Systèmes de sûreté intégrés.

Systèmes de sûreté intégrés.

Une installation de sûreté n’est pas la même chose qu’une installation électrique générale construite selon les nécessités et les normes. Ce travail a vu le jour, entre autres, après des décennies de voir le manque de bon sens dans les réalisations!

Robert Verhulst

Robert Verhulst

ISBN: 9789464802894

.

Je souhaite remercier pour l'acquisition de photos :
HTC parking & security bv Pays-Bas
Dormakaba Belgique
Idemia France
Proton Data USA
Axis communications Suède
Boon Edam bv Pays-Bas
CDVI France

Pour toute question sur ce livre:

info@rcms.expert

www.rcms.expert

L’objectif de cet ouvrage est de guider toute personne impliquée dans la conception d’un système de sûreté intégré innovant et de l’amener à une nouvelle ère en terme de technologie.

L’œuvre contient treize chapitres :

I. Concepts généraux.
II. Sûreté intégrée.
III. Contrôle d’accès.
IV. Audio et vidéo.
V. Autres moyens.
VI. Surveillance à distance
VII. Entretien et ajustements
VIII. Cybersécurité
IX. Des renseignements généraux matériaux.
X. Questionnaire.
XI. Conception.
XII. Durabilité économique
XIII. Renseignements généraux et normes

Robert Verhulst

Révision 22.0. Juin 2024

Remarque : Cet ouvrage met régulièrement en garde contre la protection des réglementations légales en matière de sécurité privée (RGPD), mais cet ouvrage ne fournit pas d'orientation sur ces réglementations légales.

Sécurité intégrée ?

Définition:

Tous les éléments, logiciels, matériels, organisation qui forment un tout pour un système de sécurité où tous ces éléments forment la connexion nécessaire à une solution de sécurité totale.

Ce que ce n'est pas :

Atteindre cet objectif ne signifie pas nécessairement un système central avec une surveillance centralisée.

Créez une matrice de dépendances pour obtenir la solution la plus adaptée à cela.

I. Concepts généraux

Sûreté ou sécurité ?

Dans la langue française, on parle, en général, de la sûreté. Toutefois, il existe une très grande distinction en termes de sécurité entre les secteurs suivants:

Secteur de la sécurité humaine :
- Sécurité incendie –
- Catastrophe naturelles
- Accident du travail
- Urgence
- Émeutes

Secteur de la protection des personnes et des valeurs, ou le terme exact est sûreté :
- Vols
- Contrôle d'accès
- Espionnage
- Sabotage
- Toute forme d'agression
- Cybersécurité
- Couverture générale et observation
- Détection des incendies

Avec les secteurs donnés ci-dessus en exemple, je tente surtout de couvrir la sûreté contre la malveillance. Il est clair que, dans le secteur de la sûreté, le danger imprévu ou incalculable joue un rôle important.

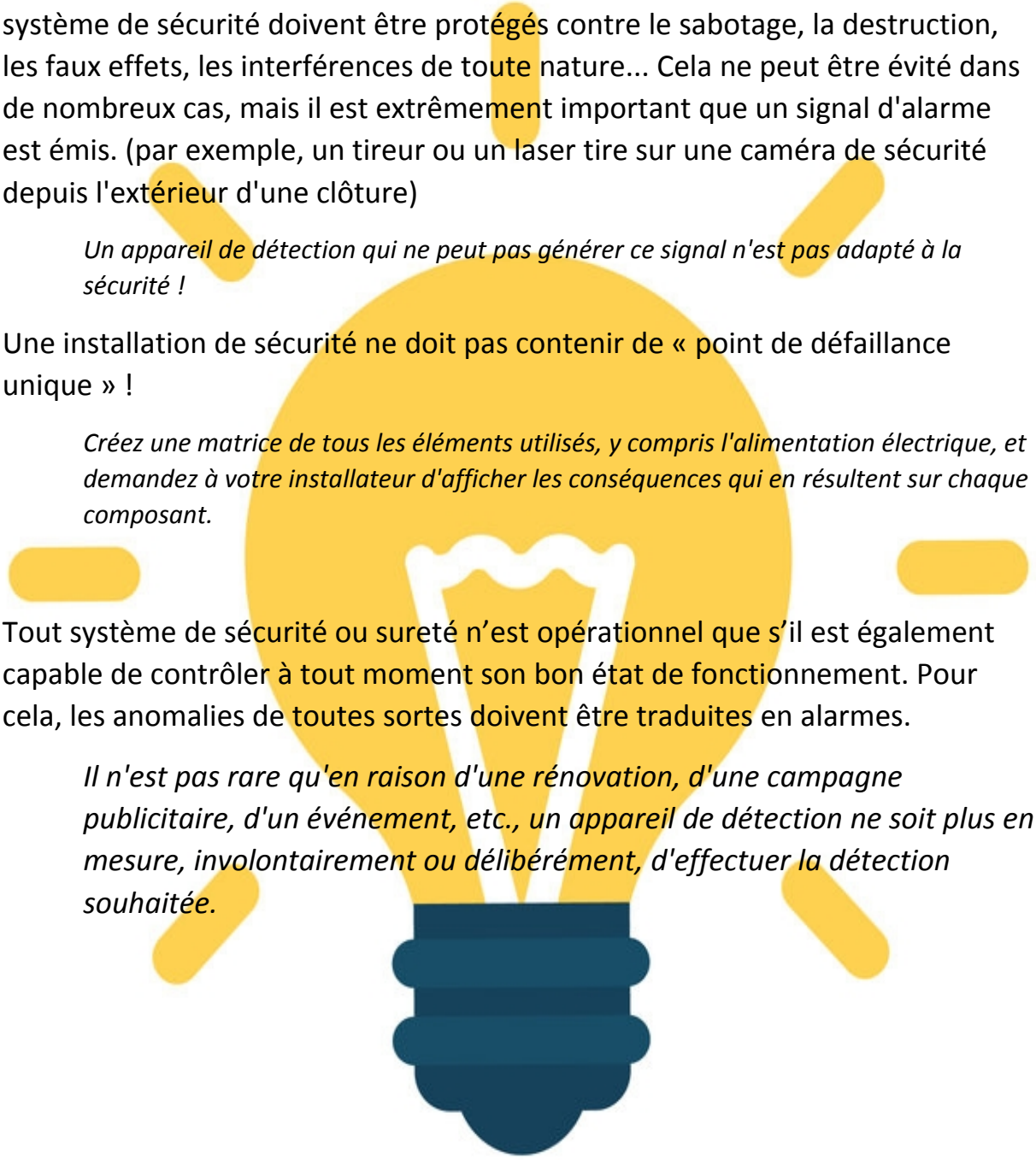
Trois points caractérises un système de sécurité :

Capteurs, caméras, sous-stations, ... tous les éléments qui font partie d'un système de sécurité doivent être protégés contre le sabotage, la destruction, les faux effets, les interférences de toute nature... Cela ne peut être évité dans de nombreux cas, mais il est extrêmement important que un signal d'alarme est émis. (par exemple, un tireur ou un laser tire sur une caméra de sécurité depuis l'extérieur d'une clôture)

> *Un appareil de détection qui ne peut pas générer ce signal n'est pas adapté à la sécurité !*

Une installation de sécurité ne doit pas contenir de « point de défaillance unique » !

> *Créez une matrice de tous les éléments utilisés, y compris l'alimentation électrique, et demandez à votre installateur d'afficher les conséquences qui en résultent sur chaque composant.*



Tout système de sécurité ou sureté n'est opérationnel que s'il est également capable de contrôler à tout moment son bon état de fonctionnement. Pour cela, les anomalies de toutes sortes doivent être traduites en alarmes.

> *Il n'est pas rare qu'en raison d'une rénovation, d'une campagne publicitaire, d'un événement, etc., un appareil de détection ne soit plus en mesure, involontairement ou délibérément, d'effectuer la détection souhaitée.*

Identifiant ?

Dans ce travail, on parle généralement d'identifiant quand on entend un moyen utilisé pour identifier une personne. Selon l'installation, il peut s'agir d'un badge, d'une étiquette, d'une clé électronique, d'un smartphone,...

Surveillance:

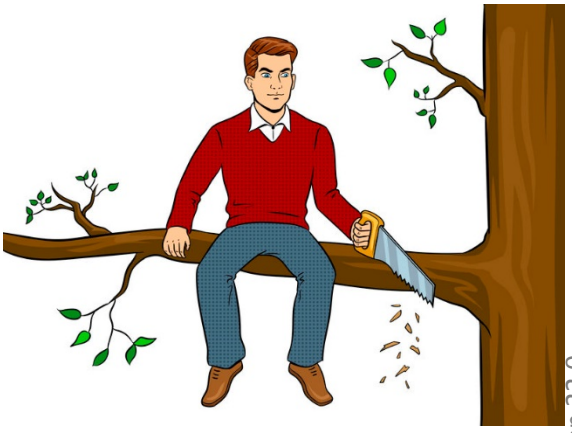
En utilisant le mot surveillance, je souhaite attirer l'attention sur une forme d'observation et de contrôle complets. Il ne s'agit pas seulement d'une alarme et d'une action, mais aussi de suivre une évolution de manière proactive, d'éviter un danger imminent et de prendre les mesures nécessaires. Cette surveillance ne peut être effectuée que par les personnes ayant une connaissance de la situation, car elle suivent jour après jour l'activité dans le domaine et ont une connaissance du passé. La surveillance à distance se limite fréquemment dans le suivi d'instructions prédéterminées et le suivi des alarmes après les faits. Elle est généralement faite par des personnes ayant peu d'affinité avec la dynamique des évènements. Dans le cas d'une surveillance sur place ou locale, le surveillant a une connaissance de l'événement et de l'environnement grâce à laquelle il peut mieux évaluer la détection et prendre des décisions proactives, tandis que la surveillance à distance devient post-événement, avec peu de connaissance de ce qui se passe sur le site et occasionnera toujours des dommages plus importants.

Indépendance:

La surveillance d'un sujet ou d'un domaine doit être indépendante de son propre fonctionnement.

Voici quelques cas qui illustrent ce principe:

- Un centre informatique est surveillé avec un certain nombre de caméras et de capteurs. Une grave erreur est de fournir l'alimentation électrique ininterrompue ou le logiciel de la surveillance dans cette même salle. En effet, une attaque pour saboter le centre informatique va



également arrêter le système de sûreté et laisser le client sans aucune preuve et sans aucun autre contrôle!

- Une caméra observe un générateur d'énergie d'urgence, mais dépend du générateur pour son alimentation.

- Un réseau doit être indépendant et géré par les services de sûreté. L'utilisation de VLAN sur un réseau existant n'est pas autorisée, car le câble physique et l'équipement sont toujours accessibles par d'autres et ne répondent pas aux mêmes exigences de sûreté.

- Une caméra d'observation est alimentée sur une prise locale, d'autres appareils tels qu'un réfrigérateur qui montre un défaut ou provoque une fuite de terre va désactiver la caméra.

Bunker?

L'endroit où les décisions de sûreté sont prises en temps réel doit être logé dans un endroit sûr et bien protégé. Une attaque sera généralement dirigée directement vers la cible et, dans ces circonstances, la sûreté doit rester en opération. Si une attaque est menée simultanément ou à l'avance contre une surveillance de sûreté, elle doit être suffisamment renforcée pour permettre un temps d'intervention externe.

Concrètement, le système central et le contrôle doivent être dans un endroit sûr qui est protégé par des moyens physiques, du contrôle d'accès et invisible de l'extérieur. Trop souvent, un gardien est considéré comme un travail de portier de nuit.

L'Internet!

La communication Internet est désormais indispensable et, dans la plupart des endroits, une très haute fiabilité peut être atteinte. Pourtant, en cas de danger comme la guerre et le terrorisme, c'est le moyen de sabotage le plus recherché !

Wifi!

Le WiFi est aujourd'hui un moyen de communication sans fil couramment utilisé. Généralement connecté à Internet, on peut communiquer en audio et vidéo presque partout dans le monde. La communication s'effectue dans la bande 2,4 GHz ou 5 GHz. Lorsqu'il y a une connexion à Internet, tous les dangers de la cybersécurité sont également présents. Cependant, la communication est assez facilement rendue inutilisable par l'utilisation d'un brouilleur. Cependant, le WiFi peut également être utilisé de manière totalement privée dans le cadre d'un réseau OT.

En anglais un brouilleur de ce type est appelé : jammer..

Dans les limites de sûreté :

Un système intégré a généralement de nombreuses connexions avec d'autres techniques. Toutefois, un opérateur ne doit pas être distrait par les événements non-liés à la sûreté. Bien sûr, une situation sécuritaire critique peut se trouver derrière toute mission non sécuritaire. Les conditions techniques critiques qui ne sont pas directement liées à la sûreté peuvent être signalées et transmises à d'autres personnes compétentes, mais cette exception doit constituer une intervention courte et doit être limitée. Ce n'est pas non plus le travail de l'agent de sûreté d'ajuster la température d'une pièce, mais une fuite d'eau peut présenter un risque pour la sûreté.

Faire une distinction entre la sûreté et la non-sûreté, éviter les constructions compliquées telles que PSIM (Physical Security Information Management) dans laquelle la surveillance et le contrôle technique ont également lieu. BCS (Building Control Systems) est un must pour les systèmes complexes, mais nécessite des compétences différentes et peut facilement être contrôlés à distance.

Clés:

Malgré toutes les nouvelles technologies, les clés physiques n'ont toujours pas disparu. Selon la taille d'un site, il y a parfois des milliers de clés physiques inutilisées, mais elles fournissent un accès malgré le contrôle d'accès électronique. Les clés physiques et les passe-partouts peuvent être recréés assez facilement et constituer une menace supplémentaire. (Ce n'est pas parce qu'un serrurier honnête fait faire une clé chez le fabricant qu'un cambrioleur ne peut pas également le faire) Attention : souvent une clé avec un accès plus faible peut être ajustée en perçant et/ou en limant pour obtenir un accès plus élevé !

Un souci majeur concerne les clés des armoires techniques qui sont généralement universelles! Gardez à l'esprit que le contact d'ouverture de l'armoire provoquera une alarme, mais ne pourra pas éviter un sabotage.

Un contact anti-sabotage est un interrupteur électrique placé à l'intérieur de l'armoire de sûreté pour signaler un accès par une alarme.

Câblage en général :

Le facteur 1 est la violabilité, un câble endommagé ou coupé aura sans doute pour conséquence de désactiver une partie de la sécurité. Une installation effectuée dans les règles de l'art signalera l'erreur, mais une partie de l'installation est et reste hors de contrôle !

Le câblage périphérique ou le câblage entre le capteur et l'unité de commande locale prend de nombreuses formes et nécessite sans exception un message d'alarme en cas de dysfonctionnement ou d'interruption !

Le câblage réseau entre les unités centrales et les contrôleurs locaux n'est jamais réalisé autrement qu'avec un réseau bien conçu avec PoE. Ce réseau consiste en une communication Ethernet TCP/IP avec communication cryptée et contrôle du tronc entre le commutateur Ethernet et le périphérique edge. Idéalement, une bande passante suffisante devrait être fournie pour permettre l'audio. Il est préférable de prévoir un réseau redondant tel qu'un câblage en boucle entre les commutateurs et les unités centrales.

Armoires à clés :

De nombreuses institutions, après avoir recherché quotidiennement la clé appropriée en possession de qui , décident d'acheter une armoire à clés. Cette étape a une grande utilité, avec une bonne gestion, vous pouvez trouver la clé, mais la sécurité et le coût de la gestion sont un facteur négatif important qui ne doit pas être sous-estimé.

Deux formes courantes :
- Armoire ordinaire avec clé où l'on retrouve l'emplacement de la clé avec des étiquettes, l'absence de clé indique que quelqu'un l'a prise. Une telle armoire nécessite une gestion minimale de la part d'un responsable qui possède la porte de l'armoire et qui tient un journal indiquant qui prend quoi et quand la clé sera restituée. Des gains d'efficacité peuvent être envisagés entre la facilité de trouver la bonne clé et une sécurité limitée. Il s'agit généralement d'un formulaire qui peut être bien utilisé pour un plus petit nombre de clés. Cependant, il existe des situations où des centaines de clés sont conservées et sept administrateurs sont employés pour gérer la salle des clés avec un minimum de deux personnes 24 heures sur 24 !
-Armoire presque similaire avec contrôle électronique. Cette armoire s'ouvre à l'aide d'un outil d'identification tel qu'un badge, un tag ou un smartphone. Cette identification donne accès à l'armoire et à un certain nombre de clés pouvant être retirées du système de serrure. Lorsque la ou les clés sont retirées, des informations chronologiques sont stockées sur la personne qui a obtenu l'accès et les clés qu'elle a emportées avec elle. Sans doute une sécurité supérieure mais un investissement coûteux qui ne résout pas le problème de la copie et du vol des clés, besoin d'une gestion et des moyens d'identification.

Conclusion : les clés mécaniques ne sont jamais sûres et limitent l'efficacité sur le lieu de travail.

Ou utilisez-vous une clé traditionnelle… ou utilisez-vous une clé électronique ?

L'utilisateur se verra accorder un accès inconditionnel sans identifier la bonne personne !

Avantage avec les clés électroniques : l'accès peut être désactivé sans remplacer la serrure.

Ancienneté:

La durée de vie des dispositifs de sûreté physiques est longue. Parcontre, ce n'est pas le cas des produits électroniques. Comme l'évolution des clés au cours du siècle dernier, la technologie de sûreté a pris des mesures pour se protéger contre les nouveaux défis en ligne avec l'évolution de la technologie informatique. En général, on peut dire qu'une installation vieille de 20 ans ne répond plus aux attentes actuelles en termes de sûreté et d'efficacité.

Préparation:

Une installation à la fine pointe de la technologie fonctionne de manière invisible pour superviser le bon fonctionnement de tous les composants de l'installation. Dans le passé, un bon détecteur infrarouge passif était souvent considéré comme de haute qualité parce qu'il n'avait jamais causé d'alarme! Dans la technologie actuelle, chaque capteur ou contrôle doit être connecté à un réseau et fournir suffisamment d'informations pour assurer sa sensibilité et son but . Assurez-vous que les images de la caméra sont visionnées régulièrement ! Une panne de caméra ou une mauvaise image ne mènera qu'à la frustration après avoir vérifié les faits.

Débarrassez-vous du détecteur PIR:

Les détecteurs PIR utilisés pour la détection de mouvement sont à la fin de leur vie, car les caméras peuvent effectuer une bien meilleure détection et en fournir des preuves. Un PIR peut être placé hors de direction ou saboté avec un spray. Une caméra ne peut-être saboter par cause d'analyse d'image interne et la communication constante. En outre, un PIR nécessite une alimentation pendant que la caméra est alimentée le long de PoE. En général, une détection ne doit plus donner d'alarme sans avoir la preuve de l'origine de l'alarme. Utilisez un tel détecteur pour allumer automatiquement la lumière, mais certainement pas comme capteur à des fins de sécurité.

Lois et règlementations :

Au cours des dernières décennies sont apparus de nouveaux règlements, normes, lois, ordonnances,... ne facilitent pas toujours l'affaire. Pire encore, il s'agit de mesure injustifié pour être considéré comme conforme à un sujet a protéger. Toutefois, ces règlements devraient être considérés comme le fondement d'un système de sûreté et non comme une fin en soi. Les instituts de sûreté nationale Français, Allemands et Anglais parlent d'une manière moderne de « guides », « guidelines», « richtlinien » dans les documents publiés.
Les lois et les normes sont élaborées sous l'influence des industriels et des lobbies et ont souvent pour conséquence qu'elles ne sont plus réfléchies mais mises en œuvre. Pire encore, la tendance actuelle est d'inspecter selon la norme plutôt que selon l'opération !

Dans mes études de conseil personnel, il ne se passe pas un mois sans que je sois confronté à des situations absurdes où la sécurité est limitée par des réglementations légales.

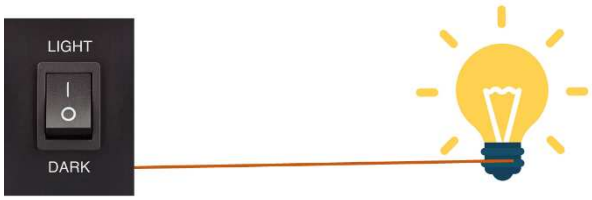
Alimentations:

Pour chaque appareil un besoin d'alimentation doit être établi, une table et une détermination de l'autonomie de chaque appareil. Il faut découvrir quels sont les facteurs dont dépend l'alimentation générale et quelles fuites de terre peuvent causer une rupture. Les documents tel que construit (AS BUILT) doivent contenir un schéma à fil unique des connexions électriques pour toutes les connexions dans le système de l'arrivée électrique à chaque appareil. Les alimentations à basse tension des appareils doivent avoir une autonomie équilibrée.

Préservation de fonction et contrôle de fonction :

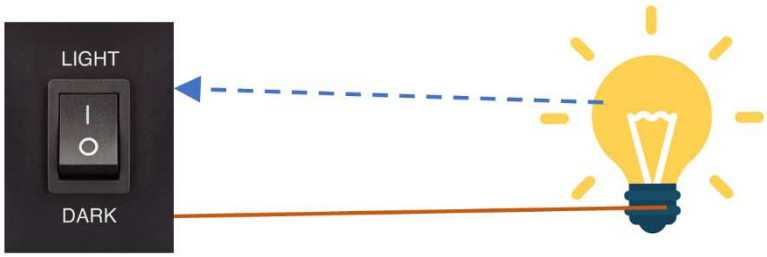
Contrairement aux installations électriques, une installation de sécurité doit être construite avec une intégrité fonctionnelle. De simples erreurs ne doivent s perturber le fonctionnement ultérieur d'un système de sécurité.

L'interrupteur d'installation d'éclairage contrôle la lampe sans contrôle du fonctionnement:



Technique de sureté :

L'interrupteur de contrôle de fonction contrôle la lampe mais la lumière résultante est vérifiée comme confirmation:



La conservation des fonctions est garantie par un câblage en boucle ou un

câblage redondant:

Les principes ci-dessus sont une première étape, mais pour de nombreuses applications et certainement pour le feu, il est également nécessaire de déterminer ce qui peut être perdu en fonctionnalité avec une seule erreur.

Intervention, évacuation, rétention:

Ces trois concepts sont liés les uns aux autres et chacun a un modèle d'exécution. Un programme de mise en œuvre et des connexions déterminés à l'avance doivent être élaborés à cet effet. Cela nécessite une observation et une maîtrise claires de la part d'un centre opérationnel.

Intervention en générale :

Dans cet article, je fais réfléchir l'expert en sécurité sur la sécurité et l'aspect sécuritaire de l'intervention en aveugle. Depuis de nombreuses années, il est possible qu'un système d'alarme déclenche une intervention directement ou indirectement sans qu'il y ait le moindre indice du danger pour l'équipe d'intervention et pour les personnes concernées ! Cette situation inimaginable ne peut être comprise que dans le cas de la sécurité des personnes et des biens, avec l'incendie comme exemple.

Conclusion : une intervention ne doit pas avoir lieu sans avoir pu identifier l'urgence avec des images, des sons ou d'autres informations détaillées qui reflètent la nature de l'urgence.

Intervention:

-Doit toujours être faite selon le plan et selon les informations relatives aux faits.

-Le centre opérationnel de sûreté, inaccessible, ne doit jamais être abandonné, sauf lorsqu'il est lui-même compromis (par exemple, incendie)

-La première intervention consiste à utiliser tous les moyens possibles télécommandés pour remédier à la situation du centre opérationnel, pour sécuriser les personnes et les ressources.

-La deuxième phase de l'intervention consiste à donner aux personnes présentes pour mener des opérations de protection. (personnel ayant une connaissance des risques et des connaissances sur le site) -La troisième phase consiste à demander un renforcement professionnel externe avec des connaissances limitées sur les risques locaux et les infrastructures. Il est important de procéder à une évaluation immédiate de la capacité extérieure d'urgence et du temps.

Quelques facteurs qui devraient être pris en compte:

1. Le parcours de l'intervenant au lieu d'intervention en tenant compte du temps d'action et des obstacles en cours de route. Veuillez noter qu'en cas d'attaque, le harceleur ne peut pas laisser la route libre et va très probablement la compliquer!
2. L'accès au site est-il possible au moment de l'intervention, (accès qui permet d'atteindre l'objectif).
3. L'orientation d'un centre de connaissances au courant du site est-elle possible pendant l'intervention?
4. L'attaque a peut-être eu lieu le long d'un passage inaccessible par l'équipe d'intervention. (p. ex. toit)
5. L'attaquant ayant connaissance du site peut planifier le chemin du retour du site autre que son chemin d'entrée.
6. L'équipe du centre de sûreté ne peut jamais participer physiquement à l'intervention et doit assurer une communication d'assistance.