce que le problème soit résolu. • Lorsque le problème est réglé, l'entrepreneur doit consigner l'incident et la solution, et fournir l'information dans un rapport d'avancement mensuel.

Barème B : **Cibles d'intervention pour la gestion des incidents de sécurité**

Le tableau suivant précise les exigences minimales à respecter par l'entrepreneur et le client pour l'établissement et la gestion des incidents de sécurité dans les installations de l'entrepreneur.

Priorité	**Description**	**Indicateurs de rendement**
1 – Critique	Incident de sécurité à priorité critique • Incidents de sécurité entraînant la défaillance à divers niveaux de tout matériel de TI du client	• L'entrepreneur doit réagir à un incident à priorité critique conformément au Barème A – Cibles d'intervention pour la gestion des incidents. • L'entrepreneur doit tenir une réunion avec le client dans un délai de 7 jours civils suivant l'incident de sécurité, afin de discuter de l'incident et des mesures prises par l'entrepreneur pour éviter que le même problème ne se reproduise.
2 – Élevée	Incident de sécurité à priorité élevée • Incidents de sécurité pouvant risquer de compromettre tout équipement TI du client ou toutes applications du client	• L'entrepreneur doit réagir à un incident de sécurité à priorité élevée conformément au Barème A – Cibles d'intervention pour la gestion des incidents. • L'entrepreneur doit tenir une réunion avec le client dans un délai de 7 jours civils suivant l'incident de sécurité, afin de discuter de l'incident et des mesures prises par l'entrepreneur pour éviter que le même problème ne se reproduise.
3 – Moyenne	Incident de sécurité à priorité moyenne • Incident de sécurité entraînant l'accès non autorisé à toute aire sécurisée • Aucune interruption du service pour le client	• L'entrepreneur doit réagir à un incident de sécurité à priorité moyenne conformément au Barème A – Cibles d'intervention pour la gestion des incidents. • L'entrepreneur doit tenir une réunion avec le client dans un délai de 7 jours civils suivant l'incident de sécurité, afin de discuter de l'incident et des mesures prises par l'entrepreneur pour éviter que le même problème ne se reproduise.
4 - Faible	Incident de sécurité à priorité faible • Atteinte générale à la sécurité, ce qui exclut l'accès non autorisé à la salle de données du client • Aucune interruption du service pour le client	• L'entrepreneur doit réagir à un incident de sécurité à priorité faible conformément au Barème A – Cibles d'intervention pour la gestion des incidents.

Barème C : **Cibles d'intervention pour la gestion des changements**

Le tableau suivant précise les exigences minimales à respecter par l'entrepreneur et le client pour l'établissement et la gestion des changements aux installations de l'entrepreneur.

Priorité	**Description**	**Indicateurs de rendement**
Priorité 1 Changement urgent non prévu	Tout changement urgent non prévu et demandé par l'entrepreneur Le changement peut entraîner une dégradation du service pour un ou plusieurs clients. Le changement peut être nécessaire pour résoudre un problème lié à l'un des éléments suivants : • barème A, incident à priorité 1, 2 ou 3; • barème B, incident de sécurité à priorité 1, 2 ou 3.	• L'entrepreneur doit aviser le bureau de dépannage du client au plus tard 15 minutes suivant la demande de changement. • L'entrepreneur doit apporter le changement dans les 24 jours suivant la demande de changement. • L'entrepreneur doit demander l'approbation lorsque c'est possible à tous les clients qui peuvent subir une dégradation ou une interruption du service causée par le changement effectué. • L'entrepreneur doit fournir au responsable technique un rapport rétrospectif au plus tard 3 jours civils suivant le changement imprévu. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».
Priorité 2 Changement urgent	Tout changement urgent prévu ou non prévu demandé par l'entrepreneur Le changement peut entraîner une dégradation du service pour un ou plusieurs clients. Le changement peut être nécessaire pour résoudre un problème lié à l'un des éléments suivants : • barème A, incident à priorité 2 ou 3; • barème B, incident de sécurité à priorité 2 ou 3.	• L'entrepreneur doit aviser le service de dépannage du client au plus tard 30 minutes suivant la demande de changement. • L'entrepreneur doit apporter le changement dans les 7 jours civils suivant la demande de changement. • L'entrepreneur doit obtenir l'approbation de tous les clients qui peuvent subir une dégradation ou une interruption du service causée par le changement. • L'entrepreneur doit fournir au responsable technique un rapport rétrospectif au plus tard 7 jours civils suivant le changement. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».

Priorité	Description	Indicateurs de rendement
Priorité 3 Changement normal	Tout changement normal prévu ou non prévu demandé par l'entrepreneur ou le client. Le changement peut entraîner une dégradation du service pour un ou plusieurs clients. Le changement peut être nécessaire pour résoudre un problème lié à l'un des éléments suivants : • barème A, incident à priorité 2 ou 3; • barème B, incident de sécurité à priorité 2 ou 3.	• L'entrepreneur et le client doivent aviser l'autre partie dans les 24 heures suivant la demande de changement. • L'entrepreneur doit apporter le changement dans les 30 jours civils suivant la demande de changement ou comme convenu avec le client. • L'entrepreneur doit obtenir l'approbation de tous les clients qui peuvent subir une dégradation ou une interruption du service causée par le changement. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».
Priorité 4 Changement prévu à court terme	Tout changement prévu à court terme et demandé par l'entrepreneur ou le client	• L'entrepreneur et le client doivent aviser l'autre partie au plus tard 14 jours civils suivant la demande de changement. • L'entrepreneur doit apporter le changement au moins 3 mois et au plus 6 mois suivant la demande de changement. • L'entrepreneur doit obtenir l'approbation de tous les clients qui peuvent subir une dégradation ou une interruption du service causée par le changement. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».
Priorité 5 Changement prévu à long terme	Tout changement prévu à long terme et demandé par l'entrepreneur ou le client	• L'entrepreneur et le client doivent aviser l'autre partie au plus tard 14 jours civils suivant la demande de changement. • L'entrepreneur doit apporter le changement au moins 6 mois après la demande de changement. • L'entrepreneur doit obtenir l'approbation de tous les clients qui peuvent subir une dégradation ou une interruption du service causée par le changement. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».

Priorité	Description	Indicateurs de rendement
Priorité 6 Changement touchant à l'information	Tout changement touchant à l'information et demandé par l'entrepreneur ou le responsable technique. Le changement ne présentera aucun risque et n'entraînera aucune interruption de service pour le client. Le changement peut se rapporter, notamment : • à la liste du personnel de l'entrepreneur; • à la liste des personnes-ressources du responsable technique; • à une demande d'ouverture de compte dans les systèmes de gestion des incidents, des problèmes et des changements.	• L'entrepreneur et le client doivent aviser l'autre partie immédiatement suivant la demande de changement. • L'entrepreneur doit apporter le changement dans les 7 jours civils suivant la demande de changement. • L'entrepreneur doit consigner le changement conformément aux exigences minimales exposées à l'appendice E, « Rapport mensuel sur les changements ».

Appendice A – **Rapport hebdomadaire d'avancement sur la mise en œuvre des services**

Voici les exigences minimales relatives au Rapport hebdomadaire d'avancement sur la mise en œuvre des services.

1 Introduction
2 Portée
3 Objectif
4 Contexte
5 Aperçu
6 Renseignements sur le projet
  6.1 Nom du projet
  6.2 Phase
  6.3 Date de début prévue
  6.4 Date de fin prévue
  6.5 Gestionnaire de projet
7 Renseignement sur la phase en cours du projet
  7.1 Réalisations durant la période visée du rapport
  7.2 Activités prévues durant la prochaine période visée par le rapport
  7.3 Activités non prévues (achevées ou à venir)
8 Enjeux et problèmes demandant une attention ou des mesures
  8.1 Problèmes liés au projet
    8.1.1 Description des problèmes
    8.1.2 État
    8.1.3 Solution proposée
    8.1.4 Date de résolution prévue
    8.1.5 Date de résolution revue
    8.1.6 Date de résolution réelle
  8.2 Risques
    8.2.1 Numéro du risque
    8.2.2 Description du risque
    8.2.3 Probabilité
    8.2.4 Incidence
    8.2.5 Atténuation
    8.2.6 Risque résiduel
  8.3 Rapport sur les retards par rapport au calendrier
    8.3.1 Activité
    8.3.2 Raison du retard
    8.3.3 Répercussions du retard
    8.3.4 Mesure visant à corriger les répercussions du retard
    8.3.5 Répercussions sur le calendrier

Appendice B – **Plan de gestion du projet de mise en œuvre des services**

Voici les exigences minimales relatives au plan de gestion du projet de mise en œuvre des services.

1 Aperçu du projet
- 1.1 Introduction
- 1.2 Stratégie du projet
- 1.3 But, portée et objectifs
- 1.4 Hypothèses et contraintes
- 1.5 Définitions et sigles

2 Organisation du projet
- 2.1 Description de la structure de gestion
- 2.2 Description de l'équipe de gestion du projet

3 Plan de travail
- 3.1 Description générale
- 3.2 Principales étapes et calendrier
  - 3.2.1 Preuve de détention du nouveau permis de construire ou de modernisation
  - 3.2.2 Examens de la conception à 33 %,66 %,99 % de l'avancement du projet
  - 3.2.3 Examen de la sécurité par le client
  - 3.2.4 Document d'attestation de la conception d'Uptime
  - 3.2.5 Permis de construction
  - 3.2.6 Achèvement de la structure du bâtiment (toit et murs extérieurs montés)
  - 3.2.7 Bâtiment connecté au réseau électrique
  - 3.2.8 Éléments électriques principaux livrés sur le site (câbles UPS, générateur, unité de distribution de l'alimentation (PDU))
  - 3.2.9 Systèmes mécaniques principaux livrés sur le site (appareil de climatisation ou refroidisseurs, roue thermique)
  - 3.2.10 Réseau de fournisseurs en télécommunications acheminé aux salles de télécommunications
  - 3.2.11 Salle des ordinateurs prête pour la mise en service du client
  - 3.2.12 Permis d'occupation
  - 3.2.13 Tous les systèmes mis en service
  - 3.2.14 Points de contrôle de la surveillance continue de la sécurité
  - 3.2.15 Essai par l'entrepreneur
  - 3.2.16 Attestation de niveau III d'Uptime
  - 3.2.17 Essai par le client
  - 3.2.18 Attestation de LEED
  - 3.2.19 Approbation du plan de transition du client

4 Plan de suivi du projet
- 4.1 Gestion des exigences
- 4.2 Contrôle du calendrier
- 4.3 Contrôle de la qualité

5 Plan de gestion des risques
- 5.1 Liste des risques
  - 5.1.1 Description du risque
  - 5.1.2 Description de l'incidence du risque
  - 5.1.3 Évaluation des probabilités
  - 5.1.4 Évaluation du risque
  - 5.1.5 Stratégies d'atténuation

6 Plan de mise en service du client, plan d'essai et plan de transition du client

6.1 Conception et aménagement de la salle de données du client.
6.2 Élaboration du calendrier de transition
6.3 Installation et aménagement (alimentation et réseau) des armoires et du matériel autonome du client
6.4 Essai des raccords d'alimentation
6.5 Essai des connexions réseau
6.6 Installation du matériel informatique du client dans les armoires
6.7 Essai de la connectivité du matériel installé du client

Appendice C – **Procès-verbaux des réunions**

Voici les exigences minimales relatives aux procès-verbaux des réunions.

1 Titre de la réunion
2 Date de la réunion
3 Heure de la réunion
4 Participants
5 Absents
6 Procès-verbal dressé par
7 Copie du procès-verbal acheminée à
8 Procès-verbal des discussions
9 Compte-rendu des décisions
10 Mesures de suivi soulevées
11 Autres affaires
12 Prochaine réunion
13 Appendice – Liste des mesures de suivi
    13.1 Aperçu
    13.2 Numéro de la mesure de suivi
    13.3 Description de la mesure de suivi
    13.4 Personne chargée du suivi (BPR)
    13.5 Date de mise en œuvre
    13.6 Date de fin
    13.7 Commentaires

Appendice D – **Rapport mensuel sur les services**

Voici les exigences minimales relatives au rapport mensuel sur les services à présenter pendant la période de mise en service du client.

1 Résumé des incidents
- 1.1 Résumé général
  - 1.1.1 Nombre total d'incidents
  - 1.1.2 Nombre d'incidents par gravité

2 Résumé des problèmes
- 2.1 Résumé général
  - 2.1.1 Nombre total de problèmes
  - 2.1.2 Nombre de problèmes en ordre de gravité

3 Résumé des solutions
- 3.1 Description du problème
- 3.2 Gravité du problème
- 3.3 Description de la solution
- 3.4 Rapidité de la solution

4 Résumé des changements
- 4.1 Description du changement
- 4.2 Importance du changement
- 4.3 Résultat du changement

5 Disponibilité du service

6 Fiabilité du service

7 Capacités du service
- 7.1 Consommation de l'électricité globale et par circuit
- 7.2 Superficie occupée
- 7.3 Réfrigération globale et pour la salle de données du client

8 Seuil à partir duquel une expansion des services est requise

9 Plans ultérieurs pour l'entrepreneur et le client

Appendice E – **Rapport mensuel sur les changements**

Voici les exigences minimales relatives au rapport mensuel sur les changements à présenter pendant la période de mise en service du client.

1 Résumé des changements non prévus de l'entrepreneur (effectués)
- 1.1 Résumé général
  - 1.1.1 Nombre total de changements non prévus
  - 1.1.2 Nombre de changements non prévus en ordre de gravité
  - 1.1.3 Liste des changements non prévus
    - 1.1.3.1 Description
    - 1.1.3.2 Gravité
    - 1.1.3.3 Résultat des changements non prévus

2 Résumé des changements prévus par l'entrepreneur (effectués)
- 2.1 Résumé général
  - 2.1.1 Nombre total de changements prévus
  - 2.1.2 Nombre total de changements prévus en ordre de gravité
  - 2.1.3 Liste des changements prévus
    - 2.1.3.1 Description
    - 2.1.3.2 Gravité
    - 2.1.3.3 Résultat du changement prévu

3 Résumé des changements prévus et demandés par le client (effectués)
- 3.1 Résumé général
  - 3.1.1 Nombre total de changements prévus
  - 3.1.2 Nombre total de changements prévus en ordre de gravité
  - 3.1.3 Liste des changements prévus
    - 3.1.3.1 Description
    - 3.1.3.2 Demandeur
    - 3.1.3.3 Gravité
    - 3.1.3.4 Résultat du changement prévu

4 Résumé des changements prévus de l'entrepreneur (à venir)
- 4.1 Résumé général
- 4.2 Nombre total de changements prévus
- 4.3 Nombre total de changements prévus en ordre de gravité
- 4.4 Liste des changements prévus
- 4.5 Description
- 4.6 Gravité
- 4.7 Résultat du changement prévu

5 Résumé des changements prévus et demandés par le client (à venir)
- 5.1 Résumé général
  - 5.1.1 Nombre total de changements prévus
  - 5.1.2 Nombre total de changements prévus en ordre de gravité
  - 5.1.3 Liste des changements prévus
    - 5.1.3.1 Description
    - 5.1.3.2 Demandeur
    - 5.1.3.3 Gravité
    - 5.1.3.4 Résultat du changement prévu

Appendice F – **Politique d'utilisation acceptable**

Tous les clients du centre de données en coimplantation doivent accepter et respecter la politique d'utilisation acceptable qui doit, à tout le moins, prévoir les conditions énoncées ci-dessous.

(a) Le client ne doit utiliser les services fournis par l'entrepreneur qu'à des fins licites.
(b) Le client ne doit pas transmettre, retransmettre, rediriger, afficher ni stocker du matériel en violation de toute loi applicable (y compris les droits protégés par droits d'auteur, secret commercial, brevet ou autre droit de propriété intellectuel ou d'autres lois ou règles semblables), normes de l'industrie ou de la communauté. Cela comprend le matériel obscène, indécent, diffamatoire, calomniateur, raciste ou menaçant.
(c) Le client ne peut s'engager dans une activité qui pourrait interférer ou interférera avec le service d'un autre utilisateur, hôte ou réseau.
(d) Le client ne peut s'engager dans la distribution de logiciels, programmes ou messages qui peuvent causer des dommages ou nuire aux personnes, données et systèmes informatiques.
(e) Le client ne peut s'engager dans des activités frauduleuses, y compris faire sciemment de fausses déclarations ou des déclarations trompeuses, présenter des écrits ou mener des activités faites dans l'intention d'inciter les gens à réagir ni de se procurer des services dans l'intention d'éviter le paiement et être hôte d'un site web qui pratique le « hameçonnage ».
(f) Le client ne doit avoir aucune activité considérée comme étant annonciatrice de tentatives de manquement à la sécurité, y compris toute forme de numérisation, de sondages ou d'autres essais ou d'activité de collecte de données.
(g) Le client ne doit pas essayer de percer les mesures de sécurité des autres systèmes.
(h) Le client ne peut essayer d'avoir un accès non autorisé comprenant un accès illégal, non autorisé ou une tentative d'accès, à d'autres ordinateurs, comptes, réseaux ou systèmes.
(i) Le client ne peut entrer aucun article interdit dans le centre de données (dans les endroits où le plancher est surélevé). Les articles interdits comprennent les articles suivants :
    - matériau combustible (p. ex. carton);
    - nourriture et boisson;
    - explosifs et armes;
    - matières dangereuses;
    - alcool, drogues illégales et autres substances intoxicantes;
    - appareils électromagnétiques;
    - matières radioactives;
    - caméras ou tout autre dispositif d'enregistrement.
(j) Le client ne peut stocker aucun matériau dans la salle de données du client (autre que les guides d'utilisation de l'équipement).
(k) Le client ne peut stocker aucun matériau dans les aires communes (c.-à-d. les corridors ou les plateformes de chargement).
(l) Le client ne peut lever les tuiles du planche surélevé ni entrer dans les murs.
(m) Le client ne peut prendre des photos sans le consentement écrit du gestionnaire des installations.
(n) Le client ne peut sous-louer ou permettre autrement l'utilisation de son espace à d'autres organismes ou personnes qui ne sont pas explicitement nommés dans le contrat du client ou lorsque le client n'a pas la responsabilité légale complète.

Appendice G – **Liste des sigles**

Sigle	Appellation complète
CPDU	Unité de distribution de l'alimentation d'armoire (barre d'alimentation)
CVCA	Chauffage, ventilation et conditionnement d'air
DAM	Déplacements, ajouts et modifications
DG	Directeur général
DPI	Dirigeant principal de l'information
EFCD	Étude de faisabilité sur les centres de données
GC	Gouvernement du Canada
GP	Gestion de produits (secteur de la DGSIT)
km	Kilomètre
kVA	Kilovoltampères
LEED	Leadership in Energy and Environmental Design
MW	Mégawatt
PDU	Unité de distribution de l'alimentation
PGP	Plan de gestion de projet
PUE	Efficacité énergétique
Rl	Réseau local
SCN	Secteur de la capitale nationale
SNMP	Protocole de gestion de réseau simple
SPC	Services partagés Canada
SRT	Structure de répartition du travail
TI	Technologie de l'information
TIA	Telecommunications Industry Association
UTP	Paire torsadée non blindée (câble UTP)
VA	Voltampères

Appendice H – **Topologie normalisée des niveaux de l'Uptime Institute (*Tier Standard: Topology*)**

Note aux soumissionnaires :

Le document «Data Center Site Infrastructure Tier Standard: Topology» suit.

Appendice I – **Exigences en matière de sécurité**

Note aux soumissionnaires :

Le document «G13-01, Pièces d'entreposage sécuritaire» et Le document «G13-02, Mur mitoyen sécuritaire» suit.

UPTIME INSTITUTE, LLC

Data Center Site Infrastructure Tier Standard: Topology

Préparé par Uptime Institute Professional Services, LLC

20 West 37th Street – 6th Floor
New York, NY 10018

Uptime Institute, LLC

Résumé: La *Tier Standard: Topology* de l'Institute est une base objective permettant de comparer les fonctionnalités, la capacité et la disponibilité prévue (ou performance) de la topologie de la conception de l'infrastructure d'un site en particulier par rapport à d'autres sites, ou pour comparer un groupe de sites. Cette Standard décrit les critères nécessaires à la différenciation des quatre classes de topologie des infrastructures de sites fondés sur des niveaux croissants de composants de capacité redondants et sur les chemins de distribution. Cette Standard met l'accent sur les définitions des quatre niveaux et sur les tests de confirmation du rendement pour déterminer la conformité aux définitions. Le commentaire, dans une section distincte, fournit des exemples pratiques de conception et de configuration des systèmes d'infrastructure de site qui répondent aux définitions de Tier comme un moyen de clarifier les critères de Classification par Tier.

Mots-clés: températures ambiantes, réponse autonome, disponibilité, classification, compartimentation , maintenance concurrente, fonction de maintenance simultanée, refroidissement continu, centre de données, thermomètre sec, double alimentation, insensibilité aux défaillances, insensible aux défaillances, fonctionnalité, infrastructure, paramètres, viabilité opérationnelle, rendement, redondant, fiabilité, niveau, sous-niveau, niveaux, topologie, thermomètre mouillé

Introduction

Cette introduction ne fait pas partie de Data Center Site Infrastructure Tier Standard: Topology de l'Institute. Elle fournit au lecteur le contexte pour l'application de la Standard.

Data Center Site Infrastructure Tier Standard: Topology de cet Institute est une réaffirmation du contenu déjà publié dans la publication de l'Institute *Tier Classifications Define Site Infrastructure Performance*. Un contenu partiel de cette publication a été réédité dans un format sur le modèle des Standards ANSI. Les futures mises à jour ou modifications à *Tier Standard: Topology* de l'Institute seront faites par un processus d'examen et de recommandations compatible avec les autres organismes de Standards reconnus.

Les Tier Classifications ont été créés pour décrire de façon constante la topologie de l'infrastructure du site nécessaire pour soutenir les opérations d'un centre de données, et non pas les caractéristiques des différents systèmes ou sous-systèmes. Les centres de données exigent le bon fonctionnement intégré des systèmes électriques, mécaniques, de chauffage et de climatisation du bâtiment. Chaque sous-système ou système doit être constamment déployé avec le même objectif de disponibilité du site pour satisfaire les besoins distincts du Tier. La perspective la plus critique dont les propriétaires et concepteurs doivent tenir compte, lorsqu'ils sont obligés de faire des compromis pour prendre une décision, est l'effet de la décision sur l'exploitation intégrée dans le cycle de vie de l'environnement informatique dans la salle des ordinateurs.

Autrement dit, la cote du Tier de la topologie d'un site entier est limitée par la capacité du plus faible sous-système qui aura une incidence sur le fonctionnement du site (le maillon le plus faible de la chaîne). Par exemple, un site avec une configuration du système d'alimentation sans coupure robuste de Tier IV combinée avec un système d'eau réfrigérée de Tier II, donne une cote de Tier II au site.

Cette définition très stricte est supportée par les cadres supérieurs, qui ont approuvé des investissements de plusieurs millions de dollars pour un rapport objectif des capacités réelles du site. Toutes les exceptions et les exclusions signalées dans les documents d'approbation seront rapidement perdues et oubliées. Si un site a été publicisé dans une organisation comme étant Fault Tolerant (Tier IV), avoir à planifier un arrêt du site à tout moment dans l'avenir ne serait pas compatible, indépendamment de toutes les exclusions en « petits caractères » qui identifient le risque avec diligence. Pour cette raison, il n'y a pas de cotes partielles ou fractionnaires de Tier. La cote de Tier d'un site n'est pas la moyenne des cotes de tous les sous-systèmes critiques de l'infrastructure du site. Le classement par Tier du site est la cote la plus basse des sous-systèmes individuels.

De même, la classification par Tier ne peut être réclamée à l'aide du temps moyen entre pannes, calculé pour la fiabilité statistique des composants pour produire une disponibilité prévisionnelle et en utilisant ce nombre pour correspondre à la disponibilité des résultats empiriques avec ceux des sites représentant les différentes Tier Classifications. Des valeurs de composant statistiquement valides ne sont pas disponibles, en partie parce que les cycles de vie des produits deviennent plus courts et qu'il n'y a pas de base de données indépendante, à l'échelle de l'industrie, pour recueillir les données de défaillance.

Enfin, cette Standard se concentre sur la topologie et le rendement d'un site en particulier. Des niveaux élevés de disponibilité pour l'utilisateur final peuvent être atteints grâce à l'intégration d'architectures informatiques complexes et des configurations de réseau qui tirent parti des applications synchrones en cours d'exécution sur plusieurs sites. Cette Standard est toutefois indépendante des systèmes d'exploitation TI du site.

Droits d'auteur

Les participants

Le contenu original de la *Data Center Site Infrastructure Tier Standard: Topology* a été développé par les personnes suivantes :

W. Pitt Turner, IV John H. Seader Vincent E. Renaud

Avec la contribution à la rédaction de :

Julian S. Kudritzki Kenneth G. Brill

Table des matières

1. Vue d'ensemble

1.1 Portée

Cette Standard établit quatre définitions distinctes pour la classification des Tier de l'infrastructure d'un centre de données (Tier I, Tier II,Tier III, Tier IV), et pour les tests de confirmation du rendement pour déterminer la conformité aux définitions. Les Tier Classifications ont été créées pour décrire de façon constante la topologie de l'infrastructure au niveau du site nécessaire pour soutenir les opérations d'un centre de données, et non pas les caractéristiques des différents systèmes ou sous-systèmes. Cette Standard est fondée sur l'hypothèse que les centres de données exigent le bon fonctionnement intégré de plusieurs sous-systèmes distincts de l'infrastructure du site, dont le nombre varie en fonction des diverses technologies (p. ex., production d'électricité, réfrigération, sources d'alimentation sans coupures, etc.) sélectionnées pour soutenir le l'exploitation.

Chaque sous-système ou système intégré dans l'infrastructure d'un site de centre de données doit être constamment déployé avec le même objectif de disponibilité du site pour satisfaire les besoins distincts du Tier.

La conformité aux exigences de chaque Tier est mesurée par des tests de confirmation axés sur les résultats et les impacts opérationnels. Cette méthode de mesure est différente de la conception d'une approche normative ou une liste du matériel nécessaire.

Les commentaires relatifs à cette Standard constituent un chapitre distinct qui donne des exemples de conception et de configuration des systèmes d'un site pour chaque niveau de topologie de Tier. La section commentaire offre également des conseils sur l'application et la mise en œuvre des définitions de Tier. En outre, la section commentaire comprend une discussion et des exemples pour aider à comprendre les concepts de Tier ainsi que des informations sur des lacunes communes de conception de la topologie.

1.2 But

Le but de cette Standard est de fournir aux professionnels de la conception, les exploitants de centres de données, et les gestionnaires non techniques, un moyen objectif et efficace pour identifier la performance prévue de différentes conceptions de topologies d'infrastructure de sites de centre de données.

1.3 Références

American Society of Heating, Refrigerating, and Air-Conditioning Engineers, *ASHRAE Handbook – Fundamentals* (La dernière version).

Institute *Fault Tolerant Power Compliance Specification, Version 2.0. Specification*

1.4 Publications connexes

Accredited Tier Designer Technical Paper Series.

Des informations supplémentaires peuvent être obtenues à www.uptimeinstitute.com/resources.

2. Tier Standards d'infrastructure du site

2.1 Tier I: Infrastructure du site de base

2.1.1 Exigence fondamentale :

a) Un centre de données de Tier I de base regroupe des composants de capacité sans redondance et une seule voie de communication sans redondance pour desservir l'environnement essentiel. L'infrastructure de Tier I comprend notamment : un espace réservé aux systèmes informatiques; un système ASC pour éliminer les surtensions, les chutes de tension et les pannes d'électricité momentanées; un système de refroidissement spécialisé; un groupe électrogène pour assurer les fonctions informatiques en cas de panne d'électricité prolongée.

b) Douze heures de stockage de carburant sur place pour le moteur du/des générateur(s).

2.1.2 Tests de confirmation de la performance :

a) Il y a une capacité suffisante pour répondre aux besoins du site.

b) Les travaux projetés nécessiteront que la plupart ou la totalité des systèmes de l'infrastructure du site soit arrêtés, ce qui touchera l'environnement essentiel, les systèmes et les utilisateurs finals.

2.1.3 Incidences opérationnelles :

a) Le site est susceptible de perturbations des activités à la fois planifiées et non planifiées. Des erreurs d'opérations (humaines) des composants d'infrastructure du site entraîneront une perturbation du centre de données.

b) Toute panne ou défaillance imprévue d'un système ou d'un composant de capacité ou encore d'un élément de communication affectera l'environnement essentiel.

c) L'infrastructure du site doit être complètement fermée sur une base annuelle pour effectuer en toute sécurité l'entretien préventif et les réparations nécessaires. Des situations urgentes peuvent nécessiter des arrêts plus fréquents. L'absence d'entretien régulier augmente significativement le risque d'une interruption non planifiée, ainsi que la gravité de la défaillance qui en résultera.

2.2 Tier II: Composants redondants des capacités de l'infrastructure du site

2.2.1 Exigence fondamentale :

a) Un centre de données de Tier II regroupe des composants de capacité redondants et une seule voie de communication sans redondance pour desservir l'environnement essentiel. Les composants redondants comprennent notamment : des groupes électrogènes de secours, des modules ASC et des dispositifs de stockage de l'énergie, des systèmes de refroidissement, des systèmes de dissipation de la chaleur, des pompes, des unités de refroidissement et des réservoirs de carburant.

b) Douze heures de stockage de carburant sur place pour une capacité de « N ».

2.2.2 Tests de confirmation de la performance :

a) Les composants de capacité redondants peuvent être arrêtés de façon planifiée sans causer de panne de l'environnement critique.

b) L'arrêt des voies de communication pour en faire la maintenance ou pour d'autres activités exige l'arrêt de l'environnement essentiel.

c) Il y a suffisamment de capacité installée de façon permanente pour répondre aux besoins du site lorsque des composants redondants sont retirés du service pour une raison quelconque.

2.2.3 Incidences opérationnelles :

a) Le site est susceptible de perturbations à la fois par des activités prévues et des événements imprévus. Des erreurs d'opérations (humaines) des composants d'infrastructure du site peuvent entraîner une perturbation du centre de données.

b) Une panne imprévue d'un composant de capacité pourrait affecter l'environnement essentiel. Toute panne ou défaillance imprévue d'un système de capacité ou d'un élément de diffusion affectera l'environnement essentiel.

c) L'infrastructure du site doit être complètement fermée sur une base annuelle pour exécuter un entretien préventif et des réparations en toute sécurité. Des situations urgentes peuvent nécessiter des arrêts plus fréquents. L'absence d'entretien régulier augmente significativement le risque d'une interruption non planifiée, ainsi que la gravité de la défaillance qui en résultera.

2.3 Tier III: Infrastructure du site avec Concurrently Maintainable

2.3.1 Exigences fondamentales :

a) Un centre de données avec fonction de Concurrently Maintainable comporte des composants de capacité redondants et de multiples voies de diffusion indépendantes pour desservir l'environnement essentiel. En tout temps, une seule voie de communication suffit à desservir l'environnement essentiel.

b) Tout le matériel informatique est à double approvisionnement tel que défini par la norme de l'Institute Fault Tolerant Power Compliance Specification, Version 2.0 et adéquatement installé pour être compatible avec la topologie de l'architecture du site. Des dispositifs de transfert, notamment des commutateurs individuels, doivent être intégrés à tout environnement essentiel qui n'est pas conforme à cette spécification.

c) Douze heures de stockage de carburant sur place pour une capacité de « N ».

2.3.2 Tests de confirmation de la performance :

a) Chacun des composants et éléments de capacité des voies de communication peut être arrêté de façon planifiée sans affecter l'environnement essentiel.

b) Il y a suffisamment de capacité installée de façon permanente pour répondre aux besoins du site lorsque des composants redondants sont retirés du service pour une raison quelconque.

2.3.3 Incidences opérationnelles :

a) Le site est susceptible de perturbations en raison d'activités non planifiées. Des erreurs d'opérations des composants d'infrastructure du site peuvent entraîner une perturbation à l'équipement informatique.

b) Toute panne ou défaillance imprévue d'un système de capacité affectera l'environnement essentiel.

c) Une panne ou une défaillance imprévue d'un composant de capacité ou d'un élément de communication pourrait affecter l'environnement essentiel.

d) L'entretien planifié de l'infrastructure du site peut être effectué en utilisant la capacité redondante des composants et des chemins de distribution redondants pour travailler en toute sécurité sur le reste du matériel.

e) Pendant les activités d'entretien, le risque d'interruption peut être élevé. (Cette condition d'entretien ne peut invalider le classement de Tier réalisé pendant les opérations normales.)

2.4 Tier IV: Infrastructure du site Fault Tolerant

2.4.1 Exigences fondamentales :

a) Un centre de données insensible aux défaillances comporte plusieurs systèmes indépendants, isolés les uns des autres, qui fournissent des composants de capacité redondants et de multiples voies de communication indépendantes, diversifiées et activées pour alimenter simultanément l'environnement essentiel. Les composants de capacité redondants et les voies de communication diversifiées doivent être configurés de telle sorte que la capacité « N » assure l'alimentation et le refroidissement de l'environnement essentiel en cas de panne de l'infrastructure.

b) Tout le matériel informatique est à double alimentation tel que défini par la norme de l'Institute Fault Tolerant Power Compliance Specification, Version 2.0 et bien installé pour être compatible avec la topologie de l'architecture du site. Des dispositifs de transfert, notamment des commutateurs individuels, doivent être intégrés à tout environnement essentiel qui n'est pas conforme à cette spécification.

c) Les systèmes complémentaires et des chemins de distribution doivent être physiquement isolés les uns des autres (cloisonnés), pour empêcher que toute cause unique puisse avoir un impact en même temps sur les deux systèmes ou les chemins de distribution.

d) Un refroidissement continu (Continuous Cooling) est nécessaire.

e) Douze heures de stockage de carburant sur place pour une capacité de « N ».

2.4.2 Tests de confirmation de la performance :

a) Une défaillance unique de tout système de capacité, composant de capacité, ou élément de distribution n'aura aucune incidence sur le matériel informatique.

b) Le système de commande de l'infrastructure réagit aux défaillances de façon autonome tout en assurant la viabilité de l'environnement essentiel.

c) Chacun des composants et éléments de capacité des voies de communication peut être arrêté de façon planifiée sans affecter les divers environnements essentiels.

d) Il y a suffisamment de capacité installée de façon permanente pour répondre aux besoins du site lorsque des composants ou chemins de distribution redondants sont retirés du service pour une raison quelconque.

2.4.3 Incidences opérationnelles :

a) Le site n'est pas sensible aux perturbations à partir d'un seul événement imprévu.

b) Le site n'est pas sensible aux perturbations de toute activité de travail prévue.

c) L'entretien planifié de l'infrastructure du site peut être effectué en utilisant la capacité redondante des composants et des chemins de distribution, pour travailler en toute sécurité sur le reste du matériel.

d) Lors d'activités de maintenance, au cours desquelles des composants de capacité redondants ou une voie de communication sont arrêtés, l'environnement essentiel est exposé à un risque accru d'interruption en cas de panne de la voie de communication active. Cette condition d'entretien ne peut invalider le classement par Tier réalisé pendant les opérations normales.

e) Le fonctionnement de l'alarme incendie, l'extinction des incendies, ou la fonctionnalité d'arrêt d'urgence (EPO) peut entraîner une perturbation du centre de données.

2.5 Systèmes moteur-générateur

Les moteur-générateur sont considérés comme la principale source d'alimentation pour le centre de données. Le service d'électricité local est une alternative économique. Les perturbations à l'alimentation locale ne sont pas considérées comme une défaillance, mais plutôt comme un état opérationnel prévu pour lequel le site doit être préparé. De même, les groupes électrogènes doivent démarrer automatiquement et assurer l'alimentation électrique en cas de panne d'électricité.

2.5.1 Site sur alimentation de moteur-générateur

Un système de moteur-générateur de Tier III ou IV, avec ses chemins d'alimentation et d'autres éléments d'appui, doit répondre aux tests Concurrently Maintainable ou de confirmation de performance Fault Tolerant alors qu'ils approvisionnent le site avec l'alimentation du moteur-générateur.

2.5.2 Limitations de durée d'exécution du manufacturier

Les générateurs à moteur pour les sites de Tier III et IV n'auront pas de limitation sur le nombre d'heures consécutives de fonctionnement lorsqu'ils sont chargés à « N » de la demande. Les générateurs à moteur qui ont une limite sur les heures consécutives de fonctionnement à « N » de la demande sont appropriés pour le Tier I ou II.

2.5.3 Limitation de durée d'exécution de la réglementation

Les systèmes de moteur-générateur ont souvent une limite annuelle réglementaire sur les heures d'exploitation à cause des émissions. Ces limites environnementales n'ont pas d'impact sur la contrainte les heures consécutives d'opération établie dans cette section.

2.6 Considérations pour la conception en fonction de la température ambiante

La capacité effective pour les équipements d'infrastructure des installations de centre de données doit être déterminée à l'état de la demande de pointe, basée sur la région climatologique et l'état d'équilibre d'exploitation des points de consigne pour le centre de données. Toutes les capacités du matériel données par les manufacturiers doivent être ajustées afin de refléter les températures extrêmes observées et l'altitude à laquelle le matériel fonctionnera pour soutenir le centre de données.

2.6.1 Conditions extrêmes annuelles pour la conception

La capacité de tous les équipements qui rejettent de la chaleur dans l'atmosphère sera déterminée à des Conditions extrêmes annuelles pour la conception qui représentent au mieux l'emplacement du centre de données dans l'édition la plus récente du ASHRAE Handbook - Fundamentals. (Chaque ASHRAE Handbook est révisé et publié tous les 4 ans.) La température humide (WB) de conception sera la valeur énumérée sous « Extreme Max WB » et la température sèche (DB) pour la conception sera la valeur pour « N = 20 ans ».

2.6.2 Points de consigne pour la salle d'ordinateurs

La capacité des équipements de refroidissement pour la salle informatique doit être déterminée à la température de l'air de retour, et l'humidité relative établie par le propriétaire, pour les opérations à l'état d'équilibre du centre de données.

2.7 Transmission des données

La transmission des données par connexions de transmission ou à fibre optique, entre les installations hors lieux et le point de démarcation de communication du centre de données, doit être conforme aux exigences des fonctions de maintenance simultanée établies pour le Tier III ainsi qu'aux exigences d'insensibilité aux défaillances et de compartimentation établies pour le Tier IV.

2.8 Réservoir de stockage d'eau

Un réservoir de stockage d'eau de réserve est exigé pour les sites de Tier III et de Tier IV dotés d'un système de refroidissement par évaporation. Par conséquent, le circuit d'eau de réserve doit être insensible aux défaillances et être doté d'une fonction de maintenance simultanée, conformément aux exigences, et doit être en mesure d'assurer l'alimentation pendant une période minimale de 12 heures.

2.9 Résumé des exigences par Tier

Un résumé des exigences précédentes définissant les quatre Tiers distincts de la classification par Tier se trouve au tableau 1.

Tableau 1: Résumé des exigences par Tier

	Tier I	Tier II	Tier III	Tier IV
Composants de capacité actifs pour supporter la charge TI	N	N+1	N+1	N Après toute défaillance
Chemins de distribution	1	1	1 actif et 1 alternatif	2 simultanément actifs
Concurrently Maintainable	Non	Non	Oui	Oui
Fault Tolerance	Non	Non	Non	Oui
Compartimentation	Non	Non	Non	Oui
Refroidissement continu	Non	Non	Non	Oui

3. Commentaire pour l'application de Tier Standard: Topology

Ce commentaire ne fait pas partie de la Data Center Site Infrastructure Tier Standard: Topology. Il fournit au lecteur le contexte pour l'application de la Standard.

3.1 Tier Standard axé sur les résultats

Les définitions utilisées dans la Tier Standard de l'Institute sont nécessairement et volontairement très larges, pour permettre l'innovation et les préférences des clients en matière de fournisseurs et d'équipements pour atteindre le Tier désiré de performance des infrastructures du site ou de disponibilité. Les Tiers individuels représentent des catégories de la topologie des infrastructures de sites qui traitent de concepts d'exploitation de plus en plus sophistiqués, conduisant à une disponibilité améliorée des infrastructures du site.

Les résultats de performance opérationnelle qui définissent les quatre Tiers de l'infrastructure du site sont très simples. Beaucoup de conceptions qui passent par une approche de liste de vérification vont échouer une approche par exigences de performances opérationnelles. Cela signifie que, en plus de l'application rigoureuse des principes d'ingénierie, il y a encore beaucoup de jugement et de flexibilité dans la conception de la disponibilité et la façon dont les sous-systèmes sont intégrés afin de permettre plusieurs modes de fonctionnement.

3.2 Impact des conditions ambiantes de conception

La capacité efficace soutenable de la plupart des équipements de refroidissement et de production d'énergie est affectée par les conditions réelles ambiantes dans lesquelles ils opèrent. Ces composants nécessitent généralement plus d'énergie pour fonctionner et fournissent une capacité utilisable moindre lorsque l'altitude et la température de l'air ambiant augmentent.

Une pratique courante pour les installations conventionnelles est de sélectionner des valeurs de calcul applicables à la plupart, mais pas à toutes les heures d'exploitation prévues pour cette installation. Cela se traduit par un choix économique de l'équipement qui répond aux exigences la plupart du temps. Ce n'est pas approprié pour les centres de données qui devraient fonctionner sur une base de 7/24 pour toujours.

Utilisant une température sèche (DB) de conception qui est dépassée 2 % du temps, pour la sélection d'un composant, ce dernier sera insuffisant pendant 175 heures par année. Bien que cela puisse sembler impliquer que le propriétaire gère un risque opérationnel d'un peu plus d'une semaine chaque année, ces heures se produisent effectivement progressivement, réparties sur plusieurs jours. La valeur de calcul de 2 % pourrait entraîner des conditions réelles qui dépassent les paramètres de conception de l'équipement pour plusieurs heures chaque après-midi pour une période de 1 à 2 mois. Une valeur de 0,4 %,

jugée conservatrice par plusieurs professionnels du design, résulte encore dans des équipements performants en deçà des besoins pour environ 35 heures chaque année.

Un autre exemple concernant les conditions ambiantes se pose lors de la sélection des systèmes de rejet de chaleur pour le système de refroidissement séparé à détente directe. Beaucoup de fabricants donnent des tableaux de sélection de produits basés sur des conditions extérieures ambiantes de 95 °F/35 °C. Ces composants ne produiront la capacité nominale indiquée que lorsqu'utilisés à une température de l'air extérieur inférieure à 95 °F/35 °C. Ces capacités des composants doivent être ajustées à la baisse pour fournir la capacité requise lorsque les températures dépassent 95 °F/35 °C.

3.3 Restrictions relatives aux limites du temps de fonctionnement des groupes électrogènes (Tier III et Tier IV)

Les restrictions relatives aux limites du temps de fonctionnement des groupes électrogènes sont conçues pour garantir que les groupes électrogènes sont en mesure d'alimenter le site sans interruption. La topologie de Tier exige que la capacité des groupes électrogènes conformes à l'une des trois principales normes ISO 8528-1 (continu, continu avec pointe, secours) soit considérée de manière différente, en fonction de la capacité nominale de chacun.

a) Les groupes électrogènes en continu peuvent fonctionner pendant une durée illimitée à leur tension nominale.

b) Les groupes électrogènes en continu avec pointes peuvent fonctionner pendant une durée limitée à leur tension nominale. Cette capacité ne satisfait pas aux exigences du chapitre 2.5. Comme indiqué dans la norme ISO 8528-1,, la capacité d'un groupe électrogène en continu avec pointes doit être ramenée à 70 % (donc réduite) pour une utilisation illimitée. Certains fabricants font état d'une capacité réduite différente (qui peut être supérieure ou inférieure à 70 %), à laquelle le groupe électrogène peut fonctionner pendant une durée illimitée, soit dans la fiche technique du produit soit dans un document distinct. La capacité certifiée par le fabricant pour un fonctionnement d'une durée illimitée servira à déterminer la conformité aux exigences du Tier.

c) Les groupes électrogènes de secours offrent, par définition, un nombre d'heures de fonctionnement annuelles limité. Cette capacité ne satisfait pas aux exigences du chapitre 2.5. Certains fabricants annoncent une capacité réduite différente, à laquelle le groupe électrogène peut fonctionner pendant une durée illimitée, soit dans la fiche technique du produit soit dans un document distinct. La capacité certifiée par le fabricant pour un fonctionnement d'une durée illimitée servira à déterminer la conformité aux exigences du Tier.

3.4 Progression des fonctionnalités par Tier

Les propriétaires qui choisissent des solutions de Tiers I ou II pour soutenir la technologie actuelle de la TI cherchent généralement une solution à des besoins à court terme. Les deux Tiers I et II sont généralement des solutions tactiques, à savoir, influencées par les coûts initiaux et les délais de commercialisation plus que par le coût du cycle de vie et les exigences de temps utilisable (ou de disponibilité). Des exigences rigoureuses de temps utilisable et la viabilité à long terme donnent généralement lieu à des solutions stratégiques que l'on retrouve plus souvent dans les infrastructures de site de Tier III ou de Tier IV. Les solutions d'infrastructure de site de Tier III ou IV ont une vie utile au-delà de l'exigence actuelle de la TI. Des solutions stratégiques d'infrastructure de site vont permettre au propriétaire de prendre des décisions stratégiques concernant la croissance et la technologie, sans contrainte occasionnée par la topologie actuelle de l'infrastructure du site.

3.4.1 Tier I

Les solutions de Tier I reconnaissent la volonté du propriétaire d'une infrastructure de site dédiée au soutien des systèmes de TI. L'infrastructure de Tier I permet d'offrir un environnement meilleur que celui d'un environnement de bureau ordinaire et comprend: un espace dédié pour les systèmes informatiques; un système d'alimentation sans coupure pour filtrer les pointes de puissance, les creux et les pannes momentanées; un équipement de refroidissement dédié qui ne s'arrête pas à la fin des heures normales de bureau; et un générateur à moteur pour protéger les fonctions de TI en cas de panne de courant prolongée.

3.4.2 Tier II

Les solutions de Tier II incluent une alimentation critique redondante et des composants de refroidissement redondants d'une capacité suffisante pour fournir une marge de sécurité accrue contre les perturbations de processus en raison de défaillances d'équipement d'infrastructure du site. Les composants redondants sont généralement des modules supplémentaires de systèmes d'alimentation sans coupure, des refroidisseurs, des équipements de rejet de chaleur, pompes, unités de refroidissement et générateurs à moteur. Un mauvais fonctionnement dans l'entretien normal entraînera la perte d'un composant de la capacité.

3.4.3 Tier III

L'infrastructure de site de Tier III ajoute le concept Concurrent Maintenance au-delà de ce qui est disponible dans les solutions de Tiers I et II. Concurrent Maintenance signifie que chacun des composants de capacité ou de distribution nécessaires pour soutenir l'environnement informatique de traitement peut être entretenu sur une base planifiée, sans impact sur l'environnement TI. L'effet sur la topologie de l'infrastructure du site est qu'un chemin de distribution redondant pour l'alimentation et le refroidissement est ajouté aux composants critiques redondants du Tier II. L'entretien permet à l'équipement et aux chemins de distribution d'être remis à neuf, sur une base fréquente et régulière.

Ainsi, le système fonctionnera de manière fiable et prévisible comme initialement prévu. En outre, la capacité de permettre l'entretien des infrastructures en même temps que le fonctionnement du site exige que chacun des systèmes ou composants qui prennent en charge l'exploitation informatique doit pouvoir être mis hors service pour un entretien programmé, sans impact sur l'environnement TI. Ce concept s'étend aux sous-systèmes importants, tels que les systèmes de contrôle pour les installations mécaniques, les systèmes de démarrage pour les générateurs à moteur, les contrôles d'arrêt d'urgence (EPO), les sources d'énergie pour les équipements de refroidissement et de pompes, les vannes d'isolement, et autres.

3.4.4 Tier IV

L'infrastructure de site du Tier IV s'appuie sur le Tier III, en ajoutant le concept de la Fault Tolerance à la topologie de l'infrastructure du site. Comparable à l'application des concepts Concurrent Maintenance, la Fault Tolerance s'étend à chacun des systèmes ou composants qui prennent en charge l'exploitation informatique. Le Tier IV considère que l'un de ces systèmes ou composants peut faire défaut ou subir un arrêt imprévu à tout moment. La définition du Tier IV de la Fault Tolerance est basée sur la défaillance d'un seul composant ou chemin de transmission.

Cependant, le site doit être conçu et exploité de manière à tolérer les effets cumulatifs de tous les composants d'infrastructure du site, de systèmes, et de chemins de distribution perturbés par la défaillance. Par exemple, la défaillance d'un seul tableau électrique aura une incidence sur tous les sous-panneaux et composants électriques qui reçoivent leur alimentation électrique en provenance de ce tableau. Une installation de Tier IV tolérera ces impacts cumulatifs sans affecter le fonctionnement de la salle informatique.

3.5 Classification fractionnelle ou incrémentale de Tier

La classification en quatre Tier Standard s'intéresse à la topologie, ou la configuration de l'infrastructure du site, plutôt qu'à une liste normative de composants, pour atteindre un résultat opérationnel souhaité. Par exemple, le même nombre de refroidisseurs et de modules d'alimentation sans coupure peut être organisé sur un seul chemin de distribution pour obtenir une solution de Tier II (composants redondants), ou sur deux chemins de distribution, ce qui peut aboutir à une solution de Tier III (Concurrently Maintainable).

Une application cohérente et transversale des concepts de la topologie par Tier pour les systèmes électriques, mécaniques, l'automatisation et autres sous-systèmes est nécessaire pour que tout site puisse satisfaire aux normes de Tier qui définissent un niveau de classification. Choisir la solution de topologie appropriée en fonction des exigences de disponibilité des TI pour soutenir les processus d'affaires bien définis, et les conséquences financières substantielles pour les temps d'arrêt, fournit la meilleure base pour des investissements dans les installations du centre de données. Lors de la conception du centre de données et pendant le processus de livraison, il est préférable que la concentration du propriétaire soit sur l'application cohérente de la Tier Performance Standard, plutôt que sur les détails qui composent l'infrastructure du site du centre de données.

Cependant, l'infrastructure du site a occasionnellement été décrite par d'autres dans l'industrie en termes de Tiers fractionnaires (par exemple, de Tier 2,5), ou Tiers incrémentiels (Tier III +, Tier III amélioré ou Tier IV léger). Des descriptions fractionnaires ou incrémentielles pour l'infrastructure de site ne sont pas appropriées et sont trompeuses. L'inclusion d'un critère ou d'un attribut d'un Tier de classification supérieur dans la conception n'augmente pas le classement général du Tier. Toutefois, l'écart d'un objectif du Tier dans un sous-système empêchera un site d'être Certifié à ce Tier.

a) Un site qui a un système d'alimentation sans coupure supplémentaire (redondant), mais qui a besoin de toutes les unités de refroidissement installées pour maintenir la température de la pièce d'ordinateur dans les limites, ne répond pas aux exigences de redondance pour le Tier II.

b) Un tableau électrique, qui ne peut être fermé sans affecter plus que le nombre redondant de pompes à eau réfrigérée secondaires (réduisant la capacité disponible à moins de N), ne répond pas à la norme Concurrently Maintainable et ne sera pas Certifié comme Tier III.

c) L'inclusion d'un système d'alimentation sans coupure calqué sur un système de Tier IV, dans un site ayant un squelette de distribution d'énergie de Tier II, donne une Certification de Tier II.

3.6 Tendances de non-conformité

Les écarts les plus importants de la Tier Standard dans la plupart des sites sont tout simplement des solutions incompatibles. Souvent, un site aura un système électrique robuste, Fault Tolerant, calqué sur une solution de Tier IV, mais utilisera un système mécanique de Tier II, qui ne peut être entretenu sans interrompre les opérations de la salle informatique. Cela se traduit par une note globale du site de Tier II.

Le plus souvent, le système mécanique ne rencontre pas les critères Concurrent Maintenance en raison du manque de coordination entre le nombre et l'emplacement des vannes d'isolement dans le chemin de distribution de l'eau réfrigérée. Un autre oubli fréquent est le branchement du circuit des composants mécaniques, qui entraîne la nécessité de fermer l'ensemble du système mécanique pour effectuer un entretien électrique. Si plus que le nombre redondant de refroidisseurs, de tours ou de pompes est hors tension pour un entretien électrique, le refroidissement de la salle d'ordinateurs est affecté.

Les systèmes électriques réussissent rarement à satisfaire les critères du Tier III ou du Tier IV, en raison des choix de conception effectués pour le système d'alimentation sans coupure et du chemin critique de la distribution de puissance. Il est presque impossible de faire la maintenance des groupes de systèmes d'alimentation sans coupure faisant appel à des commutateurs d'entrée et sortie communs sans causer de pannes de l'environnement essentiel, de sorte qu'ils ne sont pas conformes aux exigences de Tier III, en dépit d'investissements de plusieurs centaines de milliers de dollars. Les topologies qui incluent des commutateurs de transfert statique dans le chemin de puissance critique pour des dispositifs TI à simple alimentation échoueront probablement à la fois les critères de Fault Tolerance et les critères Concurrent Maintenance.

La mise en application rigoureuse des normes est nécessaire à l'obtention d'une solution intégrée pour un centre de données en particulier. Il est évident que le service TI investit énormément dans les fonctions offertes par les nouvelles technologies d'environnements essentiels. Souvent, comme les infrastructures électriques et mécaniques sont définies et les opérations de l'installation sont établies, il y a un degré croissant d'incohérence dans les solutions intégrées dans un site. Un placement dans un segment doit être complété par un investissement similaire dans chacun des autres segments si l'un des éléments de la solution combinée est d'avoir l'effet souhaité sur la disponibilité des TI. Un plan d'ensemble ou une stratégie bien exécuté(e) pour un centre de base de données doit résoudre tout l'ensemble des exigences de l'informatique et de l'installation.

Modifications à la Tier Standard : Topology.

Cette Standard tient compte des résultats du vote de 2010 du Owners Advisory Committee Les exigences de stockage de carburant du moteur-générateur sont en vigueur depuis le 1er mai 2010.

Les modifications apportées découlent de la discussion de 2012 et d'un vote du Comité consultatif des propriétaires. Toutes les mises à jour propres à cette version sont entrées en vigueur le 1er août 2012

À PROPOS DE L'UPTIME INSTITUTE

L'Uptime Institute est une organisation neutre et indépendante qui se consacre à la recherche sur les centres de données, à la formation et à la consultation, avec pour but d'améliorer le rendement et l'efficacité des centres de données par une approche collaborative et innovante. L'Uptime Institute propose ses services à tous les acteurs du secteur des centres de données, y compris aux entreprises et aux exploitants en tiers, aux fabricants, aux fournisseurs ainsi qu'aux ingénieurs et techniciens. Cette approche collaborative, associée à la capacité de l'Uptime Institute de déterminer les tendances au niveau mondial et de communiquer directement avec les propriétaires, donne naissance à des solutions et des innovations sans contraintes régionales, ce qui constitue un atout précieux pour le secteur mondial des centres de données.

Des questions?
info@uptimeinstitute.com
+1 206.706.4149

Uptime Institute™ LLC
20 West 37th Street, 6th Floor, New York, NY 10018
+1 206.706.4149 · Fax: +1 206.706.3083
http://uptimeinstitute.com · http://uptimeinstitute.com/professional-services

 TS102120-0812-FR(CA)

Guide de sécurité matérielle
Publication de l'organisme-conseil G13-01

Pièces d'entreposage sécuritaire (PES)

Le présent guide remplace toutes les versions antérieures du guide G1-029.

Ver 1.0 (Original)

Les suggestions ou commentaires relatifs au présent guide doivent être communiqués à :
Section de la sécurité matérielle, Sous-direction de la sécurité ministérielle de la GRC
1426, boul. St-Joseph, Ottawa (Ontario) K1A 0R2

Les questions peuvent aussi être envoyées par courriel à l'adresse Physec-secmat@rcmp-grc.gc.ca.

Cette publication est SANS CLASSIFICATION (à l'usage de l'organisation).
Au besoin, elle peut être fournie à des fournisseurs, conseillers et concepteurs.

Table des matières

Définitions

Autorité compétente – Habituellement l'inspecteur en bâtiment de la ville, de la municipalité ou du comté. Pour les bases des Forces canadiennes, l'autorité compétente est le directeur, Service des incendies des Forces canadiennes.

Cheville de sécurité (« *safety stud* ») – Protubérance sur la surface d'un élément de charnière mortaisée qui s'encastre dans une cavité située sur l'élément opposé lorsque la porte est fermée. (réf. : ANSI 156.1 (2006))

Coffre de sécurité – Lieu entièrement fermé ou pièce spécialement conçue servant de lieu de rangement (p. ex., pièce d'entreposage sécuritaire).

Compromission – Divulgation, destruction, suppression, modification ou utilisation non autorisées de biens ou de renseignements, ou accès ou interruption d'accès non autorisés à ceux-ci.

Côté exposé aux attaques – Côté de la porte ou du mur exposé à l'ennemi et susceptible de subir une attaque.

Détecteur de vibrations – Système à un ou plusieurs détecteurs permettant de détecter les vibrations causées par des outils de coupe électriques et à percussion. Les systèmes approuvés sont dotés d'un algorithme de sensibilité/détection pour éviter que les bruits ambiants, les bruits de fond ou les vibrations créées par des activités normales ne déclenchent de fausses alarmes.

Entreposage sur rayons ouverts – Entreposage autre que dans des coffres de sécurité ou coffres-forts approuvés. L'entreposage sur rayons ouverts comprend l'entreposage où les documents sont gardés dans des contenants ou des contenants commerciaux résistants au feu ou à l'eau.

Évaluation de la menace et des risques (EMR) – Considération des biens et des menaces portant contre ces biens, compte tenu de l'ensemble des mesures de sécurité en place ou anticipées.
La Gendarmerie royale du Canada (GRC) et le Centre de la sécurité des télécommunications Canada (CSTC) ont conjointement créé une procédure officielle, des listes de contrôle, des tableaux de valeurs et une formation connexe pour la tenue d'EMR au gouvernement du Canada appelée Méthodologie harmonisée d'évaluation des menaces et des risques (MHEMR), et en encouragent l'utilisation.

Goupille de haute sécurité (« *Maximum Security Pin* ») – Goupille de charnière qui a été fixée après son insertion par soudure, chevillage ou autre moyen permanent en vue d'éviter que la goupille de charnière puisse être retirée sans outils spéciaux. Les vis de pression ne sont pas autorisées. Offre une plus grande sécurité qu'une goupille de sécurité (« *Non-Removable Pin (NPR)* »). (réf. : ANSI 156.1 (2006)).

Goupille de sécurité (« *Non-Removable Pin (NPR)* ») – Goupille de charnière fixée à l'aide de vis ou d'autres moyens équivalents (réf. : ANSI 156.1 (2006)).

Menace de base (MB) – Menace à laquelle les ministères gouvernementaux sont couramment exposés au Canada dans des conditions de sécurité normale, comme le précise la *Norme opérationnelle sur la sécurité matérielle*.

Menace de référence (MR) – Menace qu'une mesure de protection précise (équipement, procédure ou politique) vise à limiter. Sauf indication contraire, les guides et concepts de protection de la GRC visent à atténuer une menace de référence en fonction d'une menace de base.

Paire de charnières - La pratique de l'industrie consiste à mentionner les charnières par paires. Par exemple, les portes à trois charnières sont désignées comme « 1 ½ paire ».

Pièce d'entreposage sécuritaire (PES) – Terme et abréviation officiels utilisés pour désigner une pièce conçue d'après le descriptif du guide G13-01 de la GRC.

Remarque : Le terme « pièce d'entreposage sécuritaire » ne remplace pas automatiquement le terme « pièce sécuritaire » (niveau 1 ou 2). Les pièces sécuritaires ne doivent être appelées pièces d'entreposage sécuritaire (PES) que si elles sont utilisées de façon conforme au présent guide.

Pièce sécuritaire (PS) – Terme désignant une pièce construite selon le descriptif du guide G1-029 de la GRC. Bien qu'il ne s'agisse pas d'une pratique approuvée par la GRC, ces pièces étaient souvent construites pour créer des zones de sécurité, des salles (ou suites) de travail sécuritaires ou pour l'entreposage sécuritaire (utilisation initialement prévue).

Porte d'accès de jour – Porte d'accès à une pièce sécuritaire ou à une chambre forte dotée d'un verrou principal qui, une fois déverrouillée le matin par la personne responsable, reste sécurisée par un deuxième verrou (habituellement un contrôle d'accès électronique) qui peut être ouvert (jusqu'à ce que le verrou principal soit à nouveau verrouillé) par les assistants autorisés.

Zones – Définies à la référence B.

Abréviations

AC – Autorité compétente
DE – Diamètre extérieur
DI – Diamètre intérieur
EB – Énoncé des besoins
EMR – Évaluation de la menace et des risques
GES – Guide d'équipement de sécurité
ksi – kilolivre par pouce carré (*kilopound per square inch* en anglais)
PES – Pièce d'entreposage sécuritaire
MVCF – Matériel vidéo en circuit fermé
Ø – Diamètre de barre
PS – Pièce sécuritaire (+ suffixe indiquant le « type » de pièce sécuritaire, d'après les versions antérieures du guide G1-029)
SDI – Système de détection d'intrusion

Références

A. *Politique sur la sécurité du gouvernement*
http://publiservice.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578&section=text#cha5

B. *Norme opérationnelle sur la sécurité matérielle*
http://publiservice.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text

C. *Guide d'équipement de sécurité G1-001* de la GRC
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm

D. Commissaire des incendies du Canada, RHDCC. *Norme pour entreposage des documents*
http://www.rhdcc.gc.ca/fra/travail/protection_incendies/politiques_normes/commissaire/index.shtml

E. Commissaire des incendies du Canada, RHDCC. *Interprétation technique - Porte et dispositifs d'ouverture des portes par une seule manœuvre simple*
http://www.rhdcc.gc.ca/fra/travail/protection_incendies/politiques_normes/interpretations/2008_006.shtml

F. *Guide : Exigence de verrouillage (Protégé A et B)* (publié à la rubrique « Entreposage » du Guide d'équipement de sécurité de la GRC
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0072_f.htm

Normes commerciales citées comme référence

Ces normes sont vendues par leurs associations de normalisation respectives, ou par des vendeurs de normes comme IHS Standards (http://global.ihs.com), ANSI Store (http://webstore.ansi.org) ou Techstreet (http://www.techstreet.com).

ANSI/ BHMA A156.4 : *Door Controls-Closers*
American National Standards Institute (http://www.ansi.org/)

ANSI/BHMA A156.1 : *Butts and Hinges*
American National Standards Institute/ Builders Hardware Manufacturers Association

ASTM A627-03 : *Standard Test Methods for Tool-Resisting Steel Bars, Flats, and Shapes for Detention and Correctional facilities* (http://www.astm.org)

ASTM F1267-07 : *Standard Specification for Metal Expanded Steel*
American Society for Testing and Materials

CAN/ONGC-1.60 : *Peinture-émail brillante d'intérieur aux résines alkydes / Interior Alkyd Gloss Enamel Paint*
Office des normes générales du Canada (http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html)

CSDMA 08 11 13 : *Recommended Specification for Commercial Steel Door and Frame Products*
Canadian Steel Door Manufacturer's Association (http://www.csdma.org)

EMMA 557-99 : *Standard for Expanded Metal, Introduction, Product Selection Considerations, Terminology, Manufacturing Process, Manufacturing Tolerances and Applications.*
Expanded Metal Manufacturers Association (http://www.naamm.org/emma)

HMMA 840-07 : *Guide Specification for Installation and Storage of Hollow Metal Door and Frame*

HHMA 810-09 (NAAMM Standard) : *Hollow Metal Doors*
Hollow Metal Manufacturers Association (http://www.naamm.org/hmma/)

SSMA : *Product Specifications*
Steel Stud Manufacturers Association (http://www.ssma.com/technical_library.aspx)

PARTIE I (À l'usage du ministère ou de l'organisme)

Les progrès technologiques concernant les outils portatifs ont changé la nature des *accès forcés menés ouvertement* et les *accès forcés plus élaborés*. En outre, les mémoires grande capacité peuvent désormais stocker de grands nombres d'informations, et la menace visant les renseignements personnels a beaucoup augmenté en raison du vol d'identité.
À la lumière de cette évolution des technologies et des menaces, il est recommandé de mener une Évaluation de la menace et des risques (EMR) de toutes les pièces sécuritaires existantes (ou espaces similaires construits d'après le descriptif de la version G1-029), en vue de déterminer si des modifications sont requises.

Importantes modifications de la version G13-01 :

- Le guide porte particulièrement sur les pièces d'entreposage sécuritaire (PES), un type spécial de coffres de sécurité approuvés (essentiellement une solution de rechange à l'utilisation de nombreux coffres de sécurité approuvés), et leur utilisation conforme à ce concept. La terminologie a changé : on parle désormais de pièce d'entreposage sécuritaire (PES) plutôt que de pièce sécuritaire (PS) pour souligner l'intention du concept.

- Par le passé, les niveaux (1 ou 2) des pièces sécuritaires étaient principalement déterminés par le choix du métal utilisé dans les murs. Le guide permet désormais de choisir l'un ou l'autre en fonction du coût, de la disponibilité du matériel et des préférences quant à la construction.

- Les fenêtres et les faux-plafonds ne font pas partie du concept des pièces d'entreposage sécuritaire, et sont fortement découragés. Lorsqu'ils doivent être utilisés, des mesures compensatoires devront être prises. La GRC peut fournir une orientation selon le cas.

- Le guide met désormais l'accent sur la détection rapide des accès forcés.

- Ce guide vise à optimiser l'utilisation des matériaux et composants offerts sur le marché. Dans la mesure du possible, les normes commerciales largement acceptées sont précisées.

Fonctionnement du guide

Ce guide (en particulier la partie I) est destiné aux intervenants en sécurité qualifiés et au personnel de la sécurité ministérielle qui doivent sélectionner les caractéristiques adéquates pour les pièces d'entreposage sécuritaire et les composants des systèmes de détection d'intrusion (SDI), ainsi qu'élaborer un énoncé des besoins (EB) pour guider le concepteur responsable de sa conception et de sa construction.

Processus
Une fois l'EB établi, il faut engager des architectes, ingénieurs ou constructeurs/concepteurs qualifiés détenant l'habilitation requise pour élaborer des dessins et des devis détaillés. Ceux-ci devraient comprendre les caractéristiques et composants précisés dans l'EB, et le concept doit être conforme aux exigences globales du projet (s'il s'inscrit dans un plus vaste projet) et à tous

les codes et normes d'aménagement des locaux applicables. Idéalement, la conception et l'installation des SDI devraient être effectuées par le personnel de la sécurité ministérielle. Les ministères qui n'ont pas de sections responsables des systèmes d'alarme et de détection d'intrusion devraient engager un conseiller indépendant (sans lien avec les fournisseurs ou installateurs) pour faciliter l'élaboration de l'architecture des SDI et la gestion des processus d'acquisition et de passation de marchés. Ils peuvent aussi contribuer à l'élaboration de critères de mise en service.

La raison du choix d'un composant ou d'une caractéristique (ainsi que la nature du bien et de la menace de référence) ne devrait être divulguée qu'à l'architecte, au concepteur ou à l'entrepreneur qui a besoin de le savoir et qui possède l'habilitation de sécurité nécessaire. Il faut envisager de classifier cette raison ainsi que les principales caractéristiques de sécurité.

Remarque : Le fait qu'une PES pourrait contenir des renseignements classifiés ne veut pas forcément dire que les détails de la construction de la PES devraient avoir la même classification. Mais cela veut dire que les détails de la construction (ainsi que le but et le nom de la PES) devraient être adéquatement protégés.

Il suffit souvent de trier les détails à communiquer, et de les communiquer uniquement en fonction du besoin de connaître.
L'architecte ou le concepteur devrait recevoir une orientation officielle quant à la préparation des dessins pour les soumissions ou la sous-traitance, de façon à ce que les informations névralgiques ne soient pas divulguées inadéquatement. Par exemple, le but ou le nom de la pièce ne doit pas figurer sur les dessins, les devis ou les autres documents de contrat diffusés à grande échelle. Un nom générique ou un chiffre doit être utilisé. Les sous-traitants ne doivent recevoir que l'information nécessaire à l'accomplissement de leur travail (p. ex., dessins de bâtiment et schémas de système partiels qui n'identifient pas les activités adjacentes et ne fournissent pas de détails propres à la sécurité des systèmes). Lorsque c'est faisable, les exigences en matière de sécurité doivent être incluses aux documents de contrat, pour veiller à ce qu'elles soient respectées.

But de la pièce d'entreposage sécuritaire

Une pièce d'entreposage sécuritaire vise à servir de lieu d'entreposage approuvé pour l'*entreposage sur rayons ouverts* de grandes quantités d'informations ou de biens classifiés ou très délicats, mais autres que d'intérêt national (protégés). Une pièce d'entreposage sécuritaire est essentiellement un « coffre de sécurité », et est sujette aux mêmes exigences quant au zonage.

À moins qu'elle ne respecte toutes les spécifications techniques et d'utilisation précisées dans ce guide, la pièce n'est pas considérée comme une « pièce d'entreposage sécuritaire (PES) » approuvée et ne doit pas être désignée comme telle.

Protection contre les incendies

Les exigences relatives à la protection contre les incendies (lois) ont TOUJOURS préséance sur les exigences relatives à la sécurité (politique), alors il est important d'avoir une planification adéquate et de consulter l'autorité compétente locale tôt, pour éviter des problèmes qui pourraient entraîner la suppression ou la modification d'éléments de sécurité.

Les gicleurs ne font pas partie intégrante d'une pièce d’entreposage sécuritaire, et ne devraient pas être installés à l'intérieur d'une PES, à moins que l'AC ne l'exige. Si d'autres mesures de protection contre les incendies sont requises, les documents peuvent être entreposés dans des contenants commerciaux résistants au feu placés dans la PES. Des systèmes d'extinction d'incendie par gaz inerte peuvent aussi être utilisés.

Des cloisons sèches supplémentaires ou de type X peuvent être installées pour respecter le code (ou lorsque l'AC le demande). Au besoin, une porte coupe-feu adéquatement identifiée peut être utilisée au lieu de la porte spécifiée. Il convient de noter que des exigences particulières doivent être respectées pour l'installation des serrures et de la quincaillerie sur les portes résistantes au feu. Communiquer avec l'AC locale pour obtenir de l'aide et des conseils concernant les questions liées à la sécurité et aux incendies.

Du plancher au plafond

Les murs de pièce d’entreposage sécuritaire doivent aller du plancher au plafond (du plancher fini à la face inférieure du toit de béton de structure ou du plancher), ou traverser le plafond pour former une enceinte de sécurité continue (plafond protégé). Lorsque l'espace au-dessus du plafond protégé (mesuré jusqu'à la face inférieure de l'élément de structure limite) dépasse six pouces, l'espace doit être fermé et verrouillé ou surveillé électroniquement. Dans des cas rares, le plancher pourrait aussi exiger un traitement spécial. Consulter la GRC pour obtenir des conseils à cet égard.

Menace de référence et fondement du concept de pièce d’entreposage sécuritaire

Les pièces d’entreposage sécuritaire servent principalement à protéger des attaques subreptices, mais aussi à repérer et à retarder les accès forcés. Les PES sont conçues pour être construites dans une zone de sécurité ou une zone de haute sécurité dans un immeuble du gouvernement (ou un lieu équivalent approuvé par la Direction de la sécurité industrielle canadienne (DISC) dans les locaux d'un fournisseur) dans des centres urbains. Les PES construites dans des endroits éloignés pourraient exiger des mesures de protection supplémentaires.

Une évaluation de la vulnérabilité doit être menée en vue de déterminer si un ennemi potentiel pourrait accéder au périmètre (ou à tout espace au-dessus ou au-dessous de celui-ci) de la PES sans être détecté ou observé pendant de longues périodes. Dans ce cas, des mesures supplémentaires sont requises pour limiter l'accès ou surveiller *activement* les activités dans les zones du périmètre.

Les planchers et les plafonds sont censés être constitués de matériaux très résistants aux intrusions, comme du béton de structure, des blocs de béton armé ou de l'acier recouvert de béton

(toits et planchers). Les assemblages de bois ou d'acier doivent être renforcés d'acier et surveillés par un détecteur de vibrations, tout comme les murs.

Vestibules

Le concept original des pièces sécuritaires comprenait un vestibule pour deux raisons : pour restreindre le mouvement de va-et-vient des outils à main et pour fournir une meilleure isolation sonore vers la porte. En ce qui concerne le premier objectif, la menace d'accès forcé par la porte et la quincaillerie de la PES la plus viable provient désormais d'outils électriques portatifs, et un vestibule ne permet pas vraiment de réduire cette menace. En fait, un vestibule devient désormais un espace où un ennemi pourrait se cacher pour attaquer la porte (ou le mur avoisinant). Le vestibule n'est pas non plus nécessaire pour améliorer l'isolation sonore vers la porte lorsque la PES est utilisée dans son but premier, c'est-à-dire comme une pièce d'entreposage de documents.

En conséquence, les vestibules extérieurs ne sont pas requis (bien qu'ils soient toujours autorisés) pour la construction d'une PES. Si un vestibule est construit, il doit l'être de façon à faciliter l'observation des activités à l'intérieur (p. ex. murs ou porte vitrés).

La fonction d'une « porte d'accès de jour » est facilitée par l'utilisation de verrous figurant dans le Guide d'équipement de sécurité (GES) qui offrent cette fonction, lorsque la politique ministérielle accepte cette pratique. Pour être approuvées pour cette fonction, les commandes d'accès électroniques ne doivent fonctionner que lorsque le verrou mécanique est « ouvert » (le verrouillage du verrou mécanique doit mécaniquement désactiver les fonctions électroniques, pour éviter qu'une attaque ne puisse compromettre les commandes d'accès).

Des modes de fonctionnement bien définis et respectés sont nécessaires lorsque des « portes d'accès de jour » sont utilisées. Les utilisateurs ne doivent pas être autorisés à utiliser le mécanisme de serrure électronique au lieu du verrou mécanique pendant de longues périodes (particulièrement la nuit ou les fins de semaine).

Système de détection d'intrusion (SDI)

Bien que les tôles d'acier sur les murs offrent une certaine résistance à la force, elles visent principalement à transmettre les vibrations causées par des accès forcés aux détecteurs de vibrations. La GRC a testé et approuvé un détecteur de vibration pour les murs des PES, qui figure dans le GES. Des systèmes de détection (p. ex., détecteurs de mouvement) situés à l'intérieur de la pièce d’entreposage sécuritaire peuvent aussi être utilisés, bien qu'ils ne détectent l'ennemi qu'une fois celui-ci entré, ce qui réduit le temps d'intervention.

Le tableau de sélection suggère le type de système de détection à utiliser dans diverses situations. Dans tous les cas, les systèmes d'alarme doivent déclencher une intervention fiable, opportune et adéquate.

Construction d'ouvertures pour le passage de la tuyauterie ou de câbles électriques

Dans la mesure du possible, réduire le nombre d'ouvertures destinées au passage de la tuyauterie ou de câbles électriques dans les murs des PES. Ne pas placer ces ouvertures dans la zone

d'attaque critique. Lorsque ces ouvertures sont requises, former un cadre à moins d'un pouce (25 mm) du tuyau ou conduit, et le fixer aux poteaux d'ossature à au moins deux endroits. Étendre le matériau de protection du mur jusqu'à ¾” (20 mm) du bord de l'ouverture. Étendre la plaque de parement jusqu'au tuyau ou conduit. Boucher tous les trous avec du produit d'étanchéité acoustique ou résistant au feu. Norme des produits recommandés : ASTM E 814 (UL 1479) ou CAN/ULC S115, ou tel que demandé par l'autorité compétente.

Lorsqu'il est nécessaire de tenir compte du mouvement ou de l'expansion des tuyaux ou conduits, les tuyaux ou conduits peuvent être recouverts d'un manchon métallique ajusté, et le manchon fixé mécaniquement aux poteaux d'ossature à au moins deux endroits. L'espace entre le manchon et le tuyau ou conduit doit être restreint le plus possible, et ne pas dépasser ¼”.

Des barres d'acier doivent être installées pour retarder l'accès d'une personne par un conduit dont la section transversale est supérieure à 96 po^2 et dont la dimension la plus petite est supérieure à 6”. Elles peuvent être omises si une EMR détermine qu'un accès non autorisé par ces conduits ne constitue pas une menace.
Il convient de noter que ces barres n'empêchent pas l'introduction de produits délétères (p. ex., eau, vapeurs toxiques). Si une EMR détermine que ce genre de menaces est possible, tous les conduits et ouvertures pourraient devoir faire l'objet de mesures compensatoires supplémentaires (p. ex., filtres ou clapets). Communiquer avec la GRC pour obtenir des conseils à cet égard.

Dispositifs de verrouillage de porte

Un dispositif de verrouillage de porte respectant le code (un seul mouvement, une seule action) qui accepte les serrures à combinaison approuvées a été approuvé et figure dans le GES.

Intégrité assurée par deux personnes

Certaines serrures à combinaisons électroniques mentionnées dans le GES permettent l'application d'une politique d'intégrité assurée par deux personnes (les deux personnes doivent entrer la combinaison pour ouvrir le verrou). C'est l'une des mesures de sécurité les plus efficaces qui puisse être appliquée à l'entreposage de renseignements délicats.

Vis

Les vis (y compris les « vis de sûreté » ne sont pas approuvées pour l'attache du matériau de protection des murs (tôle ou treillis) à l'ossature métallique.

Les vis peuvent être utilisées pour fixer les traverses (anti-écartement) et contreventements (stabilité) à l'ossature métallique. Elles peuvent aussi être utilisées (avec des rondelles) pour fixer les tôles d'acier aux solives de bois ou aux poteaux de bois.

Les vis à cloison sèche sont approuvées pour l'attache des plaques de parement aux poteaux de métal ou de bois.

Énoncé des besoins

Lorsque le ministère (client) n'est pas aussi le concepteur, il faut élaborer un énoncé des besoins (EB), pour préciser au concepteur exactement ce qui est nécessaire et pour déterminer les options de construction sélectionnées parmi celles présentées dans les Spécifications générales à la partie II.

L'EB et tous les documents contribuant à la sélection des éléments particuliers des PES doivent être considérés comme de nature délicate, et traités en conséquence.

Ne pas dire au concepteur pourquoi un choix a été fait à moins qu'il n'ait besoin de le savoir.

Conseils et orientation

Gendarmerie royale du Canada
Sous-direction de la sécurité ministérielle
Section de la sécurité matérielle
1426, boul. St-Joseph
Ottawa (Ontario) K1A 0R2
Sec-Equip@rcmp-grc.gc.ca

Tableau 1 - Recommandations en matière de sécurité

Sensibilité	Mesures de sécurité
Protégé A **Protégé B**	**PES non requise.** « Verrouiller » l'information (cf. référence F). Une pièce d'entreposage construite conformément au présent guide excède de beaucoup les exigences de verrouillage minimales en matière de sécurité matérielle. Voici les solutions recommandées pour l'entreposage de renseignements de niveaux Protégé A ou B, plutôt que les PES : - Contreplaqué de ½" au lieu de tôles d'acier ou de treillis d'acier - Contact de porte UL 634 et SDI (si recommandé par l'AC) - Serrure à mortaise ANSI 156.13 de classe 1 avec cylindre (à clé) de haute sécurité UL 437
Protégé C	**Ne constituant pas un danger de mort** **- Placer la PES dans une zone de sécurité.** - Détection de vibrations sur les murs (et plafond protégé au besoin) - SDI à l'intérieur de la PES - Envisager une parcellisation supplémentaire[1] - Serrures à combinaisons figurant dans le GES approuvées pour le niveau Très secret / Protégé C, ou Serrures figurant dans le GES approuvées pour le niveau Secret (si approuvé par la SDSM) **Constituant un danger de mort** - **Placer la PES dans une zone de haute sécurité** (extérieur construit selon les recommandations de l'EMR) - Détection de vibrations sur les murs (et plafond ou plancher protégé au besoin) - Détecteur de mouvements (ou autre SDI) à l'intérieur de la PES - Parcellisation supplémentaire[1,2] -Authentification à deux personnes[3] -EMR officielle pour s'assurer que les mesures sont adéquates - Serrures à combinaisons figurant dans le GES approuvées pour le niveau Très secret / Protégé C
Confidentiel	**Placer la PES dans une zone de sécurité** - Détecteur de mouvements (ou autre SDI) à l'intérieur de la PES - Serrures à mortaise à clé. ANSI/BHMA 156.13 de classe 1 ou sélectionner parmi celles figurant dans le GES - Cylindre à haute sécurité : UL 437, ANSI 156.30 de niveau A ou ANSI 156.5 de classe 1A[4] - Les serrures électroniques commerciales à clavier numérique sont permises, mais les claviers numériques « brouillés » sont privilégiés. Préciser ANSI/BHMA A156.30 de niveau B (minimum) ou UL 1034
Secret	**Placer la PES dans une zone de sécurité ou une zone de haute sécurité** - Détection de vibrations sur les murs (et plafond ou plancher protégé au besoin) - Détecteur de mouvements (ou autre SDI) à l'intérieur de la PES - Serrure à combinaison figurant dans le GES

Très secret	**Placer la PES dans une zone de haute sécurité** - Détection de vibrations sur les murs (et plafond protégé au besoin) - Détecteur de mouvements (ou autre SDI) à l'intérieur de la PES - Envisager une parcellisation supplémentaire pour le besoin de connaître[2] - Envisager l'authentification à deux personnes[3] - Serrures à combinaisons figurant dans le GES approuvées pour le niveau Très secret - EMR officielle pour s'assurer que toutes les mesures d'entreposage, d'alarme et d'intervention sont adéquates

Notes relatives au tableau

1. Les coffres anti-effraction UL 687 offrent une résistance supplémentaire considérable (ainsi qu'une parcellisation pour la ségrégation nécessaire au besoin de connaître). Bien que la pièce d'entreposage sécuritaire permette la détection précoce et retarde l'intrusion, le temps de résistance du coffre doit correspondre étroitement au délai d'intervention assuré pour une intervention adéquate.

2. Une parcellisation supplémentaire est recommandée lorsque le principe d'accès sélectif est toujours une préoccupation (cf. référence B, alinéa 7.6.7). L'information peut être parcellisée à l'aide de coffres ou d'armoires verrouillables commerciaux. On recommande d'utiliser les serrures à clé de haute sécurité UL 437.

3. Il faut aussi envisager des mesures compensatoires quant aux procédures ou à la technologie.

4. Envisager d'utiliser des cylindres de haute sécurité avec « technologie à puce » (p. ex. CLIQ^{MD}) à des fins de vérification (seulement).

Notes générales

A) Lorsqu'une EMR permet de déterminer qu'une certaine menace est bien atténuée par d'autres aspects de sécurité, l'agent de la sécurité ministérielle peut décider qu'une ou plusieurs des mesures recommandées ne sont pas nécessaires.

B) Le Centre de la sécurité des télécommunications Canada (CSTC) exige que certains équipements soient placés dans une pièce sécuritaire (antérieurement PS-2). D'autres mesures de sécurité, comme la protection contre les émanations, pourraient être requises, mais la GRC ne peut donner des conseils que sur la construction de pièces d'entreposage sécuritaire conçues pour l'entreposage de documents. Communiquer avec les Services à la clientèle du CSTC : comsecclientservices@cse-cst.gc.ca

Foire aux questions

Q1 : Pourquoi des documents cotés Protégé C dans une pièce d'entreposage sécuritaire doivent-ils aussi être entreposés dans un coffre?

R1 : La nature de la menace envers les renseignements classifiés est considérablement différente de celle envers les renseignements cotés Protégé C (surtout ceux constituant un danger de mort). Les pièces d'entreposage sécuritaire sont une solution de rechange aux coffres de sécurité approuvés, et doivent offrir la même protection. Les renseignements cotés Protégé C (surtout ceux constituant un danger de mort) sont considérés comme susceptibles aux accès forcés par un ennemi motivé, et exigent donc une résistance considérable à la force. La meilleure garantie consiste à utiliser des coffres anti-effraction UL 687 pouvant résister au moins une heure, à des fins de parcellisation supplémentaire. Les coffres fournissent en outre une parcellisation supplémentaire pour le besoin de connaître.

Q2 : Les besoins d'une pièce d'entreposage sécuritaire sont-ils comparables à ceux d'une salle de serveurs protégée, décrits dans le guide G1-031?

R2 : Les fonctions des deux pièces sont différentes. Les pièces d'entreposage sécuritaire sont conçues pour l'entreposage de documents. Elles ne sont pas destinées au traitement de l'information (ni à être occupés). Les serveurs sont vulnérables à des menaces plus variées que les documents entreposés, et les salles de serveurs comprennent de vastes systèmes de climatisation, de ventilation et de conduits (y compris à travers les murs).

Q3 : La *Norme opérationnelle sur la sécurité matérielle* précise que les renseignements cotés Confidentiel peuvent être entreposés dans une zone de travail. Pourquoi le tableau 1 recommande-t-il qu'une pièce d'entreposage sécuritaire pour les renseignements cotés Confidentiel soit placée dans une zone de sécurité?

R3 : La pièce d'entreposage sécuritaire doit être placée dans une zone de sécurité à cause des risques élevés associés à l'entreposage de grandes quantités d'informations sur des rayons ouverts. L'exigence de « surveillance périodique » d'une zone de travail ne garantit pas qu'un ennemi ne bénéficiera pas de longues périodes d'activités non surveillées. Le problème est qu'en l'absence d'une surveillance efficace 24 h sur 24, un ennemi pourrait parvenir à entrer et à exercer ses activités pendant une longue période. Des espaces de plafond non protégés ou des issues ou des ascenseurs sans alarme ou surveillance pourraient être utilisés comme voies d'accès. Si une EMR révèle que la zone de travail est suffisamment sécuritaire pour qu'un accès non autorisé soit hautement improbable, l'ASM pourrait permettre qu'une pièce d'entreposage sécuritaire y soit située.

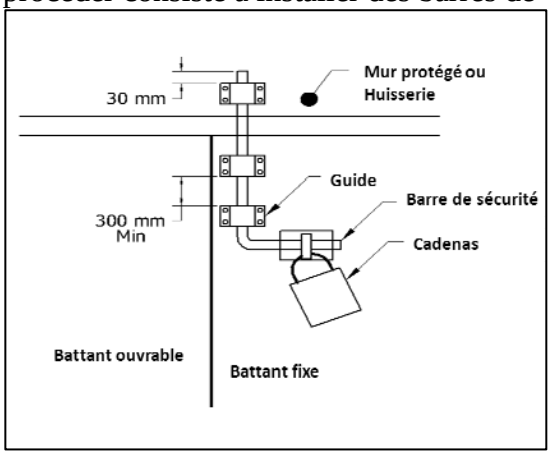
Q4 : L'espace consacré à une pièce d'entreposage sécuritaire est adjacent à un lieu public ou à un occupant n'appartenant pas au ministère. Que faire?

R4 : Une pièce d'entreposage sécuritaire ne doit jamais être située contre des murs extérieurs si ceux-ci ne sont pas faits de béton armé ou de blocs de béton armé (tous les espaces vides sont remplis). Les pièces d'entreposage sécuritaire peuvent normalement être adjacentes à des murs souterrains (sous-sol) et à des murs situés au moins à trois étages au-dessus d'une surface accessible (sol ou toit) sans mesures de protection supplémentaires.

Si l'emplacement ne peut pas être facilement changé et que le mur est en béton armé, en blocs de béton armé ou dans un matériau similaire, construire un mur pour la pièce d'entreposage sécuritaire contre le mur existant. Pour faciliter l'érection du mur, placer le treillis d'acier à l'intérieur et ne pas le recouvrir ni le bloquer complètement par des rayons. Le treillis d'acier permet aux utilisateurs de vérifier rapidement que le mur derrière le treillis est intact. Dans la mesure du possible, fournir un système de surveillance ou de détection précoce pour l'extérieur. Envisager d'utiliser des clôtures ou d'autres barrières. Lorsque la détection précoce n'est pas faisable, vérifier que le délai d'intervention en cas d'alarme du système de détection d'intrusion est adéquat.

Q5 : Nous avons déjà une porte à deux battants en acier et aimerions la garder pour notre pièce d'entreposage sécuritaire, car elle facilite l'utilisation d'un chariot élévateur à fourches. Pouvons-nous l'utiliser?

R5 : Si la porte et l'huisserie respectent les exigences en matière de construction du présent guide, vous pourriez immobiliser l'une des portes, de façon à obtenir une sécurité satisfaisante lorsque la porte est fermée et verrouillée. Une façon de procéder consiste à installer des barres de sécurité très robustes en haut et en bas de la porte, qui peuvent être verrouillées à l'aide d'un cadenas (pour éviter que des utilisateurs les ouvrent et les laissent ouvertes). Ces barres doivent avoir un diamètre d'au moins 30 mm, et être connectées à la porte à l'aide de deux guides soudés ou rivetés à la porte, et espacés d'au moins 300 mm. Les barres doivent dépasser d'au moins 30 mm une poche ou un guide soudé ou riveté à l'huisserie ou à un mur protégé. La conception des barres doit empêcher le déverrouillage lorsque le cadenas est en place. Cette approche exige de respecter rigoureusement les politiques et procédures, et doit être utilisée avec discrétion. Nommer un gardien des clés des cadenas, qui sera responsable de vérifier que la deuxième porte est immobilisée.



Q6 : Y a-t-il des restrictions quant aux prises de courant ou aux interrupteurs muraux sur les murs de la pièce d'entreposage sécuritaire?

R6 : Les murs de la pièce d'entreposage sécuritaire ont été testés sans trous ni pénétrations. Dans la mesure du possible, utiliser des luminaires montés en applique. Lorsqu'un luminaire doit être monté dans le mur, il doit être situé le plus loin possible de la porte. La boîte d'éclairage doit être en acier et soudée ou rivetée au revêtement du mur d'acier. Les câbles et les fils doivent être revêtus d'un conduit de métal ou d'un tube électrique métallique.

Les pénétrations part en part sont à éviter. Lorsque des pénétrations doivent être faites des deux côtés du mur, elles doivent être séparées d'au moins 300 mm.

Q7 : Le guide G13-01 utilise un langage impératif, et des termes comme « requis », mais ne s'agit-il pas d'un « guide »?

R7 : En tant qu'organisme-conseil, la GRC a le pouvoir de concevoir, de tester, d'évaluer et d'approuver le matériel de sécurité. Chaque ministère ou organisme a le pouvoir de décider s'il utilisera le matériel ou les concepts approuvés par la GRC, soit tels quels, soit modifiés de façon quelconque. Pour être approuvée, une pièce d'entreposage sécuritaire doit être construite selon les normes de conception de la GRC. Si toutes les normes de la GRC ne sont pas respectées, ce n'est pas une pièce d'entreposage sécuritaire approuvée par la GRC, et elle ne devrait pas être appelée pièce d'entreposage sécuritaire (PES).

Q8 : Et si l'AC exige que la PES ait deux moyens d'évacuation?

R8 : Cette question ne devrait pas se poser si la pièce conserve son but premier, soit une pièce d'entreposage de documents (relativement) petit, puisque la deuxième sortie est déterminée par l'occupation et l'aire de plancher. Mais dans cette situation, la deuxième porte de sortie ne devrait pas avoir de quincaillerie de verrouillage à l'extérieur.

Q9 : Puis-je construire une PES dans un bâtiment de bois?

R9 : La PES a été conçue pour se trouver dans une zone de sécurité ou une zone de haute sécurité, dans un immeuble du gouvernement caractéristique, en milieu urbain. Dans toute autre situation, mener une EMR en tenant compte des menaces, des biens et de la somme de toutes les mesures de protection (p. ex., emplacement sur une base militaire, patrouilles régulières et intervention rapide, etc.). Bien que ce guide ne le mentionne pas explicitement, les mesures de sécurité opérationnelles suffisantes et assurées peuvent combler des lacunes mineures quant au niveau de protection matérielle offert par un plancher et un plafond de bois. Le matériel de protection en métal et les détecteurs de vibrations doivent être installés sur le plancher et le plafond d'une PES construit dans un bâtiment en bois. Communiquer avec la GRC pour de plus amples renseignements.

Q10 : Nous allons mettre une équipe de répression dans une baie d'entrepôt avec un étage principal et une mezzanine qui s'ouvre sur l'étage principal. Il y aura toutefois des bureaux fermés à cet étage. On prévoit deux pièces d’entreposage sécuritaire/salles des pièces à conviction à l'étage principal, sous la mezzanine. Le plancher n'est pas une dalle de béton. Que devons-nous faire?

R10 : Lorsque le plafond (plancher de la mezzanine) est en bois (solive en bois ou composite avec faux-plancher en contreplaqué), nous recommandons que le plafond ait un treillis en métal déployé (3/4" - 9F, comme l'exige la construction du mur) fixé à la face inférieure (côté sécurisé) des solives de toit, et qu'un détecteur de vibrations soit installé en contact avec le treillis du côté sécurisé. Le socle du détecteur peut être installé à côté de la solive de toit (solution privilégiée). Les câbles du détecteur du toit doivent longer le côté sécurisé du plafond de la PES (dans un conduit en applique) pour rejoindre les câbles de l'autre détecteur dans le conduit commun et le tableau de commande d'alarme.

Q11 : Puis-je installer la serrure de porte à une hauteur différente pour répondre aux besoins en matière d'accès?

R11 : Habituellement, l'installation de la serrure de porte à 44 pouces au-dessus du plancher répond aux besoins en matière d'accès de tous les utilisateurs. Si la serrure est installée à moins de 42 pouces au-dessus du plancher, la traverse (entre l’huisserie et le poteau adjacent, à 48 pouces au-dessus du plancher) devrait être abaissée pour se situer à moins de 6 pouces de l'axe longitudinal de la serrure, ou des traverses supplémentaires devraient être installées à 6 pouces ou moins de l'axe longitudinal de la serrure.

Q12 : Puis-je changer la hauteur de la serrure (p. ex., pour accommoder une personne handicapée)?

R12 : Oui. Si la hauteur de la serrure est déplacée de plus 6" (150 mm), nous recommandons aussi de déplacer les traverses en conséquence.

PARTIE II - Spécifications de construction d'une PES

Spécifications générales de construction et de montage d'une PES

Remarque : Les spécifications figurant dans la présente partie doivent être modifiées au besoin, et incorporées aux documents de contrat du projet par le concepteur, conformément aux exigences du client (idéalement précisées dans un Énoncé des besoins détaillé concernant la PES) et aux exigences générales du code et du projet.

Ossature murale (figure 1)
Étendre l'ossature des cloisons du plancher au plafond.

Lisses supérieures et inférieures :
Norme SSMA : 1- 5/8” x 6”, épaisseur 18 (600T162-43); ou
De préférence : 2” x 6”, épaisseur 18 (600T200-43)

Fixer la lisse supérieure et inférieure des poteaux d'acier aux deux dalles à 300 mm d'entraxe à l'aide d'une fixation mécanique (de préférence expansible ou à double expansion) avec un effort de cisaillement permis publié d’au moins 600 lb (2640 N). Les vis non expansibles (p. ex. Tapcon) ne sont pas acceptables.

Poteaux :
Norme SSMA : 1- 5/8” x 6”, épaisseur 18 (600S162-43 : 33 ksi); ou
De préférence : 2” x 6”, épaisseur 18 (600S200-43 : 33 ksi)

Espacer les poteaux à 300 mm d'entraxe et les fixer aux lisses supérieures et inférieures au moyen de soudures ou de rivets (et non de vis).

Installer des poteaux jumelés (montants de porte) à l'ouverture de l’huisserie. Installer l’huisserie conformément à HMMA 840 07, parties 3 A, B, C, D et E (sauf que les vis doivent être remplacées par des rivets d'acier).

Installer des traverses à environ 48" du bas du mur, entre les poteaux jumelés de l’huisserie et le poteau adjacent de chaque côté de l’huisserie.

Construire les coins de mur avec des poteaux jumelés.

Remarque :

1. Il est permis de laisser un petit espace et d'utiliser des pans de cloison sèche pour consolider les sections de l’huisserie pendant l'érection du mur, pour autant que les tôles d'acier du côté exposé aux attaques soient continues et recouvrent tous les espaces.
2. Les dessins des poteaux jumelés sont représentatifs. Joindre et orienter les poteaux jumelés conformément à la pratique de l'industrie.

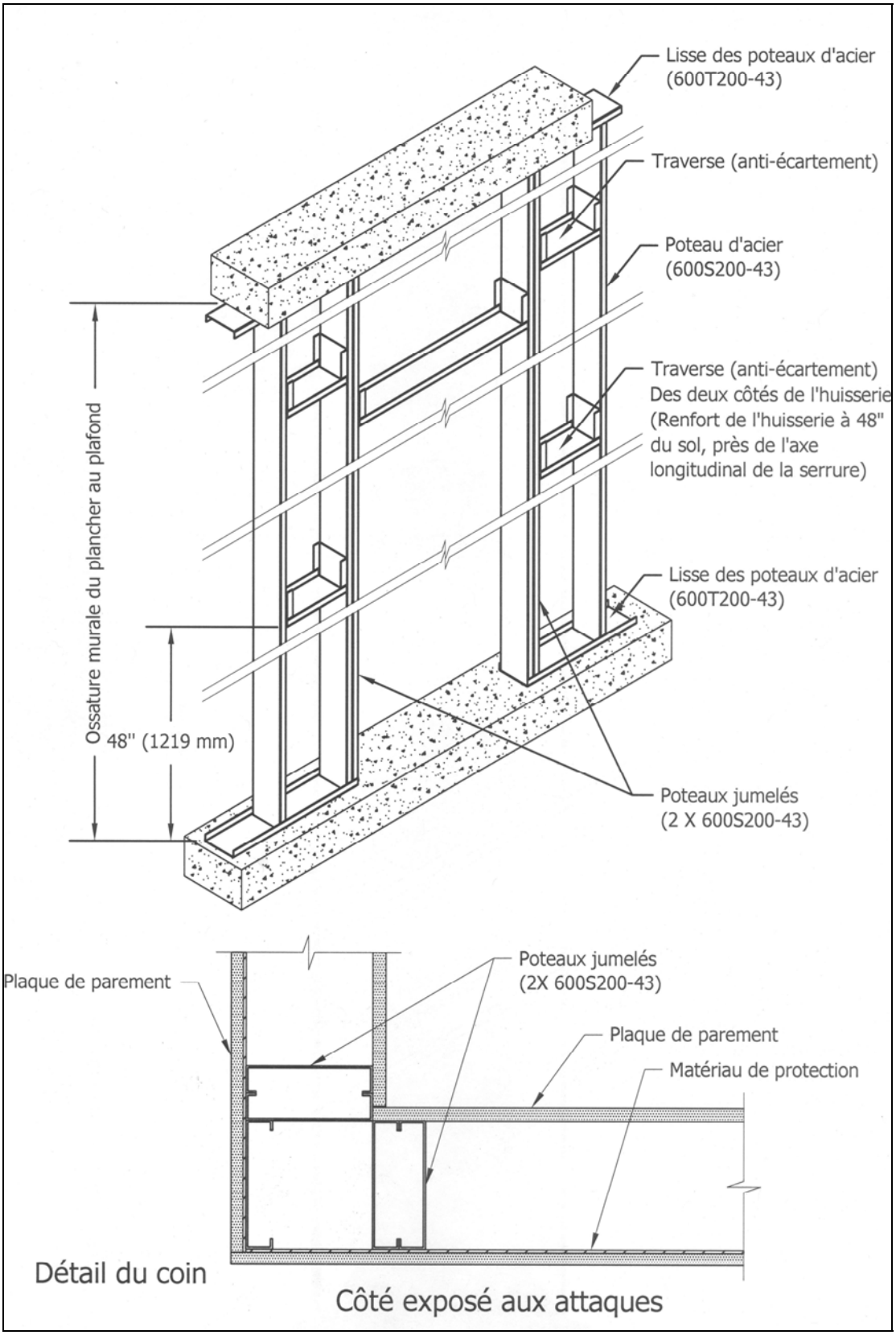


Figure 1 : Détail de l'ossature murale

Matériau de protection de mur (figures 2 à 4)

Le matériau de protection de mur peut être l'une de deux options :

Treillis métallique plat : Conforme à la norme EMMA 557-99. Style ¾-9F : épaisseur nominale du brin 0,120" (de 0,108" à 0,132"). Maille losange de 0,563" x 1,688".
OU
Tôle d'acier : Épaisseur 16, A1008 / A1008M (laminée à froid) ou A1011/ A1011M (laminée à chaud) ou équivalent.

Monter sur le mur extérieur (exposé aux attaques) de la pièce. Soutenir toutes les arrêtes à l'aide de traverses, de poteaux ou de cornières. Aligner les arrêtes des tôles à chaque jointure verticale et horizontale avec l'axe longitudinal des poteaux d'acier ou de la traverse, et fixer toutes les tôles à l'aide de soudures ou de rivets.

Remarque : Les vis (y compris les « vis de sûreté ») **NE** sont **PAS** acceptables pour la fixation permanente du matériau de protection (acier ou treillis d'acier). Les vis peuvent être utilisées pour « épingler » les tôles le temps de placer les rivets ou les soudures. Il n'est pas nécessaire de retirer les vis temporaires.

Soudage (méthode autorisée)

Treillis d'acier (figure 2) : Soudure d'angle de 3 mm le long du brin, à 200 mm d'entraxe

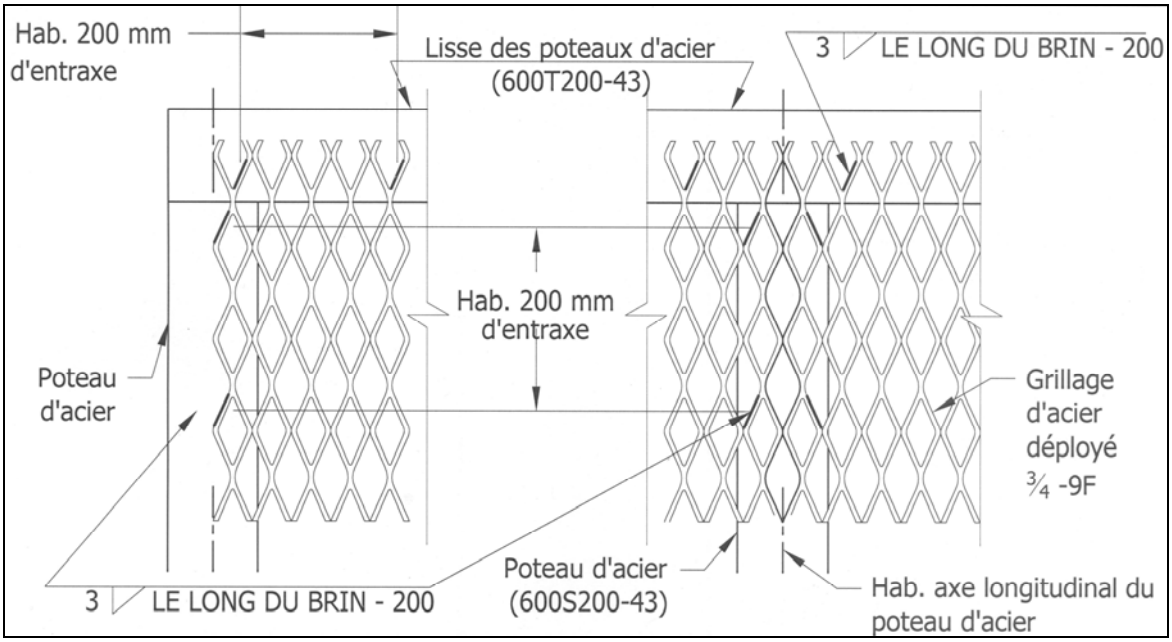


Figure 2 : Soudage du treillis d'acier

Tôle d'acier (figure 3) : Soudure d'angle de 1,5 mm d'une longueur de 15 mm, à 200 mm d'entraxe **ou**
Soudure en bouchon de 8 mm à 200 mm d'entraxe

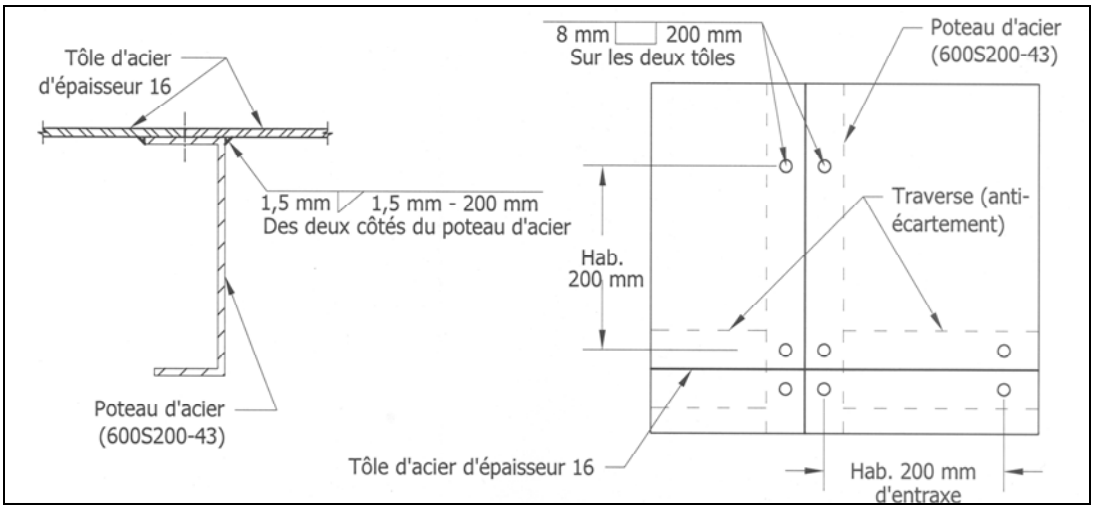


Figure 3 : Soudage des tôles d'acier

Rivets (méthode privilégiée)

Tôles d'acier : Rivets d'acier de 3/16" à 200 mm d'entraxe.
Treillis d'acier : Rivets d'acier de 3/16" et rondelles de protection (DE de 1 ½", DI de 3/16") à 200 mm d'entraxe.

Matériel suggéré :
Rivets : Rivet pop d'acier de 3/16", pièce Speaneur 301-440
Rondelles : Rondelle de protection, DE de1 ½", DI de 3/16", pièce Fastenal 1133204

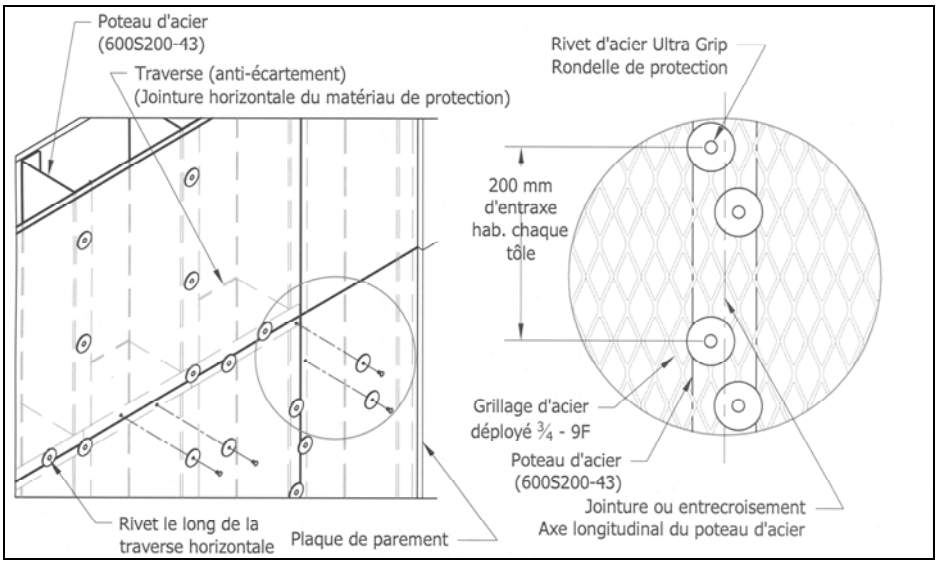


Figure 4 : Rivetage des tôles ou du treillis

Figure 5 : Exemple de jointure de treillis entrecroisés, rivetés

Zone d'attaque critique (figure 6) : Tôle d'acier d'épaisseur 16 (1,6 mm) de qualité commerciale laminée à chaud, ASTM A366, fini mat, étendue 1200 mm autour de l'huisserie à l'intérieur de la pièce d'entreposage sécuritaire et fixée conformément aux exigences en matière de rivets ou de soudures pour le matériau de protection.

Remarque : Les perforations pour des installations techniques ou des conduits ne sont pas autorisées dans la zone d'attaque critique.

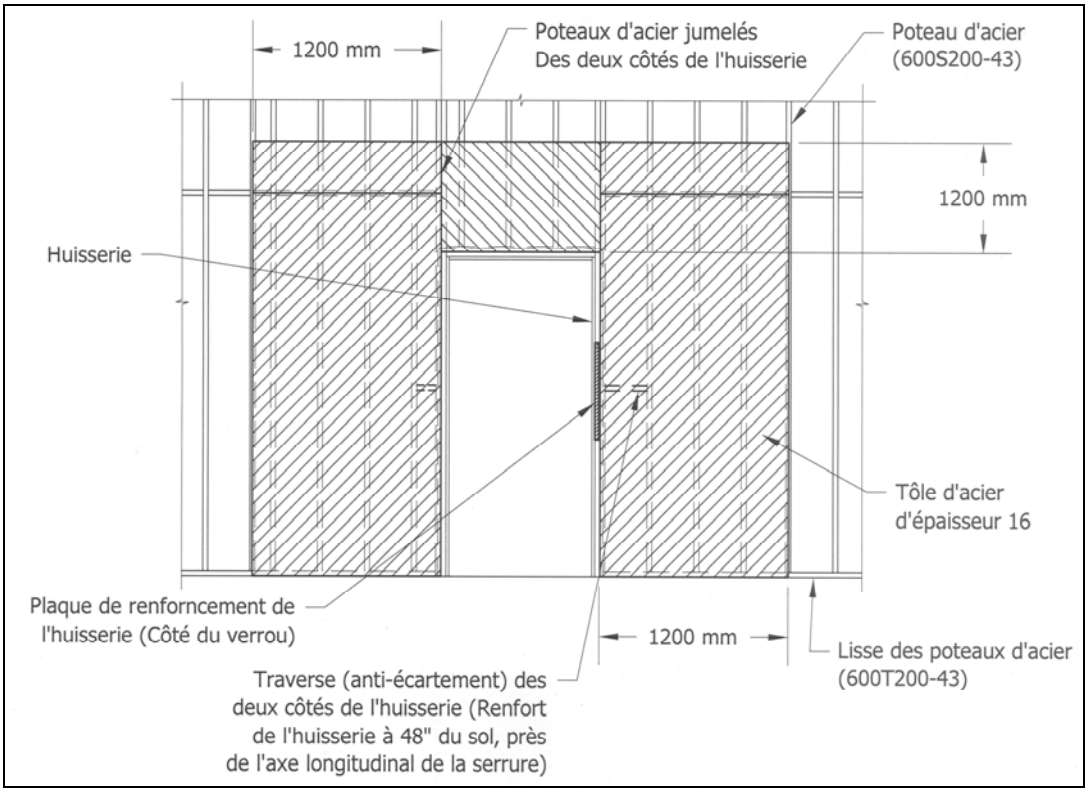


Figure 6 : Renforcement du mur de la zone d'attaque critique

Détails de finition du mur
Installer des plaques de parement de 16 mm des deux côtés du mur (l'intérieur est optionnel). Des vis à cloison sèche standard peuvent être utilisées pour fixer la cloison sèche.

Appliquer un cordon d'étanchéité acoustique résistant au feu continu des deux côtés des lisses supérieures et inférieures.

ASTM E814 (UL1479), ASTM E1966 (UL 2079) or CAN/ ULC S115 avec une résistance au feu / fumée acceptable par l'autorité compétente en la matière (AHJ).

Appliquer sur la surface extérieure du mur une couche d'apprêt ou de peinture d'impression et une couche d'émail lustré. La couche d'apprêt ou de peinture d'impression doit s'étendre au-dessus des plafonds suspendus jusqu'au bas du plafond de charpente. La peinture doit être uniforme et sans taches. Les joints ne doivent pas être visibles. Envisager d'utiliser des couleurs spéciales.

Porte, huisserie et quincaillerie

Porte et huisserie – Porte et huisserie commerciales conformes à la rubrique 08-11-13 de la publication de la CDMA intitulée *Recommended Specification for Commercial Steel Door and Frame Products.*
La porte peut être qualifiée de résistante au feu au besoin.
Éviter les portes de plus de 900 mm (36") de largeur. Les portes à deux battants exigent des mesures spéciales.

Porte :

Épaisseur du parement de porte : Acier de 16 (1,6 mm)
Construction : Âme laminée avec raidisseurs verticaux en acier à 150 mm d'entraxe (raidisseurs soudés ou laminés à chaque tôle de parement, avec les espaces vides entre les raidisseurs remplis de fibre de verre ou de matériau de type laine minérale.
Couverture des bords de porte : Rail d'affleurement supérieur et inférieur « *Flush Closing Channel* » ou « *Flush Channel* ».
Réf. : NAAMM 810-09 Partie 2. A. Figures E et F (détails d'arête).
Arêtes : Toutes les arêtes et les couvertures des bords de porte supérieurs et inférieurs doivent être soudées en continu et meulées jusqu'à être lisses.
Sens de pivotement des portes : (doit être précisé en fonction des besoins du client).

Huisserie :

Épaisseur : Acier d'épaisseur 16 (1,6 mm)
Construction de l'huisserie : Trois pièces « prêtes à assembler » soudées ou entièrement soudées sur le chantier (rénovations).
Ancrages : Ancrages au mur d'acier en forme de Z soudés à l'huisserie.
Renforcement du loquet : Selon les recommandations du fabricant de serrures. Fournir les spécifications de loquet au fournisseur/fabricant pour fournir les exigences nécessaires en matière de renforcement.

Serrures : Choisir dans le tableau 1.

Charnières : Conformes aux normes ANSI/BHMA A156.1, classe 2 et ANSI A8112 (norme des matériaux d'acier)
Mortaisée, cinq charnons, coussinets à billes, standard. Trois charnières par porte (minimum). Dimensions minimales : 114 mm (4 ½") x 114 mm (4 ½") x 3,4 mm (0,124") d'épaisseur.

Les charnières dont les cylindres se trouvent du côté exposé aux attaques (assemblage inversé ou ouverture vers l'extérieur) doivent avoir des goupilles de sécurité, des goupilles de haute sécurité ou des chevilles de sécurité/chevilles de sécurité inversées. Il convient de noter que ces charnières exigent des instructions spéciales lors de la commande.

Produits suggérés :

- Hager (http://www.hagerco.com), pièce de catalogue BB1279
- Stanley Architectural Hardware (www.stanleyhardware.com), pièce de catalogue FBB179
- Mont-Hard (Canada). Les produits Mont-Hard sont vendus par :
- Charnières Montréal (www.montrealhinge.com). Pièce de catalogue BB-1079.

Ferme-porte : Supérieur de style ANSI A156.4, classe 1
Produit suggéré : Ingersoll-Rand LCN série 4040

Seuil : En aluminium (ou autre métal), avec bande-crochet installée sur la porte qui s'emboîte au seuil.
La PES devrait être exemptée des exigences d'accessibilité du code du bâtiment lorsqu'elle n'est utilisée que pour l'entreposage de documents. Cependant, lorsque l'accès aux fauteuils roulants est requis, voici les deux produits recommandés :

- PEMKO (modèle 114) : PEMKO (Toronto) 866-243-9816 (ventes), www.PEMKO.com
- Zero International (modèle 73A) : www.Zerointernational.com

Contacts de porte : Interrupteur haute sécurité UL 634 - niveau 1 ou niveau 2.

Installation de la porte :
La porte est généralement montée de la façon habituelle (ouverture vers la pièce d'entreposage sécuritaire), mais le montage peut être inversé (ouverture vers l'extérieur) dans des situations exceptionnelles.

Renforcement de l'huisserie dans la zone de serrure : (figure 7)
Fixer une tôle d'acier de 6,4 mm x 25 mm x 610 mm à l'intérieur de l'huisserie à l'aide de soudures de pointage à chaque arête. Aligner le centre de la tôle avec le pêne de serrure.

Pour les portes à montage inversé, installer un battement de type Z recouvrant tout le montant de serrure de la porte. Le battement doit avoir une épaisseur n^{o} 14 (2 mm) et être conforme à la norme ASTM A653 ou A653M.

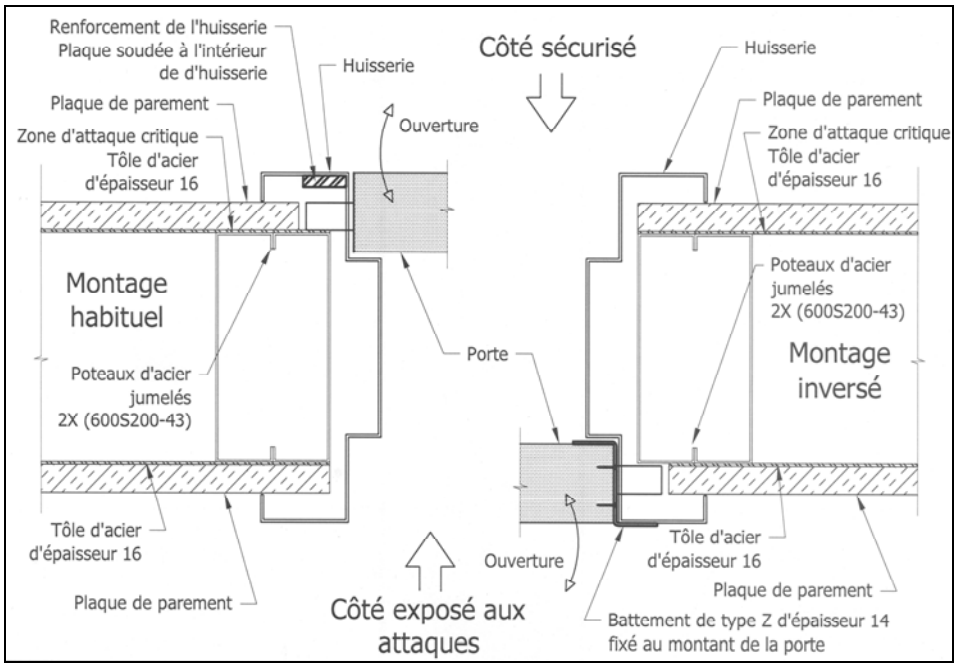


Figure 7 : Renforcement de l'huisserie

Ouvertures pour conduit de ventilation

Remarque : Lorsqu'une résistance supérieure à la coupe est requise, on peut utiliser des barres en acier résistant aux outils (classes 1 ou 2), conformément à la norme ASTM A627.

Montage au plafond : (figure 8)

1. Le manchon de conduit doit être au moins de la même épaisseur que le conduit qu'il protège.
2. La dimension générale du manchon doit être légèrement supérieure à celle du conduit.
3. Construire des cadres à l'aide de cornières en acier de 1- 3/8” x 1- 3/8” x 1/8” soudées autour du manchon de conduit (des supports de montage au plafond sont recommandés).
4. Espacer les barres sécuritaires d'acier de 3/8” Ø à 6" d'entraxe et les souder au cadre.
5. Fixer le manchon de conduit au plafond de charpente à l'aide d'attaches mécaniques.
6. Couper le matériau de protection à un maximum de ¾” du bord de l'ouverture du conduit (trois côtés).
7. Appliquer du mastic de calfeutrage résistant au feu entre le manchon du conduit et le mur fini.

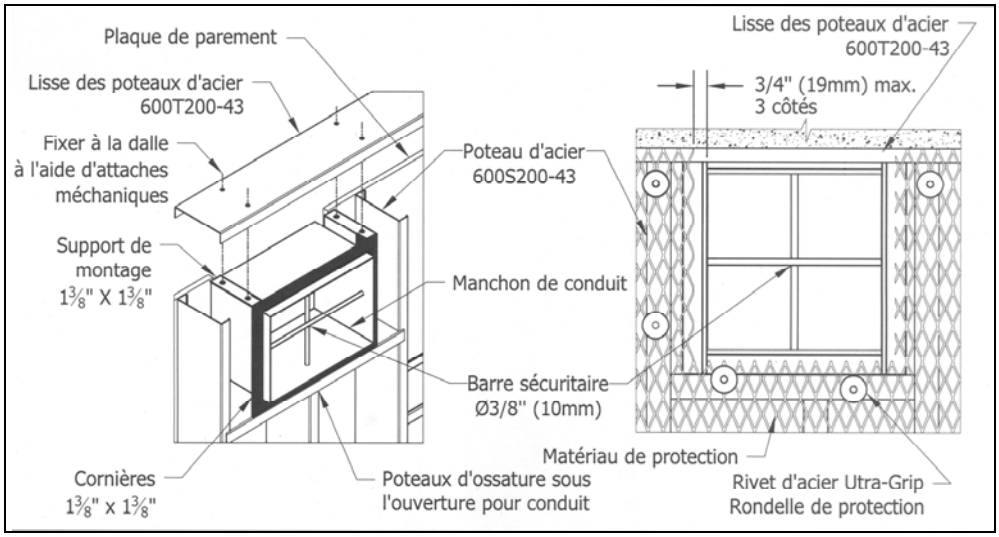


Figure 8 : Ouverture pour conduit de ventilation monté au plafond

Montage en applique : (figure 9)

1. Le manchon de conduit doit être au moins de la même épaisseur que le conduit qu'il protège.
2. La dimension générale du manchon doit être légèrement supérieure à celle du conduit.
3. Construire un cadre de chaque côté du mur à l'aide de cornières en acier de 1-3/8” x 1-3/8” x 1/8” soudées autour du manchon du conduit.
4. Espacer les barres sécuritaires d'acier de 3/8” Ø à 6" d'entraxe et les souder au cadre.
5. Fixer le manchon de conduit à l'aide ˙ boulons et d'écrous hexagonaux de ¼” de diamètre (à l'intérieur de la pièce) à 8¨ d'entraxe autour du manchon de conduit extérieur. La tête de boulon doit se trouver du côté exposé aux attaques et être soudée à au moins trois endroits sur les cornières.
6. Il faut utiliser un cadre autour du manchon de conduit.
7. Appliquer du mastic de calfeutrage résistant au feu entre le manchon de conduit et le mur fini.

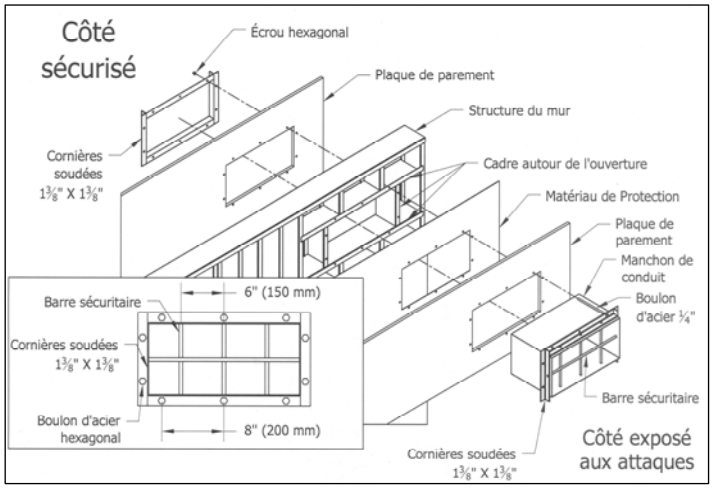


Figure 9 : Ouverture pour conduit de ventilation monté en applique

Guide de sécurité matérielle
Publication de l'organisme-conseil G13-02

Mur mitoyen sécuritaire (MMS)
Guide de l'organisme-conseil

Rev 1.0 (Original)

Les suggestions ou commentaires relatifs au présent guide doivent être communiqués à :
Section de la sécurité matérielle, Sous-direction de la sécurité ministérielle de la GRC,
1426, boul. St-Joseph, Ottawa (Ontario) K1A 0R2

Les questions peuvent aussi être envoyées par courriel à l'adresse : Physec-secmat@rcmp-grc.gc.ca.

Cette publication est SANS CLASSIFICATION (à l'usage de l'organisation).
Au besoin, elle peut être fournie à des fournisseurs, conseillers et concepteurs.

Table des matières

Figures

Définitions

Autorité compétente – Habituellement l'inspecteur en bâtiment de la ville, de la municipalité ou du comté. Pour les bases des Forces canadiennes, l'autorité compétente est le directeur, Service des incendies des Forces canadiennes.

Concepteur – Personne qualifiée (architecte, ingénieur, technologue ou autre) chargée d'élaborer le concept d'un projet précis (dessins et devis) en fonction de l'énoncé des besoins (EB) produit par le client, et conformément aux exigences globales du projet et du code.

Côté exposé aux attaques – Côté de la porte ou du mur exposé à l'ennemi et susceptible de subir une attaque.

Énoncé des besoins – Liste des besoins propres au projet dressée par le client (en particulier choix d'options de rechange) pour le mur mitoyen sécuritaire. L'EB doit être élaboré à partir des renseignements consultatifs figurant à la partie I du présent guide, ainsi que des conseils de spécialistes, au besoin.

Entreposage sur rayons ouverts – Entreposage autre que dans des coffres de sécurité ou coffres-forts approuvés. L'entreposage sur rayons ouverts comprend l'entreposage où les documents sont gardés dans des contenants ou des contenants commerciaux résistants au feu ou à l'eau.

Menace de base (MB) – Menace à laquelle les ministères gouvernementaux sont couramment exposés au Canada dans des conditions de sécurité normale, définie dans la *Norme opérationnelle sur la sécurité matérielle*.

Mur mitoyen sécuritaire – Mur résistant à la force construit conformément au Guide G13-02 de la GRC.

Salle de travail sécuritaire – Pièce, ensemble de pièces, ou espaces conçus spécialement et utilisés pour le traitement et l'entreposage sur rayons ouverts de renseignements classifiés.

Zones – Définies à la référence B.

Abréviations

dB - Décibel
DE – Diamètre extérieur
DI – Diamètre intérieur
EB – Énoncé des besoins
EMR – Évaluation de la menace et des risques
ITS – Indice de transmission du son
MMS – Mur mitoyen sécuritaire
N – Newton
Ø – Diamètre de barre

PES – Pièce d'entreposage sécuritaire
PS – Pièce sécuritaire
STS – Salle de travail sécuritaire

Références

A. *Politique sur la sécurité du gouvernement*
http://publiservice.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578&section=text#cha5

B. *Norme opérationnelle sur la sécurité matérielle*
*h*ttp://publiservice.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329&section=text

Normes commerciales citées comme référence

Les normes suivantes sont vendues par leurs associations de normalisation respectives, ou par des vendeurs de normes comme IHS Standards (http://global.ihs.com), ANSI Store (http://webstore.ansi.org) ou Techstreet (http://www.techstreet.com).

ASTM A627-03 : *Standard Test Methods for Tool-Resisting Steel Bars, Flats, and Shapes for Detention and Correctional facilities* (http://www.astm.org)

ASTM F1267-07 : *Standard Specification for Metal Expanded Steel*
American Society for Testing and Materials (http://www.astm.org/)

CAN/ONGC-1.60 : *Peinture-émail brillante d'intérieur aux résines alkydes / Interior Alkyd Gloss Enamel Paint*
Office des normes générales du Canada (http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html)

EMMA 557-99 : *Standard for Expanded Metal, Introduction, Product Selection Considerations, Terminology, Manufacturing Process, Manufacturing Tolerances and Applications.*
Expanded Metal Manufacturers Association (http://www.naamm.org/emma)

SSMA : Steel Stud Manufacturers Association (http://www.ssma.com/technical_library.aspx)

PARTIE I (À l'usage du ministère ou de l'organisme)

Fonctionnement du guide

Ce guide vise à aider les intervenants en sécurité qualifiés et le personnel de la sécurité matérielle ministérielle à élaborer un énoncé des besoins (EB) concernant la construction d'un mur mitoyen sécuritaire (MMS).

Des architectes ou concepteurs qualifiés doivent être engagés pour élaborer à partir de l'EB des dessins et des devis détaillés comprenant tous les composants et caractéristiques précisés par le client, et pour veiller à ce que le concept soit conforme aux exigences globales du projet et à tous les codes et normes d'aménagement des pièces applicables.

La raison du choix d'un composant ou d'une caractéristique (ainsi que le but d'un espace ou la nature du bien) ne devrait être divulguée qu'aux architectes, concepteurs ou entrepreneurs qui ont besoin de le savoir. Ceux-ci pourraient avoir besoin d'une habilitation sécuritaire pour recevoir cette information.

Il suffit souvent de trier les détails à communiquer, et de les communiquer uniquement en fonction du besoin de connaître.
L'architecte ou le concepteur devrait recevoir une orientation officielle quant à la préparation des dessins pour les soumissions ou la sous-traitance, de façon à ce que les informations névralgiques ne soient pas divulguées inadéquatement. Par exemple, le but ou le nom de la pièce ne doit pas figurer sur les dessins, les devis ou les autres documents de contrat diffusés à grande échelle. Un nom générique ou un chiffre doit être utilisé. Les sous-traitants ne doivent recevoir que l'information nécessaire à l'accomplissement de leur travail (p. ex., dessins de bâtiment et schémas de système partiels qui n'identifient pas les activités adjacentes et ne fournissent pas de détails propres à la sécurité des systèmes). Lorsque c'est faisable, les exigences en matière de sécurité doivent être incluses aux documents de contrat, pour veiller à ce qu'elles soient respectées.

Généralités

Depuis de nombreuses années, plusieurs ministères utilisent des parties des spécifications de construction du guide G1-029 *Pièces sécuritaires*[1] pour construire des murs autour d'espaces ministériels (p. ex. dans des tours de bureaux), d'espaces de travail, de salles des opérations, de zones de haute sécurité, etc.

Ce guide a été élaboré en vue de la construction d'un mur mitoyen sécuritaire, et pour prévenir l'utilisation inadéquate du guide *Pièces d'entreposage sécuritaire* (cf. note 1). Le fait d'avoir un terme, une abréviation, une définition et un numéro de guide propres au mur mitoyen sécuritaire (MMS) facilite aussi le renvoi au document source et évite toute confusion.

[1] Le Guide G1-029 *Pièces sécuritaires* a été mis à jour en 2013 et renommé Guide G13-01 *Pièces d'entreposage sécuritaire* pour mieux exprimer son utilisation initialement prévue.

Le concept de mur figurant dans le présent guide est une construction légère éprouvée et recommandée visant à réduire adéquatement la menace de référence pesant contre les bureaux du gouvernement en milieu urbain standard. Il fournit une résistance moyenne aux accès forcés (y compris ceux perpétrés au moyen d'outils de coupe portatifs), et une très bonne détection de ce genre d'attaques (lorsque l'équipement de détection de vibrations est installé tel que recommandé). Ce type de mur n'est pas approprié lorsqu'une Évaluation de la menace et des risques (EMR) a déterminé qu'il est nécessaire d'assurer une résistance à des accès forcés soutenus. Dans ce genre de situation, il faut envisager d'utiliser des chambres fortes évaluées par l'UL ou des barrières faites sur mesure.

Utilisation

Les murs mitoyens sécuritaires (MMS) sont adéquats pour séparer physiquement une zone de travail d'une zone d'accueil ou d'accès public ou (lorsqu'une EMR le recommande) pour séparer une zone de sécurité d'une zone de travail ou pour parcelliser une zone en particulier.

Les murs mitoyens sécuritaires facilitent la détection d’un ennemi et retardent celui-ci, ce qui permet de l’intercepter grâce à une intervention adéquate dans des délais raisonnables. Il faut souligner qu'une intervention rapide et adéquate est essentielle à l'efficacité d'un système d'alarme ou de détection et de retardement.

Insonorisation

Un MMS n'est pas conçu pour assurer la confidentialité des entretiens, et ne devrait jamais servir de séparation entre une aire insonorisée (AI) et une zone d'accès public. Une AI devrait être une pièce située à l'intérieur d'une zone de sécurité (dont les murs périmétriques peuvent être des MMS).

Cependant, l'insonorisation doit normalement être incluse de façon à réduire les bruits ambiants et limiter les possibilités d'écoute opportuniste de conversations qui, quoique non classifiées, pourraient quand même être considérées comme de nature délicate.
Une construction aboutissant à un indice de transmission du son (ITS) de 54 à 55 dB est généralement adéquate pour l'utilisation d'un MMS.

Le montage suivant fournit un ITS d'environ 54 à 55 dB :

• Deux couches de plaques de parement de 16 mm résistantes au feu
• Une couche de tôle ou de treillis d’acier déployé
• Poteaux d'acier espacés à 300 mm d'entraxe
• Matelas de fibres de verre de 150 mm d'épaisseur entre les poteaux
• Profilés souples en U espacés de 400 mm
• Une couche de plaques de parement de 16 mm résistantes au feu

Cet indice correspond à un mur sans ouvertures ni brèches. Du mastic de calfeutrage acoustique doit être appliqué entre la plaque de parement et toute surface adjacente, pour éviter que le son ne passe par les espaces et brèches.

Les portes installées avec des produits d'étanchéité commerciaux caractéristiques (ou des produits d'étanchéité acoustique mal installés ou ajustés) n'offrent généralement pas plus de 35 dB d'insonorisation, même si les portes ont une classification acoustique. Comme le but d'un MMS n'est pas l'isolation acoustique (et de nombreuses utilisations comprennent des portes et fenêtres architecturales du commerce à des fins de visibilité, d'accessibilité et d'effet sur le public), cela ne devrait pas poser de problème. Les vestibules peuvent être utiles.

Protection contre les incendies

Des cloisons sèches doubles ou de type X peuvent être installées pour respecter le code de prévention des incendies. Des panneaux isolants semi-rigides doivent être utilisés. Il ne faut pas utiliser d'isolant projeté, car il pourrait entraver la transmission des vibrations le long de la tôle d'acier.

Du plancher au plafond

Les murs mitoyens sécuritaires doivent aller du plancher au plafond, c'est-à-dire du plancher porteur fini à la face inférieure du toit ou du plafond de structure. Lorsque les toits et planchers ont une ossature de bois ou d'acier, ils doivent être renforcés d'acier comme les murs. Lorsque cela n'est pas faisable, d'autres mesures compensatoires sont nécessaires. Communiquer avec la GRC pour obtenir une orientation concernant la construction d'un plafond ou d'un plancher sécuritaire.

Construction d'un mur mitoyen sécuritaire adjacent à un autre mur

Lorsqu'un mur mitoyen sécuritaire est construit à côté de murs n'appartenant pas au ministère (p. ex., des espaces loués où aucune modification des murs n'est autorisée en vertu de l'accord d'occupation), le matériau de protection doit être installé du côté sécuritaire (intérieur) du mur, et tout le câblage électrique et d'alarme doit être placé dans un conduit monté en applique.

Conduits et autres pénétrations de service

Dans la mesure du possible, réduire le nombre de conduits et d'ouvertures de service dans les murs mitoyens sécuritaires. Ne pas placer ces ouvertures dans la zone d'attaque critique autour des portes. Lorsque ces ouvertures sont requises, les encadrer par des poteaux à moins d'un pouce (25 mm) du tuyau ou conduit, et fixer celui-ci aux poteaux d'ossature à au moins deux endroits. Étendre le matériau de protection du mur jusqu'à ¾” (20 mm) du bord de l'ouverture. Étendre la plaque de parement jusqu'au tuyau ou conduit. Boucher toutes les brèches avec du produit d'étanchéité résistant au feu. Normes recommandées : ASTM E 814 (UL 1479) et CAN/ULC S115, ou tel que demandé par l'autorité compétente.

Lorsqu'il est nécessaire de tenir compte du mouvement ou de l'expansion des tuyaux ou conduits, ceux-ci peuvent être recouverts d'un manchon métallique ajusté, et le manchon fixé mécaniquement aux poteaux d'ossature à au moins deux endroits. L'espace entre le manchon et le tuyau ou conduit doit être restreint le plus possible, et ne pas dépasser ¼".

Des barres d'acier (cf. figures 8 et 9) doivent être installées dans les conduits situés dans des zones d'accueil ou d'accès public pour retarder l'accès d'une personne par un conduit. Elles peuvent être omises si une EMR détermine qu'un accès non autorisé par ces conduits ne constitue pas une menace viable étant donné les autres mesures de sécurité. Il convient de noter que ces barres n'empêchent pas l'éventuelle destruction, modification ou interruption d'accès aux biens à l'intérieur par l'introduction d'eau ou d'autre matière par un conduit. Si une EMR détermine que ce genre de menaces est possible, tous les conduits et ouvertures pourraient devoir faire l'objet de mesures compensatoires supplémentaires (p. ex., filtres ou clapets).

Détecteur de vibrations

Bien que les tôles d'acier sur les murs offrent une résistance moyenne à la force, elles visent principalement à transmettre aux détecteurs de vibrations les vibrations causées par des accès forcés. Il est aussi recommandé d'installer un système de détection des intrusions volumétrique (p. ex., détecteur de mouvement) à l'intérieur de la pièce ou de l'espace, bien qu'il ne détecte l'ennemi qu'une fois que celui-ci a franchi le MMS, les portes ou les fenêtres et a pénétré dans la pièce. Comme la détection des intrusions a pour but de permettre une intervention visant à intercepter l’ennemi à temps, la détection lors de l'entrée dans la pièce réduit le temps d'intervention.

La GRC a testé et approuvé un détecteur de vibrations pour les MMS, qui figure dans le *Guide d'équipement de sécurité* (GES) G1-001. Pour assurer une détection conforme aux essais d’agrément, les détecteurs doivent être installés directement sur l'acier, près d’un poteau ou d'une solive, à l'aide des socles fournis par le fabricant.

Les détecteurs doivent être espacés selon les recommandations du fabricant, et il doit y avoir au moins un détecteur par segment de mur, pour garantir une bonne détection des attaques. Il faut aussi installer un détecteur sur la porte (en plus d'un interrupteur magnétique permettant de détecter si une porte est ouverte subrepticement) pour garantir une bonne détection des tentatives de coupe ou de forçage de la porte ou de la serrure.

Portes, serrures et fenêtres

Les portes et fenêtres installées dans un MMS doivent fournir une résistance modérée aux accès forcés. Elles peuvent comprendre les options suivantes : vitrage anti-effraction, pellicule plastique de sécurité, grilles ou grillages de sécurité extérieurs (habituellement des treillis en métal déployé sur des cadres d’acier) ou des volets d'acier à enroulement verrouillables. Étant donné la diversité des produits et des utilisations, la GRC n'a pas élaboré d'orientation normalisée pour ces produits.

Énoncé des besoins

Lorsque le ministère (client) n'est pas aussi le concepteur, il faut élaborer un énoncé des besoins (EB), pour préciser au concepteur exactement ce qui est nécessaire et pour déterminer les options de construction sélectionnées parmi celles présentées dans les Spécifications générales à la partie II.

L'EB et tous les documents contribuant à la sélection des éléments particuliers des pièces ou des murs doivent être considérés comme de nature délicate, et traités en conséquence.

Ne pas dire au concepteur pourquoi un choix a été fait à moins qu'il n'ait besoin de le savoir.

Conseils et orientation

Gendarmerie royale du Canada
Sous-direction de la sécurité ministérielle
Section de la sécurité matérielle
1426, boul. St-Joseph
Ottawa (Ontario) K1A 0R2
Sec-Equip@rcmp-grc.gc.ca

PARTIE II - Spécifications de construction d'un MMS

Remarque : Les spécifications figurant dans la présente partie doivent être modifiées au besoin, et incorporées aux documents de contrat du projet par le concepteur, conformément aux exigences du client (idéalement précisées dans un EB détaillé concernant le MMS) et aux exigences générales du code et du projet.

Ossature murale (figure 1)
Étendre l'ossature des cloisons du plancher au plafond.

Lisses supérieures et inférieures :
Norme SSMA : 1- 5/8” x 6”, épaisseur 18 (600T162-43);
ou 2” x 6”, épaisseur 18 (600T200-43) (option privilégiée)
Fixer les lisses d'acier supérieures et inférieures aux deux dalles à 300 mm d'entraxe à l'aide d'une fixation mécanique (de préférence expansible ou à double expansion) avec un effort de cisaillement permis publié d’au moins 600 lb (2640 N). Les vis non expansibles (p. ex., Tapcon) ne sont pas acceptables.

Poteaux :
Norme SSMA : 1- 5/8” x 6”, épaisseur 18 (600S162-43 : 33 ksi); ou
2” x 6”, épaisseur 18 (600S200-43 : 33 ksi) (option privilégiée)
Espacer les poteaux à 300 mm d'entraxe et les fixer aux lisses supérieures et inférieures au moyen de soudures ou de rivets (et non de vis).

Installer des poteaux jumelés (montants de porte) à l'ouverture de l’huisserie. Installer l’huisserie conformément à HMMA 840-07, parties 3 A, B, C, D et E (sauf que les vis doivent être remplacées par des rivets d'acier).

Installer des traverses (anti-écartement) à environ 48" du bas du mur, entre les poteaux jumelés de l’huisserie et le poteau adjacent de chaque côté de l’huisserie.

Construire les coins de mur avec des poteaux jumelés.

Remarque : Il est permis de laisser un petit espace et d'utiliser des pans de cloison sèche pour consolider les sections de l’huisserie pendant l'érection du mur, pour autant que les tôles d'acier du côté exposé aux attaques soient continues et recouvrent tous les espaces.

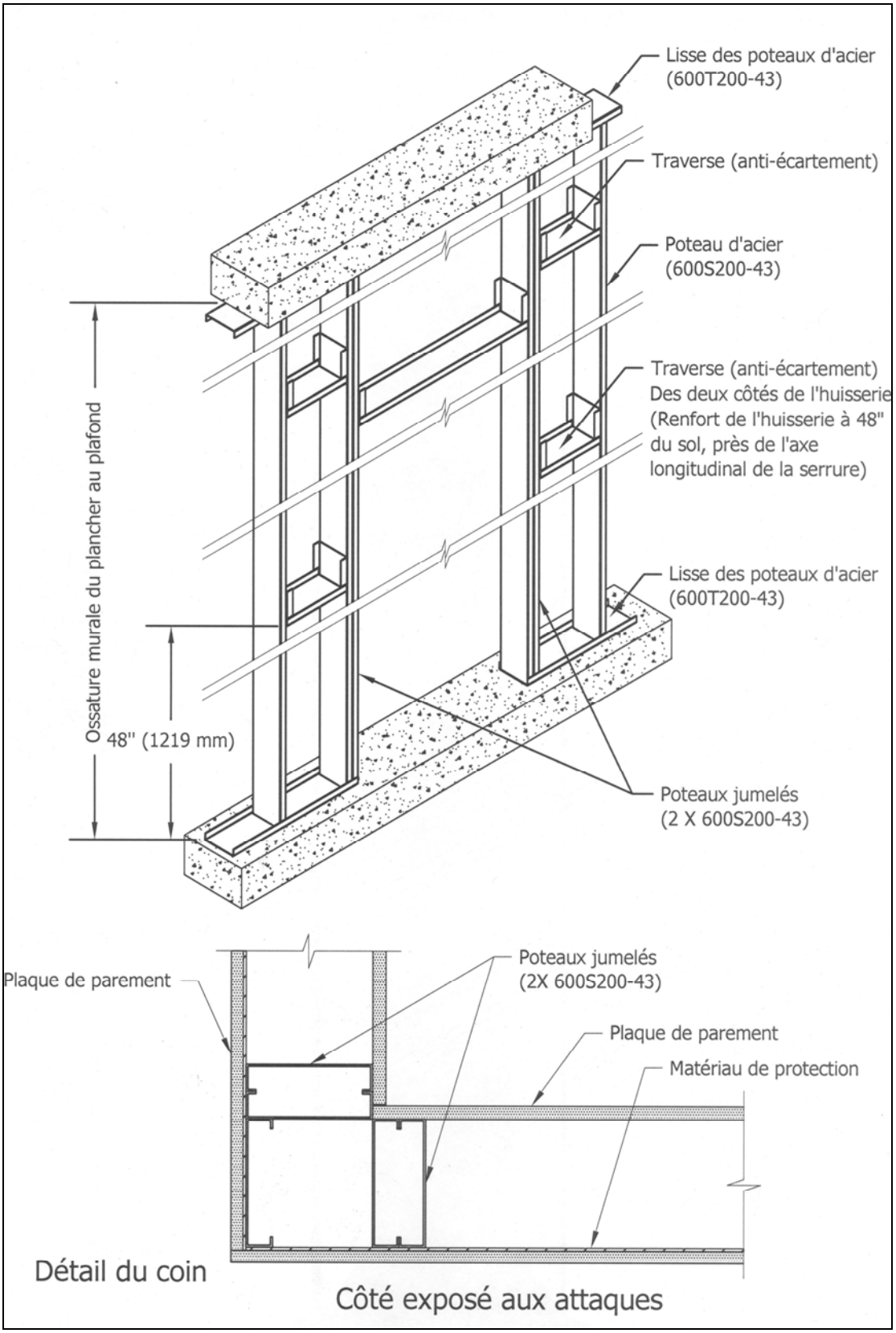


Figure 1 **:** Construction du mur

Matériau de protection de mur (figures 2 à 4)

Le matériau de protection de mur peut être l'une de deux options :

Treillis métallique plat : Conforme à la norme EMMA 557-99. Style ¾-9F : épaisseur nominale du brin 0,120” (de 0,108” à 0,132”). Maille losange de 0,563” x 1,688”.
OU
Tôle d'acier : Épaisseur 16, A1008 / A1008M (laminée à froid) ou A1011/ A1011M (laminée à chaud) ou équivalent.

Monter sur le mur extérieur (exposé aux attaques) de la pièce. Soutenir toutes les arrêtes à l'aide de traverses, de poteaux ou de cornières. Aligner les arrêtes des tôles à chaque jointure verticale et horizontale avec l'axe longitudinal des poteaux d'acier ou de la traverse, et fixer toutes les tôles à l'aide de soudures ou de rivets.

Remarque : Les vis (y compris les « vis de sûreté ») **NE** sont **PAS** acceptables pour la fixation permanente du matériau de protection (acier ou treillis d'acier). Les vis peuvent être utilisées pour « épingler » les tôles le temps de placer les rivets ou les soudures. Il n'est pas nécessaire de retirer les vis temporaires.

Soudage (autre méthode)

Treillis d'acier (figure 2) : Soudure d'angle de 3 mm le long du brin, à 200 mm d'entraxe

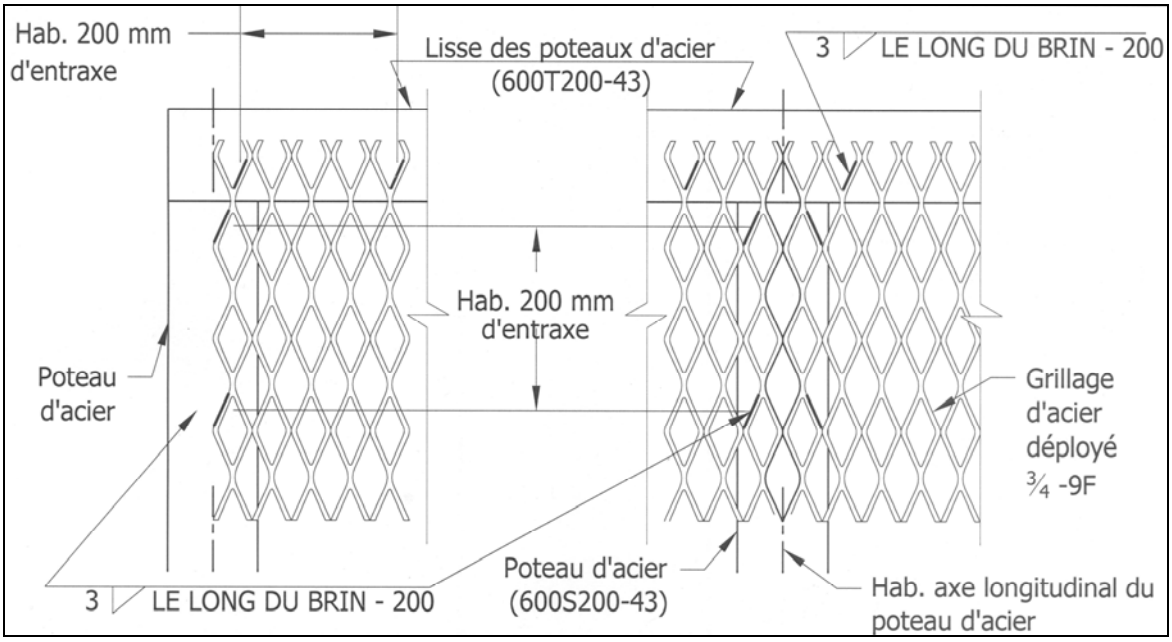


Figure 2 : Soudage du treillis d'acier

Tôle d'acier (figure 3) : Soudure d'angle de 1,5 mm d'une longueur de 15 mm, à 200 mm d'entraxe **ou**
Soudure en bouchon de 8 mm à 200 mm d'entraxe

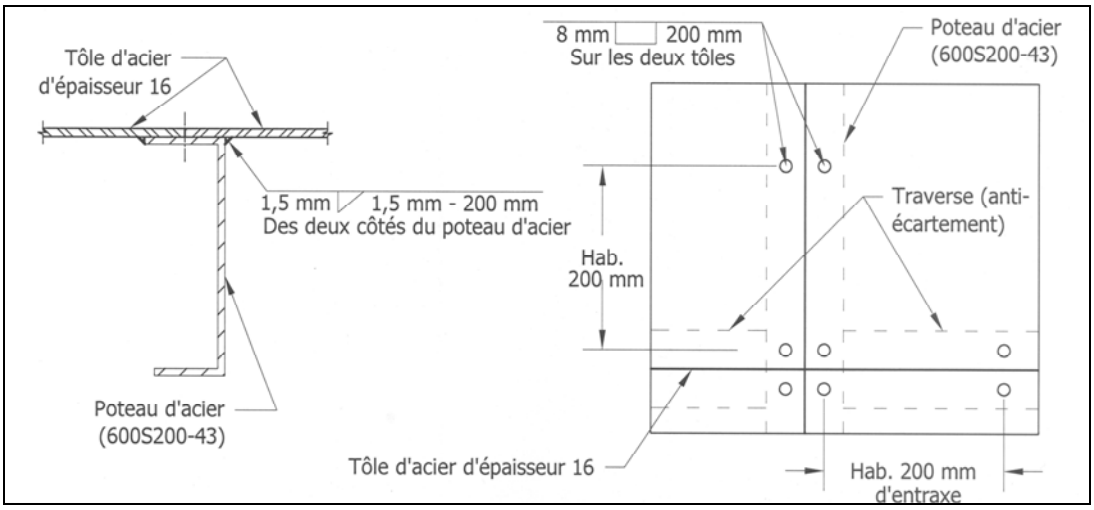


Figure 3 : Soudage des tôles d'aciers

Rivets (méthode privilégiée)

Tôles d'acier : Rivets d'acier de 3/16" à 200 mm d'entraxe
Treillis d'acier : Rivets d'acier de 3/16" et rondelles de protection (DE de 1 ½", DI de 3/16") à 200 mm d'entraxe

Matériel suggéré :
Rivets : Rivet pop d'acier de 3/16", pièce Speaneur 301-440
Rondelles : Rondelle de protection, DE de1 ½", DI de 3/16", pièce Fastenal 1133204

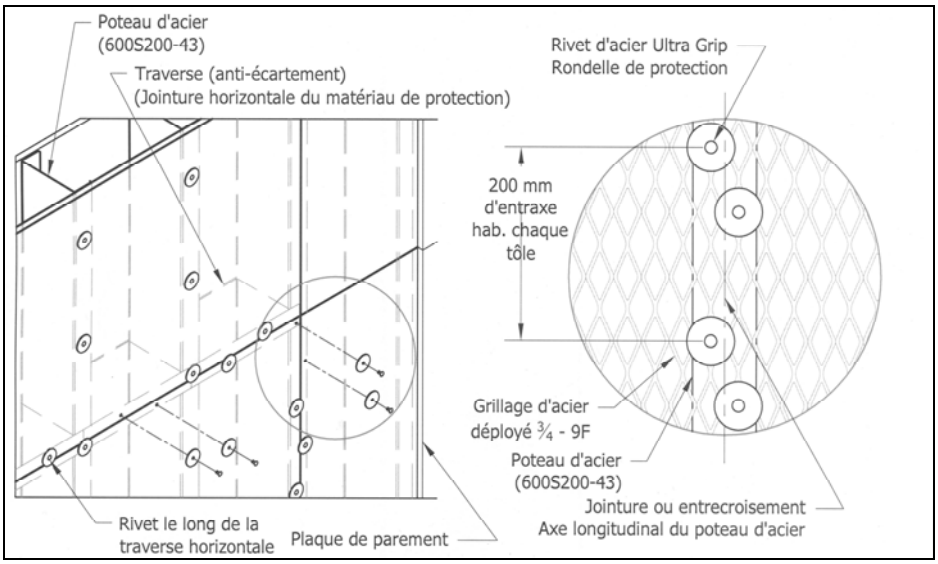


Figure 4 : Rivetage des tôles ou du treillis

Figure 5 : Exemple de jointure de treillis entrecroisés, rivetés

Zone d'attaque critique (figure 6)

Installer la tôle d'acier d'épaisseur 16 à l'intérieur de la pièce, et l'étendre jusqu'à 1200 mm autour du bord de l'huisserie. La fixer conformément aux exigences en matière de rivets ou de soudures pour la méthode sélectionnée.

Remarque : Les perforations pour des installations techniques ou des conduits ne sont pas autorisées dans la zone d'attaque critique.

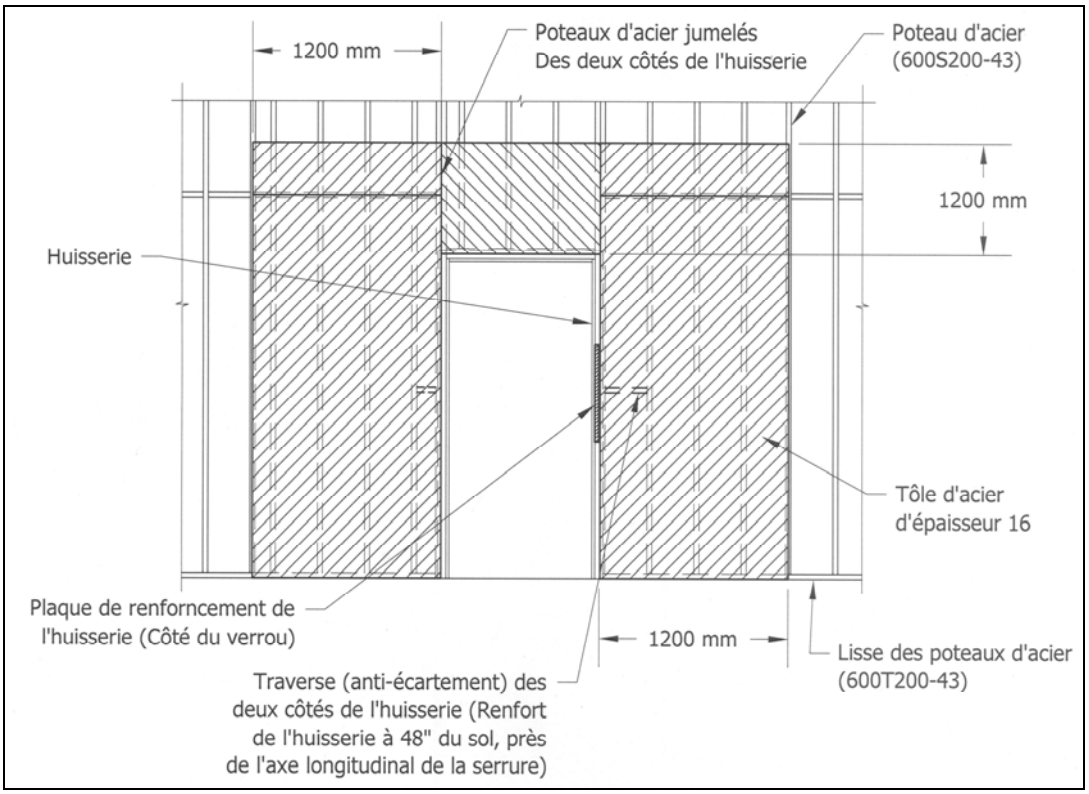


Figure 6 : Renforcement du mur de la zone d'attaque critique

Détails de finition du mur

Fixer la cloison sèche des deux côtés à l'aide de vis à cloison sèche standard.

Appliquer du produit d'étanchéité résistant au feu des deux côtés, en haut et en bas de la cloison. ASTM E814 (UL1479), ASTM E1966 (UL 2079) or CAN/ ULC S115 avec une résistance au feu / fumée acceptable par l'autorité compétente en la matière (AHJ).

Peindre la surface extérieure du mur, du plancher au plafond. La peinture doit être uniforme et sans taches. Les joints ne doivent pas être visibles.
Recommandé : Une couche d'apprêt ou de peinture d'impression et une couche d'alkyde et d'émail lustré CAN/ONGC-1.60

Renforcement de l'huisserie (au besoin) : (figure 7)

Fixer une tôle d'acier de 6,4 mm x 25 mm x 610 mm à l'intérieur de l'huisserie et aligner le centre de la tôle avec le pêne de serrure.

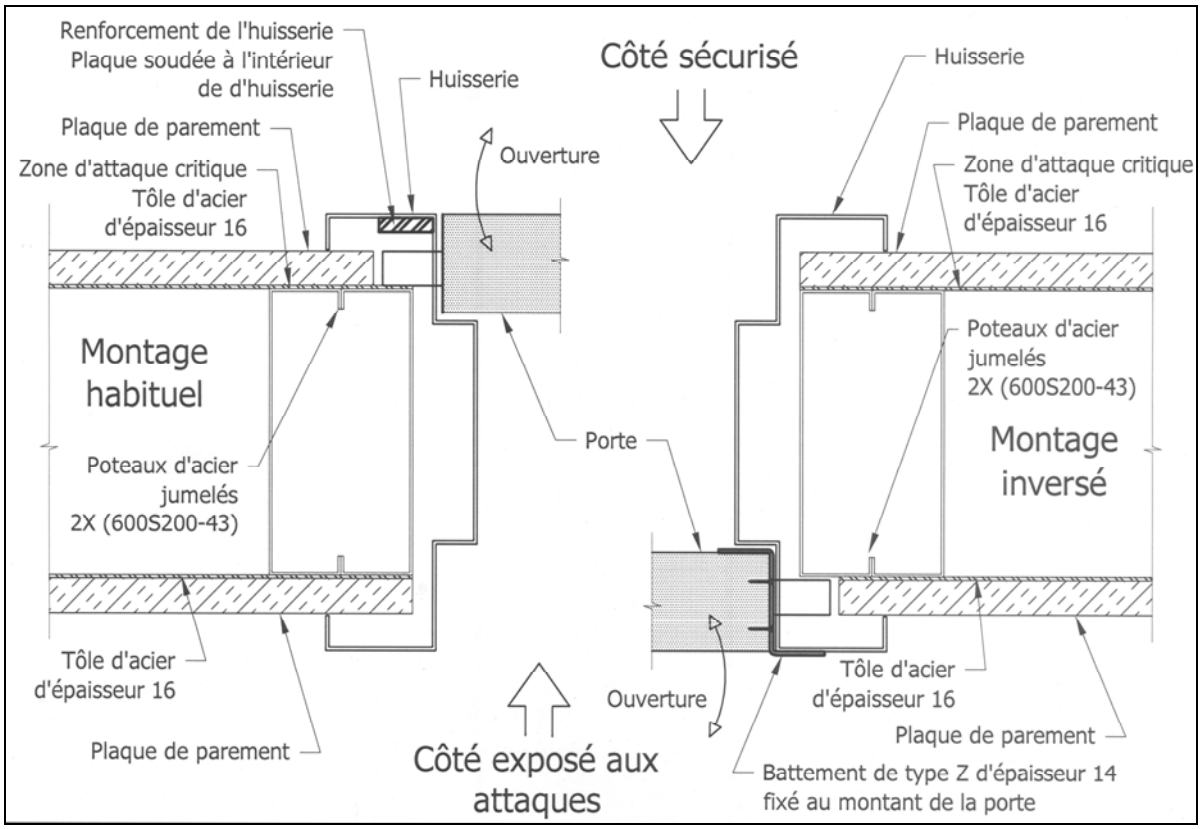


Figure 7 : Renforcement de l'huisserie

Ouvertures pour conduit de ventilation

Remarque : Lorsqu'une résistance supérieure à la coupe est requise, on peut utiliser des barres en acier résistantes aux outils (classes 1 ou 2), conformément à la norme ASTM A627.

Montage au plafond : (figure 8)

1. Le manchon de conduit doit être au moins de la même épaisseur que le conduit qu'il protège.
2. La dimension générale du manchon doit être légèrement supérieure à celle du conduit.
3. Construire des cadres à l'aide de cornières en acier de 1- 3/8” x 1- 3/8” x 1/8” soudées autour du manchon de conduit (des supports de montage au plafond sont recommandés).
4. Espacer les barres d'acier de 3/8” Ø à 6" d'entraxe et les souder au cadre.
5. Fixer le manchon de conduit au plafond de charpente à l'aide d'attaches mécaniques.
6. Couper le matériau de protection à un maximum de ¾” du bord de l'ouverture du conduit (trois côtés).
7. Appliquer du mastic de calfeutrage résistant au feu entre le manchon du conduit et le mur fini.

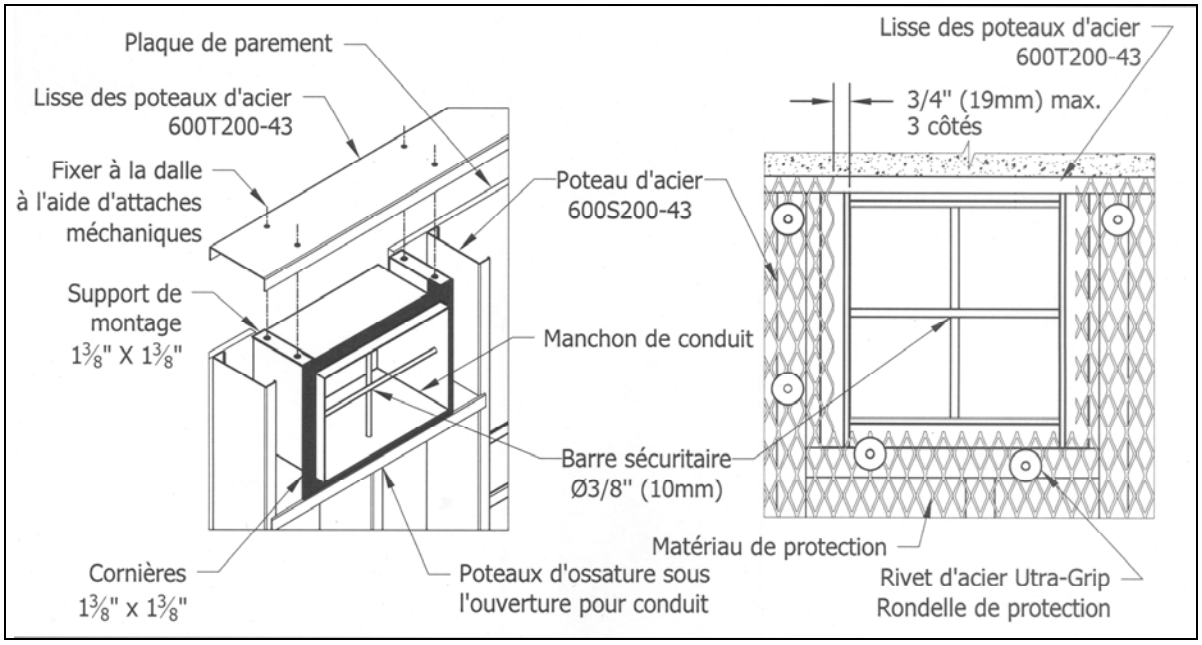


Figure 8 : Ouverture pour conduit de ventilation monté au plafond

Montage en applique : (figure 9)

1. Le manchon de conduit doit être au moins de la même épaisseur que le conduit qu'il protège.
2. La dimension générale du manchon doit être légèrement supérieure à celle du conduit.
3. Construire un cadre de chaque côté du mur à l'aide de cornières en acier de 1-3/8” x 1-3/8” x 1/8” soudées autour du manchon du conduit.
4. Espacer les barres d'acier de 3/8” de diamètre à 6" d'entraxe et les souder au cadre.
5. Fixer le manchon de conduit à l'aide de boulons et d'écrous hexagonaux de ¼” de diamètre (à l'intérieur de la pièce) à 8" d'entraxe autour du manchon de conduit extérieur. La tête de boulon doit se trouver du côté exposé aux attaques et être soudée à au moins trois endroits sur les cornières.
6. Il faut utiliser un cadre autour du manchon de conduit.

7. Appliquer du mastic de calfeutrage résistant au feu entre le manchon du conduit et le mur fini.

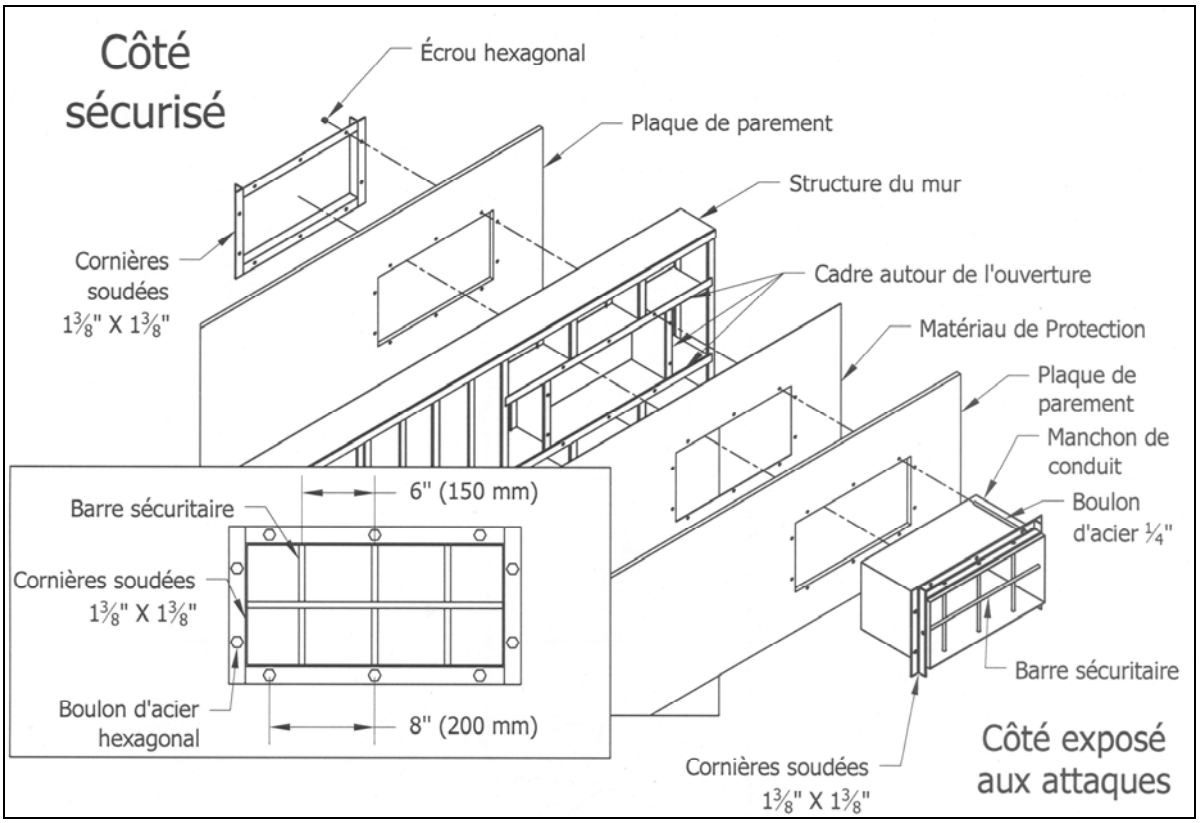


Figure 9 : Ouverture pour conduit de ventilation monté en applique