CICS
Conseil des Industries
de la Confiance et de la Sécurité

Cofis

GUIDE POUR LA PROTECTION DES SITES SEVESO ET SITES INDUSTRIELS SENSIBLES

PRÉFACE

ÉDITO

Le Préfet PASCAL BOLOT,

Directeur de la protection et de la sécurité de l'Etat,
SGDSN.

Qu'il s'agisse de points d'importance vitale, d'établissements industriels classés Seveso ou d'établissements accueillant du public, les sites sensibles sont des cibles potentielles d'actes malveillants.

Chargé de concevoir et de mettre en œuvre les politiques interministérielles de réduction des risques, le Secrétariat Général de la Défense et de la Sécurité Nationale s'attache à associer l'ensemble des acteurs publics et privés, de l'identification des menaces à l'élaboration des réponses adaptées. En tenant compte des réalités économiques, il veille aussi à promouvoir la filière des industries de la sécurité et à porter les conceptions françaises au sein de l'Union européenne.

Le renforcement de la sécurité des sites sensibles repose ainsi sur un partage des efforts entre l'Etat et les opérateurs pour consolider la culture de la sécurité, tant sur le plan humain que technologique, et pour renforcer le cercle vertueux de la confiance.

Pour la sécurité des sites industriels classés Seveso, le SGDSN a reçu mandat du Premier ministre, en 2015, après les événements de Saint-Quentin Fallavier et de Berre-L'Etang, pour coordonner les travaux interministériels.

C'est dans ce cadre que, parmi les axes d'efforts déployés, j'ai souhaité que le CoFIS puisse proposer une méthodologie d'analyse du besoin capacitaire et une offre spécifique de solutions de sécurité qui puissent être utiles aux exploitants des sites Seveso.

La publication de ce guide, réalisé par le CICS pour le compte du CoFIS, en lien avec le ministère de la transition écologique et solidaire, est l'aboutissement de ces travaux. C'est un outil qui contribue à l'effort commun pour trouver des solutions raisonnées et raisonnable face à la malveillance.

TÉMOIGNAGE

« L'UIC remercie le CICS pour avoir rédigé dans un document, de qualité et pédagogique, les démarches à suivre et les solutions proposées par les entreprises de la sureté. L'UIC remercie le CICS pour nous avoir sollicités afin d'intégrer la plupart de nos remarques »

Philippe PRUDHON
Directeur du département technique
de l'Union des Industries Chimiques

ÉDITO

MARC DARMON

Président du Conseil des industries de la confiance et de la sécurité

La protection des sites industriels face à la malveillance et au terrorisme constitue une préoccupation grandissante.

Les opérateurs SEVESO sont donc amenés à non seulement assurer la sécurité industrielle (au sens risque industriel) mais aussi la sureté de leurs sites (au sens malveillance). Le comité de la filière des industries de sécurité (CoFIS) qui réunit les pouvoirs publics, les utilisateurs et les industriels de la sécurité, a lancé une action pilote pour répondre au mieux à ce besoin émergent. Le conseil des industries de sécurité industrie de sécurité (CICS) qui a vocation à rassembler toute l'offre française, y a contribué par une étude capacitaire et industrielle, conduite en coopération avec les associations professionnelles, l'Etat et le pôle Safe, et qui se concrétise par le présent guide.

Notre objectif est de faciliter la démarche des opérateurs avec une méthodologie claire et l'accès à la plateforme des acteurs de confiance de la filière. Nous avons aussi le souci d'apporter des réponses adaptées et évolutives à travers une démarche d'ensemble et capacitaire, car aucune technologie ne peut jouer, à elle seule, le rôle de système de sécurité.

Le CICS démontre par cette action concrète son engagement à développer le dialogue de confiance entre l'offre et la demande de sécurité que vise le CoFIS, dans ce domaine comme pour l'ensemble des missions de sécurité publiques comme privées. Je remercie l'ensemble des acteurs associés à la réalisation de ce guide pour leur écoute, leurs conseils et leur confiance.

SOMMAIRE

INTRODUCTION

UN NOUVEL IMPÉRATIF POUR LES SITES

La dangerosité de certains procédés industriels manipulant des matières dangereuses a de longue date conduit à mettre en place un cadre très strict permettant d'en réduire les risques sur le plan de la maitrise des installations et des opérations vis à vis des pannes, accidents (sureté de fonctionnement). Les directives SEVESO imposent un haut niveau de prévention aux sites industriels présentant des risques d'accidents majeurs.

Le focus est bien la maitrise des processus et des opérations du point de vue des risques de défaillances techniques et humaines et de situations accidentelles, où l'erreur opératoire est étudiée mais pas les actes de malveillance. La responsabilité des opérateurs est ainsi complète s'agissant de maîtrise de la sécurité de fonctionnement pour ne pas atteindre à la sécurité des personnes.

S'agissant des risques liés à la malveillance, l'apparition plus récente des menaces n'a pas encore conduit à un cadre aussi exigeant. Les obligations légales fortes ne concernent que les activités d'importance vitale (ces activités soit ont trait, de manière difficilement substituable ou remplaçable à la production ou distribution de biens ou de services indispensables, soit peuvent présenter un danger grave pour la population)

Mais la montée générale de la menace terroriste, et des attentats impliquant directement des sites sensibles, a provoqué une prise de conscience et la nécessité de changer de modèle de pensée. L'industrie est amenée à réfléchir à la prise en compte systématique des risques liés à la malveillance et aux réponses à apporter. Cette réflexion ne concerne plus les seuls sites d'importance vitale, mais a priori tous les sites, et donc ceux qui ne disposent pas aujourd'hui du cadre ou des compétences nécessaires pour analyser le problème.

C'est pour eux que ce guide a été élaboré, avec l'objectif de faciliter et de rendre accessible la démarche.

GENÈSE ET RAISON D'ÊTRE DE CE GUIDE

A la suite de l'attentat de Saint Quentin Fallavier en 2015, dans l'ensemble des mesures prises par l'administration il a été demandé à l'industrie de sécurité à travers le Conseil de l'industrie de confiance et de sécurité (CICS) qui la représente au sein du CoFIS de présenter son offre en matière d'une part de détection d'armes et d'explosifs et d'autre part de détection de comportement anormal.

Le CICS, souhaitant contribuer à l'amélioration de la protection des sites, a pris l'initiative de répondre de façon plus large, en donnant sa vision de la problématique, son approche et en décrivant l'ensemble des capacités de protection de site. L'approche a ensuite été testée sur un site pilote. Elle a ensuite été documentée à travers ce guide à la demande du SGDSN.

La clé de cette approche est d'être raisonnée et raisonnable, c'est à dire de s'appuyer sur des solutions adaptées et abordables pour chaque situation.

L'objectif de ce guide est triple :
- Poser la problématique en termes simples sans surenchère ni alarmisme
- Donner une méthodologie générale d'approche raisonnée aux opérateurs de site
- Apporter des éléments pour les aider à élaborer et exécuter un plan de mise en sécurité

Ces éléments sont :
- Les principes fondateurs
- Les étapes et points clés d'un projet de mise en sécurité
- La liste des fonctions et capacités à mettre potentiellement en œuvre
- Un catalogue illustratif de solutions chiffrées
- L'indication d'acteurs de référence labellisés par la filière

Ce guide n'a pas vocation à être exhaustif mais illustratif. Il apporte un éclairage technologique aux principes décrits dans le guide de sensibilisation du SDSIE (Ministère de la Transition écologique et solidaire).

DÉFINITION DES TERMES

La signification des termes sécurité et sureté est échangée suivant les secteurs :

	COFIS, MINISTÈRE DE L'INTÉRIEUR, SÉCURITÉ PRIVÉE, SECTEUR NUCLÉAIRE, NUMÉRIQUE	SECTEUR AÉROPORTUAIRE, INSTALLATION CLASSÉE POUR LA PROTECTION DE L'ENVIRONNEMENT (ICPE), …
MALVEILLANCE	Sécurité	Sureté
ACCIDENTS	Sureté	Sécurité

APPROCHE GÉNÉRALE

1. PROBLÉMATIQUE

Risques et menaces

Pourquoi assurer la sécurité des sites chimiques et plus particulièrement des sites SEVESO ?

Les sites sensibles présentent des dangers qui peuvent être démultipliés et exploités par des acteurs malveillants : explosions, libération d'agents toxiques, incendies avec un impact direct ou provoqué sur la santé des personnels ou de la population. Ce sont potentiellement des armes par destination.

La menace terroriste est bien sûr la plus préoccupante, mais d'autres formes de malveillance sont possibles avec pour motivation l'idéologie, la vengeance, le chantage, etc. Ce sont ces actes graves qui motivent le plus fortement la mise en sécurité, mais d'autres points sont à prendre en compte tels que les vols de matière et d'équipements, les arrêts provoqués conduisant à des pertes d'exploitation, …

> *« Même si le maître d'ouvrage connait ses missions et obligations en termes de sûreté, il a souvent des difficultés pour les exprimer en termes d'objectifs fonctionnels et performances. »*
>
> *(Propos recueillis auprès d'opérateurs de sites)*

Les sites et plus particulièrement les sites SEVESO font face à des risques nombreux qui vont des plus bénins aux plus graves, tels que (non exhaustif) :

- Vol d'équipements
- Vol de matières dangereuses
- Manifestations d'activistes aux abords ou dans le site
- Survols ou attaques par vecteur aérien, aéronef piloté ou drone
- Sabotages logiques ou physiques, d'origine interne (par exemple employés mécontents) ou externe (criminels ou terroristes) allant de l'arrêt de l'exploitation à la destruction de l'outil industriel
- Déclenchement d'une catastrophe
- Prises d'otage et actions sous la contrainte
- Attaques terroristes visant soit à faire des victimes internes, soit à stopper durablement les opérations, soit à utiliser les installations comme armes par destination (explosions, libération de matières toxiques, …)

A la différence des risques de sûreté de fonctionnement (pannes, négligences, …), les risques de sécurité impliquent systématiquement la volonté de nuire, et leur prise en compte relève d'une autre logique. En matière de sécurité (malveillance) : la gravité de la conséquence peut rendre l'action plus intéressante pour un criminel qui pourra dès lors développer un mode opératoire approprié.

Tout opérateur doit prendre en compte ces risques et y apporter des réponses appropriées qui vont de l'acceptation des risques à la mise en place de systèmes très complets, en passant par des solutions intermédiaires. Comme il a été dit plus tôt, le niveau de la réponse dépend de chaque situation, de l'évaluation des risques et des choix de l'opérateur qui peut décider d'accepter certains risques. Une chose est sûre, on ne peut faire raisonnablement l'économie de l'analyse.

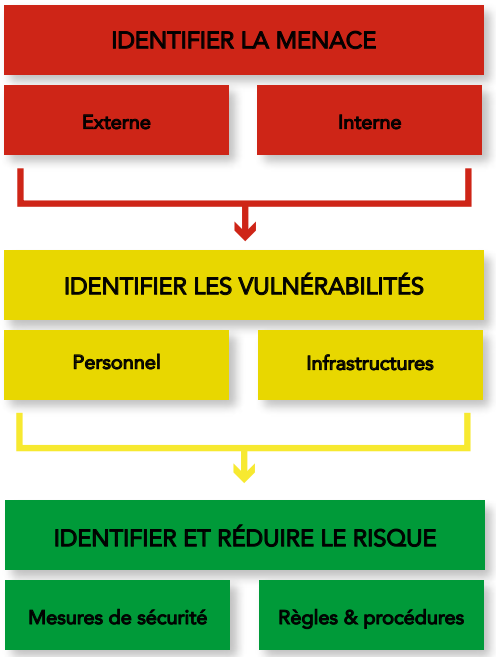
Modes opératoires et réponses
ANALYSE

Les modes opératoires des acteurs malveillants sont au cœur de la réflexion présentée par ce guide. Ce sont eux qui orientent vers les besoins de sécurité.

L'agresseur, en fonction :
- d'une part de ses connaissances du secteur, du site (exploitation, organisation, topographie, …), de ses vulnérabilités,
- et d'autre part de sa doctrine, de ses objectifs et des moyens et du temps qu'il peut mettre en œuvre,

développera un mode opératoire spécifique. L'agresseur élabore un mode opératoire qui ne laisse rien au hasard (mais dont la qualité dépend de sa propre compétence et intelligence).

> *Les technologies sont en pleine évolution et il est difficile de s'y retrouver.*
>
> *(Propos recueillis auprès d'opérateurs de sites)*



Ces modes opératoires sont évidemment très variables et peuvent aller des plus simples aux plus complexes, mais répondent schématiquement à deux types selon que l'agresseur agit en force ou qu'il agit en souplesse, par infiltration.

Mode d'action en force

Dans ce mode d'action, l'agresseur vient de l'extérieur, tente de forcer les protections et de déployer son action malveillante. C'est le mode le plus facile à combattre. En effet, la détection de l'agresseur est facilitée parce qu'il force les protections qu'elles soient à la périmétrie du site ou autour de zones plus protégées. Il est possible d'alerter les forces de sécurité immédiatement.

L'enjeu local sera de ralentir la progression et de prendre des mesures conservatoires d'urgence (MCU), telles que la mise en sécurité des personnels, l'arrêt des opérations et le blocage des commandes, etc.

Mode d'action par infiltration

Ce mode pose plus de difficultés, car :
- L'agresseur a un accès autorisé au site et agit en souplesse
- Seule la détection des signaux faibles (physiques et logiques) dans la durée permet de repérer les agissements et de donner l'alerte

> ***« Les risques et les menaces évoluent plus vite que les moyens de les combattre. »***
> *(Propos recueillis auprès d'opérateurs de sites)*

L'enjeu local sera la prise de conscience collective (sensibilisation / signalements), le décèlement précoce, et des mesures conservatoires d'urgence.

Dans les deux cas, il faut penser à la vulnérabilité des personnels en assurant leur protection physique, mais aussi en prenant en compte le fait qu'ils pourront être amenés à agir sous la contrainte. Des dispositions doivent être prises qui pourront combiner la protection des personnels et l'entrave à l'action hostile : ainsi une panic room bunkerisée pourra très utilement abriter une supervision et un poste de commande opérationnel prioritaire. Cependant, la neutralisation des agresseurs relève des forces de sécurité.

PRÉCONISATIONS DU SDSIE (MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE)

Le SDSIE a établi en 2016 un guide de « Sensibilisation à la protection des sites SEVESO contre les actes de malveillance ». Ce guide qui présente les bonnes pratiques est complémentaire du présent guide. Il recense trois agressions (vol, sabotage, acte terroriste), notant que le vol et le sabotage peuvent également être commis en lien avec le terrorisme.

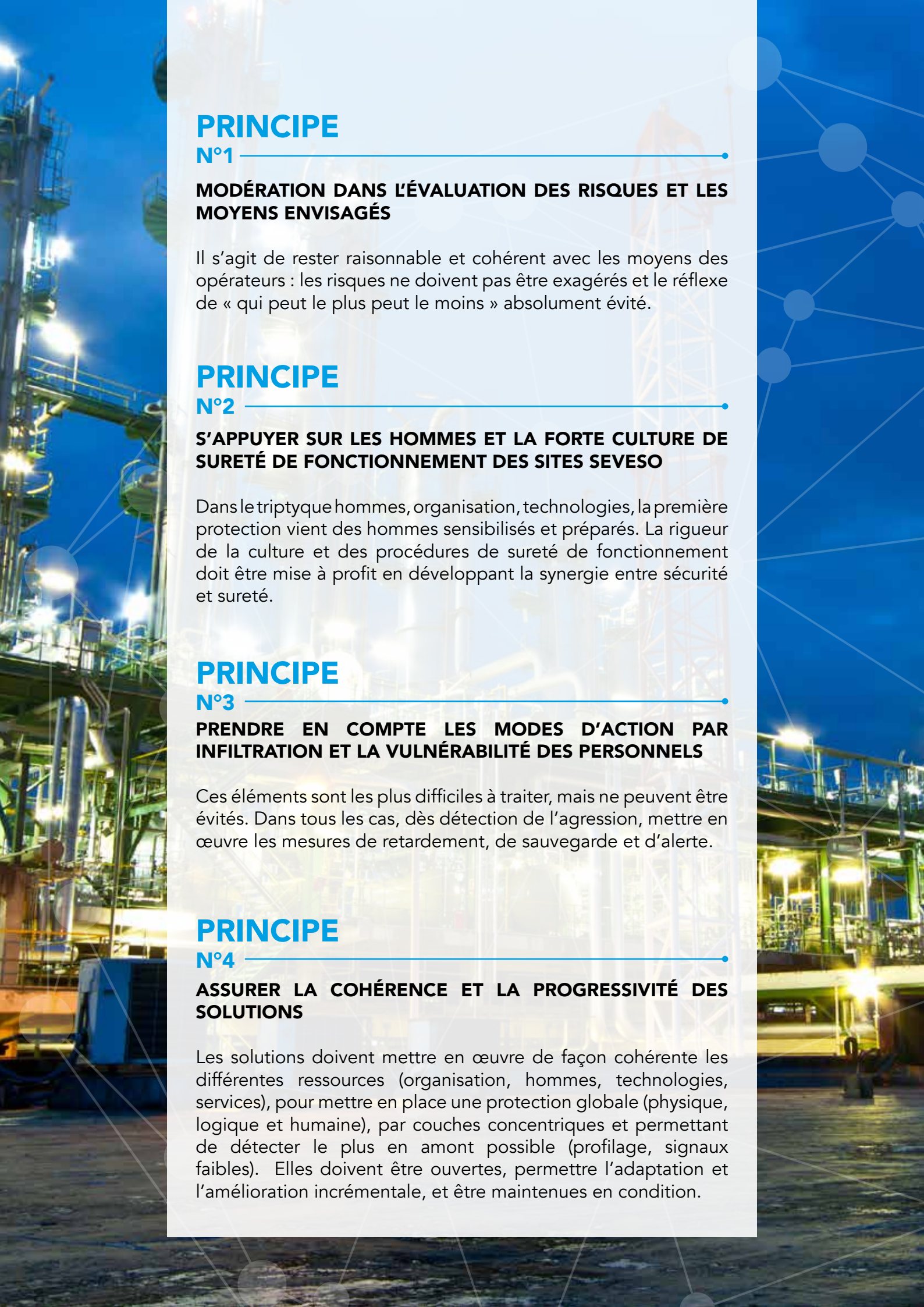
Il en appelle à quatre principes fondamentaux :
- Dissuader : éviter de faire du site une cible
- Détecter : au plus tôt pour pouvoir réagir
- Alerter : car ce sont les forces de sécurité intérieure qui vont intervenir
- Freiner : ralentir l'agression en attendant l'arrivée des forces de sécurité intérieure

2. PHILOSOPHIE / PRINCIPES FONDATEURS

La sécurité apparaît encore pour beaucoup compliquée et onéreuse, pas forcément en rapport avec la réalité des risques et les moyens disponibles. Le CICS a pris en compte cette perception. Ses travaux de 2015 à 2017 ont permis de dégager quatre principes pour une démarche de protection raisonnée, efficace et accessible. Cette démarche est nécessaire, car il est de la responsabilité de chaque site d'anticiper et de conduire au minimum une analyse sérieuse. La décision d'investir ou pas peut ensuite être prise en connaissance de cause.

> ***« La mobilité des personnels, des nouvelles relations sociales, l'usage des technologies de l'information nécessitent de revoir nos modèles d'organisation et les solutions mises en place.***
> *(Propos recueillis auprès d'opérateurs de sites)*

La protection d'un site c'est une question globale et profonde. Protéger un site ou des infrastructures, c'est disposer de moyens humains, de moyens techniques et d'une organisation. Un bon équilibre entre ces trois composantes améliore la performance et limite les investissements.



PRINCIPE N°1

MODÉRATION DANS L'ÉVALUATION DES RISQUES ET LES MOYENS ENVISAGÉS

Il s'agit de rester raisonnable et cohérent avec les moyens des opérateurs : les risques ne doivent pas être exagérés et le réflexe de « qui peut le plus peut le moins » absolument évité.

PRINCIPE N°2

S'APPUYER SUR LES HOMMES ET LA FORTE CULTURE DE SURETÉ DE FONCTIONNEMENT DES SITES SEVESO

Dans le triptyque hommes, organisation, technologies, la première protection vient des hommes sensibilisés et préparés. La rigueur de la culture et des procédures de sureté de fonctionnement doit être mise à profit en développant la synergie entre sécurité et sureté.

PRINCIPE N°3

PRENDRE EN COMPTE LES MODES D'ACTION PAR INFILTRATION ET LA VULNÉRABILITÉ DES PERSONNELS

Ces éléments sont les plus difficiles à traiter, mais ne peuvent être évités. Dans tous les cas, dès détection de l'agression, mettre en œuvre les mesures de retardement, de sauvegarde et d'alerte.

PRINCIPE N°4

ASSURER LA COHÉRENCE ET LA PROGRESSIVITÉ DES SOLUTIONS

Les solutions doivent mettre en œuvre de façon cohérente les différentes ressources (organisation, hommes, technologies, services), pour mettre en place une protection globale (physique, logique et humaine), par couches concentriques et permettant de détecter le plus en amont possible (profilage, signaux faibles). Elles doivent être ouvertes, permettre l'adaptation et l'amélioration incrémentale, et être maintenues en condition.

3. MÉTHODOLOGIE

La méthodologie proposée par le CICS repose sur des fondements classiques, mais son originalité est de donner une vision d'ensemble et des outils de maîtrise aux opérateurs. Son but est de permettre à chaque opérateur de définir et mettre en œuvre facilement un schéma directeur de protection, en pouvant se faire accompagner et recourir à des acteurs de référence.

Elle doit amener un opérateur sans culture de sécurité à se mettre facilement à niveau pour engager la sécurisation de son/ses sites sereinement.

ÉTAPES	OUTILS PROPOSÉS	ACTEURS	PARTICULARITÉS
Prise en main	Ce guide	-	Mettre la protection à la portée de tout opérateur de site
Connaissance du secteur et du site	-	Le gestionnaire du site	-
Analyse des risques et prise en compte de la menace	-	Cabinets de conseil en sûreté, opérateurs industriels, référents sûreté (Police, Gendarmerie, DREAL)	Le CICS préconise une analyse des risques au plus juste sans aucune surenchère. L'analyse conduit aux besoins de sécurisation
Génération d'options de solutions	- Analyse fonctionnelle - Catalogue de solutions - Liste d'acteurs labelisés - Configurateur (à terme)*	Cabinet d'ingénierie / Intégrateurs	Cette étape combine toutes les composantes (hommes, organisation, technologies). Les solutions sont généralement incrémentales. Elles sont élaborées en répondant à une analyse des besoins de sécurisation / plan de sécurisation
Définition du schéma directeur du système de protection	-	Cabinet / intégrateur / gestionnaire	Le schéma directeur présente les solutions retenues en fonction des niveaux de protection choisis et organise le déploiement dans la durée. Il assure la cohérence et la pérennité de la démarche.
Mise en œuvre	-	Intégrateur	Accompagner de sensibilisation, formation
Maintien en condition	-	Intégrateur / gestionnaire	Elle est essentielle pour assurer dans la durée les opérations et l'efficacité des systèmes.

** Le CICS suggère qu'un outil d'analyse et de présentation graphique de solutions soit développé pour faciliter la compréhension et les décisions des opérateurs. Un tel outil peut être disponible à horizon de 3 ans.*

Dans la mise en œuvre de la méthodologie exposée, l'opérateur de site doit veiller à choisir des acteurs, notamment les cabinets de conseil et les bureaux d'étude, qui maîtrisent parfaitement les nouvelles approches, intègrent les doctrines les plus récentes et appropriées, et adhérent aux principes fondateurs ci-dessus. Le CICS poursuivra son action en restant disponible pour indiquer aux opérateurs intéressés les outils et acteurs à leur disposition.

4. ÉTAPES CLÉS DU PROJET DE MISE EN SÉCURITÉ

Prise en main

La mise en sécurité d'un site est un projet important dont la réussite et l'efficience suppose la volonté des actionnaires et de la direction. Ce n'est pas un simple ajout marginal à un dispositif opérationnel existant, mais la mise en place d'une composante à part entière du dispositif qui nécessite d'être pris en compte et interfacé avec l'ensemble des autres composantes. C'est donc une démarche en profondeur, qui implique tous les acteurs.
Le projet démarre par la volonté affichée de la direction, la nomination d'un responsable de la sécurité directement rattaché à la direction et d'un chef de projet qui peut être la même personne.

Connaissance du secteur et du site

Une première étape importante consiste à bien connaître le site et son secteur industriel :
- Nature des produits et des opérations et risques associés
- Identification des points sensibles et des composants névralgiques : pour atteindre ses objectifs, l'agresseur doit avoir accès à des composants névralgiques (unités de production sensible, stockage de produits dangereux, centre de contrôle, …) autour desquels la protection s'articule
- Configuration du site, des accès, des zones
- Conditions et volumétrie des entrées / sorties de personnes et de matière
- Etc.

Analyse des risques et prise en compte de la menace

Cette étape est cruciale et il faut y apporter du soin et surtout une bonne dose de réalisme et de modération. Un travers courant est de maximiser la liste des menaces à prendre en compte. Il s'agit au contraire d'être très sélectif et de bien filtrer grâce à des critères essentiels : spécificité, attractivité, gravité, état de la menace, responsabilité, urgence, enjeux économiques.

Spécificité :
- En quoi la menace est spécifique à la nature de l'activité et sinon quel niveau de protection est pertinent ?
- Faut-il être plus protégé que partout ailleurs où la menace est susceptible de se matérialiser ?

Attractivité :
- Quel est le degré d'attractivité du site ?
- Est-ce que l'entreprise, l'activité, la localisation, l'image dans le public sont suffisamment attractifs pour motiver une action hostile d'ampleur ?
- Est-il plus facile de s'attaquer au site ou à la distribution des produits ?
- Facilité de mise en œuvre : est-ce que le mode opératoire d'un événement redouté est simple ou nécessite-t-il un ensemble de moyens, de conditions difficiles à réunir ?

Gravité :
- Est-ce que la réalisation du risque se traduit par une conséquence particulièrement grave (destructions importantes, grand nombre de victimes, forte désorganisation, impact financier, impact d'image…) ?
- Quel est le risque réel à la santé (personnel / population) et à l'environnement ?

Etat de la menace :
- Toute faille de sécurité n'est pas forcément utilisée par les agresseurs. Ceux-ci, notamment les terroristes, privilégient des cibles et des modes d'action. Il s'agit de suivre l'évolution de la menace pour se protéger à temps.
- Est-ce que les acteurs hostiles connus (la menace) ou potentiels s'intéressent à des attaques de cette nature ? Est-ce déjà une menace forte ou s'agit-il plutôt d'anticipation ?

Responsabilité :
- Qu'est-ce qui est du ressort de l'Etat et notamment des forces de sécurité et des forces armées ?
- Qu'est ce qui est de la responsabilité de l'opérateur et qu'est ce qui ne l'est pas ?

Urgence :
- Si la menace, n'est pas avérée aujourd'hui, mais qu'elle apparaît plus tard, est-il possible de prendre des mesures rapides pour s'en protéger ? Faut-il au contraire prendre des dispositions par anticipation car le temps ne sera pas disponible ?

Enjeux économiques :
- Quelles sont les conséquences d'agressions potentielles ?
- Est-ce que les coûts matériels et humains sont en rapport avec le coût de la protection ?

Les risques ne s'appliquent pas indistinctement ni en bloc. Afin de bien évaluer les risques il s'agit de conduire une analyse réaliste, qui sera menée conjointement par le site et des experts. Cette analyse doit prendre en compte la menace terroriste, mais aussi tous les autres volets de la malveillance, eux aussi bien évalués en termes d'occurrence et d'impact.

Toute menace doit être relativisée. Ainsi, par exemple l'usage malveillant de petits drones ne doit être crédité que de son réel potentiel de nuisance, et la menace par des aéronefs ou drones de plus grande taille sera du ressort de l'Armée de l'Air. Pour un site donné, plusieurs facteurs détermineront le besoin d'une protection périmétrique virtuelle et/ou physique légère ou très lourde, comme par exemple l'impact de blocage ou de pénétration par des manifestants ou des activistes.

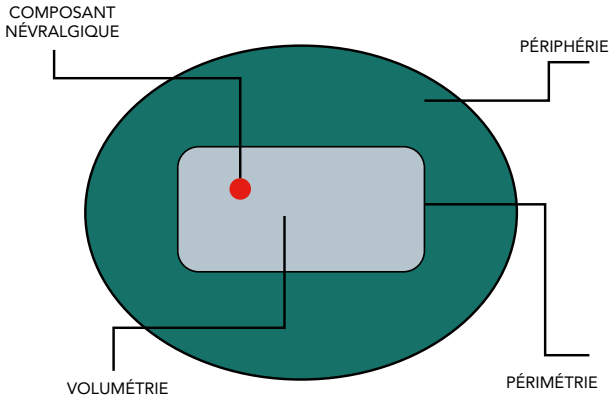
En définitive, une analyse permettra d'éviter les surenchères et favorisera une approche raisonnée et accessible de la sécurité. Elle permettra notamment :
- d'éviter de surévaluer des risques ou des menaces (par exemple pour certains sites, le survol voire l'attaque par micro-drone peut ne présenter aucun véritable danger),
- de distinguer les risques spécifiques, nécessitant une réponse propre, des risques génériques (qui peuvent se présenter dans n'importe quel environnement et auxquels il ne s'agit pas d'apporter une meilleure réponse qu'ailleurs),
- de distinguer les risques qui relèvent de la responsabilité de l'opérateur de site et ceux qui relèveraient des forces de sécurité intérieures ou des forces armées, et dont le traitement ne fera intervenir que partiellement l'opérateur.

Génération d'options de solutions

En fonction des risques et menaces retenues, de la configuration du site et de l'existant, et des niveaux de protection envisagés, des éléments de solutions et des dispositifs d'ensemble peuvent être générés, faire l'objet d'options, être évalués en coûts, performances, impact opérationnel.

PROTÉGER LES COMPOSANTS NÉVRALGIQUES

Toute solution vise à protéger les composants névralgiques. Pour détecter les tentatives d'accéder aux composants névralgiques, ou les actes précurseurs, une surveillance est exercée à la périphérie (aux abords du site voire au-delà), à la périmétrie et en volume (à l'intérieur du site). Cette surveillance est potentiellement de plusieurs natures : physique (contrôle d'accès, capteurs, vidéo, etc.), logique (connexions, logs, activité des réseaux sociaux, etc.) et humaine (signalements, etc.). La progression vers les composants névralgiques (ou la capacité à agir dessus) est freinée par différents moyens.



LES 3 VOLETS D'UNE PROTECTION EFFICACE

Toute solution comprend les volets humains, organisationnels et technologiques qui sont imbriqués. C'est conjointement, en synergie, qu'ils composent des solutions efficaces et équilibrées.

L'humain

C'est le volet le plus important :

- Le bénéfice de procédures efficaces ou d'investissements lourds peut être réduit à néant par des comportements inadaptés
- Nécessité absolue d'une sensibilisation des personnels, sur la sécurité de façon générale et sur les spécificités mises en œuvre sur le site
- Importance de l'adhésion et de la coopération des personnels vis à vis des procédures et des outils – une solution technologique performante peut être réduite à néant si le personnel la contourne
- Entraînement et mesure de la préparation par des exercices qui peuvent être couplés à ceux réalisés pour la sûreté de fonctionnement
- Importance de l'humain dans la détection des situations anormales et des signaux faibles
- La culture de sûreté et sa rigueur peuvent être mises à profit et exercées sur l'objectif de sécurité à travers une simple adaptation

Par ailleurs, une organisation de la sécurité fait très souvent appel à des entreprises de services qui fournissent les agents spécialisés requis.

L'organisationnel

Ce volet est essentiel, car c'est lui qui traduit la volonté de protection et structure l'action pour la mettre en œuvre.

- L'organisationnel est préalable à la sensibilisation et à la formation des personnels
- Il définit les responsabilités, les processus et les procédures de la protection
- Il articule la protection avec les autres fonctions du site
- Il définit l'architecture, les positionnements, les moyens à mettre en œuvre et l'action dans la durée

Les règles de base relèvent de l'organisationnel, telles que mettre tous les éléments sensibles de la protection dans des zones protégées (serveurs, commandes, clés, etc.)

Les technologies

Le volet technologique apporte aux deux premiers les outils performants et permanents nécessaires en fonction des objectifs. Ce volet est d'une telle richesse et complexité qu'il convient de l'éclairer par une vision synthétique des systèmes, des services associés et des performances disponibles.

L'étendue des possibilités et de l'offre ne préjuge pas de ce qui peut convenir à un site. Des solutions simples et abordables peuvent très bien convenir à des sites aux risques et enjeux peu élevés.

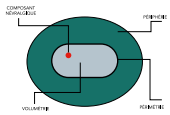
LES FONCTIONS ET LES CAPACITÉS TECHNOLOGIQUES

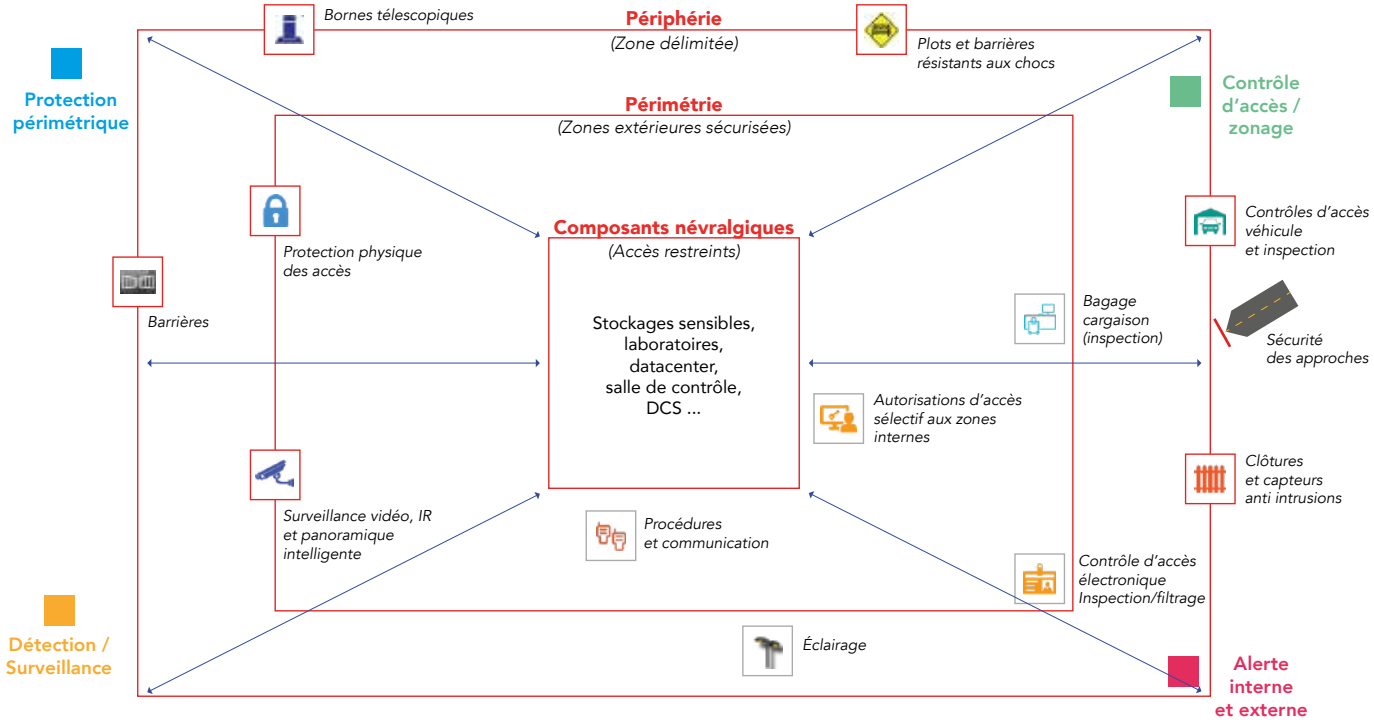
Les fonctions nécessaires répondent à de grandes problématiques :

- Protection périmétrique : isoler le site (et/ou des parties plus sensibles du site, notamment si celui-ci est très étendu) de l'extérieur et empêcher physiquement les intrusions.
- Contrôle d'accès et zonage : savoir qui a le droit d'accéder au site et pour y faire quoi, contrôler l'accès effectivement, limiter l'accès aux différentes zones en fonction des besoins, administrer les droits des utilisateurs des équipements et systèmes, savoir éventuellement en temps réel où sont les personnes.
- Détecter / surveiller : surveiller par différents moyens (video, déplacement et actions des personnes, accès aux systèmes, logs) pour détecter les intrusions, les évènements et comportements anormaux et pouvoir analyser et donner éventuellement l'alerte.
- Alerte interne et externe : informer les personnels, les forces de sécurité et les acteurs nécessaires, assurer la communication entre les acteurs, mettre en œuvre les mesures conservatoires d'urgence, protéger les personnels.
- Supervision et cyber : centraliser les informations pour mieux les analyser et décider, et assurer la protection cyber des systèmes opérationnels et de sécurité.
- Exploitation des données : recueillir ou détecter par l'analyse des données (Big data, monitoring des réseaux sociaux, autres sources possibles de données publiques ou non) les informations nécessaires pour profiler les personnels ou anticiper des actions hostiles.

Les éléments d'une solution peuvent être représentés schématiquement comme suit :

Configuration minimale (Sécurité en profondeur)





Note : beaucoup de ces fonctions peuvent être fournies comme des services par des acteurs spécialisés (surveillance video intelligente, cyber, big data, profilage, analyse d'anormalité, etc.) sur sites ou à distance.

Deux autres fonctions sont utiles aux acteurs en charge de la sécurité :

- Accompagnement : apporter à l'opérateur les capacités d'audit, de conseil, de conception.
- Intégration : la cohérence et la performance d'ensemble nécessitent que la responsabilité d'interfacer et d'articuler l'ensemble des éléments de la sécurité soit confiée à un acteur spécialisé (en évitant les solutions propriétaires pour garantir le portage).

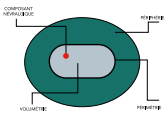
Brochure capacitaire du GICAT

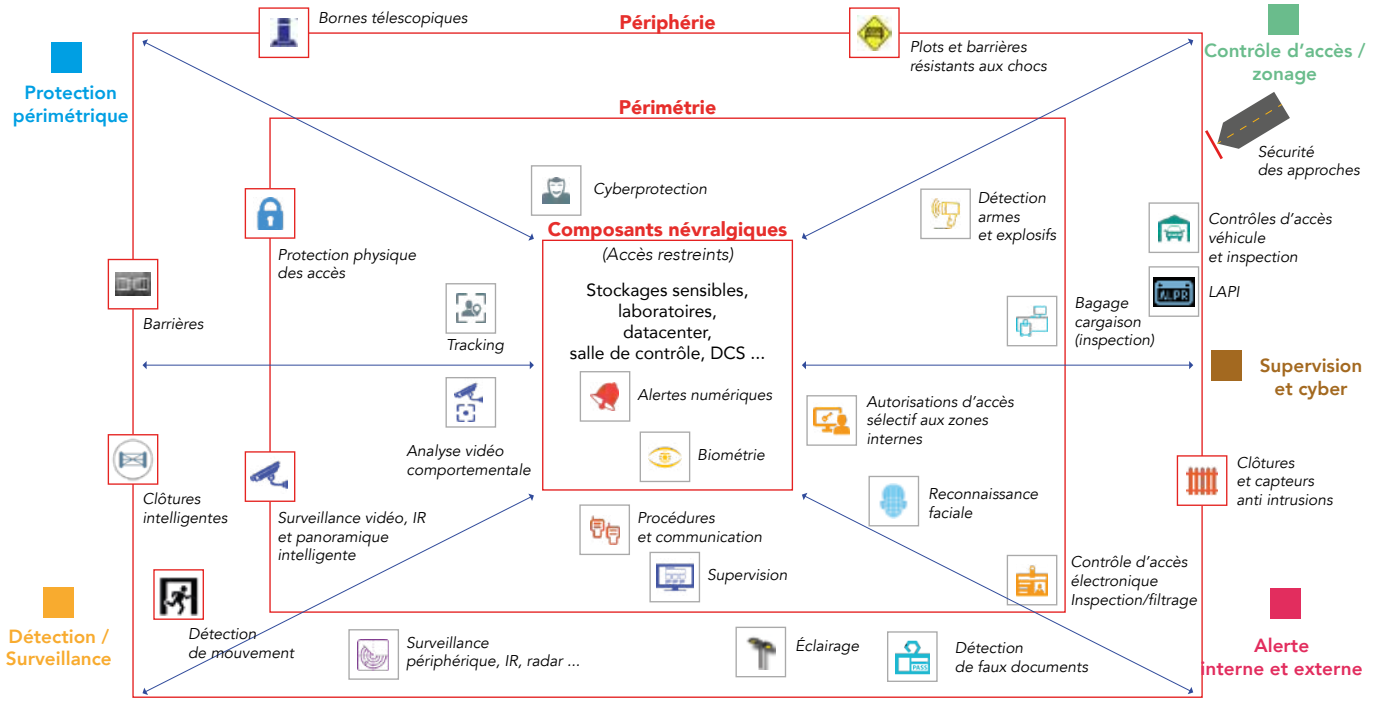
Le groupement industriel GICAT, membre fondateur du CICS et très actif sur le segment de la protection des sites, a produit en s'appuyant sur les travaux du CICS une brochure capacitaire qui se concentre sur la protection physique. Une présentation de cette brochure figure en annexe.

Configuration avancée (Sécurité dynamique dans la durée)

La configuration minimale apporte une protection basée sur l'herméticité recherchée de couches successives avec contrôles d'accès, protections physiques et surveillance limitée. C'est une configuration statique adaptée aux actions de pénétration les plus moins sévères.

Pour des sites exposés à des risques et menaces plus diversifiés (menaces internes, infiltration, actions plus sophistiquées, etc.), qui recherchent une sécurité plus étendue, dynamique et dans la durée, une configuration renforcée basée sur une approche plus pro-active est à envisager. Elle met en œuvre d'autres moyens tels que la vidéo surveillance intelligente, la détection anticipée de signaux faibles (y compris au-delà de la périmétrie) et d'actions dans la durée, le contrôle actif de la position des personnels, la supervision, la cyber-sécurité; moyens dont la performance d'ensemble est accrue par une approche globale et cohérente. Une partie des fonctions peut reposer sur des services à distance (surveillance intelligente, supervision, alertes, cyber-sécurité, surveillance des réseaux, etc.). Ces moyens plus dynamiques ne sont pas synonymes d'une explosion des coûts, d'autant plus qu'ils peuvent être judicieusement utilisés et répartis.





LES OPTIONS TECHNOLOGIQUES PRINCIPALES

Les options peuvent s'appuyer sur des configurations génériques permettant soit simplement de détecter, freiner, et alerter (en noir dans le tableau ci-dessous), soit d'assurer une sécurité dynamique dans la durée (compléments en rouge dans le tableau).

FONCTION	SÉCURITÉ	SÉCURITÉ DYNAMIQUE
Protection périmétrique	Balisage et obstacles (herses, clôtures, murs, ..)	Balisage et obstacles (herses, clôtures intelligentes, murs, double peau ..) : Réseau de capteurs intelligents
Détection / Surveillance	Capteurs anti-intrusion (barrière infrarouge, vibrations, …) Surveillance vidéo et infrarouge intelligente (sectorielle, panoramique)	Élargissement à une zone périphérique de surveillance (IR, radar,…) Capteurs anti-intrusion (barrière infrarouge, vibrations, …) Surveillance vidéo et IR intelligente / analyse comportementale Détection d'intrusion temps réel par analyse vidéo et levée de doute immédiate Détection de comportements anormaux des personnes et des matériels (alertes automatiques / règles pré-établies) Reconnaissance faciale LAPI
Contrôle d'accès / Zonage	Individu (gestion habilitation(s), inspection/filtrage Véhicule (autorisation et inspection physique) Bagage/cargaison (inspection) Autorisations d'accès sélectif aux zones internes	Individu (gestion habilitation(s), inspection/filtrage – biométrie, détection de faux documents Véhicule (autorisation et inspection physique, LAPI) Bagage/cargaison (inspection) Détection armes et explosifs : portiques, scanners, détecteurs de trace, de vapeur Autorisations d'accès sélectif et dynamique aux zones internes Tracking dans le site en extérieur et en intérieur (badges RFID, GSM, geoloc. autonome, …)
Alertes interne et externe	Procédures et communication	Procédures et communications Alertes numériques (interne, les autorités, la population exposée)
Supervision et cyber	-	Supervision locale ou distante Analyse des accès aux systèmes, des réseaux, des comportements pour identifier tout signe précurseur Cyberprotection des systèmes de sécurité

Les solutions retenues dépendent des situations et différeront par exemple suivant qu'il s'agit :

- *d'un site étendu avec peu de zones sensibles réparties*
- *Un site avec peu de systèmes industriels sensibles aux cyberattaques*
- *Un site avec plus de systèmes numériques, beaucoup de personnel, sous-traitants et visiteurs à surveiller, …*

Définition du schéma directeur

Les grandes options de solutions (décrites organisation, hommes, technologies, services) doivent être analysées en termes de coûts, performances, contraintes de mise en œuvre, facilité d'évolution, impact sur les opérations, capacité à être mises en œuvre par incréments, etc. Les choix sont reportés dans un schéma directeur qui précise :

- Le système de protection visé
- Comment il est déployé (projet de mise en place, étapes, conditions de succès, etc.)
- Le budget qui doit comprendre les coûts récurrents d'exploitation, les services et bien sûr le maintien en condition et les mises à niveau
- Les jalons, les points de décision futurs, les audits et les mesures (coûts, métriques de performance, etc.) qui permettront d'évaluer en cours de route l'efficacité de la protection
- La stratégie de réalisation (cahiers des charges, consultations, responsabilités d'intégration, etc.)

Cette étape est importante sur le plan de l'organisation, de la programmation et de la maitrise du plan de protection.

Mise en œuvre

La réalisation du schéma directeur constitue un projet à conduire avec rigueur et en veillant à disposer en interne ou en externe des compétences d'acheteur de sécurité. Comme pour toute acquisition, il s'agit de veiller à la vérification des performances spécifiées, aux garanties apportées dans la durée, et à la portabilité des solutions.

Maintien en condition / incréments

Le maintien en condition du système de protection est essentiel car son efficacité en dépend. Une fois passé l'effort initial de mise en place, il faut s'astreindre à un programme rigoureux de maintenance et de maintien en condition opérationnel du système de protection. Cela recouvre :

- L'entretien régulier des équipements (par exemple caméra de surveillance)
- La mise à jour des logiciels
- La mise à niveau permanente de la cybersécurité
- Des tests de bon fonctionnement d'ensemble du système

Les actions de maintien en condition peuvent se combiner lorsque cela s'y prête à la mise en place d'incréments fonctionnels.

LISTE DES FONCTIONS ET CAPACITÉS ASSOCIÉES

LISTE DES FONCTIONS ET CAPACITES ASSOCIEES

Les tableaux suivants donnent les fonctions et des industriels (liste non exhaustive recueillie à partir d'indications des groupements du CICS) :

PROTECTION PÉRIMÉTRIQUE

Isoler le site de l'extérieur et empêcher physiquement les intrusions

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS		
	Équipements	**Logiciels**	**Intégration**
Balisage et obstacles	Eryma group, Kopp, Soreha, Derickx, Urbaco, Amco Les Escamotables	-	Secure Systems & Services (Vinci), Engie Spie Batignolles Technologies
Réseaux de capteurs intelligents	STMicroelectronics,	Ardanti Défense	-
Stop véhicule électronique	-	-	-
Protection anti-drone	CS, MC2, Cerbair	-	CS, Cerbair
Menuisierie de sécurité	Gunnebo		

CONTRÔLE D'ACCÈS ET ZONAGE

Savoir qui a le droit d'accéder au site et pour y faire quoi, contrôler l'accès effectivement, limiter l'accès aux différentes zones en fonction des besoins, administrer les droits des utilisateurs des équipements et systèmes, savoir éventuellement en temps réel où sont les personnes.

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS		
	Équipements	**Logiciels**	**Intégration**
Biométrie	Idemia, Thales, Stid, Zalix, Abiova, STMicroelectronics, Gunnebo	Idemia, Thales, Gunnebo	Idemia, Thales, Secure Systems & Services (Vinci), Engie.
Gestion des habilitations	-	CS, Secure Systems & Services (Vinci)	-
Gestion des droits d'accès	Alcea, ARCLAN, ARD, TIL Technologies, Engie (Be-Safe.com)., Omnitech, Gunnebo	Secure Systems & Services (Vinci), Gunnebo	-
Détection de faux documents	Surys	Resocom, AT&T, Ariadnext	-
Lapi véhicule	-	TEB (Pryncar), Survision, Alphanumeric Vision	-
Inspection physique véhicule	Kopp	Kopp	-
Inspection bagages / cargaison	-	-	-
Détection d'armes et explosifs	Idemia, MC2, Sodern, Saphymo	-	-
Détection NRBC	Mirion, Bertin, Saphymo, Proengin, IMS	-	-
Autorisation d'accès sélectif et dynamique aux zones internes	Thales, Secure Systems & Services (Vinci) CDVI, Cogelec, URMET, Legrand/Bticino, Aiphone, STMicroelectronics, Engie Ineo (Be-Safe.com)	Thales, Secure Systems & Services (Vinci)	Engie
Comptage des personnes en zone, affichage dynamique	Gunnebo	Secure Systems & Services (Vinci), TEB (Pryncount), Gunnebo	Engie
Tracking interne (badges, GSM, video, …)	Airbus, Thales, Sysnav, Traqueur, Photospace, Geoloc software, Ionosys, STMicroelectronics, Maple High Tech	Airbus, Thales, Egidium, Deveryware, Traqueur, ResonateMP4, 4G Technology, Geoloc software, Novitact, Maple High Tech	Traqueur, ResonateMP4, Engie.

DÉTECTION / SURVEILLANCE

Surveiller par différents moyens (video, déplacement et actions des personnes, accès aux systèmes) pour détecter les intrusions, les évènements et comportements anormaux et pouvoir analyser et donner éventuellement l'alerte.

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS		
	Équipements	**Logiciels**	**Intégration**
Surveillance de zone périphérique	Sagem, Thales, Airbus, HGH, ASV, Exavision, Cilas, Diades Marine, SORHEA, NOVADEM, PIXIEL, ATEM, Hymatom	Ardanti Défense	Sagem, Thales, Airbus, Secure Systems & Services (Vinci), Engie, CS.
Détection d'intrusion	UTC, DELTA DORE, SEPTAM, HAGER/ DAITEM, SOMFY, COOPER SECURITE, SYNCHRONIC, LEGRAND, STMicroelectronics, HGH, Hymatom	Foxstream, Evitech,	Engie
Surveillance video	Hymatom (Visiospace), Luceor, HGH ….	CS	Engie, CS.
Surveillance video intelligente	-	Evitech, Inpixal, Foxstream, Spikenet, TEB (Digipryn), CS, HGH	Hymatom, Secure Systems & Services (Vinci), CS, Engie, Thales
Reconnaissance faciale	Idemia, STMicroelectronics	Idemia	Idemia
Détection de comportements anormaux (règles pré-établies)	-	Deveryware	Thales, Airbus
Robotique de surveillance	ECA, Nexter, Tecdron, Bertin, Fly-n-sense, Aeraccess	-	-
Détection d'anormalité par machine learning	-	Airbus	-
Détection d'anormalité dans la durée	-	Airbus, Deveryware	-

ALERTE INTERNE ET EXTERNE

Informer les personnels, les forces de sécurité et les acteurs nécessaires, assurer la communication entre les acteurs, mettre en œuvre les mesures conservatoires d'urgence, protéger les personnels.

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS		
	Équipements	**Logiciels**	**Intégration**
Procédures et communication	-	-	Secure Systems & Services (Vinci), Engie
Alertes numériques	-	Deveryware, Gedicom, ATLS, Ciitelecom, cedralis	-
Sécurité proactive (sur détection d'anormalité)	-	-	-

SUPERVISION ET CYBER

Centraliser les informations pour mieux les analyser et décider, et assurer la protection cyber des systèmes opérationnels et de sécurité

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS		
	Équipements	**Logiciels**	**Intégration**
Supervision	-	Egidium, HGH, Hymatom (Visiospace), Thales, Airbus, CS, Diades Marine, Evo-lynx, Entelec, Prysm, TEB (Prynvision), Alcea, Diginext, Ardanti Défense	Thales, Airbus, CS, Secure Systems & Services (Vinci), Scutum, Securitas, Alcea, Diginext, Engie, Omnitech
Hypervision (supervision unifiée)	-	Egidium, CS, Evolynx, En-telec, Prysm, TEB, Diginext, Engie, Hymatom, Ardanti Défense	TEB, CS, Diginext, IGO, Engie, Omnitech
Analyse dans la durée des accès aux systèmes, réseaux,…	-	-	-
Accès des systèmes de supervision à distance par les autorités	-	-	-
Réseaux de com dédiés	-	Green Communication, Luceor, Air Lynx, Syrlinks	Engie
Cyberprotection des systèmes de sécurité	STMicroelectronics	-	-
Cyberdéfense de l'outil industriel	STMicroelectronics	Thales, Airbus, Sentryo, Seclab, CS, Schnieder Electric	Engie

EXPLOITATION DES DONNÉES

Recueillir ou détecter par l'analyse des données (Big data, monitoring des réseaux sociaux, autres sources possibles de données publiques ou non) les informations nécessaires pour profiler les personnels ou anticiper des actions hostiles.

SOUS-FONCTIONS	EXEMPLES D'ACTEURS INDUSTRIELS	
	Logiciels	Intégration
Exploitation des données	Soprasteria, Airbus, Thales, CS	Soprasteria, Airbus, Thales, CS, Engie

DEUX AUTRES FONCTIONS SONT UTILES AUX ACTEURS EN CHARGE DE LA SÉCURITÉ :

Accompagnement

Apporter à l'opérateur les capacités d'audit, de conseil, de conception

Exemples d'acteurs industriels : Schneider Electric, Amarexia, Epsilon Consultants, Risk&Co, Alcea, CNPP, APSYS, Ardanti Défense

Intégration globale

La cohérence et la performance d'ensemble nécessite que la responsabilité d'interfacer et d'articuler l'ensemble des éléments de la sécurité soit confié à un acteur spécialisé (en évitant les solutions propriétaires pour garantir l'évolutivité et le portage).

Exemples d'acteurs industriels : Thales, Airbus, Securitas, Secure Systems & Services (Vinci), Engie Spie, Schneider Electric, Assystem, CS, SNEF, Scutum, Cegelec Defense, ATOS Ardanti Défense

CATALOGUE ILLUSTRATIF DES SOLUTIONS CHIFFRÉES

PROTECTION PÉRIMÈTRIQUE

M. Jérôme Murolo
j.murolo@amco.fr - GSM : 06 20 88 81 66
Tel. 04 66 33 25 70 - Fax. 04 66 33 25 71

DOMAINE PROTECTION PÉRIMÈTRIQUE

http://www.bornes-escamotables.com/defense_anti_intrusion

PRODUIT : Systèmes escamotables de protection contre les véhicules béliers

- AMCO fabrique, conçoit, installe et entretien des systèmes mobiles de sécurité (obstacles, bornes escamotables, bornes fixes, barrières) dédiés à la protection des sites sensibles contre les véhicules béliers

CARACTÉRISTIQUES PRINCIPALES

- Tous les produits de la gamme sont certifiés par Crash-tests
- Surfaces exposées aux roulements entièrement conçus en Inox
- Large gamme de produits adaptée à tous les niveaux de sécurité

BÉNÉFICES PRINCIPAUX

- Fabrication Française
- Qualité de finition
- Relation directe avec le fabricant de la conception au SAV
- Assistance aux travaux de pose
- Temps de pose réduit : 24 à 48 H

COÛT D'ACQUISITION

Catégorie A
0 à 50 K€

10 K€ pour 2 bornes manuelles
< 25 K€ pour 1 accès sécurisé par 2 bornes automatiques
< 50 K€ pour sécurisation d'un accès par roadblockers

Dario BARDI
Directeur Général
06 37 99 82 24

DOMAINE PROTECTION PÉRIMÈTRIQUE

urbaco.came.com/fr

PRODUIT : Bornes de protection contre les attaques au camion-bélier

La gamme de bornes Haute Sécurité CAME URBACO est conçue pour contrôler l'accès aux sites sensibles et protéger les points d'accès stratégiques contre les attaques au camion-bélier.

CARACTÉRISTIQUES PRINCIPALES

- Matériau : Acier haute résistance
- Diamètre de la tête de borne (mm) : Ø250 à Ø325 selon modèle
- Hauteur (hors sol) : 1000 mm
- Résistance à l'impact : de 681,2kJ à 1776kJ selon modèle
- Motorisation hydraulique : possibilité de remontée d'urgence en 1,5 seconde
- Type d'installation : Escamotable automatique, amovible et fixe

BÉNÉFICES PRINCIPAUX

- Protège les sites sensibles contre les attaques au camion-bélier
- Certifiée IWA 14-1:2013 & PAS68:2013
- 1 seule borne ONE50EVO résiste aux impacts de 2 camions de 7,5T lancés à 80km/h

COÛT D'ACQUISITION
Inférieur à 50k€ pour une solution standard de sécurisation d'un 1 accès par 2 bornes escamotables ONE 50EVO.

Catégorie A
0 à 50 k€

PROTECTION PÉRIMÈTRIQUE

CAME URBACO

Dario BARDI
Directeur Général
06 37 99 82 24

DOMAINE PROTECTION PÉRIMÈTRIQUE

urbaco.came.com/fr

PRODUIT : Roadblockers escamotables de protection contre les attaques au camion-bélier

La gamme de Roadblockers anti-intrusion CAME URBACO est conçue pour empêcher les véhicules non-autorisés d'accéder à un périmètre sécurisé. Leur large gabarit permet de condamner entièrement un accès mais également de fournir un très haut niveau de protection contre les attaques au camion-bélier.

CARACTÉRISTIQUES PRINCIPALES

- Matériau : Acier haute résistance
- Largeur (mm) : de 1000 à 4000 selon modèle (possibilité jusqu'à 9000mm)
- Hauteur (hors sol en mm) : de 800 à 1200 selon modèle
- Profondeur de scellement (mm) : de 450 à 600 selon modèle
- Résistance à l'impact : de 650,2kJ à 1 843,9kJ selon modèle
- Motorisation hydraulique : possibilité de remontée d'urgence en 1,5 seconde
- Type d'installation : Escamotable automatique faible profondeur et fixation en surface

BÉNÉFICES PRINCIPAUX

- Protège les sites sensibles contre les attaques au camion-bélier
- Crash-testés selon la norme ASTM F2656-07
- Faible profondeur de scellement (à partir de 450mm)

COÛT D'ACQUISITION

Inférieur à **50k€** pour une solution standard de sécurisation d'un 1 accès par 1 Roadblocker MRB50SH K12.

Catégorie A
0 à 50 k€

CERBAIR
ANTI-DRONE SOLUTION

Thomas Gueudet -
Directeur commercial et Business Development
+33 (0)1 74 31 23 52
contact@cerbair.com

DOMAINE PROTECTION PÉRIMÈTRIQUE

PRODUIT : La guerre électronique au cœur de la lutte anti-drone

La guerre électronique au cœur de la lutte anti-drone. Les drones menacent la confidentialité et la sécurité et présentent 4 menaces principales : attaque, collision, contrebande et espionnage. CerbAir souhaite redonner le contrôle de l'espace aérien aux opérateurs de sites sensibles avec des solutions uniques qui allient performance, juste coût, évolutivité et mobilité. Nos solutions se déclinent sur plusieurs formats et s'adaptent aux besoins et au budget de chacun.

CARACTÉRISTIQUES PRINCIPALES

Nos technologies anti-drone offrent une détection passive de tous les drones civils et sans risque d'interférence, avec une portée allant jusqu'à 5km en conditions optimales. Nous analysons tout le spectre radiofréquence (400/800/900 MHz et 2,4/5 GHz), sommes capables de localiser le pilote et suivre le drone en temps réel. Une fois détecté, l'opérateur peut forcer l'atterrissage du drone ou en prendre le contrôle.

BÉNÉFICES PRINCIPAUX

Meilleur rapport qualité-prix du marché / Solution évolutive jamais obsolète / Mode automatique ou manuel possible / Expérience opérationnelle avérée (aéroports, prisons, stades …)

COÛT D'ACQUISITION

Catégorie	
Petit Site	**10 à 50 k€**
Moyen Site	**50 à 100 k€**
Grand Site	**100 à 500 k€**

1. détecter

2. caractériser

3. neutraliser

PROTECTION PÉRIMÈTRIQUE

Viviane BRETAGNE
Directeur Commercial & Business Développement
viviane.bretagne@gunnebo.com
Mobile : +33 (6) 73 87 33 50

DOMAINE PROTECTION PÉRIMÈTRIQUE

PRODUIT : DORTEK

Solutions de menuiserie de protection des bâtiments contre les risques industriels, les attaques malveillantes ou terroristes

CARACTÉRISTIQUES PRINCIPALES

- PCS, guérites, portes, cloisons, fenêtres et SAS de sécurité
- Produits certifiés contre l'effraction, les attaques par balles, le souffle d'explosion, le feu

BÉNÉFICES PRINCIPAUX

- Assurer une protection des personnes et des centres névralgiques contre les risques industriels et les attaques externes

COÛT D'ACQUISITION

Porte de sureté 5 à 20 k€ selon dimension et niveau de résistance

Sas de sécurité 10 à 50 k€ selon les options de filtrage

Poste de sécurité 50 à 100 k€ selon dimension et niveau de résistance

TALOS KOPP
70 Rue du Général Malleret Joinville
94400 VITRY SUR SEINE
Téléphone : 01 49 40 09 04

DOMAINE PROTECTION PÉRIMÈTRIQUE

PRODUIT : PIKOSOL - Protection anti véhicules béliers

- Herse anti-véhicules suicides.
- Système de protection physique des accès véhicules.
- Réalisation de checkpoints, ou de sas véhicules pour un contrôle d'accès optimal des véhicules sur site.

CARACTÉRISTIQUES PRINCIPALES

- Largeur de passage : de 2 à 6 mètres
- Motorisation : 380VAC Triphasé (commande manuelle de secours)
- Traitement anticorrosion et revêtement polyester par thermo-laquage
- Possibilité d'asservissement avec systèmes existants
- Possibilité sans génie civil avec l'option RAMPOSOL

BÉNÉFICES PRINCIPAUX

- Déclenchement ultra rapide (0,3 sec)
- Discrète et dissuasive
- Faible profondeur de décaissement

COÛT D'ACQUISITION

Catégorie A
0 à 50 k€
(en fonction de la largeur)

COÛT D'USAGE

visites de maintenance préventive (2 par an en moyenne)
2000 € à 3000 € /an /accès pour une garantie totale (pièces + MO) en IDF.

PROTECTION PÉRIMÈTRIQUE

TALOS KOPP
70 Rue du Général Malleret Joinville
94400 VITRY SUR SEINE
Téléphone : 01 49 40 09 04

DOMAINE PROTECTION PÉRIMÈTRIQUE

PRODUIT : PLAKOSOL MOBILIS - protection anti véhicules béliers / mobile

- Obstacle anti-véhicules suicides déplaçable
- Système de protection physique des accès véhicules sans nécessité de travaux de génie civil
- Réalisation de checkpoints pour un contrôle d'accès optimal des véhicules sur un site provisoire

CARACTÉRISTIQUES PRINCIPALES

- Largeur de passage : 3 mètres
- Sans génie civil
- Poids : 5,5 T
- Centrale hydraulique 220/380VAC (commande manuelle de secours)
- Traitement anticorrosion et revêtement polyester par thermo-laquage
- Possibilité d'asservissement avec systèmes existants

BÉNÉFICES PRINCIPAUX

- Pas de génie civil
- Mise en place extrêmement rapide
- Robuste

COÛT D'ACQUISITION
Catégorie B
50 à 100 k€
(en fonction des options)

COÛT D'USAGE
visites de maintenance préventive (2 par an en moyenne)
2000 € à 3000 € /an /accès pour une garantie totale (pièces + MO) en IDF.

TALOS KOPP
70 Rue du Général Malleret Joinville
94400 VITRY SUR SEINE
Téléphone : 01 49 40 09 04

DOMAINE PROTECTION PÉRIMÈTRIQUE

PRODUIT : PLAKOSOL ULTIMA RATIO : protection anti véhicules béliers

- Obstacle anti-véhicules suicides
- Système de protection physique des accès véhicules
- Réalisation de checkpoints très haute sécurité pour un contrôle d'accès optimal des véhicules sur un site

CARACTÉRISTIQUES PRINCIPALES

- Largeur de passage : infini (système modulaire)
- Profondeur du châssis encastré : 40cm
- Centrale hydraulique 220/380VAC (commande manuelle de secours)
- Traitement anticorrosion et revêtement polyester par thermo-laquage
- Possibilité d'asservissement avec systèmes existants

BÉNÉFICES PRINCIPAUX

- Très haute performance d'arrêt
- Centrale hydraulique déportée
- Robuste

COÛT D'ACQUISITION
Catégorie A
0 à 50 k€
(en fonction du nombre de modules)

COÛT D'USAGE
visites de maintenance préventive (2 par an en moyenne)
2000 € à 3000 € /an /accès pour une garantie totale (pièces + MO) en IDF.

Antoine GRYCZKA
Directeur technico-commercial / sales technical manager
antoine.gryczka@mc2-technologies.com
Mobile : +33 (6) 88 79 39 01

DOMAINE PROTECTION PÉRIMÈTRIQUE

www.mc2-technologies.com

PRODUIT : Système de neutralisation des drones

- UAV Scrambler
- Système de brouillage et neutralisation de drones.
- Protection des zones critiques.

CARACTÉRISTIQUES PRINCIPALES

- Brouillage des systèmes de communication des drônes
- Décliné en version mobile ou fixe.
- Dimensions : 100x25x25 cm ; Poids : <10kg

BÉNÉFICES PRINCIPAUX

- Système de neutralisation efficace dont les performances ont été approuvées par les autorités Françaises.
- Autonomie de 8h pour la version mobile.

COÛT D'ACQUISITION

Catégorie A
< **50 K€**

3 rue BUFFON, 91400 ORSAY
08 20 20 08 39
pbernas@evitech.com

DOMAINE DÉTECTION SURVEILLANCE

www.evitech.com

PRODUIT : Détection et analyse de comportement individu isolé - Détection feux et hydrocarbures

- Détection d'intrusion en site sensible (surveillance périmétrie) par **analyse vidéo intelligente**
- Analyse de comportement dans le site
- Détection de départs de feux et de fuites d'hydrocarbures
- Tracking fin (dôme asservi)

CARACTÉRISTIQUES PRINCIPALES

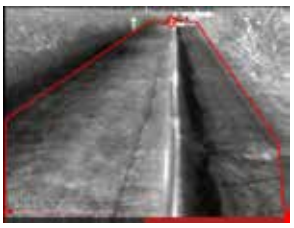
- Logiciel d'analyse d'images des caméras de vidéo protection
- Format serveur ou petits boîtiers indépendants, cyber-sécurisés,
- Intégration dans les systèmes de sécurité existants

BÉNÉFICES PRINCIPAUX

- Détection et suivi de toute cible visible à l'image (même loin)
- Très faible taux de fausses alarmes (0.5 / jour . Caméra)
- Equipe les centrales nucléaires, le port de Lyon, des raffineries telles que TOTAL, des centrales thermiques, sites gaziers …

COÛT D'ACQUISITION (pour un site de 500 m x 200 m)
Catégorie A
0 à 50 k€

Prix par nombre de caméras surveillées (compter 1 K€ / caméra),
~10-15 K€ livré configuré pour un petit site industriel de 500 x 200 m
~50-100 K€ livré configuré pour un grand site industriel



Intrusion

Comportement

détection feux / Hydrocarbures

3 rue BUFFON, 91400 ORSAY
08 20 20 08 39
pbernas@evitech.com

DOMAINE DÉTECTION SURVEILLANCE

www.evitech.com

PRODUIT : Comptage, détection et analyse de comportement foule

- Comptage de personnes (flux, densité)
- Détection de comportements dans la foule (contresens, panique,attroupements, …)
- Détection de fumées (fumigènes, feux, lacrymo…)

CARACTÉRISTIQUES PRINCIPALES

- Logiciel d'analyse d'images des caméras de vidéo protection sur des zones largement fréquentées
- Format serveur ou petits boîtiers indépendants, cyber-sécurisés,
- Intégration dans les systèmes de sécurité existants

BÉNÉFICES PRINCIPAUX

- Analyse de la foule même en foules denses
- Temps réel et statistiques journalières
- Equipe des sites majeurs à risques à l'international

COÛT D'ACQUISITION
Catégorie A
0 à 50 k€

Prix par nombre de caméras surveillées (compter 1 K€ / caméra),
~10-15 K€ livré configuré pour une petite installation (10 caméras)
~50-100 K€ livré configuré pour un grand site (100 caméras)

Comptage flux, densité

Comportement isolé

Panique

Fumée

6 rue du Dauphiné, 69120 Vaulx-en-Velin
+33 (0)4 27 11 80 30
contact@foxstream.fr

DOMAINE
DÉTECTION
SURVEILLANCE

www.foxstream.fr

PRODUIT : Détection d'intrusion en milieu extérieur

Détection d'intrusion pour protection périmétrique d'un bâtiment ou d'un site

CARACTÉRISTIQUES PRINCIPALES

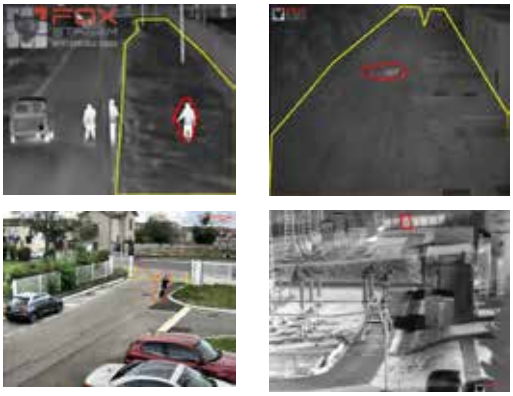
Détection automatique via analyse vidéo dans une zone prédéfinie / filtrage des fausses alarmes / transmission de l'alarme avec séquence vidéo enrichie du détourage / intégration dans les superviseurs, hyperviseurs et frontaux de télésurveillance / gamme sur serveur, en « box », embarquée
Autres fonctions : franchissement de ligne, détection de maraudage, bagage abandonné, lecture de plaques

BÉNÉFICES PRINCIPAUX

- Détection efficace et levée de doute immédiate / preuve vidéo
- Installation et paramétrage rapides et simples
- Fonctionnement en autonome ou intégré à des logiciels de supervision ou relié à la télésurveillance.

COÛT D'ACQUISITION

Vente de licences par caméra / Pour 4 caméras thermiques : analyse Foxstream-installation-formation Foxstream : le tout à 20-25 k€, fonctionnement : 10% du coût d'acquisition par an



Green Communications
86 rue de Paris – 91400 Orsay – France
contact@green-communications.fr

DOMAINE
DÉTECTION
SURVEILLANCE

www.green-communications.fr

PRODUIT : Infrastructure Internet Mobile Green PI

Infrastructure Internet mobile et sur batteries déployable à la demande pour étendre la couverture d'un réseau 4G dans un tunnel, un bâtiment ou pour connecter des zones isolées.
Présentation vidéo : https://youtu.be/2feJpTlSz7k.

CARACTÉRISTIQUES PRINCIPALES

- Un ensemble de YOI, routeurs Mesh basse consommation
- Un routeur YOI-4G/LTE équipé d'un modem 4G
- Des batteries 10 Ah de 20 h d'autonomie
- Des services locaux, hébergés dans les routeurs

(vidéo, voix, chat, web, échange de fichiers, etc.)

BÉNÉFICES PRINCIPAUX

- Créer une infrastructure de télécommunication en quelques minutes
- Travailler en autonomie grâce aux services hébergés dans le réseau
- Accéder à Internet par Ethernet ou 4G

COÛT D'ACQUISITION

Catégorie A - 0 à 50 k€
Modèle de vente : Vente de produits et de service de maintenance

Routeur Mesh basse consommation (5W)

Infrastructure Internet Mobile Green PI

HGH Systèmes Infrarouges
01 69 35 47 70 – Edouard Campana
edouard.campana@hgh.fr

DOMAINE
DÉTECTION
SURVEILLANCE

PRODUIT : Surveillance panoramique infrarouge

- Gamme de système de surveillance panoramique : capteur infrarouge thermique Spynel et logiciel de détection et tracking Cyclope
- Détection d'intrusion et surveillance de zone terrestre ou maritime
- Utilisable en mono ou multi-capteurs, intégré ou non à des plateformes

CARACTÉRISTIQUES PRINCIPALES

- Portée de détection de quelques centaines de m jusqu'à 8 km (homme marchant) / couverture horizontale 360° - verticale de 5° à 35°/ rafraîchissement 1s
- Détection de cibles terrestres, maritimes ou aériennes (y.c. drones)
- Fonctions hyperviseur / enregistrement / rejeu

BÉNÉFICES PRINCIPAUX

- Rapport coût/performance optimal
- Fonctionnement passif
- Détection / tracking automatique et anticipation des intrusions
- Nombreuses fonctionnalités et grande souplesse de configuration

COÛT D'ACQUISITION
De moins de 50k€ jusqu'à 500 k€ selon version et configuration

Bernard Leibovici, Groupe SDS - IMS
Innovation and Mesaurement Systems
53 rue Bourdignon
94100 Saint-Maur-des-Fossés - France
06 73 52 18 80 - b.leibovici@groupesds.com

DOMAINE
DÉTECTION
SURVEILLANCE

www.imsrad.com

PRODUIT : Solution CODI-NR

- Détection et identification des sources de radiation générées par des dispositifs artificiels tels que les dispositifs nucléaires improvisés (improvised Nuclear Devices) ou les dispositifs de dispersion radiologique (Radiological Dispersal Devices) :
- Assurer la sécurité des sites sensibles
- La détection et d'identification des matières nucléaires et radiologiques
- Une solution portable, efficace et communicante
- Portée par les personnes en charge de la sûreté et de la sécurité
- Permettant d'engager rapidement les actions de prévention et de protection nécessaires.

CARACTÉRISTIQUES PRINCIPALES

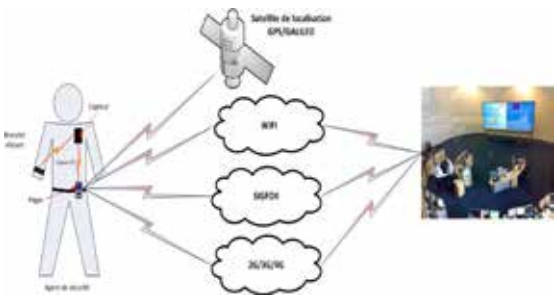
- Une solution ultra-miniaturisée
- Détection, identification et localisation de la source radioactive.

BÉNÉFICES PRINCIPAUX

la lutte contre le terrorisme nucléaire dans les zones de commerce, de loisirs et de transport, les administrations, dans un contexte de rassemblement ou de passage de personnes.

COÛT D'ACQUISITION

100 K€ pour 10 ensembles communicants complets



Synopsis solution intégrée NRBC

LUCEOR
WIMESH NETWORKS

Tél : 01 84 73 13 00
contact@luceor.com

DOMAINE
DÉTECTION
SURVEILLANCE

PRODUIT : Réseau sans fil pour la protection de sites sensibles

- Raccordement de caméras de vidéo surveillance HD
- Connexion à haut débit de véhicules, de drones, de robots et de personnels
- Raccordez n'importe quel équipement IP, partout où vous en avez besoin

CARACTÉRISTIQUES PRINCIPALES

- Réseau privé/dédié donc très haute qualité de services/de disponibilité
- Transmissions très hauts débits (jusqu'à 600Mbits/s)
- Mobilité des équipements même à très haute vitesse (plus de 300km/h)
- Réseau résilient, auto-cicatrisant, auto-configurable

BÉNÉFICES PRINCIPAUX

- Déployer vos équipements de sécurité même là où il n'y a pas de réseau
- Couverture de très grands sites sans avoir besoin de tirer des câbles
- Entièrement compatible et interopérable avec les réseaux IP existants

COÛT D'ACQUISITION

Catégorie A 0 à 50 k€
Catégorie B 50 à 100 k€
(selon la taille du site et le nombre de capteur à raccorder)

COÛT D'USAGE

Aucune licence due pour l'utilisation du spectre radio
Aucun abonnement opérateur

MODÈLE ÉCONOMIQUE

Investissement selon le nombre de routeurs et le débit de transmission nécessaire
Déploiement via un intégrateur système
Contrat annuel de support et de maintenance

mc2 technologies

Antoine GRYCZKA
Directeur technico-commercial / sales technical manager
antoine.gryczka@mc2-technologies.com
Mobile : +33 (6) 88 79 39 01

DOMAINE
DÉTECTION
SURVEILLANCE

www.mc2-technologies.com

PRODUIT : Scanner corporel passif dédié à des contrôles de sécurité

- MM-Imager
- Technologie de système d'imagerie radiométrique à ondes millimétrique.
- Dédiée à la détection d'objets cachés par les personnes sous les vêtements.

CARACTÉRISTIQUES PRINCIPALES

- Caméra radiométrique Térahertz passive.
- Détection automatique des objets suspects.
- H: 170cm, L: 75cm, l: 78cm ; Poids : 160 kg, selon les options

BÉNÉFICES PRINCIPAUX

- Ce système mesure les ondes hyperfréquences émises, réfléchies et transmises par les objets et le corps humain. Il est totalement passif ce qui le rend totalement sans danger pour les personnes scannées et les opérateurs.
- Peut travailler jusqu'à 10m de distance.
- Installation et prise en main faciles.

COÛT D'ACQUISITION

Catégorie B
Entre **100 et 250 K€**

COÛT D'USAGE

Maintenance préventive à déterminer en fonction des quantités prises.

Mirion Technologies (MGPI) SA
M. Bruno Morel
Email : bomorel@mirion.com
Tel : 04 90 59 60 20
Mobile : 06 16 24 50 79

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : Détection radiologique d'entrée de site - Lutte contre l'intrusion de matière radioactive illicite

Détection de tentative d'introduction de matière radioactive sur le site
Protection permanente des accès piétons et véhicules

CARACTÉRISTIQUES PRINCIPALES

Détecte et analyse l'activité supérieure au bruit de fond naturel
Identification des isotopes en temps réel / ségrégation entre danger réel et isotopes médicaux ou naturels
Le système est automatique et peut être rendu discret
Conforme à la norme Ansi N42-38

BÉNÉFICES PRINCIPAUX

Protection totale des accès – alarme locale et distante / adaptable avec couts d'infrastructure limités
Collecte d'indices et de preuves complètes sur alarmes (caméra, …)
Pas de compétences spécifiques nécessaires sur le site / auto-calibration
Supervision centralisée de plusieurs sites possible

COÛT D'ACQUISITION

Moins de 50 k€ pour un accès piéton (1 Spir-Ident piéton)
Moins de 100 k€ pour un accès véhicule (2 Spir-Module)
Alternative : location longue durée

Colonne « Spir-Ident piétons »

Interface exploitant simplifiée

Possible supervision et/ou accès expert à distance

Système modulaire « Spir-Module » pour accès véhicules

Jean-Frédéric REAL
jean-frederic.real@scalian.fr
06.14.40.66.83

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : DataScaleABDetect

Détection d'événement anormaux dans les flux de vidéosurveillance par réseaux de neurones profonds

CARACTÉRISTIQUES PRINCIPALES

Solution de détection basé sur l'état de l'art de l'IA (basé sur l'analyse de chaque image / robuste au tilt)
Apprentissage de comportements normaux et anormaux (mauvais sens, arrêt brusque, regarder autour, courir, …)
Mise en place de seuils d'alerte et règles d'aide à la décision configurable (configurable par un non spécialiste / visualisation en temps réel des alertes) / sauvegarde sur plusieurs mois / outil de visualisation des vidéos indexées

BÉNÉFICES PRINCIPAUX

Rapidité des remontées des alertes / Qualification des évènements grâce aux flux vidéos / Annotation automatique des vidéos / Notifications sur zone d'alerte / Aide à l'action efficace et précise

COÛT D'ACQUISITION

Plateforem Datascale : licence par nœud de stockage 7k€
Cout de Module ABDetect : licence annuelle 7k€

DATASCALE ABDetect

SCALIAN
A BRIDGE TO PERFORMANCE

Jean-Frédéric REAL
jean-frederic.real@scalian.fr
06.14.40.66.83

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : System Long Eyes

Association d'un véhicule d'intervention et d'un drone.

CARACTÉRISTIQUES PRINCIPALES

Drone en vol automatique, asservi au véhicule, pas de besoin de pilote qualifié
Autonomie jusqu'à 8 heure par alimentation / communication filaire
Possibilité de libérer le drone pour qualifier la cible au plus près

BÉNÉFICES PRINCIPAUX

Reconnaissance automatique de forme / rapidité d'intervention / sécurité de communication / autonomie / modularité du système et des capteurs / facilité d'utilisation - possibilité d'effectuer des missions en vol automatique / opérable en zones reculées grâce à la voie filaire

COÛT D'ACQUISITION

50 à 100 k€ sans véhicule + customisation selon la mission. Acquisition par briques possible.

sysnav
NAVIGATION TECHNOLOGIES

M. David Vissière,
Président
david.vissiere@sysnav.fr
02 78 00 10 91

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : Sysnav Tracking

Suivi de véhicule collaboratif ou non, indépendant de toute infrastructure, y compris du GPS / suite logicielle pour utilisation optimisée / position en temps réel ou en post traitement.

CARACTÉRISTIQUES PRINCIPALES

Autonomie supérieure à 3 mois / dimensions réduites
Intégration possible sur plateformes logicielles externes
Fonctionnalités multiples gérées au niveau balise et serveur (geofencing, alertes, évènements, …)

BÉNÉFICES PRINCIPAUX

- Disponibilité : information calculée en toutes circonstances et en tout environnement
- Précision : algorithme magnéto-inertiel précis au mètre près
- Intégrité : localisation inviolable, pas de brouillage ou leurrage possible

COÛT D'ACQUISITION

100 à 250 k€ pour 100 balises

COÛT D'USAGE

0 à 50 k€ de licence annuelle pour logiciel et abonnement pour remontée de données en France Métropolitaine

M. David Vissière,
Président
david.vissiere@sysnav.fr
02 78 00 10 91

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : Sysnav Pieton BFT

Suivi de personne, indépendant de toute infrastructure, y compris du GPS
Équipement de localisation porté, complété par une API logicielle
Position en temps réel et en post traitement (preuve juridique/ assurance).

CARACTÉRISTIQUES PRINCIPALES

Équipement léger : 100g / visualisation sur smartphone & tablette / communication Bluetooth, 868 MHz, Dect / autonomie importante (20h de marche)
Fonctionnalités multiples gérées au niveau équipement et serveur (pertes de verticalité, alertes, …)

BÉNÉFICES PRINCIPAUX

Précision : algorithme magnéto-inertiel précis au mètre près, 30 cm lorsque les plans sont disponibles
Intégrité : localisation inviolable, pas de brouillage ou leurrage possible
Disponibilité : information calculée et disponible en permanence à haute fréquence (jusqu'à 125 Hz)
Sécurité : l'utilisateur est informé mais ne peut pas neutraliser le capteur sans que l'employeur soit au courant.

COÛT D'ACQUISITION

0 à 50 k€ pour 10 équipements

COÛT D'USAGE

0 à 50 k€ de licence annuelle hors cout de mise en œuvre pour la 1ère utilisation

Thales
jean-pierre.vidal@thalesgroup.com

DOMAINE DÉTECTION SURVEILLANCE

PRODUIT : T-Smart Badge

Badge virtuel sur smart-phone pour les non-permanents sur un site

CARACTÉRISTIQUES PRINCIPALES

- Enrôlement délocalisé des visiteurs et autres non-permanents
- Support unique multi-badges
- Gestion centralisée avec capacité à maitriser dynamiquement les droits
- Suivi permanent et localisé de présence sur site

BÉNÉFICES PRINCIPAUX

- Support unique multi-domaines
- Droits contrôlables à distance
- Convivial pour le porteur

COÛT D'ACQUISITION

Non renseigné

CONTRÔLE D'ACCÈS / ZONAGE

Deveryware - 43, rue Taitbout - F-75009
Paris Standard : +33 1 80 90 54 80

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : DataScaleABDetect

NoticoSafe - NoticoPro : Alerte et information des professionnels et populations
Shale : Gestion flux 112 nouvelle génération - Adda : Plateforme de tracking sur site sécurisé.

Localisation de personnes dans une zone déterminée pour l'échange bidirectionnel d'informations et alerte des services de secours.
Exploitation d'informations de localisation pour suivi temps réel,

CARACTÉRISTIQUES PRINCIPALES

Gestion des alertes vers les services de secours (Ghale) les salariés ou équipes de sécurité et les populations dans une zone déterminée (NoticoSafe – Noticopro),
Suivi de visiteurs dans une zone réglementée, avec gestion des alertes (Adda).

BÉNÉFICES PRINCIPAUX

Anticipation des évènements,
Alerte des acteurs et intervenants directs.

COÛT D'ACQUISITION
inférieurs à 50 k€

Viviane BRETAGNE
Directeur Commercial & Business Développement
viviane.bretagne@gunnebo.com
Mobile : +33 (6) 73 87 33 50

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : SMI Server

Système intégré de management de la sureté :
contrôle d'accès, intrusion, vidéo protection

CARACTÉRISTIQUES PRINCIPALES

- Gestion des identités et des droits d'accès
- Contrôle de l'unicité de passage
- Système qualifié ANSSI

BÉNÉFICES PRINCIPAUX

- Faciliter l'exploitation de la sureté par une gestion unifiée des systèmes
- Assurer une gestion effective des passages pour connaitre la liste des présents en zones
- Gérer la traçabilité et consolider les historiques

COÛT D'ACQUISITION

Système de contrôle d'accès	1 à 3 k€ par accès
Système de vidéo-protection	0 à 5 k€ par caméra
Contôle d'unicité de passage	0 à 5 k€ par accès

CONTRÔLE D'ACCÈS / ZONAGE

MAPLE High Tech - 42, avenue du général de Croutte – 31100 Toulouse
Mobile: +33 6 07 43 83 46

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : GPS d'intérieur de précision MyFency

Suivi de personnes (visiteurs…) avec gestion des alertes en temps réel sur cartographie au moyen de la technologie Wireless FencyTag.

CARACTÉRISTIQUES PRINCIPALES

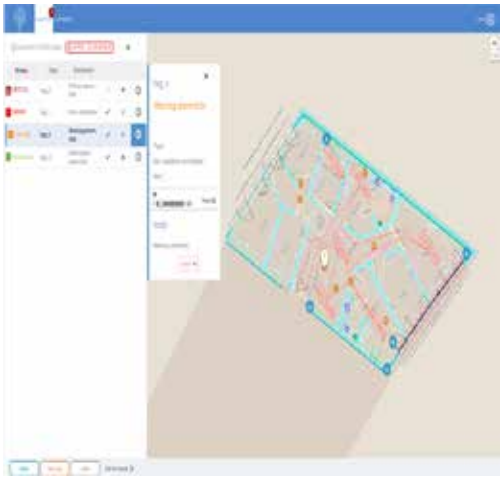
- Robuste aux environnements fortement contraints
- Localisation 2D/3D en temps réel (+/- 30 cm) de centaines de personnes dans plusieurs pièces, sur plusieurs étages de bâtiments
- Création de zones de geofencing,
- Réception et gestion de tous types d'alarmes et alerte des acteurs.

BÉNÉFICES PRINCIPAUX

- Sécurisation de personnes, de sites classés, de zones sensibles et points d'accès
- Interface générique avec tout type d'outil de surveillance existant

COÛT D'ACQUISITION

De 5 à 50 k€ (selon volumes et configuration)



RESOCOM MTM
6 rue Neuve Saint-Pierre,
75004 Paris
09 69 32 13 77

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT :

- Simple, intuitive et sécurisée, sur place ou en mobilité,
- Analyse automatique des sécurités et des informations ou signes portés sur un document,
- Automatisation des analyses et gestion des alertes en temps réel.

CARACTÉRISTIQUES PRINCIPALES

- Contrôle par saisie guidée des données sur une page dédiée (VériConsult)
- Ou au moyen d'un scanner de bureau ou spécifique (Résocan), d'un mobile ou d'une tablette (Résoboard).
- Vérification de cohérence en quelques secondes.
- Emission d'un certificat de conformité ou non-conformité.

BÉNÉFICES PRINCIPAUX

- Sécurisation des accès par une action de contrôle et de vérification des documents,

COÛT D'ACQUISITION

Inférieur à **50 k€**

COÛT D'USAGE :

Environ **0,60 euros la consultation**

SURYS

SURYS
SAM GUETTA
s.guetta@surys.com
06.76.72.24.97

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : SOLUTION D'AUTHENTIFICATION KEESING AUTHENTISCAN LITE

- Scan, Authentification et Archive de copies de document d'identité en quelques secondes
- Contrôle automatisée de la MRZ et comparaison du document avec la base de données Keesing DocumentChecker

CARACTÉRISTIQUES PRINCIPALES

- Authentification des copies des documents d'Identité
- Lien direct avec le centre d'aide Keesing

BÉNÉFICES PRINCIPAUX

- Lecteur de passeport non nécessaire
- Comparaison avec la base de données Keesing DocumentChecker

COÛT D'ACQUISITION
-

COÛT D'USAGE : (pour un contrôle de 100 000 documents par an)
1 € par contrôle

SURYS

SURYS
SAM GUETTA
s.guetta@surys.com
06.76.72.24.97

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : FILM HOLOGRAPHIQUE OPTOSEAL® ULTRA POUR PROTECTION DES CARTES PLASTIQUES

- Lamina holographique de très haute sécurité avec technologie DID™
- Technologie DID™ permettant une authentification immédiate grâce à une permutation de couleur unique lorsque le document est tourné à 90°
- Protection des données variables contre la falsification

CARACTÉRISTIQUES PRINCIPALES

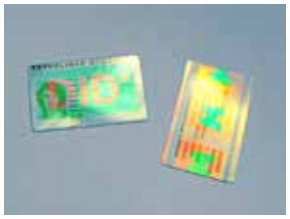
Compatible avec les 3 niveaux de sécurité (Overt, Covert, Forensic)

BÉNÉFICES PRINCIPAUX

- Difficile à contrefaire, facile à authentifier
- Design personnalisé

COÛT D'ACQUISITION
(pour 100 000 cartes émises)

Catégorie B
50 à 100 k€



CONTRÔLE D'ACCÈS / ZONAGE

SURYS

SURYS
SAM GUETTA
s.guetta@surys.com
06.76.72.24.97

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : SOLUTION D'AUTHENTIFICATION PHOTOMETRIX™

- Authentification automatisée locale du portrait du titulaire de la carte
- Le code Photometrix™ permet un contrôle étendu lorsque des caractéristiques spécifiques du titulaire de carte sont stockées dans le code (empreinte digitale, éléments de reconnaissance faciale). Cette option, par le biais du contrôle de base, relie une image authentifiée à une personne physique.

COÛT D'ACQUISITION
(pour 100 000 cartes émises)

Catégorie B
50 à 100 k€

COÛT D'USAGE
Montant forfaitaire annuel pour la maintenance de la solution
Durant l'émission des cartes : 20 000 €/an
A l'issue de l'émission des cartes : 40 000 €/an

CARACTÉRISTIQUES PRINCIPALES
Intégration d'une signature numérique dans un code barre 2D sécurisé

BÉNÉFICES PRINCIPAUX

- Authentification automatisée locale
- Possibilité de relier une image authentifiée à une personne physique

SURYS

SURYS
SAM GUETTA
s.guetta@surys.com
06.76.72.24.97

DOMAINE
CONTRÔLE D'ACCÈS
ZONAGE

PRODUIT : ETIQUETTE HOLOGRAPHIQUE POUR PARE-BRISE HOLOCIS™ ET PLAQUES D'IMMATRICULATION (en option)

- Etiquettes de haute sécurité sérialisées ou personnalisées sur demande
- Etiquettes pour plaques d'immatriculation (en option)

COÛT D'ACQUISITION
(100 000 étiquettes de pare-brise)

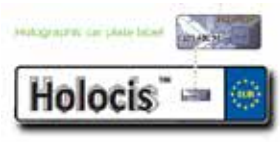
Catégorie B
50 à 100 k€

CARACTÉRISTIQUES PRINCIPALES

- Résistant à la manipulation (effet VOID)
- Identification immédiate du véhicule

BÉNÉFICES PRINCIPAUX

- Facile à implémenter
- Facile à authentifier



ALERTE INTERNE ET EXTERNE

CAIGNAULT Vanessa
Co-fondatrice & Directrice Générale
03 44 37 05 96 - 06 01 19 21 54
Email : vanessa.caignault@novitact.com

DOMAINE
ALERTE INTERNE
ET EXTERNE

PRODUIT : FEELTACT et ses applications

FEELTACT est une solution de bracelet connecté pour alerte discrète (bracelet, application mobile associée, interface web d'administration et supervision) pour professionnels à risque en zones sensibles ou travailleurs isolés.

CARACTÉRISTIQUES PRINCIPALES

Connecté par Bluetooth à un smartphone, le bracelet permet d'émettre jusqu'à 4 messages par pression de boutons et d'en recevoir sous forme de vibration autour du poignet
Autres fonctionnalités : géolocalisation, écoute passive, alertes automatiques de type DATI

BÉNÉFICES PRINCIPAUX

Solution d'alerte discrète et à portée de main / envoi-réception temps réel libérant l'attention visuelle et sonore.
Communication simultanée avec plusieurs personnes.

COÛT D'ACQUISITION

Matériel : 347€ / unité, fonctionnement 87€/an/unité, configuration des comptes : 200€ par site pour 1 à 10 comptes.

Jean-Frédéric REAL
jean-frederic.real@scalian.fr
06.14.40.66.83

DOMAINE
ALERTE INTERNE
ET EXTERNE

PRODUIT : Eyesecure

Eyesecure est une solution de sécurité globale qui permet la connexion de toutes les parties prenantes sur les gestions d'alerte sur un territoire donné quels qu'ils soients

CARACTÉRISTIQUES PRINCIPALES

Solution de sécurité collaborative
Gestion des incidents : qualification rapide et précise (messages – photos – videos – géolocalisation), interventions rapides et adaptées, meilleure couverture des alertes
Politique de sureté de l'opérateur : outil complémentaire aux moyens existants

BÉNÉFICES PRINCIPAUX

Rapidité des remontées d'alerte
Notification collective sur zone d'alerte
Cout marginal : les usagers assurent une fonction sur leurs smartphones
Déploiement et couverture progressifs

COÛT D'ACQUISITION

Abonnement au service pour opérateurs ou responsables d'usagers : entre 0 et 50k€ à l'année

AIRBUS

Lionel Maes
Airbus Defence and Space
lionel.maes@airbus.com

DOMAINE SUPERVISION ET CYBER

PRODUIT : Solution Tactical C2

Système d'information présentant la situation du site :

- Surveillance du site : alerte, position des personnels, traccking des menaces, corrélation des alertes (ex cyber et physique)
- Intégration des informations : camera de drones, capteurs du batiment (camera, RFID, …), capteurs cyber

CARACTÉRISTIQUES PRINCIPALES

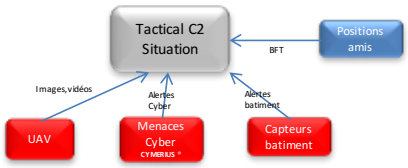
Situation 3D avec symbologie / réseaux sociaux / bandeau temporel
Formation multi-acteurs / capacité de rejeu / scénarios
Communication : messagerie, chat, interface téléphonie fixe et mobile

BÉNÉFICES PRINCIPAUX

Centralisation des informations multi-capteurs / outils de représentation / permet la vue temps réel et l'analyse temps différé

COÛT D'ACQUISITION

Licences d'utilisation par poste opérateur, prix en fonction des fonctionnalités et du volume. Possibilité de différencier les licences pour tablettes et pour le site central.
Contrat de maintenance pluri-annuel



DIGINEXT
be visionary

DIGINEXT,
Alain CARTAULT
+33 6 44 10 42 51
alain.cartault@diginext.fr

DOMAINE ALERTE INTERNE ET EXTERNE

crimson.diginext.fr

PRODUIT : CRIMSON

Avec CRIMSON, DIGINEXT propose une solution collaborative de surveillance de sites disponible H24, configurable, que ce soit pour la gestion opérationnelle de crise ou la préparation aux plans de protection. CRIMSON répond aux besoins suivants :

- Surveillance opérationnelle de site
- Hypervision multi capteurs (PSIM)
- Gestion de crise
- Formation / entraînement

CARACTÉRISTIQUES PRINCIPALES

Solution collaborative carto-centrée 2D/3D disponible sur PC et mobiles
Partage discriminé de l'info en multi-sites, multi-niveaux, interservices
Mains courantes et tableaux de bords métiers et partagés
Interopérabilité avec systèmes existants et normes NF399, EDXL…
Multiréseaux (3G/4G, bulle LTE, Wifi, Wimesh…)
Historisation horodatée pour rejeu à chaud et debriefing
Haute disponibilité et résilience de la solution

BÉNÉFICES PRINCIPAUX

Faciliter la prise de décision, fluidifier la transmission des ordres
Améliorer la préparation des équipes de surveillance et d'intervention
Identifier les bonnes pratiques en matière de sécurité et sûreté

COÛT D'ACQUISITION

Devis détaillé sur demande, prix entre **10 et 250 k€** en fonction du nombre de licences. Possibilité d'abonnement annuel.

Egidium Technologies
Tel : 0177932127
contact@egidium-technologies.com

DOMAINE SUPERVISION ET CYBER

PRODUIT : Smart Shield pour la protection de sites sensibles

- Supervision coordonnée des moyens technologiques et humains
- Adaptée à l'amélioration continue et l'ajout de nouveaux capteurs
- Déjà adoptée par de grands sites sensibles et grands événements (StadeFrance, CEA, EDF, Salon du Bourget, Cité Interdite Pékin…)

CARACTÉRISTIQUES PRINCIPALES

- Vision globale de la situation à tout instant (fusion des données capteurs sur synoptique 3D du site)
- Assistance à l'opérateur pour la levée de doute et le suivi d'intrus
- Fonctions mobiles pour les agents de sécurité
- Traçabilité complète des événements

BÉNÉFICES PRINCIPAUX

- Agilité (compatible tous systèmes et capteurs, rapide à déployer)
- Efficacité (user-friendly, outil d'aide à la décision et de retex)
- Retour sur investissement (totalement évolutif)

COÛT D'ACQUISITION
(coût pour un site, selon superficie, nombre et variété de capteurs et systèmes interfacés)

Catégories
B à D
50 à 500 k€

COÛT D'USAGE :
(pour un site)

Modèle classique:
via intégrateur système
Upfront: license + intégration/ tests sur site + formation
Récurrent:maintenance logicielle 15% de la license / an

175 rue de Massacan
34740 Vendargues
04 67 87 46 46
contact@hymatom.fr

DOMAINE ALERTE INTERNE ET EXTERNE

PRODUIT : Plateforme logicielle Visiospace

Plateforme logicielle Visiospace : fédère, via une cartographie multi-couches, des systèmes de sécurité dont la vidéo. Gère de façon géolocalisée le contenu des images des caméras, les alarmes et événements , les intervenants.

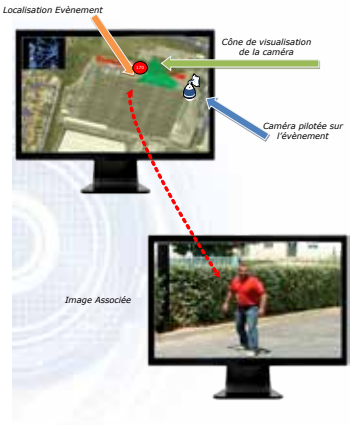
CARACTÉRISTIQUES PRINCIPALES

Représentation dynamique des zones visualisées avec localisation et qualification des intrusions et objets géolocalisables / incrustation d'objets / tracking automatique de personne ou véhicule / interface avec 150 protocoles de sécurité (contrôle d'accès, incendie, éclairage, …)

BÉNÉFICES PRINCIPAUX

Opérateur assisté en temps réel ou/et système de suivi complètement automatisé.
Recherches facilitées : les évènements et contenus vidéo sont géo-localisés à l'enregistrement.

COÛT D'ACQUISITION
Cout d'acquisition de base inférieur à 50 k€, et plus selon la quantité d'équipements gérés.



SUPERVISION ET CYBER

Société IGO Immeuble NIMAXIS. 78 rue John Mac Adam. 30900 NIMES.
Contact : philippe.bour@igo.fr
+33 (0)6 11 58 69 19

DOMAINE SUPERVISION ET CYBER

www.igo.fr

PRODUIT : Cartographie Opérationnelle 3D – Supervision des capteurs

- Plateforme logicielle 3D en capacité d'interagir avec une cartographie 3D très détaillée (d'un site, d'un territoire) et l'ensemble des capteurs fixes et mobiles de surveillance.
- Solution collaborative d'aide à la décision et d'aide à la gestion de crise.
- Sureté d'actifs sensibles.

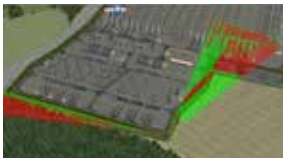
COÛT D'ACQUISITION
(pour un site d'une dizaine de km²)

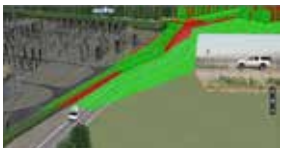
Catégorie C
100 à 250 k€

COÛT D'USAGE
A préciser :
licence d'utilisation

CARACTÉRISTIQUES PRINCIPALES

- Numérisation 3D d'un site, d'un territoire,
- Interopérabilité avec les systèmes d'informations et les normes,
- Remontée d'informations géo-localisées issues des systèmes de supervision propre à chaque type de capteurs,
- Partager une situation en 3D,
- Version Réalité Virtuelle et Réalité Augmentée,





BÉNÉFICES PRINCIPAUX

- Contextualisation cartographique en 3D des informations remontées par les capteurs,
- Gestion numérique 3D du patrimoine,
- Vision partagée d'une situation (position temps réel des acteurs,....),
- Interface utilisateur simple et intuitive,
- Aide à l'identification des emplacements des capteurs,
- Aide à la formation

François ROBEYN
+33 (0)6 26 82 30 39
francois.robeyn@secure-systems.net

DOMAINE ALERTE INTERNE ET EXTERNE

PRODUIT : Solution Iperflex

Système de management de la sécurité intégrant : contrôle d'accès, détection intrusion, vidéosurveillance, gestion des droits et des identifiants
Adapté aux sites sensibles, aux applications multi-sites et aux infrastructures critiques / solution ouverte et facilement customisable
Une suite logicielle qui permet de gérer les pré annonces visiteurs, les workflows de demande de droit, de badge, des bornes d'accueil visiteurs, …

COÛT D'ACQUISITION
(pour une configuration 50 accès, 100 caméras, 200 points)

Catégories A à C
0 à 250 k€

CARACTÉRISTIQUES PRINCIPALES

Logiciel : architecture modulaire 4 tiers recommandée par l'ANSSI / liaisons chiffrées /matériels durcis / interfaces multiples (Video Milestone, OPC, LDAP, …)

BÉNÉFICES PRINCIPAUX

- Bon équilibre entre richesse fonctionnelle et simplicité d'utilisation
- Flexibilité / Scalabilité / Sécurité de l'information (cyber proof – ANSSI niveau 1) / Grande disponibilité (électronique robuste, architectures redondantes)

SUPERVISION ET CYBER

Ardanti Défense, François Ardant
+33 (0)6 11 60 14 08
francois.ardant@ardanti.com

DOMAINE
INTÉGRATION
INGENIERIE
CONSEIL

PRODUIT : Maquette Numérique « Protection » 3D du site

- Simulation des menaces d'intrusions, piétons, véhicules, drones etc.
- Implantation virtuelle des protections: infrastructure, capteurs, gardiens
- Prise en compte des conditions jour nuit, météo

CARACTÉRISTIQUES PRINCIPALES

- Jeu de scenarios clés
- Catalogue de menaces, Bases de données de protections
- Maitrise de la confidentialité des informations
- Solution déployée sur plusieurs sites Ministère des Armées

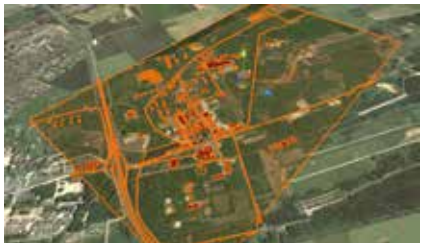
BÉNÉFICES PRINCIPAUX

- Baisse des coûts par analyse de la valeur et approche globale
- Aide à l'identification par algorithmes des vulnérabilité majeures
- Notation des gains globaux des renforcements possibles
- Tableau de Bord décisionnel de renforcement

COÛT D'ACQUISITION

(pour un site d'une dizaine de km2)

Catégories A à C
0 à 250 k€



Maquette Numérique 3D

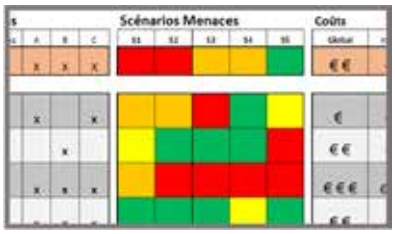


Tableau de Bord décisionnel

Gérard CORREIA
04 42 02 30 88
gerard.correia@secure-systems.net

DOMAINE
INTÉGRATION
INGENIERIE
CONSEIL

PRODUIT

Secure system & services est intégrateur de solution globale pour la protection des sites et des infrastructures critiques. Domaines d'intervention : protection périphérique/périmétrique, contrôle d'accès, vidéosurveillance, vidéo détection, analyse d'image, détection intrusion, gestion des véhicules et des parkings, système de management de l'information, poste de commandement, gestion visiteur, gestion de flux

CARACTÉRISTIQUES PRINCIPALES

Présence sur tout le cycle de vie du projet : gestion de projet, conception, ingénierie, installation, mise en service, maintenance, assistance. En cours de certification MASE et ISO27001.

BÉNÉFICES PRINCIPAUX

Responsabilité globale du projet, en pilotage de toutes les parties prenantes, dans une volonté d'engagement de résultat
Maîtrise du métier de la sûreté appliqué au contexte du métier du client
Offre 'orientée solution', en indépendance avec les fabricants d'équipements

COÛT D'ACQUISITION

-

Spie batignolles Technologies
01 47 12 59 12
stephane.deleville@spiebatignolles.fr

DOMAINE
INTÉGRATION
INGENIERIE
CONSEIL

PRODUIT : Maquette Numérique « Protection » 3D du site

- Offre globale et innovante de sécurisation passive
- Intégration de nouveaux métiers et partenaires d'excellence
- Intégration de solutions présentes et futures.

CARACTÉRISTIQUES PRINCIPALES

- Identification des Menaces via des audits de sécurité, accompagnement
- Evaluation des Parades (Prototypages, simulation)
- Réalisation des Parades (Génie Civil, Mise en place de blindage)
- Anticipation des Menaces

BÉNÉFICES PRINCIPAUX

- Une solution globale de sécurisation basée sur les besoins fonctionnels
- Un interlocuteur unique sur tout le projet de mise en place de la Sécurisation de site

COÛT D'ACQUISITION

Identification des Menaces	
Catégorie A	0 à 50 k€
Evaluation des Parades	
Catégorie C	100 à 250 k€
Catégorie D	250 à 500 k€
Catégorie E	500 à 1.000 k€
Réalisation des Parades	
> 250 K€	

COÛT D'USAGE :

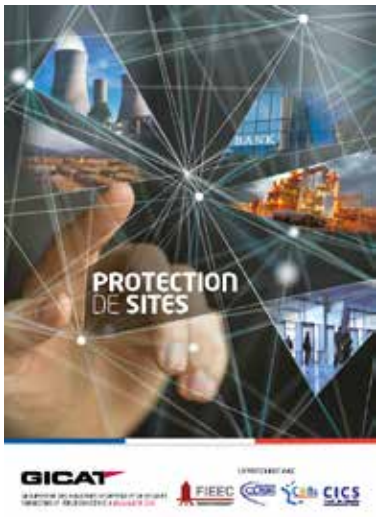
- Co-développement de prototype
- Pas de licences sur les réalisations physiques

MODÈLE ÉCONOMIQUE:

- Investissement lié à la réalisation des parades
- Prestation de conseil pour l'Identification des menaces

BROCHURE CAPACITAIRE DU GICAT

Le GICAT a consacré en 2017 une brochure capacitaire à la protection physique des sites. Cette brochure ne traite pas de la protection humaine, des mesures organisationnelles ou des mesures électroniques ou de cyber-protection. Cette brochure est disponible sur le site du GICAT (www.gicat.fr) et également sur le site du CICS (www.cics-org.fr).



Elle indique que dans tous les cas le dispositif de sécurité devra répondre a minima à huit grandes problématiques :

- Contrôle, identification et authentification : cette fonction a pour but de déterminer qui ou quoi a le droit d'entrer dans le site, ou il a le droit d'aller et de vérifier autant que possible que les identités de ces personnes et objets sont véridiques.
- Dissuasion : Une partie du dispositif doit être visible voire affichée, ceci afin d'afin de décourager les velléités d'actions malveillantes
- Retardement : il est fondamental de retarder l'intrusion ou sa progression ceci afin d'augmenter le délai disponible pour une réaction ou une intervention et les chances de succès de cette dernière. On cherche donc en pratique à élaborer un parcours d'obstacle comprenant de multiples barrières à franchir et d'éléments retardateurs.
- Détection de l'intrusion : cette détection doit être la plus précoce possible pour permettre une intervention efficace et à temps. Elle est en général à double objet : détection d'une intrusion et détection de phénomènes anormaux à l'intérieur du périmètre, tels que des incidents d'exploitation ou des comportements anormaux d'entrants « licites »
- Alerte : remontée d'information relative à une détection vers l'opérateur de sécurité du site. Les indicateurs de performance classiques sont la probabilité de détection (la plus enlevée possible) et la probabilité de fausse alarme (la plus faible possible)
- Analyse et décision : cette fonction centrale doit permettre de comprendre ce qui se passe et de déclencher les mesures appropriées. Elle comprend également souvent les possibilités de remontée de l'Alerte à un niveau supérieur ou l'appel de renforts.
- Intervention : la nature et la forme de l'intervention dépend de l'alerte (feu, intrusion, accident du travail...). Elle doit être la plus rapide et la plus efficace possible.
- Retour à la normale : cette fonction a pour but de pouvoir constater la fin de l'alerte en vue de revenir à l'activité normale.

Capacités présentées	**Protection du périmètre** Surveillance Clôtures et capteurs anti-intrusion Robots de surveillance Protection des voies d'accès physique	**Contrôle d'accès des personnes** Biométrie Contrôle et inspection des véhicules Détection armes et explosifs
Conception et mise en place Audit et conseil Modélisation et simulation Intégration Formation	**Protection de zone** Senseurs d'état Analyse vidéo et fusion de capteurs Pièges	**Exploitation** Communications et coopération Hypervision Protection de l'information Dispositifs d'alerte

CICS
Conseil des Industries
de la Confiance et de la Sécurité

LES TECHNOLOGIES FRANÇAISES AU SERVICE DE LA CONFIANCE ET DE LA SÉCURITÉ

PLUS DE 1000 ENTREPRISES AU CŒUR DE LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ

La sécurité nationale, de la prévention des risques de la vie quotidienne aux situations de crise, exige à chaque instant plus de clairvoyance, de responsabilité et de solidarité. Que nous soyons citoyens, agents ou responsables de collectivités territoriales, élus, représentants de l'Etat ou salariés d'entreprises, ces enjeux nous concernent tous. En France, déjà plus de 1000 entreprises, de la PME au grand groupe, ont décidé de se rassembler sous l'égide du Conseil des Industries de Confiance et de Sécurité (CICS) et au côté de l'Etat, au sein de la filière des industries de sécurité.

POUR UNE POLITIQUE INDUSTRIELLE AMBITIEUSE ET PARTAGÉE !

« Désormais structurée, il convient de rendre cette filière plus forte. En matière d'innovation, de financement de la recherche et d'aide à l'exportation, les synergies entre l'Etat, les collectivités territoriales et les entreprises doivent être recherchées et encouragées. Notre objectif commun est de soutenir durablement une politique industrielle ambitieuse face aux défis croissants de sécurité, dont certains sont déjà au cœur d'enjeux forts de souveraineté. »

Marc Darmon, Président du CICS

LA REPRÉSENTATION INDUSTRIELLE AU COFIS

Cofis — CICS Conseil des Industries de la Confiance et de la Sécurité

membres

ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION · FFMI · FIEEC · GICAN · GICAT · ACN · GIFAS · USP

Le CICS porte la voix de l'industrie dans les domaines de la confiance et de la sécurité et coordonne son action sur quelques grands domaines pour valoriser l'excellence technologique et opérationnelle française, faire converger les efforts de R&T, en France et en Europe autour de programmes structurants ou encore conquérir plus de marchés à l'export. Il contribue au débat institutionnel en proposant à ses partenaires publics et privés des solutions innovantes, cohérentes et efficientes à travers les volets innovation, investissement, législation, réglementation, normalisation, export, souveraineté et Europe.

UNE FILIÈRE D'EXCELLENCE

PLATEFORMES
SOLUTIONS ÉLECTRONIQUES ET NUMÉRIQUES
CYBERSÉCURITÉ

26 MILLIARDS €
DE CA EN 2016

50% À L'EXPORT

+ 4000 ENTREPRISES
DONT **90%** DE PME

150 000
EMPLOIS FORTEMENT QUALIFIÉS

DES
LEADERS MONDIAUX
SUR DES MARCHÉS CLÉS

Le périmètre d'activités du CICS est exhaustif et lui permet de couvrir l'ensemble des problématiques de sécurité, telles que : la protection contre les actes accidentels ou malveillants, la protection individuelle des forces de secours et de sécurité, la protection des infrastructures critiques, la gestion des situations d'urgence et de crise, l'alerte et information des populations, la sécurité urbaine et la vidéoprotection, la protection des transports terrestres, le contrôle des flux et la protection des frontières, la sécurité du numérique et du cyberespace, les solutions d'identité numérique et de biométrie, la lutte contre la fraude et la contrefaçon, les communications sécurisées et la résilience des réseaux, ou encore l'élucidation et traitement des grands volumes de données, ...

www.cics-org.fr - contact@cics-org.fr

CICS

Conseil des Industries
de la Confiance et de la Sécurité

17, rue de l'Amiral Hamelin
75116 PARIS

01 45 05 70 32
jroujansky@cics-org.fr

www.cics-org.fr

CICS

Conseil des Industries
de la Confiance et de la Sécurité

LE CICS A RÉALISÉ CE DOCUMENT AVEC LE COFIS ET AVEC LE PÔLE SAFE.

Le Comité de la filière industrielle de sécurité (CoFIS) a été mis en place par le Premier ministre en octobre 2013. Il a pour ambition de fédérer les efforts de l'État, des collectivités territoriales, de l'industrie, de la recherche et des grands opérateurs publics et privés, pour développer des solutions de sécurité efficaces et mondialement reconnues. La filière agit au sein d'un marché international très porteur qui couvre des sujets aussi divers que la protection des grandes infrastructures publiques et privées, la sécurité des transports, la gestion des frontières, le secours aux personnes, la lutte contre le terrorisme et la grande criminalité, la gestion de crise ou la cybersécurité. Comme tous les comités de filière soutenus par le gouvernement, le CoFIS vise à développer la compétitivité de nos grands groupes et PME, qui occupent sur le marché de la sécurité une place de premier plan.

Le Pôle de Compétitivité SAFE Cluster est positionné sur la filière industrielle de sécurité. Il anime un réseau de 450 acteurs (PME, ETI, Grandes entreprises, Centres de recherche et de formation, utilisateurs finaux) sur toute la France. Ses activités portent sur l'accompagnement à l'innovation, le développement de business, de partenariats technologiques, basés sur une bonne connaissance des usages et des besoins grâce à une grande proximité des utilisateurs finaux (sécurité intérieure, sécurité privée, opérateurs d'infrastructures critiques, Défense). SAFE est membre du réseau des Pôles européens de Sécurité, et collabore aux programmes de recherches et développements de la Commission Européenne et de l'Agence Européenne de Défense.