psm
PROTECTION SÉCURITÉ MAGAZINE
Les Solutions pour les Professionnels de la Sûreté - Sécurité

INCENDIE
DÉTECTION VIDÉO : SOUS CERTAINES CONDITIONS UNIQUEMENT !

n°252
Mars Avril 2019
26 €

entretien

DOMINIQUE LEGRAND
PRÉSIDENT DE L'AN2V
« AUTORISER LA DIVERSIFICATION DES USAGES DE LA VIDÉOSURVEILLANCE. »

vidéosurveillance
LA TRÈS HAUTE RÉSOLUTION : POUR DES APPLICATIONS SPÉCIFIQUES

risque
SITES SENSIBLES ISOLÉS, PROTECTION RENFORCÉE

DOSSIER
FORMEZ ET SENSIBILISEZ VOS SALARIÉS AUX RISQUES !

www.protectionsecurite-magazine.fr

Couleur dans l'obscurité

Caméra full-color pour la vidéosurveillance 24h/24 en couleur

Full-color

- Le capteur Full HD STARVISTM™ et l'objectif à ouverture f1.0 offrent une reproduction des couleurs intense et d'excellentes performances en lumière faible pour une image plus vive et plus lumineuse.
- La lumière blanche intelligente (modèles HAC) sert de source de lumière supplémentaire pour garantir l'exploitation de l'image, même dans l'obscurité totale.
- La technologie 3DNR et le traitement avancé de l'image fournit une image plus claire et réduit le bruit, économisant ainsi de l'espace de stockage.
- La surveillance 24/7 en couleur augmente considérablement la probabilité de recueillir des preuves valides concernant les personnes, les véhicules et les autre preuves.
- Le micro intégré et l'interface audio permettent la collecte audio sur câble coaxial en complément de la vidéo (modèles HAC).
- Solution idéale pour les applications dans des environnements faiblement éclairés, tels que les parcs de stationnement, les rues urbaines, les magasins, les écoles, etc.

Modèles recommandés

IPC-HFW4239T-ASE

Caméra IP full-color
type bullet 1080P

IPC-HDBW4239R-ASE

Caméra IP full-color
type dôme 1080P

HAC-HFW2249E-A-LED

Caméra HDCVI full-color
type bullet 1080P

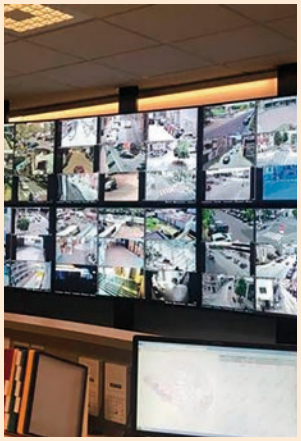
HAC-HDW2249T-A-LED

Caméra HDCVI full-color
type eyeball 1080P

DAHUA TECHNOLOGY FRANCE

Add: 49 Rue Auguste Perret, 94000 Créteil, France
Tel : +33 (0)1 48 53 70 53
Email: sales.france@dahuatech.com
www.dahuasecurity.com

CE FC RoHS ISO 9001:2000


© DR

VIDÉOSURVEILLANCE

SONY ÉQUIPE LA POLICE DE LOKEREN

Pour moderniser son installation de vidéosurveillance, la police de la ville de Lokeren (Belgique) a choisi de se doter de 120 caméras Sony, notamment du mini-dôme SNC-VM772R4K. Le nouveau dispositif, déployé par l'intégrateur Seris Technology, associe des caméras de surveillance réseau Full HD et 4K. Elle se compose également de la plate-forme de gestion vidéo Security center de Genetec. Les caméras Sony sont installées à des emplacements stratégiques, ce qui permet une couverture 24 h/24 et 7 j/7 des rues du centre-ville et des bâtiments publics, y compris du commissariat, de la bibliothèque centrale et de l'hôtel de ville de Lokeren. Grâce aux nouvelles caméras, la police dispose d'une vision plus claire de l'activité criminelle dans les rues de la ville et peut identifier plus facilement les individus suspects, la nuit et dans des conditions de faible luminosité. Les séquences vidéo de la surveillance 24 h/24 sont acheminées via un réseau de fibre optique. Les images sont contrôlées dans le bureau de répartition central, au quartier général de la police.


© DR

DRONES

DPS, PARTENAIRE DE L'ARMÉE DE L'AIR

Le groupe Drone Protect System (DPS) vient de signer un contrat majeur avec l'armée de l'air, pour la protection de ses installations sensibles. La solution 3S, retenue par l'institution et brevetée, se déploie depuis le début de l'année sur le territoire national. Le cahier des charges militaire requiert un produit robuste, fiable, efficace et facile d'emploi, capable de s'intégrer et de renforcer l'ensemble des dispositifs de protection, statiques passifs, actifs ou dynamiques. Le C2 de DPS, drone autonome sélectionné, répond à toutes ces exigences et se déploie déjà sur des sites privés, en collaboration avec de grands acteurs de la sécurité. Ce succès vient couronner une politique de Recherche et de Développement pointue et une rigoureuse exigence de conformité quant à la réglementation de l'aviation civile et aux deux décrets du 17 décembre 2015. Une législation drastique encadre le vol des drones autonomes et DPS fut précurseur en la matière en obtenant pour la première fois dès 2017, l'autorisation de la DGAC (Direction générale de l'aviation civile).
Philippe Gabet, fondateur de Drone Protect System, précise qu'il exploite depuis déjà plus d'un an un drone automatique sur un site sensible des Landes.

TÉLÉSURVEILLANCE

Orange et Groupama créent Protectline

Ce partenariat permettra à Groupama de renforcer son activité existante dans ce métier et à Orange de devenir un acteur à part entière sur ce marché, franchissant une nouvelle étape dans sa stratégie d'opérateur multiservice.

Protectline, qui opérera sur le secteur de la télésurveillance des biens, est la société créée à la suite de l'accord signé entre Groupama et Orange. Comme l'explique Stéphane Richard, président-directeur général d'Orange : *« Le lancement prochain de notre offre de télésurveillance s'inscrit dans la stratégie d'opérateur multiservice d'Orange. »*
Selon l'accord, la société Protectline sera une plate-forme commune de production et de gestion des services de télésurveillance détenue par Orange à hauteur de 51 % et de 49 % par Groupama. Protectline est une société par actions simplifiée présidée par Christian Bombrun (président du conseil d'administration), et dirigée par Benjamin Pourquié (président exécutif) et Jean-Daniel Guedj (directeur général).

Indépendance

Orange et Groupama conserveront chacun la pleine maîtrise de la distribution en commercialisant des offres personnalisées dans leurs réseaux respectifs et sous leurs propres marques.
Groupama jouit déjà d'une solide expertise dans le domaine de la télésurveillance des biens avec une gamme d'offres allant du grand public au sur-mesure. Dans le cadre du partenariat annoncé, Groupama apporte à la société commune – via sa filiale Cofintex 6 – ses compétences et son savoir-faire, son usine logistique et informatique clé en main, son réseau d'installateurs, etc.
Orange, de son côté, lancera au printemps 2019 ses offres de télésurveillance de biens à destination de ses clients fixes et mobiles grand public en France. Son ambition est de prendre une position forte sur ce marché, en s'appuyant sur sa base d'abonnés, sa marque, son réseau de distribution physique et digital et l'expertise de Protectline.


© DR

« Ce partenariat avec Orange s'inscrit pleinement dans la stratégie de Groupama qui vise à offrir des services de proximité globaux et innovants à ses sociétaires et clients. Ainsi, Orange et Groupama développeront ensemble la meilleure des offres de télésurveillance de demain, centrée sur une expérience client inédite. »

THIERRY MARTEL, DIRECTEUR GÉNÉRAL DE GROUPAMA

CONTRÔLE D'ACCÈS

Locken sécurise 17 000 sites de SPN

Pour sécuriser les accès à ses sites, Scottish Power Energy Networks (SPN), un des acteurs majeurs de la production et de la distribution d'électricité en Grande-Bretagne, s'est engagé dans un très ambitieux projet de contrôle d'accès jamais réalisé dans le secteur de l'énergie.

Dans le cadre d'un vaste programme, le groupe a retenu la dernière solution de contrôle d'accès Locken, basée sur une clé intelligente.
Celle-ci permettra la sécurisation des infrastructures de distribution d'électricité sur les 17 000 sites exploités par SPN. Il faudra trois ans pour équiper de cylindres électroniques 23 000 points d'accès, empruntés par plus de 1 000 agents.

Ouverture instantanée

La clé électronique Locken sans contact combine les avantages d'une clé mécanique traditionnelle et ceux d'une technologie d'avant-garde puisque la transmission de l'information de la clé au cylindre est effectuée par induction magnétique, et non par contact électrique. Cela permet une ouverture presque instantanée de la serrure et donne au système une fiabilité parfaite, à l'épreuve de la rouille, de l'usure mécanique ou de la poussière, même pour une installation à l'extérieur puisque la solution est certifiée IP66 à IP69.
La clé électronique comprend un module Bluetooth qui lui permet de communiquer avec le smartphone de l'utilisateur par l'intermédiaire de l'application MyLocken. Cela permet d'assurer un contrôle d'accès en temps réel à la fois fin, centralisé et adapté aux besoins de chaque agent. La solution atteint ainsi des niveaux de sécurité habituellement réservés aux systèmes de contrôle d'accès on-line.

Une seule clé

Pour répondre aux configurations d'accès de SPN, Locken déploiera essentiellement des cadenas sécurisés dotés d'un cylindre électronique. Les personnels travaillant sur les infrastructures étendues et complexes de SPN comprenant de multiples points d'accès disposeront d'une seule clé. C'est elle qui fournira au cylindre l'énergie et l'information requise pour l'ouverture.
La composante purement mécanique de cette clé duale rend la solution encore plus flexible puisqu'elle peut ouvrir des cylindres traditionnels partout où on souhaite faire coexister les deux types de serrures.


© DR

« La solution de contrôle d'accès Locken aide les opérateurs de réseaux de distribution à respecter les normes de sécurité en vigueur dans le secteur. Elle offre un contrôle d'accès simple, souple, efficace, qui peut être intégré dans les logiciels de gestion déjà utilisés par l'entreprise. Elle permet d'améliorer significativement l'efficacité opérationnelle des utilisateurs et de réduire les coûts d'exploitation des entreprises. »

CATHERINE LAUC, DIRECTRICE DU MARKETING DE LOCKEN


© Locken

LOGICIELS DE SÉCURITÉ

Azur Soft investit dans l'IA

L'éditeur de logiciels de sécurité unifié Azur Soft investit de façon majeure en recherche fondamentale sur l'intelligence artificielle et vient de conclure un partenariat sur le long terme avec Inria (Institut national de recherche dédié aux sciences du numérique), pionnier de l'intelligence artificielle en Europe.

© DR

Cet ambitieux projet va permettre à Azur Soft et à l'Inria de mettre en commun leurs compétences et de créer, ensemble, de nouvelles briques d'IA dédiées à la sécurité des biens et des personnes.
Depuis 2015, grâce à des partenariats avec des entreprises technologiques reconnues dans le traitement numérique des données vidéo, Azur Soft intègre à son offre des composants permettant d'améliorer l'efficacité de la levée de doute vidéo voire, dans certains cas, d'anticiper des événements en amont de l'alarme.

Bases d'un partenariat solide

Néanmoins, l'expérience démontre que le complément amené par la vidéo ne peut pas suffire dans un environnement disposant de systèmes anti-intrusion complexes alliant des technologies et des flux multiples, qui génèrent des faux positifs en nombre très important (plus de 8 alarmes sur 10 reçues par chaque centre de télésurveillance/assistance restent des « fausses alarmes »).
Cette collaboration permettra d'offrir aux télésurveilleurs et téléassisteurs un outil qui analysera la véracité de l'alerte et permettra ainsi de d'accélérer au maximum la prise en compte des « vraies alarmes » par l'opérateur.
« Nos marchés de sécurité unifiée évoluent rapidement et nous devons continuer à simplifier le traitement des millions d'opérations quotidiennes de nos clients. L'intelligence artificielle est LA brique innovante indispensable pour répondre à ces besoins opérationnels, explique Marc Vaillant, président directeur général d'Azur Soft. *Notre association en recherche fondamentale avec Inria, centre de recherche aux compétences et aux résultats indiscutables au niveau européen dans le domaine de l'intelligence artificielle est tout à fait originale. C'est une vision commune sur des sujets tels que l'IoT, le bâtiment intelligent ou la ville connectée qui rassemblent Azur Soft et l'Inria et qui posent les bases solides d'un partenariat sur le long terme. »*

© DR

2 QUESTIONS À
Marc Vaillant,
PDG D'AZUR SOFT

Pourquoi avoir décidé de mettre en place ce partenariat avec l'Inria ?
Je suis parti d'un constat assez simple. Avec nos clients, nous avons énormément investi en solutions innovantes , mais il est évident que notre secteur doit continuer à investir en technologies car il repose encore trop sur l'humain alors que nos clients manipulent de plus en plus de données. Ce partenariat avec l'Inria nous permettra – via la recherche fondamentale – de développer des outils qui, grâce à l'apport de l'intelligence artificielle, amélioreront de façon majeure l'efficacité du travail des opérateurs derrière leurs écrans.

Quels devraient être les premiers résultats concrets de ce travail en recherche fondamentale ?
Nous avons lancé cette année un projet de recherche, qui court sur les trois années à venir, afin qu'avec l'Inria nous soyons capables de développer un outil, basé sur le deep learning, qui apportera une réponse aux problèmes des faux positifs en intrusion, vidéoprotection, alarmes froid et téléassistance.

BIOMÉTRIE

L'aéroport de Los Angeles teste la reconnaissance faciale de Gemalto

Au Terminal 4 de l'aéroport international de Los Angeles (LAX), Gemalto est engagé dans un projet pilote en biométrie avec une importante compagnie aérienne.

© Gemalto

Grâce à l'utilisation des solutions de reconnaissance faciale du Français, les passagers verront leurs procédures d'embarquement simplifiées par rapport à celles utilisant des cartes d'embarquement traditionnelles. Ce projet répond, par ailleurs, aux exigences du service des douanes et de la protection des frontières des États-Unis (CBP).

« Être en mesure d'utiliser son visage au lieu d'une carte d'embarquement permettra non seulement de renforcer la sécurité, mais aussi d'embarquer plus facilement et rapidement, déclare Neville Pattinson, vice-président en charge des programmes gouvernementaux chez Gemalto. *La gestion des passagers évolue à l'échelle mondiale et nous sommes ravis d'être au cœur de ce changement qui permet à nos clients de proposer un service et une sécurité optimisés grâce à nos capacités biométriques. »*

La solution Live Face Identification System (LFIS) Gemalto, intégrée au bureau des agents pour faciliter l'embarquement, prend peu d'espace et permettra de futures options. Les passagers s'approcheront de la porte d'embarquement et, à la suite d'une vérification faciale effectuée par les services de contrôle des voyageurs du CBP, ils recevront une confirmation sur un écran. Une fois vérifiées, les images saisies seront effacées du système pour garantir la confidentialité des passagers.

Lors des tests biométriques réalisés par le département américain de la sécurité intérieure*, la solution LFIS a obtenu un taux d'acquisitions réussies de 99,44 % en moins de cinq secondes, un résultat très favorable en comparaison avec une moyenne de seulement 65 % sur la même durée pour les autres fournisseurs participants.

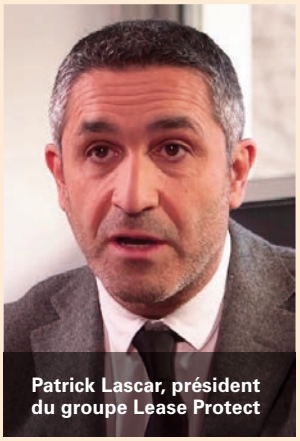
* *DHS biometric rally results*

© DR

CONTRÔLE D'ACCÈS
NOUVEAUX DISTRIBUTEURS EN FRANCE POUR PAXTON

Le fabricant anglais étend son réseau de distribution français afin de permettre aux installateurs et intégrateurs de s'approvisionner toujours plus facilement en produits Paxton. Les nouveaux partenaires, ACCF et Cinodis Technologies IP disposent désormais de toute la gamme Paxton, notamment le Net2, le système de contrôle d'accès phare de la société, et Net2 Entry, sa gamme de vidéophonie. Sylvain Pailler, directeur commercial chez Paxton, explique : *« Nous sommes ravis d'annoncer ces deux nouveaux partenariats qui permettront de nous assurer que davantage de clients en France bénéficient de notre gamme de contrôle d'accès innovante et simple à utiliser. L'expertise du marché d'ACCF et de Cinodis Technologies en fait d'excellents partenaires pour notre réseau de distribution français en pleine croissance. »*

> La liste des distributeurs français de Paxton comprend désormais :
- ACCF
- ADI Global distribution
- CCF
- Cinodis Technologies OP
- Intégral Système.



Patrick Lascar, président du groupe Lease Protect

© DR

DÉMARQUE INCONNUE
3 MILLIONS D'EUROS POUR LEASE PROTECT

NextStage AM a décidé de réinvestir 3 millions d'euros aux côtés de Patrick Lascar et Mikaël Choucroun, entrepreneurs, cofondateurs et actionnaires majoritaires du groupe Lease Protect, avec l'accompagnement d'Andera Partners via sa franchise ActoMezz, afin de poursuivre le développement du groupe, leader des solutions de lutte contre la démarque inconnue pour les entreprises. Créé en 2009, le groupe Lease Protect est spécialiste des solutions de sécurité pour lutter contre la démarque inconnue ; une activité qui repose notamment sur la location, l'installation et la maintenance de systèmes de vidéosurveillance, portiques de sécurité et de comptage clients. Le groupe a su développer une gamme étendue de solutions flexibles et innovantes (location, maintenance à distance, audit vidéo personnalisé à distance, etc.) qui s'adresse aussi bien aux PME qu'aux grands comptes comme Sephora, Sport 2000 ou IKKS.

Le groupe Lease Protect intervient sur l'ensemble du territoire grâce à ses neuf agences et a installé plus de 5 000 sites en France. Il emploie aujourd'hui plus de 120 salariés pour un CA consolidé de plus de 18 millions d'euros en 2018. *« Cette nouvelle étape de notre développement avec ce nouvel investisseur va nous permettre d'accentuer notre développement »*, se réjouit Patrick Lascar, président du groupe Lease Protec.

© DR

CONTRÔLE D'ACCÈS
KIMI RÄIKKÖNEN VA COLLABORER AVEC ILOQ

Le spécialiste des solutions de gestion des accès numériques et mobiles auto-alimentées, iLOQ a signé un contrat de deux ans avec le champion du monde de Formule 1 Kimi Räikkönen. *« Kimi est heureux de prêter son image et sa voix à la communication d'iLOQ. Nous avons toujours eu une forte présence dans les pays du Nord et notre expansion à travers l'Europe a été rapide. Mais, aujourd'hui, nous sommes prêts à conquérir le reste du monde. Nous avons déjà lancé la promotion de notre solution de pointe au-delà des frontières de l'Europe. Nous avons la conviction qu'avec Kimi comme ambassadeur, iLOQ va aller encore plus loin et que notre objectif de faciliter l'accessibilité au quotidien touchera un public plus large à l'international »*, se réjouit Joni Lampinen, directeur du marketing chez iLOQ. De son côté, le champion confie : *« Les solutions proposées par iLOQ sont très abouties sur le plan technique, mais restent extrêmement simples à utiliser pour les clients. Ce type de synergie m'intéresse vraiment. Et ceux qui travaillent sur ces solutions sont des personnes engagées, passionnées, des champions de l'innovation. Ils ne suivent pas forcément les règles établies. Ils sont prêts à sortir des sentiers battus et à faire bouger les choses. J'ai du respect pour cet état d'esprit. Je suis heureux de les aider à promouvoir l'exposition de leur marque. »*

ANALYSE ET GESTION VIDÉO

IPS débarque en France

L'Allemand IPS vient de rejoindre l'AN2V et souhaite développer son activité sur le marché français.

IPS Intelligent Video Analytics est un fabricant allemand de solutions haut de gamme d'analyse et de gestion vidéo créée en 1965. Depuis 2006, IPS fait partie de Securiton GmbH, une société du groupe Swiss Securitas. Basée à Munich, une équipe d'ingénieux développeurs de logiciels améliore constamment le portefeuille de produits IPS, produisant les meilleures solutions pour chaque client. Outre son système de management vidéo 3D, IPS propose douze modules différents d'analyse vidéo pour la détection automatique en temps réel de mouvements, de sabotage, d'intrusions, de maraudage et autres dangers. Avec une fiabilité exceptionnelle et éprouvée, les produits IPS sont déployés dans des milliers d'applications à travers l'Europe.

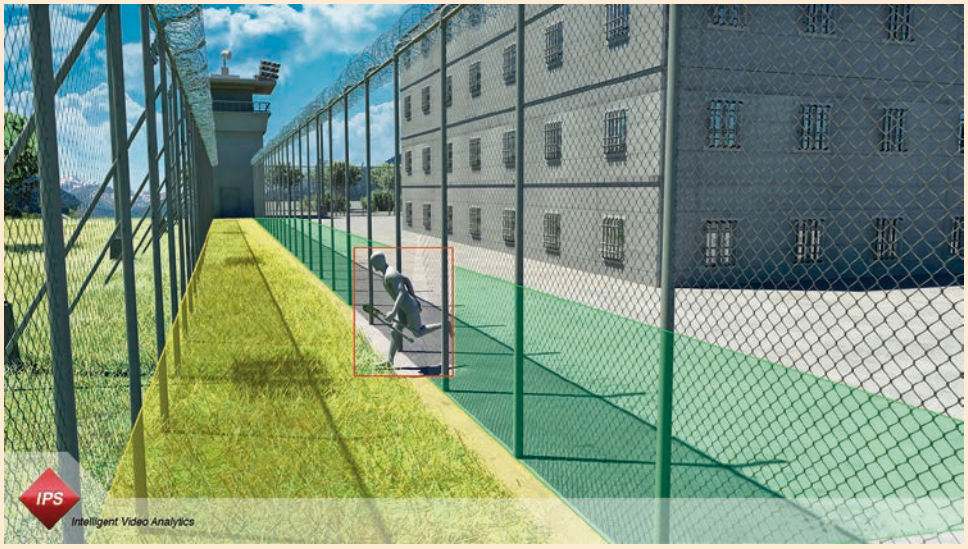
Sites sensibles

« Le succès d'IPS, en Allemagne, mais aussi aux Pays-Bas, en Suisse, en Belgique, en Norvège et en Suède, nous encourage maintenant à proposer nos analyses vidéo intelligentes en France. Les sites sensibles sont notre terrain de prédilection, explique Alain Benoit, directeur produit, marketing et ventes chez IPS. *La demande est très importante dans ce secteur, en particulier pour la sécurisation périmétrique et la recherche de suspects par analyse d'image. Un terrain où les analyses vidéo intelligentes IPS excellent ! Grâce à sa plate-forme Web IPS Analytics Manager, une grande partie des fonctions d'analyse peut également être utilisée dans les systèmes de gestion vidéo de fabricants tiers (par exemple Milestone, Hikvision, Axis). »*
Des petites entreprises aux grands acteurs mondiaux, les clients d'IPS proviennent des différents secteurs de la haute sécurité tels que gouvernement, armée, prisons, infrastructures critiques, sites pétrochimiques, centres d'appel et centres de télésurveillance. *« IPS vend ses produits par l'intermédiaire d'un solide réseau de partenaires et entretient des partenariats étroits avec des intégrateurs, des distributeurs, des centres d'appel et de télésurveillance ainsi que des partenaires technologiques de renom dans toute l'Europe »*, conclut Alain Benoit.


© DR

« La France est un marché potentiel important. Nous sommes en train de chercher des partenaires et nous avons déjà finalisé plusieurs accords avec des grands intégrateurs français. »

ALAIN BENOIT, DIRECTEUR PRODUIT, MARKETING ET VENTES CHEZ IPS



© DR

DISTRIBUTION

Thirard va distribuer la serrure connectée Li-Fi Brightlock

La serrure connectée Li-Fi de la start-up Havr sera désormais distribuée par le fabricant de serrures. Il intègre ainsi la haute technologie dans son offre.

© DR

La start-up Havr qui, il y a quelques mois, avait lancé BrightLock, la première serrure connectée Li-Fi à ouverture lumineuse, a annoncé la signature d'un contrat de distribution avec l'entreprise Thirard, fabricant de serrures et spécialiste des équipements de sécurité. Industriel reconnu sur le marché et leader dans la grande distribution bricolage, Thirard intègre de la haute technologie à son offre et propose désormais la serrure BrightLock, un produit récompensé par un « Innovation Award » au salon CES 2019.

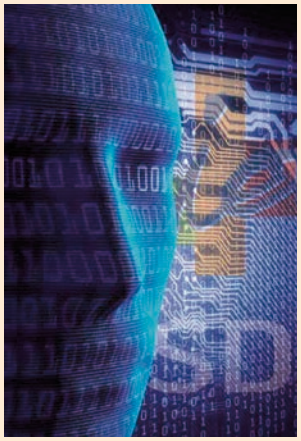
Cet accord avec l'entreprise Thirard permet à la jeune start-up Havr de démarrer la commercialisation de sa serrure connectée innovante au côté d'un industriel français historique : *« L'année 2019 est un tournant important pour nous, avec le lancement sur le marché de notre première innovation multi-primée BrightLock. S'appuyer sur le réseau de distribution et l'expérience d'un savoir-faire centenaire d'un industriel, nous apporte beaucoup de confiance et d'ambition pour cette année »*, a commenté Simon Laurent, CEO de Havr.

Outre ce contrat de distribution, Havr a également conclu un contrat de fourniture pour fabriquer les BrightLocks avec des cylindres européens haute sécurité de la société Thirard.

© DR

« Ce partenariat entre la start-up Havr et l'entreprise centenaire Thirard est un vrai enrichissement mutuel. Tout au long du process, l'innovation informatique et l'expertise mécanique ont prouvé leur complémentarité. C'est une expérience de collaboration extrêmement intéressante qui permet de lancer sur le marché un produit construit autour de technologies de pointe. L'engagement de Thirard auprès de la start-up de talent Havr démontre le dynamisme français en matière d'innovation. »

BARNABÉ CHIVOT, PRÉSIDENT DE THIRARD



© DR

RECONNAISSANCE FACIALE

ID3 TECHNOLOGIES SE DISTINGUE AUX TESTS DU FRVT

id3 Technologies a confirmé d'excellentes performances lors des tests du FRVT (Face Recognition Vendor Test), la fameuse compétition internationale d'algorithmes de reconnaissance faciale. Ce test a pour objectif de mesurer les performances des technologies de reconnaissance faciale utilisables par un large éventail d'applications de sécurité civile, de maintien de l'ordre et de sécurité intérieure. id3 se distingue par la précision de reconnaissance tout en limitant la taille des gabarits biométriques et la puissance de calcul nécessaire.

Cette technologie permet désormais la détection et la reconnaissance en temps réels de visages dans une foule en s'affranchissant des contraintes de race, d'âge, de genre et de variations d'expression faciale. Elle fonctionne également dans des conditions de faible luminosité avec une large gamme de caméras, y compris en proche infrarouge.

Les excellents résultats de ces tests ont été obtenus grâce à ses algorithmes propriétaires basés sur l'utilisation de réseaux de neurones convolutifs. Les solutions de reconnaissance faciale d'id3 Technologies ont déjà été déployées pour détecter et identifier des intrus sur des zones sensibles comme des laboratoires informatiques ou des entrepôts.

DÉFENSE/SÉCURITÉ

Le Gicat accueille 15 nouveaux adhérents

Lors de son conseil d'administration de décembre 2018, le Gicat a ratifié les adhésions de 15 nouvelles entreprises et rassemble désormais 270 sociétés françaises des secteurs de la défense et de la sécurité.

Ces nouveaux adhérents confirment la diversité du Gicat. Six se placent dans le domaine de la défense, quatre dans la sécurité et cinq autres sur les deux secteurs. Ils recouvrent des domaines variés : entre autres, l'intelligence artificielle, la robotique, la cybersécurité, les drones et le MCO des véhicules. Les neuf PME qui ont rejoint le Gicat confirment également la part importante des petites entreprises au sein de notre groupement, environ 70 %. Citons parmi ces nouveaux adhérents :

> Frenchshield : premier cluster national dédié à la sûreté. Il a pour vocation de créer un véritable pool d'expertises afin de proposer des dispositifs globaux de sûreté performants et à haute valeur ajoutée. Il s'est donné pour mission de valoriser et de promouvoir l'expertise française en matière de sûreté en proposant une offre 360° intégrée.

> Hensoldt France : la branche du groupe éponyme, propose une large gamme de solutions dans les domaines des radars terrestres et embarqués, de l'IFF, de la guerre électronique, de l'autoprotection, de la navigation et des systèmes électro-optiques. Les domaines d'Hensoldt France sont la défense terrestre (diverses solutions dans l'IFF : interrogateurs IFF mode 5 pour SACP/SATCP, calculateurs cryptographiques mode 5, balises et bancs de test, chargeurs de clés et accessoires associés), la sécurité (solutions anti-drones permettant de couvrir l'ensemble des besoins dans le domaine de la détection, de l'identification et de la neutralisation des drones intrusifs).

> MC2 Technologies développe des équipements pour la protection de sites ou infrastructures sensibles. MM-Imager, une caméra passive THz dédiée à la détection d'objets cachés portés par les personnes, présente des performances uniques offrant un fonctionnement en temps réel, un niveau de détection élevé, un large champ de vision et une bonne résolution. L'appareil, actuellement déployé en Chine, est adapté à la sécurisation des gares, des métros, des halls d'aéroport, etc.

> Serpe conçoit, déploie et maintient depuis 1976 des produits et systèmes de protection périmétrique intelligents, adaptés aux enjeux de sûreté d'aujourd'hui et de demain, pour garantir aux sites sensibles un niveau de protection optimale.

> Shark Robotics conçoit et produit des drones terrestres et accompagne ses clients dans l'ingénierie, le développement et la conception de plates-formes robotiques destinées à éloigner l'homme du risque. Shark Robotics intervient dans les domaines de la sécurité, de la défense, de l'industrie et du nucléaire.

> Sinequa est un éditeur de logiciel indépendant spécialisé dans la recherche et l'analyse de données basées sur les technologies de l'IA dont le machine learning, le deep learning et le traitement automatique du langage naturel.

> Spie Batignolles Technologies est la filiale « travaux spéciaux » du génie civil de Spie Batignolles. Son offre couvre à la fois l'intégration de solutions d'attrition de la menace en sécurisant les accès aux sites – clôtures renforcées, blindages, vitrages anti-effraction et pare-balles, entre autres. Spie Batignolles Technologies a aussi développé un procédé de blindage électromagnétique intégré dans le béton de construction des bâtiments stratégiques-procédé GreyShield.

© MC2 Technologies

VIDÉOSURVEILLANCE

Provision-ISR renforce sa distribution avec Intégral Système

Le fabricant israélien de produits de vidéosurveillance, qui s'est implanté en France début 2018, poursuit son développement de réseau de distribution.

Provision-ISR vient en effet de signer un accord avec Intégral Système, spécialisé dans la distribution des produits et services pour les professionnels de la sécurité (vidéo, intrusion, automatisme, verrouillage, contrôle d'accès).
Intégral Système qui a voulu, ces dernières années, s'investir dans une démarche de sécurité globale en investissant massivement dans d'autres domaines, offre ainsi à ses clients des solutions d'interphonie et de contrôle d'accès, en passant par la sécurité incendie mais également la vidéosurveillance. Intégral Système, dont le siège social est basé à Ferrières-en-Brie, en région parisienne, fournit à Provision-ISR une couverture nationale tout en s'appuyant sur une proximité régionale avec 12 agences réparties dans toute la France.
« En 2015, Intégral Système a décidé d'ouvrir son spectre produit en apportant son savoir-faire dans les prestations au service des installateurs, notamment pour les faire monter en compétence et les assister dans la mise en service des nouvelles technologies, commente Sébastien Lansiaux, directeur général adjoint d'Intégral Système. *Au-vu de l'état du marché de la vidéosurveillance, représenté par le diktat de certains industriels, nous avons choisi Provision-ISR pour la clarté d'un partenariat solide, efficace et professionnel mais aussi par la qualité de leur offre qui s'avère indispensable pour s'imposer sur ce marché. »*

Distributeurs spécialisés

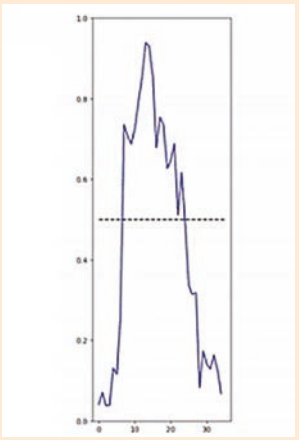
Crée en 2007 pour répondre à une demande croissante de produits de haute qualité pour couvrir l'ensemble du marché de la vidéosurveillance, Provision-ISR commercialise ses produits via un réseau de distributeurs sur les cinq continents.
Toujours dans cette stratégie de s'appuyer sur un réseau de distributeurs qualifiés, avec cette volonté de s'associer cette fois-ci avec un distributeur ayant une couverture nationale, cette signature de partenariat marque une étape importante dans le développement de Provision-ISR France.

© Provision-ISR

© DR

CONTRÔLE D'ACCÈS
HID VEUT DÉMYSTIFIER L'OSDP !

Le secteur du contrôle d'accès poursuit son essor et s'adapte aux nouvelles menaces et aux nouveaux protocoles de sécurité comme l'OSDP (Open Supervised Device Protocol), un standard de communication de contrôle d'accès qui permet une connexion sécurisée entre les lecteurs et les contrôleurs d'accès. Il est devenu une alternative face aux anciens protocoles tels que Clock-and-Data et Wiegand, vulnérables aux attaques de type « man-in-the-middle ». Avec un cryptage haut de gamme, l'OSDP résout ces problèmes de sécurité. Par ailleurs, il a fait évoluer le secteur du contrôle d'accès vers des normes ouvertes, favorisant ainsi l'interopérabilité, la flexibilité, etc. D'ailleurs, 85 % des organisations ayant mis en œuvre un plan OSDP reconnaissent un impact positif sur leur contrôle d'accès (enquête HID Global).
Autres avantages de l'OSDP : niveaux de sécurité plus élevés (cryptage de pointe AES-128), communication bidirectionnelle, coût d'acquisition réduit, user-friendly, etc.
HID Global a joué un rôle important dans le développement du protocole OSDP et peut accompagner les entreprises dans la mise à niveau de leurs systèmes de contrôle d'accès.
> Retrouvez le livre blanc sur https://info.hidglobal.com



© Veesion

ANALYSE VIDÉO
VEESION TRAQUE LES VOLEURS PAR LEUR COMPORTEMENT

Le 6 février dernier, Veesion a reçu le prix de l'innovation, à l'Agora des directeurs de la sécurité. La start-up a mis au point un système pour détecter les mouvements suspects filmés par les caméras de vidéosurveillance.
« Le vol représente une perte énorme dans le commerce de détail et seulement 5 % sont détectés par les solutions de surveillance actuelles », explique Thibault David, 25 ans, l'un des dirigeants de la start-up Veesion. Cette équipe d'anciens étudiants formés à HEC et Polytechnique, a mis au point un logiciel qui détecte les mouvements suspects sur les images des caméras de vidéosurveillance, grâce à un algorithme utilisant l'intelligence artificielle.
« Le logiciel analyse le flux des caméras et les comportements des clients comme le ferait un opérateur vidéo », poursuit Thibault David. Un opérateur jamais distrait, jamais victime de fatigue ni de mal de tête, donc un logiciel qui ferait tout comme un homme, sans défaillance... La solution repose sur le deep learning et s'intègre à un système de vidéosurveillance déjà existant.
Il devrait intéresser les supermarchés et les petits commerces, et tout particulièrement ceux qui vendent des vêtements, des bijoux et des cosmétiques, principales cibles des voleurs.

CONTRÔLE D'ACCÈS

Les tendances selon Assa Abloy

Le marché du contrôle d'accès évolue. Comment ? À quelle vitesse ? Et quels sont les facteurs qui pourraient affecter l'entreprise d'ici 2025 ? Autant de questions auxquelles Assa Abloy apporte des réponses dans une récente étude.

Les résultats de l'étude effectuée par IHS Markit pour Assa Abloy auprès des professionnels de la sécurité, montrent un développement croissant de la part des solutions sans fil sur le marché du contrôle d'accès. Pour la première fois, la part des répondants ayant un système de contrôle d'accès exclusivement câblé a chuté au-dessous de 50 %. Près des deux tiers des personnes interrogées *« ont une vision plus positive du sans-fil qu'il y a cinq ans grâce aux progrès de la technologie. »*

Les données de l'étude font ressortir une autre tendance intéressante. Les besoins sur des accès autres que des portes semblent participer à la croissance des besoins en contrôle d'accès sans fil. Notamment sur des portails protégés par des cadenas, des baies informatiques, des armoires, etc.

« C'est pour partie une question de confort, d'après Russell Wagstaff, directeur produits contrôle d'accès chez Assa Abloy Emea. *Plus on peut sécuriser d'accès avec un seul et même identifiant, mieux c'est pour les utilisateurs. Les gestionnaires de site peuvent désormais étendre et renforcer leur contrôle d'accès sur un périmètre plus large qu'avant. En outre, comme ces dispositifs sont sans fil, il est facile de mettre du contrôle d'accès, même en extérieur, avec des cadenas, batteuses et serrures de meuble. Bien choisie, la solution peut permettre de contrôler ces accès à l'identique d'une porte d'accès principal. »*

Les téléphones vont-ils remplacer les clés ?

L'utilisation des smartphones et autres appareils mobiles est aujourd'hui omniprésente mais, dans le monde des identifiants de contrôle d'accès, leur présence est encore balbutiante. De fait, les badges plastiques dominent largement sur les lieux de travail. Pourtant, utiliser son téléphone portable comme identifiant d'accès a de nombreux avantages : praticité, sûreté, coût, etc.

Mais cette étude souligne également la réticence des utilisateurs à adopter le contrôle d'accès par téléphone. Dans un sondage 2016 de Harvard Business Review, 60 % des répondants ont manifesté des inquiétudes concernant la sécurité d'utilisation du Bluetooth, dont 45 % des directeurs d'information, responsables techniques, employés IT. Ils considèrent les périphériques connectés par mobiles comme la plus grande faille dans un système de contrôle. Rien d'étonnant pour des technologies, somme toute, assez récentes…

Cependant, IHS Markit estime à 44 millions le nombre de téléchargement d'identifiants mobiles d'ici 2021, contre seulement 1 million en 2016, surtout comme un complément aux cartes plastiques et non comme remplacement. Ainsi, considérer un identifiant mobile comme une alternative est sans doute une première étape dans le changement. Et, de son côté, Gartner prévoit que 20 % des organisations utiliseront les identifiants mobiles d'ici 2020. Comme les smartphones contiennent une identification biométrique intrinsèque, cela peut éviter leur mise en place en parallèle et donc réduire quelques investissements.

Standards et intégration

Une grande majorité de professionnels de la sécurité – tant dans le cadre de l'étude que sur le terrain – reconnaissent l'importance croissante de l'intégration de plusieurs technologies de sécurité dans un environnement unique. *« L'interopérabilité est cruciale pour n'importe quel utilisateur final ayant investi dans un nouveau système de contrôle d'accès,* commente Matthias Weiss, chef de produit Aperio chez Assa Abloy Emea. *Ils ont besoin de parer à toute éventualité, et les standards ouverts leur facilitent la tâche. Ils les libèrent de la dépendance à un seul fournisseur de solution, et rendent le contrôle d'accès plus flexible. »*

> Le rapport complet est téléchargeable sur : http://bit.ly/2F3Ap70

© DRw

SÉCURITÉ ÉLECTRONIQUE

Le groupe ESI poursuit sa pénétration du marché français et international

2019 va permettre à Philippe Camilleri et Claude-Philippe Néri de signer leur vingtième année de collaboration à la tête du groupe ESI, avec la belle réussite de s'être imposé comme un des leaders européens des solutions de télésurveillance, téléassistance, etc., et un CA supérieur à 9 millions d'euros pour 2018.

Les équipes du groupe (plus de 70 personnes) ont acquis au fil des ans l'expérience nécessaire à la bonne compréhension des métiers complexes qui sont ceux de la sécurité et la maîtrise des enjeux humains et financiers importants qu'ils représentent. L'intégration progressive de nouvelles ressources a permis aux équipes de faire évoluer les outils technologiques avec les nouveaux concepts mis à disposition par le marché.
L'activité s'est progressivement segmentée en trois pôles principaux : ESI propose et intègre les solutions pour les stations de télésurveillance ou les Control Room lorsque celles-ci sont directement acquises par les utilisateurs finaux. Argos Technologies qui, au fil des ans, a repositionné son savoir-faire sur des solutions locales de sécurité : plus spécifiquement en vidéo surveillance avec SoftNet Manager et dans le monde de l'hypervision avec SpaceControl, en axant leur distribution sur la mise en place de partenariats avec des installateurs et intégrateurs à valeur ajoutée. Asplink, la plate-forme cloud de sécurité du groupe, héberge des solutions de plus en plus importantes et gère aujourd'hui plus de 20 000 raccordements. Les alarmes de ces derniers sont traitées par les clients raccordés à la plate-forme sur un modèle SaaS.

8 % en R&D

La part du CA consacré à la R&D varie selon les années entre 5 % à 8 % du chiffre d'affaires global du groupe.

Le PDG d'ESI, Claude-Philippe Néri, conforté par les excellents résultats de 2018, voit l'avenir du groupe en rose.

© DR

Ainsi, les systèmes informatiques cognitifs, qui aujourd'hui se répandent dans notre quotidien, sont en mesure de progressivement prédire les événements et d'aider à la prise de décision. Pour en tirer profit, les entreprises doivent encore faire face à de nombreux défis associés au big data. C'est sur ce chemin que, depuis plus de quatre ans, s'est installé ESI, afin de progressivement intégrer dans ses solutions des algorithmes prédictifs d'intelligence artificielle issues des technologies d'apprentissage profond (deep learning) et de filtrage d'erreurs.
Les prochaines années s'annoncent donc extrêmement prometteuses avec une spécificité actuellement atypique de conserver les 100 % des membres fondateurs à la direction du groupe. Ce particularisme garantit aux utilisateurs une stabilité du savoir-faire et de la connaissance métier, et la volonté d'avancer dans une construction et une vision structurée de l'avenir.
ESI base son approche non seulement sur la mise en place de nouveaux concepts, de nouvelles technologies, mais aussi et surtout sur la qualité de son approche.

2018 : une des meilleures années

ESI a signé avec 2018 une des meilleures années de son histoire. Le groupe a bénéficié de la stratégie mise en place deux années auparavant. Comme le signale son PDG, Claude-Philippe Néri, *« nous modernisons de façon constante nos solutions afin de permettre à nos clients actuels mais aussi à nos nouveaux utilisateurs de disposer d'outils constamment remis à niveau leur permettant de se diversifier sur de nouveaux métiers et de rentabiliser leur exploitation. »* Cette politique, associée à un dynamisme commercial mené par des équipes consolidées, a permis d'assurer une belle progression de sa pénétration de marché notamment à l'international (prés de 50 % du CA).
En fin d'année 2018, ESI a également concrétisé avec succès le lancement de sa nouvelle solution SpaceControl, hyperviseur ouvert, multisite et multiprotocole.

« Nous modernisons de façon constante nos solutions afin de permettre à nos clients de disposer d'outils constamment remis à niveau. »

CLAUDE-PHILIPPE NÉRI, PDG D'ESI

SÉCURITÉ URBAINE

Spie équipe Leipzig

L'année dernière, Spie a mené à bien l'extension du réseau numérique d'alerte de l'agglomération de Leipzig.

Ces six nouvelles installations, situées à Naunhof, Borna, Deditzhöhe, Kühnitzsch, Podelwitz et Leipzig, permettent aux centres de secours et aux unités de protection civile d'être alertés plus rapidement en cas d'urgence. Sur demande de l'agglomération de Leipzig, le réseau numérique d'alerte dédié aux services d'urgence a été placé sous la responsabilité de la régie municipale Rettungsdienst und Brandschutz Landkreis Leipzig. Ce système comprend 3 610 récepteurs mobiles (comme des pagers) et environ 300 déclencheurs d'alarme. Mais pour atteindre les zones à faible couverture radio, la régie municipale a recours depuis plusieurs années à des dispositifs numériques d'alerte (DAU). Ces derniers sont répartis sur l'ensemble de l'agglomération. Ils permettent de relayer les signaux d'alerte depuis le centre d'opérations de Leipzig vers les services de secours. Ainsi, dans l'optique de toujours améliorer les délais d'intervention, la société Spie Fleischhauer a été désignée pour installer six nouveaux dispositifs numériques d'alerte fournis par Spie Deutschland & Zentraleuropa.

Intégration au réseau existant

En raison de leur faible couverture radio, six localités pouvant bénéficier de relais d'alerte ont été identifiées par Spie au printemps 2018. Après avoir obtenu les autorisations requises, le groupe a installé et programmé les nouvelles unités, avant de les intégrer au réseau d'alerte existant. Michael Hartung, directeur de la division ICS (Information & communication services) de Spie Deutschland & Zentraleuropa, explique : *« Le déploiement des relais numériques d'alerte et de leur support technique est une tâche exigeante. Leur intégration au réseau d'alerte existant doit passer par le biais d'une liaison radio. Peu d'entreprises sont capables de proposer un portefeuille aussi complet de services à partir d'une seule source. »*

© DR

© Vanderbilt

INTRUSION
VANDERBILT CERTIFIÉ

Le spécialiste mondial des systèmes de sécurité (intrusion, contrôle d'accès, etc.) a obtenu la certification NF A2P Cyber-RTC du CNPP pour sa solution SPC. *« En certifiant nos gammes d'intrusions SPC sur les derniers référentiels CNPP NFA2P sur Cyber Type 2 et 3, Vanderbilt offre à tous ses clients une sécurité de haut niveau pour toutes les transmissions de surveillance à distance, ainsi que pour les applications cloud comme notre service SPC Connect »*, déclare Hervé Houy, responsable France chez Vanderbilt.

Et si pour tous vos besoins, il existait un site internet unique ?

protectionsecurite-magazine.fr

Infos
Archives
Annuaires
e-salon
Dossiers techniques
...

psm
Protection Sécurité Magazine

Mars | Avril 2019
n°252

SOMMAIRE

TP Media
Magazine édité par TP Media
20, rue des Petites Écuries
75010 Paris
Tél. : +33 (0)1 45 23 33 78 Fax : +33 (0)1 48 00 05 03
info@protectionsecurite-magazine.fr

BIMESTRIEL DE LA SÉCURITÉ ET DE LA SÛRETÉ
Commission paritaire : 0320 T 91736
ISSN : en cours

DIRECTEUR DE LA PUBLICATION
Vincent PERROTTE
ÉDITION / DIRECTION DE LA RÉDACTION
Christophe LAPAZ ;
Tél. : + 33 (0)6 27 37 29 22
e-mail : cl@protectionsecurite-magazine.fr
JOURNALISTE: Laurence ALEMANNI
CONCEPTION GRAPHIQUE Éric MERKI & Vincent LEVER
MAQUETTE Vincent LEVER
SECRÉTARIAT DE RÉDACTION : Frédérique GUITTON-DANIELO
PUBLICITÉ Jérôme PERROTTE ;
Tél. : +33 6 09 17 09 50 / + 33 (0)1 45 23 33 78
e-mail : jp@protectionsecurite-magazine.fr
DIFFUSION & MARKETING Hélène Duval
e-mail : hd@tpmedia.fr
SERVICE ABONNEMENTS PSM - TBS Blue - 6 rue d'Ouessant - 35760 St Grégoire ;
Tél. : + 33 (0)1 76 41 05 88 ; Fax : + 33 (0)1 48 00 05 03
e-mail : abopsm@tpmedia.fr
Abonnement 1 an France : 168 euros TTC
Étranger : 180 euros TTC
IMPRESSION CORLET. Zone Industrielle Ouest - Rue Maximilien-Vox - Condé-sur-Noireau. 14110 Condé-en-Normandie ;
Origine papier : Suède ; Taux de fibres recyclées : 0 % ;
Certification des fibres : PEFC ; Eutrophisation : 0,02 kg/T
CRÉDIT PHOTO COUVERTURE
Getty Images

Ce numéro contient un encart Preventica

ÉDITO

© DR

Le terrorisme : l'arbre qui cache la forêt

Depuis les attentats qui ont endeuillé la France, les entreprises forment leurs expatriés et voyageurs internationaux afin qu'ils respectent règles et procédures de sécurité – souvent de bon sens – pour ne pas s'exposer et exposer leur entreprise à un risque. Or, les risques visant les personnes ne sont pas uniquement les attentats. On pense évidemment au kidnapping. Mais il y en a d'autres : la corruption, l'espionnage, la violence contre les personnes… Il faut aussi les prendre en compte. Mais le collaborateur n'est pas seulement la cible de… Il peut également être à l'origine de menaces pour son entreprise dues au non-respect des règles, à de la malveillance pure ou par volonté de nuire… C'est aussi cela que doivent prendre en considération les entreprises quand elles tentent de se protéger contre le risque personnel. Or, ce n'est pas toujours fait. C'est ce que montre le dossier que nous consacrons à tous ces sujets dans ce numéro. Bonne lecture.

Christophe Lapaz, directeur de la rédaction,
cl@protectionsecurite-magazine.fr

© Azur Drones

SÉCURITÉ DES ENTREPRISES

Les drones automatiques à la conquête du ciel

Alors que désormais les opérateurs de drones doivent être titulaires du certificat de télépilote, la DGAC vient de valider un drone opérant de façon automatisée sous contrôle d'un téléopérateur. Une décision qui devrait faciliter le déploiement des drones automatiques.

Depuis quelques mois, manœuvrer un drone – quel qu'il soit – requiert des compétences techniques validées par un certificat théorique de télépilote, délivré par la DGAC et d'une attestation de suivi de formation effectuée dans un centre agréé. Azur Drones a annoncé avoir reçu en février, une des premières autorisations de la DGAC, pour un système de drone opérant de façon complètement automatisée, sous la simple supervision d'un téléopérateur formé sur Skeyetech par Azur Drones. La formation simplifiée d'Azur Drones diffère du certificat professionnel de télépilote, obligatoire depuis le 18 mai 2018, pour opérer les autres drones du marché. En effet, cette formation permet de maîtriser en quelques heures le déclenchement de missions de levées de doute ou de rondes préprogrammés ainsi que de gérer les situations d'urgence. En revanche, elle n'autorise pas à modifier les trajectoires programmées. *«Nous sommes très fiers de l'obtention de cette homologation qui récompense dix-huit mois de travail en étroite collaboration avec les services de la DGAC. Notre système a dû répondre aux exigences de l'aviation civile en matière de sécurité, de fiabilité et de qualité, exigences forcément très élevées compte tenu de son caractère totalement automatisé»*, a expliqué Stéphane Morelli, directeur général d'Azur Drones. *«Azur Drones ouvre des marchés aujourd'hui freinés par la complexité du déploiement des drones standards. Contrairement aux solutions télépilotées, nos drones sont très simples à utiliser, disponibles 24 h/24, précis et fiables»*, a précisé Jean-Marc Crépin, président d'Azur Drones. Toutefois, les sites sur lesquels devront opérer les drones, sont toujours soumis à autorisation de la DGAC.

Drone Protect System, le précurseur

À cette occasion, Philippe Gabet, directeur général de Drone Protect System a rappelé qu'il exploitait depuis plus d'un an déjà, un drone automatique sur un site sensible des Landes. *«Nous avons été précurseur dans le domaine des drones automatiques. Nous sommes à l'origine de la technologie de surveillance par drone automatisé et nous détenons un brevet depuis mai 2017. Nous avons reçu une première autorisation particulière d'exploitation de la DGAC pour un*

3 QUESTIONS À

NICOLAS MARCOU

Directeur des programmes drones, DGAC

© DR

En quoi l'homologation accordée par la DGAC à Azur Drones est-elle unique ?
Pour être précis, la DGAC a validé le principe du système du drone autonome Skeyetech d'Azur Drones. Soit, le vol automatique sur un site privé sur la base de trajectoires définies en fonction de la configuration et des installations du site, et supervisé par un « téléopérateur » ayant reçu la formation adéquate. Cette validation ne dispense pas d'une autorisation systématique de la DGAC pour chaque site, celle-ci devant s'assurer de la conformité de la demande pour le site visé, notamment par rapport aux trajets du drone, à l'implantation du site aux zones dans lesquelles le drone évolue et à la hauteur de survol. Toutefois, cette validation globale du système Skeyetech est une première et devrait faciliter le déploiement de drones automatiques pour des missions de sécurité sur des sites sensibles.

Quelle est la particularité de la formation des téléopérateurs dans ce cadre ?
Il s'agit d'une formation de télépilote « allégée » qu'Azur Drones peut délivrer, sur la base d'un plan de formation théorique et pratique que nous avons accrédité, et qui ne nécessite pas l'obtention du certificat de télépilote professionnel. Le téléopérateur est toujours en capacité de commander le retour du drone, de le faire atterrir ou de déclencher une descente d'urgence avec un parachute. Il ne peut en aucun cas modifier la trajectoire programmée.

Aujourd'hui, hors zones militaires, y a-t-il des drones automatiques en fonction ?
En 2018, Drone Protect System a obtenu une autorisation spécifique d'exploitation en vol automatique sur un site industriel dans le Sud-Ouest. Cette autorisation est en cours de renouvellement. Il y a peu d'acteurs sur le marché mais d'autres demandes sont aujourd'hui à l'étude et devraient prochainement aboutir.

site client en décembre 2017. Ces drones sont également sous la supervision d'un agent de sécurité que nous avons formé suivant un programme élaboré par la DGAC. Les autorisations annuelles sont en cours de renouvellement, et nous sommes en train de dupliquer le système sur d'autres sites. »

Drone Volt, le challenger

Avec son tout nouvel Air Shadow, Drone Volt vient rejoindre le club très fermé des fabricants de drones automatiques. Ce nouveau mini-drone professionnel entend se faire une place sur le marché des missions de surveillance, de reconnaissance d'inspection et de recherche. Programmable pour des missions automatiques, ce drone compact et résistant peut voler avec une faible signature visuelle et sonore jusqu'à 90 km/h de jour comme de nuit. L'Airshadow se décline en deux versions avec une portée allant jusqu'à 5 km. La transmission des données homme/machine en temps réel est sécurisée. *« L'Airshadow est une réelle innovation, garantissant grâce à son système d'encryptage, la confidentialité des données. Il est extrêmement robuste grâce à sa nouvelle structure. De plus, il a été conçu pour se déplacer à grande vitesse en toute discrétion. Ce nouveau drone répond à de fortes attentes du marché tout particulièrement aux États-Unis »* précise Olivier Gualdoni, PDG de Drone Volt. ■

LES DRONES FILAIRES D'ELISTAIR SÉCURISENT LE SUPER BOWL

© Elistair

Lors du 53e Super Bowl, organisé le 3 février 2019 à Atlanta, deux drones filaires Elistair ont été sélectionnés : l'un pour la diffusion TV via la chaîne de télévision américaine CNN, le second pour assister Unified Command, spécialiste de la surveillance et de la sécurisation des grands événements publics. Les équipes d'Unified Command, mandatées par la NFL (National Football League), ont connecté leur drone DJI M200 à la station Ligh-T d'Elistair, à des fins de surveillance aérienne permanente. Installé sur un toit à proximité du stade, à 50 mètres d'altitude, le drone a permis aux postes de contrôle d'Unified Command et de la NFL d'obtenir les images en direct des flux humains dans un rayon d'un kilomètre. Alimenté en permanence par la Ligh-T, il a cumulé 10 heures de vol en une seule journée, et 14 heures au total en deux jours.
Les responsables sécurité de la NFL ont exprimé leur intérêt à renouveler cette opération en raison de sa capacité à suivre un individu en continu, sans contrainte de passer d'une caméra fixe à une autre ni risque de sortie de champ du sujet.

INTRUSION

© DR

Les vols : un fléau pour les entreprises !

Essence, outils, matériels de chantier… les entreprises doivent de plus en plus faire face à des vols qui non seulement nuisent à leur activité, mais aussi à leur santé financière.

Un constat que font de nombreux chefs d'entreprises : les vols visant leurs sociétés sont de plus en plus nombreux et deviennent une véritable plaie. D'ailleurs, selon la Fédération française de l'assurance (FFA), le vol serait le deuxième risque – en fréquence – auquel les entreprises sont confrontées.

Constat que confirmait à *PSM,* l'année dernière, William Vinand, délégué général de la Fédération française du bâtiment du Val-d'Oise : *« Chaque semaine, on me remonte des dizaines de cas, rien que dans le département. Ce n'est pas tant la valeur des biens dérobés mais la désorganisation que cela entraîne. »*

Si ces vols, comme le souligne William Vinand, ont pour principale conséquence de désorganiser l'activité des entreprises touchées, ils ont également un coup financier non négligeable. C'est ce que révèle une étude de la Fédération française du bâtiment (FFB) de mars 2018. En effet, même si généralement les vols concernent du petit outillage, plus de 65 % des entreprises signalent en moyenne trois vols importants sur chantier dans l'année. Et elles constatent une augmentation de ces vols qui concernent les engins, petits ou gros, et le matériel (compresseurs, groupes électrogènes, etc.).

Un coût réel

Le coût de ces vols, pour les entreprises du BTP, par exemple, et toujours selon la FFB, est de plus en plus élevé pour les sociétés : 11 000 et 15 000 euros. Coût auquel il faut ajouter des coûts cachés et les frais générés par ces vols sur l'activité des entreprises.

17 000

Chaque année, services de police et de gendarmerie recensent plus de 17 000 cas de cambriolages de locaux commerciaux ou industriels, deuxième cible des malfaiteurs, derrière les résidences principales.

Dans son étude, la FFB illustre ce constat avec le vol d'un câble de grue : 6000 euros pour le remplacement du matériel volé et de ses accessoires. Somme à laquelle s'ajoutent les deux jours d'arrêt du chantier (10 salariés au chômage technique) dont le coût est estimé à 8000 euros, la remise en fonctionnement de la grue par un organisme agréé (1000 euros) et les pénalités de retard par rapport au planning d'exécution. Soit une perte sèche pour l'entreprise comprise entre 15000 et 20000 euros.
D'ailleurs, la FFB a initié, il y a dix ans, « Ras le vol ! », une action d'envergure pour aider les entreprises à se défendre face aux vols sur chantier. Cela consiste entre autres à mettre à la disposition des adhérents un outil d'analyse des risques et de solutions concrètes pour prévenir ce fléau. La FFB recommande, au minimum, de clôturer et verrouiller le chantier, de ne pas laisser de matériel en vue, de mettre des trackers sur le matériel, de prendre contact avec la police ou la gendarmerie pour signaler le chantier, dès que celui-ci dépasse une certaine durée, afin qu'il soit inclus dans les rondes. Pour les grands chantiers, il faut envisager des moyens plus élaborés comme un contrôle d'accès, la mise en place de caméras reliées à un centre de télésurveillance, des alarmes intrusion et éventuellement des équipes de sécurité.

Toutes les entreprises sont concernées

Les vols ne concernent pas que le BTP. Ainsi, comme le constate la CPME (Confédération des PME), les commerçants sont aussi la cible des voleurs. 75 % d'entre-eux disent avoir été victimes de tentatives de vol durant l'année 2017. Et comme dans le BTP, ces vols induisent des coûts pour les victimes : équipements avec des solutions de protection comme les portiques, les caméras de surveillance, des systèmes d'alarmes, etc. Auxquels s'ajoutent des prestations de gardiennage avec des gardiens de nuit et des vigiles dans la journée. ■

CONTRE LE SIPHONNAGE, UNE JAUGE INTELLIGENTE

Pour lutter contre les vols de carburants, certaines entreprises équipent les réservoirs de leurs camions avec une jauge intelligente qui est capable de mesurer le niveau du carburant toutes les minutes dans le réservoir afin d'alerter l'entreprise si ce niveau baisse de manière importante et brutale. Comme dans le cas d'un siphonage.

© DR

ÉTABLISSEMENTS SCOLAIRES

Deux lycées testent la reconnaissance faciale pour entrer en cours

En région Paca, deux lycées vont tester, à partir du printemps, la reconnaissance faciale à l'entrée de l'école.

© DR

Les lycées Ampère (Marseille) et des Eucalyptus (Nice) vont donc tester un système de reconnaissance faciale à l'entrée de l'établissements afin de filtrer les entrées et d'empêcher les tentatives d'intrusion. Votée en décembre dernier par la région Paca, ces tests ne font pas l'unanimité.
Du côté des établissements concernés, on justifie l'opération par la nécessité de fluidifier l'entrée dans les lycées et réduire les attroupements devant les portes des lycées lors du contrôle des carnets. Le tout pour savoir exactement qui entre dans les établissements. Le système, fourni par Cisco, se compose de portiques dotés de caméras à reconnaissance faciale. Ainsi, lorsqu'un élève se présente à la porte du lycée, il doit scanner un code QR via son téléphone portable, avant de regarder une des caméras. Si le système n'identifié par l'élève – parmi la base de données – il envoie un signal aux surveillants afin que ces derniers puissent intervenir.

Volontaires et contrôle de la Cnil

Mais certains s'opposent au recours à ces technologies de surveillance. À l'instar de Caroline Chevé, enseignante à Marseille, dans les colonnes de notre confrère *Le Parisien* : *« Le système supprime un contact essentiel dans la vie quotidienne d'un établissement. Les personnes qui s'introduisent sans autorisation dans les collèges ou les lycées le font par des entrées détournées ou en forçant l'entrée principale sans s'embarrasser de la présence ou non de caméras. »*
Le Syndicat national des enseignements de second degré (Snes), quant à lui, a déjà émis plusieurs réserves au sujet de ce dispositif. Dans un premier temps, le système sera uniquement testé sur la base du volontariat (dans chaque établissement, seulement une centaine d'élèves y participeront). Les volontaires auront d'ailleurs toujours la possibilité de se retirer dès qu'ils le souhaiteront. Par ailleurs, seuls ces derniers auront accès à leurs fichiers stockés chez Cisco. À noter, enfin, que la Cnil, qui a participé au développement du projet, va suivre sa mise en place dans les lycées. ■

3 QUESTIONS À

GAËTAN FEIGE

Responsable innovation, Cisco France

© DR

Pourquoi tester un système de reconnaissance faciale pour l'accès dans des lycées ?
La région Sud souhaite mieux sécuriser l'accès de ses établissements. Les tourniquets restent une alternative lourde à installer et ralentissent fortement les flux, ce qui est incompatible avec l'accès de centaines de lycéens sur quelques minutes. Aussi nous avons travaillé sur un système par comparaison biométrique qui permet un accès fluide, sans barrière physique tout en sécurisant l'accès à l'établissement.

Comment ce système fonctionne-t-il ?
Le système est très simple à installer : un portique, un PC et un câblage ethernet. Le lycéen ou le visiteur autorisé est doublement authentifié au niveau d'un portique, via un lecteur de badge NFC ou de QR code qui détient son identité numérique, et par la reconnaissance faciale. Deux caméras Intel (2D et 3D) grâce à des logiciels que nous avons développés, vont identifier la personne en comparant les données cryptées sur le badge du porteur. S'il y a concordance, le détenteur peut circuler librement dans la zone définie. S'il y a rejet, une alerte va être transmise à un responsable, proviseur, CPE ou autre. Le système couplé à la vidéosurveillance va pouvoir localiser l'intrus. La trajectoire de l'individu non autorisé va être suivie, sa silhouette étant cerclée de rouge sur l'écran de contrôle. Immédiatement alerté et en fonction de la situation, le responsable pourra prendre les mesures qui s'imposent.

Comment ce système s'inscrit-il dans le RGPD ?
Bien entendu, nous avons l'accord de la Cnil pour mener à bien ces essais. Pour mémoire, seule la carte (ou le QR code) détient la clé de décryptage du gabarit biométrique, lequel est également stocké sur la carte. De même, le logiciel d'analyse de la vidéosurveillance anonymise les individus tout en localisant leur présence et en indiquant autorisé/non autorisé. Cette première expérimentation au niveau mondial devrait nous permettre d'affiner le système et de l'étendre à d'autres environnements. Nous travaillons d'ores et déjà avec Bouygues construction et leur bureau d'études pour des problématiques liées à des sites sensibles.

SÉCURITÉ URBAINE

Le Palais des festivals et des congrès de Cannes labellisé « sécuri-site »

Le Palais des festivals et des congrès de Cannes est le premier site du département labellisé « sécuri-site ».

Fin janvier, la préfecture des Alpes-Maritimes a remis ce label, en présence de Stéphane Daguin, sous-préfet de Grasse, David Lisnard, maire de Cannes, Christophe Briez, commissaire central et chef du district ouest et Claire-Anne Reix, présidente du Palais des festivals, signataires de la convention.

« Securi-Site » est la reconnaissance de la politique de sûreté et de sécurité engagée par la Ville de Cannes et le Palais des festivals et des congrès en collaboration étroite avec les forces de police, les établissements de secours, les institutions nationales, locales et les équipes internes.

Le programme « tourisme et sécurité », lancé le 20 avril 2017 par le ministère de l'Intérieur, a pour objectif de renforcer la sécurité des touristes accueillis sur le sol français. Le programme prévoit le déploiement, dans chaque département, de conventions de sécurité sur des sites touristiques préalablement identifiés, et qui doivent bénéficier de mesures de sûreté propres à leur configuration. À ces conventions, vient s'ajouter le label « sécuri-site » qui fait l'objet d'un suivi par le comité départemental « tourisme-sécurité ».

Dans un contexte toujours sensible, le Palais est engagé dans une démarche proactive avec les pouvoirs publics, de manière à optimiser l'accueil des grands événements professionnels, des spectacles et des festivals.

La vigilance et la prévention, des priorités quotidiennes

Le Palais des festivals et des congrès de Cannes est donc le premier site labellisé des Alpes-Maritimes. Ce label a été attribué après étude des méthodes et moyens mis en place par le Palais, 1er site recevant du public du département (ERP). L'observation des exercices engagés pour améliorer les dispositifs et assurer les réflexes, la régularité des tests organisés et un audit réalisé in situ sont des gages des actions concrètes du Palais des festivals.

De gauche à droite : Claire-Anne Reix, présidente du Palais des festivals, David Lisnard, maire de Cannes, Stéphane Daguin, sous-préfet de Grasse et Christophe Briez, commissaire central et chef du district ouest.

© DR

Les processus et dispositifs de sécurité déployés, pendant les événements professionnels, salons et congrès mais également pour tous les événements, spectacles et festivals, répondent à un degré de vigilance élevé et adapté.

Attentes des congressistes

« Cette distinction est importante. Elle conforte nos efforts et nos engagements, positionne le site comme un lieu sûr et reconnaît le savoir-faire des équipes. Pour les organisateurs d'événements c'est aussi la garantie d'offrir à leur public des conditions de sécurité optimales. Cela reste une attente forte des congressistes notamment américains et ceux en provenance d'Asie », précise Philippe Leclerc, directeur de la sûreté et de la sécurité du Palais.

Enfin, pour David Lisnard, maire de Cannes, *« cette distinction est en parfaite cohérence avec les actions de la Ville en termes de sécurité. Cannes possède le réseau de vidéosurveillance le plus dense de France avec 629 caméras. Nous avons été la première ville de France à mettre en place un plan communal de prévention du risque terroriste dès 2016. À Cannes, village mondial, tous les nouveaux aménagements sont pensés pour protéger au mieux Cannois, congressistes et visiteurs. »* ■

LE DISPOSITIF DE SÛRETÉ ET DE SÉCURITÉ DU PALAIS

> Une équipe mobilisée 24 h/24 - 365 j/365, un site sous vidéosurveillance, des mises en situation régulières, des exercices réguliers, un plan de formation interne, une sensibilisation aux risques pour l'ensemble du personnel, une équipe qualifiée de près de 40 permanents…

> Pour tous les événements : un plan de sûreté adapté prévisionnel, des portiques, des contrôles visuels et une présence renforcée en fonction du nombre d'accrédités, une coopération avec la police municipale et nationale, une vidéosurveillance sur mesure.

SÉCURITÉ DES ENTREPRISES

Le CDSE et l'ASW Bundesverband lancent une alliance européenne

Le Club des directeurs de sécurité et de sûreté des entreprises (CDSE) et son équivalent allemand, l'ASW Bundesverband, ont signé une convention de partenariat pour développer des actions de coopération et de sensibilisation entre les deux pays dans les domaines de la sécurité, de la gestion des risques et de crise.

Alors que les membres des deux associations font face aujourd'hui aux mêmes menaces et enjeux, cette convention vise à favoriser les échanges entre les professionnels de la sécurité dans les entreprises des deux pays et les différentes autorités publiques impliquées.

Ce sont Émile Perez, directeur de la sécurité et de l'intelligence économique du Groupe EDF et administrateur du CDSE en charge des Relations Internationales du CDSE, et Volker Wagner, président de l'ASW Bundesverband, qui ont signé la convention entre les deux organisations.

« Ce rapprochement avec l'ASW Bundesverband est tout naturel et devrait nous permettre de répondre aux attentes de nos adhérents dont les activités sont de plus en plus diversifiées à l'international. Nos adhérents cherchent donc à échanger des bonnes pratiques, à collaborer avec leurs homologues étrangers… car leurs problématiques de sûreté-sécurité sont souvent comparables. Ce partenariat doit aussi permettre à l'Europe de porter une autre vision de la sécurité-sûreté, autre que l'approche anglo-saxonne, » explique à *PSM* Émile Perez. Avant de poursuivre : *« Notre collaboration avec notre confrère allemand devrait très vite déboucher sur des résultats concrets. Le premier d'entre-eux sera un événement, organisé à Paris au printemps prochain, qui nous permettra de rassembler des cadres et dirigeants de la sécurité-sûreté en entreprises venus d'autres pays pour échanger avec eux, partager nos approches et leur donner l'idée de rejoindre ce partenariat. »*

À gauche, Émile Perez, directeur de la sécurité et de l'intelligence économique du Groupe EDF et administrateur du CDSE et Volker Wagner, président de l'ASW Bundesverband.

© DR

Réunissant les professionnels allemands de la sécurité et les membres d'associations fédérales spécialisées, l'ASW Bundesverband entretient des échanges soutenus entre les entreprises, les décideurs en matière de politique de sécurité, les institutions, les universités et les centres de recherche. ■

© DR

SÉCURITÉ PRIVÉE

Croissance soutenue mais faible rentabilité

Selon une étude de l'Insee, en 2016, les 5 700 unités légales du secteur de la sécurité privée employaient 139 000 salariés en équivalent temps plein. Elles réalisaient 7,0 milliards d'euros de chiffre d'affaires.

Autre constat : l'activité progresse fortement en raison d'une demande soutenue. Le chiffre d'affaires augmente en moyenne de 3,8 % en valeur par an depuis 2010. Le secteur comprend peu de grandes entreprises, ce qui accroît la concurrence et pèse sur les prix (+ 1,2 % par an sur la période). En 2016, le taux de marge moyen n'est que de 3,7 % et 29 % des unités ont même une rentabilité négative. Cette faible rentabilité s'explique sans doute par le poids des donneurs d'ordres qui font jouer la concurrence face à un secteur modérément concentré.

Les délais de paiement des clients sont globalement élevés comparés à ceux des autres activités de soutien : un quart des unités constate un délai moyen supérieur à 75 jours de chiffre d'affaires. Par ailleurs, les rémunérations sont modestes : deux tiers des salariés perçoivent moins de 13 euros bruts par heure. La qualification et le taux d'encadrement sont faibles dans ce secteur dans lequel seuls 2 % des salariés sont des cadres. ■

→ **www.insee.fr/fr/statistiques/3648459**

MÉTIERS DE LA SÉCURITÉ ET DE LA SÛRETÉ

La CCI Paris Île-de-France et le groupe Goron créent une formation

La CCI Paris Île-de-France et le groupe Goron, l'une des premières entreprises sur le marché de la sécurité, créent une filière de formations en apprentissage préparant aux titres professionnels de niveaux V et IV dans le domaine de la sécurité des biens et des personnes. En raison du développement continu de ce secteur et d'une forte demande de personnels qualifiés, la CCI Paris Île-de-France mobilise son école l'ÉA et s'engage dans une coopération à long terme avec le groupe Goron, déjà très investi dans la formation continue au travers de sa filiale Cecys. L'objectif pour Goron est de participer à la formation de ses futurs agents sans exclure la possibilité du placement des apprentis en formation dans d'autres entreprises du secteur.

© Goron

Pour la CCI Paris Île-de-France, qui forme chaque année 15 000 apprentis, cette alliance confirme une fois de plus son engagement en faveur de l'apprentissage, une voie de formation porteuse pour les jeunes, les entreprises et l'emploi.

Le partenariat vise les premiers niveaux de qualification avec des perspectives de formations concernant les niveaux supérieurs, comme c'est déjà le cas pour L'ÉA. L'école offre en effet des formations aux premiers niveaux et comprend également des formations dans le supérieur sur la sécurité. Deux sections préparant à l'obtention de titres professionnels détenus par Formaplus 3B, partenaire du groupe Goron, ont été ouvertes à la rentrée 2018. Il s'agit du titre de niveau V « agent de prévention et de sécurité » et du titre de niveau IV « agent de prévention et de sécurité - chef de poste ». Au total, environ 40 jeunes seront formés durant cette première année, leur insertion professionnelle étant garantie. ■

DIRECTEURS SÉCURITÉ

Le Mase publie un recueil de conseils pour manager la sûreté

Le Mase publie un recueil des bonnes pratiques de sûreté pour les entreprises intervenantes et les entreprises utilisatrices, dans sa collection *« Les conseils de Masecotte »*. Ce document présente, pour les entreprises intervenantes, une définition de la politique de sûreté, les consignes et procédures permettant de maîtriser la sûreté, les formations et sensibilisations des salariés, l'analyse des incidents en matière de sûreté, le retour d'expérience, etc. De leur côté, les entreprises utilisatrices pourront y trouver des bonnes pratiques recommandées par le Mase dans le cadre du dossier de sûreté et se référant à la cartographie des zones sensibles, au contrôle d'accès et à la coordination des moyens en relation avec les forces de sécurité publique.

→ http://mase-asso.fr/wp-content/uploads/2018/12/Les-conseils-de-Masecotte-dec2018.pdf

VIDÉOSURVEILLANCE

Gros succès pour la Nuit de l'AN2V !

Le 29 janvier dernier, l'association présidée par Dominique Legrand a accueilli plus de 300 personnes au musée des Arts forains, à Paris.
Parmi les participants, quelques invités de marque : Luc Ferry, Jean-Michel Fauvergue et Philippe Gabilliet. Chacun, lors d'une intervention intéressante, a fait profiter l'assistance de son expertise ou d'un regard prospectif sur l'avenir des métiers de la sécurité.
De son côté, Dominique Legrand a profité de l'intervention du député Jean-Michel Fauvergue pour faire le point avec lui sur quelques axes de réflexion contenus dans le rapport Thourot-Fauvergue.
Les points abordés ont concerné :
- les schémas départementaux de vidéoprotection ;
- la possibilité pour les bailleurs de mettre en place de la vidéosurveillance aux abords immédiats des immeubles ;
- la nécessité de renforcer les dispositifs de mutualisation en matière de vidéoprotection ;
- la possibilité d'accorder aux communes l'autorisation d'installer des Lapi ;
- le possible accès des forces publiques aux installations privées de caméras afin de faciliter leurs missions et leurs interventions.

De gauche à droite : Georges Fenech, ex-magistrat et ancien député UMP, Luc Ferry, ancien ministre de l'Éducation nationale et Dominique Legrand, président de l'AN2V.

© DR

Autant de points sur lesquels tous les acteurs concernés par l'utilisation de systèmes de vidéoprotection attendent des réponses claires dans les mois qui viennent. ■
À noter aussi le prochain grand événement organisé par l'AN2V : Les universités de l'AN2V qui se dérouleront du 30 au 31 janvier 2020 à Lyon.

GALA DE LA SÉCURITÉ

Faire face aux enjeux de demain

Le 6 février dernier, plus de 400 participants, se sont retrouvés pour la 8e édition du gala de la sécurité, salle Wagram, à Paris.
Laurent Nunez, secrétaire d'État auprès du ministre de l'Intérieur, Jean-Michel Fauvergue, coauteur du rapport sur les réformes concernant le continuum de sécurité, et Xavier Latour, universitaire spécialiste du droit de la sécurité, ont débattu autour des futurs enjeux pour la filière de la sûreté. Quatre start-up dans le domaine de la sécurité, Heropolis, Ido-Data, Kateo et Veesion, ont pu présenter leurs innovations aux 300 décideurs présents à la soirée. Suite aux votes des participants, Veesion, a remporté le trophée de l'innovation 2019 pour son logiciel d'analyse vidéo, qui repère les voleurs dans les commerces sur la base du comportement (voir p. 10).

© Franck DUNOUAU

Cette manifestation annuelle, qui regroupe industriels, représentants d'organismes professionnels et directeurs de sécurité–sûreté du secteur public et privé, rencontre chaque année un succès grandissant. Retransmise sur les réseaux sociaux, la table ronde a été suivie en direct par 18 200 personnes uniques. D'ores et déjà, le rendez-vous est pris pour la 9e édition gala de la sécurité, qui se déroulera le 5 février 2020. ■

Agenda

MARS 2019

AccesSecurity
Du 6 au 7 mars 2019 – Marseille
http://accessecurity.fr

Security & Safety Meetings
Du 19 au 21 mars 2019 – Cannes
www.security-and-safety-meetings.com

AVRIL 2019

Conférence « Évacuation du souffle d'explosion et désenfumage »
8 avril 2019 – Paris
www.agrepi.com/rencontres

MAI 2019

Préventica Paris
Du 21 au 23 mai 2019 – Paris
www.preventica.com

JUIN 2019

Ifsec
Du 18 au 20 juin 2019 – Londres
www.ifsec.events/international

OCTOBRE 2019

APS
Du 1 au 3 octobre 2019 – Paris
www.salon-aps.com

IBS
Du 2 au 3 octobre 2019 – Paris - Porte de Versailles
http://www.ibs-event.com

Préventica Marseille
Du 8 au 10 octobre 2019 – Marseille
www.preventica.com

NOVEMBRE 2010

Milipol
Du 19 au 22 novembre 2019 – Paris-Nord Villepinte
https://event.milipol.com/2019/

PROFESSIONNELS DE LA SÛRETÉ/SÉCURITÉ

Formation de l'INHESJ

© DR

Destinée aux professionnels de la sûreté/sécurité et de la gestion des risques et des crises, la prochaine session de la formation « Security Manager » aura lieu du 1er au 3 avril 2019. Les candidatures sont ouvertes.
Objectifs de la formation :
- Définir et mettre en place une politique de prévention et de traitement des risques efficace, en développant une vision globale de la sécurité-sûreté.
- Concevoir et animer une politique de sûreté adaptée favorisant le développement de l'entreprise.
- Appréhender les fondamentaux de l'encadrement opérationnel de la gestion et de la communication de crise.

Les stagiaires de la formation spécialisée « Security Manager » sont sélectionnés sur dossier parmi les professionnels des directions sûreté/sécurité, les responsables de gestion des risques et de gestion de crises, tout professionnel issu de la sphère publique ou privée qui souhaite intégrer ces fonctions.
Le dossier de candidature, la convention et la présentation de la formation sont disponibles à l'adresse suivante : https://inhesj.fr/formations/intelligence-et-securite-economiques/nos-formations/cycles-specialises (Contact : securite-economique@inhesj.fr) ■

Carnet

MAIRIE DE PARIS

MICHEL FELKAY


© DR

Ancien commissaire divisionnaire et ex-patron de police des transports, Michel Felkay prend la direction de la DPSP (Direction de la prévention, de la sécurité et de la protection) de la Ville de Paris.
Après avoir dirigé une BAC en banlieue, Michel Felkay a été, entre autres, patron de la BAC-N (nuit) de Paris (de 1998 à 2001), commissaire central du XVe arrondissement et chef de la brigade des réseaux ferrés d'Île-de-France de 2004 à 2006.

HGH INFRARED SYSTEMS

LAURENT FULLANA


© DR

HGH Infrared Systems a nommé Laurent Fullana en tant que directeur général. Il travaillera au côté de Thierry Calmpos, président d'HGH. Âgé de 54 ans, Laurent Fullana est diplômé de l'ESPCI et de l'École centrale Paris et titulaire d'un MBA de Columbia. Jusqu'à maintenant, il était directeur général de Sofradir.

GROUPE PARTOUCHE

MARTINE MONTEIL


© DR

Le Groupe Partouche (casinos) vient de recruter Martine Monteil en tant que conseiller sur les questions de sécurité et de sûreté. Rappelons que Martine Monteil a été la première femme à prendre la tête de la direction centrale de la police judiciaire en 2004. En 2008, elle avait été nommée préfète et secrétaire générale de la zone de défense de Paris.

GROUPE PARTOUCHE

ÉRIC BATTESTI


© DR

Le Groupe Partouche a également recruté un autre « grand flic », Éric Battesti, qui aura aussi pour mission de conseiller l'exploitant de casinos sur les questions de sécurité et de sûreté. Éric Battesti a notamment dirigé les Renseignements généraux en Corse jusqu'en 2007 avant de devenir attaché de sécurité intérieure à l'ambassade de France à Londres, puis à Pékin.

DOMINIQUE LEGRAND

Président de l'AN2V

« Autoriser la diversification des usages de la vidéosurveillance. »

Depuis 2004, Dominique Legrand préside aux destinées de l'AN2V. Plus de quinze ans à se battre pour faire évoluer les mentalités autour de la vidéosurveillance et faire en sorte qu'elle soit utilisée au mieux des intérêts de tous. Il a accepté répondre aux questions de *PSM*.

Pourquoi avoir décidé, il y a maintenant quinze ans, de créer l'AN2V ?

À l'époque, en 2004, il n'existait pas en France de lieu où on pouvait réfléchir, sereinement, sur le bien-fondé de la vidéosurveillance. On déployait des caméras, sans doctrine, sans référentiels, sans bonnes pratiques, sans référents sûreté… Il faut se rappeler que nous sortions à peine de la loi de 1995. Tout restait à faire. Or, à la suite d'une rencontre entre des représentants des villes de Strasbourg et de Lyon, les participants de la réunion m'ont suggéré de créer une association pour aider les villes à partager leur expérience, leur vécu sur la vidéosurveillance. C'est comme cela qu'est née l'AN2V en se

donnant comme mission, dès l'origine, d'être le point de rencontre et d'échanges entre l'offre – tous ceux qui vivaient de la vidéosurveillance, la demande – les utilisateurs, publics ou privés – et l'État. Avec la résolution ferme et maintenue jusqu'à maintenant d'être une association neutre et indépendante. Aujourd'hui, l'AN2V compte 130 adhérents issus du monde de l'offre et leur permet de rencontrer, tous les ans, plusieurs milliers de représentants des villes françaises, de l'État, des référents sûreté… Notre force est d'être un véritable lieu de débats, d'échanges, un vrai think tank qui, tous les ans, organise des réunions dont les sujets nous sont suggérés par nos adhérents pour répondre vraiment aux questions qu'ils se posent et parler réellement des besoins sur le terrain.

Qu'est-ce qui, selon vous, a changé dans la perception de la vidéosurveillance depuis 2004 ?
Premier constat : elle s'est généralisée. Il faut se rappeler qu'au tournant de l'an 2000, la vidéosurveillance était très loin de faire l'unanimité. Big Brother, espionnage, flicage… Régulièrement des articles et des reportages dénonçaient son déploiement dans telle ou telle ville. Les débats étaient même à forte connotation politique. Il a fallu se battre pour faire évoluer les mentalités et faire retomber l'opposition. Désormais, les caméras sont d'une manière générale acceptées partout et leur installation ne suscite plus les levées de bouclier que nous avons pu connaître. Autre évolution notable : les technologies évidemment. On a peu à peu abandonné l'analogique pour passer au numérique et au tout IP. Aujourd'hui, globalement, les technologies de la vidéosurveillance sont maîtrisées et répondent, normalement, aux attentes des utilisateurs finaux. De nos jours, on ne se bat pas sur la qualité de l'image, en tant que telle, ni sur la faisabilité technologique des installations. On doit plutôt désormais se concentrer sur les problèmes d'ingénierie de la vidéosurveillance et de déploiement dans un nouveau contexte marqué par le RGPD, le risque cyber… Il faut comprendre que ce qui nuit à la vidéosurveillance est principalement dû au fait qu'on est toujours très faible sur l'ingénierie, la destination des projets, et qu'on se retrouve trop souvent avec un fort décalage entre les vœux exprimés sur le cahier des charges et le déploiement effectif des caméras et leurs conditions de maintenance. C'est un axe de travail majeur pour l'AN2V et tous ceux qui participent à ses travaux…

« L'incapacité à remonter de l'info en temps réel est le vrai point d'achoppement de la vidéosurveillance actuellement. »

Les lecteurs réguliers de *PSM* doivent le savoir : vous vous battez pour faire sauter certains freins qui nuisent à la bonne utilisation de la vidéosurveillance. Pouvez-vous nous les rappeler ?
Ils sont de divers ordres. Tout d'abord, il faut changer d'échelle. Et cesser de raisonner en termes de communes, de territoires cloisonnés. Il faut se poser la question du « bassin de vie » d'une installation de vidéosurveillance : doit-elle se contenter de filmer sur le territoire de telle ou telle commune ? À mon avis, non, car la délinquance ne s'arrête pas à la frontière d'une commune. Il faut donc, et c'est là un deuxième frein, se donner les moyens de filmer aux abords. De ne plus se servir uniquement des caméras d'une installation d'une ville. On doit, pour faciliter le travail de la police, de la gendarmerie…, pouvoir se servir aussi des caméras du domaine privé qui elles aussi filment des portions de territoire et peuvent permettre de pallier l'absence d'une caméra à tel ou tel endroit. Il faut faire sauter cette barrière entre privé et public. On marche sur la tête avec cette problématique des abords… Dernier frein : cessons d'interdire les applications Lapi ou de reconnaissance faciale possibles avec les systèmes actuels.

Vous savez ce qu'on va vous répondre : Dominique Legrand prêche pour un « super » réseau, connectant tous les réseaux existants, afin de surveiller tout le monde, tout le temps… Un projet liberticide…
Je vous répondrais que ce n'est pas la caméra qui pose problème mais celui qui est derrière son écran, qui regarde. ● ● ●

BIO EXPRESS

1988 Après Polytechnique, débute sa carrière chez Alcatel.
1998 Rejoint Thales.
2013 Directeur général adjoint et membre du comité exécutif de Thales.
Depuis 2014, président du Conseil des industries de la confiance et de la sécurité (CICS). ■

DOMINIQUE LEGRAND

Président de l'AN2V

« Ce n'est pas la caméra qui est potentiellement liberticide mais celui qui est derrière son écran, qui regarde. »

● ● ● Il faut bien comprendre que la vraie question est le nombre de moniteurs et la capacité de regarder. À quoi tout cela sert si personne n'est derrière son écran pour aider les forces de l'ordre à intervenir le plus tôt possible et éviter ainsi de se contenter de faire de la relecture et recherche de détails a posteriori, après un drame ? Quand on aura résolu le problème de qui regarde, on ne se posera plus toutes ces questions et on pourra enfin exploiter les installations de caméras comme elles devraient l'être, pour faire du temps réel. Il faut donc que ceux qui visualisent les écrans de ces grands dispositifs interconnectés aient la même formation (avancée), le même niveau de confidentialité et de discrétion qu'un OPJ.

L'État a-t-il les effectifs suffisants pour faire cela ?

Évidemment non. C'est pour cela qu'il faut interconnecter les réseaux existants, privés et publics, et les doter de capacités en intelligence artificielle afin qu'ils soient capables de remonter la bonne information, plus vite, au responsable derrière l'écran. Il faut mettre en place une sorte de super CSU ou PC de sécurité qui viendrait chapeauter les CSU et PC vidéo implantés dans la région, afin d'y faire converger les informations pour faciliter le travail des forces de l'ordre. Cette incapacité à remonter de l'info en temps réel vers les gens les plus à même d'intervenir dans un cadre légal, est le vrai point d'achoppement de la vidéosurveillance actuellement. Il faut pouvoir utiliser les images filmées en local par les systèmes privés des pharmacies, bars-tabac, commerces de proximité, entreprises... Enfin, il faudrait faire fusionner le centre d'information et de commandement (CIC) de la police nationale et le Centre d'opérations et de renseignement de la gendarmerie (Corg) pour en faire un point de concentration des données utiles aux forces de l'ordre, sous autorité de la préfecture.

Quel bilan tirez-vous de l'aide apportée par l'État pour le déploiement de la vidéosurveillance ?

Le FIPD (Fonds interministériel de prévention de la délinquance), créé par la loi du 5 mars 2007, a été très utile. Et il faut le maintenir. Ce système de cofinancement a aidé les communes à financer l'extension de leur réseau de vidéosurveillance, si cette extension était nécessaire à l'État. Là où ce dernier avait un intérêt à renforcer une installation, il prenait en charge une partie du financement. Il faut maintenir le système et permettre aux collectivités d'en profiter encore plus facilement et plus rapidement.

Pour conclure, que faudra-t-il encore changer dans l'absolu pour que la vidéosurveillance s'inscrive à part entière dans la smart city ?

Je pense qu'on doit d'abord revoir l'organisation de tous les services des communes afin qu'ils s'approprient les caméras pour en faire un outil dont l'utilisation aille au-delà de la simple surveillance. Pour cela, on doit nommer dans chaque département, bloc communal ou commune un « Monsieur Smart », à forte capacité organisationnelle, dépendant directement du maire, afin qu'il puisse veiller à ce que chaque projet d'une certaine ampleur intègre un volet « smart » pour que la Ville – le territoire – se dote de moyens qui pourront s'interconnecter, remonter de l'information, en temps réel, pour tous les services intervenant sur le territoire : police, gendarmerie, police municipale, sécurité privée... et ainsi participer réellement au continuum de sécurité. Il faut aussi autoriser la diversification des usages de la vidéosurveillance : Lapi, par exemple. Enfin, les maires doivent s'impliquer dans tout cela : la smart city, la vidéo et ses capacités, le territoire de confiance. Il faut former les décideurs. Les réseaux sont là, ou en passe de l'être, préparons-nous à les utiliser pour la sécurité de tous. ■

L'AN2V, C'EST AUSSI

4 réunions thématiques en 2019
- Jeudi 4 avril 2019 - Retours d'expérience sur les analytics audio et vidéo
- Mardi 25 juin 2019 - Innovations dans le domaine des technologies de sûreté
- Jeudi 10 octobre 2019 - Quels sont les nouveaux usages dans le domaine de la vidéoprotection ?
- Jeudi 12 décembre 2019 - Mutualisation des dispositifs de sûreté.

Les universités de l'AN2V
30-31 janvier 2020
Lyon – Espace Tête d'Or

L'AN2V est aussi un organisme de formation pour :
- la formation des opérateurs vidéo ;
- la formation technologique.

www.an2v.org

HIKVISION

DS-PR1-60

Disponible sur le Roadshow 2019

SECURITY RADAR DE HIKVISION

DISPONIBLE MAINTENANT

- Détection large à 100°, jusqu'à une distance maximum de 60m
- Localisation précise de l'emplacement et suivi du déplacement
- Détection d'intrusions, avec jusqu'à 32 intrusions
- Enregistrement vidéo possible, avec jusqu'à 4 caméras PTZ Hikvision
- Ip67 et ik09 certifiés, fiabilité par tout temps
- Diminution de fausses alarmes grâce à la technologie beam-forming et aux algorithmes d'analyse intelligente

Hikvision France
6 rue Paul Cézanne,
93360 Neuilly-Plaisance
France
T +33 (0)1 85330450
info.fr@hikvision.com

SKYHAWK
SURVEILLANCE

Ingénieux. Fiable. Sûr.

Solution de stockage Seagate conçue pour la surveillance.

1-8 To

Garantie 3 ans

Jusqu'à 64 caméras

CHARGE DE TRAVAIL 180 To par an

24/7

Capteur RV

SEAGATE

dossier

Formez et sensibilisez vos salariés aux risques !

Les entreprises n'en sont pas toutes conscientes mais leurs salariés sont exposés à des risques dans leur travail. On pense évidemment aux accidents du travail mais pas uniquement : attentat, enlèvement, corruption, vols de données… Il faut former ses collaborateurs pour qu'ils respectent certaines règles et qu'ils ne deviennent pas eux-mêmes source de risques.

© Getty image

SOMMAIRE

Les attentats et enlèvements ne sont pas les seuls risques auxquels peuvent être exposés les salariés. La tentative de corruption en est un autre.

© Getty image

Former ne suffit plus. Il faut constamment maintenir la vigilance

La formation est la première étape pour faire acquérir une culture sécurité à ses collaborateurs et les préparer à éventuellement faire face à une menace. Mais cela ne suffit pas. Vous devez constamment vous assurer que les règles apprises en formation sont respectées. Sans quoi…

Attentat, enlèvement, crime organisé, espionnage, corruption, vol… les entreprises sont toutes exposées – même si certaines pensent que cela n'arrive qu'aux autres – à des menaces. *« Et malheureusement, on n'a jamais vraiment fait le tour de ces menaces,* explique Éric Davoine, président du chapitre français d'Asis International et Regional Security Manager chez Walt Disney Company. *Il y a certes les risques classiques, comme les incendies, les accidents du travail, les risques professionnels, les vols…, mais aussi tout ce qui reste de l'inconnu, qui peut ne pas rentrer dans le spectre direct de la direction sûreté de l'entreprise et contre lequel il faut tout de même se préparer et prévoir des règles et procédures afin de protéger l'entreprise. »*

D'une manière générale, en matière de malveillance, les entreprises doivent faire face à deux types de risques liés aux personnes. *« D'une part, les risques associés aux collaborateurs, les enlèvements, les atteintes à la sûreté de l'entreprise...,* précise Olivier Hassid, directeur conseil sécurité & sûreté chez PwC France. *Et, d'autre part, les risques frauduleux comme les comportements malveillants, la corruption ou encore le vol d'informations. »*

Par conséquent, l'entreprise doit travailler sur deux axes. Organiser sa protection contre les risques liés à des collaborateurs qui peuvent être eux-mêmes malveillants. Rappelons qu'une majorité des cas de malveillance ont une origine interne ou en lien avec un collaborateur, dans une proportion comprise entre 45 et 55 %. Elles doivent parallèlement proté-

ger leurs collaborateurs contre les risques auxquels elle peut les exposer sur le lieu de travail et durant leur temps de travail, sur le territoire national ou à l'étranger.

Les choses évoluent doucement

Force est de le constater : si les entreprises ont globalement mis en place des mesures pour se protéger d'un attentat ou assurer la sécurité de leurs expatriés, tout n'est pas encore parfait en matière de risques liés aux personnes. *« On part de loin,* confirme Olivier Hassid. *Cela se met donc en place progressivement dans les mœurs mais si on se concentre sur les entreprises françaises, on en est encore au début, en phase d'implémentation. »*

Les entreprises ont une vision restreinte des risques auxquels elles peuvent être exposées. *« La menace terroriste est un peu l'arbre qui cache la forêt sur ce sujet,* reconnaît Éric Davoine. *Combien d'actes de terrorisme sur le lieu de travail a-t-on déploré en France ? Très peu. Et il est rare que les salariés y soient réellement exposés sur leur lieu de travail. Hormis le cas d'entreprises travaillant à l'international dans des zones géographiques très exposées. Or, il faudrait, qu'à l'instar des sociétés anglo-saxonnes, les entreprises comprennent que leur tableau des risques est presque sans fin et qu'il comprend des sujets très divers comme le harcèlement, les bagarres au sein de l'entreprise, les violences par arme à feu sur les lieux de travail… des sujets plus vastes que la prévention des risques à la française. »*

Point de vue que partage Nicolas Le Saux, président d'Atao Consulting : *« En matière de prévention des menaces liées aux personnes, nous sommes face à deux types de réponses. D'une part, les entreprises qui, par la nature même de leur activité, ont généralement conscience des risques et menaces auxquels sont exposés leurs personnels. Ce sont en général des entreprises dont les enjeux assurantiels importants les ont sensibilisées sur ce sujet. Et, d'autre part, des entreprises qui, même si elles s'assurent contre le risque, ont encore parfois tendance à le sous-estimer. »*

Une menace plus endogène qu'exogène

Comme le rappelle Éric Davoine, *« la menace à laquelle sont exposées les entreprises, est parfois plus endogène qu'exogène. Or, la notion de confiance dans l'entreprise est très importante. Et la menace endogène va à l'encontre de cette confiance qui doit exister entre un collaborateur et son employeur. Intégrer ce modèle de raisonnement n'est pas aisé pour l'entreprise alors qu'il est primordial pour qu'elle puisse se protéger. Elle doit donc ne pas hésiter à se doter des moyens et procédures lui permettant d'assurer sa sécurité. »*

Comment faire pour contrer la menace endogène ? Lutter contre ce qu'Éric Davoine appelle « l'insider », la personne malveillante qui a réussi à intégrer les équipes de l'entreprise qu'elle vise ?

Olivier Hassid l'a déjà évoqué, on peut se livrer à une enquête pour vérifier l'honorabilité de la personne qu'on souhaite recruter. Mais on peut aller un peu plus loin. *« L'enquête d'honorabilité – ce qu'on appelle le background check – est une première étape. Elle peut être efficace pour se protéger des tentatives de fraudes… mais elle doit toujours se faire avec l'autorisation du salarié, selon la réglementation du pays. Il faut* ● ● ●

SUR LE TERRAIN

RUDOLPHE PROUST

Directeur de sureté groupe au sein d'Altarea Cogedim

© DR

« FAIRE ACQUÉRIR LES BONS RÉFLEXES À NOS COLLABORATEURS. »

« Altarea Cogedim est un groupe foncier dont l'une des activités est la gestion de centres commerciaux. Sites qui, malheureusement, peuvent être la cible d'actes terroristes ou de malveillance. Notre rôle, au sein de la direction sûreté, est de nous doter des moyens et outils nous permettant de favoriser l'intégration des bons réflexes par les collaborateurs du groupe de manière à anticiper et à détecter les risques et menaces éventuels. La sécurité d'un centre commercial repose, à la base, sur ce qu'on appelle la "security by design", c'est-à-dire les moyens physiques et techniques qui permettront de protéger le site. Elle s'intègre dès la conception du site. Mais elle ne se limite pas à cela. Nos collaborateurs et nos prestataires doivent être en mesure de détecter et de faire remonter l'information en cas de doute vers les autorités publiques. Nous avons donc mis en place un programme de sensibilisation à la sûreté à destination de nos directeurs de centres et de leurs proches collaborateurs. Ces formations reviennent sur la politique interne en matière de sécurité sur les mesures mises en place par les pouvoirs publics, comme le plan Vigipirate, sur les évolutions technologiques, et sont régulièrement enrichies par des interventions de la gendarmerie ou de la police nationale. Il nous faut faire en sorte que nos directeurs de centre et leurs collaborateurs soient capables d'identifier une situation anormale afin de gagner en précocité pour intervenir. Nous les maintenons vigilants par des rappels réguliers via des interventions ponctuelles, sur des sujets d'actualité, sur le suivi des menaces… Ils doivent intégrer les bons réflexes, les bonnes attitudes afin de bien réagir en cas d'attaque pour ne pas se mettre en danger ou par un mauvais comportement aggraver la situation. Nous avons aussi une action à destination des salariés des enseignes implantées dans nos centres commerciaux, conjointement avec le référent sûreté (gendarme ou policier). »

OUTILS

Pensez à alerter vos collaborateurs en cas d'incident

On ne vous le souhaite pas, mais une fois l'incident en cours, il faut pouvoir diffuser rapidement des messages d'alerte et s'assurer que ces messages ont été reçus par les personnes auxquelles ils étaient destinés. La société Ascom a acquis une véritable expertise sur le sujet et met à votre disposition des moyens PTI/DATI qui permettent non seulement de demander du secours ou une aide en cas de besoin, mais de recevoir des messages d'alerte en cas d'incident. Cela peut toujours être utile.

porter à sa connaissance qu'une vérification pourra être faite dans le cadre d'une éventuelle embauche.» Avant d'ajouter : «Il faut donc commencer par cartographier les postes sensibles afin d'identifier les collaborateurs à risques. Ceux auxquels n'est associé aucun risque et ceux qui peuvent être la cible d'actes de malveillance, explique-t-il. Et, pour ce dernier cas, il ne s'agit pas seulement du top management, mais aussi des personnes dont le rang hiérarchique peut être moindre comme les assistants de la direction, de cadres dirigeants. PwC a développé une expertise sur ce sujet et accompagne les entreprises dans cette démarche en les aidant à vérifier, dans un cadre légal strict et respectant le droit français, le parcours professionnel des collaborateurs, l'identité du candidat – avec son autorisation, afin de vérifier l'honorabilité de la personne. Mais les entreprises ne doivent pas se limiter à cela. Elles doivent aussi cartographier de manière précise leurs risques malveillance. Mais peu d'entreprises le font. C'est pourtant une démarche importante qui leur permettra d'identifier les risques de malveillance globale qu'elle sera peut-être amenée à supporter comme le terrorisme, l'attentat, un enlèvement ou la corruption. Cela permet de définir des risques majeurs et de dérouler un plan de prévention et de protection, avec des mesures à mettre en place, avec une feuille de route.»

Cartographier puis former

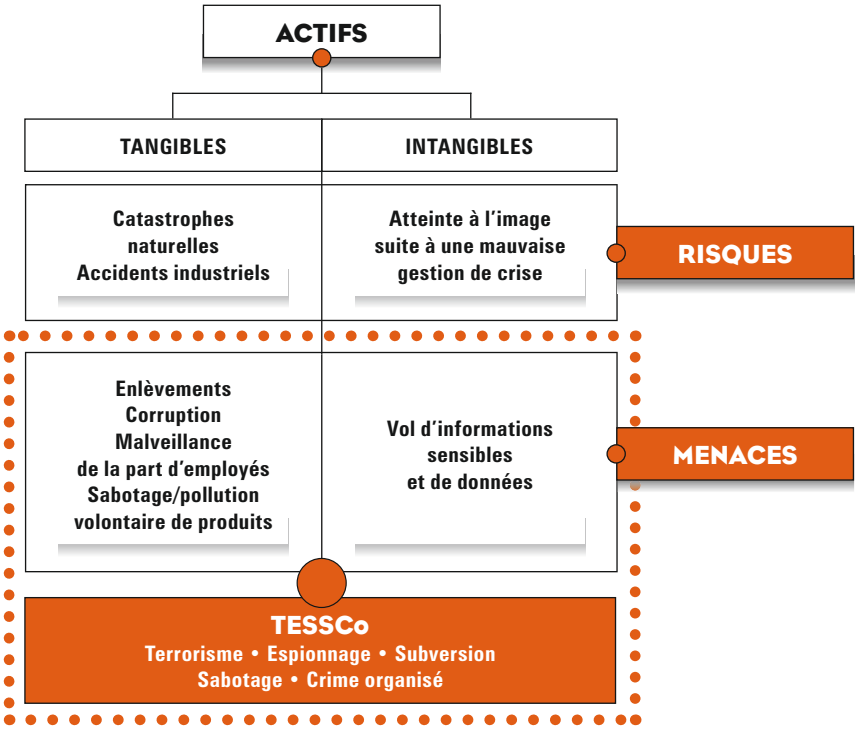
Avant d'engager la formation des salariés, il est donc important de bien identifier les risques. «Cette phase qui se situe en amont d'une action de formation est très importante, explique Alexandre Carle, Managing Director chez Other Solutions, société de gestion de risque basée à Londres. Elle permet d'évaluer les risques et de faire apparaître les moyens

© DR

«En préalable à toute formation, il faut commencer par cartographier les postes sensibles afin d'identifier les collaborateurs à risques.»

OLIVIER HASSID, DIRECTEUR CONSEIL SÉCURITÉ & SÛRETÉ CHEZ PWC FRANCE

EXEMPLE D'OUTILS SIMPLES DE CARTOGRAPHIE DE RISQUES ET MENACES



RISQUE : un événement possible, quoique incertain, pouvant porter préjudice.
MENACE : une déclaration ou une indication de l'intention d'infliger du tort ou des dommages.
TESSCo : méthodologie d'analyse des menaces exhaustive utilisée par plusieurs services de l'État en France. Aussi utilisée par l'Otan sous l'acronyme TESSOc (Terrorism, Espionnage, Subversion, Sabotage, Organized Crime).

Les expatriés ou voyageurs internationaux des entreprises peuvent être exposés à de nombreux risques. Ils doivent être formés au respect de certaines règles pour éviter que le pire arrive...

© Getty image

3 QUESTIONS À

ALEXANDRE CARLE

Managing director chez Other Solutions

© DR

Quels sont les moyens de s'assurer qu'une formation débouchera sur le respect des règles qu'elle édicte ?

Former des collaborateurs doit s'appuyer sur une bonne compréhension de la manière dont les gens opèrent. Les règles de sécurité qu'on leur communique (celles de leur entreprise) ne doivent pas être perçues comme une contrainte. La formation est donc un travail assez fin et qui doit s'appuyer sur le renforcement de la responsabilité individuelle. Et la pratique est essentielle. Mais la formation n'est qu'un outil. Nous devons également trouver des biais pour faire respecter les règles de sécurité. Il faut donc aider l'entreprise à faire émerger une culture sécuritaire allant dans les deux sens, du haut vers le bas mais également du bas vers le haut. Pour ce faire, nous aidons le client à s'appuyer sur des relais au sein de l'entreprise. Ces relais auront pour rôle de diffuser et de rappeler les bonnes pratiques et les règles.

Comment s'assurer dans le temps que les règles apprises en formation sont respectées par tous ?

Il faut constamment rappeler les bonnes pratiques et ne pas hésiter à recourir à ce que les militaires appellent le « drill ». Cela permet de garder les gens en alerte, de maintenir un niveau de sensibilisation important et un niveau de pratique digne de ce nom. Ce « drill » permet d'éviter de tomber dans la routine, de sombrer dans l'excès de confiance, la complaisance, la baisse de vigilance, le « ça n'arrive qu'aux autres »… Sur ces sujets, il faut aussi se donner les moyens de socialiser correctement et humainement les règles de sécurité. C'est-à-dire les faire comprendre en impliquant les collaborateurs, de manière à augmenter l'acceptation des règles. Cependant, si les règles ne sont pas respectées et que cela expose les personnels et/ou le projet, il est important que l'entreprise sache sanctionner lorsque cela est nécessaire.

Doit-on former tout le monde ?

Il est nécessaire que les entreprises comprennent qu'il n'y a pas de collaborateur lambda au sein d'une société. La malveillance cherchera toujours le maillon faible. On doit donc sensibiliser et former le maximum de collaborateurs. À part en premiers secours et en gestion de l'information, tout le monde n'a peut-être pas besoin d'être formé sur tout, il est important de monter un plan de formation en évaluant les types de formations nécessaires à chacun en fonction de sa position, de son rôle, de ses activités et donc des menaces auxquelles chacun est exposé.

ILS PEUVENT VOUS AIDER

L'offre en formation aux risques attentats, voyages à l'étranger ou autres est très vaste. Voici quelques exemples de ce que vous pouvez trouver sur le marché. Une liste évidemment non-exhaustive.

Risk & Co propose des formations sur la sûreté des voyageurs d'affaires ainsi que des formations à l'expatriation pour les salariés et leurs familles.
→ **www.riskeco.com**

Le groupe Geos propose des formations autour du thème de la mobilité internationale : sensibilisation voyageurs d'affaires et expatriés – briefing téléphonique, formation des voyageurs d'affaires et expatriés aux règles de sûreté, prévention et gestion du risque kidnapping, « Hostile Environment Awareness ».
→ **http://fr.groupegeos.com**

Control Risks met à votre disposition des sessions d'entraînement poussées sur le risque kidnapping, corruption ou au travail en milieu hostile.
→ **www.controlrisks.com**

Amarante International propose des formations sur la mobilité à l'international et pour les déplacements en zones sensibles pour les voyageurs d'affaires, les expatriés et leurs familles, les professionnels de la sécurité et les professionnels en milieu hostile.
→ **www.amarante.com**

Other Solutions dispose d'une offre complète de formation et de sessions d'entraînement à la sécurité personnelle sur le terrain, d'une durée comprise entre trois et cinq jours.
→ **https://othersolutions.eu**

PwC propose de vous accompagner pour renforcer votre sécurité et améliorer la sécurité de vos collaborateurs. Et peut vous aider à les former.
→ **www.pwc.fr**

● ● ● qui seront les plus à même d'en atténuer probabilité et impact. Nous avons pour but de permettre à notre client de mettre en œuvre un projet à l'international dans les conditions de sécurité requises. Pour ce faire, nous assurons la formation de ses personnels nationaux et internationaux et assurons le support du projet. Notre rôle est d'être un facilitateur, de manière à ce que le client puisse faire son métier. Mais cela se fait en respectant certains principes et prérequis. Les actions de formations pratiques sont nécessaires à la bonne préparation d'un projet, ne se font pas à la va-vite et il est important de traiter la gamme de menaces auxquelles les collaborateurs risquent d'être exposés. Les formations se conçoivent sur-mesure, en fonction de l'identité du client, de ses activités, du contexte d'opération. Ce n'est pas du générique. Nous nous adaptons aux spécificités uniques du client. De plus, nous sommes dans une approche pédagogique de faire faire, qui va donc au-delà

© Cogedim Altarea

Exemple de « comics » élaboré par la direction sûreté du groupe Altarea Cogedim pour rappeler à ses collaborateurs les consignes Vigipirate.

du faire voir et du faire entendre.» La formation du personnel doit avoir pour base l'analyse fine des conditions de l'opération, des menaces, de son environnement et des risques que peut générer l'opération elle-même. *«L'enjeu de notre action,* ajoute Alexandre Carle, *est de réunir les conditions, en partie par de la formation et l'accompagnement des collaborateurs, qui permettent de réduire la probabilité qu'une menace se réalise. Nous ne sommes pas dans la dissuasion. Notre approche est plus basée sur l'acceptation et la protection. Nous raisonnons plutôt en termes de ''profil bas'' et d'intégration du collaborateur dans l'environnement dans lequel il sera amené à travailler. Nous savons bien que cela ne s'applique pas à tous les projets et n'importe où, mais cela fonctionne très bien dans de nombreux contextes, même très exposés.»*

Plan de gestion de crise

Si tout commence avec la formation – classique ou via des outils d'e-learning, *«il faut également mettre en* ●●●

PAROLE D'EXPERT

ÉRIC DAVOINE

Président du chapitre français d'Asis International et Regional Security Manager chez Walt Disney Company

© DR

«S'ASSURER DE L'HONORABILITÉ DU COLLABORATEUR.»

«Les entreprises ne doivent pas se laisser aveugler par la seule menace terroriste en matière de protection de leurs salariés et des biens de la société. La menace qui pèse sur les sociétés, nationales ou internationales, est bien souvent endogène. Un minimum de précautions s'impose. Une enquête d'honorabilité peut être nécessaire pour certaines fonctions, pour la quelle la demande d'un bulletin n°3 de casier judiciaire n'est parfois pas suffisante. Cette enquête peut être reconduite tous les trois ans, ou lors d'un changement de poste, afin de s'assurer que la situation privée du collaborateur n'a pas changé. Cette politique de sécurité doit être affichée clairement par l'entreprise et respecter le droit en vigueur. Mais elle est un bon moyen pour faire émerger une culture sécurité chez les collaborateurs et leur faire comprendre qu'ils ne doivent pas s'exposer à certains risques pour ne pas se mettre en danger et éventuellement être à l'origine d'une menace ou d'un risque pour leur entreprise. Mais ces procédures sont assez difficiles à mettre en place une fois que le salarié a intégré l'entreprise. On est là dans une sorte de no man's land juridique assez similaire aux problèmes que les entreprises peuvent connaître avec les «fichés S.»

2 QUESTIONS À

MAXIME BLACHA

Group security director chez Sodexo


© DR

Sodexo est le plus grand employeur privé français et est très présent à l'international. Comment formez-vous et sensibilisez-vous les collaborateurs du groupe qui sont amenés à voyager dans des pays à risques ?

Sodexo emploie 450000 personnes. Sur ce nombre, environ 3500 sont amenés à voyager à l'international et parmi cette population, 200 effectuent des déplacements dans des pays classés 4 et 5, c'est-à-dire à risques élevés. Les autres niveaux étant le 1 et le 2 pour les pays à risques «faibles» comme la France et le niveau 3 pour les pays à risques «avérés» (Inde, Brésil, par exemple). Pour les collaborateurs qui se rendent dans des pays de niveaux 4 et 5, tous doivent suivre nos modules de sensibilisation (sur trois niveaux). Pour le dernier module, 90 % de bonnes réponses à un questionnaire précis sont requis afin obtenir une certification, valable six mois.
Nous avons également sur étagère la possibilité de leur faire suivre une formation spécifique, validée par la direction sécurité, (formation et sensibilisation en milieu hostile, «HEAT») pour 10 à 15 personnes, disponible deux fois par an, avec simulation d'enlèvement, apprentissage de la gestion du stress… dispensée par l'un de nos partenaires Control Risk. Pour les pays de niveau 1, 2 et 3, nous avons également mis en place des modules de sensibilisation qui permettent à nos collaborateurs d'obtenir des certifications valables deux ans ou un an (pour les pays à risques de niveau 3 équivalent chez Sodexo à notre module 2) via des mémos sécurité envoyés lors de leur réservation de voyage qui nous permettent de les informer et de les préparer au mieux pour leur déplacement professionnel.

Que faites-vous pour former vos salariés sédentaires dans des pays de niveaux 1 et 2 en matière de risques ?

Dans les pays que l'on peut qualifier de normaux, nous sommes face à une double problématique : former nos collaborateurs qui travaillent sur des sites propres à Sodexo (sièges, direction régionales, etc.) et ceux qui interviennent chez nos clients. D'une manière générale, nous avons identifiés des sites qui, par leur nature, sont plus sensibles que d'autres en raison de leur visibilité, du caractère de leur activité, de leur aspect emblématique… Nous en avons ainsi identifiés une centaine particulièrement sensibles en France et environ 300 d'une sensibilité moindre. Pour y former nos personnels, nous nous rendons régulièrement sur ces sites en question pour expliquer, sensibiliser et diffuser la politique sécurité du groupe, leur fournir de la documentation comme par exemple notre «fiche attentat»… afin de leur apprendre les bons réflexes, les bons comportements en cas d'incident et pour avoir la meilleure réaction si un problème survient.

● ● ● *place un plan de gestion de crise. Les entreprises ne doivent pas hésiter à se faire accompagner sur ces sujets. Ne serait-ce, par exemple, que pour faire vérifier l'honorabilité des tiers parties avec lesquelles elles travaillent, intermédiaires, sous-traitants, fournisseurs, grâce à un travail de recherche, d'introspection. Par ailleurs, même si les choses ont évolué après les attentats qui ont endeuillé notre pays – la menace terroriste est devenue la deuxième préoccupation des dirigeants d'entreprise, ils ont favorisé l'émergence d'une volonté et d'un besoin en formation sur les sujets relevant des attributions des directions sécurité-sûreté des entreprises. Ces dernières ont réalisé que leur dispositif était souvent inopérant et ne les préparait pas à affronter une menace. Elles ont donc engagé les actions nécessaires pour se protéger et former leurs collaborateurs pour faire face à l'incident le cas échéant, et ne pas mettre en danger leur entreprise par des comportements inappropriés ou générateurs de failles dans la sécurité de leur société»,* conclut Olivier Hassid. ■

PAROLE D'EXPERT

NICOLAS LE SAUX

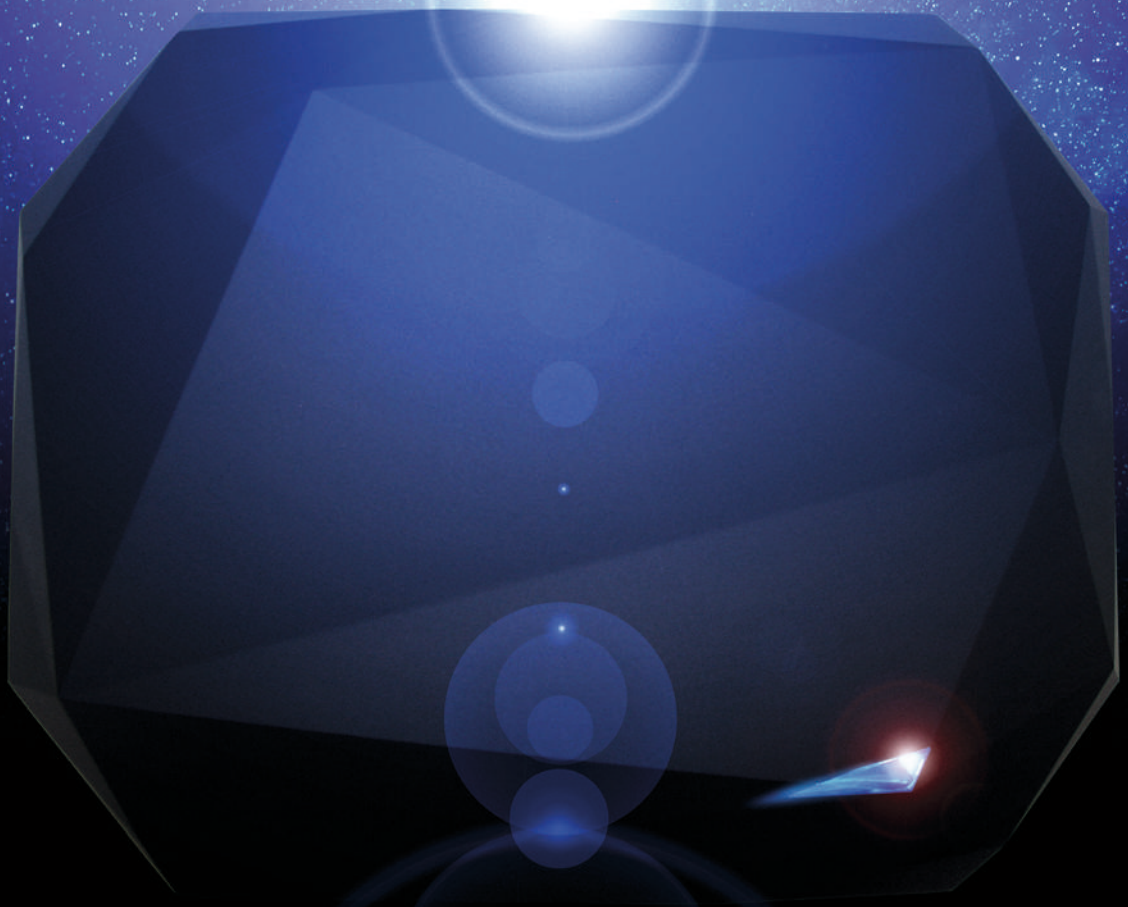
Président d'Atao Consulting


© DR

«LA FORMATION DOIT ENGLOBER DE NOUVEAUX RISQUES.»

«On peut cartographier risques et menaces en croisant ceux-ci avec les actifs tangibles et intangibles. Pour les menaces, cela peut être croisé avec la grille d'analyse Tessco (voir cartographie p.34). La corruption, par exemple, pourra constituer une menace directe pour les actifs tangibles et intangibles d'une entreprise. Ensuite, on doit se poser la question de l'origine de la menace : par qui peut-elle être générée ? Des personnes externes à l'entreprise ou son propre personnel ? Puis se demander quelles pourront être les actifs menacés par le vol, un attentat, un sabotage ? Par ailleurs, les entreprises doivent aussi prendre conscience que la nette tendance à dématérialiser le travail et les activités dématérialise aussi leur relation avec leurs prestataires externes et avec leurs collaborateurs qui ne travaillent plus dans les locaux de la société. Ils peuvent donc échapper au spectre de la direction sécurité-sûreté et augmenter l'exposition de l'entreprise aux risques. On ne sait plus vraiment, si, lorsque le collaborateur travaille à l'extérieur, c'est bien lui qui est derrière son écran ou qui utilise son téléphone mobile… La formation doit donc englober tous ces paramètres. Et ne pas se contenter de sensibiliser le top management. Une assistante d'un DRH, d'un DAF ou d'un membre du comex doit être formée et sensibilisée de la même manière que son supérieur sur le sujet. Sinon, l'entreprise est vraiment exposée à un risque.»

Identification intelligente de véhicules



Nouveau lecteur Spectre : le pouvoir de sécuriser et fluidifier vos accès parkings

Nous relevons le défi de vos accès véhicules en les rendant à la fois sécurisés et extrêmement fluides. Vous n'aurez plus à choisir entre les deux.
Notre lecteur d'identification Spectre à ultra-haute fréquence met fin aux files d'attente. Discret, élégant, flexible, parfaitement sécurisé… il assure une identification automatique et à distance des véhicules en contrôlant jusqu'à 4 voies simultanément, même dans les environnements les plus contraignants. Ce lecteur, le plus robuste de sa catégorie, bouscule les codes de la sécurité et la rend plus instinctive. Préparez-vous à découvrir l'alliance de la flexibilité et de la haute sécurité en une même solution.

ÉVOLUTIF | FLUIDE | SÉCURISÉ | AGILE | FURTIF | INSTINCTIF

www.stid-security.com

LES TROPHÉES EXPOPROTECTION 2018 — MENTION SPÉCIALE —

STid Electronic Identification

8 Awards
Security Meetings
Trophées de la sécurité
Expoprotection
ISC West
APS

La gamme Flexidome IP starlight 8000i de Bosch Security and Safety Systems dispose d'une fonctionnalité qui permet de distinguer intelligemment les vrais événements de sécurité et les fausses alertes.

© DR

La très haute résolution : pour des applications spécifiques

Contrairement à ce que l'on pourrait croire, la très haute résolution n'est pas toujours la meilleure solution en matière de vidéosurveillance. Elle répond à des besoins précis et requiert la prise en compte de certaines contraintes.

Tous les fabricants interrogés par *PSM* dans cet article le reconnaissent : ce qui était, il y a encore trois ou quatre ans, le nec plus ultra de la vidéosurveillance en matière de résolution est aujourd'hui presque le standard. *« Le Full HD est devenu le standard. Et a complétement supplanté le HD »*, confirme donc Philippe Henaine, Project Sales Manager chez Panasonic France. Même point de vue du côté de Matthieu Lucas, chef de marché sécurité chez Bosch Security and Safety Systems : *« Ce qui, hier, était considéré comme de la très haute résolution est désormais entré dans la banalité et ne correspond plus à ce que recouvrent actuellement les solutions de très haute résolution en vidéosurveillance. Aujourd'hui, on peut légitimement considérer que la très haute résolution commence avec le 4K et l'ultra HD. »* Cet unanimisme des fabricants ne doit pas masquer d'autres points de vue comme ceux du GPMSE, par la voix de Luc Jouve, président du GPMSE Installation : *« Face aux fabricants, qui ont la*

tendance légitime à vouloir innover toujours plus, on peut à juste titre se demander si du côté des installateurs et des utilisateurs finaux, la course à l'armement vers des solutions de vidéosurveillance toujours plus puissantes répond aux attentes et aux besoins réels du marché et du terrain. »
Alors qu'en est-il réellement de la très haute résolution ? À quoi sert-elle ? Quels sont ses atouts et ses inconvénients ? Éléments de réponses.

Petit rappel technique

Il convient de rappeler quelques principes simples. La résolution d'une caméra définit le nombre de pixels disponibles pour enregistrer une séquence vidéo. Cette résolution est généralement définie en mégapixels, soit le nombre de millions de pixels du capteur utilisé. *« Plus le capteur offre de mégapixels, plus grand sera le nombre d'informations enregistré par la caméra,* explique Xavier Delacour, Sales Director Europe II chez Vivotek. *Chez Vivotek, par exemple, notre gamme de très haute résolution ou ultra HD sont des caméras 4K jouissant de résolutions allant de 3840 x 2160 à 30 images par seconde à des résolutions de 1920 x 1080 avec 120 images par seconde. »*

La caméra multicapteur WV-X8570N est capable de fournir des images nettes et de couvrir une zone à 360° dans les conditions les plus difficiles.

« Ce qui, hier, était considéré comme de la très haute résolution est désormais entré dans la banalité. »

MATTHIEU LUCAS, CHEF DE MARCHÉ SÉCURITÉ CHEZ BOSCH SECURITY AND SAFETY SYSTEMS

Le 4K est désormais considéré comme le standard de la très haute résolution. *« Si la très haute résolution peut atteindre des résolutions allant jusqu'à 20 millions de pixels, voire plus, la 4K est en train de devenir la résolution classique en matière de très haute résolution,* confirme Xavier Sanchez, ingénieur des ventes chez Axis Communications. *Mais il faut garder à l'esprit que la très haute résolution requiert de disposer d'un optique conçu pour supporter de telles résolutions. Sans cela, on risque fort d'être déçu. »*
Chez Hikvision, le 4K est aussi le standard. *« En très haute résolution, notre gamme commence évidemment au 4K mais va bien plus loin. Nous proposons désormais des solutions allant de 8 millions de pixels à 32 millions,* explique Jean-Marie de Troy, directeur commercial chez Hikvision France. *12 millions de pixels via nos solutions* ● ● ●

POINT DE VUE D'UN FABRICANT

PHILIPPE HENAINE
Project Sales Manager chez Panasonic France


© DR

« DES SOLUTIONS MULTICAPTEURS POUR APPLICATIONS EN EXTÉRIEUR. »

« Nous proposons des solutions multi-capteurs dédiées aux applications urbaines pour remplacer les dômes motorisés. Par exemple, nos modèles WV-X8570N qui offrent une qualité d'image extrême – avec 4 capteurs 4x4K (33 MP), 3840x2160, 15 FPS – pour une capture des données dans les conditions les plus extrêmes. Cette caméra est la solution idéale pour la surveillance des zones urbaines telles que les intersections et les carrefours. Les caméras multicapteurs i-Pro Extreme disposent de quatre objectifs repositionnables qui permettent la couverture en continu d'une zone à 360°. Grâce aux capteurs d'image 4K, les images de véhicules sont nettes et claires même en mouvement rapide avec la technologique Panasonic iA (intelligence automatique). »

3 QUESTIONS À

LUC JOUVE

Président du GPMSE Installation


© DR

La très haute résolution est-elle la panacée en matière de vidéosurveillance ?
Si on se place du point de vue des installateurs et des utilisateurs finaux, il faut savoir raison garder en matière de capacités des caméras et ne pas se laisser aveugler par les discours des fabricants. Il faut toujours garder à l'esprit ces questions primordiales : que veux-je faire avec mes caméras ? Quel est l'intérêt de la très haute résolution ? Passer à la très haute résolution ne va pas sans contraintes. En effet, il faut reconnaître que les caméras évoluent plus vite que les infrastructures sur le terrain, chez les utilisateurs finaux. La très haute résolution implique de disposer de réseaux, de bande passante, de moyens de compression, de capacités d'exploitation et de stockage très importants. Pour certaines applications, la très haute résolution est très utile. Mais ce n'est pas une solution miracle.

Justement, quelles sont les applications pour lesquelles le recours à la très haute résolution est justifié ?
Si on veut faire de l'identification dans un stade, une gare, un aéroport ou un espace public, la très haute résolution est tout à fait pertinente. Il ne faut pas croire que l'analogique ou le HDTVI veut nécessairement dire mauvaise résolution. Et bien des secteurs l'utilisent encore comme le bancaire, le nucléaire…
Et remplacer une très grande installation analogique par du tout numérique a un coût énorme pour une plus-value qui paraît bien aléatoire pour certains.

Quels conseils donner à un utilisateur qui souhaite se doter de solution très haute résolution ?
Il doit faire appel à un installateur digne de ce nom, certifié Apsad, qui sera capable de le conseiller et de l'accompagner. De réaliser, par exemple, une étude de risques ainsi qu'une analyse des besoins précise et d'aider l'utilisateur à décrire ce qu'il veut et définir la finalité du système. Alors, il pourra choisir la solution technique correspondant à ses besoins réels.

● ● ● *monocapteurs et 32 millions de pixels avec des solutions dotées de quatre capteurs de 8 millions de pixels chacun. Mais notre gamme comprend aussi des caméras fixes, des caméras mobiles, des bullets, des dômes intérieurs et extérieurs, ainsi que des enregistreurs. Ces solutions permettent de capturer du contenu dans une résolution quatre fois supérieure au Full HD standard, soit de passer de 1920 x 1080 pixels (Full HD) à 3840 x 2160 pixels. Ces solutions fournissent des images en UHD incroyablement nettes, claires, et permettent une meilleure utilisation des données vidéo. La 4K, qui augmente le nombre de pixels et donne une meilleure qualité d'image, va apporter une aide à l'analyse des vidéos et extraire plus d'informations. »*

CHEZ AXIS : DÔME MULTICAPTEURS

L'Axis Q3708-PVE est une caméra réseau à dôme fixe comportant trois capteurs. Elle donne une vue d'ensemble panoramique à 180° de vastes zones avec une seule caméra pour une utilisation dans des conditions difficiles d'éclairage, de jour comme de nuit, explique Xavier Sanchez, ingénieur des ventes chez Axis Communication. Elle réalise des vidéos fluides très détaillées, en filmant avec une résolution quadrivision à 30 images par seconde. Elle offre une technologie de plage dynamique étendue (WDR) - forensic capture pour une clarté garantie même lorsqu'il existe des zones d'ombre et de lumière dans la scène. Elle est également dotée de la technologie Axis Zipstream, qui réduit le stockage et la bande passante requis jusqu'à 50 % tout en saisissant des détails importants en qualité d'image maximale.

De vraies contraintes

Il ne faut pas croire que la très haute résolution est désormais la panacée en matière de vidéosurveillance ou vidéoprotection. *« Le Full HD a toujours l'avantage – par rapport à la très haute résolution – de permettre d'avoir une meilleure vision des mouvements et de mieux gérer les contre-jours,* tient à préciser Philippe Henaine de Panasonic France. *Bien maîtrisé, il est aujourd'hui le vrai standard de la vidéosurveillance. Mais il faut reconnaître que les évolutions technologiques venues des solutions grand public influent grandement le monde de la vidéosurveillance, et peu à peu les caméras 4K auront très vite les mêmes caractéristiques que les Full HD. »*
Alors comment faire la différence et comment choisir sa solution ? Il faut comprendre que, malgré ses indéniables avancées techniques, la très haute résolution ne va pas sans contraintes. *« Tout d'abord, la taille des images implique de disposer d'une bande passante capable de transmettre de tels flux d'informations. Il faut aussi prévoir des moyens de compression idoines,* ajoute Xavier Sanchez. *Par ailleurs, la très haute résolution*

La caméra Axis Q1659 dispose d'une résolution ultra haute (20 MP) pour fournir des images bien contrastées, des détails précis. Équipée d'un capteur d'image APS-C Canon, elle est accompagnée d'un grand choix d'objectifs EF/EF-S Canon.

Caméra dôme 32 mégapixels de Hikivision : pour avoir des images en très haute résolution.

requièrent des conditions de luminosité stables, à moins de disposer d'outils pouvant contrebalancer les variations de la luminosité, comme le WDR ou le Dynamic. »
Xavier Delacour fait le même constat que ses confrères : *« Les caméras très haute résolution sont certes capables de fournir des images de plus en plus nettes pour voir de plus en plus de détails – a posteriori – grâce à un zoom numérique, mais elles nécessitent une bande passante considérable pour la lecture en continu des vidéos et un espace de stockage très important pour l'enregistrement des séquences. C'est pour ces raisons que les fabricants développent également des technologies de compression vidéo afin de réduire considérablement le flux de données et, en conséquence, de réduire le coût de leur stockage. »*

Quelles applications ?

La très haute résolution ne peut être déployée partout. Elle sera très utile pour des applications précises. *« Ce type de caméras permet d'augmenter de manière considérable les détails de l'image,* explique Jean-Marie de Troy. *Elle sera donc à privilégier pour des applications en live afin de fournir à l'opérateur, grâce l'intelligence intégrée dans les caméras, des images très détaillées pour lui permettre, par exemple, de reconnaître un billet de banque. La très haute résolution, compte tenu des détails qu'elle fournit, sera aussi très utile pour dans le cas de la relecture de séquences vidéo pour faire de la reconnaissance, de la recherche ou de l'identification a posteriori. Mais il faut rappeler que, dans tous les cas, le capteur et l'optique doivent être de très bonne qualité. »*

« La très haute résolution est très efficace pour voir des champs larges, même dans des conditions de luminosité difficile. »

JEAN-MARIE DE TROY, DIRECTEUR DES VENTES CHEZ HIKVISION FRANCE

Pour Philippe Hénaine, *«la très haute résolution est très efficace pour filmer des champs larges, en extérieur ou en intérieur, avec très peu de contre-jour. On peut ainsi remplacer deux ou trois caméras Full HD par une seule caméra 4K, afin d'élargir l'angle, pour voir plus large. Elle permet aussi de zoomer dans l'image pour faire de la recherche de détails précis. »*
Chez Bosch Security and Safety Systems, le vaisseau amiral en matière de très haute résolution est la gamme Flexidome IP starlight 8000i. *« Elle dispose de fonctionnalités innovantes, Intelligent Video Analytics, qui améliorent la précision de la solution de sécurité en distinguant intelligemment les vrais événements de sécurité et les fausses alertes, dus à des environnements difficiles comme la neige, le vent, la pluie, la grêle et les reflets de l'eau,* explique Matthieu Lucas. *Il s'agit là d'un autre avantage non négligeable pour les utilisateurs qui sont uniquement avertis qu'en cas d'absolue nécessité. Elle convient parfaitement pour des applications de haute sécurité, permet la détection automatique d'objets sur de grandes distances et, dans un autre registre, permet de générer des métadonnées à des fins statistiques dans des environnements comme les villes ou les centres commerciaux... »*
« On utilisera la très haute résolution sur des grands parkings, dans de grands halls comme les gares ou les aéroports, sur de grands sites industriels, ajoute Xavier Sanchez. *Elle sera donc plutôt à privilégier sur des sites de très grande surface afin de pouvoir exploiter, a posteriori, l'image et de visualiser en live les sites, en conservant du détail dans toute l'image. »* Avant de conclure : *« Elle permet aussi de surveiller des sites déportés grâces à des caméras équipées de focales très larges pour assurer une surveillance discrète à longue distance de sites ou de quartiers sensibles. »* ■

PAROLE D'EXPERT

XAVIER DELACOUR

Sales Director Europe II chez Vivotek

© DR

« LA TRÈS HAUTE RÉSOLUTION N'EST PAS UN IMPÉRATIF. »

« En matière de vidéosurveillance, il faut toujours garder à l'esprit la question suivante : de quelle résolution ai-je vraiment besoin et pour quoi faire ? Disposer de plus de résolution est toujours une bonne chose mais cela ne veut pas dire nécessairement que c'est un impératif pour l'utilisation que vous voulez faire de vos caméras. Les utilisateurs n'ont donc pas besoin de remplacer toutes les caméras par des caméras haute résolution, s'ils savent également dans quelless zones et quels espaces ils ont le plus besoin de voir des détails. Ensuite, ils doivent s'assurer que toute leur installation – y compris les NVR, VMS, moniteurs, etc. – sont capables de prendre en charge la très haute résolution pour des résultats cohérents et satisfaisants. »

La caméra Vivotek FD9391-EHTV est une nouvelle caméra réseau à dôme extérieur, équipée d'un capteur 4K ultra HD avec une résolution 3840 x 2160 à 30 ips. Grâce à la technologie Vivotek WDR Pro, ce dome est capable de capturer des images de haute qualité dans des environnements très contrastés.

Si le badge reste très présent dans le contrôle d'accès temporaire, les systèmes à clés électroniques, badges virtuels ou QR code offrent des alternatives de plus en plus prisées.

Contrôle d'accès temporaire : des accès à la carte

Accorder et suivre les accès, de façon fiable, pour une ou cent personnes, pour des périodes temporaires allant de quelques heures à quelques jours est un vrai casse-tête pour les gestionnaires sécurité. Les fabricants de contrôle d'accès proposent un large éventail de solutions avec une tendance marquée à la dématérialisation.

Campings, chantiers, parcs d'exposition, foyers sociaux, résidences de tourisme... des établissements très différents qui ont tous en commun de devoir gérer les accès d'un grand nombre de personnes – ou de véhicules – pour des périodes très courtes. De même, dans de nombreuses sociétés, l'intervention de sous-traitants ponctuels ou d'entreprises extérieures génère un trafic croissant, qu'il faut contrôler, tant pour des questions de sécurité que de facturation de prestations, sans pour autant mobiliser inutilement du personnel.

Les clés intelligentes, souplesse et sécurité

Si beaucoup de sociétés utilisent des systèmes de badges pour leurs accès principaux, il reste, dans toutes les entreprises, de très nombreux locaux uniquement accessibles par clés. D'un côté, il peut paraître disproportionné et coûteux de câbler une porte qui ne sera utilisée que très occasionnellement, de l'autre, les clés mécaniques, surtout sur les sites étendus, ne sont pas sans poser problème aux services généraux (organigrammes complexes, pertes et vols de clés – avec éventuellement obligation de changer le cylindre, duplication non contrôlée, etc.). La clé électronique, comme celles proposées par Locken, Assa Abloy ou Iloq, représente une alternative intéressante. Plus chère au départ qu'une clé mécanique ou qu'un badge, elle s'avère plus économique sur la durée. En cas de perte ou de vol, il suffit d'annuler les droits sans changer le cylindre. De plus ces clés fonctionnent sur des cylindres autonomes et sans câblages, qui peuvent se substituer aux cylindres standards en quelques minutes. *« Le gros avantage des clés mécatroniques,* souligne Catherine Laug, directrice marketing de Locken, *est qu'elles permettent une gestion très fine des droits d'accès, comme pour des systèmes à badges. On peut accorder à un intervenant ponctuel des droits temporaires qui deviennent caducs à la fin de la*

mission. En ce qui concerne nos clés Bluetooth, la clé mécatronique communique avec le smartphone de l'usager via l'APP MyLocken. Elle permet alors un contrôle centralisé et une gestion des accès au cas par cas, et en temps réel. Les intervenants sur de grandes infrastructures ou des sites complexes aux multiples accès disposent ainsi d'une clé unique. Mais elle offre une souplesse d'utilisation supplémentaire : sa composante purement mécanique permet d'ouvrir les cylindres mécaniques classiques partout où coexistent les deux types de serrure dans le même système. »

Les badges virtuels se substituent aux cartes physiques

Les serrures autonomes peuvent s'ouvrir avec des clés, mais aussi avec des badges ou des téléphones portables, un badge virtuel étant transmis sur le smartphone. Pour Martial Benoit, directeur commercial de Deny Security, les serrures autonomes sont des systèmes légers qui permettent une gestion pointue des plages horaires et des accès temporaires. *« Selon la configuration, nous proposons soit les cylindres autonomes (Optima Lock Mifare), soit les* ●●●

SUR LE TERRAIN

Zefil choisit Protec Cliq pour ses intervenants permanents et occasionnels

Zefil, société publique locale, gère du transport de communications par fibre optique pour les professionnels de la métropole toulousaine. Elle assure les derniers mètres entre l'opérateur et le bâtiment de la société cliente en connectant ainsi 1 000 entreprises auprès de 40 opérateurs présents dans la région. Zefil dispose de nombreux locaux techniques disséminés dans les 37 communes de la métropole toulousaine, tous sont équipés de diverses serrures avec clés mécaniques. Michaël Combes, directeur des systèmes de Zefil, affiche sa satisfaction : *« Après appel d'offres, nous avons retenu le système de clés Abloy Protec Cliq qui nous permet d'assurer la sécurité des locaux, tout en octroyant les droits d'accès de manière très fine. Les employés et les prestataires permanents disposent chacun d'une clé qu'ils mettent régulièrement à jour sur un boîtier ou grâce à une application Bluetooth sur leur smartphone. Si nous devons accorder des droits temporaires à un prestataire ponctuel, il suffit de lui remettre une clé programmée pour un ou plusieurs locaux, avec des plages horaires définies. Un système qui allie flexibilité, sécurité et simplicité. Je n'ai plus aucune remontée de la part de mes prestataires et c'est un vrai confort pour tous. De plus, le fait que les cylindres soient autonomes, sans aucun besoin d'apporter l'électricité sur site, a facilité l'installation en remplacement des cylindres préexistants. »*

CAMPINGS, NAXI CAM GÉRE LES ACCÈS VÉHICULES GRÂCE À LA LECTURE DE PLAQUES

Inaxel, éditeur de logiciels spécialisé pour l'environnement des campings, propose avec Naxi Cam une gestion des accès véhicules grâce à la lecture de plaques. L'objectif ? Fluidifier le trafic, contrôler les accès et faciliter l'enregistrement des clients qui peut être fait au moment de la réservation ou à l'arrivée. Ce système fiable permet de paramétrer les droits d'accès pour des durées variables et des horaires, en fonction du type d'utilisateurs : client, personnel, fournisseurs, secours, etc. Le système permet une visualisation en direct des passages ou avec la recherche d'historique. Une solution sans badge ni code, confortable aussi bien pour les utilisateurs que les gestionnaires, qui permet de maîtriser les accès véhicules.

© Gettyimages

3 QUESTIONS À

THIERRY CHEP

Président de Neoaxess

© DR

Quelle est l'activité de Neoaxess ?
Neoaxess est le leader national en matière de contrôle des accès au sein des chantiers avec plus de 600 chantiers équipés à ce jour. Fournisseur référencé auprès des majors du BTP, la société Neoaxess propose des solutions composées de services, de matériels et de logiciels qui permettent de superviser tous les aspects du contrôle d'accès physique et qui contribuent à lutter contre le travail illégal au sein des chantiers.

Quelle est la priorité de vos clients en ce qui concerne le contrôle d'accès de leur chantier ?
Les questions de sécurisation et de lutte contre le travail illégal ont eu de plus en plus d'impact sur les chantiers de BTP ces dernières années, et le contrôle d'accès est l'un des composants clés dans la mise en place de solutions face à ce genre de problématiques.
En plus de se prémunir contre les problèmes d'intrusion et de vols, et de prévenir les risques d'incidents en interdisant l'accès aux personnes non autorisées, le contrôle d'accès physique couplé à une solution logicielle dédiée, permet de s'assurer que les dossiers administratifs ou les éventuelles habilitations professionnelles sont toujours valides lors de l'accès des intervenants concernés. Ces sujets intéressent au plus haut point les maîtres d'ouvrage et les donneurs d'ordres qui sont solidairement responsables pour les cas d'infractions au Code du travail lorsque ces dernières sont commises par des entreprises sur les chantiers. Le risque peut en en effet être pénal et se doubler d'un préjudice économique.

Quelles sont les particularités de votre logiciel Visioaxess Chantiers ?
Visioaxess Chantiers est une suite logicielle développée par Neoaxess et qui permet de gérer des opérations de quelques centaines à plusieurs dizaines de milliers d'utilisateurs. Elle permet d'assister les responsables en charge de la sûreté dans leurs missions du quotidien, ou encore les logisticiens, avec des fonctions complètes et exclusives pour les chantiers, comme l'enregistrement des intervenants, des sous-traitants et des visiteurs dans une application unique, le pré-enregistrement et la télétransmission des documents administratifs pour les intervenants avant leur intervention (portail Web pour les sous-traitants), la validation en temps réel des fiches des personnes enregistrées (sources de données clients ou plates-formes légales), le contrôle automatique de validité de la carte professionnelle du BTP... pour n'en citer que quelques-unes.

● ● ● *plaques béquilles (Optima Hand). L'Optimal Lock Mifare fonctionne aussi bien en version off-line – les droits d'accès sont dans le cylindre ou le badge, qu'en version on-line autorisant alors une gestion jusqu'à 3 000 cylindres en temps réel. D'une grande flexibilité, il peut également évoluer d'un fonctionnement off-line vers un mode on-line, sans aucun changement de cylindre. Avec un PC et quelques badges on peut monter un contrôle d'accès temporaire. C'est un système qui convient parfaitement à l'événementiel (location et gestion de salle), et qui peut se gérer à distance avec un simple téléphone portable pour des installations jusqu'à 50 portes. »* Badges et codes virtuels, peuvent coexister, comme pour CDVI, très implanté chez les bailleurs. *« Dans les résidences et les logements, il y a une foultitude d'employés et de visiteurs, pour la maintenance, les services aux personnes ou la propreté,* explique Pascal Leroux, vice-président de CDVI. *Certains sont permanents, d'autres temporaires ou très ponctuels. Or, les codes d'accès sont souvent très largement partagés. Avec notre système digicode Galeo 4.0, qui peut s'implémenter en local ou en IP, nous pouvons transmettre des "codes cachés". Le sous-traitant présentera son smartphone devant le digicode Galeo 4.0 qui lira le code NFC ou Bluetooth sans que le porteur n'en ait connaissance. Il pourra pénétrer dans les bâtiments et dans les locaux qui lui sont accessibles, pour les plages horaires et une durée déterminée. Les résidents, eux, pourront s'ils le souhaitent continuer à utiliser un badge d'accès, nos lecteurs étant multi-technologies. Notre système Galeo 4.0 rencontre également beaucoup de succès pour la location entre particuliers. Une situation où les propriétaires demandent une gestion fiable de l'accès à leur logement pour des périodes de quelques jours. »*

Le contrôle d'accès sans clé, sans badge ni réseau

Plus de clé, ni de badges, pas de réseau et toujours du contrôle d'accès ? C'est possible ! Il s'agit de FacilitAccess, développé par Spartime. *« FacilitAccess est une solution universelle idéale pour tout site qui souhaite mettre en place un contrôle d'accès temporaire,* assure Patrick Say, CEO de Spartime. *Nous avons totalement supprimé la gestion des clés et des badges pour la remplacer par la transmission d'un code clavier temporaire ou d'un QR code. Plus besoin de wi-fi, de Bluetooth, de NFC ou de GSM. Aucune appli à charger sur son smartphone. Notre solution peut être utilisée partout, y compris en zone blanche ! »* De quoi s'agit-il ? *« Notre plate-forme de gestion va générer automatiquement un code clavier ou un QR code et va le transmettre au destinataire par mail ou SMS. Il suffira de taper le code sur le clavier ou de présenter le QR code devant le lecteur pour ouvrir la porte, un casier ou même une barrière de parking. Ce code temporaire peut être délivré pour un passage unique ou pour une période limitée. Nos matériels de contrôle d'accès n'ont pas nécessairement besoin d'être reliés à un réseau électrique, ils fonctionnent sur piles ou en courant faible. Un système qui a convaincu des gestionnaires de clubs sportifs, d'espaces de coworking, d'hôtels, de parkings, de garde-meubles ou de palais des congrès par exemples... La seule contrainte, en cas d'installation en zone non connectée, est de devoir se déplacer sur le lieu où se trouve le lecteur pour récupérer l'historique – jusqu'à 2 000 passages enregistrés. Une recherche somme toute assez peu fréquente. Le gain pour l'établissement est certain. Nous avons estimé que la gestion d'un badge prend une*

quinzaine de minutes – sans compter le coût matériel. Lorsqu'il s'agit de gérer un grand nombre d'utilisateurs sur des périodes très courtes, le calcul est vite fait !»

Des logiciels interopérables ou multifonctions

Y compris lorsqu'il s'agit d'accès de courtes durées ou ponctuelles, le contrôle d'accès nécessite souvent d'être couplé à d'autres systèmes qui ne relèvent pas forcément du domaine de la sécurité : gestion des présences, facturation, planning, habilitations et autorisations diverses, etc.

La force d'un logiciel résidera dans sa capacité à dialoguer avec les autres logiciels. *« FacilitAccès présente l'avantage d'être facilement interopérable avec la plupart des logiciels de gestion, comme un grand nombre de logiciels utilisés par les clubs de tennis pour gérer leurs réservations : lorsque l'adhérent réserve son court, le code ou le QR code d'accès temporaire est automatiquement émis en confirmation. Si nécessaire, l'adhérent pourra également accéder aux locaux et aux vestiaires. »* Cette interopérabilité est essentielle comme le souligne Pascal Leroux : *« Notre système Galeo 4.0 pourra, par exemple, être associé à une gestion de comptage décomptage. C'est actuellement le cas pour les accès véhicule des visiteurs dans un certain nombre de campings. Le contrôle d'accès va pouvoir s'interfacer avec des applications tierces. »*

Pour Néoaxess, spécialisé dans le contrôle d'accès de chantiers, certaines fonctions doivent être intégrées dans le logiciel lui-même, comme le détaille Thierry Chep, CEO de la société : *« Dans le cadre de la lutte contre le travail illégal, il est nécessaire, préalablement à la délivrance d'un badge d'accès, de contrôler les documents légaux des intervenants, par exemple carte BTP, carte d'identité, attestation Urssaf, lettre de mission pour un intérimaire, documents spécifiques si l'entreprise est étrangère, etc. Visioaxess Chantiers, notre suite logicielle, va permettre de valider en temps réel les fiches des personnes enregistrées, contrôler automatiquement la validité de la carte professionnelle du BTP et éditer les badges par profil pour identifier rapidement les intervenants et leurs droits au sein du chantier. Mais nous allons encore plus loin avec la gestion des vestiaires (casques, bottes et EPI), la gestion des livraisons, le comptage et la localisation automatique des personnes et des engins… Des applications désormais indispensables parmi toutes celles spécifiques au monde du BTP. »*

Locken

Locken propose une solution de contrôle d'accès basée sur une clé électronique à technologie inductive. Ce procédé exclusif permet d'associer, avec une fiabilité unique, les avantages d'une serrure traditionnelle mécanique et ceux d'une solution électronique d'avant-garde. La transmission des informations entre la clé et le cylindre s'effectue non par contact électrique, mais par induction magnétique, ce qui permet une ouverture presque instantanée.

© LOCKEN

La communication entre la clé et le cylindre s'effectuant sans contact, elle n'est pas perturbée par les problèmes d'oxydation, d'usure ou de poussières présents dans le cylindre. Grâce à son module Bluetooth, la clé mécatronique communique avec le smartphone de l'usager via l'APP MyLocken. Elle permet alors un contrôle centralisé et une gestion des accès au cas par cas et en temps réel. Cette solution ne nécessite aucun câblage sur le site ni batterie dans la serrure, puisque c'est la clé qui fournit au cylindre l'énergie et les informations nécessaires à son ouverture. Les utilisateurs intervenant sur de grandes infrastructures ou des sites complexes aux multiples accès disposent ainsi d'une clé unique. Mais elle offre une souplesse d'utilisation supplémentaire : sa composante purement mécanique permet d'ouvrir les cylindres mécaniques classiques partout où coexistent les deux types de serrure dans le même système.

LA PAROLE DE

BÉATRICE DECOSSE

Dirigeante de Pollux

© DR

« PLUS BESOIN DE SE DÉPLACER POUR ACTUALISER LES BADGES. UN VRAI CONFORT ! »

« Nombre de foyers sociaux accueillent des résidents sur des périodes temporaires, allant de quelques jours à quelques mois. Un système de contrôle d'accès électronique est la solution la plus adaptée pour concilier gestion des clés, sécurité et indépendance des résidents. En effet, ces établissements sont confrontés à un fort turn over des occupants. D'un côté, les résidents veulent accéder librement à leur logement, de l'autre, le gestionnaire doit gérer en permanence les nouveaux arrivants, les partants, les clés perdues ou reproduites illégalement. La solution Easylock, que nous avons installée sur ce type d'établissements, est un système de contrôle d'accès simple et sûr pour des établissements jusqu'à 150 portes.
À l'entrée de l'établissement, est placée une borne d'actualisation. Lorsque le résident se présente au niveau de la borne, le badge est lu et les droits d'accès mis à jour (nouveaux droits, prolongation du séjour ou blocage). Les droits d'accès sont alors transportés par les badges, permettant ainsi à l'usager d'accéder aux portes autorisées. Il pourra alors accéder aux parties communes et à son logement. L'intérêt de cette solution est que la mise à jour peut se faire à distance via le cloud, sans nécessité pour le gestionnaire d'avoir le badge physiquement, ni besoin de se déplacer dans la résidence. Les droits peuvent également être modulés en fonction du porteur, salarié ou résident. Aucune intervention n'est nécessaire sur les cylindres des portes, la totalité des droits étant sur les badges. Enfin, cela résout l'épineuse question des pertes de clés. Nos cylindres Easylock, fabriqués en France, s'installent facilement, sans travaux, en remplacement de cylindre mécanique standard. Bien plus économique qu'un système à clé, cette solution est parfaitement adaptée au secteur médico-social, maisons de retraite, centres de réadaptation et autres structures de taille moyenne. »

Contrôle d'accès : les lecteurs

Longue distance, intelligents, autonomes, interactifs… rapide aperçu des lecteurs et solutions de contrôle d'accès performants.

NET2 ENTRY TOUCH - PAXTON

CONTRÔLE D'ACCÈS INTELLIGENT

© Paxton

Son écran est équipé d'un ensemble de fonctionnalités haut de gamme, notamment un écran tactile couleur de 17,78 cm (7 pouces) de très grande qualité ainsi que des options de personnalisation ; le Net2 Entry peut donc être utilisé sur de plus nombreux sites. Pouvant être utilisé idéalement dans de nombreux endroits, notamment dans les bâtiments commerciaux, les installations de loisirs et les hôtels, la fonctionnalité avancée et l'utilisation intuitive de Net2 Entry Touch signifie que les installateurs peuvent désormais offrir à leurs clients une option haut de gamme en matière de sécurité, dans le cadre de la gamme Entry Net2.
Conçue en réponse directe aux réactions des installateurs, la nouvelle platine tactile est proposée en trois variantes ; montage encastré, en surface et capot anti-pluie. La platine est classée IK7 en matière de protection contre les chocs, sans oublier un écran anti-éblouissement et facile à lire pour optimiser la consultation quotidienne. La nouvelle interface utilisateur est simple et facile à parcourir, disposant de fonctionnalités de recherche dynamique aux côtés d'options personnalisables de marketing de la marque.
Net2 Entry n'est composé que de trois composants qui se détectent automatiquement à l'installation : une platine extérieure, un moniteur intérieur et un contrôleur de porte pour une solution vraiment plug and play. ●

© Vanderbilt International

ALIRO - VANDERBILT INTERNATIONAL

10000 UTILISATEURS ET 100000 CARTES

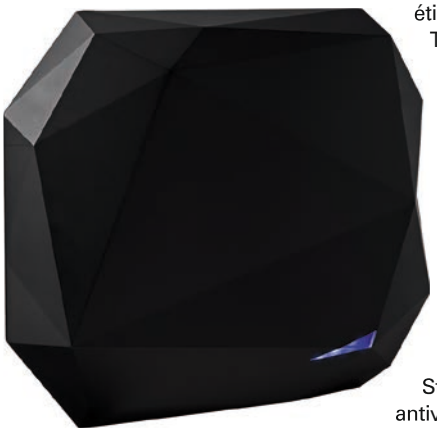
La version 1.15 du logiciel Aliro conjugue améliorations et innovations par rapport à la version précédente (lancée fin 2014). C'est le premier système de contrôle d'accès logoté Vanderbilt. Aliro dispose d'une architecture simplifiée combinée à un logiciel convivial et des applications mobiles intuitives. Grâce à la souplesse de son fonctionnement, le système est gérable à tout instant depuis n'importe quel appareil disposant d'une connexion internet. En complément des 11 langues européennes en standard, la version 1.15 du logiciel en ajoute quatre nouvelles : le russe, le polonais, le tchèque, le grec, et permet d'attribuer à chaque utilisateur de ce système sa propre langue de travail. Facile à configurer, le logiciel détecte automatiquement les unités de contrôle d'accès du système et leur attribue des adresses IP disponibles sur le réseau informatique, pouvant gérer jusqu'à 512 portes, 10000 utilisateurs et 100000 cartes d'accès. Aliro utilise des lecteurs de cartes MiFare DESfire ultraperformants dotés d'un écran Oled intégré affichant des messages et des instructions en fonction des identifiants de connexion et de la langue individuelle des utilisateurs, ce qui permet d'interagir directement avec le porteur de la carte. ●
➔ **CARACTÉRISTIQUES :** • Grâce à la fonction gérant le contour lumineux du lecteur, il est possible d'associer des couleurs et des séquences personnalisables à différents types d'événements. • L'ajout d'une fonction « liste de présence » permet, en cas d'urgence, de disposer d'un rapport récapitulant les personnes présentes dans l'immeuble et leur emplacement actuel.

SPECTRE - STID

LECTEUR LONGUE DISTANCE ÉVOLUTIF

Conçu pour le contrôle et l'identification longue distance des véhicules, le lecteur Spectre ultra hautes fréquences allie sécurité et évolutivité. Les performances d'identification (jusqu'à 13 m) offrent un confort et une fiabilité de lecture exceptionnels pour des accès véhicules fluides. Une à quatre antennes peuvent être connectées au lecteur pour répondre à de nombreuses configurations : flotte hétérogène de véhicules (légers, poids lourds, motos, etc.), identification sur larges voies ou contrôle d'accès de quatre voies de véhicules. En quelques secondes, le lecteur se configure par câble USB/micro USB ou par badge UHF. Son système Quickset compatible avec la norme VESA 75x75 permet une installation optimale quelle que soit la configuration du site. Le fonctionnement du lecteur peut être piloté par une boucle au sol ou un détecteur de passage. Écoresponsable dans sa conception, Spectre assure la lecture des indentifiants 100 % passifs (sans batterie ni pile).

➔ **CARACTÉRISTIQUES :** • Fréquences porteuses : 865 – 868 MHz : 866 MHz ETSI (Europe), Maroc... 902 – 928 MHz : 915 MHz FCC Part 15 (USA)… • Compatibilité puces : EPC Class 1 Gen 2 / ISO 18000 – 63 • Lecture seule ou lecture écriture • 1 à 4 antennes • Distance de lecture : jusqu'à 13 m avec étiquette ETA et tag passif Teletag selon les conditions d'utilisation • Interface de communication : sortie TTL standard, protocole ISO2 (Data Clock) ou Wiegand ; RS232 avec protocole de communication sécurisé SSCP ; RS485 avec protocole de communication sécurisé SSCP • Résistance aux intempéries IP66 – Structure renforcée antivandales IK10.



© Stid

© HID

EDGE EVO SOLO - HID

LECTEUR AUTONOME

Edge Evo Solo est un lecteur autonome et connectable par IP. La solution repose sur un navigateur Web standard et ne nécessite aucune autre installation logicielle sur les ordinateurs. Ce lecteur fait partie de VertX, la plate-forme de contrôle d'accès de HID Global qui propose une large gamme d'unités de traitement logiques et permet le développement de systèmes de contrôle d'accès aux fonctionnalités avancées comme la gestion à distance, la surveillance en temps réel, la création de rapports détaillés et d'autres applications annexes.

➔ **CARACTÉRISTIQUES :** • Edge Evo Solo utilise un navigateur Web standard et ne nécessite aucune installation de logiciels. Il permet également d'alimenter d'autres appareils via Power-over-Ethernet (PoE), réduisant ainsi les frais d'installation d'une alimentation séparée. En remplaçant son firmware, il peut être transformé en Edge Evo Host et ainsi être connecté à distance au système en fonction de l'augmentation de la demande en termes de contrôle d'accès.

ARCHITECT - STID

LECTEURS ÉVOLUTIFS

Architect est une gamme modulaire de lecteurs sécurisés 13.56 MHz alliant performances et simplicité. Un cœur électronique RFID permet de connecter un ensemble de modules complémentaires : clavier, biométrie, écran tactile, etc. La modularité est simple, économique et apporte au client une parfaite autonomie dans la gestion de la sécurité de ses accès. Ces lecteurs ultra-sécurisés intègrent les dernières technologies Mifare, DESFire et LEGIC Advant et des solutions innovantes comme un détecteur d'arrachement par accéléromètre.

➔ **CARACTÉRISTIQUES :** • Ces lecteurs sont développés sur des technologies ouvertes et interopérables, permettant à l'utilisateur de rester autonome dans la gestion de sa sécurité, et lui donnent la possibilité de développer ses propres applications sans aucun verrouillage technologique du constructeur RFID. La modularité de la gamme permet d'apporter plus de disponibilité et de service tout en optimisant la gestion des stocks par la diminution du nombre de références de 40 %.

© Stid

Unités mobiles de détection : de plus en plus populaires...

On les rencontre de plus en plus sur le terrain, sur des chantiers, lors d'événements ou de rassemblements publics, afin d'assurer une protection, plus ou moins longue, temporaire ou pas, des sites.

La solution Vigitracking d'IP Mirador détecte les intrusions et déclenche immédiatement les procédures définies.

© IPMirador

Les unités mobiles de détection associent la détection infrarouge, des caméras de surveillance, un système de sonorisation voire d'éclairage. Qu'il s'agisse des solutions proposées par les sociétés Solidbot, Ranc Développement, IP Mirador, VPS, Hymatom ou Onet, elles permettent toutes de déployer rapidement les technologies nécessaires à la protection temporaire d'un site. Et de venir appuyer les forces de sécurité sur le terrain.

Faciles à installer et à déplacer, autonomes sur de longues durées, résistantes aux intempéries et aux dégradations, les unités mobiles de surveillance ont donc tout pour séduire les responsables de sécurité de chantiers. Ces caissons, qui peuvent être livrés par n'importe quel transporteur ou être déplacés comme une simple remorque, sont de véritables centres de surveillance. Sur le mât télescopique, quatre caméras dômes jour/nuit qui permettent de couvrir un espace à 360°, des capteurs infrarouges, un éclairage puissant qui se déclenche avec la détection d'intrusion, une alarme sonore de 135 Db et un haut-parleur pour passer des messages d'alerte. L'ensemble est relié à un serveur qui transmet les informations par GSM, 3G/4G à un centre de télésurveillance déporté. Autonomes grâce à des piles à combustibles et des panneaux solaires, elles peuvent fonctionner sans recharge pendant plusieurs mois. *« Ce sont des unités qu'apprécient les sociétés de sécurité pour des missions sur des sites temporaires ou des chantiers mobiles* assure Christophe Segall, directeur général d'IP Mirador. *Nos unités ont été, par exemple, utilisés lors de travaux de réfection de clôture de centrale nucléaire, mais aussi sur des sites isolés. Elles sont particulièrement adaptées aux chantiers mobiles, ferroviaires ou autoroutiers. Le chargé de sécurité a simplement à s'assurer que l'unité est placée judicieusement par rapport à la zone à protéger. Le paramétrage des caméras et des capteurs est fait à distance par la centrale de surveillance qui gère la sécurité du chantier comme si elle y était. »*

« Les unités mobiles de détection ou de surveillance doivent être conçues comme des solutions globales. »

ROMAIN CILLE, PRÉSIDENT DU CONSEIL D'ADMINISTRATION DE RANC DÉVELOPPEMENT

Associer technologies et humains

Comme le soulignait prédemment Christophe Segall, les sociétés de sécurité n'hésitent plus à recourir à ce type de solutions en soutien des agents déployés sur le terrain. Ce que confirme ● ● ●

LE POINT DE VUE D'UN FABRICANT

CHRISTOPHE SEGALL
Directeur général d'IP Mirador

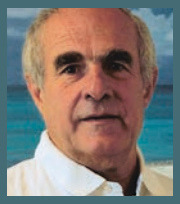
© DR

« SE DÉPLACER SELON L'ÉVOLUTION DU SITE. »

« En matière d'unité mobile de détection, la principale contrainte est constituée par l'environnement dans lequel elle sera déployée et qu'on ne maîtrise pas toujours. Mais une fois ce paramètre pris en considération et le problème de l'alimentation résolu, les unités mobiles comme notre Cube peuvent aisément assurer la sécurité d'un site, d'un chantier et même se déplacer selon l'évolution du site. Le Cube se compose de caméras extérieures pour la détection vidéo, de deux radars longue portée 24 GHz pour la protection périmétrique, qui permettent de piloter le dôme sur la cible et d'assurer une couverture du site à 200 °. Il est insensible à la pluie, aux ombres, etc. Nous proposons aussi un système plus léger, le Mob-TX pour la mise en surveillance vidéo instantanée des sites sensibles. La solution est dotée de trois dômes motorisés intelligents avec logiciel de détection d'intrusion. Cette solution assure la remontée d'alarme vidéo en cas de détection d'être humain ou de véhicule sur 200 m de rayon. »

PAROLE D'EXPERT

BERNARD TAILLADE
Hymatom


© DR

« L'ALIMENTATION EST LA PRINCIPALE CONTRAINTE À PRENDRE EN COMPTE. »

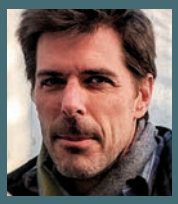
« Les unités mobiles permettent d'assurer de manière ponctuelle et temporaire la sécurité d'événements sportifs, des chantiers, des rassemblements de personnes, des zones de campings pendant la période estivale… L'alimentation du système reste la principale contrainte à prendre en considération quand on souhaite utiliser ce type de surveillance. Notre système Visiospace, quant à lui, s'interface avec 200 types de capteurs et constitue de ce fait une solution qui s'adapte assez facilement aux besoins des sites et des clients. On peut aussi mettre en place une solution intégrant différents microsystèmes mobiles qui viendront communiquer avec le système central. »

© DR

Les systèmes de détections autonomes de Solidbot assurent des détections périmétriques jusqu'à un kilomètre.

LE POINT DE VUE D'UN FABRICANT

MAXIME DE BROUX
Dirigeant de Solidbot


© DR

« ELLES SE DÉPLOIENT EN QUELQUES MINUTES. »

« Les unités mobiles Solidbot ont été développées pour être déployées en quelques minutes par n'importe quelle personne sans connaissances techniques. L'unité se positionne comme une simple remorque. Le mat se déploie automatiquement à 6 m et permet de faire face à des vents de plus de 100 km/h. Les systèmes de détections autonomes assurent des détections périmétriques jusqu'à un kilomètre. Les alertes sont envoyées depuis l'unité centrale vers une caméra PTZ autodirigée permettant à la centrale de surveillance de faire la levée de doute de jour comme de nuit et de communiquer directement avec le site grâce à un puissant haut-parleur et des spots leds directionnels. Entièrement autonome, grâce à son générateur à pile combustible, ses batteries et ses panneaux solaires, elle peut fonctionner sans raccordement pendant plus d'un an, sans avoir à aller sur site. Enfin, la transmission des données peut se faire en 3/4G, wi-fi longue portée ou satellite. »

● ● ● Pascal Pech, directeur général des activités du groupe Onet : *« Aujourd'hui, les professionnels de la sécurité privée ne peuvent plus se contenter de proposer à leurs clients des prestations ne reposant que sur des agents de sécurité. Nous nous devons de nous positionner comme des intégrateurs de solutions de sécurité associant ressources humaines et technologiques. Les unités de détection mobile comme notre Exosphère ou d'autres actuellement disponibles sur le marché permettent de répondre à des besoins exprimés par nos clients qui cherchent à pouvoir disposer rapidement de moyens technologiques pour sécuriser des sites et optimiser l'efficacité des forces de sécurité sur le terrain. »*

« Les unités mobiles de détection ou de surveillance comme notre Mobilguard doivent être conçues comme des solutions globales. Les utilisateurs recherchent en effet les moyens de sécuriser temporairement un site avec des moyens associant différentes technologies et rapide à déployer, explique Romain Gille, président du conseil d'administration de Ranc Développement. *Et ça que le site soit exposé à une menace terroriste ou à une situation de vulnérabilité ponctuelle. »*

Outre la surveillance électronique, les unités mobiles peuvent être pilotées ou servir de PC puisqu'elles intègrent souvent des moyens permettant de réceptionner et de traiter des alarmes.

Créer un périmètre de sécurité

« L'intérêt des unités mobiles est donc de pouvoir créer assez vite un périmètre de sécurité sur un site où les moyens technologiques et de communication fixes sont difficiles à déployer. C'est cette problématique qui a été à l'origine de la création de Mobilguard, explique Romain Gille. *Le but est de créer un périmètre de surveillance d'environ 5 000 m² grâce à des barrières IR radio, auxquelles on associe des caméras et divers autres accessoires qui viennent se greffer sur l'unité. L'intérêt de disposer d'éléments radio préside dans le fait qu'il permet de remonter facilement les informations à un opérateur ou un centre de surveillance. »*

Les unités mobiles sont donc conçues comme des microsystèmes de surveillance et de détection d'intrusion. *« Il s'agit de concevoir une solution sur laquelle pourront venir se greffer, facilement, et selon les besoins du client, différents éléments comme des caméras dotées de capteurs, des solutions de détection radar, etc., qui seront capables de communiquer avec le système de supervision,* ajoute Bernard Taillade de la société Hymatom. *On peut les alimenter avec des batteries, des capteurs solaires ou via le réseau d'éclairage présent sur le site. »* ● ● ●

LE POINT DE VUE D'UN FABRICANT

ROMAIN GILLE

Président du conseil d'administration de Ranc Développement

© DR

« DIMINUER LE COÛT DE LA PRESTATION HUMAINE. »

« Il faut le reconnaître, la première motivation des utilisateurs finaux pour utiliser des unités mobiles de détection et de surveillance est de diminuer le coût de la prestation humaine. Il peut être aussi de rationnaliser et d'utiliser plus efficacement les agents sur le terrain. Mobilguard a été conçue comme une solution de sécurisation autonome, mobile, temporaire et évolutive. Elle se présente sous la forme d'une unité installée sur remorque pour pouvoir se déployer très rapidement, tout en étant autonome puisqu'elle peut être alimentée par panneaux photovoltaïques et batteries. La solution se déploie très rapidement en environ une heure et demie. Actuellement, nous disposons en France de sept Mobiguard à Marseille, quatre à Paris et quatre à Lyon. »

Mobilguard de Ranc Développement a été conçue comme une solution autonome, mobile, temporaire et évolutive.

© DR

PAROLE D'EXPERT

PASCAL PECH

Directeur général des activités sécurité et accueil du groupe Onet

© DR

« ÉTENDRE LE PÉRIMÈTRE DE SÉCURITÉ. »

« En matière de protection des sites, on est face à deux choix. L'offre historique reposant sur des solutions physiques comme les obstacles, les câbles choc, etc. Et une offre plus technologique reposant sur de la détection périmétrique virtuelle reposant sur des capteurs vidéo pour de la détection via l'image faite soit par un agent, soit par l'IA. Nous avons conçu notre solution Exosphère en partant de ce constat et y avons intégré des caméras fixes pour la détection périmétrique et un ballon captif équipé d'une caméra d'une portée de 2 km. Le tout pouvant être complété par des drones. Cette solution permet de sécuriser de manière temporaire des sites industriels qui souhaitent étendre leur périmètre de sécurité et détecter l'intrus qui tente de franchir la protection périmétrique, afin de gagner en précocité. On peut aussi assurer la protection d'événements temporaires, de grands rassemblements de personnes sur des sites qui n'ont pas d'infrastructures sur lesquelles ils auraient pu déployer des moyens fixes. Enfin, on peut également utiliser Exosphère lors d'une catastrophe, d'un accident en soutien des forces de sécurité et des équipes de secours sur le terrain. »

Exosphère, d'Onet, une solution brevetée pour une coopération de sécurité.

© Onet

Un véritable centre de surveillance

Qu'il s'agisse d'IP Mirador, Ranc Développement, Solidbot, Onet, etc., les unités mobiles sont conçues comme des centres de surveillance autonomes. *« Des solutions comme notre Cube embarquent un centre de surveillance et sont donc très adaptées au déploiement sur des chantiers mobiles, ferroviaires et autoroutiers,* explique Christophe Segall. *Mais il faut que ces outils soient faciles à installer et à déplacer, autonomes, sans liaisons électriques sur de longues durées, résistantes aux intempéries et aux dégradations. Elles doivent pouvoir être livrées par n'importe quel transporteur où être déplacées sur une remorque. Le Cube est doté d'un mât télescopique qui s'élève jusqu'à 10 m, embarque quatre caméras jour/nuit à 360°, des capteurs infrarouges et un éclairage puissant qui se déclenche au moment de l'intrusion. Le système est compatible avec la réception sur smartphone relié à un serveur qui transmet en 3G/4G à un centre de télésurveillance distant. Le paramétrage se fait à distance par le PC de surveillance qui gère la sécurité du site. »*

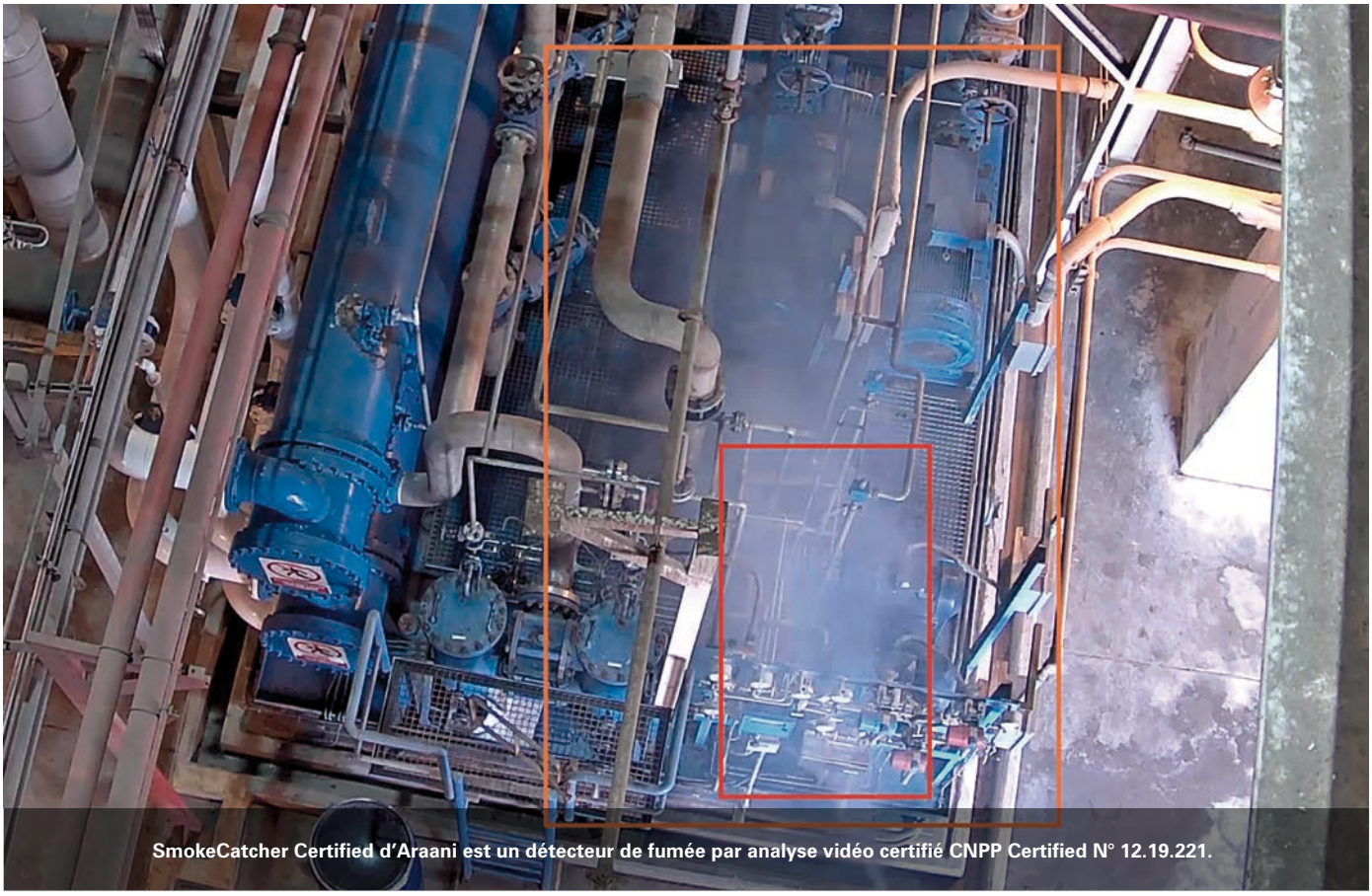
« En revanche, tient à préciser Romain Gille, *il est souhaitable de maîtriser toute la chaîne allant de la surveillance à la remontée d'alarmes, en passant par la télésurveillance. Et de ne pas se contenter d'une simple levée de doute. Cette maîtrise de la chaîne de sécurité permettra d'assurer au mieux la sécurité du site protégé. Par ailleurs, compte tenu du fait que les sites sur lesquels sont déployés ce genre d'outils sont parfois de nature très différente, il est très important de communiquer au mieux avec le client et de connaître les particularités du site et les risques auxquels il peut être exposé, afin de prendre les meilleures décisions le moment venu. »*

VOUS CHERCHEZ

UN DISTRIBUTEUR ?
UN INSTALLATEUR ? UN INTEGRATEUR ?
DU MATERIEL DE VIDEOSURVEILLANCE ?

- Trouver un distributeur près de chez vous
- Contacter un installateur, un intégrateur, ...
- Découvrir les équipements de sécurité (videosurveillance, contrôle d'accès, alarmes, ...) que proposent les Fabricants

Si vous souhaitez faire figurer votre entreprise dans cet annuaire, merci de nous contacter au 01 45 23 33 78 ou à info@protectionsecurite-magazine.fr



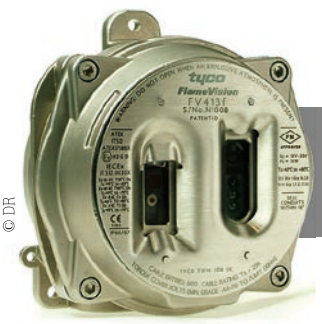
SmokeCatcher Certified d'Araani est un détecteur de fumée par analyse vidéo certifié CNPP Certified N° 12.19.221.

© Araani

Détection vidéo : sous certaines conditions uniquement !

Sur certains sites, la détection incendie traditionnelle se révèle impuissante. On peut alors envisager – sous des conditions strictes et précises – de recourir aux technologies d'analyse d'images ou thermographiques. Mais, attention, il s'agit toujours de lutte contre l'incendie. Et cela ne s'improvise pas !

Les solutions de détection incendie conventionnelles sont maîtrisées et ont fait la preuve de leur efficacité. Mais elles peuvent, dans certains cas et sur certains sites, montrer des limites. Ce que confirme Ronan Jézéquel, ingénieur développement au CNPP : *« Dans les déchetteries, dans certains volumes de très grande hauteur ou encore dans certains sites industriels, le recours à la détection incendie conventionnelle s'avère impossible. On peut alors*



© DR

FV400 : un détecteur de flamme Triple IR FlameVision FV413f de Tyco.

PAROLE D'EXPERT

NICOLAS SOCHARD

Responsable commercial France chez Araani

© DR

« NOTRE SOLUTION JOUIT DE LA CERTIFICATION DU CNPP. »

« Araani est une entreprise belge spécialisée dans le domaine de la VSD (Vidéo Smoke Detection) qui a obtenu la certification CNPP Certified sous le N° 12.19.221 avec sa solution SmokeCatcher Certified. Nous intégrons dans notre solution de détection incendie par analyse d'images nos propres algorithmes. Grâce à ces derniers, la caméra devient un capteur intelligent de détection de fumée. SmokeCatcher Certified est constamment auto-testée afin de s'assurer de sa disponibilité en cas de nécessité : vérification du champ de vision, luminosité minimale de 15 lux, qualité de la focalisation, contrôle du logiciel… Si un des paramètres testés n'est pas bon, le système signale un défaut au SSI. Par ailleurs, notre solution est alimentée en 24 volts via un AES – comme un capteur incendie conventionnel – et non en PoE qui n'est pas fiable. On peut associer SmokeCatcher Certified à un VMS pour des raisons de confort mais il faut absolument séparer les deux réseaux. Araani a un réseau de partenaires certifiés pour la mise en œuvre de la solution SmokeCatcher Certified qui comprend des sociétés expertes dans le domaine de l'incendie : ASI, CHUBB, Desautel, Eurofeu et Securitas Technologie. Des techniciens de chacun de ces partenaires ont suivi une formation sur la mise en œuvre de la solution SmokeCatcher Certified afin de garantir une pérennité de la solution. »

envisager, sous certaines conditions, d'utiliser les capacités des caméras – classiques ou thermiques – pour assurer la lutte contre le feu. Et donc se servir de systèmes de détection d'incendie par vidéo (ou VSD "video smoke detection"). Deux différentes technologies sont aujourd'hui disponibles et ont fait la preuve de leur pertinence. Sous certaines conditions évidemment. »

Analyse d'image ou détection thermique

Les deux technologies évoquées par l'expert du CNPP sont : les systèmes de détection de fumée ou de flamme par analyse d'images, d'une part, et, d'autre part, la détection de chaleur grâce à des caméras thermiques. *« Dans le premier cas, un algorithme permet d'analyser l'image et de détecter une fumée et son développement. Dans l'autre, la caméra thermique thermique permet de voir et de mesurer les points chauds via la mesure de température,* ajoute Ronan Jézéquel. *Et déclenche une alarme si un certain seuil de température est dépassé. »*

Ces solutions techniques sont certes efficaces et leurs performances théoriques bonnes. *« Ces nouveaux moyens de détection sont utiles car ils permettent de répondre à des besoins précis là où les produits normalisés ne sont pas possibles,* tient à ajouter Franck Lorgery, président du Gesi. *Mais attention, il ne faut pas que cela soit parasité par une approche plus marketing que réellement technique de la part de certains fabricants de solutions de vidéosurveillance. On ne peut pas les mettre partout. Nous* ● ● ●

© DR

Dahua propose une gamme de caméras thermiques dotées de capacités de détection incendie dont le modèle DH-TPC-SD8620-TB qui peut détecter un feu à grande distance. Une fonction particulièrement utile pour la lutte contre les feux de forêts.

© DR

« Ces caméras sont des détecteurs, une alarme feu. Cela doit rester leur unique finalité ! »

FRANCK LORGERY, PRÉSIDENT DU GESI

sommes sur un marché de niche, aux contraintes techniques précises. Ce n'est pas de la vidéosurveillance mais bien de l'incendie. Et ces systèmes doivent être conçus, installés, maintenus comme des systèmes incendie. Avec les mêmes exigences... »

Ces caméras sont des capteurs !

Il faut bien faire comprendre à certains professionnels que les caméras utilisées dans le cadre de la détection incendie doivent être considérées comme des capteurs incendie à part entière. *« Nous sommes ici en présence de capteurs incendie. Cela implique de se poser les bonnes questions et de comprendre que nous sommes dans le monde de l'incendie. Ce qui implique un changement de culture par rapport aux pratiques du monde de la malveillance,* insiste Ronan Jézéquel. *On doit donc s'interroger sur les performances réelles des caméras : quelle est la rapidité de la détection ? À quelle distance ? Cette détection est-elle fiable ? Le système est-il toujours disponible ? De réelles contraintes non seulement pour le choix de la caméra mais aussi en ce qui concerne son installation. On ne s'improvise pas installateur de caméras de détection incendie. »*

Il faut bien comprendre et insister sur le fait que les caméras utilisées pour de la détection incendie sont, comme tient à le préciser Nicolas Sochard, responsable commercial France chez Araani, *« des solutions qu'on doit déployer lorsque la détection conventionnelle n'est pas adaptée ou en soutien d'une installation classique. Il ne faut surtout pas laisser croire, ou s'imaginer, qu'elles peuvent venir remplacer de la détection conventionnelle qui, rappelons-le, a fait ses preuves. »*

On ne fait pas de la levée de doute !

Utiliser ces caméras comme des capteurs à part entière implique donc de comprendre certaines choses. *« On ne peut pas utiliser l'image éventuellement disponible sur ces caméras pour faire de la simple levée de doute,* insiste Vincent Chevallier, responsable audit et qualité au sein du Réseau DEF. *Ces caméras doivent permettre de faciliter et améliorer l'intervention. Cela requiert donc nécessairement de se déplacer sur zone pour constater et agir face au risque incendie. On ne peut en aucune manière se passer de cette levée de doute physique. L'image reste du confort mais peut donner des informations permettant de sécuriser l'intervention, en anticipant sur les moyens de protection idoines à mobiliser. »*

Il faut aussi insister sur le fait que quand on installe une solution de détection incendie par analyse d'image, elle doit être dédiée aux systèmes de sécurité incendie. *« Cela implique de disposer d'un réseau de communication dédié entre le système de sécurité incendie et les caméras qui sont utilisées en tant que détecteurs. On doit donc bien veiller à ce que les flux de données restent indépendants »*, ajoute Vincent Chevallier.

Quelles applications ?

On l'aura compris, le déploiement de caméras dans le cadre d'une installation de détection incendie ne doit concerner que des cas et des sites très particuliers. *« Les caméras de détection*

DU CÔTÉ DU FABRICANT

PATRICK GROSCLAUDE

Chef de produits FGDS chez Dräger Safety France

© DR

« Notre gamme de détecteurs visuels de flamme se compose de deux produits : le Dräger Flame 3000 et le Dräger Flame 5000. Grâce à leurs capacités d'analyse d'images via un algorithme, ils analysent la flamme et valident, ou pas, que ce que voit la caméra est bien un feu. Le Dräger Flame 5000, dès qu'il détecte une flamme, enregistre 7,5 secondes avant la détection et 7,5 secondes après afin de permettre d'analyser l'image pour ensuite modifier l'algorithme et éviter que cette image soit à nouveau prise en compte s'il s'agissait d'une fausse alarme. »

© DR

Le Dräger Flame 5000 est un détecteur visuel de flamme antidéflagrant basé sur une analyse du spectre visible de la flamme. Chaque détecteur fonctionne de manière autonome et intègre, dans un seul et même appareil, une vidéosurveillance, un traitement numérique du signal vidéo et un algorithme d'analyse d'images qui permet d'interpréter les caractéristiques de la flamme.

LE POINT DE VUE D'UN FABRICANT

OLIVIER KACHEL

Responsable marché et applications au sein du Réseau DEF

© DR

« LE DÉPLOIEMENT DE CES SOLUTIONS NE S'IMPROVISE PAS ! »

« Les capteurs de détection incendie par analyse d'images font maintenant partie intégrante d'un SSI. Le déploiement de ces solutions doit être rigoureux et faire l'objet d'une analyse de risques fine. Nous restons dans le domaine de la sécurité incendie et, à ce titre, devons garantir une précocité de détection, tout en prenant en compte ce qui pourrait perturber ce type de technologie. Pour cela, nous préconisons une période d'apprentissage de plusieurs semaines à l'issue de la mise en service, afin d'ajuster le paramétrage du système et aussi pour s'affranchir des éléments perturbateurs liés à l'environnement du site. Le "zéro fausse alarme" est difficile à garantir car, dans ces contextes, certaines poussières ont un comportement semblable à celui de la fumée. L'assistance de l'image vidéo prend alors tout son sens, pour permettre à l'exploitant de prendre la bonne décision dès l'apparition d'une alarme. »

par analyse d'images peuvent être déployées sur des sites difficiles dont les contraintes topographiques, de production ou d'exploitation rendent inefficaces les solutions conventionnelles, explique Nicolas Sochard. *On pourra par exemple les installer sur des sites de stockage et de traitement des déchets, dans de très grands locaux industriels, dans des environnements à hauts risques ou sur des sites sur lesquels un trop grand nombre d'alarmes est généré... Ou dans les cas imposant une détection très précoce afin de protéger de la plus-value.»*

Même constat au sein du Réseau DEF: *«Cette technologie s'adresse à la surveillance de zones spécifiques, là où la détection traditionnelle montre ses limites, comme les locaux de très grands volumes et de grandes hauteurs ou dans les sites de traitement des déchets. Ces environnements contraignants nécessitent une analyse de risque précise qui prend en compte les éventuels phénomènes perturbateurs liés à l'exploitation des sites: fumées naturelles de décomposition des déchets organiques, vent, pluie, gel, poussières... La détection incendie par analyse d'images peut également avoir du sens en complément d'une détection traditionnelle pour la surveillance* ●●●

© DR

La gamme de caméras thermiques d'Hikvision est vaste. Elle comprend entre autres le dôme DS-2TD4166T-25/50 qui est très utilisé pour assurer la détection incendie dans les déchetteries.

DU CÔTÉ DU FABRICANT

FRANCK CARETTE

Product Manager Thermal Products chez Hikvision


© DR

«Un départ de feu ou une élévation de température sont souvent invisibles à l'œil nu. Et quand la fumée apparaît, il est parfois déjà trop tard. L'intérêt des caméras thermiques utilisées pour détecter un départ de feu réside dans le fait qu'elles "voient" avant qu'apparaisse la fumée et détectent tout point chaud visible à la surface des matériaux. Mais attention, les caméras thermiques ne voient pas à travers les objets! Toute notre gamme de caméras thermiques est conçue pour faire de la mesure de température – de la thermographie – et envoyer une alarme si nécessaire. Attention encore une fois: toutes les caméras thermiques ne sont pas conçues pour faire de la thermographie. Dans l'étude de chaque cas, Il faut prendre en considération la qualité du capteur et de la résolution qui doivent être en adéquation avec ce type d'application. Afin de faciliter le choix de la bonne caméra, nous proposons un outil, le Hikvision Thermal Design Tool (téléchargeable gratuitement).»

3 QUESTIONS À

RONAN JÉZÉQUEL

Ingénieur développement au CNPP


© DR

Certains ont tendance à croire que les caméras de surveillance peuvent tout faire. La détection incendie n'y échappe pas. Que leur répondez-vous?

Les caméras traditionnelles ou thermiques jouissent de caractéristiques techniques qui, en théorie, pourraient en faire une alternative efficace aux solutions de détection conventionnelles. Mais cela n'est envisageable que sur certains sites où, justement, la détection conventionnelle montre ses limites. La détection incendie via des caméras peut venir en soutien d'une installation conventionnelle si cette dernière montre certaines limites, mais ce n'est pas souhaitable. Par ailleurs, il faut bien faire comprendre aux utilisateurs, aux installateurs et aux fabricants que les caméras utilisées dans l'incendie ne doivent plus être considérées comme des caméras mais comme des capteurs incendie à part entière, avec toutes les contraintes techniques, d'installation, de maintenance... que cela implique.

Justement, quels sont les impératifs et les contraintes à prendre en considération pour ce type d'utilisation des caméras?

Les caméras doivent tout d'abord être dédiées à la détection de flamme ou de fumée. Et pas pour autre chose. Cela implique donc qu'elles soient compatibles avec les centrales incendie du marché. Qu'elles respectent les contraintes de compatibilité électromagnétique et donc environnementales et qu'elles puissent assurer leur mission, même en cas de variation de l'éclairage. Il s'agit là de contraintes non négociables et qui pour la plupart n'ont rien à voir avec celles de la vidéosurveillance. Par ailleurs, il faut marteler le fait que l'installation de ce type de solution ne s'improvise pas. Nous sommes dans le monde de l'incendie. C'est pour cela que le CNPP a le projet d'encadrer l'installation de ces systèmes par une règle d'installation. Ce qui suppose une analyse des risques spécifiques, des contraintes en matière de conception des systèmes et des recommandations précises en ce qui concerne leur exploitation et leur maintenance.

Quels sont les axes de travail du CNPP pour encadrer les caméras utilisées en détection incendie?

Nous avons lancé une certification des produits spécifique et préparons un cadre avec et pour les installateurs. Les premiers produits certifiés seront rendus publics prochainement. Nous avons ainsi défini des spécifications techniques pour la détection de fumées et/ou de flamme et pour la détection de chaleur, qui formulent les exigences minimales applicables et proposent de mesurer les caractéristiques principales de ces deux types de systèmes. Le système devra également être capable d'apprendre de ses erreurs. Il faudra accompagner l'utilisateur pendant les premières semaines suivant la mise en œuvre pour affiner les paramètres des caméras qui déclencheront des fausses alarmes pendant cette période.

SUR LE TERRAIN

Airbus déploie la solution Réseau DEF

Il y a dix ans déjà, le site Airbus de Toulouse testait une solution anglaise de détection incendie grâce à des caméras. Aujourd'hui, c'est la solution FireEye de Réseau DEF qui protège des halls de 10 000 m² et de plus de 40 m de haut. *« Confrontés à la difficulté de déployer une installation de détection conventionnelle dans un hall de ces dimensions, nous sommes contraints de nous appuyer sur des caméras dédiées à la détection incendie. En l'occurrence les caméras Bosch intégrées dans la solution FireEye de Réseau DEF,* explique Jean-François Andreu, expert incendie chez Airbus Opération à Toulouse. *Aujourd'hui, grâce à une dizaine de caméras, nous pouvons assurer une détection précoce d'un départ de feu. Pour en arriver là, il a fallu effectuer des tests mais surtout consacrer plusieurs semaines à l'apprentissage du système afin de supprimer totalement les fausses alarmes que peut générer un tel environnement : luminosité, vent qui fait bouger les caméras, etc. »*

© Airbus/ F. Langelot

● ● ● *de process à valeur ajoutée, afin de gagner en précocité et ainsi sauvegarder les données, comme dans les laboratoires de recherche par exemple »*, ajoute Olivier Kachel, responsable marché et applications au sein du Réseau DEF.

Le Gesi veille…

« Nous sommes convaincus par l'utilité de ce principe de détection qui s'avère un complément idéal à nos produits normalisés – EN 54 – pour des applications particulières. Il n'en faut pas moins rester vigilant sur des dérives d'utilisation, martèle le président du Gesi, *qui pourraient nuire au bien de cette solution technique. Nous en avons déjà fait les frais par l'introduction d'une technologie utilisée en sureté mais qui avait besoin de maturité pour être respectable dans la sécurité incendie. Nous partageons la performance, la fiabilité, cependant, dans nos exigences produits, nous avons la répétabilité et la disponibilité à des situations extrêmes. Nos systèmes doivent être à tout moment capables de signaler un feu ou un dérangement lors de la présence d'un court-circuit sur une liaison. Il faut faire preuve de bon sens, les enjeux ne sont pas les mêmes. Le Gesi s'est donc saisi du sujet afin de cadrer les choses et a mis en place un groupe de travail sur les applications possibles des caméras en détection de fumée. De toute façon, il faut bien l'avouer, ces capteurs d'un nouveau genre ne jouissent pas du retour d'expérience d'un détecteur traditionnel… »*, conclut Franck Lorgery. ■

Fire Eye de Def se compose de caméras intelligentes embarquant des algorithmes permettant de détecter les fumées et les flammes dans ces environnements spécifiques, en s'affranchissant du phénomène de stratification. Fire Eye est particulièrement adaptée à la surveillance de zones relativement spacieuses, ouvertes ou semi-ouvertes.

© DR

© DR

« Ce genre de solution ne doit pas venir remplacer tout ou une partie de la détection conventionnelle. Elle doit se limiter à des cas très particuliers. »

VINCENT CHEVALLIER, RESPONSABLE AUDIT ET QUALITÉ CHEZ RÉSEAU DEF

DU CÔTÉ DU FABRICANT

MANUEL PINHEIRO

Responsable produits feu France et Belgique chez Johnson Controls

© DR

« Les caméras utilisées en détection incendie ne doivent pas remplacer une solution de détection traditionnelle si cette dernière peut être déployée efficacement. Chez Johnson Controls, nous utilisons depuis plusieurs années l'imagerie vidéo associée à des détecteurs d'incendie pour gagner en précocité. Notre détecteur FlameVision FV400, certifié NF-SSI et SIL2, est doté d'une caméra vidéo et d'un capteur de flamme triple IR qui permet de détecter un départ de flamme à plus de 50 m. Ces solutions sont complexes à déployer et requièrent de réelles compétences. Il faut considérer de nombreux paramètres : l'implantation et le calibrage des caméras, les exigences liées au domaine incendie… Tout cela nécessite d'accompagner le client dans l'analyse du risque, la définition de ses besoins, les ajustements inévitables après la mise en œuvre, etc. »


SIEMENS
Ingenuity for life*
SECURITY & SAFETY MEETINGS
Un lieu idéal est un lieu sûr.
Contrôle d'accès, vidéosurveillance, détection d'intrustion, protection périmétrique, hypervision.
Nos solutions innovantes pour la surveillance et le contrôle centralisé de vos accès et espaces pour une sécurité totale des personnes et des biens.
*L'ingéniosité au service de la vie
siemens.fr/perfect-places

Sites sensibles isolés, protection renforcée

Réseau limité ou inexistant, raccordement électrique difficile, délai d'intervention allongé… la configuration des sites sensibles isolés peut complexifier leur mise en sécurité. La protection de ces sites passe par la mise en place de solutions spécifiques qui tiennent compte de leur isolement et des risques que pourraient entraîner une intrusion ou un acte malveillant.

Transformateurs électriques, champs d'éoliennes, réserve d'eau potable, sites SNCF, antennes télécom… Souvent isolés, ces sites peuvent être la cible de dégradations ou d'intrusions qui risquent d'avoir des conséquences sérieuses. Les gestionnaires doivent donc protéger ces lieux en fonction de leur sensibilité, avec des systèmes adaptés à la configuration locale, de la clôture aux outils de détection et de contrôle d'accès, en tenant compte des délais d'intervention. D'où l'importance de dissuader, de limiter les fausses alertes et de qualifier au mieux les événements.

Dissuader, détecter, repousser et retarder

La protection physique constitue le premier rempart contre les actes de malveillance. À commencer par la clôture, comme le précise Florian Barbier, directeur d'activité Serpe : *« Solide, visible et délimitant clairement l'espace à protéger, une clôture doit avoir un rôle détecteur, dissuasif, répulsif, et retardateur. Toutefois, sur un site isolé, où le temps d'intervention est accru, deux paramètres sont très importants : une détection précoce et fiable sur clôture, et engendrer un retard maximum. Quant à la maintenance du système, elle doit être la plus simple possible. Ainsi, nous avons équipé de nombreux sites isolés de notre clôture détectrice à fils tendus Capfit 50. Facile à mettre en place, ce système a une durée de vie qui peut dépasser trente ans dans certains cas, ce qui offre un ratio performance/coût de possession sans égal. Il détecte les coupures et les écartements avec une grande fiabilité : on relève au maximum une fausse alarme par kilomètre et par an. C'est un capteur plébiscité par les sites sensibles, d'autant qu'il peut être raccordé facilement en contacts secs, ou en bus RS485 via le concentrateur Serpe Box, qui dialogue en IP avec tout type de superviseur. Le superviseur pourra alors commander des asservissements et transmettre les informations sur l'événement. L'autre système qui nous est de plus en plus demandé sur les sites sensibles est la clôture électrifiée détectrice, pour laquelle nous utilisons notre électrificateur Jaguar 400, qui a une forte action répulsive grâce à des impulsions 10 000 volts, et permet de détecter le toucher et les coupures de la clôture. »*

Vidéo : réduire le niveau de consommation de la bande passante

Coupler la clôture avec une vidéosurveillance, qui est aujourd'hui une évidence sur la plupart des sites industriels ou commerciaux, est plus discuté sur un site isolé. En cause, la

© DR

Iloq

C'est une prouesse technique : les clés électroniques Iloq assurent le déverrouillage, la gestion des droits et une traçabilité, sans batterie ni câblage ! Dans cette technologie brevetée, la simple insertion de la clé dans la serrure va être suffisante pour produire l'énergie temporaire nécessaire à la lecture des droits sur une puce RFID et au déverrouillage. La solution S10 comprend clé et cylindre, la solution S50 utilise un smartphone et le NFC qui communique les droits et l'énergie nécessaire à l'ouverture. Une solution Greentech, qui est particulièrement adaptée aux sites isolés pour lesquels il n'y a pas d'alimentation électrique au niveau des accès. Ce système qui peut venir en remplacement de cylindres standards existe aussi en version cadenas.

PAROLE D'EXPERT

PHILIPPE BÉNARD
Ingénieur avant-vente, Axis


© Axis

« LA TRANSMISSION DE DONNÉES RESTE LE MAILLON FAIBLE DES SITES ISOLÉS SENSIBLES. »

« Aujourd'hui, il existe une large palette d'outils pour mettre en sécurité un site isolé sensible, y compris en l'absence de réseau électrique. Nos caméras et radars, peuvent être alimentés par des sources solaires ou éoliennes combinées. Nous avons des solutions avec des piles à combustibles à l'éthanol qui peuvent fonctionner en toute autonomie sur des périodes de quinze jours à trois semaines. En revanche, le point crucial pour la protection d'un site isolé reste la transmission des données en temps réel. Si le site se trouve en zone blanche et dans l'impossibilité de raccorder à un réseau (G3/G4/ filaire, etc.), selon la sensibilité du site et les risques liés à une intrusion ou à une dégradation, il faudra, outre un renforcement des moyens physiques de protection et dissuasion, envisager une liaison satellitaire, afin de recueillir les alarmes et de pouvoir intervenir en cas d'événement. »

transmission d'images qui peut consommer beaucoup de bande passante, et des connexions parfois difficiles. « *La réduction de la consommation énergétique et de la bande passante n'est pas propre aux sites isolés, mais devient plus ardue lorsque le raccordement électrique est médiocre et la connexion limitée en 3G voire 2G,* souligne Philippe Henaine, directeur commercial de Panasonic France. *Or, sur un site isolé, il est primordial de conserver au maximum la qualité d'image, afin de qualifier au mieux les événements et de n'enclencher des interventions, parfois éloignées, que si cela est nécessaire. Nos caméras consomment très peu d'énergie et intègrent la technologie Smart Coding. Ce système réduit automatiquement la capture d'image de 30 images/seconde à 1/min, en l'absence de mouvement anormal. L'intelligence embarquée va distinguer un mouvement dû à une présence d'un mouvement récurrent comme des branchages mus par le vent, les vagues ou les pales des éoliennes. On va ainsi conserver la qualité de l'image mais obtenir une bande passante de l'ordre de 50 ko, c'est-à-dire une réduction allant jusqu'à 95 %. Nos caméras bénéficient également de la fonction autoVIQS (Variable Image Quality on Specific Aera) qui va se focaliser sur la zone de mouvements pertinentst et va donc réduire automatiquement la qualité de l'image dans les zones étant sans intérêt. Les images peuvent également être enregistrées de manière cryptée sur la carte SD de la caméra pour les sites non connectés.* »

Transmission des données

Point crucial sur un site isolé : la transmission des données. VDSYS, fabricant français leader sur le marché des antennes radio avec 25 000 sites équipés, conçoit des solutions radio ● ● ●

Axis

Le radar hyperfréquence D2050-VE Network Radar Detector qui fonctionne par effet doppler est en mesure d'identifier des personnes, des véhicules ou des objets en mouvement (vélo, moto, etc.). Très fiable, avec un taux d'alarmes intempestives extrêmement faible, ce radar effectue une détection à 120° avec une portée de 50 m. En cas d'événement, il est en mesure d'indiquer la position, l'angle et la vitesse d'un objet en mouvement. Adapté aux environnements extérieurs, il réduit les fausses alarmes déclenchées par la pluie, la neige, les insectes ou les ombres. Compatible avec les principaux fournisseurs VMS.

© Axis


© DR

Videofield
La caméra MotionViewer sans fil OMV-VX, fonctionne sur piles et est actionnée par détection de mouvement. Conçue pour les applications extérieures où la levée de doute vidéo est nécessaire, L'OMV-VX est constituée d'une caméra numérique, d'un détecteur de mouvement à infrarouge passif et d'un module radio Wiselink. Le module radio utilise une technologie de spectre étalée, interactive et cryptée pour une communication bidirectionnelle sans fil sécurisée avec la centrale d'alarme. La caméra se compose d'un capteur CMOS et d'un objectif 90 degrés. Quatre leds infrarouges permettent une distance d'illumination de nuit de 12 mètres. La détection de mouvement en infrarouge passif est assurée par deux lentilles de Fresnel. La zone de détection par défaut est de 90° avec une portée maximale de 12 mètres. L'OMV-VX est utilisée pour protéger les installations extérieures où la fiabilité de la détection est nécessaire.

hautes performances pour toutes les applications nécessitant l'utilisation d'un réseau sans fil (WLAN). *« VDSYS garantit des infrastructures radio hautement sécurisées et d'une fiabilité à toute épreuve,* indique Abdel Benothmane, président de VDSYS. *Nos antennes sont avant tout conçues pour la transmission très haut débit (jusqu'à 860 megabits par lien), de données sous toutes leurs formes : images, voix, données informatiques, téléphonies, alarmes, contrôle d'accès, ce qui permet de les intégrer dans un système de sécurité global. Si nous sommes très présents dans la vidéoprotection urbaine, nous avons développé une gamme adaptée aux sites isolés sensibles qui présentent des risques explosifs, comme des plates-formes pétrolières, des sites nucléaires, Seveso, militaires, etc. Cette gamme Atex est d'une grande résistance physique (IP 67 et IK10)., Elle fonctionne de -40 °C à +71 °C, résiste au brouillard salin (IEC 68-2-11) et au vent jusqu'à 240 km/h, et la portée des antennes atteint plusieurs kilomètres. Nos supports sont livrés complets, paramétrés avec les éléments du site. Pour les installateurs ce sont des solutions plug and play. Nous utilisons un protocole propriétaire de transmission qui garantit une immunité optimale contre les tentatives de piratage des données., et nous pouvons implémenter un double code AES 256 bits. Ces produits sont agréés par le ministère de la Défense. Comparé au câble, la transmission radio est cinq à dix fois moins chère, très simple à installer puisqu'il n'y a aucun génie civil, et d'une grande souplesse dans la mesure où il suffit de déplacer l'antenne en cas de changement de configuration du site. »*

Contrôler les accès

Comme sur tout site, le contrôle d'accès est essentiel, avec une traçabilité des accès et des événements. Pour des accès ponctuels, par exemple de maintenance, la solution de clés électroniques permet de tracer les accès, en temps réel si la connexion réseau est possible ou en différé en l'absence de réseau. Un certain nombre d'acteurs sur le marché propose des solutions de clés électroniques sans câblage, Assa Abloy, Iloq, Locken pour n'en citer que quelques-uns, qui permet de se dispenser d'un raccordement électrique au niveau des accès. *« Il est difficilement imaginable de câbler l'intégralité des accès sur un site de distribution électrique ou des locaux techniques dispersés sur le territoire,* remarque Mélanie Dubus, responsable marketing d'Assa Abloy, qui équipe les locaux techniques du

3 QUESTIONS À

PHILIPPE COSSAIS

Responsable déploiement et maintenance des infrastructures réseaux Orange


© DR

Que représentent pour vous les sites isolés ?
L'infrastructure d'Orange est extrêmement diversifiée, entre les pylônes qui portent les antennes, les bâtiments techniques et les armoires de rues, nous avons plus de 100 000 points. 25 000 points réseaux mobiles, 15 000 petits bâtiments techniques, un millier de sites de plus de 100 m² et une centaine de sites stratégiques. Si ces derniers, souvent en périphérie urbaine, disposent de personnel sur place, c'est plus rarement le cas des autres bâtiments. Dans la plupart de nos bâtiments, on va retrouver des alimentations électriques, des coffrets et des baies informatiques, des systèmes de climatisation et de réfrigération, de la protection incendie et des alarmes techniques. L'ensemble de ces éléments va devoir être régulièrement maintenu, contrôlé, mais aussi protégé des dégradations.

Comment assurez-vous la protection d'autant de sites ?
Nous avons un référentiel de sécurité pour le groupe et nous adaptons la sécurité à la sensibilité du site, avec a minima un contrôle d'accès via des clés électroniques. Les sites les plus sensibles auront bien entendu une protection renforcée avec vidéosurveillance, système anti-intrusion, contrôle d'accès suivi en temps réel. Pour les petits sites, avec un passage occasionnel, nous avons opté pour un équilibre entre économie et sécurité, avec le système de clés Cliq d'Assa Abloy. Nous gérons un parc de 24 000 clés pour l'ensemble de nos points d'accès.

Quels sont les avantages et les limites de ce système ?
Nous avons choisi d'accorder les droits à nos salariés pour trois ans, avec une synchronisation obligatoire tous les quinze jours, soit sur une borne fixe dans nos bureaux, soit sur boîtier mobile connecté pour les opérateurs nomades. Nos sous-traitants disposent aussi de clés. Le premier avantage est pour la traçabilité. Nous savons qui est le dernier intervenant sur un site et pouvons suivre les incidents s'il y a lieu. Ensuite, nous en avons fini avec les énormes trousseaux de clés, les duplications, les passes égarés, les organigrammes inextricables... et des techniciens qui se retrouvaient sans cesse devant un bâtiment sans pouvoir entrer. Cependant, ces clés demandent une vraie pédagogie. Si, en interne, l'utilisation est acquise, avec de nouveaux arrivants ou des externes, il faut bien sensibiliser au fait qu'il ne faut pas forcer – avec le risque de détériorer le cylindre ou la clé, et attendre le bip d'autorisation. Une habitude à prendre qui simplifie les tâches des opérateurs qui n'ont plus qu'une seule clé pour l'ensemble de leurs interventions.

www.iloq.com

01 81 80 14 30
france@iloq.com

KIMI RÄIKKÖNEN
OFFICIAL PARTNER

LA PAROLE À

PHILIPPE BILLET
Directeur général, Ascom


© Axis

« SUR LES SITES ISOLÉS, LA PROTECTION DES HOMMES PEUT SE COMBINER À LA GESTION DES ALARMES. »

« Les entreprises ont aujourd'hui l'obligation de fournir aux travailleurs isolés des dispositifs d'alerte, pour lancer les secours en cas de malaise ou d'agression. Spécialiste de la gestion des flux informatiques et des alarmes techniques, nous avons développé une plate-forme logicielle Mercury et Unite qui permet d'assurer la protection des travailleurs isolés, mais aussi de pouvoir remonter sur le même outil les alarmes techniques (fumée, incendie, panne machine, fuite de liquides, intrusion, ouverture de vannes, etc.). L'intérêt de notre solution est qu'elle est conçue de façon à localiser précisément par exemple l'incident, que ce soit un malaise ou une panne, et ce, quel que soit le mode de transmission. Pour les travailleurs isolés, cela peut se faire grâce des antennes radios et des récepteurs de type pager avec un coût minime, du GSM pour ceux qui ont des smartphones ou même des connexions DECT. L'intérêt de couvrir les trois modes de transmissions est de pouvoir s'affranchir des "zones d'ombres" sur un site, mais aussi d'éviter les interférences électromagnétiques. C'est un système que nous avons pu mettre en place dans un usine de production d'eau potable, très automatisée et hautement sensible.
Avec nos plates-formes logicielles, le client peut être prévenu en temps réel en cas d'intrusion, de perte de verticalité d'un de ses rondiers, mais aussi de toute anomalie liée à la production afin de réagir rapidement. »

● ● ● groupe Orange. Par ailleurs, la gestion des clés distribuées à de nombreux intervenants extérieurs réguliers ou ponctuels est très complexe et coûteuse, sans garantir la sécurité des sites dès l'instant qu'une clé est égarée. *« La solution Locken est particulièrement adaptée à ce contexte,* explique Catherine Laug, responsable marketing de Locken. *Les cylindres sont passifs. Il est donc inutile de les relier au réseau de distribution électrique : c'est la clé qui fournit l'énergie et les autorisations d'accès pour l'ouverture des portes. Ces cylindres électroniques, qui s'installent facilement en lieu et place des cylindres existants, n'exigent pas de maintenance. Ces particularités facilitent l'exploitation des sites isolés. Avec la clé électronique de dernière génération, la transmission des informations entre la clé et le cylindre s'effectue sans contact grâce à la technologie inductive. Cela permet à la clé électronique de communiquer les droits au cylindre même si celui-ci est obstrué par le sel, la pollution, la poussière ou encore s'il a subi une oxydation de surface provoquée par l'humidité des sites : les faux contacts ne sont plus un obstacle à la transmission de l'information. »* Iloq va encore plus loin avec un système breveté ne nécessitant aucune batterie que ce soit dans le cylindre ou dans le cablâge, tout en enregistrant les informations de traçabilité et de droits dans la clé. Si le site permet de recevoir du réseau, les droits peuvent être affinés en temps réel avec des systèmes comme Cliq d'Assa Abloy ou My-Locken. *« Les droits,* précise Catherine Laug, *peuvent être modulés en fonction du profil de l'utilisateur et paramétrés finement selon les lieux et les heures autorisés. Combinée à l'application MyLocken et aux nouvelles technologies (RFID, Beacon), celle-ci permet d'envoyer aux agents des messages de vérification relatifs à leur habilitation ou aux consignes de sécurité requises (port d'un casque, nécessité de présence d'un second collaborateur, etc.). De même, les intervenants peuvent communiquer avec le système central (déclarations de présence sur site, signalement d'anomalies, etc.). »*

Brinno

Spécialiste des suivis de chantiers, Brinno, le constructeur tawaïnais, dispose d'une petite caméra de sécurité, la MAC200, déclenchée par un détecteur de mouvement (PIR), ou à intervalle régulier ou en mode hybride (intervalle de temps + détecteur de mouvement). De jour comme de nuit, grâce à un capteur IR, elle enregistre les images sur sa carte SD. Résistante aux intempéries, cette caméra autonome alimentée par une simple pile d'une durée de vie d'un an, convient pour des sites isolés non alimentés électriquement et notamment en vidéo-élucidation (zone de dépôts sauvages, parkings isolés, sites désaffectés, etc.)

© DR

Drones automatiques, la vigilance 4.0

Mobile, rapide et précis, le drone commence à se développer dans la sécurité. Pour Philippe Gabet, président de Drone Protect System, le drone autonome trouve naturellement sa place dans la protection des sites isolés sensibles. *« Lorsqu'on parle de sites militaires ou de sites sensibles, une intrusion peut être considérée a priori comme malveillante, avec des risques non négligeables pour les primo-intervenants. En cas d'alarme sur clôture, le drone se déplace automatiquement en quelques dizaines de secondes sur l'événement et peut transmettre une évaluation précise de la menace au poste central, en évitant d'exposer inutilement les personnes. L'avantage du drone est bien sûr la rapidité, le fait qu'il puisse – contrairement à une caméra fixe, se déplacer pour supprimer les angles morts ou suivre une cible et qu'il fera difficilement l'objet de dégradation volontaire. Le drone, que nous avons mis en place en France sur un site sensible, se déclenche automatiquement et peut être opéré à distance par un simple opérateur formé. Dans un avenir très proche, les drones pourront communiquer avec des robots terrestres qui interviendront en lieu et place des hommes, dans des situations critiques, que l'on pense malveillance, accident majeur ou catastrophe. Il est au cœur d'un dispositif de sécurité communiquant aidant à la prise de décision. Le drone permet dès aujourd'hui de repenser les outils de sécurité et de redéployer les moyens pour une plus grande efficacité et une meilleure protection. »* ■

ESI GROUP

SpaceControl

Gestion centralisée pour Smart Project

+33 (0) 4 93 94 84 10
info@esigroup.eu / www.esigroup.eu
Le Sun Eden - 362 Avenue du Campon - 06110 Le Cannet FRANCE

ESI

ARGOS

+33 (0) 1 48 53 73 40
info@argostechnologies.eu / www.argostechnologies.eu
5 rue Walter Gropius - Immeuble ATHENES - 94150 Rungis FRANCE

Guide ANNUEL d'Achat

www.protectionsecurite-magazine.fr

RETROUVEZ PLUS DE PRESTATAIRES, LEURS ÉQUIPEMENTS ET SERVICES SUR LE SALON ONLINE

e-salon-protectionsecurite.fr

Si vous souhaitez figurer dans cette rubrique, merci de nous contacter sur
info@protectionsecurite-magazine.fr
ou au 01 45 23 33 78

DÉTECTION - ALARME

AE&T
www.aet.fr/fr/

ARD
www.controle-acces.fr

BY DEMES FRANCE
www.bydemes.com

BOSCH
www.boschsecurity.fr

FOXSTREAM
www.foxstream.fr

GUNNEBO FRANCE
www.gunnebo.com

HONEYWELL
www.honeywell.com/security/fr

IZYX SYSTEMS
www.izyx-systems.com

LEGRAND
www.legrand.fr

MAGNETA
www.magneta.fr

MWS
www.mws.fr

myfox
Regent Park II – Bât I
2460 l'Occitane
31670 Labège
Tél. 0 800 100 100
hcpro@myfox.fr
www.myfox.pro

OPTEX
www.optex-security.com

PROSEGUR FRANCE
www.prosegur.fr

RISCO GROUP
www.riscogroup.com

SCHNEIDER ELECTRIC
www.schneider-electric.com

SCUTUM
www.scutum.fr

SEPTAM
www.septam.fr

SERIS SECURITY
www.seris.be

SERVIACOM
www.serviacom.fr

SORHEA
www.sorhea.fr

SURTEC
www.surtec.tm.fr

SYNCHRONIC
http://www.synchronic.fr

TIL TECHNOLOGIES
www.til-technologies.fr

VANDERBILT
10, place Fulgence Bienvenue
77600 Bussy Saint Georges
Tél. 0825 16 11 77
www.vanderbiltindustries.com

ZENITEL
www.stentofon.fr

VIDÉOSURVEILLANCE

AASSET SECURITY
www.aasset-security.fr

ACALBFI
www.acalbfi.fr

ALL PRODUCTS
www.all-products.com

ARECONT VISION
www.arecontvision.com

AVIGILON CORPORATION
www.avigilon.com

AXIS COMMUNICATION
www.axis.com/fr

BOSCH
www.boschsecurity.fr

bydemes GROUP
BY DEMES FRANCE
22/24 rue Lavoisier
Bâtiment B, 1er étage D
92 000 Nanterre (France)
Tél : +33(0) 147240626
france@bydemes.com
www.bydemes.com

CISCO SYSTEMS
www.cisco.com

CITELUM
www.citelum.com/fr

COMPUTAR / GANZ
www.cbc-cctv.com

CONSORT NT
www.consortnt.com

D-LINK
www.dlink-com/fr

DAHUA
www.dahuasecurity.com/fr

DELTA SECURITY SOLUTIONS
www.delta2s.fr

DIGITAL BARRIERS
www.digitalbarriers.com

ECCTV
www.ecctv.fr

EET EUROPARTS FRANCE
http://fr.eetgroup.com

ERYMA SÉCURITÉ SYSTÈMES
www.eryma.com

EVITECH
www.evitech.com

EXAVISION
www.exavision.com

FLIR
www.flir.com

FOXSTREAM
www.foxstream.fr

FUJIFILM
www.fujifilm.eu/fr

GENETEC
www.genetec.com

GEUTEBRÜCK
www.geutebruck.com

HANWHA TECHWIN
www.hanwha-security.eu/fr

HIKVISION
www.hikvision.com

HONEYWELL
www.honeywell.com/security/fr

HYMATOM
www.hymatom.fr

IDIS EUROPE
www.idisglobal.com

INDIGO VISION
www.indigovision.com

INEO
www.cofelyineo-securite.fr

IOTEO
www.ioteo.com

IZYX
www.izyx-systems.c

JF TECH
www.jftech.com
sales@jftech.com

JVC PROFESSIONAL FRANCE
www.jvcpro.fr

MERIT LILIN
www.meritlilin.fr

MILESTONE SYSTEMS
www.milestonesys.com

MOBOTIX
www.mobotix.com

MYFOX
www.myfox.pro

NEXTIRAONE
www.nextiraone.eu/fr

OPTEX
www.optex-security.com

PANASONIC
http://business.panasonic.fr

PELCO
www.pelco.com

PROSEGUR FRANCE
www.prosegur.fr

RSI VIDEO TECHNOLOGIES
www.videofied.com

SAMSUNG TECHWIN EUROPE
www.samsungsecurity.fr

SCUTUM
www.scutum.fr

SERVIACOM
www.serviacom.fr

SONY
www.sony.fr/pro/products/videosecurity

STIM
www.stim.fr

SVD - SYSTÈMES VIDEO DIGITAL
http://svd-france.com

SYNOLOGY
www.synology.com/fr-fr/

TAMRON FRANCE
www.tamron.fr

TEB
www.teb-online.com

TIFALI
www.tifali.com

TIL TECHNOLOGIES
www.til-technologies.fr

VANDERBILT INTERNATIONAL
www.vanderbiltindustries.com

VEDIS
www.vedis.pro

VIVOTEK

Mail:
salesvivotekfrance@vivotek.com www.vivotek.com

VIZEO
www.vizeo.eu

WESTERN DIGITAL FRANCE
www.wdc.com/fr/

IDENTIFICATION CONTRÔLE D'ACCÈS

ABIOVA
www.abiova.com

ABUS FRANCE
www.abus.com

ACIE AUTOMATISME
http://aciesecurite.com

AIPHONE
www.aiphone;fr

ALCEA
www.alcea.fr

ASSA ABLOY FRANCE
www.assaabloy.fr

BOSCH
Des technologies pour la vie

32 avenue Michelet
93400 Saint Ouen
Tél. 0 825 12 8000
Tél. 0 825 12 8000
fr.securitysystems@fr.bosch.com
www.boschsecurity.fr

CAE GROUPE
www.cae-groupe.fr

CASTEL
COMMUNICATION ET SÉCURITÉ

Z.I. St Lambert des Levées
49400 Saumur
Tél. 02 41 40 41 40
info@castel.fr
www.castel.fr

DEISTER ELECTRONIC FRANCE
www.deister.com

DIRICKX GROUPE
www.dirickx.fr

ERYMA SECURITE SYSTEMES
www.eryma.com

FOXSTREAM
www.foxstream.fr

Genetec™

Genetec Europe
6 Rue Daru,
Paris 75008
Tél. 01 44 69 59 00
info@genetec.com

GEUTEBRÜCK
www.geutebruck.com

HID GLOBAL
www.hidglobal.fr

HONEYWELL
www.honeywell.com/security/fr

HOROQUARTZ
www.horoquartz.fr

ILOQ
www.iloq.com/fr

IZYX SYSTEMS
www.izyx-systems.com

izyx systems
Tél. 03 88 75 32 32
info@izyx-systems.com
www.izyx-systems.com
FABRICANT INNOVANT
Solutions de contrôle d'accès et de sécurité électronique

KABA
www.kaba.fr

LOCKEN SERVICES
www.locken.fr

MYFOX
www.myfox.pro

NEDAP FRANCE
www.nedap.fr

PAXTON
www.paxtonaccess.fr

PRASTEL

ZI ATHELIA II
225 impasse du Serpolet
13600 La Ciotat – France
Tél : 04.42.98.06.06
Mail : info@prastel.com
Site internet : www.prastel.com

PROSEGUR FRANCE
www.prosegur.fr

REXEL
www.rexel.fr

RISCO
www.riscogroup.com

SALTO SYSTEMS FRANCE
www.saltosystems.com/fr

SCUTUM
www.scutum.fr

SEPTAM
www.septam.fr

SERIS SECURITY
www.seris.be

SERVIACOM
www.serviacom.fr

SIEMENS
www.siemens.fr/buidingtechnologies

SIMONS VOSS TECHNOLOGIES
www.simons-voss.fr

SEWOSY
Fabricant

13b rue Saint-Exupéry
ZA de l'Aérodrome - CS20152
F-67503 Haguenau Cedex

Tél. : +33(0)3 90 59 02 20
Fax : +33(0)3 90 59 02 19

www.sewosy.com

STANLEY SECURITE FRANCE
www.stanley-securite.fr

STID
www.stid.com

SYNCHRONIC
www.synchronic.fr

TECHNICOB
www.technicob.com

TIL TECHNOLOGIES
www.til-technologies.fr

UHLMANN & ZACHER
www.uundz.com

UNIACCESS
www.uniaccess.fr

VANDERBILT INTERNATIONAL
www.vanderbiltindustries.com

ZENITEL
www.stentofon.fr

LUTTE CONTRE LE FEU

ASD
Systèmes de détection incendie

2 ter avenue de France
B.P. 33
91301 Massy
Tél. 01 69 93 81 90
www.asd-incendie.fr

AVISS SECURITE
www.aviss-securite.fr

BOSCH
www.boschsecurity.fr

COOPER SAFETY FRANCE
www.cooperfrance.com

DEF
www.def-online.com

DUBERNARD
www.dubernard.fr

EDC PROTECTION
www.edc-protection.com

EIFI
www.eifi-incendie.fr

EUROFEU
www.eurofeu.fr

FRANCE INCENDIE
www.france-incendie.fr

GROUPE GORGE
www.groupe-gorge.com

INEO
www.cofelyineo-securite.fr

MYFOX
www.myfox.pro

NISCAYAH
www.stanley-securite.fr

PX TECHNOLOGIES
http://pyrexx.com/detecteurs-de-fumee

SERVIACOM
www.serviacom.fr

SLAT
www.slat.com

TYCO FIRE PROTECTION
www.tfppemea.com

ZETTLER
www.zettlerfire.com

CNPP
www.cnpp.com

DEKRA INDUSTRIAL
www.dekra-industrail.fr

EXAVISION
www.exavision.com

SOCOTEC
www.socotec.fr

SCUTUM
www.scutum.fr

PROTECTION PÉRIMÉTRIQUE

GEUTEBRÜCK
www.geutebruk.com

HYMATOM
www.hymatom.fr

OPTEX
www.optex-security.com

OREP
www.orep-securite.com

SORHEA
www.sorhea.com/fr

UTC CLIMATE, CONTROLS & SECURITY
www.ccs.utc.com/ccs/en/worldwide

CONTRÔLE D'ACCÈS

SmartRelais 3 Advanced, le contrôleur dernière génération de SimonsVoss

SimonsVoss, spécialiste des contrôles d'accès intelligents, vient de lancer la solution SmartRelais 3 Advanced, une passerelle d'accès en ligne, composée d'un contrôleur connecté au logiciel LSM (Locking System Management) installé sur le PC du client et d'un ou plusieurs lecteurs externes qui communiquent en temps réel les données aux supports d'identifications respectifs.

« Simple, sûr, flexible et économe, le SmartRelais3 Advanced permet d'avoir les avantages d'un réseau en ligne sans sa complexité d'installation ! » précise Éric Nottin, directeur technique de SimonsVoss France.

Le SmartRelais 3 Advanced est un génie polyvalent qui joue, en tant qu'unité de commande, plusieurs rôles dont celui de passerelle haute performance dans un réseau virtuel. Il peut lire, collecter et écrire les informations sur les supports d'identifications (cartes ou transpondeurs). Les cartes vont communiquer avec les serrures pour remonter les informations au SmartRelais 3 Advanced qui, en temps réel, communique avec le logiciel (LSM).

Le contrôleur va alimenter le lecteur via le réseau Ethernet et jouer l'intermédiaire entre le logiciel LSM et le lecteur. L'intelligence et les contacts d'ouverture sont présents uniquement dans le contrôleur. Raccordé à ce dernier, le lecteur externe va collecter et envoyer le flux d'informations en fonctionnant avec l'aide de supports d'identification non seulement actifs (transpondeurs) mais aussi passifs (cartes ou badges). Pour des entrées multiples, il est possible de relier jusqu'à trois lecteurs externes via le câble Ethernet RS485 dans votre bâtiment.

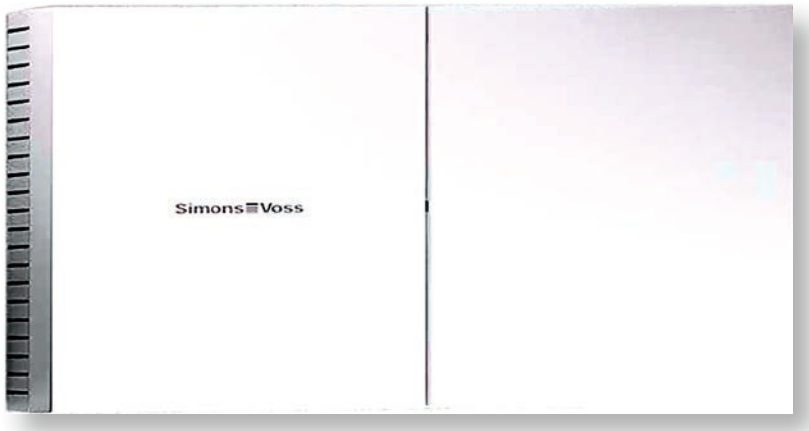
SmartRelais3 Advanced se distingue de ses prédécesseurs par des fonctionnalités avancées :

• Le rechargement des droits d'accès éphémères pendant un temps défini (budget temps). Ce système de fonctionnement renforce la sécurité des accès dans les bâtiments disposant d'une entrée principale obligeant les utilisateurs à rebadger sur la borne principale pour recharger leurs droits d'accès.

• Le système viral : lorsqu'un badge est égaré, le gestionnaire du site transmet les informations à la borne d'actualisation qui met à jour automatiquement la blackliste sur les badges des utilisateurs tierces, ces derniers communiqueront cette même blackliste aux serrures lors du passage sur la porte. Un moyen rapide de bloquer une carte égarée dans un bâtiment.

• La possibilité de combiner les différents types de mises en réseau : mise en réseau virtuelle des fermetures autonomes, mise en réseau directe « online » (WaveNet) des composants de fermeture, programmation sur place des fermetures à l'aide de l'appareil de programmation SmartCD. Le réseau virtuel est combinable et évolutif avec toutes les solutions de SimonsVoss Technologies. ■

→ **www.simons-voss.com/fr**



3 QUESTIONS À

JEAN-PHILIPPE VUYLSTEKE

Président de SimonsVoss France

© DR

En quoi la solution SmartRelais 3 Advanced est-elle innovante ?

Elle est issue d'une nouvelle plate-forme électronique, Advanced XChange, qui implique un protocole de sécurité renforcé au niveau du matériel et des communications ultrarapides et sécurisées. Elle bénéficie d'une électronique beaucoup plus performante et surtout de notre nouveau réseau virtuel hybride.

Quelle est la particularité de ce réseau hybride ?

Il peut être utilisé aussi bien avec des technologies passives comme un système de badges classiques RFID, Mifare ou DesFire qu'avec la technologie active brevetée SimonsVoss, de transpondeur qui communique à très basse fréquence. Pour les installateurs, l'intérêt est de pouvoir choisir la technologie active ou passive en fonction des contraintes du site, mais aussi de pouvoir sans difficulté l'intégrer à un système déjà en place. Comme il ne nécessite pas l'ajout de nœud réseau sur les cylindres, ni d'antennes supplémentaires, cela en fait un produit adapté à une large cible de clientèle, aussi bien dans les bâtiments santé, éducation, tertiaire ou encore industriels, à des coûts compétitifs, notamment en comparaison avec une solution full réseau.

Quels sont les avantages de votre transpondeur ?

Ce système, unique sur le marché, délivre un identifiant radio inviolable et incrackable. La mise à jour se fait par transmission virale, du transpondeur aux cylindres et vice-versa. De plus, il confère une très grande autonomie : alors que les cylindres et poignées sécurisés du marché permettent de 20000 à 80000 manœuvres, notre système par transpondeur garantit 300000 manœuvres, soit sept à dix ans d'autonomie.

LUTTE CONTRE LE FEU

Vernis intumescent Promadur pour le bois

Le nouveau vernis intumescent Promadur de Promat, permet de prolonger et de renforcer la stabilité structurelle des ossatures intérieures en bois. Un atout supplémentaire pour ce matériau qui tend à s'imposer de plus en plus sur le marché de la construction et notamment dans le cadre de projets architecturaux d'IGH. Promadur est un vernis transparent intumescent complété par un vernis de finition Promadur Topcoat pour la protection incendie des structures intérieures en bois (poteaux, poutres, planchers et cloisons en bois). L'alliance du vernis intumescent transparent et de son vernis de finition permet d'améliorer la réaction au feu des structures intérieures en bois, pour tout type de bâtiment, en neuf comme en rénovation, tels que les hôtels, les restaurants, les écoles, les bâtiments publics, les musées, les bibliothèques, les bureaux et les maisons individuelles. ■

→ **www.promat.fr**

© Promat

CARACTÉRISTIQUES

- Grâce à ses excellentes propriétés, Promadur garantit une protection efficace : avec 470 g/m² minimum de protection Promadur, un bois standard passe d'une réaction au feu de D-s1, d0 (M3) à B-s1, d0 (M1). En cas d'incendie, il s'expanse et forme une couche épaisse, isolant thermiquement la surface en bois de l'oxygène de l'air.
- Sa mise en œuvre est facile, rapide et économique. Une seule couche de Promadur d'environ 362 µm d'épaisseur suffit pour couvrir une surface de 26,60 m². Le vernis doit être appliqué avec soin sur un support sain et dépoussiéré à l'aide d'une brosse ou d'un rouleau (pour de petites surfaces) ou d'un pulvérisateur Airless pour recouvrir rapidement et de façon homogène de plus grandes superficies.

CONNECTIQUE

SDC-PoE24, un switch layer 2,24 ports chez Slat

Slat poursuit le développement de son offre avec le SDC-PoE24, un switch PoE / PoE+ 24 ports full Gigabit manageable et sécurisé par Micro-UPS intégré. Cette nouvelle solution répond aux problématiques de qualité de service des applications de type contrôle d'accès, vidéosurveillance, gestion technique des bâtiments intelligents et management des systèmes médicaux.

Pour répondre à l'augmentation des data transmises, assortie d'un besoin de fonctionnement en temps réel et à la généralisation des superviseurs délocalisés dans les data centers, les bâtiments s'équipent eux aussi d'autoroute de données à base de fibres optiques. La conversion se fait sur des nœuds de réseau qui dispatchent les informations et fournissent la puissance aux objets du bâtiment. Mais ces nœuds de réseau sont devenus également des points de fragilité pour la continuité de service. Face à ces enjeux, Slat a développé le SDC-PoE24, un switch concentrateur permettant le raccordement Ethernet de 20 périphériques par câble RJ45 avec alimentation en PoE et quatre ports fibre optique. Au-delà des spécificités de base, Slat a ajouté trois systèmes de sécurité :

- Au niveau électrique : un convertisseur intégré pour assurer l'alimentation du switch et de tous les objets connectés en PoE, une protection contre les microcoupures, un maintien de l'alimentation en cas de coupure de secteur.
- Au niveau fonctionnel : un monitoring permanent. Une fonction réflexe déclenche en cas de défaillance d'un objet et un reboot automatique pour assurer la remise en service. Si l'objet ne répond pas, une alerte est envoyée au superviseur.
- Au niveau réseau : une supervision cryptée avec échange de certificat pour éviter les intrusions et malversations. La compatibilité aux protocoles Radius et 802 1X pour l'authentification des objets raccordés au réseau. Des protections contre les attaques par déni de service ou usurpation d'adresse. ■

→ **www.slat.fr**

CONTRÔLE D'ACCÈS

Lancement de l'interphone vidéo DoorBird

© DoorBird

Le fabricant berlinois Bird Home Automation Group élargit sa gamme d'interphones vidéo IP avec le nouveau DoorBird D2101IKH. Ce nouveau modèle est équipé d'un panneau d'informations et d'un clavier intégré pour le contrôle d'accès par codes PIN. Parmi les autres composants de ce puissant interphone et solution de contrôle d'accès, citons une caméra grand angle, un lecteur RFID, un bouton d'appel et un système audio bidirectionnel.
L'interphone vidéo DoorBird D2101IKH IP est étanche et fabriqué en acier inoxydable. Le bouton-poussoir d'appel est rétroéclairé par un symbole de cloche gravé et est également fabriqué en acier inoxydable. Le D2101IKH est le premier modèle DoorBird à être équipé d'un panneau d'information rétroéclairé.
Le panneau d'informations est une fenêtre rétroéclairée dans laquelle des panneaux imprimés ou des graphiques peuvent être insérés pour afficher l'adresse ou d'autres informations.
Avec le DoorBird D2101IKH, les utilisateurs peuvent accéder aux locaux en utilisant l'application DoorBird, un lecteur RFID intégré ou en entrant un code PIN sur le clavier. Des codes d'accès individuels peuvent être attribués, par exemple, à un service de nettoyage pour permettre l'accès à des heures programmées ou une seule fois. ■

→ **www.doorbird.com**

CARACTÉRISTIQUES

- Jusqu'à huit smartphones ou tablettes peuvent être connectés à l'interphone de porte D2101IKH.
- Lorsque la sonnette retentit, les utilisateurs sont alertés par une notification push sur leur appareil mobile. Après avoir ouvert la notification push, l'utilisateur peut voir et parler au visiteur via l'application DoorBird.
- Avec l'application DoorBird, les utilisateurs peuvent ouvrir des portes à distance pour autoriser l'entrée des invités ou permettre aux coursiers d'effectuer leurs livraisons. Les parents peuvent aussi déverrouiller la porte d'entrée pour leurs enfants s'ils ne sont pas à la maison.

VMS

VisiMax, version 8.8

CASD a lancé sur le marché des VMS le tout dernier VisiMax : la version 8.8. Trois innovations majeures viennent compléter un panel de fonctionnalités déjà impressionnant et au plus près des attentes des utilisateurs :
la géolocalisation des patrouilles sur le terrain dans le SIG (en partenariat avec la société Sysoco),
la prise en charge de l'accélération matérielle (GPU) et la visualisation du parc caméra via le SIG dans le portail Web, disponible sur n'importe quel smartphone ou tablette.
Géolocalisation des signaux de radiocommunication : VisiMax propose désormais un nouveau module de géolocalisation, compatible avec la solution de radiocommunication Sysoco. Ce module vous permet de récupérer la position des signaux radio sur une cartographie SIG, afin de renforcer la sécurité des équipes terrain.
Prise en charge de l'accélération matérielle (GPU) : VisiMax intègre sur sa nouvelle version l'accélération matérielle via le processeur graphique, permettant d'alléger l'utilisation du processeur et d'afficher un plus grand nombre de flux, notamment pour les flux de haute qualité. Cette fonctionnalité est compatible avec les GPU NVIDIA de la série Pascal/Turing.
Visualisation des caméras via le SIG dans le portail Web : grâce à la nouvelle version de VisiMax et son portail Web, l'utilisateur est désormais en mesure de récupérer la position de ses caméras sur votre cartographie SIG et d'en afficher le flux depuis n'importe quel smartphone ou tablette. ■

© Sbat

→ **www.casd.fr**

CONTRÔLE D'ACCÈS

HID Global crée HID Origo

© HID Global

La nouvelle plate-forme cloud HID Origo est désormais disponible. Elle couple les technologies HID de gestion des identifiants mobiles (avec prochainement des services de géolocalisation) et son architecture étendue de contrôle des accès. Cette plate-forme propose un modèle favorisant la création d'applications innovantes : elle offre une suite complète d'outils et de services d'intégration, de mise en œuvre et de développement, tous visant à simplifier, pour le nombre croissant de nouveaux développeurs et revendeurs, la mise sur le marché de solutions de contrôle des accès.
La plate-forme embarque les connexions avec le cloud et les fonctionnalités dédiées aux objets connectés dans des extensions d'applications destinées aux appareils mobiles, aux lecteurs et aux contrôleurs HID. Elle donne aux développeurs un accès direct à ces équipements via des interfaces de programmation (API) et des kits de développement (SDK) dédiés qui ont déjà fait leurs preuves avec la solution d'accès mobile de HID. Elle permet également de réaliser des analyses de données pour de nouvelles applications : configuration de lecteur à distance, maintenance prédictive des systèmes de contrôle des accès, mais aussi détection des intentions, pour personnaliser et fluidifier davantage l'expérience de l'environnement de travail. ■

→ **www.hidglobal.fr**

DRONES

Drone Volt lance Airshadow

Airshadow de Drone Volt est un mini-drone compact et résistant qui peut voler avec une faible signature visuelle et sonore jusqu'à 90 km/h de jour comme de nuit.
L'Airshadow se décline en deux versions avec une portée allant jusqu'à 5 kilomètres. La transmission des données homme/machine en temps réel est sécurisée par l'utilisation de l'algorithme d'encryptage AES-256 se faisant en toute sécurité. Le drone est, par ailleurs, doté d'une faible signature visuelle et sonore.
Avec sa caméra et son détecteur infrarouge, il peut acquérir avec une grande précision images et vidéos, de jour comme de nuit, comme par exemple des plaques d'immatriculation ou des visages.
Capable de voler dans des conditions climatiques difficiles, de pluies modérées et de vents jusqu'à 40 km/h, la structure rigide de son châssis en nylon renforcé en fibres de carbone le rend plus résistant aux chocs et lui confère une excellente robustesse.

© Drone Volt

L'Airshadow est compact et simple à transporter (31 x 33 cm et 15 cm de hauteur). Aucun montage n'est requis pour son utilisation. Ultrarapide, il peut atteindre une vitesse de vol de 90 km/h et peut voler pendant 20 minutes avec un large rayon d'action et une portée de transmission vidéo maximum de 5 km.
L'application Drone Volt Control permet de programmer simplement différentes missions et de suivre l'évolution des données télémétriques sur l'écran de contrôle.
Deux versions disponibles :
- Avec une caméra performante de 180 grammes. Cette double caméra stabilisée EO-EI (Electro-Optical-Infra Rouge) pour des images de qualité de jour comme de nuit. Son zoom numérique x 20 lui permet de capturer des images détaillées.
- Avec une optique couplant une caméra thermique 160 x 120 et une caméra couleur 2 mégapixels.
Il est possible de basculer d'une caméra à l'autre ou d'afficher les deux avec le mode « picture-inpicture ». ■

→ **www.dronevolt.com/fr**

© DR

« Vingt ans de lutte pour la moralisation de la profession. »

DANIÈLE MESLIER
Présidente de l'Association nationale des métiers de la sécurité

L' Association nationale des métiers de la sécurité (ADMS) a vingt ans. L'occasion de donner la parole à Danièle Meslier, sa présidente, pour faire le point sur ses actions passées et futures.

Accompagnée des membres fondateurs, j'ai créé l'ADMS en 1999. Cet anniversaire est l'occasion pour moi de remercier les participants : adhérents, partenaires pour leur présence et leur fidélité qui pour certains dure depuis vingt ans comme Verspieren et maître Ghislaine Moulai, le CNPP, représenté pour cet anniversaire par son délégué général, les salons Préventica et Expoprotection... D'autres organisations professionnelles et personnalités extérieures étaient également présentes. L'ADMS est une grande famille qui rassemble des personnes ayant les mêmes valeurs de professionnalisme et de respect.
Sa principale mission porte sur les conseils et assistance auprès de ses adhérents, plus particulièrement les PME, privilégiant les problèmes rencontrés sur le terrain : accompagnement pour la mise en conformité au RGPD, etc.

Moraliser la profession

L'ADMS, très tôt, s'est donné pour mission de moraliser l'ensemble de la profession, tant du point de vue installation que pour la maintenance des systèmes électroniques. Ainsi, l'ADMS œuvre depuis 2014 pour attirer l'attention de l'État, pour intégrer ces activités dans le périmètre du Cnaps.
Démarche renouvelée en 2017 auprès du délégué aux coopérations de sécurité en présence d'Elisabeth Sellos Cartel, que nous remercions pour l'intérêt qu'elle a bien voulu porter à l'ADMS depuis 2007. Nous avons noté avec plaisir que ce point a été retenu dans le rapport sur le continuum de sécurité rédigé par les députés Jean-Michel Fauvergue et Alice Thourot.
En ce qui concerne la moralisation de la sécurité privée, nous avons commencé nos premières démarches en 2005 auprès de la Dilti (Délégation interministérielle pour la lutte contre le travail illégal) pour attirer l'attention de l'État sur les pratiques frauduleuses de certaines entreprises. Le commissaire chargé de mission qui nous avait reçu était présent pour les vingt ans de l'ADMS. Cette rencontre a été suivie par la mise en place de la première convention nationale pour la lutte contre le travail illégal déclinée par la suite toujours sous l'impulsion de l'ADMS.

Continuum de sécurité

L'ADMS n'a eu de cesse de mettre tout en œuvre pour lutter contre ce fléau : participation à la charte de bonnes pratiques d'achat de prestataires de sécurité privée, rédaction d'un document « Questions - Réponses » destiné aux donneurs d'ordres rédigé dans le cadre du comité de suivi de la convention nationale, organisation de conférences avec la Direccte, l'Urssaf et le Cnaps pour informer les donneurs d'ordres.
Ces conventions permettent l'échange d'informations entre les différentes instances signataires, sécurité publique et sécurité privée.
Nous avons, depuis la création du Cnaps, invité ses représentants à nos différentes réunions permettant ainsi des échanges constructifs qui ont toujours été enrichissants pour les deux parties. Pascal Gérard, directeur adjoint chargé des opérations, nous a fait le plaisir de venir partager ce moment avec nous.
D'autre part, un certain nombre de points mentionnés dans le rapport sur le continuum de sécurité rejoint nos préoccupations et correspond à notre analyse de l'évolution de la profession.
Nous aurons l'occasion d'en reparler prochainement. ■

DANIÈLE MESLIER ■ **JANVIER 1997** Création de l'ADMS regroupant installateurs, télésurveilleurs, gardiennage, intervention, constructeur. ■ **JANVIER 2012** Reprise et mise en place du service qualification et vérification Apsad : intrusion-télésurveillance-incendie au CNPP à Vernon. ■ **JANVIER 2014** Développement du «syndicat» regroupant installateurs et télésurveilleurs.

VOUS CHERCHEZ DES SOLUTIONS DE SURVEILLANCE, D'IDENTIFICATION, ... ?

VISITEZ LE 1ER SALON ONLINE SUR LA SURETE ET LA SECURITE !

1 Vous choisissez le hall que vous souhaitez visiter

2 Vous sélectionnez les catégories de produit que vous recherchez : vidéosurveillance, identification, contrôle d'accès, détection, alarme...

3 Vous consultez tranquillement les fiches techniques des produits, visionnez les vidéos de démonstration, les documentations techniques, les catalogues, faites en direct des demandes de devis, ...

Un salon permanent, ouvert 365 jours par an, afin de vous permettre de trouver et choisir tranquillement le matériel ou produit que vous recherchez et contacter directement le fabricant.

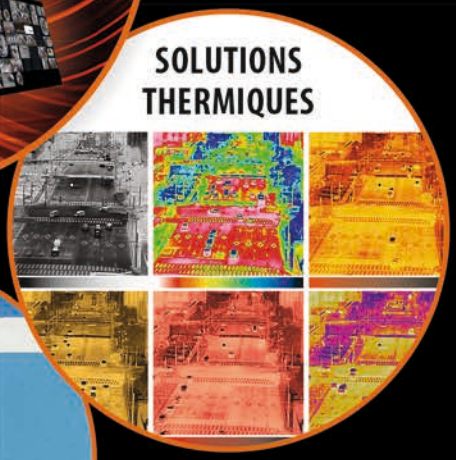
Si vous souhaitez faire figurer vos produits sur ce salon online, merci de nous contacter : **info@protectionsecurite-magazine.fr**

e-salon-protectionsecurite.fr

WISENET

SOLUTIONS

HANWHA TECHWIN, LEADER SUR LE MARCHÉ DE LA VIDÉOPROTECTION



www.hanwha-security.eu

Hanwha Techwin