psm

PROTECTION SÉCURITÉ MAGAZINE

Les Solutions pour les Professionnels de la Sûreté - Sécurité

n°257

Janvier Février 2020

26 €

VIDÉO-SURVEILLANCE

MONITEURS : UNE IMPORTANCE SOUS-ESTIMÉE

Entretien

YVAN DE MESMAEKER,

SECRÉTAIRE GÉNÉRAL DE L'EUROPEAN CORPORATE SECURITY ASSOCIATION

« IL FAUT RENFORCER L'ÉCHANGE D'INFORMATIONS ENTRE LE PUBLIC ET LE PRIVÉ. »

Contrôle d'accès

RECONNAISSANCE FACIALE ET BIOMÉTRIE DE LA MAIN, UNE CROISSANCE TIMIDE

Incendie

SPRINKLEURS : UNE EXTINCTION À L'EFFICACITÉ ÉPROUVÉE

DOSSIER

L'IA AU SERVICE DE LA SÉCURITÉ ?

+ L'ANNUAIRE DE LA SÉCURITÉ SÛRETÉ AVEC CE NUMÉRO !

www.protectionsecurite-magazine.fr

IPC AI RÉPONDENT À DIVERSES EXIGENCES

Une série complète d'IPC AI, basée sur un algorithme puissant d'apprentissage, permet diverses applications.

Reconnaissance faciale

Masquage de confidentialité

SMD

Protection périmétrique

Metadonnées

- Les séries Ultra-AI avec leur chipset amélioré, englobant la structuration vidéo, la reconnaissance faciale et la protection de la vie privée, a été conçue pour les projets complexes.
- Les séries Pro-AI prennent en charge la capture des visages, le comptage de personnes et les métadonnées vidéo, ainsi que la vigilance périmétrique pour le marché des petites et moyennes entreprises.
- Les séries Value-AI avec leur protection périmétrique et leur solution SMD plus conviennent aux plus petits marchés.

IPC-HFW5442E-Z4E

IPC-HFW5442T-AS-LED

IPC-HFW5541T-AS-PV

IPC-HDBW7442H-ZFR

IPC-HFW7442H-ZFR

Dahua Technology France
49 rue Auguste Perret, 94000 Créteil France
01 48 53 70 53
sales.france@dahuatech.com / support.france@dahuatech.com
http://www.dahuasecurity.com/fr

CAMÉRAS IP

Un marché aux belles perspectives

Le marché mondial des caméras IP devrait atteindre une valeur marchande de 20 milliards de dollars d'ici 2025. Contre 8 milliards de dollars en 2018.

© DR

Tels sont les chiffres extraits d'une récente enquête publiée par Global Market Insights. À en croire cette étude, le marché des caméras IP devrait donc connaître une croissance substantielle de 14 % d'ici 2025, avec plus de 100 millions de caméras produites dans le monde.

Ces perspectives qui vont réjouirent tous les acteurs de la vidéosurveillance, ont plusieurs raisons. Tout d'abord, l'explosion des technologies intégrées aux caméras IP stimulent évidemment la croissance sur des marchés toujours plus demandeurs comme les transports et les infrastructures urbaines.

Par ailleurs, les besoins nationaux de certains pays comme l'Inde ou la Chine – dans lesquels les autorités consomment toujours plus de caméras réseaux pour leurs besoins de sécurité et de surveillance – soutiennent la demande. Un chiffre illustre ces besoins : à elle seule, la Chine abrite environ 200 millions de caméras. Et en déploie toujours plus. L'Inde participe également au mouvement et va encore plus avoir besoin de caméras réseau puisque les autorités y déploient un des plus vastes programmes de reconnaissance faciale. Ce ne sont pas moins de 280 000 caméras qui devraient être installées, dans les années à venir, dans la mégapole de Delhi… dont 140 000 installées en 2019.

Croissance de l'IR

Côté technologie, l'infrarouge devrait connaître de beaux jours. Ce type de caméras représenterait aujourd'hui environ 30 % du marché mondial des caméras IP. Et leur capacité à voir dans des conditions de faible luminosité ou la nuit va encore soutenir le marché car les autorités publiques et les États sont de plus en plus friands de ces technologies pour sécuriser l'espace urbain. Certains secteurs d'activités sont aussi particulièrement demandeurs en caméras IP. Ceux de la banque, de la finance… se tournent de plus en plus vers des solutions de caméras IP centralisées pour gérer les données générées par les caméras.

Selon Global Market Insight, l'Amérique du Nord reste un marché dominant pour l'industrie des caméras IP en 2018, avec une part de marché de 35 %, et les tendances vers la numérisation et l'industrie numérique offrent des opportunités importantes. Par ailleurs, aux États-Unis, l'expansion et l'automatisation des points de vente au détail appartenant à des leaders de l'industrie comme Wal-Mart, Costco Corporation et Kroger Company constituent des opportunités de croissance notable du marché.

Toujours plus de caméras…

Selon les prévisions de l'ONU, les zones urbaines abriteront 68 % de la population mondiale d'ici 2050, contre 55 % aujourd'hui. Pour assurer la sécurité et gérer ces zones urbaines toujours plus importantes, il faudra des réseaux toujours plus grands, où les caméras IP joueront un rôle important.

14 %

C'est le taux de croissance annoncé du marché mondial de caméras IP d'ici 2025.

SÉCURITÉ ÉLECTRONIQUE

Securitas reprend Cezzam

Avec cette opération, Securitas Technologies renforce sa présence géographique en Île-de-France et en Normandie où Cezzam est particulièrement actif.

© Getty images

Le spécialiste de la sécurité électronique Securitas Technologies a donc repris trois fonds de commerce de Cezzam, incluant des activités d'installation, de maintenance et de SAV de systèmes de sécurité électronique. *« Les fonds de commerce Cezzam concernés par cette acquisition comptent 36 collaborateurs, et ont réalisé un chiffre d'affaires de 5,7 millions d'euros à fin juin 2019,* précise Gilles Bonnefoy, directeur de Securitas Technologie France. *Grâce à cette opération, nous affichons pour l'année 2019, une croissance de 10 % de notre CA, qui s'établit à 50 millions d'euros. »* Cezzam est bien implanté dans le nord de la France (siège à Beauvais) et à Rouen. Ce qui permet à Securitas de profiter de cette présence pour renforcer la sienne dans ces régions. *« Le secteur de l'Île-de-France se développe beaucoup. Les sièges sociaux y sont nombreux et il nous fallait accroître notre présence dans cette région pour profiter des possibilités de cross selling avec Securias Surveillance. La proximité de Beauvais avec l'Île-de-France nous permet donc d'être encore plus présent dans la région. »*

Associer humain et technologies

Cezzam est un intégrateur complet, qui maîtrise l'intrusion, le contrôle d'accès et la vidéosurveillance. *« Cette société connaît bien les problématiques complexes en matière de systèmes de sécurité électronique,* ajoute Gilles Bonnefoy. *Et ses compétences et expertises correspondent parfaitement à notre volonté d'intégrer de la technologie à notre offre de services et de prestations. Par ailleurs, Cezzam est très bien implanté chez quelques grands comptes dont nous n'étions pas encore partenaires… »*
À noter que le dirigeant de Cezzam, Philippe Hubeau, devient directeur régional de la région Nord-Est (Paris, Strasbourg, Lille auxquelles s'ajoutent Rouen, Amiens et Beauvais). Cette direction régionale est ainsi la plus importante de Securitas Technologies avec un chiffre d'affaires de 13 millions d'euros.

© DR

« Cette acquisition a pour objectif de renforcer les équipes techniques, commerciales et administratives de la région Nord-Est de Securitas Technologies, sur un périmètre couvrant Paris, la Normandie et la Picardie. Notre ambition est de continuer à progresser dans nos savoir-faire techniques. »

GILLES BONNEFOY, DIRECTEUR SECURITAS TECHNOLOGIES FRANCE

© DR

SERVICES DE SÉCURITÉ ALLIED UNIVERSAL ET SOS SECURITY FUSIONNENT

Allied Universal, société de sécurité filiale du Français Wendel, et SOS Security viennent d'annoncer leur fusion. Fondée en 1969, la société SOS Security apporte à Allied Universal son savoir-faire en matière de services de sécurité. Elle dispose de bureaux dans cinq pays et emploie 15 000 salariés qui fournissent des services de sécurité, de sûreté, de protection rapprochée, de renseignement et de conseil dans le monde entier.
L'an dernier, elle a affecté des agents à plus de 2 000 missions dans plus de 100 pays à travers sa filiale AS Solution.
La fusion entre Allied Universal et SOS Security donne naissance à un prestataire de services qui se différencie dans le secteur mondial de la sécurité par :
un effectif combiné de plus de 230 000 professionnels de la sécurité ; les capacités de SOS Security sur les marchés internationaux et dans le domaine de l'analyse du renseignement ; des solutions technologiques de pointe, intégrées et complètes d'Allied Universal ; une expertise en gestion des risques axée sur le conseil en sécurité, les enquêtes, la protection des personnes et les réactions à adopter face à des menaces, des catastrophes ou des situations d'urgence ; des services de gestion des mouvements de foule…

SÉCURITÉ PHYSIQUE ET ÉLECTRONIQUE

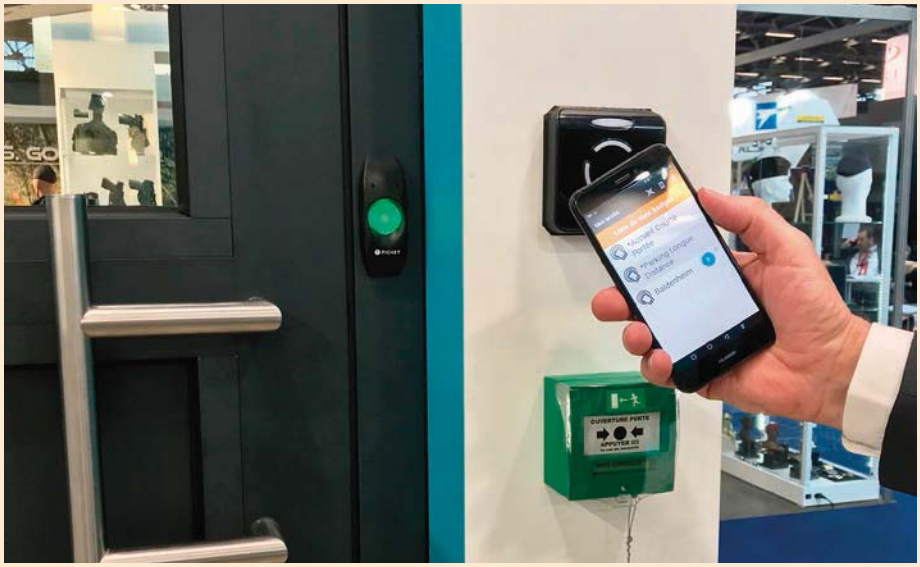
Fichet Group s'inscrit dans le continuum sécurité

Il y a un an, Gunnebo cédait ses filiales françaises, belges et luxembourgeoises au fond d'investissement Open Gate Capital. Fichet Group, né de cette cession, maîtrise aujourd'hui à 100 % sa filière de production avec deux usines en France.

« *La création de ce groupe nous a permis de renforcer le développement et la commercialisation de nos solutions de sûreté pour adresser nos marchés – dont le haut risque – avec une offre parfaitement cohérente, qui s'inscrit pleinement dans le continuum sécurité*, explique Jean-Charles Proskuryn, Strategic business developer chez Fichet Group. *Notre objectif est de concevoir des dispositifs de protection graduels fondés sur la complémentarité des moyens afin de protéger les personnes ainsi que les biens matériels et immatériels de nos clients.* » L'offre de Fichet va donc aujourd'hui de la protection périphérique des sites jusqu'à la défense des zones les plus sensibles en passant par la protection périmétrique des bâtiments. Elle associe des éléments de sécurité passive (menuiseries de sûreté multirésistantes, coffres-forts, etc.) et de sécurité active pour protéger les infrastructures contre les attaques physiques et cyber. « *Notre offre s'adresse entre autres aux sites à hauts risques, aux OIV, aux institutions régaliennes...*, poursuit Jean-Charles Proskuryn. *Et sur ces marchés, être français est un véritable atout en matière de souveraineté technologique et informationnelle.* »

Une menace protéiforme

Les organisations et entreprises doivent aujourd'hui faire face à des menaces qui n'ont plus grand-chose à voir avec celles qu'elles devaient affronter il y a encore quelques années. Ce que confirme Jean-Charles Proskuryn : « *Les entreprises et organisations doivent aujourd'hui s'équiper avec des solutions qui les protègent contre des attaques de plus en plus virulentes et protéiformes dont le risque cyber n'est pas le moindre. C'est pour cela que la double qualification Anssi que nous avons obtenue pour notre système de contrôle d'accès SMI Server est un réel atout. Ceci nous oblige à nous maintenir dans un process d'amélioration continu pour faire évoluer nos systèmes et respecter sur le long terme les critères de confiance définis par l'Anssi.* »



© DR

© DR

2 QUESTIONS À Jean-Charles Proskuryn,

DIRECTEUR BUSINESS DÉVELOPPEMENT CHEZ FICHET GROUP

Il y a maintenant plus d'un an que Fichet Group a été créé. Comment se porte le groupe ?
Nos résultats sont en croissance. Nous avons réalisé 125 millions d'euros de CA l'année dernière et avons pour objectif d'atteindre 128 millions cette année. Nous employons aujourd'hui 850 personnes dont 37 dédiées à la R&D, avons 16 agences en Europe à partir desquelles nos 250 experts et techniciens accompagnent nos clients et partenaires sur le territoire national.

Fichet Group veut clairement s'inscrire dans le continuum sécurité. Par quoi cela passe-t-il ?
Il faut répondre aux attentes des clients de manière pertinente et cohérente. Pour cela, il faut leur proposer des solutions faciles d'utilisation, plug & play et homogènes. C'est-à-dire qui leur permettent de faire converger sécurité électronique (vidéo, intrusion et contrôle d'accès) et physique. Notre objectif est de garantir à nos clients la disponibilité, l'intégrité et la confidentialité de leur chaîne de sûreté.

INCENDIE

Un marché soutenu par la réglementation mais...

Après la croissance des années 2014-2015, le marché français de la sécurité incendie a reculé en 2016. Pour se stabiliser en 2019. Un marché soutenu par la réglementation qui encadre la maintenance et la vérification des installations.

Tels sont quelques-uns des chiffres extraits d'une récente étude publiée par Xerfi-Precepta* qui estime ce marché à environ 3,2 milliards d'euros répartis entre l'extinction (pour environ 40 %), la détection (autour de 30 %), le compartimentage-désenfumage (quelque 20 %) et les véhicules de lutte contre l'incendie (environ 8 %). Et à l'avenir, les évolutions réglementaires (lois Elan et Essoc notamment) seront l'un des moteurs du marché.

Porté par les achats de renouvellement, ce marché conserve une certaine attractivité grâce à la récurrence des revenus provenant des contrats de maintenance. *« L'activité est en effet soutenue par des mesures réglementaires qui encadrent l'installation, la maintenance et la vérification des équipements, en particulier pour les établissements recevant du public (ERP). En outre, les assureurs jouent activement leur rôle de prescripteurs auprès des entreprises et des particuliers »*, explique Nicolas Le Corre, chargé d'études senior chez Xerfi-Precepta. Avant d'ajouter un bémol : *« Toutefois, le repli des autorisations de mises en chantier de logements [...] affectera en particulier l'activité des segments de la détection pour les entreprises ainsi que du désenfumage et du compartimentage d'ici 2022 tandis que celles de la détection pour les particuliers et de véhicules anti-incendie devraient en profiter. »*

Un leader américain et des Français bien placés

Selon Xerfi-Precepta, à travers sa division Chubb, le géant américain UTC occupe ainsi une position de leader sur le marché hexagonal. Johnson Controls est également un acteur de poids. Tout comme des fabricants de matériel électrique comme Siemens, Legrand ou Hager sur certains segments.

Quant aux spécialistes français, ils sont bien placés dans leur domaine respectif. *« Desautel, Eurofeu et Andrieu figurent ainsi parmi les principaux fabricants d'extincteurs en France alors que DEF est l'un des leaders de la détection »*, souligne Nicolas Le Corre.

© Getty images

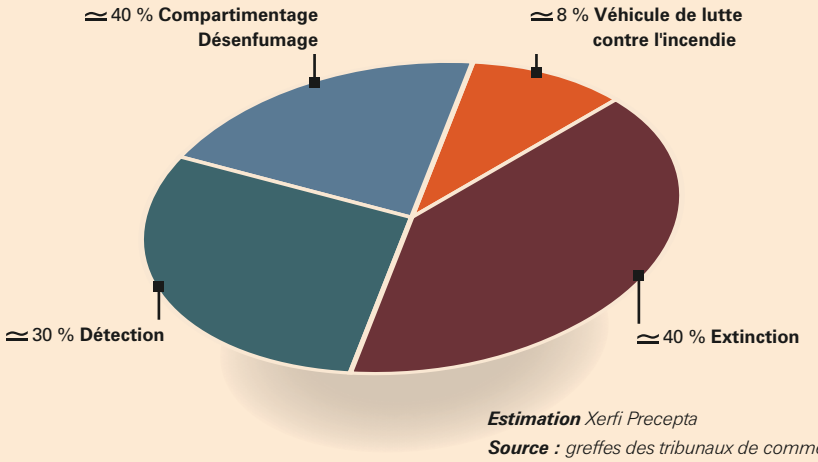
Nouvelles technologies

L'arrivée des robots et des drones se précise dans le secteur. Dans ce contexte, les opérateurs historiques multiplient les initiatives. Le fabricant de véhicules anti-incendie Sides a ainsi noué un partenariat technique et commercial avec Sharks Robotics, fournisseur de robots d'assistance et d'extinction. Car robots et drones pourraient bel et bien s'imposer demain comme des équipements incontournables en matière de sécurité.

**Le marché de la sécurité incendie à l'horizon 2022 - Stratégies d'intégration et de consolidation, évolutions législatives, innovations technologiques : quelles perspectives pour les acteurs ?*

LA SÉCURITÉ INCENDIE : UN MARCHÉ DE 3,2 MD€ EN FRANCE

Unité : *part en % de marché en 2018*



Estimation *Xerfi Precepta*
Source : *greffes des tribunaux de commerce*

VMS

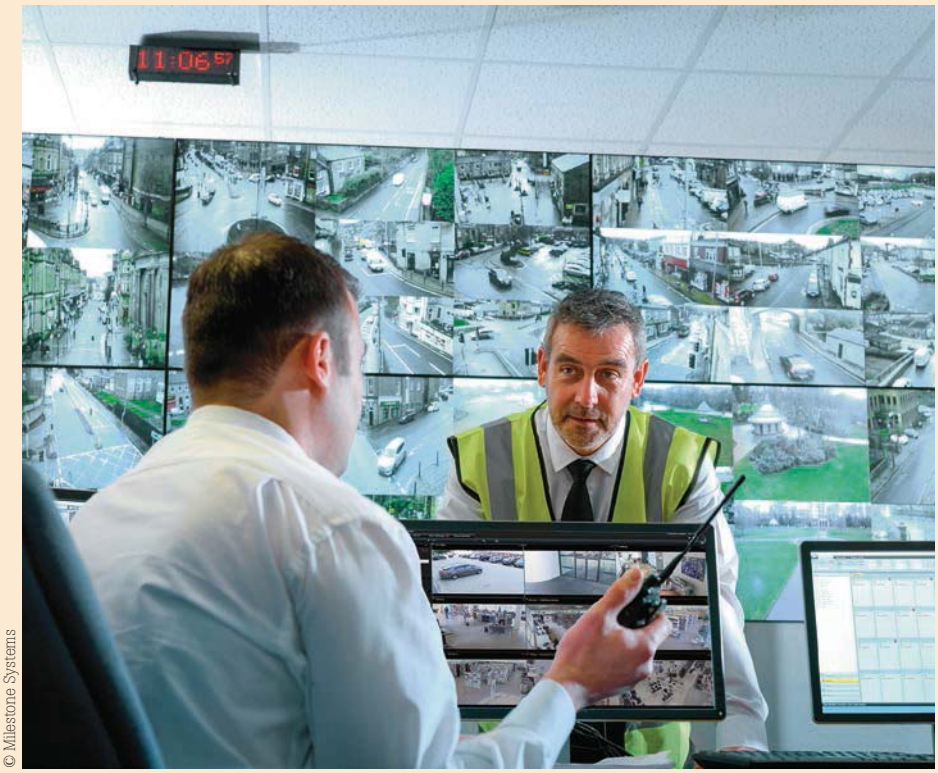
Belle année 2019 pour Milestone Systems

Avec une croissance record, Milestone Systems France a conclu l'année 2019 en beauté. Porté par de nouveaux marchés et le besoin en outils ouverts, Milestone peut envisager l'avenir sereinement.

« *Le bilan 2019 de Milestone Systems en France est plus que positif. Notre chiffre d'affaires a connu une augmentation de 20 % par rapport à 2018. Ce qui est un très bon résultat puisque dans une récente étude IHS Market prévoyait, pour le marché des VMS, une croissance comprise entre 4 et 5 %* », se réjouit Rémy Deutschler, directeur général de Milestone Systems France. Comment expliquer cette forte croissance ? Le directeur général poursuit : « *Elle trouve son origine dans la remise à niveau de nombreuses installations chez nos clients. Ils veulent sortir d'une logique propriétaire, fermée. Ils recherchent donc des outils ouverts. Ce qu'est réellement l'Open Platform de Milestone. Lors d'une remise à niveau d'une installation de sécurité, elle permet de choisir en toute liberté les systèmes et outils qu'on souhaite y intégrer.* »

Des marchés porteurs

Outre le besoin en solutions ouvertes, l'activité de Milestone est aussi portée par des marchés particulièrement demandeurs et pour lesquels le spécialiste des VMS a décidé de concentrer ses efforts. « *Dans le transport, le retail, la logistique… nos solutions suscitent un grand intérêt,* poursuit Rémy Deutschler. *Elles sont ouvertes et permettent de créer un écosystème de la sécurité dans lequel il est facile de venir intégrer tel ou tel outil, telle ou telle solution.* » Avant de conclure : « *Mais au-delà de cette capacité à l'ouverture, nous sommes aussi capables de répondre à de nouveaux besoins. Grâce à nos solutions, les utilisateurs peuvent analyser les données pour faire autre chose que de la sécurité. Dans le retail, par exemple, un VMS bien conçu facilitera l'exploitation des données à des fins marketing. Il devient un vrai outil d'aide à la vente, à l'optimisation de l'expérience du client.* »



© Milestone Systems

© DR

2 QUESTIONS À Rémy Deutschler,

DIRECTEUR GÉNÉRAL DE MILESTONE SYSTEMS FRANCE

À l'heure où les installations de sécurité sont de plus en plus complexes et composées d'outils divers, le VMS n'est-il pas devenu le cœur d'une installation ?

Le VMS est aujourd'hui l'outil indispensable quand on veut exploiter au mieux son système de vidéosurveillance. Mais il permet aussi d'aller au-delà de ce simple management de la vidéo. Chez Milestone, nos VMS associés à XProtect permettent de s'engager dans ce que nous appelons « Beyond Security », c'est-à-dire mettre les données collectées et analyser au service d'autres applications : marketing, gestion et contrôle des flux de marchandises… C'est ce qui porte notre activité sur les marchés du retail et de la logistique.

Vous pouvez vous appuyer sur un réseau solide de distributeurs reconnus. Pensez-vous le densifier ?

Nous collaborons actuellement avec sept partenaires distributeurs : Noemis, Axone, Tracor, ADI, CCF, Anixter et EET, connus et reconnus. Et ce réseau fonctionne très bien. Mais, toujours dans l'optique de nous rapprocher de marchés qui tendent de plus en plus vers l'IT, il n'est pas exclu que nous ne soyons pas, dans les mois qui viennent, intéressés par des partenariats avec un ou des distributeurs hyperspécialisés en IT qui nous permettraient d'adresser des marchés de niche…

ENTREPRISES DE SÉCURITÉ

Anticip acquiert Risk&Co

En reprenant Risk&Co, Anticip donne non seulement naissance au numéro 1 français des entreprises de services de sécurité et de défense, mais aussi à un des leaders européens du marché.

Depuis plusieurs mois, le monde des entreprises de services de sécurité et défense est agité par des rachats et rapprochements. Et les Français sont très actifs. Ainsi, en juin dernier, Anticip, un des leaders français de la sécurité et sûreté privée fondée par l'ancien du GIGN, Cyrille Peguilhan, et Richard Terzan, ex-responsable des risques spéciaux de la Sofema, s'alliait à CEIS, cabinet spécialisé dans le conseil en intelligence stratégique. Et on parlait déjà d'une possible acquisition de Risk&Co qui venait de rejeter l'offre d'Amarante.

En ce qui concerne Risk&Co, c'est désormais chose faite puisque Anticip a annoncé, à l'occasion du dernier salon Milipol, le rachat de Risk&Co.

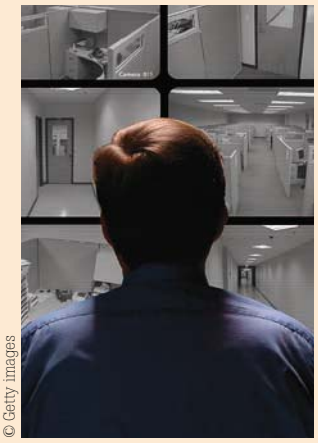
Au cours du premier semestre 2019, les actionnaires et les dirigeants des deux sociétés avaient entamé des discussions autour d'un rapprochement capitalistique. Depuis le 18 novembre dernier, le principe et les modalités du rapprochement envisagé, qui verra Anticip acquerir le contrôle direct de Risk&Co SA, ont été arrêtés. Avec cette opération, le Groupe Risk&Co achève sa transformation, débutée en juillet 2017, sous la présidence de Nathalie Felines. Après s'être recentré sur son cœur de métier (le conseil et l'ingénierie) en cédant des activités non cœur comme la vente d'équipements aux États, le Groupe Risk&Co a renforcé sa position en redéfinissant son offre et sa stratégie commerciale en acquérant de nouveaux clients de renom.

Un leader européen

À elles deux, Anticip et Risk&Co comptent d'ores et déjà des filiales en Afrique du Sud, aux Émirats arabes unis et au Nigéria, et peuvent s'appuyer sur les solutions technologiques de pointe qui ont fait la renommée d'Anticip, tant dans la conduite des opérations en zones à risques que dans le domaine du travel risk management. Ainsi rapprochées, elles deviennent non seulement le leader d'un marché français en pleine recomposition mais surtout elles concrétisent leur ambition de devenir la première entreprise de services de sécurité et de défense (ESSD) de dimension européenne.

© Risk&Co

Risk&Co est un spécialiste de la gestion des risques à l'étranger.



© Getty images

TÉLÉSURVEILLANCE

BRINK'S ET SOTEL NÉGOCIENT

Vers une cession de la filiale télésurveillance de Brink's ? Il semblerait que ce soit le cas puisque Brink's a ouvert des négociations exclusives avec le groupe Sotel pour la cession de Brink's Téléservices, filiale du groupe Brink's spécialisée dans les activités de télésurveillance professionnelle. Brink's Téléservices réalise un chiffre d'affaires de 4,7 millions d'euros en 2018 et emploie 41 salariés sur deux stations de télésurveillance (Paris et Toulouse). Brink's entend ainsi finaliser sa stratégie de recentrage sur son cœur de métier et confier, à l'un des acteurs majeurs du marché, la télésurveillance de son réseau d'agences et de sa flotte de véhicules. Sotel, chiffre d'affaires Groupe de 16 millions d'euros en 2018, confirmerait ainsi son ambition de développement après les acquisitions récentes de SCS et AG Veille en visant le renforcement de sa position sur ses marchés stratégiques : télésurveillance, installation de systèmes d'alarme, interventions de sécurité et formation.

BIG DATA

Deveryware, le Français qui monte

Créée en 2003, le Français Deveryware est devenu un des experts européens des technologies d'investigation et des services pour la sécurité globale, la sécurité des États, des entreprises et des populations, grâce aux technologies numériques et à l'intelligence artificielle.

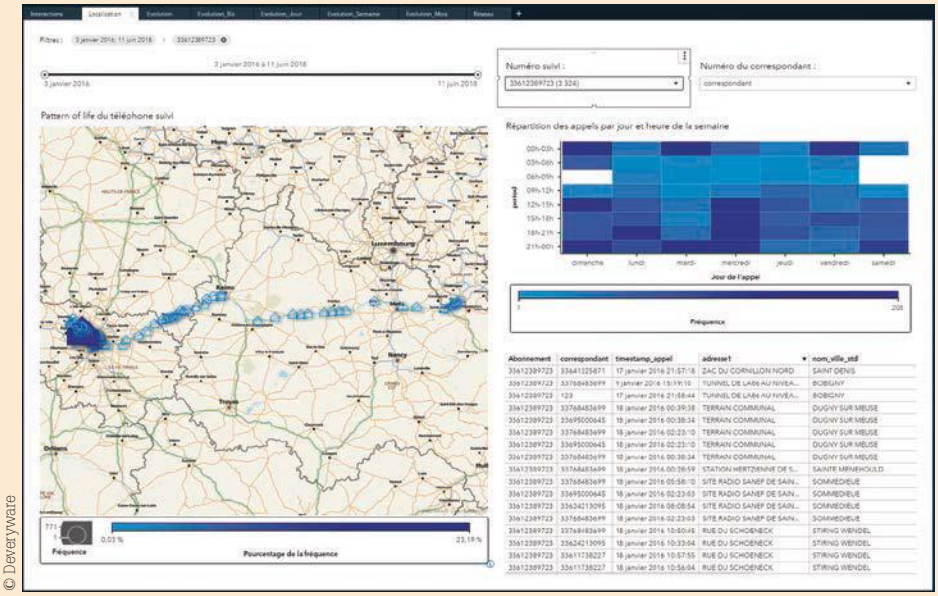
« *Grâce aux nouvelles technologies et à l'arrivée de l'intelligence artificielle (IA) dans nos métiers, nous pouvons aujourd'hui concevoir, développer et commercialiser une offre de solutions B2G (gouvernements/administrations) et B2B, et proposer aux utilisateurs finaux, publics comme privés, des outils pour les accompagner et les aider dans leurs missions stratégiques de sécurité* », explique Alain Vernadat, directeur général de Deveryware. Avant de poursuivre : « *Si aujourd'hui, nous sommes assez loin de notre cœur de métier originel – des solutions de géolocalisation temps réel en mode Saas – c'est en partie grâce à nos opérations de croissance externes qui nous ont permis de diversifier nos savoir-faire et expertises et apporter de la valeur ajoutée à nos clients dans les enquêtes, par exemple pour le monde judiciaire ou pour la sécurité/sûreté, qu'il s'agisse des États ou des entreprises.* »

Les acquisitions évoquées par Alain Vernadat sont celles de trois acteurs réputés : OAK Branch et Resiliency (respectivement en juillet et septembre 2018) et TracIP (avril de l'année dernière).

Trois spécialistes

OAK Branch est un spécialiste français de l'analyse big data pour les métiers du renseignement et de l'investigation judiciaire. Resiliency, quant à elle, propose, depuis plus de dix ans, aux collectivités et aux entreprises des prestations d'audit, de conseils, de formations *in situ* et numérique sur la préparation et la gestion/communication des situations d'exceptions ou sensibles. Enfin, TracIP est le premier laboratoire d'expertise judiciaire français et le spécialiste du traitement des données numériques critiques.

« *Aujourd'hui, grâce à notre savoir-faire propre et ceux que nous ont apporté ces trois sociétés, nous sommes capables de proposer aux utilisateurs finaux une large gamme d'outils et de solutions qui permettent de récupérer des données, de les traiter et de les analyser afin d'automatiser certaines tâches complexes,* conclut le directeur général de Deveryware.



© Deveryware

© DR

2 QUESTIONS À Alain Vernadat,

DIRECTEUR GÉNÉRAL DE DEVERYWARE

Pouvez-vous nous présenter rapidement l'offre de Deveryware ?

Nos solutions associent géolocalisation, big data et forensic (l'expertise judiciaire numérique) afin de proposer aux forces de police françaises des solutions puissantes et complètes pour collecter et analyser plus de données (localisation, traces numériques, etc.) afin d'accélérer et de faciliter leurs enquêtes.
De nouvelles possibilités illustrées notamment à travers la fonctionnalité d'analyse des fadettes lancée cette année et qui complète l'éventail de données exploitées par les solutions Deveryware (DeveryLoc/DeveryLight). Ou encore notre plateforme clés en main de géolocalisation pour la sécurité intérieure, déployable sur tout cloud souverain et entièrement administrable par le client.

Nous sommes début 2020. Quel bilan faites-vous de l'activité de Deveryware au cours de 2019 ? Quels sont vos objectifs ?

Deveryware se porte bien.
Et nos récentes acquisitions ont encore permis de renforcer notre présence sur nos marchés. Nous avons réalisé, en 2019, un chiffre d'affaires de 30 millions d'euros. Mais nous ne comptons pas en rester là. Notre objectif est clairement de doubler la taille de l'entreprise d'ici 2024. Cela passera évidemment par des innovations et de la R&D à laquelle nous consacrons déjà 10 % de notre CA, des opérations de croissance externe et le renforcement de notre présence à l'international.

INTRUSION

Changement d'actionnariat chez France Infra Rouge

Il y a quelques mois, Jean-Luc Lecointe, le fondateur de France Infra Rouge, a passé la main et confié la destinée de FIR à Éric Le Corre, Olivier Héridel et Vincent Chéret. Tous trois désormais actionnaires du spécialiste français des caméras infrarouges et de l'imagerie thermique.

« *Notre volonté, avec mes coactionnaires, est de garantir que le savoir-faire reconnu de France Infra Rouge reste le même,* explique d'emblée Éric Le Corre, son président. *Aujourd'hui, nous sommes clairement identifiés comme le distributeur français de solutions d'imagerie thermique et de caméras infrarouges comme celles de Hikvision ou de Flir, dont nous sommes le principal distributeur sur le marché français. Et nous entendons bien le rester.* »
FIR emploie 14 personnes et réalise un chiffre d'affaires d'environ 4 millions d'euros. « *Notre volonté est clairement d'être présents sur tous les marchés de l'infrarouge car les caméras IR sont de plus en plus utilisées dans des applications allant de la déperdition d'énergie dans les bâtiments à la mesure de température dans les process industriels, en passant par les applications médicales et, évidemment, la lutte contre l'intrusion où les caméras IR permettent de voir, quel que soit le temps, de jour comme de nuit* », poursuit Éric le Corre.

Un spécialiste des audits

Autre corde à l'arc de FIR : les audits. En effet, avant tout déploiement de solutions IR, il est bon de s'assurer que les caméras vont bien voir ce qu'elles doivent voir. Et donc qu'elles sont bien positionnées. Ici, FIR peut vous aider. « *En effet, après avoir réalisé une étude préalable du site, de ses contraintes, et analyser ses risques, pour vous choisir la solution technique la plus adaptée, nous pouvons, grâce à un quad doté d'un mât téléscopique avec différentes caméras, vérifier le pré-positionnement de vos caméras pour s'assurer qu'elles verront bien ce qu'elles sont supposées voir* », conclut Éric Le Corre.

© France Infra Rouge

© DR

2 QUESTIONS À Éric Le Corre,

DIRECTEUR GÉNÉRAL DE FRANCE INFRA ROUGE

Quels sont les secteurs les plus porteurs actuellement pour France Infra Rouge ? Ceux qu'il faudrait développer ?
Il est patent que la lutte contre l'intrusion est un des marchés les plus dynamiques actuellement. Les technologies y sont maîtrisées et le coût des caméras est bien inférieur à ce qu'il été il y a encore quelques années. Ce qui permet à de nombreux sites, et non plus uniquement des sites particulièrement sensibles, de s'équiper. D'un autre côté, la détection précoce de départ de feu, avec possibilité d'extinction automatique est aussi un marché porteur. Et les solutions que proposent désormais FIR répondent à ces besoins spécifiques.

D'ailleurs, à ce sujet, vous proposez deux solutions particulièrement innovantes : Pyrosmart et VigiFIRe. Pouvez-vous nous les présenter ?
Pyrosmart surveille et scanne en continu une zone sur 360°, à l'aide de deux caméras associées, une thermique IR qui mesure la température à distance, et une caméra visible pour la levée de doute. Ces informations, et alarmes préselectionnées, sont poussées vers le centre de surveillance du site. Plus encore, la zone surveillée est cartographiée en 3D, pour, en cas de choix d'extinction automatique, de piloter avec précision le jet d'un canon à eau, et d'attaquer un départ de feu de manière quasiment chirurgicale. VigiFire, plus récemment développé par FIR, permet également une surveillance de détection précoce de départ de feu par caméra thermique, avec une analyse des zones de servitude, pour limiter les fausses alarmes.

© Siemens

CONTRÔLE D'ACCÈS
SIPASS INTEGRATED DE SIEMENS LABELISÉE PAR LE CSF INDUSTRIES DE SÉCURITÉ

Siemens a été labellisé par le Comité stratégique de filière (CSF) « Industries de sécurité » pour sa solution SiPass Integrated, son système de contrôle d'accès.
Afin d'identifier les solutions innovantes qui répondent au mieux à ces enjeux, le CSF Industries de Sécurité a entamé une démarche auprès des industriels et éditeurs de solutions de sûreté. Organisée en deux phases, une présélection sur dossiers et un grand oral, cette initiative a permis de référencer 135 solutions pertinentes labellisées par la filière pour une durée de cinq ans, dont la solution de contrôle d'accès SiPass Integrated de Siemens. Cette dernière est destinée à équiper tous les établissements, du plus critique au plus courant. Modulaire, elle peut en effet s'adapter à l'évolution des besoins de chaque organisation grâce à de nombreuses extensions logicielles, et s'intègre à tous les environnements informatiques. La solution peut également être utilisée en tant que poste de gestion de sûreté, et intégrer un dispositif de contrôle d'accès, de détection d'intrusion et de vidéosurveillance dans un seul et même système.

©Eagle Eye Networks

VIDÉOSURVEILLANCE/ CONTRÔLE D'ACCÈS
ROADSHOW EAGLE EYE NETWORKS

L'équipe Eagle Eye Networks et Brivo prennent de nouveau la route en mars 2020. Et feront étape à Paris le 26 mars 2020.
> www.een.com/een_brivo_roadshow_2020/

VIDÉOSURVEILLANCE
LA THERMIQUE À LA PORTÉE DE TOUS CHEZ HIKVISION

Les caméras thermiques sont de plus en plus utilisées dans la vidéosurveillance. Mais longtemps, leur déploiement pâtissait du coût et de leur complexité à installer et paramétrer. C'est en partant de ce constat que Hikvision a lancé, lors du dernier salon APS, une nouvelle gamme de caméras thermiques Bi-Spectrum, dotées de quatre fonctions importantes et cumulables : la détection périmétrique, la mesure de température, la détection incendie et la détection de fumeurs. Le tout pour un coût inférieur à 600 euros.
« Ces caméras, disponibles en version Bullet (modèle 2617) et en version Turret (modèle 1217), doivent permettre à nos partenaires installateurs d'intégrer dans leur offre des caméras thermiques à un coût très réduit, explique Franck Carette, directeur Europe des produits thermiques chez Hikvision.
Autre atout pour les installateurs : nous avons veillé à ce qu'elles soient simples à installer. »

DRONES

Trois solutions Drone Volt labellisées JO 2024

Trois drones sont labellisés par le CSF. Valable pour cinq ans, ce label vient récompenser la pertinence technologique des solutions de Drone Volt.

Drone Volt et son partenaire Groupe Protec ont annoncé, à l'occasion du dernier salon Milipol, la labellisation « Grands Événements, dont les jeux Olympiques Paris 2024 » de trois solutions drones pour une durée de cinq ans par le CSF (Comité stratégique de la filière) « Industries de sécurité. »
Les solutions labellisées sont :
- L'Hercules 10 v2 filaire : relié à une station d'alimentation, ce drone filaire peut voler et effectuer une surveillance en continu jusqu'à 100 mètres d'altitude en stationnaire.
- L'Hercules 10 v2 : équipé du système Flir Ibac 1 qui permet la détection d'agents biologiques. À noter que l'Hercules 10 peut embarquer aussi d'autres capteurs, dont la caméra Pensar programmable avec des algorithmes d'intelligence artificielle qui permet l'analyse en temps réel d'images ou de données pour une large étendue d'applications telles que les missions de reconnaissance et de détection.
- L'Hercules 2 : un minidrone professionnel de deux kilos entièrement réalisé en impression 3D. Facilement transportable, il est équipé d'une caméra jour et infrarouge pour les missions de surveillance.

Cinq ans et cinq critères
Le label a été attribué pour une durée de cinq ans par un jury d'experts indépendants incluant des experts métiers, des utilisateurs de solutions pour la sécurité de grands événements, ainsi que des experts techniques. Pour chacune des solutions labellisées, le jury s'est appuyé sur cinq critères liés à :
la qualité de l'entreprise, la solution technique, l'innovation, l'impact social et légal, le développement et/ou la production en France.
« Nous sommes fiers de l'obtention, au côté de notre partenaire Groupe Protec, de ce label pour une manifestation aussi prestigieuse que les jeux Olympiques Paris 2024. La synergie entre notre expertise technologique dans les drones et le savoir-faire en sécurisation de sites et d'événements du Groupe Protec aboutit à une véritable reconnaissance de la filière pour nos solutions innovantes », déclare Olivier Gualdoni, PDG de Drone Volt.

© DR

CONTRÔLE D'ACCÈS

Evva célèbre un siècle d'innovations

« Start-up depuis 1919 ». C'est avec ce slogan, pour le moins original, que la société Evva, spécialiste du contrôle d'accès mécanique et électronique vient de célébrer son centenaire d'existence. Et c'est débordant de projets innovants que la start-up entend entamer son deuxième siècle.

Fondée en 1919, à Vienne, Evva, acronyme de « Erfindungs-Versuchs-Verwertungs-Anstalt » qui signifie « Institut d'invention, d'essai et d'application », vient de célébrer en novembre dernier son centenaire. *« Inventer, faire des essais, tester et mettre des produits innovants sur le marché : ce que font aujourd'hui les start-up, c'est ce qu'Evva faisait déjà en 1919 et ce qu'elle continue à faire »*, remarque Michael Kiel directeur des opérations. Une politique d'innovation continue pour ce leader mondial des systèmes de contrôle d'accès mécanique et électronique qui possède actuellement plus de 300 brevets aussi bien dans le domaine des serrures mécaniques que dans celui des serrures électroniques. On lui doit, notamment, le premier cadenas à cylindre en 1937. Pour ne citer que quelques étapes, en 1979, Evva a mis sur le marché le système de MCS, développé avec l'université de Vienne, qui reste un des systèmes de sécurité les plus connus au monde. En 2014, Evva lance les plateformes d'accès électroniques Xesar et AirKey. En 2017, la PME innove avec quatre nouveaux produits : l'Accessdesigner, le 4KS, le système à 4 courbes et le cylindre Hybrid.

Partenariat et développement durable

Mais l'innovation c'est aussi une affaire de collaboration. L'entreprise a noué des partenariats étroits avec l'université technique de Vienne dans le cadre de l'usine pilote 4.0 et pour le développement de cobots. Elle est également associée au centre autrichien pour la production digitale qui se consacre à la réalisation d'une numérisation continue de la commande à la livraison en passant par la production. Production qui, dès 2005, sous l'impulsion de son PDG Stefan Ehrlich-Adám, s'est engagée dans une voie durable et responsable, notamment, en adhérant au concept de Clean Production (réduction de l'emploi des huiles industrielles, production d'électricité par photovoltaïque...). Des initiatives qui ont été récompensées par de nombreux prix environnementaux (Trigos, Klima : aKtiv...) *« Nous considérons cette responsabilité comme une manière d'agir qui correspond aux besoins de la génération actuelle et évite la mise en danger des perspectives et des ressources des générations suivantes. Il s'agit, en effet, non seulement de définir des valeurs, mais de les vivre pleinement, »* a déclaré Stefan Ehrlich-Adám.

© DR

© DR

3 QUESTIONS À Stefan Ehrlich-Adám,

CEO EVVA-GROUP

Après un siècle d'existence, que faut-il retenir d'Evva ?

S'il y avait un seul chiffre à retenir, ce serait 382, qui correspond au nombre de brevets que nous avons déposés. C'est le symbole de notre engagement permanent dans le processus d'innovation. Depuis cinq ans, les investissements en recherche et développement sont de l'ordre de 6 à 8 %, ce qui est considérable pour une entreprise de notre taille et dans notre secteur.

En 2017, vous vous êtes retirés du capital de Salto. N'était-ce pas risqué ?

Nous avions anticipé la perte de chiffre d'affaires. Nous finissons 2019 à 86 millions d'euros de chiffres d'affaires. Cela correspond à l'objectif que nous nous sommes fixé : revenir aux 100 millions d'euros d'ici 2021, en nous positionnant aussi bien sur le secteur mécanique que sur le secteur électronique avec des produits qualitatifs et innovants.

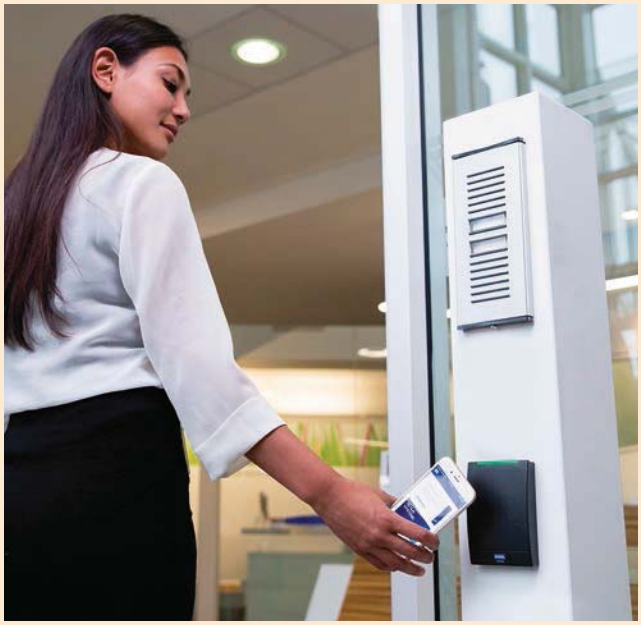
Comment pensez-vous convaincre le marché français ?

« Le compagnon fiable » de nos revendeurs n'est pas un simple slogan, mais un engagement de notre part de loyauté et de fidélité auprès de nos partenaires. Outre des produits performants, nous sommes en mesure de leur proposer ce que nous appelons des profils individualisés qui permet de gérer des sous-systèmes de serrures et clés en toute autonomie. Nous restons des experts de la clé mécanique mais avec l'intégration de solution électronique, nous apportons une vraie valeur ajoutée.

CONTRÔLE D'ACCÈS

Partenariat entre HID Global et VMware

VMware et HID Global veulent, avec ce partenariat, faciliter le déploiement des solutions mobiles mises au service du contrôle d'accès.



© HD

Ce partenariat a pour but de favoriser l'adoption en masse du contrôle des accès via des appareils mobiles pour les espaces physiques et virtuels en combinant HID Mobile Access, module d'ouverture des portes de bâtiments et VMware Workspace One, plateforme d'espace de travail digital intelligente qui permet de gérer toute application sur tout type d'appareil.
Grâce à cette collaboration, les utilisateurs de Workspace One pourront désormais ouvrir les portes de bâtiments à l'aide de leur smartphone en toute sécurité. Une possibilité offerte dans le cadre d'une expérience mobile davantage unifiée qui donne aussi accès à des applications, des ordinateurs, des réseaux et des services autour des données et du cloud.
Les identifiants mobiles HID sont communiqués à Workspace One par le biais de la plateforme de contrôle des accès HID Origo qui, hébergée dans le cloud, dispose d'une suite d'outils et de services autour de l'intégration, de l'habilitation et du développement. Cette suite simplifie la tâche des partenaires de HID et d'un nombre croissant de développeurs et de revendeurs : ils peuvent en effet mettre plus facilement sur le marché des solutions de contrôle des accès mobiles. La plateforme facilite par ailleurs la mise à disposition à distance de nouveaux identifiants mobiles à un utilisateur, en cas de perte ou de changement de son smartphone ou de tout autre appareil mobile.

INNOVATIONS

BIEN CHOISIR VOTRE MATÉRIEL EN 2020 GRÂCE AU E-SALON PSM !

En novembre dernier, vous avez reçu le dernier *Guide d'Achat 2020* de *PSM*.
Mais, grâce à son salon online *PSM*, vous pouvez aussi y retrouver tous les produits dont vous avez besoin, visionner des vidéos, consulter la documentation technique, faire des demandes de devis, contacter directement le fabricant, etc.
Que vous soyez intégrateur, installateur, bureau d'étude, distributeur ou responsable de sécurité… vous allez pouvoir comparer le matériel disponible sur le marché et bien sélectionner vos futurs investissements pour 2020.
Bref, avec ce salon online, vous

© HD

avez un outil complet pour vous permettre de prendre les bonnes décisions d'achat ou d'investissement en matière d'équipements, de produits, de petits matériels ou de services.
> e-salon PSM : http://e-salon-protectionsecurite.fr/

ABONNEZ-VOUS MAINTENANT À PSM !

protectionsecurite-magazine.fr/abonnement

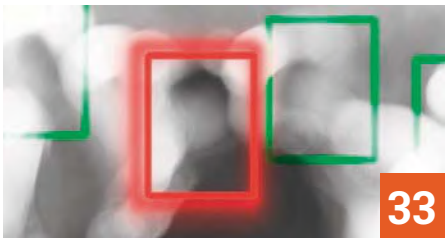
psm
PROTECTION SÉCURITÉ MAGAZINE

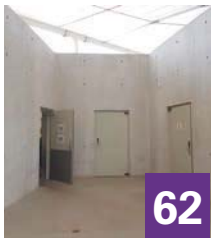
Les solutions pour les professionnels de la Sûreté - Sécurité

psm
Protection Sécurité Magazine

Janvier | Février 2020
n°257

SOMMAIRE





3 **actus prestataires**

16 **actus sûreté**

28 **entretien**
YVAN DE MESMAEKER
Secrétaire général de l'European Corporate Security Association

33 **dossier**
L'IA AU SERVICE DE LA SÉCURITÉ ?

42 **vidéosurveillance**
Moniteurs : une importance sous-estimée

46 **contrôle d'accès**
Reconnaissance faciale et biométrie de la main, une croissance timide

50 **focus**
Serrures : autonomes et numériques

52 **intrusion**
Les obstacles physiques : pas si rustiques que ça

58 **incendie**
Sprinkleurs : une extinction à l'efficacité éprouvée

62 **risque**
Bien protéger les sites vacants

70 **quoi de neuf ?**
Que proposent les fabricants pour la sécurité et la sûreté ?

74 **c'est vous qui le dites !**
DANIÈLE MESLIER, présidente de l'Association nationale des métiers de la sécurité

TPMedia
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

Tous droits de reproduction, textes et illustrations, même partiels, sont soumis à l'accord préalable de la publication.

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
CHEF DE RUBRIQUE: Laurence ALEMANNI
Tél. : +33 (0) 6 49 05 83 73
e-mail : la@protectionsecurite-magazine.fr
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 : 181 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 AZUR DRONES et un encart *Annuaire de la Sécurité Sûreté 2020*

ÉDITO

© DR

Les Français à la pointe de la techno

Si l'intelligence artificielle est de plus en plus à l'ordre du jour dans la sécurité, elle n'en pose pas moins quelques problèmes. Ne serait-ce qu'en matière de fiabilité des bases de données et des applications de reconnaissance faciale. Comme vous pourrez le constater dans le dossier que nous lui consacrons dans ce numéro. Autre constat. Et c'est une bonne surprise. Dans l'IA, la France n'a pas à rougir de ses savoir-faire. De nombreuses entreprises ont conçu et développé des applications basées sur l'IA, particulièrement innovantes.
Pourquoi nous arrêtons-nous à « développé » ? Tout simplement parce qu'à l'inverse de ce qui se fait dans d'autres pays – et nous ne parlons pas de la Chine – les ingénieurs et développeurs français ont beaucoup de mal à expérimenter sur le terrain leurs solutions. C'est fort dommage car, en matière d'IA, cette phase d'expérimentation est primordiale. Il serait donc dommage que, dans les années qui viennent, les pouvoirs publics ne permettent pas, dans un cadre réglementaire précis, d'expérimenter sur le terrain les savoir-faire français. Ne serait-ce que pour lutter à armes égales avec leurs concurrents…

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

VIDÉOSURVEILLANCE

40 % des caméras ont un risque cyber

© Getty images

Une étude réalisée par Genetec révèle que près de quatre caméras de vidéosurveillance sur dix présentent un risque de cybersécurité dû à un micrologiciel obsolète.

Cette étude* montre par ailleurs que jusqu'à 68,4 % des caméras de sécurité d'une entreprise, soit près de sept sur dix, n'ont ainsi pas été mises à jour avec la dernière version disponible de leur micrologiciel.
Lorsqu'on déploie la dernière version d'un micrologiciel, ce n'est pas seulement pour pouvoir profiter de nouvelles fonctionnalités intéressantes, mais également pour bénéficier, dès leur disponibilité, des dernières mesures de protection en matière de cybersécurité – une étape cruciale pour assurer la résilience d'une entreprise face aux cyberattaques.

© DR

« Nos données indiquent que 53,9 des caméras dotées d'un micrologiciel obsolète présentent des vulnérabilités de cybersécurité connues. »

MATHIEU CHEVALIER, LEAD SECURITY ARCHITECT CHEZ GENETEC

Des vulnérabilités de cybersécurité connues

Toujours selon Genetec, près d'une entreprise sur quatre (23 %) n'utilise pas de mots de passe uniques sur ses caméras de sécurité, mais le même mot de passe pour toutes les caméras d'un même fabricant. Il suffit d'une seule caméra compromise pour offrir un point d'accès facile aux pirates informatiques.
Jusqu'à récemment, les caméras IP étaient livrées avec des paramètres de sécurité par défaut, y compris au niveau des informations de connexion administrateur, par ailleurs souvent accessibles au public sur les sites Web des fabricants. La plupart des fabricants de caméras demandent désormais aux utilisateurs de définir de nouveaux mots de passe et identifiants administrateur lors de l'installation. Mais les entreprises, les villes et les institutions gouvernementales disposant d'équipements plus anciens n'ont bien souvent jamais mis à jour leurs mots de passe, compromettant potentiellement les autres données et systèmes critiques qui se trouvent sur leur réseau.

23 %
C'est le pourcentage d'entreprises qui n'utilisent pas de mots de passe uniques sur ses caméras de sécurité.

Une seule caméra suffit...

« Notre étude montre que, malheureusement, l'approche informatique qui consiste à "configurer et oublier" reste répandue, mettant en danger la sécurité de toute une entreprise et la vie privée des individus. Il suffit d'une seule caméra avec un micrologiciel obsolète ou un mot de passe par défaut pour créer une faille dans laquelle un attaquant peut s'engouffrer et compromettre l'ensemble du réseau. Il est essentiel que les entreprises soient aussi proactives dans la mise à jour de leurs systèmes de sécurité physique que dans celle de leurs réseaux informatiques », conclut Mathieu Chevalier, Lead Security Architect chez Genetec. ■

** L'étude a été menée sur un échantillon de 44763 caméras connectées àdes systèmes prenant part au programme facultatif d'amélioration des produits de Genetec.*

RECONNAISSANCE FACIALE

La Cnil lui dit non dans les lycées

Le 17 octobre, la Cnil, saisie par la région Paca, a considéré que ce dispositif concernant des élèves, pour la plupart mineurs, dans le seul but de fluidifier et de sécuriser les accès n'apparaît ni nécessaire ni proportionné pour atteindre ces finalités.

© Getty images

Dans un précédent numéro de *PSM**, nous avions évoqué des tests de la reconnaissance faciale pour sécuriser l'accès à deux lycées dans le sud de la France. Le lycée niçois des Eucalyptus et le lycée Ampère à Marseille attendaient le feu vert de la Cnil pour mettre en place un portique virtuel de contrôle d'accès à leurs établissements par reconnaissance faciale.
Nous connaissons désormais la position de la commission… Pour étayer sa décision, la Cnil explique qu'elle a *« considéré que le dispositif projeté est contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD (Règlement général sur la protection des données) »* et que *« les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge. »*

Des dispositifs intrusifs

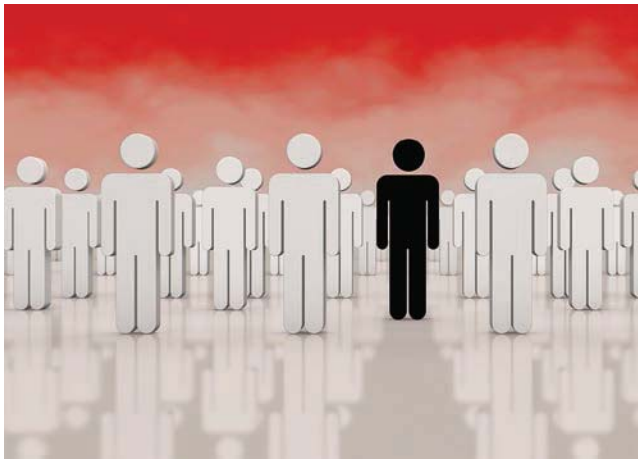
Dans sa décision, la commission rappelle aussi *« que les traitements de données biométriques sont d'une sensibilité particulière, justifiant une protection renforcée des personnes. Notamment, les dispositifs de reconnaissance faciale sont particulièrement intrusifs et présentent des risques majeurs d'atteinte à la vie privée et aux libertés individuelles des personnes concernées. Ils sont par ailleurs de nature à créer un sentiment de surveillance renforcé. »*
Avant d'ajouter : *« Ces risques se trouvent accrus lorsque les dispositifs de reconnaissance faciale sont appliqués à des mineurs qui font l'objet d'une protection particulière dans les textes nationaux et européens. »*
Compte tenu de ces réserves et du fait de l'existence de moyens alternatifs moins intrusifs, comme un contrôle par badge, la Cnil a considéré que le recours à la reconnaissance faciale pour contrôler les accès à un lycée apparaît disproportionné. ■

* *PSM n° 252, mars-avril 2019.*

PRÉVENTION DE LA RADICALISATION

Un guide de l'Uclat

Ce guide, intitulé *Guide de prévention de la radicalisation dans la fonction publique. Quels outils statutaires de prévention et d'action ?* a été élaboré avec le concours de la Direction des libertés publiques et des affaires juridiques, de l'Unité de coordination de la lutte antiterroriste (Uclat), de la Direction générale des collectivités locales et de la Direction générale de l'offre de soins. Il vise à rappeler les moyens d'action pouvant être mobilisés par les administrations ainsi que les procédures à mettre en œuvre face à des agents signalés comme radicalisés. L'enjeu est d'assurer la sécurité et de contribuer à prévenir et lutter contre la radicalisation violente, tout en veillant à faire preuve de mesure et de discernement en vue d'éviter toute attitude pouvant conduire, à l'inverse, à des discriminations. ■



© DR

→ **www.fonction-publique.gouv.fr/files/files/publications/coll_outils_de_la_GRH/guide-prevention-radicalisation.pdf**

CONTRÔLE D'ACCÈS

L'ESTP s'équipe avec une solution autonome

© DR

L'école spéciale des Travaux publics, du bâtiment et de l'industrie (ESTP Paris), créée en 1891, s'équipe depuis deux ans avec des solutions de contrôle d'accès autonome de Simons Voss.

Cet établissement d'enseignement supérieur privé reconnu par l'État dispose de trois campus : Cachan Paris et Troyes, et un futur campus qui verra bientôt le jour à Dijon. Composé de 25 bâtiments disposés sur 7 hectares, le campus Cachan accueille 2 800 élèves par an. La gestion d'un si grand nombre de bâtiments et de portes avec des clés physiques est possible mais peu pratique : soit les gestionnaires se retrouvent avec de grands trousseaux de clés pour ouvrir différentes portes, soit une clé passe-partout est dupliquée et constitue un risque évident pour la sécurité. De plus, le coût de remplacement, la gestion et la maintenance peuvent s'avérer très coûteux.

Pour mieux contrôler l'accès dans ses locaux et aussi faire face à des problèmes d'organigrammes de clés, l'école a opté pour des serrures électroniques Simons Voss. Celles-ci sont installées sur plus de 100 portes (dans quatre bâtiments), principalement celles des bureaux, locaux de stockage, salles de travail, laboratoires d'enseignements et de recherche, ainsi que des salles BIM (Building Information Modeling). Ces dernières contiennent 48 postes informatiques servant à concevoir des projets de construction et d'exploitation de bâtiments.

300 000 manœuvres

L'école a ainsi opté pour la solution 3060 de Simons Vossen, version autonome avec deux produits :

- La plaque-béquille numérique SmartHandle 3062 dont le montage se fait rapidement, sans câblage ni perçage, grâce à sa fonctionnalité SnapIn. Ceci permet de garder les portes existantes intactes. Avec environ six ans d'autonomie, le changement fréquent des piles est évité sur la SmartHandle 3062. Les béquilles intelligentes vont enregistrer jusqu'aux 3000 derniers événements.
- La béquille sur rosace SmartHandle AX, béquille électronique de dernière génération qui est fortement sollicitée pour ses différentes fonctionnalités innovatrices et évolutives grâce auxquelles elle répond aux plus hautes attentes en matière de sécurité. Nouveauté Simons Voss, elle ornera prochainement d'autres portes du campus Cachan car elle dispose, entre autres, d'une autonomie record d'environ 300 000 manœuvres.

Simple d'exploitation, la version autonome du Système 3060 permet la transmission des droits d'accès directement sur le badge qui, lors du premier passage, les transmettra et les enregistrera automatiquement sur les portes.

L'école a remplacé toutes les clés mécaniques par des cartes de type Mifare, déjà utilisées pour accéder au parking et à l'établissement, et sur lesquelles vient se rajouter l'encryptage des droits du personnel pour accéder au bâtiment et à ses salles. ■

2 QUESTIONS À

STÉPHANE GRAS

Responsable sécurité-sûreté et prévention des risques du campus Cachan

© DR

Pourquoi avez-vous choisi les solutions Simons Voss ?
Avec le déploiement des solutions Simons Voss, nous confirmons notre volonté d'augmenter la sécurité sur nos campus et dans les zones sensibles, tout en diminuant l'utilisation des clés mécaniques dont la perte dans la nature nous exposait à une gestion coûteuse et complexe à moyen terme. En utilisant les systèmes de fermeture électronique Simons Voss, on peut non seulement attribuer les badges nominatifs aux utilisateurs mais aussi bloquer les accès en interrogeant directement la serrure en cas de leur perte ou de leur vol. Ceci est une véritable économie de temps et d'argent.

Le déploiement est-il terminé ?
Pas du tout. Notre objectif est d'équiper l'ensemble des campus des systèmes de fermeture Simons Voss afin d'avoir une gestion multisite et multiutilisateur centralisée avec une seule base de données en système réseau en ligne.

CONTINUUM DE SÉCURITÉ

Consultation sur le Livre blanc de la sécurité intérieure

Le ministère de l'Intérieur a lancé sa consultation pour l'élaboration du Livre blanc de la sécurité intérieure. Ce document constituera le document de référence du ministère et définira les objectifs de la politique de sécurité intérieure de la France.

Au cours des prochains mois et jusqu'au début de l'année prochaine, quatre groupes de travail vont ainsi se réunir, réfléchir et consulter largement afin de mener un diagnostic précis et proposer des solutions innovantes pour la sécurité de la France. Ces groupes de travail s'articulent autour des thèmes suivants : l'organisation des services, partenariat et continuum de sécurité, les ressources humaines et matérielles, les technologies. Le groupe 2, Partenariat et continuum de sécurité, dont l'animation a été confiée au préfet Philippe Galli, concerne plus particulièrement la sécurité privée.

Ses objectifs sont :

- Lier des partenariats solides : développer le rôle des acteurs non régaliens, en appui de l'action des forces de sécurité, en veillant à l'interopérabilité de l'ensemble des acteurs et pour permettre aux forces de sécurité intérieure de se concentrer sur leurs missions essentielles.

© Getty images

- Mieux former : accompagner la montée en puissance des polices municipales et des sociétés de sécurité privée.

- Mieux prévenir : assurer une meilleure prise en compte des élus et des collectivités locales au sein des dispositifs partenariaux de sécurité.

- Agir pour la vidéoprotection : construire un cadre juridique adapté pour mieux intégrer l'apport de la vidéoprotection dans les stratégies de sécurité territoriales. ■

INCENDIE

Les lauréats des oscars de la FFMI

Le 20 novembre a eu lieu la remise des oscars de la sécurité incendie par la FFMI. Remis depuis plusieurs années, ces oscars récompensent les meilleures stratégies en matière de sécurité incendie.

Cette année, la FFMI a distingué trois entreprises :

- Firemob, lauréat dans la catégorie « Innovation » La solution Firemob consiste à proposer une solution mobile de détection incendie au moment où les bâtiments sont particulièrement vulnérables, en phase chantier ou lors d'événements ponctuels. L'oscar a été remis à Céleste Dechalus, directrice des opérations chez Firemob.

- Eovi MCD Mutuelle, lauréat dans la catégorie « Prévention incendie ». Eovi MCD Mutuelle a mis en place un ambitieux programme de prévention incendie auprès de l'ensemble de ses salariés : création d'un e-learning, sessions de formation en unité mobile… C'est Caroline Laurent-Billet, responsable hygiène, sécurité, sûreté, qui a reçu l'oscar.

- Informatique CDC (Groupe Caisse des dépôts), lauréat dans la catégorie « Management de la sécurité incendie ». Informatique CDC a été récompensé pour son engagement en matière de gestion du risque incendie en constante évolution, qui ne se limite pas aux seules exigences règlementaires. L'oscar a été remis à Pascal Rayé, consultant sureté et sécurité physique, et à Christophe Cavrot, directeur. ■

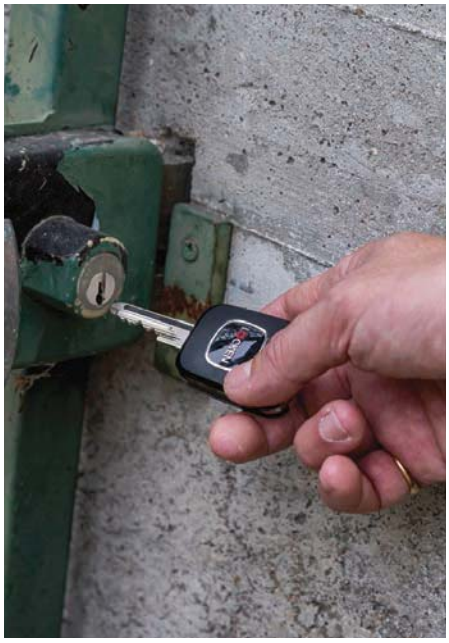
Pascal Rayé (Informatique CDC), Régis Cousin (président FFMI), Céleste Dechalus (Firemob), Caroline Laurent-Billet (Eovi MCD Mutuelle), David Giret (colonel de sapeurs-pompiers professionnels à la DGSCGC).

© DR

CONTRÔLE D'ACCÈS

Enedis opte pour une solution dernier-cri

Enedis cherchait à moderniser la gestion des accès de la moitié des postes sources de son réseau national. L'opérateur a opté pour une clé dernière génération.



© DR

Clos par une enceinte de sécurité avec portail extérieur, les postes sources comprennent plusieurs transformateurs, qui peuvent être situés en extérieur ou sous abri, et un bâtiment technique. Ces dispositifs représentent de nombreux accès qui doivent être sécurisés. Sans une solution performante, la gestion des clés est complexe et l'efficacité opérationnelle diminuée.
Les postes sources sont des sites sensibles, dont l'accès est strictement réglementé. Le risque électrique est permanent, toute intrusion peut avoir des conséquences dramatiques.

1 100 postes sources

C'est la société Locken qui a été choisie pour moderniser la gestion des accès de la moitié des postes sources du réseau national d'Enedis : l'Île-de-France et deux importants ensembles régionaux (Pays de la Loire et Bretagne, Vallée du Rhône, Alpes et Paca). Après une phase de tests, Enedis a opté pour la clé électronique de dernière génération fabriquée par Iseo. Celle-ci permet une ouverture instantanée du cylindre et élimine les risques de faux contacts grâce à une technologie innovante sans contact par induction.
La solution est en cours de déploiement dans la partie ouest de l'Île-de-France où plus de la moitié des postes sources – plus de 25 sur 50 – sont déjà équipés. À l'échelle nationale, le déploiement complet de la solution, soit 1 100 postes sources, devait être terminé fin 2019.
La solution est d'autant plus pertinente que la maintenance des postes sources nécessite l'intervention de nombreux agents. Pour la seule partie ouest de l'Île-de-France, Locken prévoit de fournir 800 clés intelligentes.

Gestion de crise plus fiable

Leurs utilisateurs ne sont pas tous des employés d'Enedis, comme le confirme Maxime Lebœuf, responsable de projets chez Enedis : *« Même si ce sont principalement des personnels d'Enedis qui travaillent sur ces sites, ils doivent être accessibles aussi aux sous-traitants qui assurent des travaux d'extension et de renouvellement mais aussi certaines opérations de maintenance, ainsi qu'aux agents de RTE, gestionnaire du réseau de transport d'électricité, en charge des lignes à très haute tension qui aboutissent aux postes sources. La gestion électronique des accès limite drastiquement le risque d'intrusion lié à l'utilisation des clés mécaniques. »*
Avant d'ajouter : *« Grâce au système Locken, nous pouvons dorénavant autoriser l'accès à nos sous-traitants pendant une période donnée sur une zone définie. Dans la configuration choisie par Enedis, les droits d'accès mémorisés par les clés électroniques doivent être renouvelés chaque jour par l'utilisateur de la clé à travers les dispositifs dédiés. La désactivation d'une clé, par l'intermédiaire du logiciel central de gestion (LSA, Locken Smart Access) est donc effective presque immédiatement. Cela nous procure aussi un outil fiable de gestion de crise »*.

> *« La gestion électronique des accès limite fortement le risque d'intrusion lié aux clés mécaniques. »*
> **MAXIME LEBŒUF, RESPONSABLE DE PROJETS CHEZ ENEDIS**

Une contrainte : des sites dispersés

Chez Enedis, Locken équipe des accès extérieurs, situés souvent dans des lieux isolés, en pleine nature. La clé, porteuse de l'énergie qui déclenche l'ouverture du cylindre, ne suppose aucun câblage des portes. Enedis étudie la possibilité d'élargir l'utilisation de la clé électronique aux parties les plus sensibles des bâtiments techniques, notamment l'accès aux salles de contrôle commande, le véritable cerveau du poste source. Enedis envisage également de remplacer la totalité des cylindres des postes sources afin de limiter les risques liés à la coactivité, qui implique que plusieurs opérations puissent être menées simultanément sur un même poste source. ■

VIDÉOPROTECTION

Bologne améliore son réseau

La ville de Bologne voulait investir dans une solution de vidéoprotection lui permettant de surveiller les douze portes routières d'accès à la ville afin de fournir aux autorités des informations fiables en temps réel sur la mobilité urbaine.

L'objectif était de fournir un outil permettant aux autorités de prendre des mesures de planification stratégique et de redistribuer de manière optimale la circulation sur le réseau routier.
Après de nombreux tests de différentes solutions, il a été décidé d'installer 89 caméras Wisenet fabriquées par Hanwha Techwin. La solution déployée est composée de caméras dédiées au comptage et à la classification des véhicules et de caméras LAPI installées au niveau des portes stratégiques. Ces caméras surveillent les deux sens de circulation pour permettre aux autorités locales d'étudier les flux d'accès à la ville les plus importants et les plus stratégiques.

© DR

65 nouvelles caméras

Vingt-quatre des caméras installées sont des caméras bullet Wisenet XNO-6120R/TD équipées de Traffic Data, une application embarquée, développée en coopération avec Sprinx Technologies, qui facilite la collecte de données statistiques sur les flux de véhicules. En faisant le suivi des véhicules se déplaçant dans le champ de vision d'une caméra, l'application est capable de fournir des informations sur le nombre, la classification et la vitesse moyenne des véhicules.
L'équipement est complété de 41 caméras dômes PTZ IR 23x Wisenet SNP-L6233RH en 2 mégapixels, installées aux principaux croisements de la ville, afin de permettre aux opérateurs de salles de contrôle de zoomer pour voir en détail les incidents. ■

30 - 31 JANVIER 2020

les universités de l'AN2V

• 2 plénières avec des intervenants prestigieux
• 12 ateliers de perfectionnement
• 50 partenaires industriels
• 700 professionnels

Lyon
Espace Tête d'Or

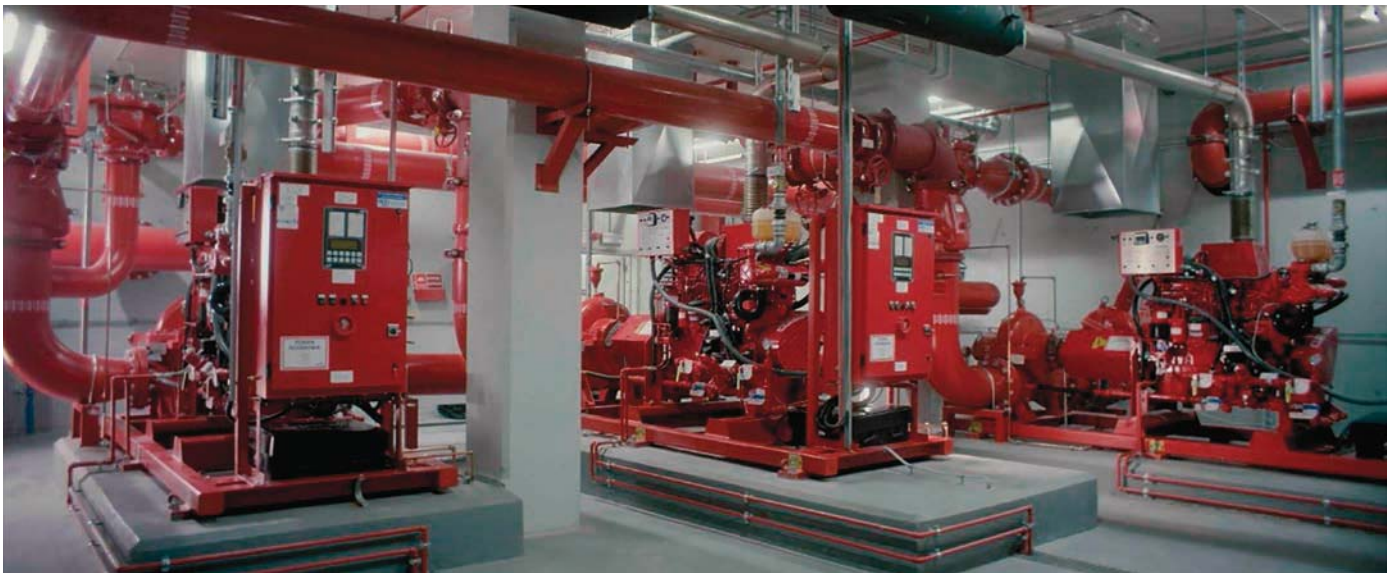
Inscription
www.an2v.org

Renseignements
Rémi Fargette
rf@an2v.org
+33 6 28 45 04 27

AN2V

INCENDIE

Chantier record pour Spie



© Spie

Spie a mené à bien l'implantation d'un dispositif d'extinction d'incendie à mousse chaude dans un entrepôt de près de 70 000 m³ de la société Parys. Il s'agit actuellement d'un des plus volumineux et modernes d'Europe.

Comme Parys, fabricant et distributeur de produits d'entretien automobile, stocke de nombreuses substances inflammables dans l'entrepôt de son client, Spie a opté pour la mise en place d'un dispositif d'extinction à mousse légère et chaude permanent. Les capteurs du dispositif peuvent détecter un incendie en une fraction de seconde et activer ainsi le dispositif dans la foulée. *« Cela signifie qu'un début d'incendie peut être combattu à la vitesse de l'éclair. Trois minutes seulement après la détection de l'incendie, toute la pièce se remplit de mousse, bloquant ainsi l'approvisionnement en oxygène des flammes, que l'incendie ait débuté au sol ou sur les rayonnages,* explique Micha Turek, chef de la division ventes et systèmes de protection incendie de Spie, en Pologne. *Dans la plupart des cas, il n'est même pas nécessaire d'appeler les pompiers. »*
La rapidité du dispositif permet d'obtenir un système de pompage extrêmement puissant équipé de trois pompes à moteur diesel prêtes à déverser plus de 40 000 litres de substance d'extinction par minute. En comparaison, jusqu'à présent, un dispositif de taille normale ne pouvait rejeter qu'environ 7 000 litres par minute.

Mousse assurée, même par fortes chaleurs

Depuis des années, la mousse légère constitue la technique d'extinction standard pour les sapeurs-pompiers et dans de nombreux secteurs industriels, y compris l'industrie chimique et pétrochimique. L'innovation technologique de Spie repose sur l'utilisation d'un dispositif qui, en cas d'incendie, peut également produire de la mousse légère à partir de gaz de combustion chauds d'une température supérieure à 800 °C. Un paramètre qui peut jouer un grand rôle lors d'incendies d'origine liquide. Le développement dynamique des gaz émis entraîne une élévation brusque et rapide de la température et ainsi de la production massive de fumée qui, à son tour, mélangée à l'air du hangar, est utilisée pour la production de mousse. *« Nous avons pu mettre en œuvre ce système grâce à de nombreuses années d'expérience, tant en Pologne que sur les marchés internationaux, et à la grande expertise de nos collaborateurs hautement qualifiés,* conclut Michael Turek. *Un système d'une telle dimension est une première en Pologne. La taille des dispositifs d'extinction à mousse légère du marché est généralement deux fois inférieure tout au plus. »* ■

> *« Avec ce type d'installation, dans la plupart des cas, il n'est même pas nécessaire d'appeler les pompiers. »*
>
> **MICHA TUREK, CHEF DE LA DIVISION VENTES ET SYSTÈMES DE PROTECTION INCENDIE, SPIE POLOGNE**

À RETENIR

Les installations sprinkleurs ont ceci de particulier que leur conformité est liée à la compatibilité du couple installation/activité.
Cela veut dire que le niveau de protection doit être harmonisé avec l'activité.

CADRES DE LA SÉCURITÉ

MBA « Management de la sécurité » de la Gendarmerie nationale

Depuis 2014, la Gendarmerie nationale propose aux cadres supérieurs et dirigeants du public ou du privé le MBA spécialisé « Management de la sécurité » pour se former aux enjeux et missions du manager sécurité.

© DR

«Avec ce MBA, la Gendarmerie nationale souhaitait – et elle était précurseur en la matière – mettre en relation des cadres du public et du privé pour parler de sûreté. Une démarche vraiment en avance, à une époque où on ne parlait pas encore de continuum sécurité, souligne le chef d'escadron Olivier Anceau, chef du département MBAsp. *Tous les ans, ce MBA accueille un tiers d'auditeurs issus de la gendarmerie et deux tiers d'auditeurs externes venus du secteur public (des officiers d'autres armées, des fonctionnaires d'administrations centrales, des cadres d'entreprises publiques) ou du secteur privé.»*

Ouvert à des cadres pouvant justifier d'un niveau d'études équivalent à bac +5 et de cinq ans d'expérience professionnelle, le MBA accueille tous les ans entre 30 et 40 personnes sur le site de l'École militaire à Paris. *«Au cours de cette formation, les auditeurs bénéficient d'enseignements universitaires de haut niveau, de conférences thématiques et de voyages d'étude, complétés par la rédaction puis la soutenance d'un mémoire pro»*, poursuit le commandant Anceau.

Formation certifiée

Le MBA est certifié titre 7 CNCP et Datadock. *«Cette formation en part-time est exigeante et demande un investissement personnel important. Nous faisons d'ailleurs passer un entretien préalable aux candidats pour nous assurer de leur motivation et de la possibilité pour eux de s'investir jusqu'au bout du cursus,* ajoute Olivier Anceau. *De septembre à janvier, ils devront assister à la partie académique et de janvier à juin suivre les formations spécifiques. Et ce, à raison d'une à deux semaines par mois.»*

Bénéficiant de prestigieux partenariats (Paris II, HEC, le Cnam, le CDSE, ASIS International, l'Agora des directeurs sécurité, IESAS, Airbus helicopter, Renault, la Marine nationale, le MTES, etc.) le MBAsp s'adresse au haut encadrement de la sûreté dans les entreprises et les organisations. ■

→ En savoir plus : www.mba-securité-eogn.fr

SÉCURITÉ PRIVÉE

15 entreprises lancent l'OPSE

La sécurité des événements sportifs, culturels, des foires et salons… repose aujourd'hui très largement sur les entreprises de sécurité spécialisées dans l'événementiel. Afin de promouvoir leur savoir-faire, ces entreprises ont décidé de s'unir. L'objectif avoué de l'Organisation des professionnels de la sécurité événementielle (OPSE), qui regroupe donc des PME et ETI françaises spécialisées dans la sécurité des événements, est, outre la promotion de leurs compétences et expertises, de peser dans le débat public.

Leur constat est en effet unanime : la profession, telle qu'ils la pratiquent et telle que celle-ci est reconnue par leurs clients est menacée, compte tenu notamment de la réglementation en vigueur et de ses évolutions inadaptées aux contraintes de nos activités ; de l'intérêt opportuniste, en raison des grands événements à venir, porté au secteur par des acteurs non spécialisés.

L'OPSE veut aussi travailler sur les enjeux fondamentaux du secteur : valorisation du métier, de sa singularité et des compétences de ses acteurs ; réglementation en vigueur et notamment le droit du travail qui ne prévoit aucun statut adapté aux métiers de la sécurité événementielle ; l'environnement concurrentiel, afin de peser face à la concurrence d'acteurs généralistes de la sécurité… ■

SÉCURITÉ PORTUAIRE

Première mondiale en France

Eamus Cork Security a choisi le drone autonome d'Azur Drones, intégré au système de gestion vidéo de Genetec, pour protéger une installation portuaire du grand port maritime de Dunkerque.

Eamus Cork Security, spécialiste de la sûreté portuaire, protège depuis juillet 2019 une installation portuaire du grand port maritime de Dunkerque avec le drone autonome Skeyetech d'Azur Drones couplé au système de gestion vidéo Security Center Omnicast de Genetec. Complémentaire aux dispositifs humain et technique existants, l'ensemble permet de renforcer la surveillance du site et notamment de la zone d'accès restreint. Le port de Dunkerque devient ainsi le premier port dans le monde à s'équiper d'une telle technologie de surveillance.
Dunkerque est un des plus gros ports français avec, chaque année, un transit de plus de trois millions de passagers et de sept millions de tonnes de fret. Le Code international de sûreté (ISPS) impose une surveillance accrue et un contrôle permanent des installations portuaires avec des mesures renforcées pour les zones d'accès restreint. Le partenariat conclu entre Azur Drones et Eamus Cork, en collaboration avec Genetec, concourt ainsi à cet objectif.

© DR

Complément à la présence humaine

« En raison de son activité dense et des exigences réglementaires, l'installation portuaire doit être sécurisée 7 jours sur 7 et 24 heures sur 24. Il est apparu évident de compléter notre présence humaine et le système de caméras de surveillance de l'exploitant avec de la technologie drone. Le système Skeyetech, intégré à la solution de gestion vidéo de Genetec, permet d'améliorer la réactivité et l'efficacité des équipes de sécurité qui surveillent les installations », explique Thomas Ditacroute, directeur d'exploitation chez Eamus Cork.
Le drone autonome Skeyetech peut en effet décoller à tout moment, d'un simple clic, pour assurer des missions de surveillance de façon complètement autonome. Doté de caméras optique et thermique, il est opérationnel de jour comme de nuit pour réaliser des levées de doutes, des rondes périmétriques ou suivre des interventions à distance. Il s'agit du premier système de drone sans télépilote homologué en Europe pour des vols hors vue. ■

SÉCURITÉ

Au cœur de la campagne des municipales

Comme le confirme une récente enquête Odoxa-CGI France Info, la sécurité sera au cœur de la campagne de prochaines municipales.
En effet, les Français expriment une réelle attente sur le sujet. D'une manière, ils plébiscitent l'action de leurs maires et se montrent favorables à certaines mesures. En tête, le fait de permettre aux polices municipales d'intervenir dans les parties communes des immeubles (88 % des sondés).
Autre constat : les mesures visant à renforcer les moyens sécuritaires matériels et humains (dont certaines existent déjà dans plusieurs communes) remportent un franc succès.
Ainsi, deux autres mesures sont citées par au moins huit sondés sur dix :
- la mise en place de patrouilles d'agents en civil pour lutter contre les flagrants délits et faire de la prévention (souhaitée par 85 %) ;
- l'augmentation du nombre de caméras de vidéosurveillance (80 %).
Enfin, d'autres, dans 72 % des cas, souhaitent la création d'une application pour smartphone de signalement des incivilités du quotidien (voitures mal garées, dépôts sauvages, etc.). ■

© Getty images

→ **www.odoxa.fr/sondage/priorites-francais-municipales-futurs-maires-attendus-securite-lenvironnement**

VIDÉOSURVEILLANCE

Des géants chinois à l'index

© DR

La mise sur le réseau des infrastructures de sécurité pose des problèmes de sécurité. Par ailleurs, certaines solutions de vidéosurveillance et autres ne sont pas toujours protégées contre la menace cyber et l'exploitation des données. Parfois ce n'est pas volontaire, parfois ça le serrait. Ainsi, on sait que l'administration américaine a dans son collimateur plusieurs géants chinois de l'électronique. Les raisons invoquées : craintes d'espionnage, vols de technologies et accusations de violation des droits de l'Homme. En l'occurrence, la persécution des Ouïgours par Pékin.
Après avoir mis sur une liste noire, les géants Huawei et Dahua Technology, Washington serait prêt à prendre des sanctions contre le leader mondial de la vidéosurveillance : Hikvision. Raison invoquée : Hikvision participerait, selon certaines associations de défense des droits de l'Homme, à la persécution des Ouïgours, minorité ethnique de confession musulmane vivant dans l'extrême ouest de la Chine.
Les restrictions que l'administration américaine imposerait à Hikvision pourraient être semblables à celles imposées à ses compatriotes. En particulier, la limitation de l'accès aux marchés et fournisseurs américains. ■

SAPEURS-POMPIERS

Le Sénat dit non aux violences

Dans un rapport rédigé par les sénateurs Troendlé, Kanner et Hervé, figurent 18 propositions pour lutter contre les violences, de plus en plus récurrentes, visant les soldats du feu. En effet, ces violences sont en augmentation constante avec 1914 agressions de plus en 2017 qu'en 2008. Soit une hausse de 213 % ! Et 2019 ne devrait pas déroger à cette triste règle.
Le rapport contient entre autres ces trois propositions :
- Agir en amont pour limiter la menace via une campagne de sensibilisation à la situation des sapeurs-pompiers.
- Mieux agir pendant l'agression pour en limiter les effets en définissant mieux les missions des sapeurs-pompiers.
- Agir après l'agression pour réparer les conséquences en facilitant le dépôt de plainte des sapeurs-pompiers victimes. Elle souhaite également que les SDIS saisissent la justice par l'intermédiaire d'un dépôt de plainte ou d'un signalement. ■

TRANSPORTS PUBLICS

Renforcement de la sécurité sur les réseaux

Île-de-France Mobilités a dévoilé son Plan sécurité de transports en commun. Parmi les mesures proposées, citons, le recrutement de 200 agents de sécurité auprès de sociétés privées sur l'ensemble du réseau et de 500 agents supplémentaires pour la police ferroviaire de la SNCF (Suge). Le plan prévoit aussi de nouveaux outils pour aider les agents dans leur mission.
Ainsi un centre unique de coordination de sûreté est prévu pour l'été 2021, pour rassembler tous les personnels dédiés à la sureté des voyageurs franciliens (police, gendarmerie, SNCF, RATP, Optile) sous l'autorité du préfet de police pour une meilleure efficacité sur le terrain, déjà financé à hauteur de 8,5 millions d'euros par Île-de-France Mobilités.
Les caméras-piétons vont être généralisées à l'ensemble des agents du GPSR. S'y ajoute la généralisation de la vidéoprotection dans les RER, trains, métros, tramways et bus. Aujourd'hui, 63 000 caméras équipent l'ensemble des véhicules du réseau.

© Getty images

Le plan contient également la création d'un haut-commissaire pour la sûreté dans les transports en commun au sein d'Île-de-France Mobilités. Il sera chargé du pilotage stratégique de la sûreté et de la lutte contre la délinquance et les incivilités dans les transports relevant de la compétence d'Île-de-France Mobilités. Enfin, il préconise des expérimentations autour de la vidéo intelligente, avec notamment la création avec la RATP d'un laboratoire d'intelligence artificielle, le Lab'IA Vidéo pour traiter les images vidéo. ■

SÉCURITÉ ET SÛRETÉ

Guide pratique et juridique

© DR

Olivier Hassid, directeur sécurité chez PwC Paris, a publié un ouvrage intitulé *Sécurité et sûreté : guide pratique et juridique. Prévenir les risques et les menaces.* La sécurité et la sûreté connaissent un essor important dans les entreprises et dans les organisations en général. Les directions sécurité et sûreté ou les directions de la sécurité des systèmes d'information ont la lourde tâche d'assurer, à la fois, la sécurité des personnes et notamment des collaborateurs en déplacement, et de protéger les biens pour se prémunir contre le vol, protéger le patrimoine informationnel de l'entreprise ou se prémunir contre les cyberattaques. Par ailleurs, la variété des menaces suppose une palette de mesures qui peut aller aussi bien de moyens technologiques comme l'usage de la biométrie, le recours à des agents de sécurité ou encore la vérification de l'intégrité des candidats au moment du recrutement. Les auteurs, sur ces sujets, ont pu constater que de nombreuses entreprises se mettent hors-la-loi et sont « non conformes » car elles maîtrisent imparfaitement le droit. Alors que peut-on faire en matière de surveillance, de contrôle et de vérification ? Comment se prémunir des menaces sans déraper et se mettre en danger ? Ils répondent à ces questions en rappelant les mesures légales à mettre en place et en se basant sur des cas concrets. Un tour de force qui intéressera aussi bien les dirigeants d'entreprise de plus en plus sensibles aux risques de sécurité et de sûreté que les professionnels du domaine, les directions juridiques mais aussi un large public de plus en plus préoccupé par l'équilibre précaire entre sécurité et droit. ■

→ **Olivier Hassid, *Prévenir les risques et les menaces*, Legitech, Paris, 2019.**

Carnet

AXIS COMMUNICATIONS

PEDRO ALFARO

© DR

Pedro Alfaro a été nommé au poste de directeur technique et formation pour l'Europe du Sud chez Axis Communications. Auparavant à la tête d'Axis d'Espagne en tant que directeur national des ventes, Pedro Alfaro aura pour mission de diriger et de renforcer l'équipe régionale technique et formation qui assistera les ventes et les activités commerciales, en établissant des objectifs opérationnels et en s'alignant avec la stratégie segments et business du groupe. Il succède à Mario Vigevani, qui, après huit années à ce poste, prend la fonction de EMEA Portfolio Strategy Director au sein d'Axis.

AXIS COMMUNICATIONS

MATTEO SCOMEGNA

© DR

Axis Communications a annoncé la nomination de Matteo Scomegna au poste de directeur eégional Europe du Sud. Matteo Scomegna sera à la tête d'une équipe de 80 personnes et définira la stratégie ainsi que la planification de toutes les activités de la région d'Axis en Europe du Sud (Italie, Espagne, France, Portugal, Grèce, Israël, Malte, Chypre, Algérie, Tunisie et Maroc). Chez Axis depuis 2007, Matteo Scomegna a assuré des fonctions importantes en Italie et à l'étranger jusqu'à son dernier poste de directeur commercial Europe du Sud. Il succède à Edwige Maury, qui prend sa retraite après avoir travaillé douze années dans l'entreprise.

SCUTUM SECURITY FIRST

DAMIEN STRIEBIG

© DR

Damien Striebig a quitté la Gendarmerie nationale pour devenir PDG de Scutum Security First (SSF), spécialisée dans la prévention et la gestion des risques à l'international. Général de division, il était commandant de la Garde républicaine depuis 2014.

Agenda

JANVIER 2020

Nuit de l'AN2V
Le 29 janvier 2020 – Paris
https://an2v.org/nuitan2v/

Universités de l'AN2V
Du 30 au 31 janvier 2020 – Lyon
https://an2v.org/universites-an2v/

FÉVRIER 2020

Gala de la sécurité
Le 6 février 2020 – Paris
www.galas-agorafonctions.com/gala-securite/

Sécuri'Days
Du 26 au 27 février 2020 – Deauville
www.securi-days.fr/

MARS 2020

Security/Safety Prevention Meetings
Du 17 au 19 mars 2020 – Cannes
www.security-and-safety-meetings.com

MAI 2020

Ifsec
Du 19 au 21 mai 2020 – Londres
https://www.ifsec.events/international/

Préventica Nord
Du 26 au 28 mai 2020 – Douai
https://www.preventica.com

SEPTEMBRE 2020

Trophées de la sécurité
Le 28 septembre 2020 – Paris
https://www.tropheesdelasecurite.fr/

Préventica Lyon
Du 29 septembre au 1 octobre 2020 – Lyon
https://www.preventica.com

NOVEMBRE 2020

Expoprotection
Du 03/11 au 05/11/2020 – Paris
https://www.expoprotection.com/

© DR

COOPÉRATIONS DE SÉCURITÉ

Philip Alloncle quitte la DCS

Philip Alloncle était à la tête de la Délégation aux coopérations de sécurité depuis 2016. Il rejoint à la fois le ministère de l'Éducation nationale et de la Jeunesse et celui de l'Enseignement supérieur, de la Recherche et de l'Innovation en tant que haut fonctionnaire adjoint de défense et de sécurité.
Le colonel Denis Nauret, délégué adjoint aux coopérations de sécurité, a précisé que la délégation existe toujours et qu'elle poursuit son dialogue avec les métiers de la sécurité privée.
«Je tiens à remercier chaleureusement le préfet Philip Alloncle pour son écoute, sa grande implication et les nombreux travaux qu'il a menés, avec toute son équipe, en faveur de la profession, depuis 2016», a déclaré Jean-Christophe Chwat, président du GPMSE Fédération. ■

YVAN DE MESMAEKER,

secrétaire général de l'European Corporate Security Association (Ecsa)

« Il faut renforcer l'échange d'informations entre le public et le privé. »

© DR

Pour le secrétaire général de l'ECSA, dans le contexte actuel, la collaboration entre public et privée doit être améliorée. Il faut, pour affronter le terrorisme ou le crime organisé, aller chercher les compétences et les informations là où elles se trouvent.

Pouvez-vous nous présenter l'Ecsa ? Son rôle ? Ses missions ?

En 2005, à l'occasion de discussions avec Eurojust, Europol et des directeurs sécurité d'organisations et d'entreprises, il est apparu qu'il manquait, au niveau européen, un groupement, une association similaire à ce que veut être l'Asis au niveau international, mais qui reste très marquée par la culture américaine. Or, nous constations déjà à l'époque qu'il existait des spécificités régionales – asiatiques, européennes, africaines, sud-américaines… – en ce qui concerne les problématiques liées à la sécurité des États et des entreprises. Spécificités qui nous paraissaient nécessaires de respecter en choisissant plutôt une approche régionale de ces questions, et à mettre en place des alliances avec d'autres associations comme l'ISMA, le CDSE en France, l'ASW en Allemagne, le RSMF au Royaume-Uni,… Les objectifs de l'ECSA sont multiples. Le

premier est d'offrir à ses membres un espace, un forum, dans le cadre duquel ils peuvent échanger sur des sujets les concernant, partager des informations sensibles, se former et réseauter. L'Association a également pour objectif d'assurer la liaison et de promouvoir les synergies entre les entreprises, le monde académique et les autorités. Nous cherchons aussi à favoriser et à développer la coopération public-privé qui est si importante en matière de lutte contre toutes les formes de malveillance. Nous sommes installés à Bruxelles, ce qui nous permet d'avoir accès aux institutions européennes et aux divers centres de gravité européens.

Vous évoquiez à l'instant la coopération entre le secteur public et le privé. On en parle beaucoup en France dans le cadre du continuum sécurité. Quel constat faîtes-vous de cette coopération ? Est-elle ce qu'elle devrait être ?

La coopération entre le secteur public, c'est-à-dire le régalien, et le secteur privé – professionnels de la sécurité privé – et les entreprises – qu'elles disposent ou pas d'une direction sécurité – a toujours été complexe et très marquée par un vieux réflexe de l'État : la sécurité et ses sujets connexes relèvent du régalien. L'État « tolère » la sécurité privée et accepte à petits pas de collaborer. En ce qui concerne les relations entre les services des États, quel que soit le pays, et les entreprises et organisations privées, les échanges ne vont pas toujours d'elles-mêmes. Or, je pense, que dans une mondialisation toujours plus présente, le concept d'une sécurité relevant seulement des seuls États est un cadre dépassé. Par définition, les États sont des espaces géographiques délimités par leurs frontières. Au-delà de celles-ci, leur capacité à agir est beaucoup plus contrainte. À l'inverse, les grandes entreprises internationales s'inscrivent dans une réalité économique internationale. Tout comme le terrorisme ou le grand banditisme. Un grand groupe qui travaille à l'international s'occupe de la sécurité de ses collaborateurs – quelle que soit leur nationalité – et de la communauté qu'ils constituent. C'est patent dans le cas de la protection des expatriés et des voyageurs des grandes entreprises internationales. Les entreprises sont donc contraintes d'avoir une approche internationale de la sécurité, de gérer autant que possible les environnements politiques, sociaux, économiques… dans lesquels elles travaillent. Alors que les États, en-dehors de leurs frontières, ne contrôlent pas grand-chose. Les entreprises connaissent donc bien le terrain, collectent d'importants volumes de données et d'informations pour assurer leur sécurité et savoir ce qu'ils doivent protéger, où qu'ils soient. Il semblerait donc logique qu'entre États et entreprises existent un réel dialogue et de vrais échanges d'informations.

« Face au terrorisme, insistons sur la résilience de nos sociétés. Il faut en finir avec la peur. »

Que manque-t-il pour que cette collaboration, que vous appelez de vos vœux, devienne réalité ?

Normalement, un État, en tant que tel, devrait toujours être un partenaire de l'entreprise. Or, dans bien des cas, une autorité étatique conçoit l'échange d'informations dans un sens unique : elle reçoit l'information. Et se fait tirer l'oreille pour en donner. C'est flagrant dans le cas de la lutte contre la radicalisation. Les entreprises signalent aux services de renseignements la possible radicalisation violente d'un ou de plusieurs de leurs collaborateurs. Ensuite, et sauf contact individuel privilégié, elles restent dans le flou le plus total et ne savent pas ce sur quoi a débouché ce signalement. Dans certains cas, les services de renseignements préfèrent que la personne signalée reste à son poste. Elle est en quelque sorte « fixée ». Mais l'ignorance dans laquelle demeure l'employeur le conduit parfois à prendre des mesures radicales, comme un licenciement, alors que dans la réalité, ce licenciement n'était pas nécessaire. Il faut donc définir des critères fondamentaux qui faciliteront les échanges d'informations entre les États et leurs services, et le secteur privé.

Quels sont ces critères qui permettraient de favoriser les échanges entre le public et le privé ?

Le premier est évidemment la confiance. Puis-je faire confiance à la personne ? Cela passe par exemple par des habilitations sécurité, qui ne sont rien d'autres que des « certificats de confiance ». D'ailleurs, dans certaines entreprises, des cadres jouissent d'habilitation de sécurité. Le deuxième est évidemment le secret profes- ● ● ●

BIO EXPRESS

Depuis 2005 Secrétaire générale de l'Ecsa, secrétaire général et membre du Conseil d'Athena (Association des anciens des Hautes Études sécurité & défense).
Depuis 2010 Directeur des Hautes Études police, justice & sécurité d'entreprise, de l'école des officiers de la Police Intégrée, de l'Institut de formation judiciaire, de la Fédération des entreprises de Belgique et les universités de Liège et de Gand.
2017 Reçoit le titre d'officier dans l'Ordre de la Couronne pour sa contribution dans le domaine de la sécurité. ■

YVAN DE MESMAEKER,

secrétaire général de l'European Corporate Security Association (Ecsa)

« La coopération entre le secteur public et le secteur privé a toujours été complexe. »

© DR

sionnel qui pourrait, par exemple, être étendu à la direction sécurité des entreprises. Le dernier est ce qu'on peut appeler « le besoin d'en connaître » qui se résume à cette question : est-il nécessaire de transmettre telle ou telle information à telle ou telle personne ? Ces critères permettraient de définir un cadre qui pourrait s'appliquer au-delà du domaine régalien afin de faciliter les échanges d'informations. Prenons un exemple : celui de la lutte contre la fraude. Je pense que les services des États auraient tout intérêt à collaborer de manière beaucoup plus étroite avec les spécialistes des entreprises qui luttent contre la fraude et la contrefaçon. Cette collaboration, en bonne intelligence, s'inscrirait, en prenant le cas de la France, dans le continuum de sécurité.

Quelles sont, selon vous, les principales menaces auxquelles doivent faire face les entreprises aujourd'hui ?

Le terrorisme en est évidemment une. Mais je pense qu'on lui donne une importance qu'il n'a pas et que d'ailleurs recherchent les terroristes. Entendons-nous bien, je ne dis pas que la menace est moindre qu'on ne le croit ou que l'impact sur les personnes touchées ne serait pas chose grave. Mais je pense que son impact réel sur les économies des États, sur leur fonctionnement, est moindre que son impact psychologique. À ce sujet, les médias amplifient cet impact. En outre, il est scandaleux que certains médias – les chaînes d'information continue en l'occurrence – transmettent en direct des images d'interventions policières. Je pense que face au terrorisme, il faut en finir avec la peur. On devrait sans doute plus insister sur la résilience de nos sociétés. Elles ont fait preuve d'une étonnante capacité à rebondir, à « résilier ».

Voulez-vous dire qu'on parle trop du terrorisme au risque d'en oublier d'autres menaces ?

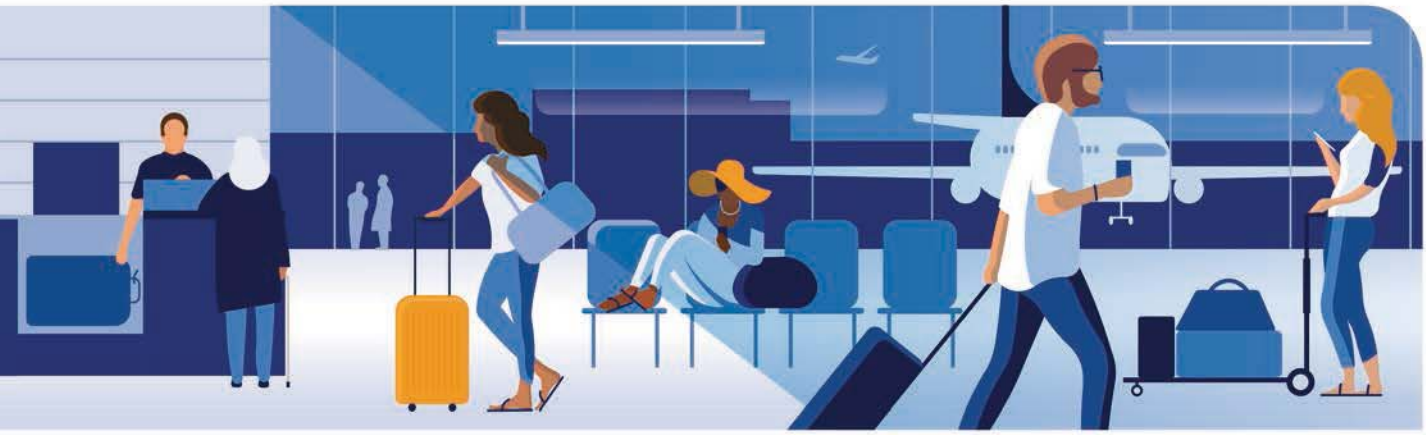
Pas tout à fait. Le terrorisme est une menace. Pour nos sociétés, pour notre activité économique… Mais le terrorisme auquel nous devons faire face aujourd'hui a certes un impact psychologique important (et même disruptif du fait de l'amplification par les médias) mais un impact matériel limité. Il ne s'est pas encore attaqué à des infrastructures véritablement vitales pour nos économies et le bon fonctionnement de nos États. Si cela arrivait, l'impact serait bien plus grand. Pensons à Al-Qaida. Cette organisation terroriste avait une stratégie, était capable de penser et de concevoir des actions complexes et impressionnantes. Souvenons-nous du 11 septembre qui a sidéré le monde. À l'inverse, l'État islamique n'est pas du tout dans le même mode d'action. Ils tuent des gens et c'est horrible, mais sans impact sur le fonctionnement technique des pays. C'est à faire face à un terrorisme de type Al-Qaida que nous devons préparer nos pays. Pour que le cas échéant, c'est-à-dire le jour où une organisation terroriste pourra s'attaquer à un OIV ou organiser une cyberattaque massive, au niveau d'un continent ou mondial, nos sociétés, nos États, nos organisations puissent faire face et continuer à fonctionner… De plus, nous sommes dans un contexte de forte instabilité. En Afrique, au Moyen-Orient et même aux États-Unis, en Turquie… partout nous rencontrons des situations déséquilibrées, des situations « inflammables ». Si une région basculait, ce basculement pourrait avoir comme conséquence un effet dominos qui impacterait les économies de nos pays. C'est à cela aussi que doivent se préparer les entreprises et les États. Par ailleurs, on ne peut ignorer la forte capillarité entre le terrorisme et le crime organisé et leur puissance financière. Comment lutter contre ce rapprochement ? L'efficacité des actions des États est limitée par des lois, des obligations et est le plus souvent limité à un cadre restreint. Je pense qu'ici aussi la collaboration avec les entreprises internationales – plus agiles – serait utile. Il nous faut, encore une fois, favoriser les synergies entre les responsables sécurité du secteur privé et les États pour que les moyens, les expertises, les informations… de chacun soient mis au service de la sécurité de tous. ■

L'ECSA EN BREF

Fondée en 2005, l'European Corporate Security Association regroupe des responsables en charge de la sécurité dans les grandes sociétés, les organisations et institutions européennes et internationales. Installée à Bruxelles, elle a pour objectifs de contribuer à la sécurité, à la continuité ou à la résilience des sociétés, organisations et institutions.

Tout le monde.

Partout.



Tous les jours.

L'ordinaire exige une protection extraordinaire.

genetec.com/fr

En savoir plus sur le logiciel qui gère le quotidien sur
genetec.com/protectingeeveryday

Genetec™

© 2017 Genetec Inc. GENETEC et le GENETEC LOGO sont des marques commerciales de Genetec Inc., qui peuvent être déposées ou en instance de dépôt dans plusieurs pays

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

dossier

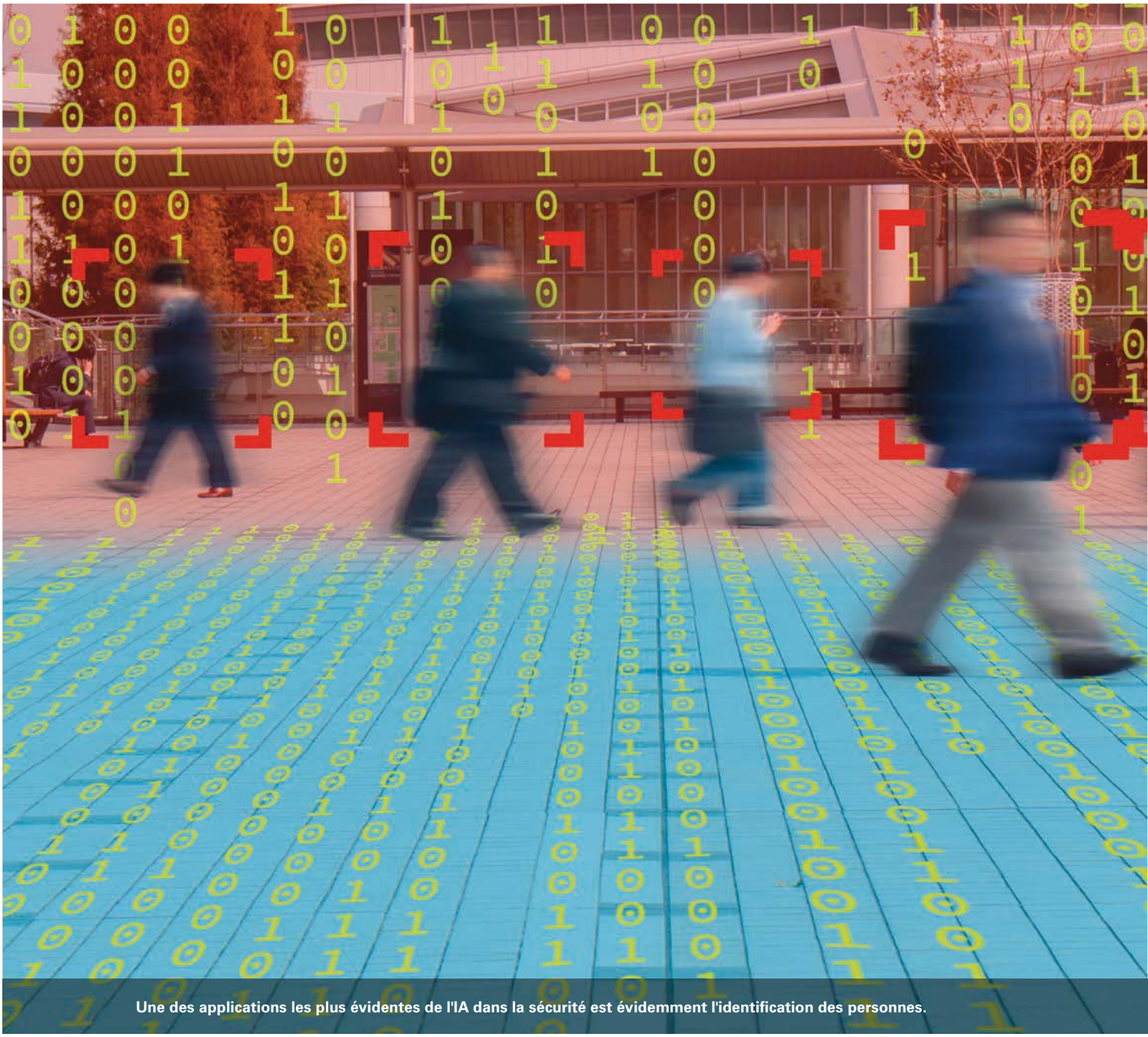
L'IA au service de la sécurité ?

L'intelligence artificielle est plus que jamais d'actualité dans le monde de la sécurité. Tant chez les fabricants de solutions que chez les utilisateurs. Mais, concrètement, que permet-elle de faire et dans quelles mesures ?

© Getty images

SOMMAIRE

→ **L'IA de plus en plus présente dans la sécurité** **34**
→ Où commence l'IA ? 35
→ Que peut faire l'IA ? 36
→ Un domaine de prédilection : la vidéo 37
→ Est-elle vraiment intelligente ? 39
→ Une intelligence intrusive ? 40



© Getty images

Une des applications les plus évidentes de l'IA dans la sécurité est évidemment l'identification des personnes.

L'IA de plus en plus présente dans la sécurité

Réellement intelligente ou juste plus rapide, l'IA ouvre de vraies perspectives à tous les acteurs de la sécurité. Les progrès accomplis sont certains comme le simple fait de reconnaître un objet, un individu. On n'en est pas encore à l'identification mais cela viendra sans doute. Et les Français sont plutôt bons !

PAROLE D'EXPERT

JEAN-MARIE BAILLY
Président d'Aquilae

© DR

« L'IA EST UN OUTIL D'AIDE À LA PRISE DE DÉCISION. »

« Grâce à l'IA, on peut faire beaucoup de choses lorsqu'on est capable de créer une signature électronique d'anomalies qu'on souhaite faire ressortir. Mais cela nécessite une importante phase d'apprentissage. Et il ne faut pas imaginer que l'IA peut tout faire. Elle ne peut pas fonctionner, efficacement et de manière sûre, si, derrière l'IA, il n'y a pas une décision humaine. Nous devons donc concevoir l'IA comme un outil d'aide à la prise de décision. On doit remonter les informations vers l'IHM (interface homme-machine) afin qu'elle localise les anomalies, en temps réel, pour aider l'opérateur devant son écran à valider l'anomalie, prendre la bonne décision, puis engager la bonne procédure. L'analyse des flux vidéo permet de faire de nombreuses choses aujourd'hui. Mais, malheureusement, nous sommes contraints par la réglementation française qui ne nous aide pas à expérimenter, dans un cadre précis, nos outils. En effet, l'IA nécessite de pouvoir utiliser un peu de biométrie (couleurs de cheveux, largeur d'épaules, etc.), or on nous interdit souvent de le faire. Aujourd'hui, nous sommes capables, chez Aquilae, de détecter un colis abandonné, même s'il y a du monde autour de lui, et de remonter dans les flux vidéo pour retrouver la personne à laquelle il appartient. L'IA peut aussi être très utile pour détecter des comportements anormaux, susceptibles d'être ceux de personnes malveillantes, comme les maraudeurs ou les pickpockets. Nous travaillons aussi avec des logisticiens et des industriels pour suivre des colis ou détecter des anomalies dans les process de fabrication. »

A en croire Vladimir Poutine, « celui qui sera leader dans l'intelligence artificielle, sera le maître du monde ». Rien de moins. Aux États-Unis, l'agence de recherche Darpa a investi deux milliards de dollars dans l'IA. Tandis qu'en France, le gouvernement a décidé d'y consacrer un milliard d'euros d'investissement. Tout cela pour dire que l'IA est plus que jamais un des défis technologiques qui vont mobiliser les États, les ingénieurs et autres chercheurs dans les années à venir. Et, évidemment, la sécurité sera de plus en plus friande d'applications et d'outils basés sur l'IA, afin d'améliorer et de renforcer la sécurité dans les espaces publics mais aussi au sein même des entreprises et des organisations.

Mais que recouvre concrètement l'IA ? Il s'agit, pour faire simple, de toutes les technologies et techniques qui doivent permettre de rendre intelligentes les machines. C'est-à-dire de leur donner la capacité d'imiter une partie de l'intelligence humaine. Une des techniques liées à l'IA dont on parle le plus est le deep learning. Il s'agit d'un processus qui permet à l'ordinateur d'apprendre par lui-même, après avoir été programmé pour le faire. Pour cela, il doit pouvoir disposer de très importantes bases de données pour les exploiter et s'en « servir » pour faire des analyses, comparer, « apprendre »…

Les données et le big data sont donc un des nœuds de la guerre de l'IA car plus elle dispose de données, plus la machine devient efficace, performante. Et autonome pour la réalisation de certaines tâches.

Fanch Francis, directeur général d'OAK Branch, filiale de Deveryware, explique que « l'IA est un ensemble de théories et de techniques permettant de simuler l'intelligence et la prise de décision par des machines. Elle est constituée par le machine learning, le deep learning et de nombreux sous-domaines, comme le traitement du langage naturel, qui permettent de répondre à diverses problématiques ». Avant d'ajouter : « On retrouve ainsi de l'IA dans le domaine médical, pour une approche médicale personnalisée et une meilleure lecture des radiographies ; dans l'industrie des objets connectés, pour analyser le flux émanant des équipements ; dans le domaine de l'investigation, pour traiter des données textuelles, images ou vidéos et reconnaître des personnes par leur style d'écriture, leur voix ou leur visage par exemple. »

Où commence l'IA ?

Le deep learning est une sous-catégorie du machine learning constituée par les différentes formes de réseaux de neurones. Ils permettent de modéliser des relations non linéaires complexes, mais nécessitent souvent de grands échantillons de données pour obtenir des modèles généralisables. Le deep learning, quant à lui, a permis d'augmenter significativement les performances pour le traitement de données non structurées (texte, son et image).

2 QUESTIONS À

NICOLAS LE SAUX

Président d'Atao Consulting

© DR

On parle beaucoup d'IA dans la sécurité et de ses avantages. N'a-t-elle que des avantages ?
La sécurité est probablement le domaine d'application de l'IA qui pose le plus de difficultés et, principalement, celui de la reconnaissance faciale en raison de son manque de fiabilité. En 2017, lors du carnaval de Nothing Hill à Londres, 35 suspects identifiés par un logiciel d'IA s'avèrent être autant d'erreurs. En 2019, le National Institute of Standards and Technology, une agence fédérale américaine, a examiné 189 logiciels et algorithmes produits par 99 éditeurs du monde entier. Cette étude met en avant qu'un visage de type afro-américain ou asiatique a de dix à cent fois plus de probabilité de faire l'objet d'une erreur d'identification qu'un visage de type caucasien…

Existe-t-il d'autres problèmes ?
En effet. Les algorithmes d'IA sont intrinsèquement biaisés car la majorité de leurs développeurs sont des hommes, bien portants, issus d'un environnement privilégié. Cela induit des biais cognitifs dans l'intelligence développée par ces logiciels… Se pose également la question de la « prise de décision » des logiciels d'IA, de sa fiabilité et même de sa compatibilité avec notre environnement démocratique européen : les leaders mondiaux de l'IA ne venant pas de pays connus pour leur respect des libertés individuelles. Dans le domaine de la sécurité privé, l'IA permet au logiciel de se substituer à l'humain ou de le compléter. Une proposition intéressante pour les sociétés moyennes agiles où l'IA permettra de surmultiplier leur capacité opérationnelle sans surcoût social, mais plus menaçante pour les gros opérateurs dont le modèle économique repose sur de la prestation au volume à bas prix…

© Getty images

LE POINT DE VUE D'UN FABRICANT

RÉMY DEUTSCHLER
Directeur général de Milestone Systems France

© DR

« DES BESOINS RÉELS. »

« Avec notre partenaire Veer, nous avons développé des solutions liées à la classification des objets et proposons des applications qui permettent d'identifier des comportements, de reconnaître les modèles et types de véhicules, d'évaluer la qualité d'un produit pendant sa fabrication… Si ces outils fonctionnent, il faut reconnaître que leur efficacité est liée à la stabilité de l'environnement dans lequel ils sont déployés. Les besoins en IA sont réels, mais il existe un grand décalage entre les grandes structures et les organisations qui sont capables d'exploiter ces outils, d'en exprimer le besoin, et les structures plus petites alors que l'IA, hors du domaine purement sécuritaire, peut aussi être très utile pour assurer la sécurité des process industriels ou pour utiliser la vidéo à d'autres fins comme dans le domaine du marketing dans la distribution. »

● ● ● « L'IA commence à partir du moment où on utilise des algorithmes qui apprennent avec des observations et qui tentent de modéliser des relations généralisables à d'autres échantillons de données, poursuit Fanch Francis, le directeur général d'OAK Branch. En effet, l'IA automatise les processus répétitifs d'apprentissage et de découverte par le biais des données ; elle s'adapte également par des algorithmes d'apprentissage progressifs. »

Que peut faire l'IA ?

En restant schématique, l'IA est aujourd'hui capable de réaliser deux types d'actions : appréhender une situation et prendre une décision en identifiant les différents éléments d'une image, un comportement atypique dans une vidéo ou une anomalie. L'IA est aussi capable d'identifier la catégorie à laquelle appartient un objet, un élément d'une image. On comprend donc aisément pourquoi l'IA intéresse tant le monde de la sécurité, qu'il soit public ou privé.
Ainsi, les États ont très vite compris que l'IA pouvait avoir des domaines d'applications dans la sûreté et la sécurité. Sans se focaliser sur le cas très particulier de la Chine, de nombreux États s'en servent pour détecter des comportements inhabituels dans les images saisies par les caméras de vidéosurveillance, pour reconnaître des visages ou encore pour détecter des armes.

Les États se servent également de l'IA pour surveiller et analyser nos mails, nos messageries instantanées, nos réseaux sociaux, pour détecter, dans le contenu des messages, des menaces, la récurrence de certains termes, d'expressions ou de groupes de mots.
Longtemps réservées au domaine régalien, les capacités de l'IA sont aujourd'hui à la portée des organisations privées et des autres entreprises. Ces dernières peuvent aujourd'hui se servir de l'IA pour, à partir de rapports de visites de contrôle, d'interventions, de rapports d'incidents… faire de la maintenance préventive.
Elles peuvent aussi s'en servir pour détecter des fraudes sur un réseau bancaire, faire de la veille économique, détecter des comportements types ou anormaux pour des applications marketing par exemple… Le champ est très vaste. Ce que confirme Axel Méry, CTO de Fujitsu France et directeur de centre d'excellence en intelligence artificielle : *« L'IA a un grand nombre d'applications en matière de sécurité/sûreté. Il est possible, d'une part, d'assurer la sécurité au travail des personnes en détectant des situations à risques et, d'autre part, d'aider à la sécurisation dans l'espace public, des sites privés, aider à détecter des attaques, retrouver des personnes, détecter des fraudes dans le commerce de détail, sécuriser les flux financiers… Elle est donc parfaitement légitime dans la sécurité. »*

Un domaine de prédilection : la vidéo

C'est sans doute celui dans lequel, en matière de sécurité, le potentiel de l'IA suscite le plus d'intérêt. Et de nombreuses recherches. ● ● ●

PAROLE D'EXPERT

AXEL MÉRY
Directeur technique de Fujitsu France

© DR

« CONCEVOIR LES SOLUTIONS QUI RÉPONDENT AUX BESOINS. »

« Fujitsu a installé en France son centre d'expertise en intelligence artificielle dont le principal objectif est de travailler sur les applications concrètes de l'IA dans divers domaines dont la sécurité. L'IA peut y être très utile et le sera certainement encore plus dans les années à venir. Lors de JO 2024 par exemple, L'IA aidera à assurer la sécurité du public en supervisant les queues et zones de concentration de la foule ou en retrouvant des personnes. Nous avons déjà conçu et développé des outils dans lesquels l'IA nous permet d'apporter des réponses à des problématiques comme les vols à l'étalage dans la distribution. Par exemple, dans le cas des caisses automatiques où le client scanne lui-même ses achats, nous proposons un outil qui permet, en utilisant une caméra, de valider par la vision que l'article scanné correspond bien au code-barres présenté. Tout l'enjeu de l'IA est de développer et de concevoir des outils, des logiciels qui répondent à un besoin réel des utilisateurs finaux européens et français, en s'assurant de respecter les réglementations et les lois en vigueur. Notre vision de l'IA est d'aider l'humain à être plus efficace et lui permettre de se concentrer sur la résolution des problèmes plutôt que sur leur détection. »

© Getty images

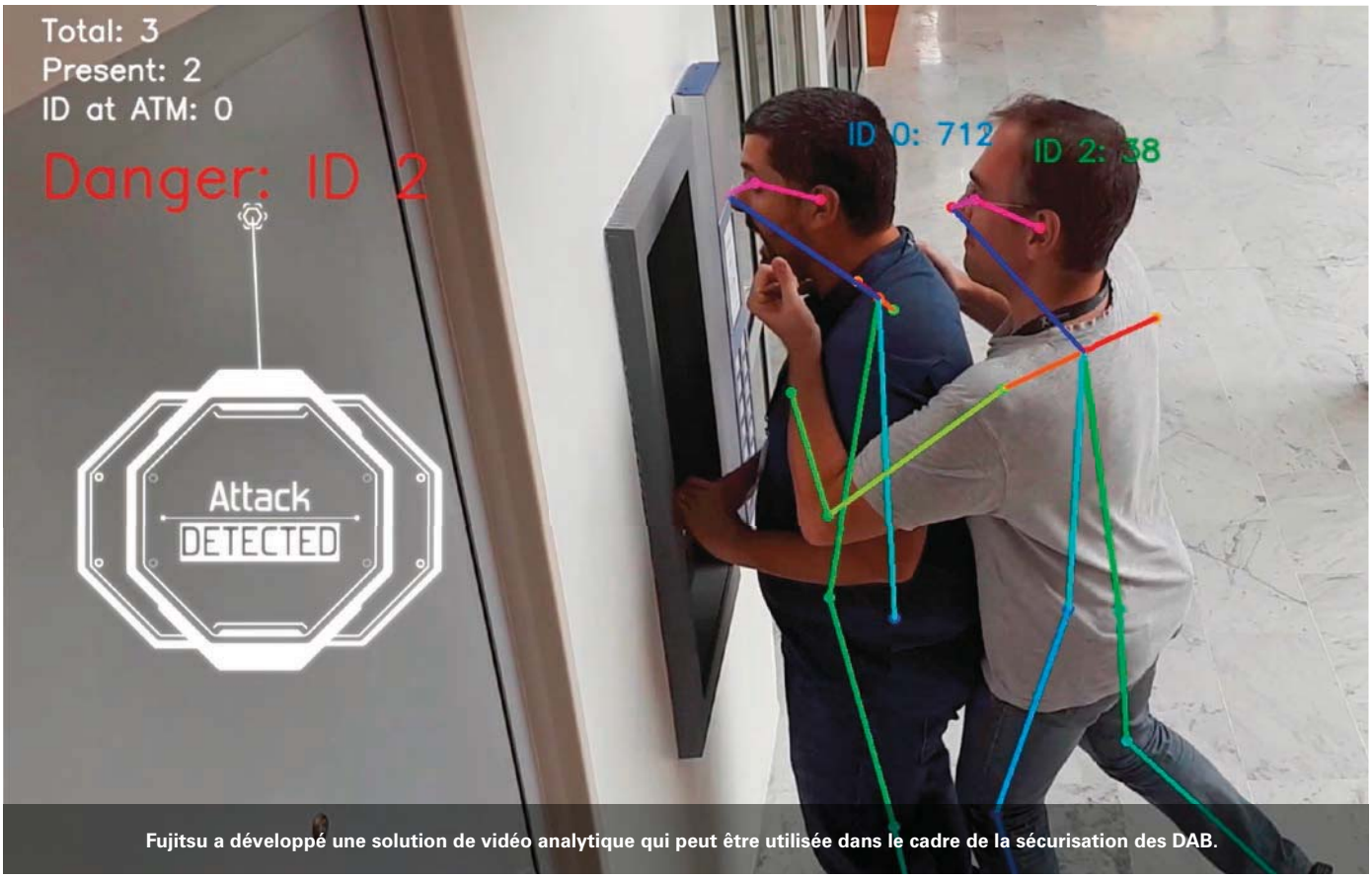
LE POINT DE VUE D'UN FABRICANT

XAVIER FÉRY
PDG de Komanche

© DR

« CHAQUE COUCHE D'IA DOIT PARLER AVEC LES AUTRES »

« Notre objectif est d'intégrer ou de développer une chaîne de valeur où chaque élément est constitué d'intelligence et de sécurité. Cette solution, constituée de caméras disposant d'un firmware "K safe" qui utilise des blocs et optiques certifiés CCC (Common Critéria Certification) ou des puces d'identification Trend Net, est fluidifiée et protégée par son nouveau VMS français "KxvKorp", chiffré en AES 256 pour gérer jusqu'à 50 NVR ou 1 000 caméras. Doté d'une supervision vidéo native, il permet aussi de détecter des mouvements avancés, de reconnaître des objets, de gérer des lignes, de détecter des couleurs... Mais surtout, jamais un réseau vidéo n'a été aussi bien protégé, car les échanges se font en triple authentification via un OpenVPN avec certificat en AES256 auquel nous avons ajouté une clé Hardware concaténée avec la licence ainsi qu'un mot de passe serveur généré aléatoirement au moment du raccordement VPN. C'est de cette manière que chaque brique de Komanche optimise et fluidifie la sécurité des solutions de vidéoprotection tout en optimisant les critères de détection automatique d'incident. Car chaque couche d'intelligence et de sécurité parle avec les autres… »



Fujitsu a développé une solution de vidéo analytique qui peut être utilisée dans le cadre de la sécurisation des DAB.

© Fujitsu

DU CÔTÉ DES START-UP

PHILIPPE ROCHARD
Président directeur général de Dipix Systems

© DR

« RECONNAÎTRE UN COMPORTEMENT ANORMAL EST DÉJÀ UNE PROUESSE ! »

« Dipix Systems est un éditeur de solutions logicielles. Il se différencie par l'emploi et la combinaison des technologies de réalité augmentée, réalité virtuelle et intelligence artificielle sur appareils mobiles (smartphones, tablettes). Nous élaborons des applications qui exploitent ainsi ces technologies de façon optimisée sur des appareils aux capacités réduites. Là est la prouesse. Notre matière première est la donnée 3D photoréaliste. Aidée de l'IA et du computer vision, elle nous permet de nouvelles approches de simulation et de compréhension du monde réel.
Par exemple, l'une de nos solutions phare vise à tout savoir des matériels, simplement en les observant, et ce en partie en associant 3D et IA. Une autre solution consiste à scanner en temps réel un espace physique en reconnaissant des éléments architecturaux précis comme des murs et délivrer instantanément un plan 2D/3D à l'échelle réelle. L'IA ne cesse de progresser et constitue une valeur ajoutée indéniable pour le monde de la sureté et de la sécurité. Là où l'informatique traditionnelle dite « déterministe » bute en raison d'une incapacité à s'auto-adapter, l'IA fournit cette alternative à travers laquelle elle peut produire en temps réel des résultats précis à partir de volumes conséquents de données aussi variables que les lois qui les régissent. L'IA devient peu à peu la réponse aux nouvelles exigences sociétales et sécuritaires. Chez Dipix Systems, nous travaillons à rendre ces IA d'une part performantes en mixant les contextes d'usages où bientôt il s'agira de reconnaître mais aussi d'identifier des états, des situations, des comportements, et d'autre part autonomes grâce aux travaux que nous réalisons sur les mobiles. »

● ● ● L'IA, dans le domaine de la vidéosurveillance, permet d'optimiser les recherches d'informations dans le flux constant et de plus en plus important des images fournies par les caméras. Et d'exploiter très rapidement les données. La vidéosurveillance dite intelligente permet donc de faire beaucoup de choses :

- Détecter et prévenir des actes terroristes en identifiant des individus recherchés grâce à la reconnaissance faciale ou à l'exploitation de données biométriques. La reconnaissance faciale pourrait donc devenir, si certaines limites législatives sont levées, une des applications où l'IA pourra constituer une aide précieuse pour les services de sécurité et les forces de l'ordre. Comme l'identification beaucoup plus rapide d'un individu.
- L'IA peut aussi permettre de détecter des attroupements qui pourraient éventuellement déboucher sur une situation dangereuse. La vidéosurveillance intelligente offre ici la possibilité d'anticiper certaines situations à risques.
- On peut également répérer des incivilités et identifier leurs auteurs en exploitant toutes les données saisies par les caméras et en recherchant des signes distinctifs.

2 QUESTIONS À

FANCH FRANCIS

Directeur général d'OAK Branch

© DR

En quoi l'IA peut-elle permettre aux entreprises et organisations de mieux lutter contre les fraudes, l'espionnage… ? Contre les actes de malveillance ?

La prise de décision d'un être humain est souvent dépendante de ses expériences passées. Néanmoins, un être humain ne peut avoir connu une infinité d'expériences et il est difficile pour lui de généraliser cette prise de décision de manière précise lorsque ce nombre augmente fortement.
Par exemple, pour de la lutte contre la fraude, un être humain peut observer au bout de nombreux cas de fraude que celle-ci peut être corrélée avec un grand nombre de versements, de gros versements ou la combinaison des deux. Cependant, il va être difficile pour lui d'estimer si ce qui doit tirer une sonnette d'alarme est le fait d'effectuer 100 ou 150 virements par semaine, ou peut-être simplement 75 virements mais avec de très gros montants. L'IA permet d'estimer précisément l'ensemble de ces facteurs afin de répondre à une question précise (ex : maximiser le nombre de fraudes détectées, minimiser le pourcentage de fausses alertes, etc.). Il est possible de lutter contre l'espionnage en utilisant des algorithmes permettant de détecter des intrusions dans des systèmes, en détectant des fausses informations (fausses identités, fake news, etc.).
Ou encore, il est possible de superviser les métadonnées (des données qui permettent de décrire d'autres données telles que date de collecte, niveau de confiance, sensibilité, etc.) c'est-à-dire autre chose que le contenu lui-même (conformité au RGPD oblige).
Cette supervision permet la génération d'alertes sur des accès non conformes, des effacements illégaux ou encore du stockage anormal. Là où une plateforme analytique apporte le plus d'atout c'est dans le domaine du croisement et de la fusion de données. Aujourd'hui des millions d'euros sont dépensés pour la collecte de données de toutes sortes. Cependant, l'analyse de ces données est confiée à un simple tableur. Sans une plateforme analytique telle que celle que propose OAK Branch et le groupe Deveryware, impossible de trouver le lien entre des lignes de bases de données, des emails et des rapports stockés dans un file system.
Les sujets où le recoupement de données au moyen d'une plateforme analytique sont multiples : fusion de données sécuritaires (rapport d'experts, retours terrains, réseaux sociaux) pour estimer le niveau de risque d'un pays ; analyse de contenu anonyme pour détection d'accès illicites, détection de fraudes complexes, etc.

Le domaine de l'IA a un véritable intérêt stratégique pour les États et les OIV. Comment pourrait-on soutenir les Français qui développent des solutions face aux géants asiatiques et autres ? Ne serait-ce que pour protéger les données exploitées…

Il ne faut pas confondre la capacité logicielle et la capacité fonctionnelle. OAK Branch utilise différentes plateformes pour adresser différents sujets. La souveraineté dépend du niveau de maîtrise de la plateforme, pas seulement de l'origine du code source. Ainsi une plateforme nationale, mais dont le client ne maîtrise pas les capacités n'est pas une plateforme souveraine.
La souveraineté est l'absence de monopole capacitaire. Pour protéger les Français qui développent des solutions logicielles et/ou fonctionnelles, il faut empêcher le nivellement par le bas qui surviendrait si l'État ne subventionne que les géants français du domaine.

- On peut aussi effectuer de la lecture de plaques d'immatriculation pour savoir si les véhicules sont autorisés à pénétrer dans telle ou telle zone de l'aéroport, localiser des objets abandonnés, une intrusion dans les zones sensibles…
Ajoutons à cela, la détection d'indices et l'aide lors d'une enquête judiciaire qui sont un des champs d'application de l'IA. À ce sujet, il faut souligner que le Conseil de l'Europe a adopté la première charte éthique européenne relative à l'utilisation de l'IA dans le système judiciaire.

Est-elle vraiment intelligente ?

Question iconoclaste ? Peut-être, mais certains considèrent, à l'instar de Genséric Cantournet, président de Kelony, que l'IA n'est pas intelligente. *« Elle est rapide, démultiplie les capacités de calculs. Ce n'est pas de l'intelligence. Et compte tenu des milliards investis dans l'IA,* ●●●

PAROLE D'EXPERT

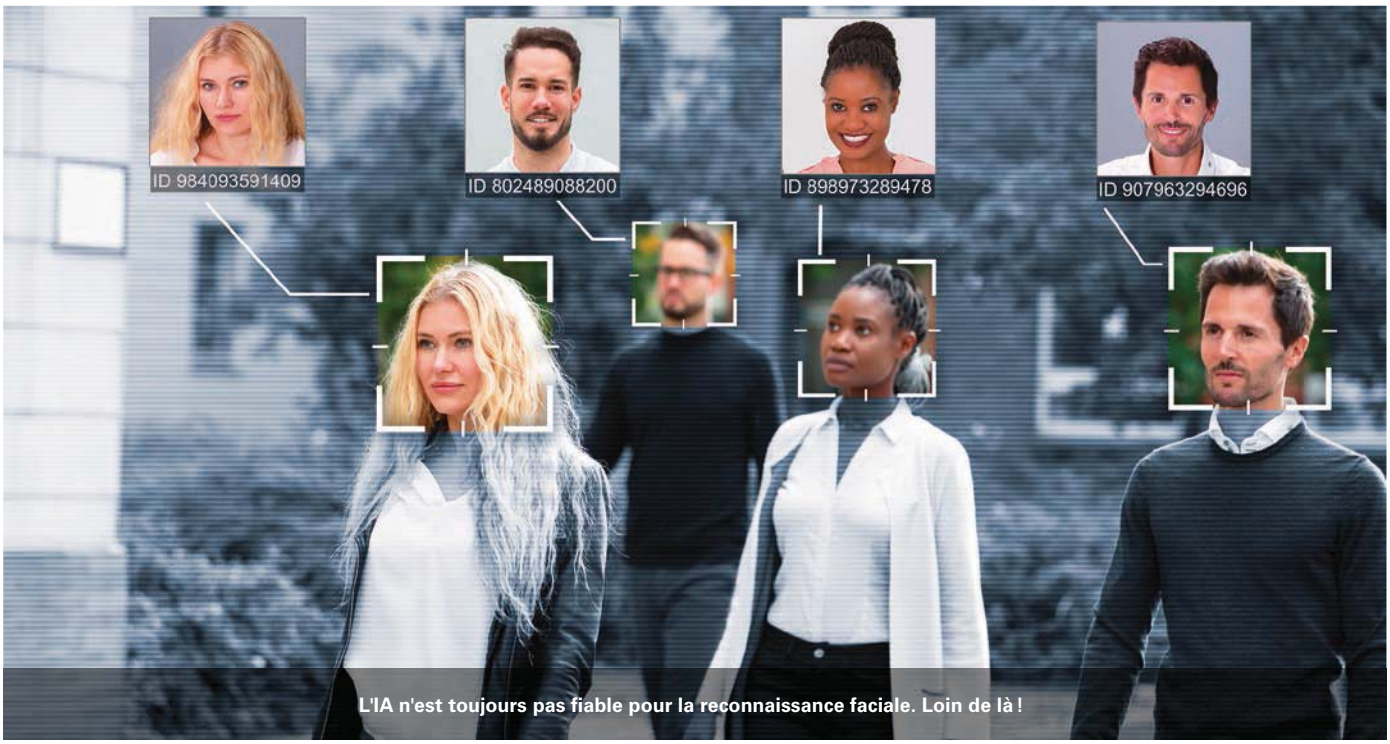
GENSÉRIC CANTOURNET

Président de Kelony

© DR

« ELLE N'EST PAS INTELLIGENTE ! »

« L'IA est une formidable avancée technologique si on la considère pour ce qu'elle est. C'est-à-dire un outil qui, à partir d'une masse de données très importantes, peut calculer plus vite et fournir à l'humain des informations qui lui permettront de réagir plus vite et mieux. Cela dit, on ne doit pas s'interdire de se poser certaines questions. Qui a programmé la machine ? Quid des bases de données et de leur fiabilité ? Sont-elles mensongères ? Contiennent-elles des omissions, des erreurs de perspectives ou des biais cognitifs ? À partir de quel cadre de référence ont-elles été bâties ? Avant de laisser la machine décider en matière de sécurité, il faut tout de même se poser ces questions et faire en sorte de disposer de bases de données correctes, des outils de traitements adéquats qui seront capables d'analyser correctement les données. Je le répète, l'IA n'est pas intelligente. C'est un formidable levier en matière de puissance de calcul, qui fait plus vite ce qu'on lui demande de faire… Mais qui, je le répète, se contente de calculer plus vite des opérations mathématiques pour manipuler des données de façon mécanique à partir d'énormes masses de données. »



L'IA n'est toujours pas fiable pour la reconnaissance faciale. Loin de là !

© Getty images

● ● ● *on en attend beaucoup trop,* explique le président de Kelony. *L'IA telle qu'on nous la présente aujourd'hui est essentiellement basée sur des méthodes qui ne sont pas nouvelles comme les modèles d'apprentissage par inférence. Qu'est-ce qui définit l'intelligence ? Ce sont les capacités humaines à comprendre, raisonner et percevoir la vérité et à déterminer la validité d'une information. L'intelligence permet à un être humain de résoudre un problème sachant qu'il comprend en quoi ce problème consiste. L'IA ne comprend rien du tout. Or, sans compréhension il n'y a pas de capacité de faire face à des circonstance imprévues… Par ailleurs, l'IA a-t-elle conscience du risque ? On parle d'outils dédiés à la sécurité des personnes et des biens ! L'IA se contente de calculer plus vite des opérations mathématiques pour manipuler mécaniquement des données à partir d'énormes masses de données. »*

Une intelligence intrusive ?

Qu'elle soit intelligente ou pas, l'IA et son utilité ne doivent pas gommer les éventuelles menaces qu'elle peut faire peser sur les libertés individuelles et publiques. De nombreux juristes s'inquiètent du

PAROLE D'EXPERT

MARC VAILLANT
président directeur général d'Azur Soft

© DR

« PRÉVENIR LES RISQUES GRÂCE À L'ANALYSE. »

« L'IA a de nombreux champs d'application. On pense évidemment à l'analyse de séquences vidéo pour la reconnaissance de plaques, la détection de comportements, l'analyse des flux de personnes. Elle peut aussi être utilisée pour analyser des données biométriques. Elle sert également pour détecter des armes. Ainsi la société Liberty Defense qui utilise l'IA pour lutter contre les crimes à main armée. Son système Hexware utilise l'imagerie 3D et l'IA pour détecter les menaces lorsque des groupes de personnes passent près de ses capteurs. Cette technologie peut être utilisée en intérieur ou en extérieur, et peut détecter aussi bien les armes métalliques que non métalliques. Le développement croissant d'outils intégrant de l'IA s'explique par le fait qu'elle permet de prévenir un risque via l'analyse de comportement et de détecter, par exemple, le maraudage. On peut aussi identifier une personne via la reconnaissance faciale et permettre une interpellation ou de retrouver des personnes portées disparues. Chez Azur Soft nous proposons des outils d'aide à la prise de décision plus rapide, plus stratégique car tous les domaines de la sécurité sont susceptibles d'avoir recours à l'IA et tous les systèmes de sécurité transmettent des données. Par ailleurs, je voudrais souligner que les avancées à la fois en investissements et travaux juridiques autour du cloud français sécurisé sont une excellente initiative, elles avancent correctement. Sera-ce suffisant ? Difficile à prévoir, le temps du numérique et du législatif ne coïncident que très rarement. La commande publique est toujours bienvenue mais elle ne fait pas tout. Il faut qu'elle soit amplifiée auprès des grands donneurs d'ordres parapublics et des grandes entreprises privées (dans un contexte type Cluster intelligence artificielle et sécurité). Les PME innovantes manquent de visibilité auprès des grands groupes, les mises en relation sont donc indispensables. »

DU CÔTÉ DES START-UP

JULIEN TROMBINI
Cofondateur et président de Two-i

© DR

« LA PERTINENCE DES BASES DE DONNÉES EST PRIMORDIALE. »

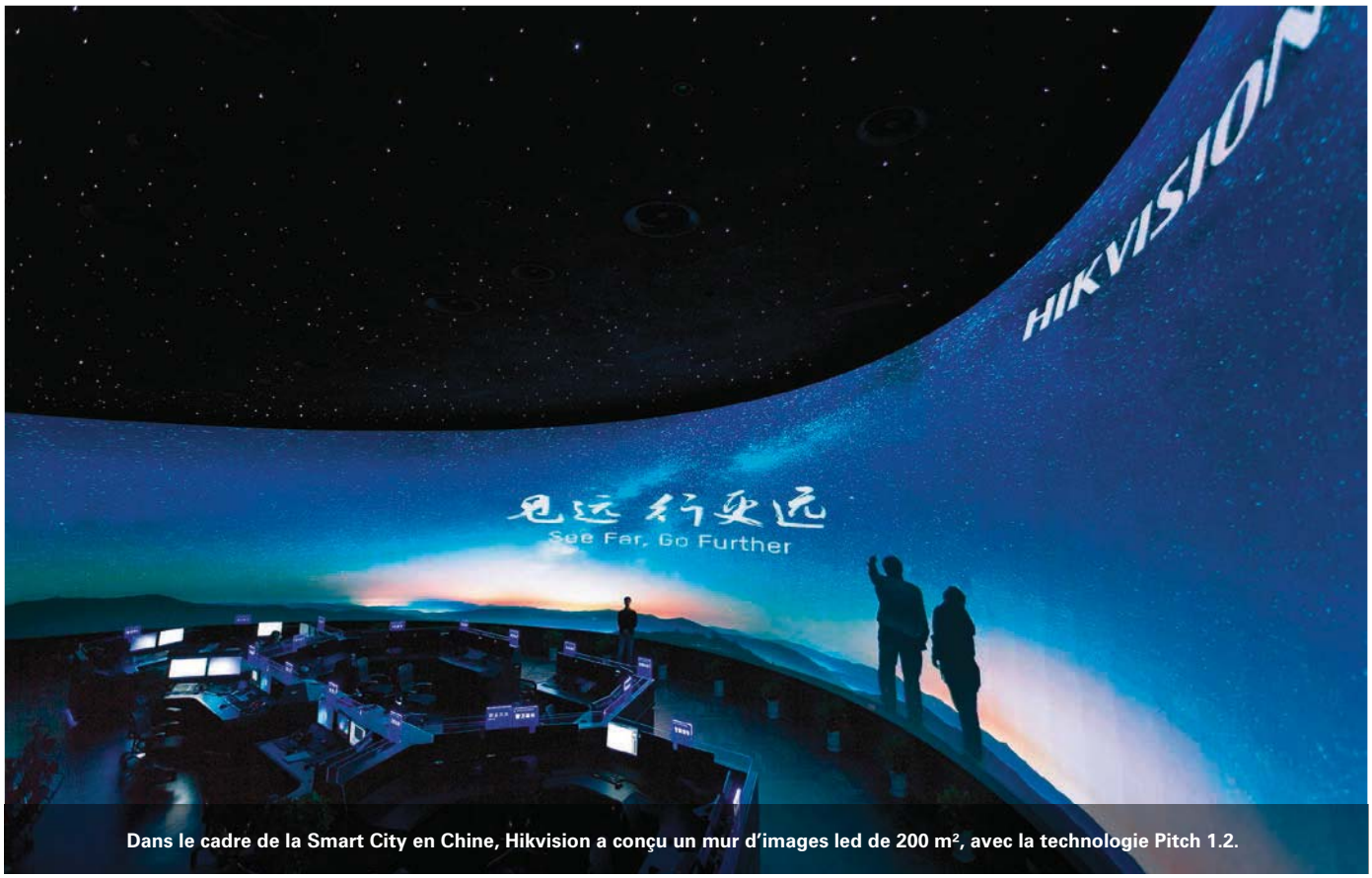
« Le cœur de l'activité de Two-i est la vision par ordinateur. C'est-à-dire l'analyse des flux vidéo dans leur totalité. Cette analyse intelligente des flux vidéo a naturellement des applications dans la sécurité. On peut faire la différence entre une personne et un animal, de jour comme de nuit, distinguer un homme d'une femme, détecter du maraudage, la formation de foule, analyser des émotions ou le rythme cardiaque d'une personne, détecter des expressions liées à la douleur… Nous avons ainsi conçu un véritable outil de sécurité qui vient directement se connecter sur le flux des caméras existantes du site. Efficace même sur de très longues distances, il peut fonctionner avec des caméras standards, sans qu'il soit nécessaire d'en déployer d'autres, le tout en temps réel. En matière d'IA, la problématique numéro 1 est le couple précision/rappel : c'est-à-dire concevoir une solution qui soit réellement capable de voir tout ce qui se passe dans l'image, avec la détection de tous les objets. Pour y arriver, nous avons non seulement conçu nos propres algorithmes, mais aussi nos propres bases de données, primordiales en matière d'IA. Nous sommes donc capables de faire beaucoup de choses, mais pour cela il nous faudrait un cadre réglementaire plus précis et que plus de place soit laissée aux donneurs d'ordres et aux industriels pour faire des expérimentations.
La reconnaissance faciale focalise les débats, à tort selon moi, car elle ne constitue qu'une toute petite partie des possibles applications de l'IA dont la majeure partie ne pose pas de problème du point de vue du respect des libertés individuelles. »

grand nombre de données traitées automatiquement et craignent le caractère intrusif de ce traitement par l'IA.
Par ailleurs, dans le cas de la reconnaissance faciale basée sur l'IA, elle est bien plus performante que l'œil humain. Et même si les personnes sont informées, cette technologique n'est pas sans risque pour les libertés individuelles.
Il faut donc intégrer la protection des données personnelles dès la conception d'outils intelligents afin de se conformer au RGPD mais aussi pour éviter tout risque de piratage.
Autre question : que se passera-t-il si un système dit intelligent se trompe, commet une erreur ? Qui sera responsable : l'utilisateur du système ? Son fabricant ?
Dans les faits, le danger est que bien que conçue par l'homme, l'IA développe sa propre intelligence, en apprenant par elle-même. Quelle place restera-t-il à l'humain ? Il devra garder la main et avoir le dernier mot. ■

PETIT POINT DE RÈGLEMENT

On ne peut pas tout faire

Si dans certains pays, comme l'Espagne, l'IA est déjà utilisée pour reconnaître des individus, en France, ce genre d'application est très encadrée. Ainsi, une entreprise fermée au public qui veut croiser des bases d'images et un fichier pour suivre un individu, doit réaliser une étude d'impact, depuis l'entrée en vigueur du RGPD.
Il lui faudra ensuite demander l'avis de la Cnil, en expliquer les finalités du système, les moyens utilisés pour garantir la confidentialité et l'intégrité des données. Mais il y a fort à parier que la Cnil invaliderait le projet.
Dans le cas des lieux ouverts au public, c'est le Code de la sécurité intérieure qui s'applique. La mise en fonctionnement d'un dispositif de vidéoprotection est soumise à une autorisation préalable délivrée par le préfet. Pour l'analyse comportementale (chute d'une personne, objets perdus, etc.), l'autorisation préalable suffit quand la finalité du système est uniquement d'alerter en cas de situation à risque. Pour identifier des personnes, il faudrait déposer un dossier à la Cnil.



Dans le cadre de la Smart City en Chine, Hikvision a conçu un mur d'images led de 200 m², avec la technologie Pitch 1.2.

© Hikvision

Moniteurs : une importance sous-estimée

Un système de vidéosurveillance ne se compose pas uniquement de caméras, d'un logiciel, d'unités de stockage… La qualité des moniteurs qui permettront aux opérateurs de regarder les images – en direct ou en différé – est aussi très importante. Et elle est parfois négligée…

On peut évidemment visionner les flux d'images d'une installation de vidéosurveillance sur n'importe quel type d'écran à partir du moment où on souhaite les consulter sur un téléphone mobile, une tablette, un écran d'ordinateur... Cela peut se faire pour des consultations ponctuelles, comme dans le cas d'une levée de doute après un déclenchement d'alarme. Pour un usage plus intensif, plus régulier, vous devrez privilégier un moniteur conçu pour la vidéosurveillance. Un écran LCD, par exemple. Or, (trop) souvent, faute d'anticipation, de budget dédié ou par méconnaissance, les opérateurs dans les PC de sécurité sont contraints de travailler avec des moniteurs de piètre qualité. Ce que confirme José Lazaro, responsable technique chez Feeder : *« La qualité du moniteur est très importante. Ne serait-ce que pour éviter la fatigue visuelle de l'opérateur. Or, il faut bien le reconnaître, trop souvent, les moniteurs sont la partie délaissée d'une installation de vidéosurveillance. Les gens investissent dans leurs réseaux, leurs caméras, logiciels et unités de stockage et oublient que le moniteur est tout de même au cœur du système. C'est une lapalissade mais il faut le rappeler : bien voir en vidéosurveillance est absolument primordial. »*

Point de vue que partage Lumen Liu, business development manager chez Hikvision France : *« Aujourd'hui, l'évolution des caméras de surveillance passe de la résolution HD à la résolution 4MP ou même 4K, mais certains installateurs et utilisateurs sont toujours habitués à acheter des écrans bon marché via les canaux de distribution informatiques : basse résolution (moins de 1080P), angle de vision étroit (l'image peut être vue clairement uniquement si l'on se tient face à l'écran), faible luminosité. »*

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

© DR

Le moniteur SMT-403 d'Hanwha Techwin est doté d'un écran à led 40 ou 19 pouces. Il jouit d'une durée de vie de 30 000 heures et d'un temps de réponse compris entre 5 et 5,9 ms. Son taux de contraste est de 1 000 : 1 en 19'' et de 5 000 : 1 en 40''.

Un élément essentiel

Mais pourquoi le moniteur est-il si important dans une installation de vidéosurveillance ? *« Si la qualité du moniteur est trop basse, l'image ne sera pas suffisamment claire ou les couleurs de l'écran seront déformées. Quel que soit le prix de la caméra, les performances de l'ensemble du système de vidéosurveillance en seront considérablement réduites,* poursuit Lumen Liu. *Bien que le prix d'un moniteur ne représente qu'une petite partie de la valeur de l'ensemble du système de sécurité, il est véritablement l'élément central. Sans un bon, l'utilisateur final ne pourra pas visionner les images correctement. »*

Partant de ce constat, un moniteur doit répondre à certains critères. *« Chez Feeder, nous distribuions les solutions du Japonais Eizo qui fabrique des moniteurs de qualité, conçus pour les infrastructures de vidéosurveillance, depuis plus de cinquante ans,* précise José Lazaro. *Un moniteur digne de ce nom doit être doté d'une dalle mate, anti-reflets. Il doit aussi jouir de certaines caractéristiques. On privilégiera, par exemple, ainsi la technologie IPS, la plus qualitative, car elle permet de restituer le plus de couleurs, tout en étant la plus adaptée en termes d'angle de vision puisqu'elle élimine les pertes de contrastes sur les côtés de l'écran. Il fau-* ● ● ●

PAROLE D'EXPERT

JOSÉ LAZARO
Responsable technique chez Feeder

© DR

« PENSEZ À VOS OPÉRATEURS DERRIÈRE LEURS ÉCRANS ! »

« D'une manière générale, les moniteurs ne font pas toujours l'objet de la même attention que celle accordée au choix des caméras ou des unités de stockage. Nous devons donc éduquer le marché. Lorsqu'on explique à nos clients les raisons pour lesquelles disposer de moniteurs dignes de ce nom est primordial, ils comprennent assez vite. Il faut penser aussi aux problèmes de la lumière bleue et faire en sorte de s'équiper avec des moniteurs dotés d'une fonctionnalité de réduction de cette lumière. L'anti-scintillement, ou anti-flickering, est aussi très important. Ce scintillement peut apparaître sur des écrans LCD dans les basses lumières. Et certaines personnes sont très sensibles à ce scintillement qui peut les fatiguer. Il ne faut pas oublier que l'opérateur est souvent très proche des écrans. Avec de mauvais écrans, ses yeux vont se fatiguer et une dalle brillante, comme celle que nous privilégions pour nos télévisions, va fatiguer l'opérateur. »

CÔTÉ SOLUTIONS

Le haut de gamme chez Eizo

Chez Feeder, vous pourrez trouver le moniteur Eizo FDS 2340 WIP (disponible en 23 et 46 pouces). Il s'agit d'un écran IP qui se connecte directement dans l'environnement des cameras afin de décoder, de manière autonome, les flux de 16 caméras, sans avoir besoin d'une unité centrale puisqu'il suffit juste de le brancher sur le câble réseau. Ainsi, ce moniteur est dédié au seul affichage des caméras avec une interface dédiée à la visualisation. Autre atout non négligeable de ce moniteur : étant indépendant du reste de l'infrastructure, il ne constituera pas une faille cyber…

© DR

PROVISION ISR®
Now you can see!
ONE STOP SHOP
L'ACCESSOIRE IDÉAL POUR COMPLÉTER VOTRE INSTALLATION.
Moniteur écran de vidéosurveillance haute-résolution, de petite taille, ultra-fin, encastrable. Un design travaillé pour une discrétion adaptée à votre lieu : Accueil, bureau, caisse, bar ...
• Disponible en 7" ou 10"
• Ecran TFT
• Résolution HD
• Entrées : VGA, HDMI, BNC
• Boutons tactiles
• Kit d'encastrement inclus
• Angle de vision : 85°
Provision-ISR France , 65 Bis Avenue de l'Europe , 77 184 Emerainville
Tel : 01 85 90 03 90 - info@provision-isr.fr
www.provision-isr.com - www.provision-isr.fr

3 QUESTIONS À

LUMEN LIU

Business Development Manager chez Hikvision France

© DR

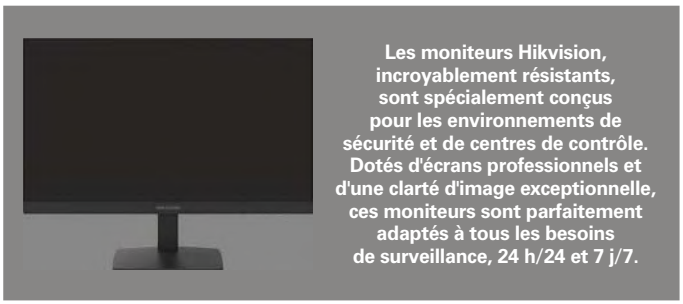
À quoi faut-il faire attention pour choisir des moniteurs adaptés à son réseau de surveillance et à ses caméras ?
Il est primordial de choisir un écran ayant la capacité de fonctionner en continu 7 jours sur 7 et 24 heures sur 24. Deuxième point important, la résolution de l'écran. Par exemple, dans les scènes complexes comme les villes et la circulation, les caméras utilisées sont dotées de la technologie 4K. Il est donc préférable d'utiliser un moniteur de même résolution.

Pouvez-vous nous présenter la gamme de moniteurs Hikvision et ses principales caractéristiques et atouts par rapport aux produits concurrents ?
Tous les moniteurs Hikvision peuvent fonctionner 24 heures sur 24, 7 jours sur 7. Ils offrent une résolution allant du Full HD à la 4K et sont disponibles dans des tailles allant du 19 au 65 pouces. Il existe de nombreuses options. Nos écrans et nos caméras ont été ajustés en couleur pour donner une reproduction plus réaliste de la scène. Les écrans 4K de Hikvision peuvent améliorer les performances globales d'un système de vidéosurveillance. En plus des moniteurs, nous proposons également des murs d'images LCD et led pour les grandes salles de surveillance ou les centres commerciaux.
Nous avons notre propre solution complète qui comprend un logiciel, un décodeur, un contrôleur, des supports et des écrans. Il s'agit, aujourd'hui, de la solution la plus rentable sur le marché.

● ● ● *dra aussi veiller à ce que le moniteur dispose de la bonne connectivité : port HDMI, Display port. Sur certains écrans Eizo, on propose même les port VGA et DVI pour qu'ils puissent intégrer dans une installation un peu ancienne... Il faut comprendre que les moniteurs ne sont pas des produits aussi basiques qu'ils en ont l'air et qu'un bon moniteur est un vrai condensé de technologies. D'autres modèles disposent d'un port USB type C, lancé par Apple, qu'on retrouve dans les ultra-portables et qui permet de réduire l'encombrement des moniteurs. »*

Des caractéristiques essentielles

Un moniteur doit être lumineux. Mais pas trop sous peine d'être à l'origine d'une fatigue visuelle pour l'opérateur. *« Il doit être doté d'une fonction qui permet d'adapter automatiquement la luminosité de l'écran en fonction de l'environnement lumineux. À l'instar de ce que peuvent faire aujourd'hui tous les smartphones,* insiste José Lazaro. *On veillera aussi à ce que les écrans ne soient pas trop brillants. Il faut éviter les dalles trop agressives pour les yeux. On pourra aussi choisir des moniteurs équipés de speakers en face avant afin de permettre à l'opérateur, d'un PC de télésurveillance par exemple, de pouvoir disposer d'un retour audio. »* Avant de poursuivre : *« Il faut raisonner en termes d'ergonomie. Dans les PC dotés de murs d'écrans, il faut choisir des moniteurs sans bords ou aux bords très réduits afin de pouvoir disposer d'une configuration multi-écrans uniforme, sans rupture entre les différents écrans. »*



© DR

Les moniteurs Hikvision, incroyablement résistants, sont spécialement conçus pour les environnements de sécurité et de centres de contrôle. Dotés d'écrans professionnels et d'une clarté d'image exceptionnelle, ces moniteurs sont parfaitement adaptés à tous les besoins de surveillance, 24 h/24 et 7 j/7.

Enfin, n'oubliez pas de demander l'avis de vos opérateurs, leur ressenti. Eux seuls pourront vous dire, si, à l'usage, tel ou tel moniteur leur convient, leur permet d'effectuer leur travail dans de bonnes conditions, sans trop de fatigue visuelle... ■

LE POINT DE VUE D'UN FABRICANT

JEAN-GUILLAUME SIMON

Pre-Sales & Technical Manager chez Hanwha Techwin France

© DR

« UN BON MONITEUR N'EST PAS UN LUXE ! »

« On constate trop souvent que certains installateurs et utilisateurs essayent de rogner leur budget pour des matériels pourtant très importants comme les moniteurs. Or, disposer de moniteurs de bonne qualité n'est pas un luxe inutile. Ne serait-ce que pour assurer un certain confort à l'opérateur devant les écrans. On doit donc veiller à ce que les moniteurs intègrent un certain nombre de caractéristiques. Premièrement, il ne faut pas oublier qu'ils vont fonctionner 24 h/24 et 7 j/7. Ils doivent donc jouir d'une durée de vie étendue. Chez Hanwha, nos moniteurs 40'' et 22'' ont une durée de vie de 30000 heures. Il faut aussi faire attention à la consommation pour qu'elle ne soit pas trop élevée. Nos moniteurs consomment 24 et 60 Watts maximum. Le contraste est aussi très important, ainsi que leur temps de réponse. L'angle de vue est aussi primordial.
Nous proposons ainsi des écrans avec un angle de vue de près de 180°. Enfin, ils doivent disposer d'une bonne luminosité. Notre gamme répond à ces critères. Par ailleurs, je tiens à souligner que, d'une manière générale, nos moniteurs sont garantis trois ans, avec la possibilité d'une extension à cinq ans pour nos partenaires Step, soit une garantie équivalente à celle que nous appliquons à nos caméras. »

IPS

Intelligent Video Analytics

VideoManager 3D Technology

Intelligent Video Management Software

La solution idéale pour la poursuite automatique des objets détectés

IPS VideoManager 3D VMS aide votre personnel de sécurité à gérer les incidents graves.

Le système vidéo suit l'objet détecté en le passant automatiquement d'une caméra à l'autre.

Pas besoin pour l'opérateur de contrôler manuellement les caméras PTZ, les opérateurs du système peuvent travailler bien plus efficacement.

Securiton GmbH
IPS Intelligent Video Analytics
www.ips-analytics.com

Inclinable, le lecteur à reconnaissance faciale FaceStation 2 est adapté aux PMS.

© DR

Reconnaissance faciale et biométrie de la main, une croissance encore timide

Bien que les applications de reconnaissance faciale sur smartphone et sur le Web aient popularisé la technologie, son utilisation pour le contrôle d'accès reste extrêmement faible. Quant aux lecteurs biométriques de la main ou des empreintes digitales, leur usage reste cantonné aux zones sensibles des entreprises.

« *Sur mille lecteurs de badge vendus dans le monde, cinq sont des lecteurs biométriques,* indique Baudoin de Genouville, directeur général de Suprema Systems. *Et sur ces cinq lecteurs, dans 95 % des cas, il s'agit de lecteurs d'empreintes digitales. La seconde technologie biométrique qui connaît une forte croissance dans le monde est la reconnaissance faciale. Ce sont sur ces deux technologies, qui présentent des caractéristiques particulièrement intéressantes pour le contrôle d'accès, que Suprema a décidé de se focaliser.* »

En contrôle d'accès, la légitimité d'une personne repose sur les facteurs d'authentification bien connus : ce que je possède (une

Grâce au dernier algorithme de reconnaissance faciale développé par Suprema, et grâce à son processeur quatre cœurs 1,4 GHz haut de gamme, FaceStation 2 offre les services de reconnaissance faciale les plus rapides au monde : jusqu'à 3000 reconnaissances par seconde !

© DR

LA PAROLE À

STEVEN COMMANDER
Director, Design In and Specification Sales chez HID Global

© DR

« QUEL QUE SOIT LE LECTEUR, LE PORTEUR DOIT GARDER LA MAÎTRISE DE SES DONNÉES »

« Les technologies biométriques restent une niche dans le contrôle d'accès, même si on perçoit une tendance très nette à la hausse. Pour l'instant, les technologies de reconnaissance faciale induisent encore trop de rejets pour être utilisées largement dans le contrôle d'accès. Ce n'est pas forcément un problème, si l'on doit si reprendre à trois fois pour allumer un smartphone. En revanche, pour le contrôle d'accès, au sein duquel les utilisateurs attendent de la fluidité, cela peut être un frein, notamment pour un accès très emprunté. Le lecteur d'empreinte multispectral (réseau veineux et empreinte digitale en surface) que nous avons développé apporte un moyen d'authentification très forte, avec un taux de faux positif très bas (0,3 %). Encore réservée aux zones sensibles des entreprises (salle informatique, laboratoire, etc.), cette technologie suscite de plus en plus d'intérêt, car elle combine la sécurité d'une forte authentification et une simplicité d'emploi, tout en étant conforme au RGPD. Toutefois, nous restons attentifs à l'évolution du marché et des technologies. »

clé, un badge, un passeport), ce que je sais (mot de passe, code) et enfin qui je suis grâce à un élément indissociable de ma personne (visage, main, empreinte, iris). Or si cette dernière couche biométrique d'identification reste très forte et ne peut ni se transmettre ni se modifier, son utilisation est à double tranchant. Facile pour l'utilisateur qui possède toujours l'élément biométrique avec lui, elle est très fiable et confirme de manière quasi certaine l'identité des personnes. En revanche, c'est une donnée permanente et durable dont on ne peut se défaire – contrairement à un badge ou à un code. Pour éviter une utilisation malveillante ou détournée des données biométriques à l'insu de son propriétaire, la Cnil – en accord avec le RGPD – a décidé que l'utilisation des systèmes biométriques doit être strictement encadrée.

Trouver le bon gabarit

L'entreprise qui souhaite utiliser un contrôle d'accès biométrique doit en démontrer la nécessité absolue en précisant ce qui justifie le recours à ce niveau d'authentification (détention de substances dangereuses, armes, manipulations d'objets à forte valeur, accès à des fonds ou à des travaux de recherche sensibles, etc.). Les systèmes biométriques utilisent des mesures de caractéristiques morphologiques qui sont mémorisées sur des gabarits. Le règlement type de la Cnil liste trois différents types de gabarits, en fonction de la façon dont les données des ● ● ●

© DR

Fujitsu PalmSecure truedentity est une solution d'authentification multifactorielle qui combine la technologie PalmSecure de numérisation des veines de la paume avec trudentity, une solution d'authentification ultra-sécurisée. Ce système permet une authentification sans équivoque et protège de manière fiable l'accès aux espaces physiques, aux systèmes ou aux informations sensibles. Fujitsu PalmSecure truedentity convient aussi bien aux services en ligne qu'aux systèmes de gestion d'identité logique ou physique de contrôle d'accès.

DU CÔTÉ DES START-UP

Keopass, la clé biométrique universelle

Keopass est une clé qui comporte un lecteur d'empreinte dernière génération, avec analyse biométrique intégrée et communications chiffrées en AES. Universelle, cette clé peut fonctionner avec n'importe quel de terminal (fixe ou mobile) équipé en Bluetooth ou en USB, et d'OS (Windows, Mac, iOS, Android, Linux, Chromebook, etc.). En fonction de la version de KeoPass, elle garantit une authentification forte aux accès logiques, avec ou sans verrouillage automatique, aux accès physiques (bâtiments, équipements, etc.) ou les deux. Simple à déployer et à utiliser, elle ne nécessite aucune installation d'applications ou de pilotes. La clé biométrique KeoPass existe en deux versions : accès logique uniquement (génération et saisie de mots de passe à partir des empreintes digitales) ou accès logique et physique (via lecteur RFID/NFC existant ou passerelle BLE dédiée) avec sécurité biométrique intégrée. La clé Keopass est conforme aux recommandations de l'Anssi et de la Cnil pour le renforcement de vos politiques de mots de passe dans le cadre de la RGPD notamment.

© DR

Déployé dans de plus en plus d'aéroports, le système de contrôle d'accès par reconnaissance faciale Parafe est aussi celui dont l'acceptation est la meilleure parmi la population française.

© DR

Le lecteur d'empreintes digitales iCLASS SE RB25F est un lecteur/contrôleur robuste, polyvalent et puissant qui répond aux besoins élevés en matière de contrôle d'accès physique. Sa précision et sa rapidité de lecture des empreintes offrent un confort inégalé pour les utilisateurs : en moins d'une seconde, l'empreinte est vérifiée, réduisant considérablement les délais de traitement et donc les attentes qui accompagnent souvent d'autres solutions biométriques. Grâce à son capteur multispectral, le lecteur iCLASS SE® RB25F permet de capturer des images à la fois à la surface et sous la surface de la peau, de sorte que tous les types d'empreintes digitales puissent être lus rapidement et de manière fiable quelles que soient les conditions météorologiques (humide, sec, etc.) ou l'aspect du doigt (sale, ridé, etc.). Ce lecteur intègre également une détection du vivant pour éviter la fraude au doigt coupé. Il valide aussi en temps réel que l'empreinte digitale n'est pas falsifiée. L'appareil est également livré avec la fonctionnalité de « doigt sous la contrainte » (seconde empreinte digitale affectée à une fonction « alerte » par exemple), ainsi qu'une protection optique intégrée qui envoie une alarme automatique en cas de tentative d'arrachement du lecteur.

© DR

● ● ● personnes sont stockées. Dans le gabarit de type 1, l'individu concerné est le seul à détenir le gabarit – et donc ses données personnelles – sous la forme d'un badge. Pour le type 2, le gabarit est stocké dans une base de données collective, mais les données sont cryptées. Elles ne pourront être lues que sur intervention du salarié concerné, via la présentation d'un badge ou le renseignement d'un mot de passe. Enfin dans le type 3, les gabarits de tous les salariés sont contenus dans une base centralisée, et le salarié n'a pas à présenter de badge ou de code d'accès pour s'authentifier. Selon la Cnil, le gabarit de type 1 est à privilégier, car il limite le risque d'accès non autorisé aux données biométriques de la personne. « *Le système de stockage sur badge individuel,* remarque Baudoin de Genouville, *favorise la technologie d'empreintes digitales. Une empreinte nécessitera 300 octets et un visage en infrarouge trois kilos octets s'il est compressé. Non compressé, il faudra compter plus de 90 kilos octets, et donc envisager un gabarit de type 3.* »

LA CNIL A RETOQUÉ DEUX PROJETS DANS DES LYCÉES

Le 17 octobre dernier, les membres de la Cnil se sont prononcés sur une expérimentation qui prévoyait le recours à la reconnaissance faciale à l'entrée de deux lycées de la région Paca.
La solution envisagée avait fait l'objet d'une analyse d'impact relative à la protection des données (AIPD) par la région Paca et les deux lycées expérimentateurs. Après un examen attentif du projet, la Cnil a considéré que ce dispositif concernant des élèves, pour la plupart mineurs, dans le seul but de fluidifier et de sécuriser les accès n'apparaissait ni nécessaire ni proportionné pour atteindre ces finalités.
En effet, les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge.

Reconnaissance de la main en perte de vitesse

Les lecteurs de reconnaissance du contour de la main – essentiellement le lecteur Handkey – semblent en perte de vitesse. Ils ont pourtant une utilisation encore assez importante pour l'accès aux restaurants scolaires avec les solutions d'Alise. Une autre utilisation a émergé avec les situations de migrations internationales : l'accès dans des camps de réfugiés. Il a ainsi été mis en place au camp d'accueil provisoire de Calais. Fujistu a pour sa part un lecteur des veines palmaires qui trouve des débouchés dans les data centers et des zones hautement sécurisées.

Lecteurs d'empreintes digitales à la hausse

« *En cas de besoin de gabarit de type 1, c'est une solution idéale, car à peine 0,1 % de la population possède des empreintes digitales qui ne peuvent pas être lues par un lecteur Suprema,* souligne Baudoin de Genouville, le directeur général de Suprema. *L'empreinte ne change pas au cours du temps et le nombre de rejet est très faible. Aujourd'hui, on trouve des lecteurs très robustes qui peuvent être placés en extérieur.* »

La reconnaissance faciale, tendance mais encore peu utilisée

La reconnaissance faciale est séduisante pour son côté « Frictionless ». Toutefois, elle reste encore lente (de deux à quatre secondes par personne, selon le lecteur) et induit beaucoup de rejets. C'est aussi une technologie encore chère, autour de 1 000-1 500 euros le lecteur. De plus, elle nécessite de bonnes conditions de luminosité et il n'y pas encore de lecteur avec des certifications IP (65 ou 67) pour un usage extérieur. ■

SUR LE TERRAIN

Reconnaissance faciale, 60 % des Français attendent un cadre protecteur et clair

Quelle perception ont les Français de la reconnaissance faciale ? En novembre dernier, l'institut Ifop a mené une enquête pour le think tank Renaissance numérique, auprès d'un échantillon de 2 000 personnes représentative de la population française. Il en ressort une forte notoriété de la reconnaissance faciale, malgré un faible déploiement des usages : 88 % des répondants ont déjà entendu parler de la reconnaissance faciale, et 57 % estiment savoir précisément de quoi il s'agit. Quand ils sont usagers, les sondés ont plutôt confiance dans ces technologies, avec des taux de confiance supérieurs à 70 % quel qu'en soit l'usage. À noter que les usages qui reçoivent le plus d'avis favorables, correspondent à ceux les plus déployés, à savoir le contrôle aux frontières et le déverrouillage du smartphone ou d'applications sur celui-ci. Il semblerait que la perception positive repose avant tout sur la praticité de ces technologies. Si l'acceptation est bonne pour des applications relevant de la police et de la justice, respectivement 70 % et 65 % de taux de confiance, les Français sont plus méfiants vis-à-vis des usages commerciaux : seuls 44 % des sondés estiment ces usages acceptables, et à peine 38 % estiment avoir confiance dans les entreprises privées pour utiliser de manière responsable la reconnaissance faciale. Enfin, la protection de la vie privée et l'atteinte aux libertés fondamentales sont les principales inquiétudes. 60 % des Français expriment une attente forte pour un cadre protecteur clair et estiment que cette mesure est prioritaire et 22 % souhaitent un moratoire avant toute décision de déploiement tant que les conséquences de la technologie n'ont pas été mesurées. Les usages n'étant pas encore très déployés, cette enquête invite ainsi à prendre le temps d'un débat.

© DR

Suprema BioLite N2 est un terminal Suprema externe d'empreintes digitales de deuxième génération qui fournit des fonctionnalités complètes de contrôle d'accès et de temps/présence, basées sur la nouvelle plateforme de technologie et de sécurité biométrique de Suprema. BioLite N2 offre des performances et une sécurité de pointe grâce au tout dernier algorithme d'empreintes digitales de Suprema, associé au plus performant capteur d'empreintes digitales au monde. Abrité dans son boîtier IP67 robuste, BioLite N2 ajoute une pointe de flexibilité à la conception de systèmes grâce à la technologie de lecture RFID multiCLASS.

Votre contact Républik Sécu :
Marion Latard
06.58.02.95.77 - m.latard@republik-mdc.fr
https://republik-mdc.fr

RÉPUBLIK SECU

Serrures : autonomes et numériques

Dans le monde de la serrure, la tendance est plus que jamais à l'autonomie en énergie, au sans fil et à la dématérialisation des clés. La preuve !

SMARTHANDLE AX – SIMONS VOSS

SERRURE NUMÉRIQUE

La nouvelle plaque-béquille SmartHandle AX de Simons Voss est le premier produit de la génération AX (Advanced Xchange).
Sa structure modulaire, son design particulièrement adapté aux bâtiments modernes et son autonomie optimisée font de la SmartHandle AX LA solution pour les portes intérieures. Les utilisateurs pourront également bénéficier des fonctionnalités Bluetooth Low Energy (BLE) et Phone2Door disponibles en 2020.
La plaque-béquille SmartHandle AX s'appuie sur des contrôleurs modernes ultra-performants (32 bits) et sur une architecture de sécurité intrinsèque (ISA), basée en permanence sur le «Secure Element» qui constitue l'ADN du produit. Le nouveau système d'exploitation Axeos facilite la programmation des cartes ou des transpondeurs qui s'effectue en quelques secondes.
Cette nouvelle béquille sur rosace complète la gamme des poignées SmartHandle Simons Voss et facilite le remplacement des poignées mécaniques existantes, également sur rosace.
La modularité, une robustesse dédiée pour un usage intensif, la compatibilité avec les produits de première génération, l'installation sans perçage, une autonomie plus importante (jusqu'à 300000 manœuvres), une certification sur les portes coupe-feu et la possibilité de manipuler la béquille et de programmer les accès à l'aide d'un smartphone via Bluetooth Low Energy «BLE Ready» font de la SmartHandle AX un produit évolutif et pérenne.

© DR

AIRKEY – EVVA

POUR UNE GESTION DES CLÉS INGÉNIEUSE

Le cylinder AirKey permet d'ouvrir les portes avec son smartphone, d'attribuer des clés par SMS et d'organiser très simplement en ligne l'ensemble de votre installation de fermeture.
Les avantages d'AirKey : envoyer des clés sur des smartphones par internet, application et gestion online gratuites, idéal pour les petites installations de fermeture jusqu'aux installations complexes, qualité de produit et sécurité des données d'Autriche
Le cylindre AirKey convient pour l'intérieur et pour l'extérieur. Équipé d'une protection anti-perçage et anti-arrachage, d'un frein de rotation et d'un «Secure Element» intégré pour la sauvegarde sûre des données, il est le produit central de la sécurité au sein du système AirKey. Grâce à sa conception modulaire, le cylindre peut être monté et adapté en longueur de manière très simple.
La gamme est complétée par : le cylindre Hybrid qui combine électronique et mécanique ; la batteuse à came AirKey pour les cases postales, les armoires de classement et les armoires à pharmacie ; le lecteur mural AirKey (utilisable à l'intérieur et à l'extérieur) qui, combiné à son unité de contrôle, est approprié pour la commande fiable d'éléments de verrouillage électroniques de portes coulissantes et battantes, en tant que commande d'ouverture électronique.

© DR

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

© DR

ILOQ S10 – ILOQ

LE VERROUILLAGE ÉLECTRONIQUE GREENTECH SANS BATTERIE

iLOQ S10 est un système de verrouillage autonome en énergie, strictement sans câblage et sans batterie, ni dans la clé ni dans le cylindre. Ce système révolutionnaire récupère l'énergie générée lors de l'insertion de la clé. Cette solution écologique et économique ne nécessite aucune maintenance et minimise les coûts d'exploitations des serrures. iLOQ S10 résout les problèmes de copie ou de perte de clés. La programmation des clés et des cylindres s'effectue depuis le logiciel iLOQ S10 Manager (ajout, modification et suppression des droits d'accès). Les clés perdues peuvent être blacklistées, puis reprogrammées si elles sont retrouvées. En bref, iLOQ remplace les organigrammes de clés mécaniques par une gestion électronique des accès.

Communication sécurisée : identifiant, mot de passe et Token administrateur pour sécuriser la connexion ; cryptage des données : chiffrement AES-256 de toutes les communications ; autorisation de déverrouillage : authentification réciproque entre le cylindre et la clé.
Capacité : 1 000 000 cylindres, 32 000 clés, 1 000 administrateurs ; 16 000 derniers événements stockés par cylindre ; etc.

→ CARACTÉRISTIQUES :

- Cylindre modulaire (30 à 100 mm) et reprogrammable.
- Certifié EN15684, Vds et SKG***.
- Remontée et stockage des 500 derniers événements (sans pile).
- Protocole sécurisé SHA-1 pour la communication entre la clé et le cylindre.
- Programmation et gestion des accès, via le logiciel SaaS, iLOQ S10 Manager, hébergé sur serveur cloud ISO/IEC 27001 : 2013.

SMARTAIR – JPM

NOUVEAU CYLINDRE À BOUTON

Ce nouveau cylindre à bouton SMARTair de JPM est un système de verrouillage sans fil conçu pour tout type de portes (verre, aluminium ou bois) pour lesquelles l'installation d'une béquille est difficile. Il permet de remplacer rapidement un cylindre mécanique par un cylindre avec accès électronique contrôlé en temps réel, sans perçage, ni câblage.
Partie intégrante du système de contrôle d'accès SMARTair, le nouveau cylindre à bouton est une solution intelligente à lecteur RFID intégré, plus résistante encore aux intrusions, compatible avec la solution de contrôle d'accès via smartphone SMARTair Openow. Il peut être combiné aux autres solutions SMARTair pour faciliter la gestion d'accès et la circulation dans les lieux de travail. Alimenté par piles, il permet de choisir entre plusieurs systèmes, ou même de combiner plusieurs options : Wireless Online (autonome en temps réel sans fil), Update On Card (autonome en réseau virtuel, mise à jour par badge), Offline (autonome hors ligne), Stand Alone (autonome sans poste d'administration).

© DR

Les bornes conçues par Amco protègent le périmètre de la tour Eiffel.

© Getty images

Les obstacles physiques : pas si rustiques que ça

Plus que jamais, les obstacles physiques sont des éléments incontournables pour sécuriser certains sites et lutter contre les tristement célèbres voitures-béliers. Pour cela, ils doivent faire preuve d'une résistance éprouvée et être, malgré leur robustesse, l'objet de certaines attentions.

Les obstacles physiques, pour extérieur ou intérieur, ont le vent en poupe. Qu'il s'agisse de herses, de bornes escamotables, de roadblockers… ils permettent de limiter les flux de personnes ou de véhicules, de délimiter des zones interdites aux voitures, d'interdire l'accès physique à un site. *« Jusqu'à il y a peu, les obstacles physiques comme les bornes, escamotables ou pas, étaient plutôt utilisés dans une logique de circulation, pour délimiter une zone interdite aux véhicules, par exemple, et réservée aux piétons. Et se fondaient dans leur environnement,* explique David Andrieux, responsable secteur chez Faac France. *Aujourd'hui, et compte tenu du contexte que nous connaissons tous, les gammes évoluent et sont complétées par des produits plus lourds, plus résistants aux impacts d'une voiture-bélier. On se situe donc plus dans une logique de lutte contre le terrorisme et de sécurisation de zones. »*

Un marché porteur

Depuis les attentats qui ont frappé la France, les obstacles physiques, qui étaient jusqu'alors principalement utilisés pour délimiter des zones dans les villes ou protéger des bâtiments officiels et autres ambassades…, se répandent dans les villes pour lutter contre les voitures-béliers.

Un des exemples les plus célèbres est évidemment la tour Eiffel puisque, pour protéger le public d'une éventuelle attaque terroriste, outre la paroi de verre qui ceint désormais le monument, a été installé un dispositif de protection anti-véhicule-bélier avec l'implantation de bornes sur les deux axes routiers qui bordent la tour.

« Les obstacles physiques étaient très appréciés dans les villes pour créer des zones piétonnes, par exemple, poursuit David Andrieux. *Et les obstacles durcis, plus lourds et résistants étaient plutôt réservés aux sites Seveso, aux OIV, à certains*

CÔTÉ SOLUTIONS

FirstLane d'Automatic Systems

Le FirstLane est un couloir rapide qui s'intègre parfaitement dans n'importe quel type d'environnement. La gamme FirstLane comprend deux modèles : le FirstLane 960 et le FirstLane 970. Tous les deux offrent les mêmes caractéristiques et fonctionnalités. La seule différence concerne la largeur de passage. Avec son système de détection Diras (Detection Infra Red Automatic Systems), FirstLane peut suivre les utilisateurs tout au long du couloir, en assurant leur sécurité pendant l'ouverture et la fermeture des obstacles. Grâce à ses rayons IR multidirectionnels et algorithmes prédictifs, il analyse et anticipe la taille, la position, la vitesse et la direction de l'utilisateur à l'intérieur du couloir. En outre, il reconnaît facilement les fraudes et les passages intrusifs.

© DR

bâtiments officiels. Aujourd'hui, on est clairement dans une logique de déploiement pour répondre à la menace terroriste et sécuriser l'espace public. » Compte tenu des besoins exprimés actuellement, de nombreux fabricants, à l'instar de Faac, complètent leurs gammes avec des produits plus résistants afin de pouvoir adresser ces nouveaux marchés.

Pas si simples à installer

Les obstacles physiques installés en périphérie ou en périmétrie des sites sont des matériels robustes. Normalement très résistants. Mais cela ne veut pas dire qu'ils ne requièrent pas un minimum d'attention comme le conforme Loup Blanpain de Saint-Mars, gérant de Travaux Généraux de l'Ouest (TGO) : *« Les obstacles physiques pour extérieur sont des solutions rustiques, robustes qui nécessitent cependant un minimum de compétences en matière d'installation et de maintenance. Ainsi, lors de l'étude du site et l'analyse des risques préalables à l'installation, il faudra prendre en compte certains points qui vont avoir une influence sur le choix du matériel. Je pense, par exemple, à la configuration de la voirie. Si la voie d'accès au site est droite, elle favorisera la prise de vitesse du véhicule. Il faudra donc déployer des moyens, comme des chicanes fixes, qui permettront de casser la vitesse du véhicule. »*

Il faudra aussi faire attention au type d'utilisation et au fonctionnement de l'obstacle : un usage domestique nécessite des solutions moins lourdes que la protection d'un site industriel ou tertiaire. On veillera aussi, pour les solutions qui sortent du sol, à mettre en place une signalisation adéquate avec asservissement pour, d'une part, avertir du fonctionnement ● ● ●

LE POINT DE VUE D'UN FABRICANT

JÉRÔME MUROLO
Responsable commercial chez Amco

© DR

« NOUS FAISONS SUBIR À TOUTES NOS SOLUTIONS UN DOUBLE CRASH TEST. »

« Amco, fondée en 1992, conçoit, développe, fabrique et teste des obstacles physiques depuis 2005. À l'origine, notre cœur de métier c'était les bornes automatiques ou mécaniques, les bornes escamotables pour les forains et les bornes citoyennes, devenues aujourd'hui les bornes arrêt-minute. En 2002, nous avons fourni à la tour Eiffel huit bornes automatiques de contrôle d'accès. Puis, suite aux attentats de Londres en 2005, nous avons été sollicités pour développer une borne escamotable permettant de sécuriser les accès de l'esplanade de la tour Eiffel. Nous avons ainsi conçu et développé, à partir d'un cahier des charges précis, une première borne résistant à un impact d'un véhicule de 6,8 tonnes lancé à 80 km/h. Deux lots de cinq de ces bornes ont ensuite été déployés, en 2006, sur le site. Depuis, nous avons étoffé notre gamme de bornes puisqu'elle se compose désormais de huit bornes automatiques qui ont toutes subi avec succès nos doubles crash tests. C'est-à-dire qu'elles fonctionnent toujours après le premier impact. Il n'est pas très compliqué de détruire un véhicule avec une borne escamotable. Mais il est beaucoup plus complexe de concevoir un produit qui permettra de maintenir le niveau de sécurité d'un site après un premier impact ou un second. »

CÔTÉ SOLUTIONS

Jusqu'à 80 km/h chez Faac

Faac propose deux bornes escamotables – modèles J355 HAM30 J355 HAM50 – très similaires à première vue. Elles ne se différencient, principalement, que par leur capacité d'arrêt. La J355 HAM50 (certifiée selon les normes PAS 68 : 2013 et IWA 14-1 : 2013) est en mesure d'arrêter un camion de 7,5 t, lancé à 80 km/h, dans des configurations à une seule unité. La J355 HAM30 (certifiée selon la norme ASTM F2656-07), quant à elle, peut stopper un véhicule de 6,8 t lancé à 50 km/h, dans des installations à une seule unité.

© DR

LE POINT DE VUE D'UN FABRICANT

PHILIPPE LOUBOUTIN
Commercial grands comptes IDF-Ouest chez Magnetic Autocontrol

© DR

« RAPIDITÉ ET ESTHÉTISME. »

« Nous sommes une filiale du groupe Faac. Nous concevons et commercialisons des barrières pour véhicules et obstacles pour piétons dans le monde entier. Des marchés particulièrement porteurs en ce moment. Nos produits sont destinés au contrôle des véhicules et des piétons pour des sites sensibles comme les aéroports, les ports, les stades et les métros. Notre gamme se compose d'obstacles physiques, de barrières levantes, de bornes escamotables, de couloirs rapides, de portillons motorisés, de tripodes… Outre la vente de produits, nous sommes capables de réaliser une expertise des sites, d'étudier leurs risques afin de leur proposer la solution la plus pertinente. En effet, comme dans le contrôle d'accès, en matière d'obstacles physiques, il faut savoir arbitrer entre la sécurité et la fluidité des flux. Un tripode, par exemple, sera moins rapide qu'un couloir rapide. Il faut aussi tenir compte des contraintes du site et de la population qu'il accueille. La tendance actuelle en matière d'obstacles physiques est clairement à la rapidité de passage et à un travail sur l'esthétisme. C'est cette approche qui nous a conduit à concevoir nos couloirs rapides FlowMotion avec le designer italien Pininfarina. »

CÔTÉ SOLUTIONS

FlowMotion de Magnetic Autocontrol

FlowMotion, le dernier-né de la gamme de couloirs rapides de Magnetic Autocontrol, a été conçu en partenariat avec un des grands noms du design mondial : Pininfarina. Fabriqué en polymères, et non en Inox, FlowMotion se caractérise donc par un design ultra-soigné mais aussi par son caractère « durable » car il est entièrement recyclable.

© DR

CÔTÉ SOLUTIONS

Herse escamotable lourde TKB chez TGO

La herse TKB est composée de robustes poinçons d'acier pleins d'épaisseur 20 mm espacés de 200 mm qui sortent du sol de 450 mm et agissent comme un obstacle escamotable, pour empêcher le passage des véhicules non autorisés. Quand les pointes sont sorties, la herse peut bloquer tout type de véhicules jusqu'à une vitesse d'environ 80 km/h.

© DR

● ● ● de la borne, par exemple, et, d'autre part, faire fonctionner la borne ou la herse en coordination avec le portail.
« Lors de l'installation, on veillera aussi à la pente de la voirie, ajoute Loup Blanpain de Saint-Mars *pour s'assurer que le drainage se fait bien ou pour éviter que la tranchée ou le trou dans lequel disparaît l'obstacle ne soit rempli par des déchets, des feuilles mortes, de l'eau stagnante… car l'entretien de ce type de solution est assez complexe. »*

Rustiques mais complexes

Lors de l'installation, on fera aussi très attention à l'environnement dans lequel vont être installés les obstacles. En surface et en sous-sol. Il faut adapter le type d'obstacle aux réseaux présents dans l'environnement. Qu'il s'agisse des réseaux pluviaux, téléphoniques, gaz ou électriques. *« L'installation de certaines bornes peut nécessiter des travaux de génie civil à des profondeurs assez importantes. Jusqu'à deux mètres pour certaines bornes,* poursuit le gérant de TGO. *Si on ne prend pas certaines précautions, on peut donc tomber sur un réseau enterré et l'abîmer. »*
Un autre conseil : pensez à l'environnement immédiat de la borne, de la herse… Il serait dommage de vous équiper avec un système coûteux et résistant, alors que le reste de votre enceinte ne serait constitué que d'une simple barrière… qui sera très vite identifiée comme la faiblesse de votre installation périmétrique physique.
Respecter certaines règles en matière de maintenance est également primordial. Ces matériels sont plus coûteux qu'une simple barrière automatique. Par ailleurs, ils induisent des coûts en matière de génie civil. On veillera donc à bien les ● ● ●

CÔTÉ SOLUTIONS

ALE A25-100-C80 : le « monstre » d'Amco

En matière de borne escamotable, la ALE A25-100-C80 est sans doute ce qui se fait de mieux actuellement. En effet, cette borne du Français Amco a subi, comme ses petites sœurs, un double crash test avec un camion de 12 tonnes lancé à 80 km/h. Elle a non seulement stoppé le véhicule mais aussi fonctionner à nouveau. Du jamais vu !

© DR

LE POINT DE VUE D'UN FABRICANT

DAVID ANDRIEUX
Responsable secteur chez Faac France

« LA MAINTENANCE EST TRÈS IMPORTANTE. »

« Ces matériels ont un coût certain. À l'achat, d'une part, mais aussi lors de leur installation en raison des travaux de génie civil qu'ils nécessitent. Par conséquent, il faut les maintenir correctement afin d'éviter qu'ils ne se détériorent trop vite. Les obstacles escamotables sont enterrés. Ils requièrent donc une maintenance curative, ne serait-ce que pour nettoyer le système de drainage qui peut être rempli de feuilles mortes, de saletés et autres détritus. Il faut sortir la borne au moins une fois par an pour nettoyer le puits perdu. Par ailleurs, lors du choix du matériel, on veillera à choisir une solution adaptée à la population du site. Sur un site Seveso, chez un OIV…, on peut déployer une solution un peu contraignante en matière de gestion des flux. Les gens y acceptent les règles de sécurité et en comprennent le bien-fondé. En revanche, sur un site tertiaire ou industriel, on rencontre parfois des populations qui respectent moins les règles, feront le "petit-train", seront pressées… On choisira une solution qui permet d'assurer une fluidité suffisante pour que l'obstacle ne devienne pas une contrainte. »

9ème édition
Gala Directeurs Sécurité
JEUDI 6 FÉVRIER 2020
Au Pavillon d'Armenonville

Thématique :
LA PLACE DU DIRECTEUR SÉCURITÉ DANS LE CONTINUUM DE SÉCURITÉ
Rencontrez et échangez avec près de 250 Directeurs de la Sécurité/Sûreté de grandes entreprises publiques et privées lors d'une soirée d'exception
Au Gala 2019 ils étaient :
412 participants
18 500 personnes sur les réseaux sociaux
www.gala-securite.com
#GalaSECU
PARTENAIRE MÉDIA psm
UN ÉVÉNEMENT
PARTENAIRE WEB MÉDIA
A L'INITIATIVE DE
Agora Fonctions
AGORANEWS SECURITE
Agora des Directeurs de la Sécurité

2 QUESTIONS À

LOUP BLANPAIN DE SAINT-MARS

Gérant de Travaux Généraux de l'Ouest

© DR

Quels sont les points de vigilance quand on installe un obstacle physique ?
Malgré la résistance éprouvée de ce type de matériel, on doit veiller à respecter certaines règles d'installation – car mal posé, l'obstacle durera à peine cinq ans – et de maintenance. Par ailleurs, il ne faut pas oublier que les obstacles escamotables vont être enterrés. Donc exposés, non seulement aux intempéries, mais aussi à l'humidité du sol. Ces matériels doivent donc être protégés contre la corrosion, non seulement pour leurs composants externes, mais aussi pour tout ce qui est enterré.

Lors de l'utilisation de ces matériels, à quoi doit-on faire attention ?
Sur les herses, par exemple, il y a de nombreux points de cisaillement et des zones de pincement. Il faut que ces zones soient protégées afin d'éviter qu'un pied ne soit malheureusement coincé dans cette zone lors de la fermeture de la herse. On veillera aussi à installer un feu rouge-vert. En cas d'incident, le franchissement du feu rouge permet de dédouaner l'exploitant du site.

● ● ● entretenir. *« Ce sont des matériels qui peuvent avoir des rythmes de fonctionnement assez élevés,* conclut Loup Blanpain de Saint-Mars. *On doit donc les vérifier au moins deux fois dans l'année. Cela suppose de démonter le système, de sortir la borne, pour vérifier l'état de l'installation. Il faudra à cette occasion fermer la voie. On ne peut donc pas se permettre d'avoir un obstacle capricieux, fonctionnant mal et nécessitant d'incessantes inspections ou réparations. »* ■

CÔTÉ SOLUTIONS

Barrière HD3000 de Delta Scientific

La barrière HD300 de Delta Scientific est capable de stopper net un véhicule 6,8 tonnes lancé à 80 km/h. Autre atout, elle est capable d'effectuer 1 million de cycles sans tomber en panne. Après une ouverture qui se fait en 1,5 seconde, lors de l'impact, la barrière ne bouge pas et détruit le véhicule, lui causant de graves dommages. La barrière pénétrant d'1,80 m dans la partie avant du véhicule, jusqu'à l'habitacle. Les fondations ont une profondeur de 61 cm, ce qui réduit les problèmes liés au passage de tuyaux sous-terrains, lignes électriques, fibres optiques ou autres.

© DR

LE POINT DE VUE D'UN INTÉGRATEUR

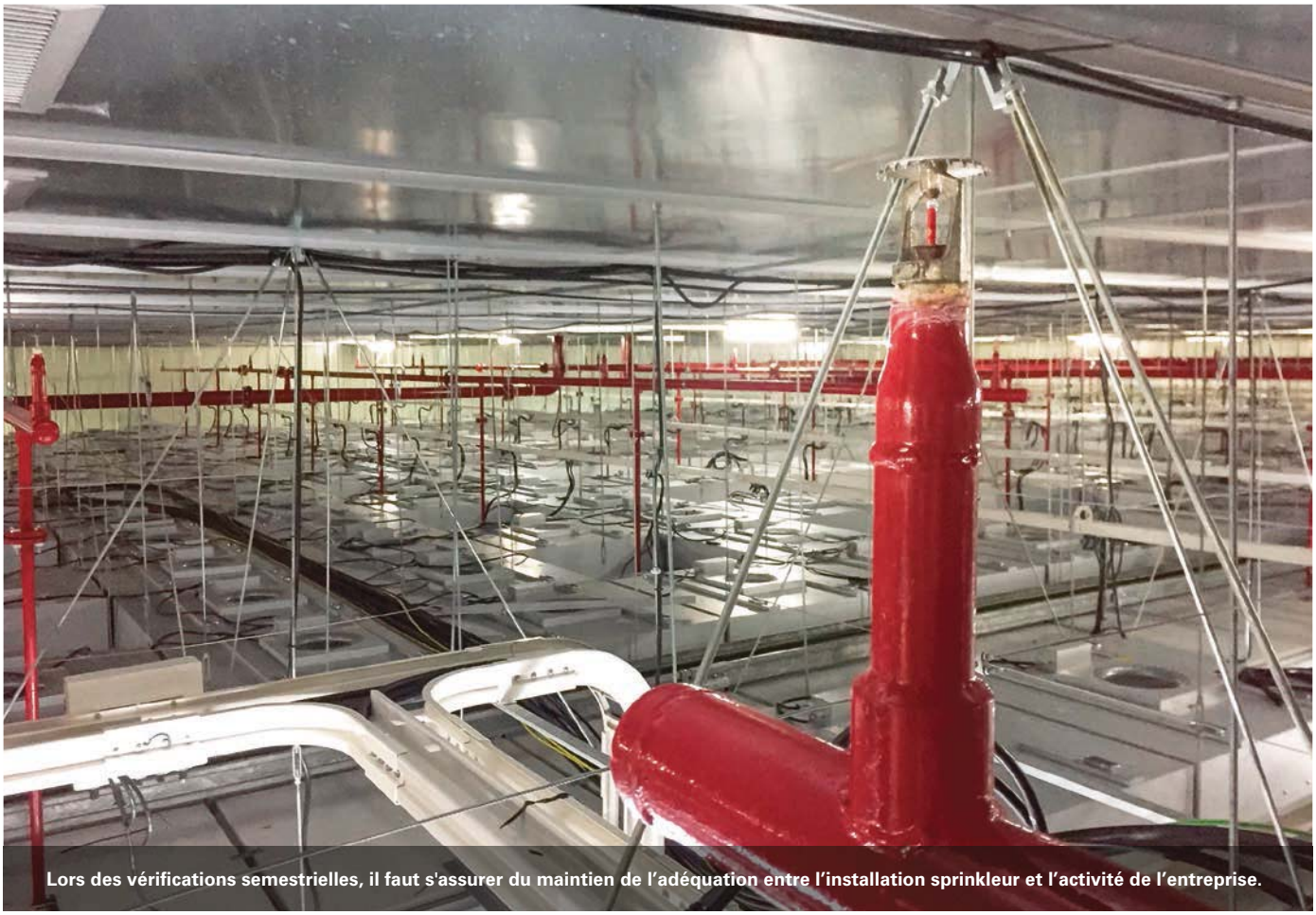
FRANÇOIS VÉDRINE
Directeur général de DEF Sûreté

© DR

« PRIVILÉGIER PLUSIEURS NIVEAUX D'OBSTACLES PHYSIQUES. »

« Les obstacles physiques s'inscrivent dans une stratégie de sécurisation qui vise à ralentir la personne malveillante et protéger des zones sanctuarisées. Nos clients cherchent un intégrateur capable de leur proposer une approche globale de la sécurité. C'est-à-dire un interlocuteur unique qui peut associer des solutions de sécurité électronique – contrôle d'accès, vidéosurveillance, détection d'intrusion – à des solutions de protection physiques comme les barrières et autres obstacles, immatériels ou pas. Afin de choisir les obstacles physiques les mieux adaptés, il est impératif de réaliser une étude du site, de sa topographie, de son environnement et des risques auxquels il pourrait être amené à faire face. On pourra ainsi privilégier plusieurs niveaux d'obstacles physiques – clôtures renforcées, bornes, herses, couloirs rapides, etc. – associés à des moyens électroniques. Il faut aussi raisonner en termes d'homogénéité. Il paraît évident qu'il serait aberrant de se doter d'une clôture renforcée de 2,5 m de haut et de l'associer à un portail d'1 m. On doit raisonner logique de hauteur, logique de performance. Ensuite, on veillera à être vigilant sur la maîtrise des flux et la conception des endroits qui permettent d'accéder au site. Enfin, il faut s'adapter à la culture sécurité de l'entreprise. Elle est très importante. Sur des sites militaires, chez des OIV, les personnels seront plus à même de se plier à des règles et procédures de sécurité strictes et de les respecter. »

ARD
www.ard.fr
La sûreté
c'est bien plus
qu'une porte à
équiper
ARD s'appuie sur son expertise pour trouver la solution adaptée à vos besoins et vous accompagner tout au long de votre projet.
Fabrication Française
depuis plus de 35 ans
Une société
membre du groupe
vitaprotech
www.ard.fr
contact@ard.fr
+33 (0) 492 525 800



Lors des vérifications semestrielles, il faut s'assurer du maintien de l'adéquation entre l'installation sprinkleur et l'activité de l'entreprise.

© Getty images

Sprinkleurs : une extinction à l'efficacité éprouvée

Les sprinkleurs sont un des moyens d'extinction les plus fiables. Mais pour que cette efficacité soit garantie, ils doivent être installés et maintenus selon des règles précises.

Depuis 1881, les sprinkleurs ont fait la preuve de leur efficacité. Et ce, grâce au travail de professionnels comme les membres du Groupement français des installateurs de sprinkleurs (GIS) qui fabriquent, installent, testent, maintiennent… les sprinkleurs. Avec succès, puisque comme le rappelle sur son site le GIS, la France connaît le meilleur taux de performances pour ce mode d'extinction, parmi tous les États membres. Dans 85 % des cas en effet, le déclenchement de seulement cinq têtes de sprinkleurs aboutit à la maîtrise totale de l'incendie déclaré. Cette méthode d'extinction est très efficace avec un taux européen global d'extinction de 98 %, selon l'INRS.

Une installation sprinkleurs se compose d'une source d'eau constituée d'une ou plusieurs pompes qu'alimentent des réserves d'eau ; d'un ou plusieurs postes de contrôles (qui permettent un découpage en zone de la protection), de canalisations et de têtes sprinkleurs.

DES RÉFÉRENTIELS FONDAMENTAUX

- **La règle Apsad R1 : la plus couramment utilisée**
- **La norme Afnor NF EN 12 845**
- **Les règles du CEA 4001, NFPA, FMG, etc.**

Concrètement, l'installation est maintenue en permanence sous pression d'eau. Les ampoules des têtes sprinkleurs, lorsqu'elles sont soumises à une augmentation importante de la température (lors d'un incendie), éclatent pour permettre le déversement de la quantité d'eau prévue pour contenir le feu.

Innover ? C'est possible !

S'il est difficile d'innover sur le principe même du sprinkleur, on peut toutefois moderniser les composants de l'installation. *« On peut tout à fait innover sur l'application de l'objet sprinkleur et le type de risque auquel il devra faire face,* confirme Pascal Bichet, président de Minimax France, la filiale d'un des grands de l'incendie, l'Allemand Minimax Viking. *Par exemple, nous avons conçu un système sprinkleur qui permet de déverser une plus grande quantité d'eau pour combattre des feux à fort potentiel calorifique. On peut aussi innover sur l'installation elle-même. Nous avons ainsi réalisé un capteur qui permet de contrôler, en direct, la qualité de l'eau et alerter le responsable maintenance si nécessaire. »*

Attention à la maintenance

Une installation aussi belle et pointue soit-elle, devra être maintenue dans les règles afin d'être certain, le cas échéant, qu'elle se déclenchera le moment venu. *« Une installation mal ou pas maintenue risque de ne pas être fonctionnelle. On s'astreindra donc à des opérations de maintenance préventive sur les cuves, les pompes, les postes de contrôle, sur* ● ● ●

PAROLE D'EXPERT

PASCAL BICHET
Président de Minimax France

© DR

« LA MAINTENANCE EST TRÈS IMPORTANTE. »

« Minimax France, filiale de Minimax Viking fabrique, installe, maintient et conçoit des sprinkleurs, des systèmes d'extinction par gaz, des solutions de détection incendie et des extincteurs portatifs.
De ce fait, nous pouvons aider et conseiller les responsables de sites et établissements à concevoir leur installation et à la maintenir correctement. La maintenance est en effet très importante. Ne serait-ce que pour s'assurer, d'une part, que le moment venu, l'installation pourra consommer le volume d'eau prévue car, de cette quantité d'eau définie lors de la conception de l'installation, dépend la qualité de l'extinction. On ne peut pas ici faire preuve d'économie.
En revanche, il est tout à fait possible de limiter la consommation d'eau lors des essais hebdomadaires de la pompe. Nous proposons ainsi une solution qui permet d'utiliser l'eau utilisée pour ce test pour refroidir le système. Par ailleurs, chaque zone d'extinction de l'installation doit disposer d'un point test qui permet de tester le démarrage de la chaîne d'extinction sans être contraint de déclencher l'ensemble de l'installation. »

SUR LE TERRAIN

Sulo fait confiance à la Sprinkbox

« Sulo, qui emploie 8000 personnes dans le monde, principalement en Europe et dans une moindre mesure en Amérique du Sud, développe des solutions pour la gestion des déchets et accompagne les collectivités et les entreprises pour atteindre leurs objectifs de recyclage. Nous fabriquons ainsi, sur le site de Nantes, des conteneurs ménagers (poubelles) en plastique. Sur le site, je suis rattaché à son service maintenance, fonction dans le cadre de laquelle je dois assurer la surveillance de notre importante installation sprinkleurs qui protège la totalité de nos unités de production. Soit plusieurs milliers de mètres carrés. Avant de nous équiper avec la Sprinkbox d'Engie Axima, nous ne pouvions visualiser les anomalies détectées sur notre installation sprinkleur qu'à un seul endroit. Ce qui n'était pas toujours confortable sur un site d'une taille importante comme celui de Nantes. En effet, la Sprinkbox est un boîtier électronique intégré directement sur l'installation sprinkleur, qui permet de collecter les données grâce à un ensemble de sondes et de capteurs et ainsi d'améliorer la fiabilité de la sécurité tout en anticipant les pannes et l'usure de l'installation.
Avec la Sprinkbox, je reçois les informations et autres anomalies détectées sur mon téléphone portable. Je sais ainsi, en temps réel, ce qui se passe et peux immédiatement, si nécessaire, demander à un de mes collègues de se rendre dans la zone concernée pour vérifier l'information. Cela nous permet d'évaluer la gravité de l'anomalie et de prendre les mesures nécessaires si besoin est. La prise en main de cet outil est très facile, très intuitive. En outre, pendant les essais de nos sprinkleurs, nous sommes informés des débits de manière instantanée, des défauts éventuels… »

Christophe Matuchet, responsable maintenance chez Sulo.
© DR

2 QUESTIONS À

JEAN-CLAUDE ENTZ

Directeur du développement Europe & Afrique chez Johnson Controls

© DR

Est-il possible d'innover pour une solution d'extinction aussi éprouvée et reconnue que le sprinkleur ?
Tout à fait. Nous avons ainsi lancé sur le marché américain, dans le cadre de notre démarche Smart Building, un sprinkleur électronique EAS-1. L'innovation réside dans le fait que c'est soit l'élévation de température qui active le sprinkleur, soit le système de détection incendie, dédié au sprinkleur, qui déclenche la percussion du sprinkleur. Nous travaillons actuellement à son lancement sur le marché européen, dont la France. Nous avons aussi mis au point le SprinklerSense. Il s'agit d'un indicateur de passage d'eau intelligent qui permet de récupérer des informations en continu comme le passage d'eau, la température de l'eau, la présence d'eau ou de débris dans la tuyauterie et la détection de fuite par trois sondes de contacts. Ce qui peut être très utile dans le cadre de la maintenance d'une installation.

Justement, en matière de maintenance, quels sont les points de vigilance ? Et quels outils proposez-vous pour aider à la conception des installations sprinkleurs ?
En matière de maintenance, il faut être très vigilant sur la source d'eau : qu'il s'agisse des pompes (diesel ou électrique) et des postes de contrôle, car ils sont au cœur du système. Pour le reste, et outre les vérifications visuelles à faire toutes les semaines, les standards comme la norme NFPA 20 ou la Règle R1 définissent la périodicité des vérifications pour les joints de clapets, les joints de trappes, etc. Pour répondre à la seconde partie de votre question, nous avons conçu notre propre logiciel d'aide à la conception d'un réseau sprinkleur – compatible avec un outil BIM – qui permet de réaliser des calculs hydrauliques, de lister le matériel nécessaire… Nous mettons ce logiciel à disposition des installateurs, des BE, et il est déjà utilisé par FM Global.

● ● ● *tous les éléments au cœur de l'installation »*, insiste Pascal Bichet. Avant d'ajouter : *« Il faudra aussi réaliser, chaque semestre, une visite qui permettra de vérifier que l'installation – certes conçue pour durer trente ans – est toujours en adéquation avec le risque. C'est-à-dire que compte tenu de l'évolution de l'entreprise, de ses process, de ses locaux et de leur destination, l'installation sprinkleur correspond toujours aux risques qu'elle est censée affronter. Ces visites de risques sont obligatoires. »*

Quid du sprinkleur résidentiel ?

Cette année a été marquée par l'ouverture du règlement de certification à d'autres certifications comme l'EN 12845n la NFPA 13 ou la la NFEN 16925. *« Cette dernière est la nouvelle norme concernant la conception et l'installation du sprinkleur résidentiel*, précise Frédéric Proust, président du GIS. *Cela veut dire que désormais, on peut envisager, pour un certain nombre de bâtiments, de recourir aux sprinkleurs en complément de la sécurité incendie. La liste de ces bâtiments à usage résidentiel – logement, habitat collectif, maison de santé, crèches, centres de repos pour les personnes âgées, logements étudiants, petits hôtels – va nécessiter une adaptation dans la version française de la norme. Toujours est-il que cette dernière donne désormais la possibilité, dans le cadre de l'utilisation de nouveaux matériaux comme le bois, d'envisager l'installation de sprinkleurs résidentiels lors de la conception d'un bâtiment résidentiel. »* ■

1 500 000

On dénombre environ 1,5 million de têtes sprinkleurs installées en France et 11 millions en Europe (contre 45 millions aux États-Unis).

Source : *GIS*

PAROLE D'INSTALLATEUR

CHRISTIAN GUILLOT

Président d'EFG

© DR

« LA CONFORMITÉ DU SPRINKLAGE EST LIÉE À LA COMPATIBILITÉ DU COUPLE INSTALLATION/ACTIVITÉ. »

« EFG (Entreprise Florent Guillot) a été fondée il y a quarante ans. Nous sommes installateurs-mainteneurs certifiés Apsad IF1 et E1. Nous pouvons intervenir en amont d'un projet sprinkleur afin de définir les critères de risques et le niveau de protection à appliquer ou en réponse à des appels d'offres, sur la base d'un cahier des charges. Faire appel à un installateur mainteneur certifié est très important car un système sprinkleur a ceci de particulier que sa conformité est liée à la compatibilité du couple installation/activité. Cela veut dire que le niveau de protection doit être harmonisé avec l'activité. Ainsi, lors des vérifications périodiques (semestrielles), il faudra vérifier le maintien de cette adéquation entre l'installation sprinkleur et l'activité de l'entreprise. Si cette dernière a changé, si la destination des locaux a évolué… il faudra vérifier que le système est toujours à même d'assurer sa mission. Dans le cas contraire, on complètera l'installation pour la rendre conforme et, dans les cas extrêmes, on la remplacera. On doit être très attentif à la maintenance des installations sprinkleurs car ce sont des systèmes qui veillent. On doit donc régulièrement vérifier les automatismes de démarrage et les performances des matériels afin de s'assurer que, le moment venu, le système fonctionne parfaitement. Il fait appel à des mainteneurs certifiés qui assureront la traçabilité de leurs interventions et la mise à jour des dossiers techniques. »

© Getty images

La maintenance d'une installation de sprinkleurs doit être faite par un professionnel certifié.

LE POINT DE VUE DU GIS

FRÉDÉRIC PROUST
Président

© DR

« IL FAUT FAIRE APPEL À DES INSTALLATEURS CERTIFIÉS. »

« Du point de vue réglementaire et certification, il faut retenir que cette année, en ce qui concerne > les installateurs, les référentiels IF1 et E1 ont évolué. Par ailleurs, signalons l'ouverture du règlement de certification à d'autres certifications comme l'EN 12845n la NFPA 13 ou la NFEN 16925. Concrètement, cela veut dire, que pour ces nouveaux référentiels de conception, de réalisation et de réception des installations sprinkleurs, les choses se font de manière homogène. Cela permet aux utilisateurs et aux assureurs qui gèrent des grands comptes internationaux de se servir de ces référentiels pour la conception, la réalisation et la réception des installations sprinkleurs. »

La protection commence par la sécurisation des accès avec l'installation de portes blindées et de serrures robustes, et la mise en place d'une alarme anti-intrusion.

© Assa Abloy

Bien protéger les sites vacants

La France compte plusieurs millions de sites vacants. Que la vacance soit temporaire, saisonnière ou de plus longue durée, il est primordial de préserver l'intégrité du patrimoine. Des mesures de protection adaptées sont indispensables pour que le site vacant ne perde pas de valeur et puisse accueillir, dans les meilleures conditions possibles, une nouvelle activité.

Combien de sites vacants en France ? Selon l'Insee, 9,6 % des logements seraient vacants – soit environ 2,6 millions de logements sans occupants. Côté bureaux, sites commerciaux ou industriels, la situation est équivalente. Dans la région Île-de-France, pas moins de 3,4 millions de mètres carrés de bureaux n'ont pas trouvé preneurs, soit 5 %. Au total, on estime que plus de cinq millions de locaux ou habitations se retrouvent vacants – sans compter les établissements ayant une activité saisonnière (stations de ski ou balnéaires, parcs de loisirs, résidences étudiantes, thermes, bâtiment de stockage ou de transformation de produits agricoles, etc.) qui ont une vacance de fait, toute une partie de l'année.

Des risques tout aussi présents que sur des sites occupés

De nombreux propriétaires ou gestionnaires de ses sites – les locaux vacants étant la plupart du temps vides – se contentent

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

LA PAROLE À

CATHERINE LAUG
Directrice marketing, Locken

© DR

« FACILE À INSTALLER, LES CYLINDRES ÉLECTRONIQUES AUTONOMES LOCKEN, CONVIENNENT PARFAITEMENT POUR VERROUILLER L'ACCÈS À DES LOGEMENTS VIDES ET EMPÊCHER L'ACCÈS NON AUTORISÉ. »

« Les cylindres autonomes Locken équipent un parc de logements sociaux vacants en Grande-Bretagne. Nous avons plus de 300 cylindres différents de façon à s'adapter à tout type de portes. Sans câblage ni batterie, le bailleur peut les installer facilement en lieu et place du cylindre mécanique de l'ancien locataire. En période de vacance, le gestionnaire du site a accès à tous les logements vides, avec une clé unique, afin d'y effectuer des travaux ou de faire des visites. Il pourra également tracer les accès. Ultra-robustes, ils résistent à des manipulations répétées et répondent aux normes antivandalismes (EN1303/grade 2), niveau le plus élevé pour la résistance aux attaques mécaniques. Dès que le logement trouve preneur, le cylindre est retiré et remplacé par celui privatif du locataire. Le cylindre Locken récupéré va pouvoir être placé sur une autre porte. »

de verrouiller les accès, sans assurer de protection particulière, pour éviter des frais de gardiennage.
« C'est à mon sens, une erreur, assure Jean-Christophe Chwat, président directeur général de VPS. *Un bâtiment vacant, non sécurisé, peut être une source de coûts importants. Des dégradations, volontaires ou non, peuvent rapidement s'aggraver, si elles ne sont pas immédiatement prises en compte. D'autant que, par définition, les sites sont vides, et qu'il peut donc s'écouler un temps assez long avant que des dommages ne soient signalés… D'autre part, les vols sont également un risque non négligeable, car ils ne concernent pas uniquement les équipements. Le vol de métaux, par exemple, peut endommager des structures et induire, par la suite, des remises en état longues et coûteuses. »*
L'occupation illégale – le squat – est également une source d'inquiétude, car outre les potentiels dommages, elle peut entraîner des difficultés pour récupérer le bien. Sans compter la question de la responsabilité, comme le précise Philippe Bénard, Business Developper d'Axis Communication. *« Sur des sites industriels, il peut rester des produits toxiques ou des équipements dangereux. En cas de déversement et de pollution environnementale, ou d'accident de personne, y compris s'il agit d'un intrus, la responsabilité du propriétaire reste engagée. D'où l'importance de s'assurer qu'aucune personne non autorisée ne pénètre sur le site, avec des outils de dissuasion, anti-intrusion et de remontée d'alertes rapides en cas d'intrusion avérée. »* ●●●

SUR LE TERRAIN

Simons Voss protège les accès d'une grande station de ski des Alpes

Cette station de ski, située dans les Alpes, couvre un large domaine ouvert au public de mi-novembre à début mai. Le site comprend de nombreux locaux techniques qui protègent du matériel sensible comme des armoires électriques ou des mécanismes de remontées, des locaux de stockage de matériel, mais également des accès aux cabines de téléphériques. Isolés et vacants toute une partie de l'année, ces différents locaux doivent faire face au risque de vol et de dégradation de matériel coûteux. De plus, la plupart des bâtiments sont situés à plus de 2 300 mètres d'altitude et subissent des tempêtes de neige et températures allant jusqu'à - 20 °C ! Il fallait donc opter pour une solution résistante à l'humidité et au froid en conditions extrêmes. La station a choisi d'équiper plus d'une centaine de portes extérieures de cylindres sans fil Simons Voss autonomes en énergie. Cette technologie garde une autonomie optimale de 150 000 manœuvres (jusqu'à cinq ans en mode veille), un atout non négligeable quand les portes sont difficiles d'accès. Grâce à une gestion à distance en temps réel (logiciel LSM de la solution 3060), le responsable peut contrôler les portes, programmer les accès et gérer les identifiants. Une solution qui permet d'éviter les déplacements inutiles du personnel sur des accès éloignés et isolés tout en assurant la sécurité du site !

© DR

LA PAROLE À

STÉPHANE ABBOU
Assa Abloy

© DR

« LA PROTECTION D'UN SITE NEUF VACANT DOIT ANTICIPER LA PROTECTION DU SITE EN ACTIVITÉ. »

« Nous travaillons fréquemment avec des maîtres d'œuvre sur la protection d'immeubles en blanc. En général, en attente d'un preneur, le maître d'œuvre va vouloir équiper les portes extérieures, les accès palier, les ascenseurs, (soit 3 % des portes), mais il ne va pas s'engager sur tous les accès ne connaissant pas la future configuration.
Il est pourtant intéressant d'anticiper le futur système de contrôle d'accès pour favoriser une installation rapide et limiter les travaux ultérieurs. En plaçant des serrures électriques câblées en périmétrie des bâtiments, les informations seront remontées en temps réel sur le système de contrôle d'accès pour assurer une performance de verrouillage. Par la suite, le bailleur pourra, en fonction de la disposition des cloisons, placer des systèmes de serrures autonomes. Éventuellement, on peut aller plus loin en préparant un précâblage au niveau des plafonds et des hubs, ce qui permettra au preneur d'installer des produits de contrôle d'accès non filaire, sans avoir de travaux lourds à prévoir. En ce sens, le système Aperio convient parfaitement. De plus, ce dernier est compatible avec la majorité des éditeurs de contrôle d'accès (Alcea, Castel, Genetec, Synchronics, Nedap, Till technologies, etc.). Ainsi, un preneur pourra gérer de façon autonome les parties communes des accès du bâtiment et de ses propres locaux. »

SUR LE TERRAIN

Le sanctuaire de Montligeon, un lieu de repos sécurisé par JPM

© DR

Le sanctuaire de Montligeon est un lieu de retraite et de séminaires qui s'étend sur un grand domaine, avec des bâtiments et des logements utilisés de façon intermittente, qui peuvent être vacants durant de longue période. Ce sanctuaire cherchait une solution lui permettant, d'une part, d'alléger le budget, de résoudre les problématiques de perte de temps liés au remplacement de clés volées ou perdues, et de s'assurer de la sécurité des lieux non occupés ; et d'autre part, les issues de secours de secours devaient être conformes à la norme EN1125 pour permettre une évacuation sûre et efficace en cas d'incident.
La basilique Notre-Dame de Montligeon a choisi es barres anti-panique Fluid et le contrôle d'accès Smartair Update on Card. Des béquilles et des lecteurs muraux Smartair ont été installés sur les portes donnant sur l'extérieur devant être en libre accès la journée et contrôlées le soir.
La salle informatique, le service des archives et l'ensemble des zones sensibles ont aussi été équipées de ce système afin de limiter l'accès aux personnes autorisées.
Au besoin, il est désormais possible de tracer les entrées des usagers, et de bloquer les accès en cas de perte de clés.

Verrouiller efficacement

Clôturer le site et le verrouiller est l'une des premières actions à entreprendre. L'idéal étant de garder une traçabilité des accès. Pour Catherine Laug de chez Locken, un système autonome comme la clé électronique par induction apporte une solution tout à fait adaptée : *« Elle permet une ouverture presque instantanée et donc une utilisation parfaitement fluide. 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 présentes dans le cylindre. Elle offre ainsi une robustesse appréciable sur des sites où il y a peu de passage. Enfin, et surtout, elle fonctionne sans problème, s'il n'y a pas de raccordement électrique, ce qui est souvent le cas sur les sites vacants. »*

Dissuader

La dissuasion reste un outil essentiel de la préservation des bâtiments. *« C'est la raison pour laquelle,* précise Olivier Berudeau de Camelot Europe, *nous avons mis à notre offre deux types d'outils de dissuasion : l'entretien, y compris des espaces verts, et nos unités mobiles de protection. Un bâtiment bien entretenu, sans tag ni vitre cassée, ne sera pas perçu comme abandonné et sera moins susceptible d'être dégradé.*

SOLUTION PRODUIT

Axis D2050-VE Network Radar Detector

L'Axis D2050-VE Network Radar Detector est un radar fiable et précis qui détecte les intrus sur un site et transmet en continu des notifications d'incident précises, quelles que soient les conditions météorologiques. Doté d'une couverture de détection horizontale de 120 degrés et d'une portée de 50 mètres, le détecteur Axis D2050-VE indique la position, l'angle de déplacement et la vitesse exacts d'un objet en mouvement. Protégé contre le vandalisme et adapté aux environnements extérieurs, le détecteur Axis D2050-VE réduit les fausses alarmes déclenchées par la pluie, la neige, les insectes ou les ombres. Ce radar détecteur complète efficacement le système de vidéosurveillance et propose un filtrage à distance, des zones de détection personnalisables et le suivi automatique de radar Axis pour les caméras PTZ.

© DR

3 QUESTIONS À

JEAN-CHRISTOPHE CHWAT

Président du groupe VPS

© DR

Comment se positionne VPS sur la protection des locaux vacants ?

La protection des locaux vacants est une activité que nous avons « inventée » en France, il y a vingt-cinq ans. Aujourd'hui, nous protégeons 19 000 sites vacants à travers nos trois filiales. VPsitex est en charge de la protection de 17 000 locaux vacants au moyen de trois types de solutions qui peuvent être combinées : blindages et fermetures physiques des sites, mise en place d'alarmes intrusion, et des moyens humains (gardiennages, rondiers, maîtres-chiens, etc.). La deuxième filiale, VPS Prodomo s'attache à la sécurité de sites vacants particuliers que sont les chantiers et les échafaudages. Ce sont des solutions activées lorsque le chantier est inoccupé. Enfin, depuis deux mois, la filiale VPS Résidence temporaire a démarré son activité. Il s'agit, comme l'autorise désormais la loi Élan, d'empêcher l'intrusion et l'occupation illégale en plaçant des occupants temporaires dans les locaux à protéger.

Quels sont les moyens que vous proposez pour protéger les sites vacants de vos clients ?

Il n'y a pas de réponse unique : il faut commencer par un audit du site et évaluer les risques en fonction de la situation géographique, de l'environnement et des locaux eux-mêmes : quels sont les accès possibles (portes, fenêtres, etc.), leur résistance, l'inventaire des valeurs qui pourraient susciter la convoitise – équipement mais aussi présence de métal comme le cuivre dans des tuyauteries ou des câblages, les dangers potentiels sur le site. En fonction de ces paramètres, on pourra proposer une protection qui pourra s'adapter s'il y a des changements dans l'environnement (manifestation à proximité, nomades, hausse de la délinquance, etc.). On recommande *a minima* une fermeture physique de tous les accès du site. On peut proposer une solution anti-intrusion raccordée à une centrale de télésurveillance, ou des inspections aléatoires pour évaluer l'état des sites et intervenir si on constate des dégradations ou des anomalies. Ce sont des solutions temporaires que nous installons dès que le site retrouve une activité.

Quelles sont, à votre avis, les erreurs à éviter ?

Ne rien faire ! Le coût résultant d'une occupation illégale et de dégradations est infiniment plus élevé que le coût d'une solution de protection. Négliger l'audit préalable : on voit trop souvent des sites bien protégés au niveau de la porte, mais où les intrus sont entrés par la fenêtre ! Enfin, l'alarme anti-intrusion autonome reliée à une centrale n'est pas un luxe, surtout sur des sites isolés sur lesquels des personnes déterminées finiront par entrer. L'investissement sur la protection est à mon avis minime par rapport à un risque de destruction par incendie.

© DR

3 QUESTIONS À

OLIVIER BERBUDEAU

Directeur France, Camelot Europe

Quelle est l'activité de Camelot Europe ?
Créée en 1993, Camelot Europe est une société européenne, spécialiste de la gestion et protection de l'immobilier vacant. Nous gérons 10000 projets immobiliers. Présents en France depuis 2011, nous proposons une offre de service globale. Nous nous chargeons de gérer, protéger, entretenir tout type d'immobiliers vacants – y compris des terrains vides. Nous pouvons également installer des résidents temporaires, sélectionnés et gérés par Camelot Europe, afin de maintenir le bâtiment vacant protégé et préservé (salariés en mobilité, apprentis, personnels du BTP ou start-up pour les locaux commerciaux), dans le cadre de l'article 29 de la loi Élan.

De quels outils disposez-vous pour la protection de sites ?
Nous utilisons toute la gamme de technologies disponibles : verrouillage et blindage des accès (éventuellement murage ou tôlage des accès), systèmes de détections, anti-intrusions, vidéosurveillance (reportée sur un centre de télésurveillance agréé), etc. Nous avons mis au point des tours mobiles constituées d'un mât télescopique de treize mètres de hauteur, sur lequel nous pouvons installer des caméras et des détecteurs infrarouges et thermiques avec une portée de 200 m. Nous pouvons y associer de la sonorisation et de l'éclairage en fonction des besoins du client.
À ce jour, nous disposons de plus de 500 tours mobiles, que nous mettons à disposition de nos clients durant les périodes de vacance de leurs sites.

Quels conseils donneriez-vous à un responsable de sûreté dont le site va être vacant ?
Lorsque c'est possible, il faut anticiper la vacance et mettre en place les outils de protection dès le départ des occupants. Chaque site est particulier et nécessite une protection sur mesure. Pour être rationnelle et efficace, elle doit être étudiée conjointement avec un spécialiste.

● ● ● *L'autre outil – nos tours de protection – nous permet d'interpeller via un système sonore un intrus détecté dans un périmètre non autorisé. Un système très dissuasif qui évite bien souvent d'avoir à intervenir sur place. »*

Miser sur les systèmes anti-intrusions

Il est important de prévenir les intrusions en agissant dès les tentatives de pénétration pour éviter que les personnes puissent s'installer, voler ou dégrader. C'est là où le rôle de la télésurveillance est essentiel. Outre les caméras et les détecteurs sur clôture, de plus en plus d'entreprises proposent les tours mobiles de détection (IP mirador, Solidbot, VPsITEX, Camelot Europe, etc.). Ces tours autonomes sur batteries, qui s'installent facilement avec une simple remorque et grâce à un mât télescopique, peuvent surveiller un rayon de plusieurs centaines de mètres. En fonction de la localisation, on peut y adapter de la sonorisation, de l'éclairage, des capteurs thermiques, de la vidéosurveillance. Ces tours sont particulièrement adaptées aux sites extérieurs.

La protection par occupation

Autre solution qui commence à émerger depuis quelques mois en France, grâce à la loi Élan, la protection par occupation. *« Au lieu d'empêcher l'intrusion,* explique Jean-Christophe Chwatz, *nous allons installer des occupants pour la période de vacance du bâtiment. Cette formule, très populaire en Grande-Bretagne et aux Pays-Bas, présente des avantages indéniables : les locaux seront occupés et les dégradations seront limitées. Les personnes ou les entreprises disposent d'un logement ou d'un espace, parfois très bien situé, à un bail très avantageux, moins de 200 euros par mois, quels que soient la surface et l'emplacement. Pour le propriétaire, c'est l'assurance de récupérer son bien dès qu'il a trouvé preneur, dans la mesure où le contrat stipule que les occupants le sont à titre temporaire et ne sont pas considérés comme des locataires. »* ■

LA PAROLE À

PHILIPPE BENARD

Ingénieur développement Axis Communication

© DR

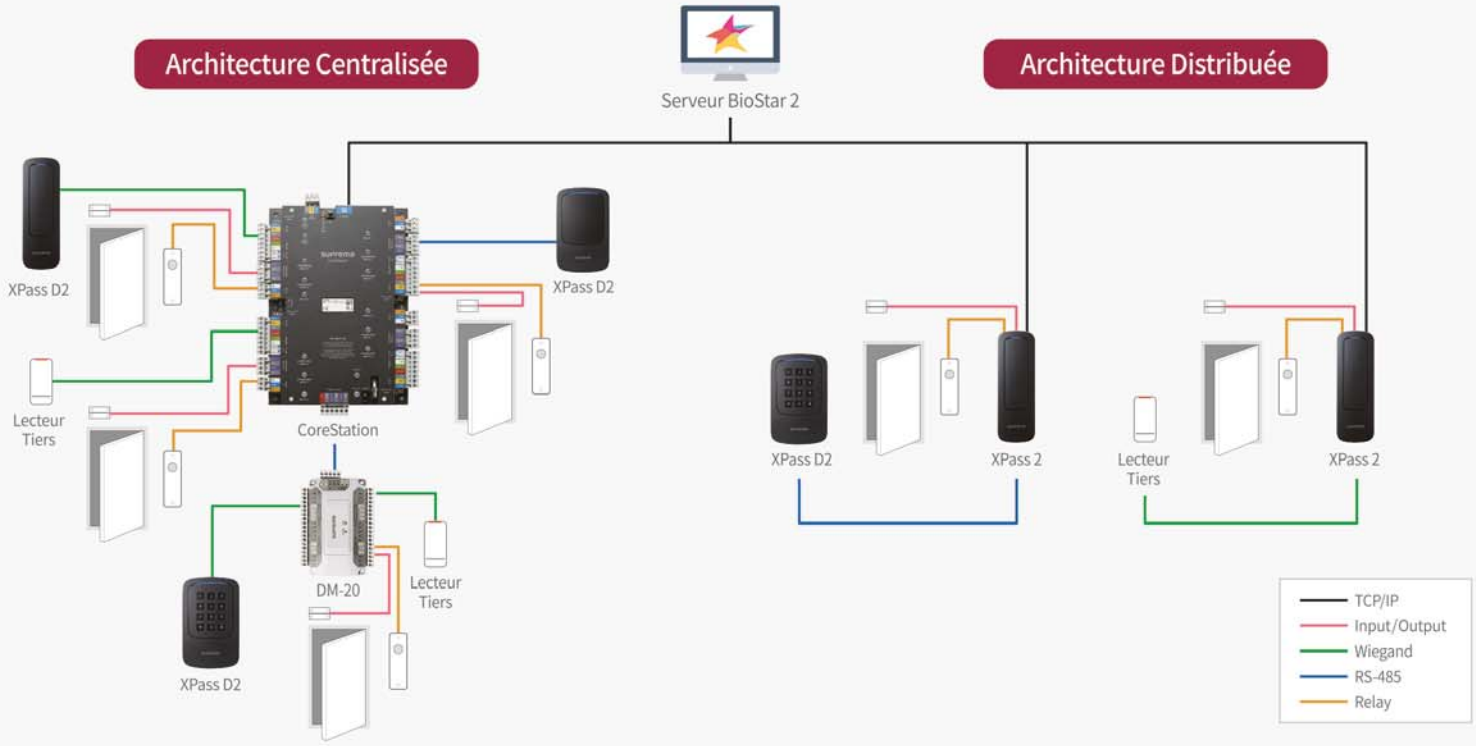
« LA DÉTECTION EN PÉRIMÉTRIE EST ESSENTIELLE POUR INTERVENIR PRÉCOCEMENT. »

« Un site industriel vacant, désaffecté ou un site en activité doivent être protégés de la même façon. Il faut cependant garder en tête que contrairement à un site en activité, sur un site vacant, il n'y aura personne pour lever une alerte. Sur un site industriel, il est aussi important de prendre en compte la dangerosité (transformateurs, produits et cuves, etc.) qui peuvent être à l'origine d'accidents graves. Il est donc important de pouvoir se reposer sur des outils fiables de détection de jour comme de nuit. Un radar comme le D2050-VE D'Axis, couplé à une caméra jour nuit, apporte une solution intéressante. Le balayage du radar permet de couvrir une surface de 2500 m² et la caméra va resserrer le point d'intrusion. Cet ensemble peut être combiné à une diffusion sonore, qui permet d'envoyer un message d'interpellation – généralement suffisant pour éloigner les intrus. Ce système peut aussi renvoyer sur un télésurveilleur qui pourra enclencher une intervention si nécessaire. Autre outil qui peut s'avérer efficace, la caméra thermique en protection de façade de bâtiment qui va détecter une présence. Celle-ci présente l'avantage d'être un simple capteur (pas d'image de personnes identifiable) et, de ce fait, n'est pas soumis à la réglementation de la vidéosurveillance. »

suprema

Adaptez l'architecture système à votre contrôle d'accès

Centralisée / Distribuée (CoreStation + XPass D2 / XPass2 + XPass D2)
Client Web
Code PIN et/ou RFID (Mifare, Desfire EV1 – EV2)
CSN ou SECURE ID mise en oeuvre gratuite (DES/3DES ou AES128)
Accès avec votre Mobile (NFC ou Bluetooth)



Suprema France SARL
16bis rue Grange Dame Rose 78140 Vélizy-Villacoublay, France
T | +33 (0) 7 81 35 23 45 E | sales_fr@supremainc.com

www. supremainc.com/fr

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

Adetec
8 rue de l'angoumois
95100 ARGENTEUIL
Tél.: 01 39 81 85 45
contact@adetec.com
www.adetec.com

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

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

by demes 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

CASD
Solutions de vidéoprotection
CASD
296 Rue de la Béalière
38113 Veurey Voroize
Tél. +33 (0) 4 76 72 80 59
Fax. +33 (0) 4 76 72 90 24
casd@casd.fr - www.casd.fr

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

IZYX
www.izyx-systems.c

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

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.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
Making life accessible
27 rue du Chemin Vert
75011 Paris
01 81 80 14 30
france@iloq.com
www.iLOQ.com

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

© DR

CONTRÔLE D'ACCÈS

Poignée électronique H100 Aperio

Il y a dix ans, Assa Abloy lançait sa gamme Aperio. Il y a quelques mois, la poignée électronique Aperio H100 recevait le prix «Innovative Achievement Award» du Detektor International et le titre de «Produit de l'année - Contrôle d'accès» d'Intersec. Cette poignée électronique Aperio intègre la puissance, la flexibilité et les fonctionnalités du contrôle d'accès sans fil dans une simple poignée de porte. Avec la possibilité de l'installer facilement sur toutes les portes intérieures, son lecteur RFID intégré et son intégration aux systèmes de contrôle d'accès leaders du marché, la poignée H100 permet d'étendre le contrôle d'accès à de nombreuses portes intérieures de manière économique. Aucun câblage n'est nécessaire et la H100 fonctionne avec un système de contrôle d'accès en online ou offline. Ces poignées électroniques H100 peuvent être complétées par les poignées Vercy AH500 au design coordonné, tout comme le reste de la gamme Assa Abloy All by Design. La gamme de produits Aperio comprend des cylindres, des béquilles sur plaque, des poignées sur rosace et des serrures électroniques pour sécuriser et contrôler en transmettant l'état des portes en temps réel au système de contrôle d'accès centralisé. Ces lecteurs sans fil apportent une solution économique grâce à une installation simple et rapide, sans câblage et à moindre frais de maintenance. Plus besoin de remplacer les cylindres mécaniques sur les portes en cas de perte de clés puisqu'un badge peut être désactivé (et réédité) facilement à distance. Des campagnes préventives de remplacement de piles sur les lecteurs Aperio peuvent être programmées sereinement grâce à l'information «pile basse» transmise sur le système. Une interface unique contrôle toutes les portess en filaire et toutes les portes équipées de lecteurs sans fil Aperio en mode online (via des hubs de communication Wiegand, RS485 ou IP qui connectent jusqu'à 16 appareils Aperio au logiciel administrateur) ou offline (OSS Standard Offline). ■

→ **www.assaabloy.fr/Aperio**

3 QUESTIONS À

MÉLANIE DUBUS

Directrice marketing contrôle d'accès chez Assa Abloy

Qu'est-ce qui différenciait Aperio des autres solutions de contrôle d'accès lors de son lancement il y a dix ans ?
Son facteur différenciant résidait dans le fait qu'il s'agissait, dès l'origine, d'une solution intégrable et intégrée dans un système de contrôle d'accès. Elle répondait à une problématique courante à l'époque – et qui l'est toujours – étendre un système de contrôle d'accès à l'ensemble des portes d'un bâtiment, même aux portes secondaires, afin de pouvoir les gérer en temps réel. La gamme se caractérise aussi par la qualité des cylindres des poignées de portes ; cylindres dans lesquels vient s'intégrer l'électronique.

Vous avez apporté un soin tout particulier au design des produits composant la gamme. Pourquoi ?
Il est important de pouvoir s'équiper avec des solutions dont le design est cohérent. Ainsi la poignée mécanique Vercy AH500 jouit de la même approche All by Design d'Assa Abloy que la poignée électronique Aperio H100. C'est très important pour de nombreux utilisateurs mais aussi pour les architectes qui recherchent souvent des solutions au look soigné.

Cette gamme évolue-t-elle encore ?
Nous travaillons le design de l'ensemble de la gamme pour qu'elle s'intègre toujours mieux dans les bâtiments. Nous faisons aussi évoluer nos firmwares en fonction des usages du contrôle d'accès afin de maintenir le niveau de compatibilité de la gamme avec les technologies et fonctionnalités du contrôle d'accès. Compatibilité qui est la force d'Aperio.

VIDÉOSURVEILLANCE

Caméra réseau 4K Axis pour voir encore mieux

© DR

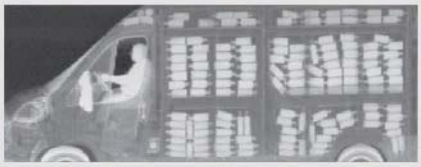
Équipée d'un zoom 4x et d'un objectif Canon, la caméra réseau Axis Q1798-LE est certifiée IP66, IP67 et IK10. Elle peut également supporter des températures extrêmes allant de -40 °C à -60 °C. Axis Communications a équipé cette caméra réseau de fonctions de sécurité comme le firmware signé et le démarrage sécurisé. Elle embarque également la technologie Axis Lightfinder 2.0. qui permet d'augmenter la sensibilité à la lumière, d'attribuer des couleurs plus naturelles dans l'obscurité et d'améliorer la netteté sur des objets mobiles. De plus, l'éclairage IR intégré à la caméra offre une surveillance discrète dans l'obscurité totale, allant jusqu'à 50 m, voire plus selon la scène. La nouvelle caméra réseau Axis prend en charge l'alimentation PoE et une alimentation CC redondante. Par ailleurs, les données enregistrées par l'appareil sont sauvegardées si une coupure d'électricité survient. En ce qui concerne la compression, la fonctionnalité Axis Zipstream – compatible H.264 et H.265 – réduit les besoins en bande passante et en stockage. D'autres dispositifs peuvent être connectés à cette caméra réseau via les ports d'E/S afin de déclencher des alarmes ou des actions. L'entrée surveillée peut alors émettre une notification en cas de connexion interrompue. ■

→ **www.axis.com**

CARACTÉRISTIQUES

- Résolutions 4K/10 MP
- Capteur ultra-sensible à la lumière
- Objectif Canon 12 - 48 mm
- Technologie Axis Lightfinder 2.0
- Technologie Axis Zipstream compatible H.264/H.265

L'image montre des narcotiques cachés



L'image révèle de l'alcool de contrebande, caché pour éviter de payer des droits de douane

L'image accompagne une éventuelle menace radioactive

© DR

CONTRÔLE D'ACCÈS

Système d'inspection mobile non intrusif du fret et des véhicules

Développé par AS&E et commercialisé par HTDS en France, le système ZBV Classe S est la dernière version de la solution d'inspection non intrusive de véhicules et de fret la plus vendue dans le monde. Intégré dans un véhicule utilitaire de type fourgon Classe S, ce système d'inspection intelligent permet notamment de détecter les menaces et la contrebande.
Ce système a la particularité de pouvoir contrôler aussi bien tout type de véhicules que les conteneurs de fret ou encore autres objets en passant simplement devant eux. Ainsi, lorsque le système ZBV passe devant un objet suspect, une image radiographique rétrodiffusée apparaît sur la console de l'opérateur en temps réel à l'intérieur du fourgon.
Entièrement mobile, autonome et pouvant être déployé immédiatement en réponse aux menaces de sécurité, le nouveau système ZBV Classe S fournit un champ de vision complet des véhicules, y compris les pneus.
D'autre part, le système ZBV utilise la technologie Z Backscatter pour une image photographique qui révèle les menaces et la contrebande que les autres systèmes à rayons X à transmission unique peuvent ne pas détecter. Grâce à son imagerie facile à interpréter pour une analyse rapide, le système ZBV S permet un criblage à haut débit des véhicules et du fret à une vitesse de balayage pouvant aller jusqu'à 10 km/h. ■

→ **wwww.htds.fr**

CARACTÉRISTIQUES

- Mode d'analyse statique
- Console de l'opérateur à distance
- Kit de surveillance de la zone radiographiée
- Détection de menaces radioactives
- Identificateur d'isotopes
- Système de rétrodiffusion Mini Z portatif
- Kit de mise en réseau sans fil
- Notification de scan audible

ÉCLAIRAGE

Lampe de poche tactique Streamlight Protec 90

© DR

Protac 90 est une lampe de poche tactique très puissante et ultra-compacte. Avec sa tête pivotante à 90° et son clip multifonction conçu pour s'adapter à différents systèmes d'accroches dont le Molle, la nouvelle Protac offre de nombreuses options de port idéales pour le port mains libres. Programmation TEN-TAP - 3 programmes disponibles : fort/stroboscopique/faible, Fort uniquement, faible/fort • Fonctionne avec 1 pile CR123A ou 1 pile AA Lithium ou 1 pile AA alcaline • Puissance de la lampe avec pile CR123A : Intensité forte : 300 lumens, distance d'éclairage de 147 m, autonomie 1 h 45 ; Intensité faible : 40 lumens, distance d'éclairage de 53 m, autonomie 14 h ; Strobe pour la signalisation ou la désorientation : autonomie 2 h 30. ■

→ **www.streamlight.com**

CARACTÉRISTIQUES

- IPX7 imperméable à 1 mètre pendant 30 minutes
- Résistance aux chocs de 2 mètres testée
- Fabrication en aluminium anodisé durable avec lentille en verre résistant aux chocs
- Clip de poche amovible
- Conforme à RoHS

VIDÉOSURVEILLANCE

Firefly DL : une caméra pour le deep learning

Flir Systems vient de lancer la Flir Firefly DL, une caméra intégrant l'apprentissage en profondeur (deep learning) par inférence grâce à la technologie Flir Neuro. Avec sa petite taille, son faible poids, sa consommation électrique minimale et ses capacités d'apprentissage profond, la caméra Flir Firefly DL est idéale pour une intégration dans des systèmes mobiles, de bureau et portables.

La Firefly DL permet aux fabricants, ingénieurs et constructeurs d'équipements de développer et de déployer rapidement des solutions pour des tâches d'automatisation complexes. En outre, les constructeurs de systèmes peuvent réduire le coût et la complexité de leur travail en déployant un réseau de neurones entraîné directement sur la caméra, éliminant ainsi la nécessité pour un système hôte de mener à bien les tâches de classification, de détection et de localisation d'objets. La Firefly DL associe les performances de vision industrielle au deep learning pour résoudre des problèmes complexes et subjectifs, comme la reconnaissance des visages. ■

© DR

→ **www.flir.com**

CONTRÔLE D'ACCÈS

Interphone vidéo connecté

© DR

Hi)Pro S500 est le nouvel interphone vidéo de Fenotek. Il permet de répondre avec son smartphone aux visiteurs qui sonnent au domicile que l'on soit chez soi ou à l'autre bout du monde. Doté d'une caméra haute définition, il permet de voir son interlocuteur et de discuter avec lui. Il est même possible d'ouvrir le portail ou d'allumer les lumières à distance avec son téléphone. Le Hi)Pro-S500 sera disponible uniquement au travers d'un réseau professionnel d'installateurs et de fabricants. Un système d'appairage par scan permet de fluidifier et de simplifier linstallation. L'objectif étant de raccourcir le temps d'intervention de l'installateur sur le chantier et de minimiser les risques d'erreur de saisie. Par ailleurs, Hi)Pro S500 propose un nouveau système de détection de mouvement qui utilise la technologie IMD (Intelligent Motion Detection). Il s'agit d'un système de captation et d'analyse par zones qui permet une surveillance précise et analytique des évènements devant la maison. Ce système permet d'envoyer une alerte en temps réel uniquement lorsque quelqu'un rôde devant la porte d'entrée. ■

→ **www.fenotek.com**

LUTTE CONTRE LE FEU

Gamme complète de calfeutrements

Créée en 2007 et basée à Ermont, la société 2F Protection fabrique une gamme complète de produits dédiés au calfeutrement de pénétration coupe-feu des bâtiments tertiaires, industriels, des ERP (Établissements recevant du public), des IGH (Immeubles de grande hauteur), etc. : enduits et mastics coupe-feu, mortiers coupe-feu, pâtes coupe-feu, sacs coupe-feu. Classés EI 60 à 240, les produits 2F Protection garantissent une performance coupe-feu de une à quatre heures selon la configuration. Ils bénéficient tous d'un procès-verbal de classement délivré par le CSTB ou Efectis. Fabriqués dans le Gard, ils sont distribués en direct, dans un délai de deux à trois jours. En plus de la fabrication de produits de calfeutrement, 2F Protection réalise toutes les opérations de protection au feu des câbles, canalisations et conduits traversants, offrant ainsi une prestation complète aux prescripteurs (bureaux d'études et de contrôle) et gestionnaires de bâtiments : • Application des produits de calfeutrement coupe-feu • Cheminements techniques protégés (CTP) et volumes techniques protégés (VTP) • Maçonnerie coupe-feu • Flocage coupe-feu • Carottage. Ils peuvent être commandés en ligne. ■

→ **www.2fprotection.fr**

© DR

OFFRE PACK psm
PROTECTION SÉCURITÉ MAGAZINE

- Le magazine PSM
- La e-newsletter tous les 15 jours
- Les archives en libre accès sur Internet
- Le Hors-Série Sécurité Privée
- Le Guide d'Achat
- L'Annuaire de la Sécurité Sureté

...

BULLETIN D'ABONNEMENT À RETOURNER À
PSM / TBS Blue – 6, rue d'Ouessant – 35760 St Grégoire. Tél : 01 76 41 05 88. Fax : 01 48 00 05 03. abopsm@tpmedia.fr

Oui, je souhaite m'abonner à PSM pour 1 an (6 numéros) : **103 € TTC au lieu de ~~168~~ €**

J'économise + de 65 €, soit + de 45 % de réduction !

Je règle : ☐ chèque > à l'ordre de PSM ☐ à réception de la facture

Mes coordonnées :

NOM _____ ADRESSE _____
PRÉNOM _____
SOCIÉTÉ _____ CODE POSTAL _____
E-MAIL _____ VILLE _____

Le tarif indiqué est valable jusqu'au 31/12/2020 (TVA : 2.10%) en France seulement. Pour l'étranger, nous consulter.
Conformément à la loi « Informatiques et libertés », vous disposez d'un droit d'accès et de rectification aux informations vous concernant auprès de l'éditeur.
TP Média : SARL au capital de 20.000 € - 488 819 137 RCS PARIS

© DR

« À l'État de contrôler les donneurs d'ordres publics. »

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

Depuis de longues années, l'ADMS et sa présidente Danièle Meslier ne ménagent pas leurs efforts pour lutter contre le travail illégal dans la sécurité. Malgré cela, les déviances perdurent…

Le travail illégal est toujours un mal endémique dans nos métiers. Malgré les efforts du Cnaps et des groupements professionnels du secteur, ce qu'il faut bien qualifier de délits perdurent. On constate tous les jours des situations qui n'ont rien à voir avec le droit du travail, la concurrence saine entre entreprises, les relations entre donneurs d'ordres et prestataires ou des conditions de travail dignes de ce nom… On pourrait multiplier les exemples de comportements, de méthodes indignes. Fausse sous-traitance, fonctionnement de certaines prestataires comme des entreprises de travail intérimaire, travail le week-end non déclaré ou non payé comme il le devrait, travail de nuit, prestations vendues à des coûts scandaleusement bas… Autant de dérives qui l'ADMS et d'autres dénoncent depuis des années et qui entraînent le non-respect des grilles de salaires, des conventions salariales… Et que dire des conditions de travail des agents de ces sociétés ? Certains dorment dans leur propre voiture avec leur chien. D'autres, sur les sites des clients, n'ont pas de vestiaires à disposition, pas d'espaces de repos ou de détente…

Le secteur public devrait donner le bon exemple

L'État et les pouvoirs publics, si prompts à taper sur les donneurs des entreprises privées lorsqu'elles ne respectent pas la législation en matière de droit du travail, sont loin, très loin, d'être aussi exigeants envers eux-mêmes. Ainsi, certains donneurs d'ordres publics emploient des agents non déclarés ou sans carte professionnelle ! Tout le monde est coupable. Donneurs d'ordres comme prestataires. Tout cela pour diminuer les charges sociales. Car il faut bien comprendre que dans ces cas, on ne peut pas payer ses frais professionnels à un agent. Comprendre aussi qu'on rognera pour lui payer comme il se doit ses heures de travail effectuées la nuit ou durant le week-end. C'est un véritable cercle vicieux qui nuit, à l'heure où on nous parle de continuum sécurité, de collaboration public-privé, à l'image de nos métiers.

Des mesures s'imposent

Le Cnaps fait dans la mesure de ces moyens. Quand il constate qu'en employeur est dans l'illégalité, il peut lui imposer une interdiction temporaire. Mais que faire de plus ? D'autant plus que cette interdiction ne semble respectée pas puisque, dans certains cas, on a pu constater que la personne concernée par l'interdiction continuait à travailler ! On peut certes ensuite transmettre le dossier au procureur. Mais ce genre d'affaire est-il la priorité des procureurs ? Le préfet, quant à lui, de son côté, peut ordonner une fermeture administrative. Serait-ce suffisant ? Est-ce que cela dissuaderait les autres ? Il faut absolument que toute la branche se saisisse du sujet. Réellement. Il faut instaurer une solidarité financière réelle entre le maître d'ouvrage et le donneur d'ordres.
Par ailleurs, il faut impérativement mettre en place des contrôles visant les donneurs d'ordres publics.
Mais ce n'est pas le Cnaps qui peut le faire. C'est à l'État de contrôler et sanctionner les donneurs d'ordres publics.
Il faut agir au plus vite. La sécurité privée doit changer de visage pour relever les défis qui se présentent à elles et les événements de demain comme les jeux Olympiques de Paris en 2024 pour lesquels il va falloir recruter plusieurs dizaines de milliers d'agents de sécurité… ■

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. ■ **JUILLET 2019** L'ADMS rejoint la FSP (Fédération française de la sécurité privée).

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

DS-KH6320-WTE1 DS-KD-ACW
DS-KH8350-WTE1 DS-KD-M/E
DS-KH8520-WTE1 DS-KD-KK
DS-KD8003-IME1 DS-KD-KP

SYSTÈME D'INTERPHONE DE DEUXIÈME GÉNÉRATION

SÉCURITÉ CONNECTÉE = VRAIE PAIX DE L'ESPRIT

- Points forts
- Configuration simplifiée
- Design ultra-mince
- Interface utilisateur conviviale
- Excellente expérience d'interphone vidéo