

Fondement de l’atténuation des risques liés aux véhicules hostiles

GSMGC-025 (2026)

Rédigé par :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
Direction générale,
73, promenade Leikin, Ottawa (Ontario) K1A 0R2

Date de publication : 2026-10-01
Date de mise à jour :

Avant-propos

Le guide Fondement de l'atténuation des risques liés aux véhicules hostiles est une publication NON CLASSIFIÉE, diffusée avec l'autorisation du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (POSM de la GRC).

Il s'agit d'une publication du gouvernement du Canada qui sert de guide pour répondre au besoin d'un guide de base pour informer les spécialistes fonctionnels de la sécurité matérielle travaillant pour les ministères, les organismes et les employés du gouvernement du Canada (GC).

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

Reproduction

La présente publication peut être reproduite textuellement, dans son intégralité et sans frais, à des fins didactiques et personnelles uniquement. Il faut obtenir une autorisation écrite du POSM-GRC pour en faire des adaptations, en extraire des passages ou l'utiliser à des fins commerciales.

Date d'entrée en vigueur

La date d'entrée en vigueur de GSMGC-025 (2026) – Fondement de l'atténuation des risques liés aux véhicules hostiles est 2026-10-01

Registre des modifications

No de modification	Date	Par	Résumé de la modification

Remarque : C'est le POSM-GRC qui est autorisé à apporter des modifications.

Contenu

Avant-propos i
Reproduction i
Date d'entrée en vigueur i
Registre des modifications i
1. Introduction 4
1.1. But 4
1.2. Applicabilité 4
1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle 4
1.4. Considérations relatives à la technologie de l'information 4
1.4.1. Évaluation de la sécurité et autorisation 5
1.4.2. Considérations relatives à l'informatique quantique 5
2. Coordonnées 6
3. Acronymes 6
4. Glossaire 6
5. Fonction d'atténuation des risques liés aux véhicules hostiles 8
5.1. Mesures d'atténuation permanentes 8
5.2. Mesures d'atténuation temporaires 9
6. Évaluation de la dynamique des véhicules 10
7. Menaces liées aux véhicules 10
7.1. Tactiques de véhicules hostiles 11
7.1.1. Engin explosif improvisé embarqué dans un véhicule (VBIED) 11
7.1.2. Le véhicule en tant qu'arme 12
7.1.3. Attaque de véhicules à plusieurs niveaux 12
7.2. Exploits 13
8. Mesures d'atténuation et de protection contre les véhicules hostiles 14
8.1. Apaisement de la circulation 14
Figure 1 – Exemple de chicane 14
8.2. Distance de sécurité 15
Figure 2 – Exemple d'image de distance de sécurité 15
8.3. Zones piétonnes protégées 15
8.4. Bornes et barrières 16
Figure 3 : Exemple d'image de bornes rétractables métalliques installées 16
Figure 4 : Exemple d'image de bornes rondes en béton installées 17

Figure 5 : Exemple d'image de barrières de sécurité rétractables pour véhicules 17
Figure 6 : Exemple d'image de barrières de sécurité temporaires déployables pour véhicules 18
8.5. Points de contrôle des véhicules 18
8.6. Fermetures temporaires 18
8.7. Aménagement paysager 19
9. Normes, essais, sélection des produits 19
10. Détermination des exigences 20
10.1. Évaluation de la menace et des risques (EMR) 21
10.2. Conception fondée sur les menaces 21
10.2.1. Évaluation des menaces 21
10.2.2. Collecte de renseignements 22
10.2.3. Analyse préliminaire 22
10.2.4. Analyse secondaire 22
11. Cycle de vie du projet d'atténuation des véhicules hostiles 23
11.1. Conception 23
11.2. Construction 23
11.3. Opérer 24
11.4. Remplacement/mise hors service 24
12. Prévention du crime par l'aménagement du milieu 24
13. Références et documents sources 24
14. Promulgation 26

1. Introduction

La GRC, en tant que principal organisme responsable de la sécurité matérielle pour le gouvernement du Canada (GC), est chargée de fournir des conseils et des orientations sur toutes les questions relatives à la sécurité matérielle.

1.1. But

Le présent document a pour but de fournir aux spécialistes fonctionnels de la sécurité matérielle du GC des conseils sur les fondements de l'atténuation des véhicules hostiles.

1.2. Applicabilité

Le présent guide s'applique à l'élaboration de stratégies de sécurité matérielle pour les ministères et organismes où des menaces véhiculées sont possibles. Le public visé comprend les spécialistes fonctionnels de la sécurité matérielle, le personnel de gestion et les décideurs ayant un pouvoir de gestion ou d'acceptation des risques au sein du ministère ou de l'organisme qui travaillent à l'atténuation des risques posés par les véhicules hostiles.

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

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

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

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

1.4. Considérations relatives à la technologie de l'information

Les aspects liés aux technologies de l'information (TI) ne sont pas toujours nécessaires lors de l'élaboration de plans de solutions de sécurité matérielle. Il existe toutefois une menace en constante évolution concernant les systèmes informatiques et, compte tenu de la convergence entre la sécurité matérielle et la sécurité informatique, il est essentiel d'évaluer

les risques liés aux applications informatiques et aux logiciels connectés à un réseau qui assurent le fonctionnement et le soutien des équipements dans les bâtiments gérés par GC. Ces systèmes de contrôle peuvent notamment concerner, sans s'y limiter, l'éclairage de sécurité, les portails périphériques, les portes, les systèmes de chauffage, de ventilation et de climatisation (CVC), etc.

1.4.1. Évaluation de la sécurité et autorisation

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

1.4.2. Considérations relatives à l'informatique quantique

Les ministères et organismes du gouvernement du Canada sont chargés de gérer les risques liés à la cybersécurité dans leurs domaines de compétence, ce qui inclut les systèmes fonctionnant en conjonction avec les systèmes de sécurité matérielle. Il est important que l'ensemble du personnel du gouvernement du Canada soit conscient de la menace que représente l'informatique quantique et de l'impact qu'elle pourrait avoir sur les systèmes qu'il utilise ou dont il est responsable. Les ordinateurs quantiques utiliseront la physique quantique pour traiter des informations et résoudre des problèmes qu'il est impossible de résoudre avec les capacités informatiques actuelles.

La cryptographie, qui est l'étude des techniques utilisées pour rendre illisibles des informations en clair, puis les reconvertir dans une forme lisible, est un moyen efficace de protéger la confidentialité et l'intégrité des informations de l'administration fédérale. L'avenir de l'informatique quantique menace de rendre inefficace une grande partie de la cryptographie que nous utilisons actuellement, et des mesures doivent être prises pour protéger l'administration fédérale et la « pérenniser ». Il est recommandé aux ministères et aux organismes de faire évoluer leurs solutions de cybersécurité existantes vers l'utilisation de la cryptographie poste-quantique (PQC), qui consiste des algorithmes conçus pour être résistants à l'informatique quantique tout en pouvant être exécutés sur un ordinateur classique. Pour plus d'informations sur l'informatique quantique et la PQC, les ministères et les organismes sont invités à contacter le Centre canadien de cybersécurité (CCCS).

Afin de gérer efficacement la menace quantique, le CCCS recommande aux ministères et aux agences d'évaluer le niveau de sensibilité de leurs informations et d'en déterminer la durée de vie, afin d'identifier celles qui pourraient être exposées à

un risque. Ils doivent également revoir leur plan de gestion du cycle de vie informatique et leur budget afin de prévoir les mises à jour logicielles et matérielles susceptibles d'avoir un impact significatif et sensibiliser leur personnel à la menace quantique. Pour plus d'informations, veuillez-vous reporter à la directive de cybersécurité ITSE.00.017 du CCCS.

2. Coordonnées

Pour de plus amples renseignements, veuillez communiquer avec :

Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73 promenade Leikin, arrêt postal 17
Ottawa, ON
K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

Acronymes/abréviations	Définition
ARVH	Atténuation des risques liés aux véhicules hostiles
ASTM	Société américaine pour les essais et les matériaux
DGS	Directive sur la gestion de la sécurité
EAS	Évaluation de sécurité et autorisation
EEI	Engin explosif improvisé
EM	Expert en la matière
EMR	Évaluation de la menace et des risques
GC	Gouvernement du Canada
GRC POSM	GRC Principal organisme responsable de la sécurité matérielle
IPO	Instructions permanente d'opérations
NPSA	« National Protective Security Authority » (Royaume-Uni)
PSG	Politique sur la sécurité du gouvernement
PCAM	Prévention du crime par l'aménagement du milieu
SCT	Secrétariat du Conseil du Trésor du Canada
VADS	« Vehicle Attack Delay Standard »
VBIED	Engin explosif improvisé placé dans un véhicule
VIP	Personnes très importante

4. Glossaire

Terme	Définition
Actif	Actifs corporels ou incorporels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources

	financières, à la confiance des employés et du public et à la réputation internationale.
Attaque en maraude	Attaques violentes à évolution rapide où des auteurs de menace se déplacent dans un endroit dans le but de faire des victimes et de détruire des biens.
Atténuation des risques liés aux véhicules hostiles	Mesures de protection autour d'un immeuble ou d'un complexe visant à empêcher des véhicules hostiles de s'en approcher de trop près.
Conception fondée sur les menaces	Appliquer des mesures préventives et des garanties dans la conception d'un bâtiment, d'une installation ou d'un espace. Fondé sur les principes énoncés dans le document de l'Agence internationale de l'énergie atomique intitulé *Menaces de référence*.
Contrôle de l'accès	Assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint, en effectuant le triage des visiteurs et du matériel aux points d'entrée par les membres du personnel, les gardes ou de façon informatisée et, lorsque requis, en surveillant leur déplacement à l'intérieur de l'installation ou des zones d'accès restreint en les escortant
Distance de sécurité	Distance entre une menace potentielle et le bien ou l'actif.
Évaluation de la menace et des risques (EMR)	Processus d'évaluation des actifs d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques.
Installation	Lieu physique utilisé dans un but particulier. On entend par installation une partie ou la totalité d'un immeuble, soit un immeuble, son emplacement et ses alentours, ou encore une construction qui n'est pas un immeuble. Le terme désigne non seulement l'objet même, mais aussi son usage (p. ex. champs de tir, terres agricoles).
Menace	Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.
Menace fondée sur la conception	Un profil du type, de la composition, des capacités, des méthodes, du dommage prévu et/ou de l'intensité d'une menace délibérée, accidentelle ou naturelle sur laquelle reposent les activités techniques et les opérations de sécurité d'une installation.
Menace interne	Cas où des membres du personnel, autorisés à entrer ou à travailler dans une installation du GC, se livrent à des actions délibérées contre le GC, leur employeur ou leurs collègues. Les actes peuvent comprendre des activités criminelles, des menaces ou des actions physiques, de l'espionnage, de la subversion et du sabotage.
Mesures de protection	Actifs ou contrôles externes qui réduisent les risques aux employés, d'autres actifs ou la prestation de services en diminuant la probabilité d'un événement menaçant, en réduisant la probabilité de compromission, ou atténuer la gravité du résultat par une

	interaction directe ou indirecte avec les valeurs de l'actif, les menaces ou les vulnérabilités.
Périmètre	Ligne de sécurité continue entourant une zone sécurisée.
Point d'entrée sécurisé/ « sally port »	Une entrée/sortie sécurisée et contrôlée comprenant deux ensembles de portes/barrières, où une seule s'ouvre à la fois pour éviter le talonnage.
Risque résiduel	Le risque subsistant après la sélection et la mise en œuvre de mesures de protection.
Tolérance au risque	Volonté d'une organisation d'accepter ou de rejeter un niveau donné de risque résiduel (exposition). La tolérance au risque peut varier d'un organisme à l'autre, mais elle doit être bien comprise par les personnes qui prennent des décisions liées au risque sur une question donnée.

5. Fonction d'atténuation des risques liés aux véhicules hostiles

L'atténuation des risques liés aux véhicules hostiles (ARVH) est un élément clé de la sécurité matérielle visant à réduire les risques posés par les menaces émanant de véhicules. L'ARVH est la sélection et la mise en œuvre de mesures de protection adaptées pour atténuer les menaces propres à un site, généralement déterminées par la réalisation d'une évaluation de la menace et des risques (EMR), et l'utilisation d'une approche de conception axée sur la menace et l'élaboration de mesures de protection appropriées aux conditions les plus probables d'un incident de sécurité.

Les mesures ARVH sont le déploiement intégré de processus, de procédures et de barrières physiques de sécurité pour contrer les menaces véhiculées. Elles comprennent généralement une combinaison de mesures de sécurité matérielle, de sensibilisation et de formation à la sécurité, de sécurité opérationnelle, de gestion de la circulation et de mesures de modération de la circulation.

5.1. Mesures d'atténuation permanentes

Les installations et les terrains autour de l'installation occupés par les ministères et organismes gouvernementaux pendant de longues périodes, qu'ils soient loués ou propriétaires, nécessiteront probablement des mesures de protection permanentes contre les ARVH. Ces mesures de protection seront mises en place et entretenues pour assurer une protection constante de l'installation, garantissant que le niveau de risque résiduel quotidien est égal ou inférieur à la tolérance au risque du ministère ou de l'organisme. Les spécialistes fonctionnels de la sécurité matérielle devraient être inclus le plus tôt possible dans la planification des nouvelles installations et des rénovations des installations existantes afin de s'assurer que les mesures de sécurité matérielle sont incluses dans le plan de projet. Les stratégies permanentes d'ARVH utiliseront une combinaison d'atténuations et de mesures de protection décrites à la section 8 du présent guide.

5.2. Mesures d'atténuation temporaires

Des mesures de protection ARVH temporaires sont souvent requises lorsqu'il est nécessaire de protéger une zone au-delà de ses exigences habituelles. Cela est le plus souvent dû à un afflux de personnes dans une zone, ce qui augmente le risque que celle-ci soit ciblée par des acteurs malveillants pour causer le plus de victimes. Cela peut inclure, sans s'y limiter :

- **Événements publics gérés par le gouvernement :** Les salons de l'emploi, les conférences publiques ou les célébrations ou cérémonies où des membres du public se rassemblent en masse sur la propriété du gouvernement ou dans un espace événementiel géré par un ministère ou un organisme gouvernemental. L'augmentation de la densité de piétons nécessitera une augmentation des mesures de sécurité pour assurer la sécurité des participants et des employés du gouvernement.
- **Réunions de fonctionnaires et de VIP :** Lorsqu'un nombre exceptionnellement élevé d'employés de la fonction publique se réunissent pour des événements de réseautage, des sommets ou des groupes de travail prévus, il peut être nécessaire de renforcer temporairement les mesures de sécurité matérielle dans l'installation qui accueille l'événement. La menace d'un incident augmente avec l'ampleur du rassemblement, si des VIPs sont présentes (comme des diplomates étrangers, des élites du secteur privé ou des hauts fonctionnaires) ou si le rassemblement fait l'objet d'une couverture médiatique.
- **Manifestations antigouvernementales :** Lorsque des manifestations antigouvernementales sont attendues à proximité ou à proximité d'installations ou d'événements gouvernementaux, le risque d'une menace véhiculée par un véhicule augmente d'autant. Il est recommandé que le ministère ou l'organisme à proximité ou ciblé par les manifestations travaille avec les organismes locaux d'application de la loi compétents (service de police compétent) pour coordonner les efforts visant à minimiser les risques pour les biens et les employés du gouvernement. Il peut s'agir de fermetures temporaires de routes, de l'installation de barrières temporaires pour les véhicules ou de la réduction du personnel sur place pendant la durée des manifestations.

Plusieurs facteurs propres à ces scénarios doivent être pris en compte lors de l'évaluation visant à déterminer l'étendue des mesures de sauvegarde temporaires supplémentaires, y compris, mais sans s'y limiter :

- **Taille et densité prévues de la foule :** Les événements impliquant de grands groupes de personnes et/ou des foules denses présentent un risque de préjudice plus élevé que les événements impliquant de plus petits groupes de personnes et/ou des foules dispersées.
- **Durée de l'événement :** Plus la durée de l'événement augmente, plus le risque de préjudice augmente.
- **Attention des médias/incidence sur les intervenants :** Les événements qui devraient attirer beaucoup l'attention des médias ou qui impliquent des groupes marginalisés qui ont été historiquement ciblés par des individus ou des groupes présenteront un risque de préjudice plus élevé que les événements qui ne devraient attirer que peu ou pas

d'attention médiatique ou ne pas impliquer spécifiquement des groupes marginalisés.

6. Évaluation de la dynamique des véhicules

Une évaluation de la dynamique des véhicules est une évaluation scientifique d'un site particulier, qui recueille des données sur la façon dont les différentes marques et modèles de véhicules pourraient se comporter, et leur impact potentiel lors d'un événement ARVH. Cela peut fournir des données précieuses qui peuvent être utilisées lors de l'élaboration d'une stratégie ARVH. La méthodologie d'évaluation de la dynamique du véhicule comprend généralement :

- Profiler les véhicules en fonction de la taille, du poids, de la puissance et de la conception;
- Analyse des voies d'accès potentielles en fonction des routes existantes, des pentes, des mesures physiques d'apaisement de la circulation et de la friction de surface pour déterminer les paramètres possibles de déplacement des véhicules;
- Analyse des vecteurs d'attaque pour déterminer les angles d'approche potentiels et les vitesses possibles des véhicules;
- Évaluer les schémas de déplacement potentiel des véhicules sous différentes charges, vitesses, terrains et conditions météorologiques;
- Déterminer et analyser les voies d'évacuation potentielles des véhicules, tant pour l'auteur de la menace que pour l'évacuation des civils; et
- Évaluer les mesures de protection ARVH existantes et leur efficacité dans leur environnement opérationnel. (Remarque : les cotes des essais de produits sont déterminées dans des environnements contrôlés et peuvent ne pas fonctionner exactement comme elles le feraient dans un environnement d'exploitation unique).

Les évaluations de la dynamique des véhicules sont propres à chaque site et peuvent inclure des considérations supplémentaires en plus des exemples ci-dessus. Les évaluations dynamiques des véhicules peuvent être intégrées à diverses évaluations de sécurité, comme une EMR, en fournissant des données empiriques et des considérations propres aux véhicules pour appuyer les stratégies de protection recommandées.

7. Menaces liées aux véhicules

Les incidents liés à des véhicules sont en hausse à l'échelle mondiale en raison de leur grande disponibilité et du faible niveau de compétence requis pour les utiliser à des fins hostiles. Les menaces véhiculées vont du vandalisme aux attaques sophistiquées ou agressives menées par des auteurs de menaces, qui peuvent accéder aux véhicules par plusieurs moyens, notamment :

- Propriété : un véhicule appartient à l'auteur de la menace ou est immatriculé au nom de celui-ci;
- Emprunté : un véhicule est prêté par un tiers non conscient de l'usage prévu ou complice;
- Loué : un véhicule est loué auprès d'une entreprise, à l'aide de vrais ou de faux justificatifs d'identité;
- Vol : vol d'un véhicule immobile et sans surveillance (verrouillé ou avec les clés dans le

contact) ; ou
- Détourné : saisie d'un véhicule occupé ou stationné à l'intérieur ou à l'extérieur d'une zone protégée.

7.1. Tactiques de véhicules hostiles

Les véhicules peuvent être utilisés de diverses manières pour permettre aux auteurs de menaces d'atteindre leurs objectifs. Cela pourrait inclure l'utilisation d'un véhicule comme arme, notamment dans le cadre d'attaques à la voiture bélier contre des piétons ou des biens. Les véhicules peuvent également faciliter la livraison ou la dissimulation de dispositifs malveillants ou de groupes d'acteurs malveillants. Quelle que soit l'intention, les tactiques de véhicules hostiles comportent souvent des indicateurs qui peuvent servir d'indicateurs précurseurs d'une attaque imminente. Lors d'un incident de sécurité impliquant un véhicule, il est peu probable que le conducteur respecte le code de la route. Les indicateurs d'alerte précoce comprennent, sans s'y limiter :

- Traversée d'espaces verts comme des champs, des terrains de loisirs et des parcs;
- Stationnement illégal;
- Ne pas tenir compte des feux de circulation;
- Conduire à des vitesses élevées;
- Conduire du mauvais côté de la route;
- Conduire sur les trottoirs ou les sentiers piétonniers; et
- Entrer dans les zones piétonnes.

7.1.1. Engin explosif improvisé embarqué dans un véhicule (VBIED)

Un VBIED consiste en un engin explosif improvisé (visible ou dissimulé) situé à l'intérieur d'un véhicule, qui est ensuite transporté vers une cible. L'auteur de la menace tentera de s'approcher le plus possible de sa cible pour causer le plus de dommages possible. Il peut s'agir d'une zone densément peuplée pour maximiser les pertes ou d'un endroit essentiel aux opérations de la cible, comme de l'équipement industriel ou un entreposage de matériel.

L'auteur de la menace peut tenter de le faire secrètement, en utilisant le véhicule pour dissimuler l'engin explosif et son intention. Dans ces cas, il tentera d'attirer le moins de soupçons possible, en utilisant peut-être des documents falsifiés ou en tirant parti d'une menace interne pour accéder aux zones contrôlées de la cible sans déclencher d'alarme. Une méthode de diffusion secrète peut être choisie pour permettre à l'auteur de la menace de s'échapper avant que l'EEI explose, ou pour qu'il explose plus tard lorsqu'il aura un effet maximal (par exemple, le garer près de l'entrée d'un bâtiment, dans l'intention de le faire exploser à l'heure prévue de l'arrivée ou du départ du personnel).

Par ailleurs, un auteur de menace peut tenter une attaque plus directe et plus ouverte ; la forme la plus courant étant un attentat-suicide. Dans le cadre de ces attaques, l'auteur de la menace conduit le VBIED directement à l'endroit ciblé et la fait exploser immédiatement. Ils peuvent tenter une attaque à plusieurs niveaux, en utilisant le véhicule de livraison pour transporter les attaquants qui mettront pied à terre et

poursuivront l'attaque à pied avant que la VBIED n'explose. Quel que soit l'objectif, la vitesse et l'agressivité définiront son approche ; Il ne respectera pas le code de la route, tenteront de contourner les obstacles ou de les franchir et pourraient percuter de manière opportuniste des piétons à l'approche de la cible.

Les effets de la détonation d'un VBIED comprennent : l'explosion, la boule de feu, la fragmentation primaire et secondaire et le choc au sol.

La distance de sécurité en cas d'explosion (la distance entre l'appareil et le bien) est le facteur le plus important pour déterminer l'étendue des dommages qui peuvent être causés. L'optimisation de la distance de sécurité en cas d'explosion réduira les dommages subis par le bien. Les effets et les mesures d'atténuation d'une attaque à l'engin explosif sont abordés plus en détail dans le document GSMGC-002 Guide d'atténuation des effets du souffle d'explosion.

7.1.2. Le véhicule en tant qu'arme

Les véhicules eux-mêmes peuvent être l'outil principal du plan d'un auteur de menace, utilisant sa masse et sa vitesse pour attaquer une cible. Parfois appelée attaque à la voiture-bélier ; l'utilisation d'un véhicule comme arme est l'acte intentionnel de conduire un véhicule :

- Sur un individu ou dans des foules de personnes pour causer des pertes ; ou
- Conduire délibérément un véhicule contre une infrastructure pour endommager ou perturber son fonctionnement. Cela peut indirectement entraîner des préjudices pour les personnes, perturber le fonctionnement d'un site ou d'un événement ou, plus largement, des services ou des fournitures essentiels.

La conduite d'un véhicule dans la foule est considérée par les auteurs de menaces comme attrayante parce qu'elle est susceptible de faire de nombreuses victimes, qu'elle est peu complexe, abordable, qu'elle nécessite peu de planification et de compétences et qu'elle est perçue comme moins susceptible d'être détectée à l'étape de la planification. Les routes qui comportent de longues sections droites dégagées de toute obstruction et un manque de délimitation physique entre les zones réservées aux véhicules et les zones piétonnières (comme les bornes) augmentent la vulnérabilité d'un lieu à une attaque utilisant un véhicule comme arme.

Les attaques de véhicule en tant qu'arme sont souvent la première partie d'une attaque en couches. Ces attaques commencent souvent sur la voie publique avec peu ou pas d'avertissement et peuvent être suivies d'une attaque en maraude utilisant des armes blanches, des armes à feu ou des engins hostiles lancés à la main.

7.1.3. Attaque de véhicules à plusieurs niveaux

Une attaque de véhicule à plusieurs niveaux, également connue sous le nom d'attaque à la voiture complexe, est une combinaison de différents types d'attaques. Les attaques multicouches sont beaucoup plus sophistiquées, nécessitent plus de planification et de ressources et elles sont extrêmement dévastatrices si elles sont menées avec succès.

Dans le cas d'une attaque au véhicule à plusieurs niveaux, un auteur de menace emploiera une combinaison d'au moins deux des tactiques suivantes :

- Faciliter la livraison d'attaquants armés, secrètement ou ouvertement;
- Livraison ou dissimulation d'une VBIED;
- Mener une attaque à l'aide d'un véhicule comme arme, soit comme diversion, soit comme effort principal ; et
- Exécution d'une attaque secondaire visant les premiers intervenants ou les points d'évacuation.

7.2. Exploits

Il existe sept exploits que les auteurs de menaces peuvent utiliser pour contourner les mesures de sécurité opérationnelles ou physiques. Chacun de ces exploits doit être pris en compte lors de l'analyse des vulnérabilités dans le cadre des activités de gestion des risques et des évaluations des menaces. Les sept exploits sont :

- **Garé :** Un véhicule peut être garé légalement ou illégalement à proximité ou à l'intérieur du périmètre d'une installation. Avant une attaque, un véhicule peut être stationné à plusieurs reprises dans le même secteur pour créer une familiarité et peut être abandonné pendant une courte ou une longue période;
- **Empiètement :** Un véhicule peut exploiter les lacunes de la protection du périmètre, traverser lentement ou franchir un périmètre considéré comme sécurisé, ou suivre l'accès légitime du véhicule par un point de contrôle routier à une seule couche;
- **Pénétration :** Un véhicule peut être utilisé à basse ou haute vitesse pour enfreindre les mesures de sécurité. Les attaques à basse vitesse peuvent impliquer une utilisation agressive et répétitive du véhicule contre les mesures de sécurité ou d'autres obstacles pour accéder au site;
- **Tromperie :** Les attaquants peuvent contrefaire ou voler des documents, mentir ou modifier l'apparence de leur véhicule ou d'eux-mêmes pour donner l'impression d'être légitimes. Un « cheval de Troie » est un véhicule modifié pour reproduire un accès légitime. Un « mulet à son insu » est un conducteur légitime qui livre sans le savoir un EEI, des armes ou des agresseurs sur un site;
- **Coercition :** Un conducteur légitime, le personnel de sécurité à un point de contrôle des véhicules ou des employés pourraient être forcés de faciliter l'accès à un site. Ces personnes elles-mêmes, ou d'autres personnes qu'ils connaissent, peuvent être menacés de violence ou soumis à une influence indue par des pressions mentales telles que la corruption ou le chantage;
- **Menace interne :** Une personne ayant un accès légitime facilite ou permet volontairement une attaque en contournant les mesures de sécurité localement ou à distance, en gérant ou en accordant des droits d'accès, ou en interférant avec les mesures de sécurité ; et
- **Sabotage :** Attaque cybernétique ou physique visant à modifier, à affaiblir ou à désactiver une barrière, tout en cherchant à ne laisser aucune trace.

8. Mesures d'atténuation et de protection contre les véhicules hostiles

Lors de la mise en œuvre de mesures d'atténuation et de protection contre les véhicules hostiles, un large éventail de tactiques potentielles peuvent être utilisées, chacune offrant son propre ensemble d'avantages. Le choix de la stratégie la plus appropriée nécessite une évaluation minutieuse du contexte spécifique, en soupesant des facteurs tels que la nature de la menace, l'environnement dans lequel les mesures seront mises en œuvre et l'équilibre entre la sécurité, l'accessibilité et la commodité opérationnelle. En évaluant minutieusement les forces et les faiblesses de chaque option, les spécialistes fonctionnels de la sécurité peuvent s'assurer que les mesures de protection choisies sont à la fois efficaces et proportionnelles aux risques en cause.

8.1. Apaisement de la circulation

La modération de la circulation implique l'utilisation de éléments de conception et de mesures physiques pour réduire la vitesse des véhicules et contrôler la circulation dans les zones identifiées où des mesures de protection contre les ARVH sont requises. Les ralentisseurs, les chicanes, les voies rétrécies, les passages pour piétons surélevés et les revêtements routiers texturés en sont des exemples. En ralentissant la circulation, ces mesures peuvent aider à réduire la probabilité et la gravité des attaques de véhicules hostiles tout en améliorant la sécurité des piétons.

Figure 1 – Exemple de chicane



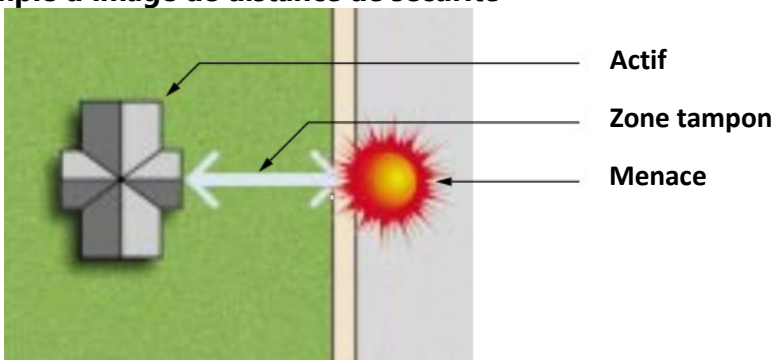
Source: Vue aérienne de la célèbre rue Lombard San : 1538941079 de photos | Shutterstock

Texte de remplacement : La figure 1 représente une vue aérienne de Lombard Street, à San Francisco, illustrant l'utilisation de chicanes.

8.2. Distance de sécurité

La distance de sécurité est l'espace intentionnel maintenu entre un véhicule représentant une menace potentielle et le bien, l'immeuble ou la foule protégés. La zone tampon créée réduit les effets d'un VBIED et donne au personnel de sécurité plus de temps pour détecter, évaluer et répondre aux menaces. Les distances de sécurité peuvent être obtenues grâce à l'aménagement paysager, à des points d'accès contrôlés ou au placement stratégique de barrières. Un examen plus approfondi de l'atténuation des effets d'explosion, y compris la distance de sécurité se trouve dans GSMGC-002 Guide d'atténuation des effets du souffle d'explosion.

Figure 2 – Exemple d'image de distance de sécurité



Source: Guide de protection de la force d'installation de l'armée de l'air américaine

Texte de remplacement : La figure 2 illustre un exemple de distance de sécurité, montrant le bien et la menace séparés par des flèches représentant la distance de sécurité.

8.3. Zones piétonnes protégées

Une zone piétonne protégée est une zone désignée et accessible exclusivement à la circulation piétonnière. Une zone piétonne protégée doit avoir un périmètre physique englobant entièrement l'espace et des barrières classées à un niveau approprié pour empêcher les véhicules hostiles de pénétrer dans la zone protégée. Tous les points d'accès des véhicules à une zone protégée pour les piétons, qu'il s'agisse pour une intervention d'urgence ou pour l'entretien, doivent être contrôlés et sécurisés immédiatement après le passage des véhicules approuvés. Des bornes rétractables ou des barrières résistantes aux chocs peuvent être envisagées pour les points d'accès. Les zones à aménager en tant qu'aires protégées pour les piétons comprennent les zones d'attente pour le transport en commun, les sentiers piétonniers, les zones adjacentes aux entrées et sorties des bâtiments et les zones où la circulation automobile et la circulation piétonnière coexistent.

8.4. Bornes et barrières

Les bornes et les barrières sont des structures de sécurité matérielles fixes ou amovibles conçues pour empêcher l'accès non autorisé des véhicules aux zones protégées. Elles peuvent être faites d'acier, de béton armé ou d'autres matériaux à haute résistance, et peuvent être permanents, rétractables ou temporaires. En plus de leur fonction de sécurité, les bornes peuvent être intégrées à la conception esthétique du site, se fondant dans le mobilier urbain pour maintenir un aménagement accueillant.

Figure 3 : Exemple d'image de bornes rétractables métalliques installées



Source: Borne en acier inoxydable entrant dans une zone piétonne Photo 1409046014 | Shutterstock

Texte de remplacement : La figure 3 représente une rangée de bornes métalliques installées.

Figure 4 : Exemple d'image de bornes rondes en béton installées



Source: Borne en béton ronde en forme de sphère Photo de stock 1929188162 | Shutterstock

Texte de remplacement : La figure 4 représente une rangée de bornes sphériques en béton installées.

Figure 5 : Exemple d'image de barrières de sécurité rétractables pour véhicules



Source: Bornes automatiques Bornes de levage rétractables Enable Photo 1715463778 | Shutterstock

Texte de remplacement : La figure 5 représente des barrières métalliques rétractables pour véhicules en position déployée..

Figure 6 : Exemple d'image de barrières de sécurité temporaires déployables pour véhicules



Source: Barrière de sécurité rétractable rouge Installation d'une 2717133665 photo de stock pour piétons | Shutterstock

Texte de remplacement : La figure 6 représente une barrière pour véhicule mobile ARMIS ONE déployée.

8.5. Points de contrôle des véhicules

Les points de contrôle des véhicules sont des points d'entrée contrôlés où les véhicules sont arrêtés, inspectés et vérifiés avant d'être autorisés à accéder à une zone sécurisée. Ces points de contrôle peuvent inclure le personnel de sécurité, la technologie de balayage des véhicules et les barrières qui peuvent être levées ou abaissées selon les besoins. Les points de contrôle des véhicules peuvent être conçus comme un point d'entrée sécurisé / « sally port » pour fournir une sécurité supplémentaire et empêcher le talonnage. Un point d'entrée sécurisé / « sally port » est une entrée sécurisée comportant deux barrières qui ne s'ouvrent pas en même temps. Un véhicule passerait par la première porte et attendrait qu'elle se referme derrière lui avant que la seconde ne s'ouvre pour permettre l'accès à l'installation. Pour fonctionner correctement, l'espace entre les deux barrières doit être isolé par des barrières pour véhicules afin qu'un véhicule puisse passer les deux portes à tour de rôle pour entrer dans l'installation. Les points de contrôle des véhicules peuvent servir à la fois de mesure dissuasive et de détection, garantissant que seuls les véhicules autorisés peuvent accéder aux zones désignées. Les points de contrôle des véhicules peuvent être installés de façon permanente ou temporaire, selon les besoins.

8.6. Fermetures temporaires

Les fermetures temporaires consistent à restreindre l'accès des véhicules à certaines rues ou zones pendant une période définie, souvent lors d'événements très médiatisés, de niveaux

de menace élevés ou de situations d'urgence. Les fermetures peuvent être imposées à l'aide de barrières temporaires, de personnel de sécurité ou d'une présence policière, et sont particulièrement efficaces pour gérer les risques à court terme sans nécessiter de modifications permanentes des infrastructures. La mise en œuvre de ces fermetures nécessitera une coordination et une autorisation des autorités locales ou du service de police compétent qui gère les routes.

8.7. Aménagement paysager

L'aménagement paysager peut être utilisé de diverses manières dans une stratégie ARVH, soit comme couche complémentaire, soit comme élément de l'application d'une autre mesure de protection. Les mesures de modération de la circulation sont généralement rendues possibles par un aménagement paysager spécialement conçu. Il existe une certaine complémentarité entre les barrières de sécurité et l'aménagement paysager, comme les jardinières testées et évaluées selon les mêmes normes que celles utilisées pour les bornes et les barrières. Les forêts denses ou les arbres de grande taille peuvent être pris en compte lors de l'élaboration d'une stratégie ARVH, offrant un effet d'atténuation similaire à celui des barrières et des bornes. S'ils sont inclus dans une stratégie ARVH, les forêts et les arbres doivent être évalués par un ingénieur pour s'assurer qu'ils offrent le niveau de protection nécessaire. Tout arbre ou forêt utilisé dans le cadre d'une stratégie ARVH devrait se trouver sur la propriété de l'installation, et l'enlèvement des arbres ou des forêts ne devrait être envisagé que si des mesures de protection de remplacement sont mises en œuvre à l'avance. Des talus et des fossés peuvent également être mis en place pour accroître l'efficacité d'autres mesures de protection, comme l'installation d'un fossé devant une clôture résistante aux chocs. Tout aménagement paysager utilisé dans le cadre d'une stratégie ARVH doit être examiné et approuvé par des professionnels qualifiés pour s'assurer que l'aménagement paysager prévu aura l'effet souhaité contre un véhicule hostile.

9. Normes, essais, sélection des produits

Il est recommandé qu'une barrière déployée pour atténuer le risque posé aux biens par les menaces véhiculées soit une « barrière de sécurité des véhicules cotée » qui a subi des essais officiels d'impact de véhicule. Les normes d'essai ne sont pas interchangeables ; si une EMR a permis de déterminer un niveau de protection particulier, il ne faut pas s'en écarter, à moins qu'une analyse supplémentaire ne confirme que d'autres niveaux de performance seraient appropriés pour atténuer le risque à un niveau acceptable. Vous trouverez ci-dessous les normes reconnues en matière d'impact de véhicules qui sont utilisées pour mesurer l'efficacité d'une mesure d'ARVH :

- Organisation internationale de normalisation ISO 22343-1 :2023 Sécurité et résilience — Barrières de sécurité pour véhicules Partie 1 : Exigences de performance, méthode d'essai d'impact de véhicule et évaluation des performances;
- Société américaine pour les essais et les matériaux (ASTM) F 2656 – Méthode d'essai normalisée pour les essais de collision des barrières de sécurité des véhicules; et
- NPSA « Vehicle Attack Delay Standard (VADS) ». « VADS » permet de tester les barrières

de sécurité des véhicules contre les impacts répétés et agressifs de véhicules. Blogue sur les normes ARVH.

Bien que les méthodes de test varient légèrement d'une norme à l'autre, elles évaluent toutes les performances d'une mesure ARVH lors d'un impact précis. Cette condition d'impact est souvent déterminée par le type de véhicule d'impact (comme un véhicule de tourisme ou un véhicule lourd), le poids du véhicule d'impact, la vitesse du véhicule d'impact, l'angle d'impact et la distance de pénétration (comme la distance entre le point d'impact et le point d'immobilisation du véhicule).

10. Détermination des exigences

Lors de l'élaboration des exigences de sauvegarde pour une stratégie ARVH, une attention particulière doit être accordée aux considérations déterminées à la fois par le site, les actifs à protéger et par les types potentiels de véhicules hostiles qui peuvent se manifester comme des menaces. Voici les éléments à prendre en considération :

- Vitesses maximales potentielles (comme la longueur des routes avec un plan direct vers le bien) ;
- Taille du véhicule (p. ex. disponible sur le marché ou personnel) ; et
- Types d'attaques (comme l'utilisation d'un véhicule comme arme, VBIED ou attaques multicouches).

Il existe plusieurs méthodologies pour aider à déterminer les exigences en matière de mesures de protection de l'ARVH. Une EMR est l'approche la plus globale, car elle tient compte du plus large éventail de points de données pour aider à déterminer les exigences appropriées et proportionnelles. Les exigences peuvent également être déterminées en utilisant des évaluations des menaces fondées sur la conception, qui nécessitent moins d'investissement en ressources qu'une EMR, mais qui contiennent à leur tour moins d'éléments de preuve à l'appui de la décision. Une fois que la nature de la menace est comprise, les spécialistes fonctionnels doivent adopter une approche méthodique pour déterminer les exigences du projet et cerner les vulnérabilités. Les facteurs suivants sont jugés utiles pour évaluer le risque à chaque point d'accès :

- **Distance d'approche en ligne droite jusqu'au site :** Les longues approches en ligne droite vers les installations et les terrains de l'événement donnent aux conducteurs hostiles une approche qui leur permet d'accélérer à des vitesses plus élevées, augmentant ainsi la probabilité de franchir des barrières. Les endroits avec de longues approches droites présentent un risque de préjudice plus élevé que les endroits avec des sections courtes ou curvilignes.
- **Largeur de la chaussée :** La largeur de la chaussée influe sur la vitesse des véhicules. Il est plus facile d'atteindre des vitesses plus élevées sur une route à large section transversale (comme une artère à six voies) que sur une route à voies étroites et à stationnement sur rue le long des trottoirs.
- **Limite de vitesse affichée :** La limite de vitesse affichée sur une route est souvent

établie en fonction des caractéristiques de la route telles que la largeur, la présence d'un terre-plein central, le type de surface, les objets en bordure de route et la présence de piétons. La limite de vitesse affichée sur une route est un bon indicateur des vitesses minimales qu'un conducteur hostile peut atteindre sur la route. Les routes où les limites de vitesse affichées sont plus élevées permettront probablement aux conducteurs hostiles de se déplacer à des vitesses d'approche plus élevées vers une entrée.

- **Distance jusqu'à l'intersection signalée :** Les conducteurs hostiles forcés de s'arrêter à une intersection avec signalisation rencontrent des obstacles naturels qui pourraient les empêcher d'accélérer à des vitesses plus élevées à l'approche d'un point d'accès.
- **Distance de sécurité :** La distance de sécurité est la distance disponible entre les mesures de l'ARVH (telles que les bornes et les barrières) et la cible. La distance de sécurité disponible déterminera le type de mesure à utiliser et l'emplacement de son installation.

10.1. Évaluation de la menace et des risques (EMR)

L'EMR est un processus utilisé pour cerner, analyser et traiter les vulnérabilités observées par rapport aux menaces connues ou prévues, afin d'établir l'environnement de risque, et fait partie intégrante de la stratégie globale de gestion des risques d'un ministère ou d'un organisme. La portée et l'application des EMR varient, mais ce processus peut permettre une plus grande efficacité dans la détermination et la résolution des vulnérabilités tout au long d'un projet de construction. Le POSM de la GRC peut fournir des renseignements supplémentaires sur le processus d'EMR dans le document GSMGC-022 (2024) Guide d'évaluation des menaces et des risques ou en communiquant avec RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

10.2. Conception fondée sur les menaces

La conception fondée sur les menaces est un profil du type, de la composition, des capacités, des méthodes, des dommages projetés et/ou de l'intensité d'une menace délibérée, accidentelle ou naturelle sur laquelle reposent l'ingénierie et les opérations de sécurité d'une installation. Cela est fondé sur les principes présentés dans GSMGC-014 Considérations relatives à la sécurité matérielle dans la conception des installations. La conception fondée sur les menaces vise à éliminer ou à réduire l'impact des menaces exploitant les vulnérabilités dans la conception ou l'emplacement d'une installation; par conséquent, les deux devraient être utilisés en tandem. Les étapes de la conception axée sur les menaces sont les suivantes :

10.2.1. Évaluation des menaces

La phase d'évaluation des menaces de la conception fondée sur les menaces exige la collecte de tous les renseignements pertinents pour une évaluation préliminaire des menaces nécessitant des mesures d'atténuation intégrées à la conception d'un bâtiment, d'une installation ou d'un espace. Les renseignements recueillis au cours d'une EMR peuvent être inclus dans cette phase, car ils appuient le même objectif.

10.2.2. Collecte de renseignements

Le processus de collecte de renseignements vise à déterminer et à énumérer les menaces potentielles pour l'installation proposée. Souvent identifiées lors d'une EMR, ces renseignements peuvent inclure la motivation de la menace, l'intention, la capacité et les événements historiques. Il faut consulter des sources d'information fiables, notamment les organismes de renseignement et d'application de la loi, les ministères et organismes gouvernementaux, les rapports d'incident, ainsi que les EMR historiques et actuelles et d'autres évaluations des risques pertinentes. La crédibilité de l'information et de sa source devrait être évaluée de la même manière qu'une EMR. La collecte de renseignements devrait être une activité continue tout au long du cycle de vie d'une stratégie de conception fondée sur les menaces afin de confirmer que l'information demeure pertinente et reflète les données les plus à jour.

10.2.3. Analyse préliminaire

Les renseignements obtenus sont ensuite analysés pour documenter les motifs, les intentions et les capacités crédibles des menaces potentielles. L'analyse devrait porter une attention particulière aux menaces potentielles qui sont pertinentes et pertinentes au regard du mandat du ministère ou de l'organisme et à l'emplacement de l'installation. L'objectif de cette phase est de fournir une évaluation crédible des menaces potentielles, y compris la composition, la motivation, l'intention et les capacités.

Les caractéristiques suivantes de chaque menace doivent être prises en compte dans l'analyse; toutefois, il se peut qu'il n'y ait pas de données disponibles en raison du manque d'information ou du manque d'information crédible pour chaque menace :

- Motivation;
- Intentions;
- Outils;
- Compétences techniques;
- Compétences en cybersécurité;
- Connaissances;
- Financement;
- Menace interne;
- Tactiques;
- Complexité;
- Fréquence des événements historiques; et
- Attractivité de la cible.

Le produit de cette phase est un document d'évaluation des menaces qui décrit l'environnement des menaces et toutes les menaces connues à prendre en considération. Comme il a été mentionné précédemment, l'information provenant d'une EMR peut être utilisée dans l'élaboration du document de conception fondée sur les menaces.

10.2.4. Analyse secondaire

Le document d'évaluation des menaces est ensuite analysé en fonction des attributs

disponibles. La pertinence de chaque menace peut être déterminée en fonction de la motivation, de l'intention et de la capacité de nuire. Les menaces plus pertinentes devraient être considérées comme plus probables que les menaces jugées moins pertinentes. Les menaces ayant des caractéristiques similaires peuvent être regroupées en types de menaces définis en fonction de caractéristiques communes. Dans le cadre de ces types de menaces plus larges, d'autres considérations peuvent inclure des facteurs propres au site et à l'activité, tels que les procédures opérationnelles, l'emplacement et l'accessibilité de l'installation, ainsi que les modes ou itinéraires de transport vers et depuis le site. Les renseignements analysés sont ensuite compilés dans un document donnant un aperçu de la menace, ainsi que de ses attributs, caractéristiques et probabilités liées à l'installation. Les résultats de ce document ainsi que de l'EMR peuvent être utilisés pour élaborer la stratégie ARVH pour l'installation.

11. Cycle de vie du projet d'atténuation des véhicules hostiles

Chaque mesure de protection devrait avoir un plan de gestion du cycle de vie qui couvre tout, de l'approvisionnement à la mise hors service ou au remplacement.

11.1. Conception

Une stratégie ARVH doit être élaborée avant son installation. La mise en œuvre des exigences en matière de sécurité physique dans un projet dès les premières étapes peut réduire les coûts et garantir que les instructions permanentes d'opérations (IPO) sont élaborées conjointement avec les mesures de protection ARVH supplémentaires. Il est important d'inclure les données recueillies dans les EMR initiale à ce stade du projet pour s'assurer que la stratégie ARVH répond aux menaces particulières auxquelles l'installation est confrontée.

Il est essentiel de comprendre les capacités et les limites des produits et des stratégies individuels avant de les acheter. Il s'agit notamment de s'assurer qu'ils sont installés correctement pour maximiser la résistance aux véhicules et que les produits offrent le niveau de protection pour lequel ils sont certifiés.

11.2. Construction

Une fois qu'une stratégie ARVH est terminée, il est important de s'assurer qu'elle est installée conformément aux spécifications, car cela maximisera la résistance aux véhicules. Un dispositif de protection mal conçu ou mal installé peut créer des vulnérabilités qui empêchent le dispositif de protection de fonctionner comme prévu. Lors de l'installation, il faut faire preuve de prudence et d'attention pour s'assurer que les produits sont installés conformément aux instructions du fabricant. Il est recommandé que les spécialistes fonctionnels de la sécurité matérielle et les experts en la matière, qui connaissent bien les exigences de construction, évaluent périodiquement le processus d'installation pour

s'assurer qu'il est conforme aux exigences d'installation, ainsi qu'aux normes et exigences municipales, provinciales, territoriales et fédérales applicables.

11.3. Opérer

Lorsque les dispositifs de protection ARVH sont installés, il est important de bien les entretenir. Un équipement mal entretenu entraînera inévitablement des défaillances ou une dégradation, ce qui augmentera la probabilité d'un incident ou entraînera des coûts plus élevés en raison du remplacement. Cela pourrait également avoir une incidence sur les opérations de sécurité de l'installation, créant des vulnérabilités qui peuvent être exploitées par un véhicule hostile.

11.4. Remplacement/mise hors service

Un plan doit être mis en place pour le remplacement ou la mise hors service de chaque mesure de protection. Il peut s'agir de facteurs tels que la durée de vie prévue de l'équipement avant de son remplacement. Les conditions à prendre en compte comprennent la fréquence d'utilisation, les conditions météorologiques et la fréquence de l'entretien préventif. Tout contrat connexe doit également être pris en compte, comme les contrats d'entretien ou la location d'équipement de sécurité privée.

12. Prévention du crime par l'aménagement du milieu

La prévention du crime par l'aménagement du milieu (PCAM) est une approche multidisciplinaire de la prévention du crime pendant la planification, l'aménagement et la conception de la sécurité d'un environnement qui est complémentaire à GSMGC-019 – Guide de Protection, Détection, Réponse, et Récupération. La conception et la gestion des environnements naturels et artificiels des installations peuvent permettre aux ministères et aux organismes de dissuader les actions criminelles ou hostiles tout en gérant en toute sécurité les mouvements de personnes dans une installation. Ces principes visent à influencer positivement les comportements et les activités tout en décourageant les actions indésirables du personnel, des visiteurs et des acteurs de menaces potentiels.

13. Références et documents sources

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale
- Directive sur l'obligation de prendre des mesures d'adaptation
- Guide à l'intention des employé.e.s deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale
- Mesures d'atténuation contre les véhicules hostiles de l'Ontario Traffic Council (janvier 2023)

- Guide de protection de la force d’installation de l’armée de l’air américaine
- GSMGC-002 Guide d'atténuation des effets du souffle d'explosion
- GSMGC-019 Guide de Protection, Détection, Réponse, et Récupération
- GSMGC-014 Considérations relatives à la sécurité matérielle dans la conception des installations
- Menace fondée sur la conception
- GSMGC-022 Guide d'évaluation des menaces et des risques
- ARVH - Résistant aux chocs | NPSA

14. Promulgation

Révisé et recommandé pour approbation

J'ai examiné le document GSMGC-025 (2026) – Fondement de l'atténuation des risques liés aux véhicules hostiles, et j'en recommande l'approbation.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2026.10.22 09:52:06 -04'00'

Shawn Nattress, Date
Gestionnaire
GRC, Principal organisme responsable de la sécurité

Approbation

J'approuve par la présente le document GSMGC-025 (2026) – Fondement de l'atténuation des risques liés aux véhicules hostiles.

Bissonnette,Philippe Yvon,000133440

Bissonnette,Philippe Yvon,000133440
2026.10.22 10:00:59 -04'00'

Philippe Bissonnette, Date
(I) Directeur, Sécurité matérielle
Gendarmerie royale du Canada