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: 9789464485783

.

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

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 six 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. Renseignements généraux et normes

Robert Verhulst

Révision 11.0. Janvier 2022

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.

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.

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.

Certaines institutions disposent d'un logiciel de gestion des clés, d'un système ou d'un fonctionnaire. Souvent, la clé est liée à un porte-clés électronique avec détection de clé dans une armoire ! Une nouvelle approche basée sur les nouvelles technologies peut conduire à un retour sur investissement important avec une sûreté accrue.

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 et changé à distance.

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 .

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.

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.

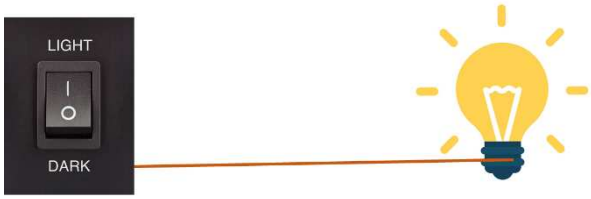
Alimentations:

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 :

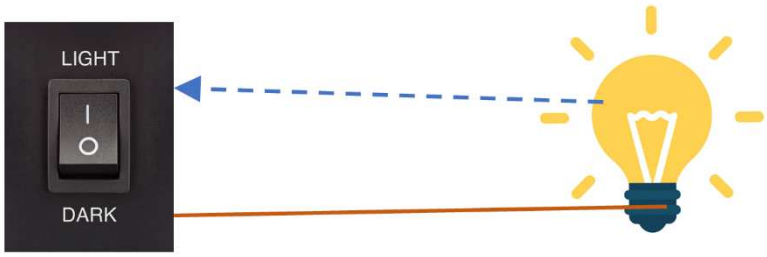
Contrairement aux installations électriques, une installation de sécurité doit être construite avec une intégrité fonctionnelle. De simples erreurs ne doivent s perturber le fonctionnement ultérieur d'un système de sécurité.

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:

-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.