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

CONTRÔLE D'ACCÈS

RECONNAISSANCE FACIALE, LA BIOMÉTRIE QUI MONTE

n°251
Janvier Février 2019
26 €

entretien

MARC DARMON
PRÉSIDENT DU CSF INDUSTRIE DE SÉCURITÉ
« LA CRÉATION DU CSF MONTRE L'IMPORTANCE QU'ACCORDE L'ÉTAT À LA SÉCURITÉ. »

vidéosurveillance

PENSEZ À VOUS PROTÉGER CONTRE LES CYBERMENACES !

risque

ESPACE PUBLIC SOUS L'ŒIL DES CAMÉRAS

DOSSIER
SÉCURITÉ ET SMART CITIES

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

www.protectionsecurite-magazine.fr

La plateforme Dahua VMS est désormais disponible sous Windows

DSS Pro 7.0

- Un logiciel Windows facile à utiliser avec un tout nouveau design
- Prend en charge toute la gamme de produits Dahua
- Utilise l'architecture Client Server (C / S) et la conception modulaire, permettant un déploiement flexible
- Prend en charge la redondance à chaud qui garantit la fiabilité du système pour les applications critiques
- Prend en charge l'accès aux principaux équipements de vidéoprotection par les protocoles standards ONVIF ou PSIA
- Équipe professionnelle pour répondre à une variété de besoins personnalisés

DSS

CE FC RoHS ISO 9001:2000

DAHUA TECHNOLOGY FRANCE
49 rue Auguste Perret, 94000 Créteil, France
Tél : 01 48 53 70 53
Email : sales.france@dahuatech.com /support.france@dahuatech.com
http://www.dahuasecurity.com/fr


© Risk&Co


© DR

CONSEIL EN SÉCURITÉ

LE GROUPE RISK&CO EST À VENDRE

Le bruit courait. Il a été confirmé. Le groupe français Risk&Co, spécialisé dans le conseil et l'ingénierie en sûreté-sécurité, a été mis en vente par Latour Capital, son actionnaire majoritaire.
Créée en 1994, Risk&Co s'est vite imposée sur son marché via des contrats avec des grands groupes internationaux privés comme Samsung et Total – pour lequel la société assurait la sécurité de ses sites au Yémen – et des institutions nationales. Risk&Co est désormais l'un des trois leaders de son marché, avec Geos et Amarante international. Malgré ses bons résultats, et comme de nombreux autres acteurs du secteur, Risk&Co a vu son chiffre d'affaires baisser en 2018 passant de 25,4 millions d'euros à 20 millions.
Qui pour reprendre Risk&Co ? On parle d'Amarante International et de l'Adit. En effet, Amarante international était très intéressé par la reprise de Geos. Mais l'affaire lui a échappé puisque c'est justement l'Adit qui s'est offert Geos *(voir ci-contre).* Mais il va aussi falloir compter avec des groupes étrangers…

SÉCURITÉ INCENDIE

GROUPE GORGÉ SE SÉPARE D'AI GROUP

AI Group, filiale du pôle Vigians du Groupe Gorgé et spécialiste de la protection incendie des grands risques industriels, a enregistré des pertes en 2017 et au premier semestre 2018 impactée par la baisse des investissements dans l'Oil & Gas. Son redressement, entamé en 2018, a été mis en question par la mise en place des sanctions américaines visant l'Iran qui représente un marché important de la société.
Ne souhaitant pas être exposé avec des activités dans une zone visée par des sanctions renforcées, Groupe Gorgé a donc cédé la société à son management qui poursuivra ses activités sur les sites de Naintré et Paris, où elle emploie 30 salariés.
Sur les neuf premiers mois de 2018, AI Group a généré un chiffre d'affaires de 5,6 millions d'euros. Rappelons que Groupe Gorgé est un groupe indépendant présent dans des industries de haute technologie. Ses activités s'inscrivent dans les secteurs de la sécurité et de la protection en environnements extrêmes ainsi que dans le secteur de l'impression 3D. Le groupe emploie environ 2000 personnes, est implanté dans huit pays, et exporte directement environ 30 % de son activité.

ESSD

L'Adit s'offre Geos

Une acquisition qui permet à l'Adit de diversifier son offre de services et de venir titiller ses concurrents anglo-saxons.

Grâce à cette acquisition l'Adit va en effet mettre un pied sur le marché de la sécurité dans les zones à risques sur lequel le savoir-faire du Français Geos n'est plus à démontrer. Créé en 1997, le groupe Geos est ce qu'on appelle une ESSD (entreprise de services de sécurité et de défense) spécialisée dans la protection des personnes (délégations ou diplomates) et de la sécurité des sites industriels. Le groupe assure aujourd'hui un suivi dans plus de 160 pays et compte plus de 330 collaborateurs.
Cette acquisition offre également à l'Adit – dont le chiffre d'affaires a été multiplié par quatre depuis 2010 (pour atteindre 45 millions d'euros cette année) – l'opportunité de se poser en concurrent direct des acteurs anglo-saxons du secteur comme le groupe américain Kroll ou l'Anglais Control Risks.

Un leader français

La reprise de 92 % du capital (actuellement détenu par la société d'investissement Halisol) de Geos permet donc à l'Adit de voir son chiffre d'affaires dépasser les 70 millions d'euros et ses effectifs passer à 500 personnes.
L'Adit est contrôlé à 66 % par Weinberg Capital Partners, 34 % par BPI France (les 10 % détenus par l'État ont fait l'objet d'un reclassement le 29 juin).
Comme le confie Alain Juillet à notre confrère *Challenges*, *« il manquait un acteur français capable d'affronter ces géants, l'Adit est en train de le devenir. L'idéal serait d'atteindre de 120 à 150 millions d'euros de chiffre d'affaires pour peser à l'international »*. Avec ce rachat, qui intéressait aussi Amarante International, qui serait sur les rangs pour reprendre le Français Risk&Co, l'Adit est désormais en droit d'espérer…


© Getty Images

VIDÉOPROTECTION

Foxstream acquiert Cossilys21

Avec cette acquisition, Foxstream complète son offre et va pouvoir s'implanter sur d'autres marchés. Par ailleurs, les deux sociétés vont également pouvoir profiter d'une capacité en R&D accrue.

© DR

Le Lyonnais Cossilys21 propose des solutions intelligentes de vidéoprotection. La société équipe de grandes banques nationales, de nombreuses banques régionales ainsi que des commerces. La société entretient depuis longtemps déjà des liens de partenariat avec Foxstream. Et quand Alain Ghaye, président et actionnaire principal de Cossilys21, a souhaité céder son entreprise pour partir à la retraite, c'est naturellement que l'idée de ce rapprochement entre les deux sociétés est née.

Ce projet a été mené en lien avec le directeur général de Cossilys, François Bureau, associé à part entière dans le projet de reprise.

« L'offre de Cossilys21, qui associe un savoir-faire dans la manipulation de la vidéo et dans la gestion de parcs, est fortement complémentaire de l'offre de Foxstream, dont le savoir-faire est plus dans l'analyse de la vidéo, déclare Jean-Baptiste Ducatez, Pdg de Foxstream. *Les compétences de ces deux équipes seront un atout important pour relever les futurs défis technologiques de notre profession, le cloud, le deep learning, la cybersécurité, etc. C'est une belle aventure humaine qui commence. »*

Du côté de Cossilys, on se réjouit de ce rapprochement : *« C'est une alliance stratégique et industrielle de deux sociétés en croissance, reconnues dans leur secteur,* commente François Bureau. *La synergie de nos technologies et de nos expertises permettra, avec Foxstream, de satisfaire davantage nos clients. Et dès 2019, un plan d'investissement ambitieux va renforcer nos capacités d'innovations. »*

Après le rachat de la société grenobloise Blue Eye Video fin 2014, cette nouvelle opération de croissance externe confirme les ambitions de Foxstream d'être un acteur fortement présent dans les technologies de pointe sur le marché français et étranger de la sécurité, et de la gestion de flux.

© DR

2 QUESTIONS À Jean-Baptiste Ducatez,

PDG DE FOXSTREAM

Pourquoi avez-vous décidé d'acquérir Cossilys21 ?

Tout d'abord parce que je connais bien cette société et que son président, Alain Ghaye, m'avait fait part, il y a plus d'un an, de son souhait de céder sa société avant de prendre une retraite bien méritée. Ensuite, parce que Cossilys21, spécialiste de l'enregistrement et de la manipulation de la vidéo, un des acteurs majeurs sur le secteur bancaire, vient tout naturellement compléter l'offre et le savoir-faire de Foxstream, spécialisée dans l'analyse vidéo et très peu implanté sur les marchés de Cossilys21. Il y a donc une vraie logique à nous rapprocher d'eux, tant en termes de marchés que de complémentarité de nos offres respectives. Je tiens d'ailleurs à souligner que l'opération s'est très bien déroulée et que le directeur général actuel de Cossilys21, François Bureau, nous a grandement facilité les choses. Et nous n'avons aucunement l'intention de faire disparaître la marque Cossilys21, pérenne et reconnue sur ses marchés.

Quel bilan tirez-vous de l'année écoulée ?

Foxstream se porte bien. Notre exercice 2018 qui va se clôturer en mars prochain nous permet très raisonnablement d'espérer une croissance de notre CA comprise entre 10 et 15 %. Taux de croissance assez similaire d'ailleurs à celui de Cossilys21 qui va clore son année sur une croissance supérieure à 12 %. Enfin, l'acquisition de Cossilys21 nous a permis de doubler la taille de notre département R&D. Ce qui va nous permettre évidemment de continuer d'innover afin de répondre aux besoins du marché de la vidéo et de nous pencher sur des technologies comme le cloud, le deep learning…


© Paxton

CONTRÔLE D'ACCÈS

PAXTON ÉQUIPE LES POMPIERS

Les pompiers de Humberside (Royaume-Uni) avaient besoin d'une solution de contrôle d'accès capable de sécuriser plusieurs sites sur un même système. Ce système devait être robuste et fiable pour maintenir la sécurité des locaux tout en permettant une entrée et une sortie faciles en cas d'urgence. Des autorisations d'accès flexibles sur 12 des casernes de pompiers de la région étaient également essentielles. Les pompiers de Humberside ont collaboré avec Delta Security Systems Ltd pour recommander une solution de contrôle d'accès pouvant répondre à leurs besoins. Basée à Hull, Delta Security Systems fournit des systèmes de sécurité électroniques à usage domestique et commercial. Ils ont recommandé le système de contrôle d'accès phare de Paxton Net2, avec PaxLock Pro, contrôle d'accès sans fil avec une poignée de porte et Net2 Entry et un système de vidéophonie IP. PaxLock Pro est le dernier ajout à la gamme de contrôle d'accès sans fil de Paxton. Il peut être installé en mode autonome ou dans le cadre d'un système en réseau Net2, sans nécessiter de matériel supplémentaire. Adapté à de nombreux sites et soumis à de nombreux tests répondant aux normes industrielles les plus strictes, notamment en ce qui concerne les portes coupe-feu, PaxLock Pro offre un contrôle d'accès polyvalent sans fil avec un design moderne et contemporain fabriqué pour durer.

© DR

SÉCURITÉ PRIVÉE

SERIS A LA CONFIANCE DE KIABI

Depuis quelques mois, les équipes Seris assurent les prestations de sécurité de 57 magasins Kiabi répartis sur l'ensemble du territoire. En coordination avec la Direction nationale des enseignes de la distribution, les agences régionales prennent en charge cette nouvelle enseigne. Spécialiste de la distribution spécialisée, Seris met en œuvre toute son expertise afin d'accompagner Kiabi et déployer un dispositif de sécurité optimisé pour l'ensemble de ses magasins. Dans le respect des consignes de surveillance du magasin, les agents de sécurité ont pour missions l'accueil et le contrôle d'accès, la surveillance de l'accessibilité des locaux, du secteur caisse, la réduction de la démarque inconnue ou encore la lutte contre les incivilités. Enfin, pour garantir un suivi permanent des prestations, un espace collaboratif a été mis en place, facilitant ainsi la communication entre les différents acteurs du dispositif de sécurité.

SÉCURITÉ PRIVÉE

Un Brexit lourd de conséquences pour les Britanniques...

Depuis le Brexit, les entreprises britanniques de sécurité ont perdu quelques marchés importants concernant la sécurité des instances de l'Europe dans les zones à risques. Les Français vont-ils savoir en profiter ?

Compte tenu que l'UE ne peut disposer de ses propres forces de sécurité, elle a donc confié la protection de ses instances diplomatiques au secteur privé. Marché juteux jusqu'à il y a peu, trusté par les entreprises d'outre-Manche, le Brexit pourrait bien redistribuer les cartes... En effet, pour préparer le Brexit, l'UE a inséré dans les appels d'offres du Service européen pour l'action extérieure (SEAE) une nouvelle clause qui précise *« qu'à la suite du retrait du Royaume-Uni de l'UE, les règles d'accès aux procédures de passations de marchés de l'UE pour les acteurs [...] établis dans des pays tiers s'appliqueront aux candidats et soumissionnaires du Royaume-Uni en fonction du résultat des négociations »*. Si les contrats en cours ne sont pas impactés par cette nouvelle disposition, elle implique que les Britanniques risquent de se voir fermer les marchés de l'UE.

Le Français Amarante décroche deux marchés

La filiale du groupe Seris a déjà décroché deux contrats importants avec GardaWorldl (Canada). Le premier, auparavant détenu par G4S, concerne la protection des personnels européens chargés d'apporter à Bagdad une assistance technique au gouvernement irakien. Le second, d'un montant de 85 millions d'euros pour six ans, a pour objet la protection de la délégation de l'UE en Afghanistan. Contrat jusqu'à maintenant dans l'escarcelle de l'Anglais Page et pour lequel G4S et la société américaine Constellis étaient sur les rangs.


© DR

SÉCURITÉ INCENDIE

Siemens retenu par le Normandy

La division Building Technologies de Siemens et Siemens Financial Services ont remporté le marché pour la migration complète du système incendie du bâtiment du Centre de rééducation et réadaptations fonctionnelles en milieu marin.

© DR

Siemens a modernisé le système de sécurité incendie du Centre de rééducation et réadaptations fonctionnelles en milieu marin (CCRF) Le Normandy, à Granville (50). Engagé dans une politique qualité et gestion des risques, l'établissement a été certifié V2014 par la Haute Autorité de santé en 2016, sans aucune réserve ni recommandation. Soucieux de maintenir cette qualité et d'assurer la sécurité des personnes dans ses bâtiments, l'établissement a souhaité rénover tout son système de sécurité incendie sans perturber le travail des 500 professionnels soignants et la guérison des patients. La division Building Technologies de Siemens et Siemens Financial Services ont remporté le marché pour la migration complète du système incendie du bâtiment du CRRF comprenant le système de détection incendie et le système de mise en sécurité. Tous les détecteurs incendie ont été remplacés, une centrale SDI Sinteso FC2060 en baie avec plus de 550 têtes de détection Sinteso FDO221 a été installée, ainsi que 11 tableaux reports d'exploitation à textes clairs FT2011 et un CMSI STT20 avec plus de 60 modules électroniques adressables gérant les DAS et les commandes terminaux (DCT), comme les trappes de désenfumage, les portes coupe-feu et les diffuseurs sonores et lumineux.

« Au-delà du fait que les équipes Siemens ont été à notre écoute, les interlocuteurs ont montré leur compréhension du besoin. La difficulté ne les a pas arrêtés et la solution de financement a été adaptée en prenant en compte nos contraintes budgétaires », explique Lionel Chauveau, responsable des services économiques et techniques du Normandy.

Le Centre de rééducation et réadaptations fonctionnelles en milieu marin Le Normandy de Granville accueille 4 000 patients par an, en hospitalisation à temps complet ou de jour, sur ses deux sites. Ouvert en mai 1967, il a pour vocation la rééducation de la fonction d'un membre ou d'une articulation, la rééducation neurologique et la réinsertion socio-familiale et professionnelle du patient.

© DR

CONTRÔLE D'ACCÈS
DÉNY SECURITY INVESTIT DANS SON OUTIL DE PRODUCTION

Spécialiste du contrôle d'accès et des organigrammes, Dény Security est un des leaders français de la protection des sites à forte implication sécuritaire. Pour renforcer ses positions sur le marché du contrôle d'accès, Dény Security a décidé d'investir 550 000 euros dans son outil de production. Soit l'un des plus gros investissements de l'entreprise depuis plus de quarante ans. Résultat d'une étude approfondie de trois ans, l'investissement réalisé pour la fabrication de son cylindre mécanique historique se répartit en R&D, prototypes et essais fonctionnels, dépôt de brevets, codéveloppement avec un prestataire externe d'une machine à soudure laser… Cet investissement a permis également d'améliorer la productivité (optimisation des temps de montage de 11 à 7 pièces, capabilité du process de production, réduction des rebuts...).

SÉCURITÉ ÉLECTRONIQUE

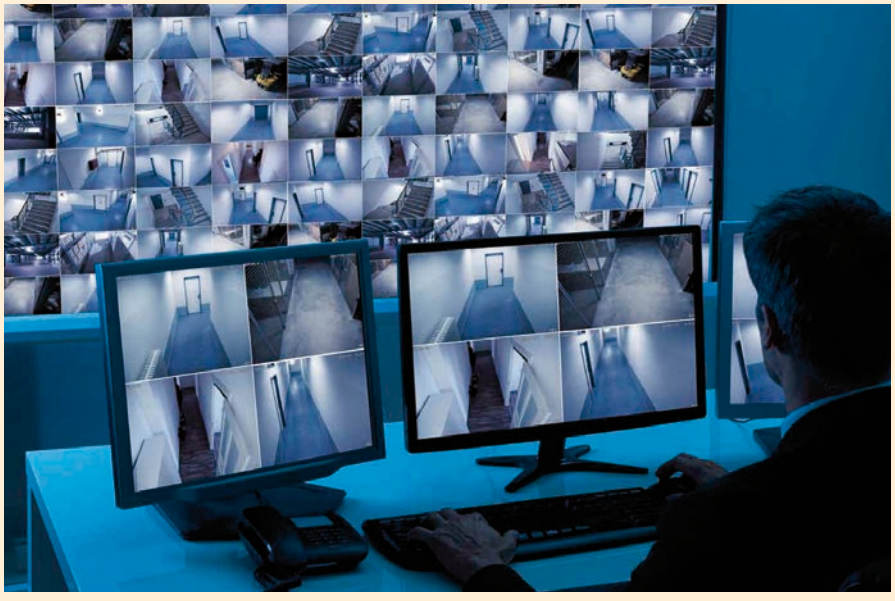
Nouvelle acquisition pour Azur Soft

Le spécialiste des solutions de sécurité unifiée Azur Soft vient d'acquérir Saratec, éditeur de logiciels français reconnu pour ses solutions intelligentes de sécurité et de sûreté. Pour Azur Soft, cette acquisition s'inscrit dans un plan stratégique amorcé il y a douze mois avec le rachat de Systel.

Saratec permet à Azur Soft de consolider son offre globale de sécurité unifiée au travers de solutions d'hypervision visant à unifier les opérations liées à la sécurité et la sûreté provenant de systèmes hétérogènes et à rendre toutes les tâches facilement accessibles grâce à une application client intuitive et unique.
« La synergie des technologies présente une forte complémentarité et une combinaison des savoir-faire respectifs avec pour objectif de déployer très largement les solutions. Le rachat de Saractec renforce les équipes techniques et commerciales ainsi que la capacité d'innovation d'Azur Soft sur ses marchés historiques de télévidéosurveillance/téléassistance, qui continue à être l'une des entreprises la plus reconnue de son secteur.»

Intérêt mutuel

Pour Marc Vaillant, Pdg d'Azur Soft, *« cette opération de croissance externe est au cœur de la stratégie d'Azur Soft et marque une étape supplémentaire dans notre volonté d'accroître nos investissements tant organiques qu'en croissance externe. Cette nouvelle acquisition vient compléter et renforcer l'ensemble de notre offre inégalée de collecte, de traitement et de transmission des informations de sécurité. »*
Chez Saratec, on se réjouit de l'opération. Comme le confirme Olivier Rancillac, son fondateur : *« Nous sommes ravis de rejoindre le groupe Azur Soft. Désormais, les solutions Saratec bénéficieront de la capacité d'innovation, de la dynamique marketing et de la solidité financière de la société Azur Soft. En unissant nos forces, nous allons accompagner davantage nos clients à travers le monde. Nos entreprises se complètent parfaitement : nous avons le même engagement en faveur de l'excellence technique et de l'innovation au service du client. »*
Rappelons que début 2017, Azur Soft a acquis Systel, un éditeur de progiciels temps réel dédiés à la sécurité, à la sûreté et à la surveillance technique. La fusion des offres des deux sociétés permettait déjà des synergies fonctionnelles, techniques et opérationnelles majeures.


© DR


© DR

Marc Vaillant

PDG D'AZUR SOFT

Que vous apporte l'acquisition de Saratec ?
Azur Soft veut résolument rester concentré sur le cœur de son métier qui est la télésurveillance et la télé-assistance. Mais avec le rachat de Saratec, nous préparons les années à venir pour nous positionner sur l'hypervision et faire d'Azur Soft un acteur à part entière de la gestion centralisée de la sécurité. Ce qui nous permettra aussi d'adresser de nouveaux marchés verticaux et d'offrir à nos partenaires télésurveilleurs de diversifier leur offre, notamment en matière de services, auprès de leurs clients. Cette deuxième acquisition est en cohérence avec notre plan stratégique amorcé il y a 12 mois avec une première acquisition, celle de la société Systel, positionnée sur le marché de l'hypervision des systèmes de sécurité.

Quel bilan tirez-vous de l'année 2018 ?
Il est plus que positif. Nous avons su « digérer » l'acquisition de Systel (en 2017), tout en développant notre activité à l'export où nous avons fait de gros progrès sur la zone alémanique. Dans les mois qui viennent, nous allons poursuivre notre rythme d'une introduction par an sur un marché étranger pour maintenir la croissance de notre chiffre d'affaires qui a atteint 6 millions d'euros l'année dernière.

RECONNAISSANCE FACIALE

Zetes a la confiance du club de Molenbeek

Le club de football belge RWD Molenbeek teste actuellement un système de reconnaissance faciale afin de faciliter et de fluidifier l'accès au stade des supporteurs.

© DR

Ainsi, les fans peuvent d'ores et déjà télécharger leur photo d'identité au moment de l'achat de leur billet en ligne pour permettre aux deux caméras de vidéosurveillance, installées à l'entrée, de comparer les photos téléchargées et les personnes dans la file d'attente. Résultat : un accès coupe-file pour les supporters reconnus. Ce portail automatique sera installé début 2019. La reconnaissance faciale est circonscrite aux contrôles d'accès ; il s'agit donc d'un avantage supplémentaire proposé aux abonnés du club, pour qui oublier son billet papier ne sera désormais plus synonyme de privation de stade ! Ce système, installé par Zetes, s'appuie sur la technologie de reconnaissance faciale de Panasonic. *« Grâce au système de détection, avec son logiciel de traitement des données rapide et fiable, nous disposons d'un accélérateur des contrôles d'accès au stade »*, explique Thierry Dailly, président du RWD Molenbeek.

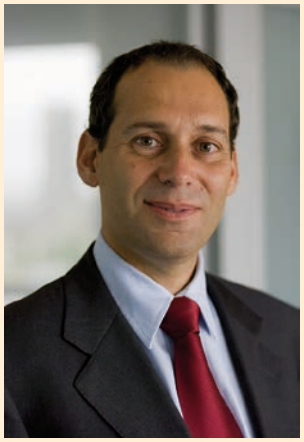
Pas d'enregistrement des images

Les photos téléchargées par les supporters sont stockées sur un serveur du RWDM, qui n'est pas raccordé à internet ni aucun autre réseau. Seul le personnel habilité du RWDM y a accès. Par ailleurs, les images prises par les caméras à l'entrée ne sont pas enregistrées afin de protéger la vie privée des supporters. Le système est encore en phase de test pour le moment, et la reconnaissance faciale n'est pas complètement opérationnelle. L'installation des portails automatiques, début 2019, permettra l'achèvement du test.

Rappelons qu'en avril 2017, Panasonic est devenu actionnaire majoritaire de Zetes, avant d'en prendre le contrôle à 100 % en juillet de la même année. Zetes, fondée en 1984, employait 1 100 personnes dans 21 pays de la région Emea en 2016. Le siège de la société se situe à Bruxelles.

ALAIN WIRTZ, PDG DE ZETES

« Ce projet est un exemple parfait des synergies innovantes nées de l'alliance entre Zetes et le groupe Panasonic. Le cœur de métier de Zetes ce sont les technologies d'identification. Nous espérons que ce projet offrira une vitrine à nos produits. La durée du test sera d'une année. »


© DR

INDUSTRIES DE SÉCURITÉ
MARC DARMON EST LE PRÉSIDENT DU NOUVEAU CSF*

Le gouvernement vient de créer un comité stratégique de filière (CSF) dédié aux industries de sécurité au sein du Conseil national de l'industrie (CNI). Sa présidence a été confiée à Marc Darmon, directeur général adjoint de Thales et président du Conseil des industries de la confiance et de sécurité (CICS).

Les comités stratégiques de filière correspondant chacun à une filière stratégique de l'industrie française, ont pour mission d'identifier de façon convergente, dans des « contrats de filière », les enjeux clés de la filière et les engagements réciproques de l'État et des industriels, d'émettre des propositions d'actions concrètes et de suivre leur mise en œuvre.

La filière des industries de sécurité, jusqu'à présent structurée dans le cadre du comité de filière des industries de sécurité et avec la participation du comité des industries de confiance et de sécurité, représente aujourd'hui plus de 4 000 entreprises travaillant dans la sécurité physique et numérique, 151 000 salariés et un chiffre d'affaires de 25 milliards d'euros dont 13 milliards d'euros à l'export.

** Marc Darmon est aussi président du CICS.*

© Vivotek

VIDÉOSURVEILLANCE
VIVOTEK RÉCOMPENSÉ

Six produits Vivotek de surveillance IP ont été récompensés lors des derniers Taiwan Excellence Awards. Il s'agit des caméras réseau H.265, IB9365-EHT, FD9365-EHTV et IP9191-HP. Ces trois caméras disposent d'un logiciel anti-intrusion Trend Micro embarqué, leur permettant de détecter automatiquement et de prévenir toute attaque sur l'identifiant mais également de bloquer tout événement suspect. Ainsi, les utilisateurs pourront bénéficier de hauts niveaux de sécurité réseau. La caméra ultra-HD IP9191-HP délivre des images d'une résolution quatre fois supérieure à celle de caméras standard, la qualité vidéo a été considérablement améliorée, lui permettant de capturer précisément les détails les plus fins. Des caméras réseau 180° et 360°, FE9391-EV, MS9390-HV et CC8371-HV, toutes équipées d'illuminateurs infrarouges garantissent une sécurité 24 heures sur 24.

© DR

PRESTATIONS DE SÛRETÉ
LE GROUPE RISK&CO VA CONSEILLER PARIS

La Business Unit Ingénierie de sûreté/sécurité du Groupe Risk&Co a remporté un important appel d'offres attribué par la Ville de Paris. Le marché concerne la réalisation de prestations d'audit-sûreté pour la sécurisation de plusieurs sites emblématiques de la capitale, comme le parvis de la cathédrale Notre-Dame, ou des infrastructures publiques comme la gare Rosa Parks. Et ce alors que la ville se prépare à accueillir de nombreuses manifestations culturelles et sportives dans les années à venir, à l'instar des Jeux Olympiques et Paralympiques de 2024. Dans ce contexte, le Groupe Risk&Co et ses ingénieurs-conseils concourent à la sécurisation de la capitale et de ses habitants.
Créé en 1994, le Groupe Risk&Co est le leader français du conseil et de l'ingénierie dans les domaines de la sûreté-sécurité et de la gestion des risques en France et à l'international. Le groupe propose un accompagnement global et intégré dans le domaine de la sûreté à l'international : dépollution pyrotechnique des futurs sites d'implantation, vérification de l'honorabilité des partenaires locaux, accompagnement des voyageurs d'affaires, mise en sûreté des expatriés, protection des infrastructures physiques et sécurité des systèmes d'information.

VIDÉOPROTECTION

Cibest reprend l'activité d'Eolane

Grâce à cette acquisition, Cibest va pouvoir se positionner sur les marchés de la vidéoprotection, du wi-fi haut débit, du comptage passagers, etc.

Cibest, spécialiste des solutions pour les transports et spécialisé dans la vidéoprotection, a repris l'activité vidéoprotection embarquée du groupe de sous-traitance Eolane, qui sera exploitée à travers la marque SCENE+. Dans le même temps, Cibest et Eolane initient un partenariat industriel et commercial assurant la continuité des fabrications en France et la pérennité des solutions existantes.
L'acquisition des activités de vidéoprotection permet à la société Cibest, implantée à Besançon, de maîtriser le cycle complet des produits de vidéoprotection de la conception des matériels et des logiciels à la fabrication et leur déploiement. Cibest sera ainsi en mesure de répondre à des offres complètes intégrant vidéoprotection, wi-fi haut débit, comptage passagers, écoconduite, etc. Combiné avec les compétences logicielles du groupe Cibest, le rapprochement permettra également d'accélérer les cycles d'innovation de ces solutions. Suite à cette acquisition, les activités combinées du nouveau groupe représentent un chiffre d'affaires de plus de 8 millions d'euros et un effectif global de 52 collaborateurs répartis sur les sites de Besançon, Paris et Belfort.
« Avec cette nouvelle acquisition, nous engageons Cibest et toutes ses équipes dans une nouvelle phase de développement de l'entreprise. Nous sommes ravis d'accueillir les équipes d'Eolane et de les associer à cette aventure », souligne Jean-Michel Favaro, président du Groupe Cibest.

© Eolane

DRONES

Genetec et Azur Drones signent un partenariat

La surveillance par drone est de plus en plus d'actualité dans le monde de la sécurité. La toute récente association entre Azur Drones et Genetec en est une nouvelle preuve.

© DR

Ce partenariat a pour objectif d'intégrer le drone automatisé Skeyetech dans la plate-forme de sécurité Security Center afin de permettre aux équipes de sécurité de contrôler des drones de surveillance directement depuis Security Center. Fruit de trois ans de recherche et développement par les équipes d'Azur Drones, Skeyetech est un outil de surveillance par drone automatisé plutôt abouti. En effet, grâce à sa station d'accueil et de rechargement, le drone Skeyetech est opérationnel 24 h/24 et 7 j/7 pour des rondes automatiques ou des missions de levée de doutes en cas d'alerte. Rapide et performant, le drone améliore significativement la réactivité des équipes de sécurité tout en évitant de les mettre en danger.

Des clients demandeurs

« Nos clients sont en recherche constante de nouvelles solutions pour renforcer la sécurité de leurs sites sensibles, explique Jordan Jaumeau, directeur du groupe de partenariats au développement chez Genetec. *Capables d'arriver en quelques secondes sur une zone d'alerte, les drones fournissent des informations précieuses sur la situation et permettent ainsi aux opérateurs de prendre rapidement les bonnes décisions opérationnelles. Qu'ils soient utilisés pour des rondes périmétriques, évaluer des incidents à distance ou suivre des interventions, les informations fournies par les drones Skeyetech pourront, grâce à ce partenariat, être collectées et exploitées directement dans l'interface Security Center. »*

JEAN-MARC CRÉPIN, PRÉSIDENT D'AZUR DRONES

« Nous sommes persuadés que les drones vont bouleverser le marché de la sécurité dans les années à venir. C'est pour cela que nous avons développé la solution 100 % automatisée Skeyetech. Le partenariat stratégique avec Genetec va permettre aux acteurs de la sécurité d'exploiter enfin le plein potentiel d'un drone de surveillance. »

© DR

ESSD
AMARANTE INTERNATIONAL RETENUE PAR L'UE

Le Français Amarante international (20 millions d'euros de CA en 2018), allié au Canadien GardaWorld, a été choisi par l'Union européenne pour assurer la sécurité des personnels et des sites de l'UE à Kaboul (Afghanistan). Ce contrat de quatre ans reconductible sur deux ans, est d'importance : 85 millions d'euros, auxquels s'ajoutent 40 millions afin de couvrir d'éventuelles autres prestations. Amarante et GardaWorld vont déployer 300 personnes : une centaine d'expatriés, autant de TCN (Third Country Nationals, en l'occurrence des Gurkhas) et une centaine d'employés locaux.
Garda assure la gestion des activités quotidiennes, de la logistique et des prestations pratiques, tandis qu'Amarante est chargée du contrôle qualité et de la relation client.
Pour Amarante, dont un des actionnaires est le groupe Seris depuis 2015, ce contrat vient s'ajouter à d'autres contrats remportés au Tchad, en RCA/Burundi, au Niger, au Venezuela, en Irak et en Afghanistan.

© DR

INTRUSION

BY DEMES GROUP DISTRIBUE VISONIC

By Demes Group est depuis peu le nouveau distributeur officiel pour la France des systèmes de sécurité Visonic, filiale du géant Johnson Controls.
Cet accord va permettre aux clients de By Demes Group d'avoir un accès direct aux produits Visonic avec un stock permanent et le meilleur service possible. Ils comprennent les centrales câblées Visonic Hybrid et les systèmes par radio Powermaster 10/30/33, intégrant la technologie PowerG et certifié NF-A2P.
Les produits sont déjà disponibles pour tous les clients de By Demes France et sont commercialisés à travers son vaste réseau, avec l'excellent support technique et commercial qui caractérise le distributeur leader en matériel électronique de sécurité sur le marché ibérique et de référence au niveau international.
Visonic rejoint ainsi l'ensemble de grandes marques de vidéosurveillance, d'intrusion et de contrôle d'accès distribuées par By Demes Group en France : Huyndai, Dahua, Pyronix, Rosslare…

ROBOTS

Le robot de TBC en test chez Engie

Le premier prototype de robot autonome de sécurité, Jack, développé par la société TBC-France, a été livré, le 25 octobre 2018, au Lab Drones & Robots du Crigen, le centre de recherche corporate du groupe Engie.

Le partenariat entre TBC-France et Engie Lab Crigen vise à finaliser le développement du robot et cadre une collaboration technique basée sur un processus de conception centré sur l'utilisateur.
Le robot Jack de TBC-France a été identifié par le Lab Drones & Robots du Crigen comme la meilleure solution technologique terrestre pouvant répondre aux besoins de sécurisation des sites du groupe ou exploités par Engie.
Les enjeux des tests utilisateur en conditions réelles et les codéveloppements sont importants à la fois pour TBC-France et pour le Crigen. Ils doivent permettre à TBC-France de valider le prototype de Jack, ses performances et ses fonctionnalités. Des résultats positifs ouvriront au robot les marchés ciblés par TBC-France dont celui de l'énergie. Pour le Crigen, l'objectif est d'implanter ses propres briques technologiques (navigation, sécurisation du robot, insertion dans un environnement industriel) pour répondre aux besoins d'Engie, de vérifier la fiabilité de Jack pour en faire une référence à recommander aux directeurs de sites et d'étudier les possibilités de complémentarités avec d'autres solutions de sécurité et les possibilités d'évolution de l'équipement (ajout de capteurs de mesures).

IA embarquée

Le robot autonome de surveillance Jack est équipé d'une intelligence artificielle embarquée, d'une navigation ultra-précise et de technologies évoluées pour patrouiller – en toute autonomie – de grands périmètres intérieurs et extérieurs, et procéder à des levées de doute rapides en cas d'alarme.
Ses huit caméras visibles et infrarouges ainsi que sa caméra PTZ lui permettent de transmettre en temps réel les images au poste de surveillance, de jour comme de nuit, et de détecter d'éventuelles anomalies.
Cyril Nguyen, directeur de la sureté du groupe Engie, considère que *« le secteur de la sécurité et de la surveillance connaît lui aussi sa révolution avec l'arrivée de solutions drones et robots. C'est un enjeu fort pour le groupe tant pour la protection de ses propres sites tertiaires et industriels, que pour le développement des offres de service auprès de ses clients. Les activités R&D du Crigen visent, avec des partenaires comme TBC-France, à la mise au point de solutions internes innovantes associant des drones et des robots pour répondre rapidement aux besoins opérationnels du groupe. »*

© DR

ANALYSE VIDÉO

Pryntec renforce son réseau de vente indirecte avec Azenn

Le spécialiste des solutions hardware et software pour l'analyse d'images vidéo Pryntec, marque du groupe TEB, continue ainsi son extension dans la commercialisation de ses solutions en signant son deuxième distributeur en France.

Fort d'un réseau national de près de 3 000 revendeurs et donc de partenaires essentiels pour la marque, Azenn est un acteur de poids, partenaire privilégié de nombreux intégrateurs et installateurs professionnels nationaux et spécialistes régionaux.

Ce rapprochement va permettre à Pryntec de partir à la conquête de nouveaux marchés comme les data centers, la logistique ou encore les infrastructures de bâtiments. *« Il y a une synergie évidente entre notre expertise et le cœur d'activité d'Azenn, qui a permis d'aboutir à ce partenariat. Avec l'IP, la vidéo est devenue un média important dans les infrastructures réseaux et les professionnels de l'IT doivent désormais gérer le réseau vidéo. Face à ce marché dynamique et en forte croissance, nous avons la capacité de répondre aux problématiques de ces spécialistes et développer nos parts de marché sur l'ensemble des projets vidéo »*, explique Emmanuel Dubois, directeur commercial et marketing de Pryntec.

Certification Pryntec

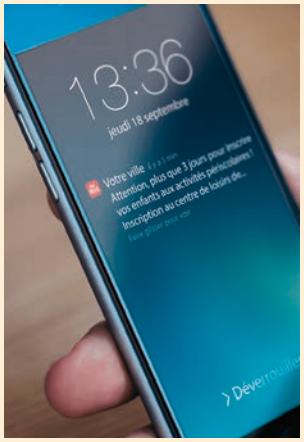
Afin de proposer les meilleures solutions de vidéosurveillance et d'analyse de flux, les équipes d'Azenn ont été certifiées Pryntec pour maîtriser l'ensemble des solutions catalogue du groupe et ainsi les valoriser auprès de leurs différents partenaires sur le terrain.

« Nous avons la volonté de placer Pryntec parmi les acteurs qui compte au sein de notre large écosystème d'installateurs, d'intégrateurs et de revendeurs. En étant "Distributor certified" Pryntec, Azenn a également la capacité de valoriser des solutions catalogue agiles, fiables et au savoir-faire technologique reconnu. Pryntec a également à cœur de proposer des solutions pour répondre à tous les besoins, y compris ceux non couverts par la vidéo traditionnelle. C'est une vision que nous partageons », confirme Gaetano Schembri, responsable marketing & communication d'Azenn.

Azenn apportera sa dimension conseil et valorisera les quatre solutions piliers Pryntec : le TUB Camera et la borne vidéo mobile, d'une part, et les solutions logicielles Digipryn et Prynvision d'autre part.

Des solutions particulièrement adaptées pour pénétrer des secteurs sur lesquels Azenn était peu présent : la grande distribution et la logistique, la vidéo urbaine, l'intelligence artificielle…

© Azenn



© DR

INTÉGRATEURS
SOGETREL INVESTIT DANS NEOCITY

Sogetrel, ETI indépendante et leader français de l'intégration de réseaux et de systèmes de communication, annonce son entrée au capital de Neocity, start-up innovante et déjà acteur de référence sur le marché des applications mobiles pour les villes.

Cet investissement, mené au côté de la Caisse des dépôts et des consignations, vise à consolider le partenariat stratégique entre l'intégrateur et la start-up, pour apporter toujours plus de service aux collectivités innovantes et connectées.

Créée en 2014, Neocity conçoit des applications sous iOS et Android pour les mairies, afin de faciliter la vie des citoyens et d'établir un nouveau canal de communication entre les élus et les administrés.

Sogetrel s'appuie ainsi sur cette expertise pour mettre le citoyen au cœur de la démarche Smart City de ses clients collectivités, comme le montrent les projets en cours à Chartres et Asnières.

Pour Xavier Vignon, président de Sogetrel, *« cet investissement s'inscrit dans l'ADN entrepreneurial du groupe Sogetrel et confirme nos fortes ambitions sur la thématique de la Smart City et des usages numériques au service des territoires. »*

CONTRÔLE D'ACCÈS

Nouveau contrat pour STid outre-Atlantique

Le Français Stid renoue avec le succès aux États-Unis. Le service de police de l'université du Texas, à Arlington, a implémenté sa solution d'accès mobile.

© DR

Pour contrôler les accès à ses locaux et faciliter les migrations technologiques vers des niveaux de sécurité avancés, la police de l'UTA d'Arlington a sélectionné les lecteurs Architect Blue multitechnologies et la solution STid Mobile ID. Cette solution mobile réinvente le contrôle d'accès en rendant l'identification ludique et beaucoup plus instinctive pour l'utilisateur. Elle transfère le badge d'accès sur le smartphone avec des modes d'identification innovants, en complément du badge.

STid s'est démarqué rapidement

« Nous avons analysé l'ensemble des solutions du marché. L'ergonomie, le niveau de sécurité et les outils de configuration simplifiant la mise en œuvre de la solution sont les critères qui ont permis à STid de se démarquer très rapidement. Plus de 130 utilisateurs, officiers de police et professionnels de la sûreté utilisent STid Mobile ID au quotidien – indispensable pour protéger l'accès à nos infrastructures », témoigne un sergent-chef de la police de l'université du Texas d'Arlington.

De son côté, Vincent Dupart, directeur général de STid, conclut : *« Ce nouveau déploiement est le résultat de l'adoption croissante de nos lecteurs d'accès haute sécurité et instinctifs sur le territoire nord-américain. Il s'inscrit dans notre stratégie de développement initiée en 2013, année où STid devient le premier fabricant à obtenir la certification de sécurité de premier niveau (CSPN) délivré par l'Anssi. En 2016, STid a entrepris une diversification géographique de ses activités en ouvrant des bureaux à Londres et à Mexico. STid poursuit cette année son développement sur le marché nord-américain et ouvre STid NA Inc. à Irving (Texas) en proposant les lecteurs de contrôle d'accès les plus récompensés au monde. »*

Le petit français n'a pas fini de challenger les gros puisqu'il prévoit un plan d'investissement entre 2019 et 2023 pour devenir le référent européen du contrôle d'accès.


© DR

3 QUESTIONS À Vincent Dupart,

DIRECTEUR GÉNÉRAL DE STID

Cette nouvelle référence aux États-Unis est la preuve de la pertinence de votre développement outre-Atlantique…

Tout à fait. Il vient matérialiser les efforts que nous avons fournis depuis un peu plus d'un an pour nous implanter sur le marché américain. Mais nous n'allons pas nous arrêter là. Nous avons encore un certain nombre de projets sur lesquels nous nous positionnons et pour lesquels nous espérons bien voir nos efforts couronner de succès et qui viendront valider encore plus fortement notre stratégie de développement sur le marché américain et y renforcer nos ambitions.

Quel bilan tirez-vous de l'année écoulée ? Quels sont vos objectifs pour celles à venir ?

2018 a confirmé la bonne santé de STid. Par ailleurs, pour accompagner notre développement, nous allons réinjecter 5 millions d'euros dans l'entreprise – via de l'endettement et une augmentation de capital – pour accompagner notre croissance, renforcer notre R&D, développer nos filiales à l'étranger et recruter 22 personnes en 2019. Nous nous sommes d'ailleurs donner des objectifs ambitieux. D'ici 2023, nous espérons atteindre un CA de 40,4 millions d'euros – 35,4 millions pour le contrôle d'accès et 5 millions pour la traçabilité – répartis comme suit : 20,4 millions d'euros en France et 20 millions d'euros de CA à l'export. Nous allons revoir notre distribution en faisant en sorte que nos produits y soient plus présents via nos partenaires constructeurs.

INCENDIE

Le Réseau DEF innove dans le recrutement

Démarche innovante dans le monde de la sécurité incendie : pour attirer et recruter, le Réseau DEF a créé son premier Mooc. Son objectif est aussi de pré-qualifier et former les candidats.

Pour bien informer les candidats en phase de recherche d'emploi et fluidifier les premières phases du processus de recrutement, le Réseau DEF vient de créer son premier Mooc métiers de la sécurité incendie.

« C'est un nouveau canal de recrutement qui est 100 % en phase avec les attentes des jeunes générations, note Djamila Nahet, DRH du Réseau DEF. *Outre son pouvoir d'attraction, il nous permet de nous assurer de la motivation des candidats, de tester leurs compétences et de les former avant même leur intégration. Je trouve aussi que c'est un formidable outil d'orientation pour les jeunes qui découvrent nos métiers et notre entreprise. Et le message est clair : ce sont votre motivation et vos compétences qui vont faire la différence ! »*

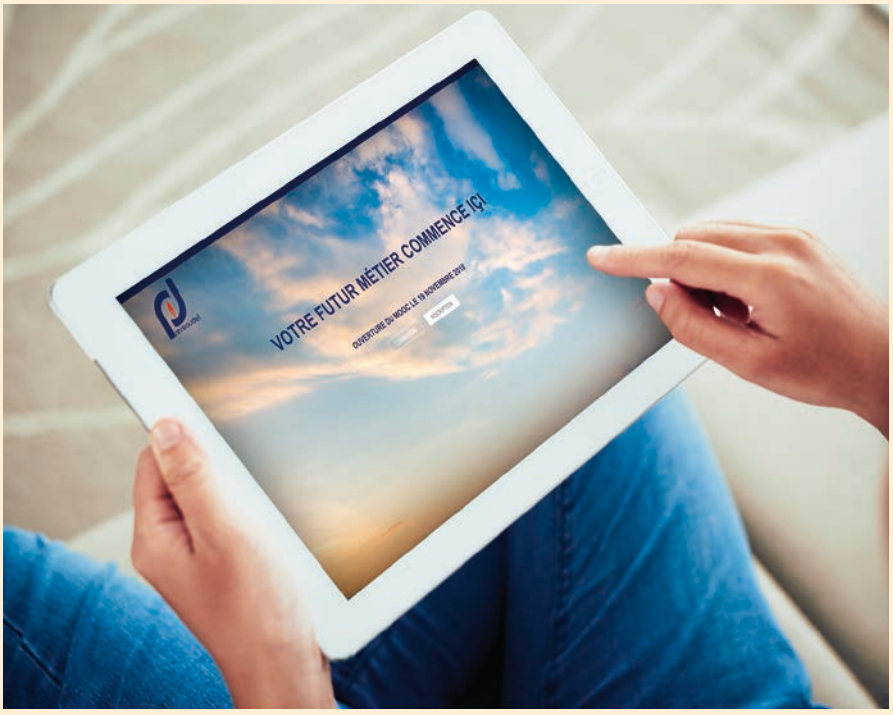
Formation ouverte à tous

Une formation en ligne, gratuite et ouverte à tous, permet aux candidats de découvrir le secteur de la sécurité incendie et de choisir de se former à l'un des trois grands métiers qui recrutent : technicien, commercial ou bureau d'études.

À travers ce module (2 heures de formation), le candidat va découvrir tous les aspects de son futur métier via des contenus pédagogiques et ludiques : témoignages vidéo, ressources documentaires, quiz... Chapitre après chapitre, il va ainsi monter en compétences et être sélectionné à la fin, non plus pour son seul diplôme, mais bien pour ses compétences et son appétence pour le poste choisi.

Le Réseau DEF a ouvert la première session en novembre dernier. Elle sera encore accessible jusqu'à fin janvier 2019 et quatre sessions jalonneront l'année 2019 en mars, juin, septembre et novembre. L'adresse de connexion pour découvrir ce Mooc et intégrer le processus de recrutement :

➔ https://recrutement.reseau-def.com



© DR

© DR

2 QUESTIONS À Djamila Nahet,

DRH DE RÉSEAU DEF

Quels sont les constats qui ont présidé à la création de ce Mooc ?

Nous sommes partis d'un constat assez simple : il est de plus en plus difficile de recruter dans nos métiers. Nous sommes loin de l'époque où il suffisait de passer une annonce pour recruter de nouveaux collaborateurs. Par ailleurs, nous constatons que les compétences requises se font de plus en plus rares et nous avons du mal à trouver les profils qui nous intéressent, faute de formations scolaires dédiées à la sécurité incendie. Enfin, notre secteur crée des emplois et il nous semblait nécessaire d'ouvrir le champ des possibles pour permettre à un large panel de chercheurs d'emploi de nous découvrir et de s'engager sur cette voie.

Concrètement, comment cela fonctionne-t-il ?

Le Mooc est un des moyens innovants que nous mettons en place pour « réinventer le recrutement ». Il nous permet de toucher une cible très large de candidats apprenants et d'attirer par exemple plus de femmes sur les métiers techniques. Gratuit et ouvert à tous 24 h/24, le Mooc permet non seulement aux candidats intéressés de faire acte de candidature mais aussi d'acquérir certaines compétences utiles dans notre secteur. Il devrait aussi susciter la curiosité chez les candidats, et leur montrer que nos métiers et filières sont innovants technologiquement.

Découvrir la sécurité incendie, s'engager dans cette filière et découvrir le Réseau DEF sont les pierres angulaires de notre Mooc. Il a été réalisé par nos collaborateurs pour recruter leurs futurs collègues et démontre que nos équipes sont impliquées dans la vie des 60 entreprises du Réseau DEF.

VIDÉOSURVEILLANCE

Axis a toujours la confiance du Puy du Fou

Entre Axis et le célèbre parc d'attractions, c'est une longue histoire puisque voilà déjà dix ans que la première caméra du fabricant suédois a été déployée sur le site par l'intégrateur I3S Intégration. Aujourd'hui, le parc dispose de 300 caméras.

L'un des projets les plus emblématiques est le développement de l'installation de vidéoprotection du plus grand spectacle de nuit au monde : La Cinéscénie. 13 200 spectateurs présents chaque soir, 4 000 comédiens bénévoles y évoluent, plongés dans le noir et à ciel ouvert. Il a fallu installer 35 stations de travail dédiées à la surveillance des images des caméras pour pouvoir réagir rapidement en cas d'incident, guider les secours depuis le poste de sécurité pour les spectateurs en situation de malaise ou encore sécuriser la circulation des piétons aux abords des tribunes – et notamment en cas d'évacuation. En 2017, le spectacle évolue et intègre des drones synchronisés dans la scénographie. Le directeur sécurité du Puy du Fou, Laurent Martin, et Jean-Marie Laurent d'I3S Intégration déploient donc des caméras Axis P1435-LE pour surveiller les drones à 350 mètres du sol et des caméras Axis P1367 pour zoomer sur la scène et ainsi assurer une surveillance des artifices après leur déclenchement. Aujourd'hui, 300 caméras IP Axis sont installées sur l'ensemble du site et couvrent la quasi-totalité du parc. Par ailleurs, quelques caméras analogiques ont été conservées et sont reliées au réseau par des encodeurs Axis.

Contrôle d'accès Axis

Satisfait des fonctionnalités proposées par les caméras Axis et préférant s'adresser à un fournisseur unique, Jean-Marie Laurent commence à déployer en 2017 du contrôle d'accès pour gérer les flux entrants des salariés et des bénévoles. Des portiers vidéo IP AXIS A8004-VE sont installés avec des caméras Axis P3225-LVE pour la levée de doute en cas d'oubli de badge d'accès. Les produits sont connectés à Genetec Synergis, cette solution Axis/Genetec a l'avantage d'être autonome localement lors d'une coupure logicielle ou de réseau. À la reconnexion, l'historique des accès est rétabli et transféré de manière automatique.
D'ici 2020, entre 80 et 100 caméras supplémentaires seront installées pour répondre au développement du parc et aux innovations apportées à l'offre de spectacles. L'objectif reste de minimiser le temps de détection et de réaction pour apporter une aide aux opérateurs sur place.

© DR

© Mobotix

VIDÉOSURVEILLANCE

MOBOTIX, CERTIFIÉE CONTRE LES CYBERATTAQUES

On le sait, le fabricant allemand a développé le « concept cactus » pour un système vidéo de bout en bout fiable et entièrement protégé contre les cyberattaques. Mobotix a passé avec succès les tests de sécurité numériques répondant aux exigences de BSI (Office fédéral allemand de la sécurité des technologies de l'information), l'institution allemande équivalente à son homologue en France, l'Anssi. Ces tests ont été effectués par Syss, une entreprise certifiée par BSI et réalisés sur notre gamme Mx6 et sur notre logiciel MxMC garantissant un système de vidéoprotection intègre.

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 2019
n°251

SOMMAIRE

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

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

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

Ce numéro contient *L'annuaire de la sécurité sûreté* et un encart AccesSecurity

ÉDITO

© DR

On doit pouvoir expérimenter !

Notre dossier sur les smart cities le démontre une fois de plus : les fabricants et développeurs français de solutions de sécurité n'ont pas à rougir face à la concurrence étrangère. Mais, malheureusement, ces solutions ne peuvent pas, à l'inverse de ce qui se fait dans certains pays, être expérimentées et testées en grandeur nature…

Un exemple : un système intégrant du deep learning ou de l'auto-apprentissage doit pouvoir être évalué sur le terrain. Or, les concurrents de nos acteurs nationaux peuvent le faire beaucoup plus facilement et sur de plus grandes échelles. Alors que, s'il y a bien un domaine dans lequel la phase de tests et d'expérimentation est incontournable, c'est bien celui, que nous nommerons, au sens large, de l'intelligence artificielle.

Cette impossibilité de tester l'efficacité d'une solution est une vraie distorsion de concurrence à laquelle doivent faire face les Français. Il faut absolument que les pouvoirs publics se penchent sur la question dès maintenant. Afin que les grands événements internationaux que va accueillir notre pays – Coupe du monde de rugby, JO à Paris…– soit sécurisés par des solutions françaises ayant fait la preuve de leur pertinence. Ne serait-ce que pour en faire une vitrine de nos savoir-faire…

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

© Getty Images

SÉCURITÉ DES ENTREPRISES

Fonction sûreté : comment réussir sa transformation au sein de l'entreprise ?

Les métiers de la sécurité changent. Ne serait-ce qu'à cause de l'apparition des nouvelles menaces comme la cybersécurité ou la menace terroriste. Dans une étude*, le cabinet PwC apporte un éclairage et des pistes afin de relever ce défi majeur.

Parmi les tendances clés identifiées par les experts PwC, la centralisation de la fonction sûreté est actuellement à l'œuvre. En effet, plus de 50 % des entreprises interrogées tendent à centraliser leurs dispositifs de sûreté en créant un seul département au niveau central, pilotant la gouvernance et les opérations. Ainsi, les directions centrales de sûreté se structurent autour de pôles de compétences dotés d'experts en matière de sûreté physique, de gestion de crise, d'intelligence économique, d'investigation et de cybersécurité.

« On assiste à une véritable transition dans la structure organisationnelle des départements sûreté des entreprises. Il y a un début de prise de conscience des dirigeants quant à la nécessité de professionnaliser et de structurer cette fonction au sein de l'entreprise, explique Olivier Hassid, directeur conseil en sécurité, sûreté des infrastructures et intelligence économique chez PwC. *C'est souvent l'arrivée d'un nouveau directeur sûreté qui permet d'impulser ces changements. »* L'apparition de nouvelles crises de sûreté à l'instar de NotPetya/WannaCry et les menaces terroristes ont également été déterminantes.

Force est de constater que les entreprises françaises sont moins matûres sur la centralisation de la fonction sûreté par rapport aux entreprises anglo-saxonnes.

Ce nouveau modèle implique l'implémentation d'un nouveau cadre de référence qui s'articule autour de trois lignes de défense qui s'appuie sur la définition claire et préalable des rôles et des responsabilités propres à chaque fonction.

Différentes lignes de défense

Ainsi, la première ligne de défense est chargée d'appliquer les politiques et les procédures de sûreté et de gérer les incidents et les risques au quotidien. La deuxième ligne de défense est responsable de la gouvernance en matière de sûreté. À ce titre, elle est à l'origine de la définition et de l'articulation de la stratégie, des politiques et des standards de sûreté. La troisième ligne de défense élabore et met en œuvre un programme d'audit permettant à la direction générale de s'assurer de la capacité de l'organisation à maîtriser ses risques en contrôlant, à échéances régulières, la mise en œuvre des standards.

« Au-delà du modèle centralisé, il est important de développer

2 QUESTIONS À

OLIVIER HASSID

Directeur conseil en sécurité, sûreté des infrastructures et intelligence économique chez PwC

Quels sont les principaux enseignements de votre étude ?

Le premier est évidemment le fait que nous assistons à une véritable transformation de la fonction sécurité-sûreté dans les entreprises. Tant en termes de maturité que de professionnalisation. Les directions sécurité-sûreté, que ce soit aux États-Unis, en Allemagne, au Japon ou en France, sont de plus en plus centralisées et fonctionnent comme un pôle central, un véritable « Corporate Security » qui prend en charge la rédaction des standards, vérifie leur déploiement, réalise des audits… Parallèlement, on constate également un changement dans les profils recrutés par les directions sécurité-sûreté. On y intègre désormais des experts des données, de la cybersécurité… favorisant ainsi le rapprochement entre les directions sécurité-sûreté et les directions informatiques. Par ailleurs, notre étude montre que les entreprises ont compris qu'il fallait sortir de la logique du fonctionnement en silo et donc favoriser la collaboration entre toutes les directions qui ont à traiter du risque et de ses possibles impacts pour l'entreprise et son activité. Enfin, on doit souligner le fait que de plus en plus de sociétés se dotent de plates-formes de gestion de l'information pour remonter des incidents – cyber ou sûreté – afin de disposer de tableaux de bord, d'indicateurs leur permettant d'anticiper, de prévenir les crises.

Quels sont les points d'amélioration que révèle votre étude ?

Pour le cas de la France, on doit souligner le fait qu'à l'inverse des groupes anglo-saxons, par exemple, il existe un vrai retard sur ce que nous appelons « la troisième ligne de défense. » C'est-à-dire le fait de faire vérifier, valider sa politique de sécurité-sûreté par un tiers de confiance. Chose que certains de nos clients étrangers nous demandent régulièrement. Par ailleurs, et ce pour toutes les entreprises, quelle que soit leur nationalité, leurs directions sécurité-sûreté ne sont pas encore assez impliquées en matière de « compliance » et ne participent pas, par exemple, à la vérification préalable de l'intégrité des tiers parties travaillant avec leur entreprise. Enfin, en ce qui concerne la gestion de crise, la direction sécurité-sûreté doit encore définir son scope d'intervention et aller au-delà de la simple action sécuritaire.

une véritable culture de sûreté car l'efficacité de la fonction sûreté repose aussi sur l'engagement de tous les collaborateurs de l'entreprise qui deviennent aujourd'hui des véritables ambassadeurs et acteurs de la sûreté. L'entreprise doit pouvoir favoriser l'appropriation de cette culture grâce à des formations individualisées pour les personnes à hautes responsabilités ainsi que des mesures concrètes parfois innovantes comme des bootcamps sûreté ou des "serious game" qui sont de plus en plus utilisés au sein des entreprises », poursuit Olivier Hassid.

L'IE au cœur de ce nouveau modèle

Afin d'être proactive et toujours plus efficace, la fonction sûreté est en quête de nouveaux outils techniques et organisationnels. D'après l'étude, plus de 80 % des entreprises interrogées ont des services dédiés à l'IE. Rattachées à la direction sûreté ou à la direction de la stratégie, les cellules d'intelligence économique sont chargées d'identifier les menaces et de les réduire, mais aussi de favoriser le développement de l'entreprise et d'être un soutien aux dirigeants dans la prise de décisions.

De plus, compte tenu du besoin permanent de veille liée aux enjeux de sûreté, les grands groupes internationaux mettent en place des centres d'analyse de risques et de réaction (« Security Operations Centers ») qui assurent le monitoring de situations opérationnelles 24 h/24. Cette pratique est notamment très efficace en matière de cybersécurité, enjeu majeur qui mobilise différentes expertises au sein de l'entreprise.

Meilleure collaboration face à la cybersécurité

PwC constate que les responsables sûreté ont également vu leur rôle évoluer : ils sont aujourd'hui majoritairement rattachés à un membre du comité exécutif ce qui permet au département sûreté de gagner en crédibilité et en légitimité. Le directeur sûreté peut être à la fois considéré comme le responsable de la sécurité physique et de la sécurité de l'information. Dans certains cas, il peut même être également le responsable de la sécurité digitale.

Ainsi, l'étude souligne la nécessité du décloisonnement entre les fonctions et la mutualisation des compétences avec la direction de la sécurité des systèmes d'information. Ceci est aujourd'hui d'autant plus crucial face aux cybermenaces. Selon l'étude, si près d'une entreprise sur deux a entamé cette démarche, seuls 17 % des responsables de la sécurité des systèmes d'information (RSSI) sont aujourd'hui rattachés au directeur de la sûreté. ■

***** *PwC, « La transformation de la fonction sûreté : vers un nouveau paradigme. Retours sur les pratiques d'entreprises à l'échelle mondiales ».*

CYBER INTELLIGENCE : PWC PEUT VOUS ACCOMPAGNER

Le pôle Cyber Intelligence de PwC rassemble l'ensemble des expertises cyber au sein de PwC : cybersécurité, sécurité, sûreté, intelligence économique, gestion de crise et investigations. Ces 150 experts en France proposent un ensemble complet de services touchant tous les aspects du risque cyber : de la stratégie jusqu'aux opérations, en passant par la gestion de crise. Comme le souligne Ludovic de Beauvoir, managing partner clients and markets chez PwC, ce pôle a pour rôle *« d'accompagner les entreprises sur leurs enjeux cruciaux de cybersécurité et de sécurité. »* À noter que le pôle a été récemment rejoint par Thierry Delville, ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.

© Getty Images

MÉTIERS DE LA SÉCURITÉ/SÛRETÉ EN ENTREPRISE

Le CDSE dresse un panorama de la filière

La commission carrière, emploi, formation du CDSE a publié son étude sur la filière sécurité-sûreté corporate* (SSC). Le constat est clair : pour assurer la « sécurité globale » en entreprise, la filière des métiers SSC doit se consolider pour affronter des défis de plus en plus complexes.

Face à la diversification des menaces et des risques (cyber, terrorisme, géopolitique), les enjeux de sécurité et de sûreté doivent être intégrés pleinement à la stratégie des entreprises. Cette diversification s'accompagne d'une complexité croissante, qui accentue le besoin de spécialisation et d'expertise des métiers de la filière.

Confrontées à ce double phénomène, les directions sécurité-sûreté en entreprise doivent adapter leur organisation et leurs besoins souvent méconnus. Par ailleurs, un travail important d'harmonisation de la communication sur ces métiers doit être mené.

Ce qu'il faut retenir de cette étude :

- La direction SSC évolue vers un positionnement d'anticipation, de prévention, de protection et de création de valeur, en véritable partenaire business ;
- Dans 74 % des cas, la direction SSC est rattachée à la direction générale ou au secrétariat général ;
- Que ce soit au sein des entreprises ou auprès d'acteurs institutionnels externes (États, collectivités, ambassades), la direction SSC multiplie les interactions et doit adapter son positionnement ;
- Pour attirer et fidéliser les futurs directrices et directeurs sécurité-sûreté corporate, la filière doit construire des parcours de carrières et accentuer la féminisation de ses métiers.

Un référentiel métiers

Cette étude a permis au CDSE de créer un référentiel des métiers de la SSC, répartis en 12 fonctions identifiées, de la gouvernance au conseil ou au déploiement opérationnel. Pour le CDSE, ce référentiel inédit doit permettre de faire émerger un positionnement collectif de la filière, au service de la « sécurité globale » des entreprises. ■

** Étude sur la filière sécurité-sûreté corporate : enquête statistique par questionnaire auprès de 187 répondants issus d'entreprises membres du CDSE dotées d'une direction sécurité-sûreté corporate (SSC) en France, suivie de 30 entretiens avec des acteurs de la filière sécurité-sûreté en entreprise.*

TRANSPORTS EN COMMUN

La Ratp teste les caméras mobiles pour ses équipes de sûreté

Depuis quelques semaines, la RATP expérimente l'utilisation de caméras mobiles au sein de ses équipes de sûreté. L'agent peut, par exemple, déclencher une vidéo, et au besoin fournir des images grâce à un logiciel de preuves numériques. Les caméras testées sont fournies par Axom qui équipe déjà plusieurs villes en France et dans le monde. Comme au Royaume-Uni où au terme d'un appel d'offres et d'une période de test à l'échelle nationale, Axon a ainsi déployé 2840 caméras piétons pour la police britannique des transports (BTP) fin 2017. Le système de gestion numérique des preuves Evidence.com est venu également compléter l'équipement matériel pour une durée légale d'utilisation de cinq ans. *« Cet essai de caméras piétons au cours de la dernière année s'est révélé utile pour accélérer les décisions de justice en faveur des victimes,* expliquait à l'époque Paul Brogden, chef adjoint du BTP. *Non seulement les caméras fournissent des preuves vitales dans certains cas, mais elles protègent également les agents contre les plaintes malveillantes et rassurent le public lorsqu'ils arpentent les stations et les trains. »* ■

© GEOFFROY VAN DER HASSELT / AFP

FORMATION INCENDIE

Le Gefpi lance un label


© Gefpi

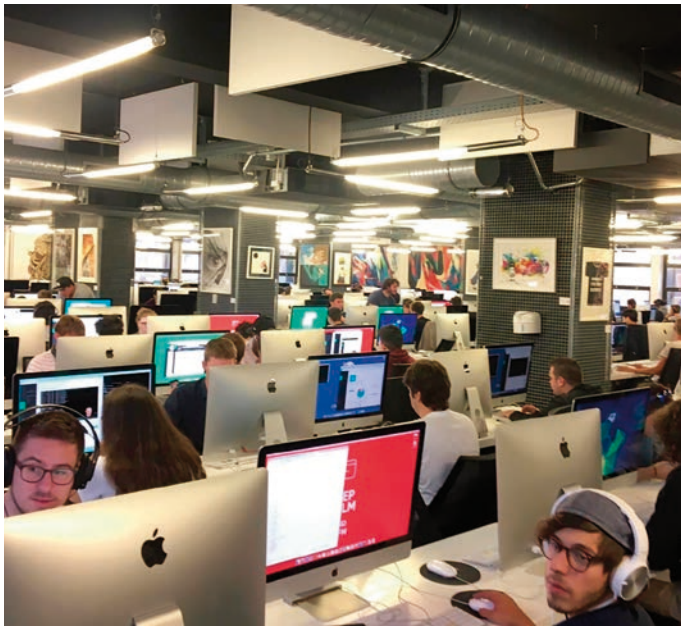
Un constat d'abord : face à une offre pléthorique et une obligation de formation, les employeurs semblent souvent désorientés. C'est pourquoi le Gefpi a décidé d'apporter des éléments clairs d'aide au choix. Sur la base d'un travail d'analyse fourni, de retours d'expériences partagés, et avec le concours d'une tierce partie indépendante, le Gefpi est donc à l'origine de la création d'un label distinctif en faveur des bonnes pratiques du domaine de la formation-prévention au risque incendie. Le label Gefpi, décerné sur la base d'un référentiel, définit ce que doivent être les actions, les méthodes et les outils nécessaires au niveau de qualité requis tout au long du processus de formation. Le Gefpi (Groupement des entreprises de la formation-prévention au risque Incendie) est né en 2015 de la volonté d'entreprises spécialistes de la sécurité-incendie de promouvoir une offre de service de haute qualité en matière de préparation des personnes face à ce risque important. Il regroupe des intervenants reconnus en matière de formation et il vise à une promotion continue des bonnes pratiques. Il fait partie de la FFMI. ■

➔ **www.ffmi.asso.fr**

VIDÉOSURVEILLANCE

La Cnil met en demeure l'école de Xavier Niel

Usage abusif de la vidéosurveillance ? C'est ce que semble croire la Cnil dont la présidente, début octobre, a mis l'association « 42 » en demeure de mettre en conformité avec la Loi informatique et libertés son système de vidéosurveillance. L'association « 42 », de Xavier Niel, est une association à but non lucratif qui, en 2013, a créé l'école « 42 », établissement ayant vocation à former des étudiants dans le domaine de l'informatique. L'école compte environ 800 étudiants inscrits chaque année. En février 2018, la Cnil a procédé à un contrôle dans les locaux situés à Paris.
Elle a notamment constaté que des caméras filmaient en permanence les espaces de travail des étudiants, les bureaux dédiés au personnel administratif ainsi que des lieux de vie comme la cafétéria. En outre, les personnes filmées n'étaient pas correctement informées. Par ailleurs, la plupart des images issues de la vidéosurveillance étaient accessibles en temps réel aux étudiants sur le réseau intranet de l'école à partir de leur espace personnel.
La présidente de la Cnil a donc mis en demeure l'association de redimensionner son système de vidéosurveillance en cessant de filmer en permanence les salles de cours et lieux de vie. Elle rappelle ainsi à l'association que la Cnil considère de manière générale comme excessif tout système de vidéosurveillance plaçant des salariés ou des étudiants sous surveillance constante.
La commission a également rappelé que l'accès aux images issues du dispositif devait être strictement réservé aux personnes habilitées, en raison de leur fonction au sein de l'école. Elle a enfin demandé à l'association de fournir une information complète et immédiate à toute personne


© 42

susceptible d'être filmée par le dispositif.
Dans un communiqué, la Cnil rappelle que *« cette mise en demeure n'est pas une sanction. En effet, aucune suite ne sera donnée à cette procédure si l'association "42" se conforme à la loi dans le délai de deux mois qui lui est imparti. Dans ce cas, la clôture de la procédure sera elle aussi rendue publique. Si l'association ne se conforme pas à la mise en demeure, la présidente saisira la formation restreinte. »* ■

TRANSPORTS FERROVIAIRES

Un PC sécurité ultra-moderne à la Part-Dieu

2 millions d'euros. C'est le coût de l'investissement consenti par la région Auvergne-Rhône-Alpes pour se doter d'un PC de sécurité ultra-moderne, le CRST (Centre régional de sécurité des transports), installé à la Part-Dieu.
Ce PC, géré par SNCF Gare & Connexions, est relié, à l'heure actuelle, à neuf gares jugées sensibles. Il en réceptionne, via la fibre, les images de vidéosurveillance en haute-définition (stockées 30 jours). Comme le souligne notre confrère *Les Échos*, *« un événement détecté à l'une des tables de "vidéo-patrouille", opérées de 6 h 45 à 22 h 15 par 13 agents de la sécurité ferroviaire, est signalé au poste de commandement national de sûreté. Celui-ci, délocalisé, coordonne l'action des officiers de terrain, et peut demander l'intervention de la police ou de la gendarmerie. »*
Le CRST devait être relié, fin 2018, à 32 gares à forte circulation, et sera connecté à 123 gares en 2021, grâce au déploiement de 1 900 caméras (pour un


© Michel Pérès

budget de 22 millions d'euros sur un budget total de 85 millions d'euros pour la sécurisation des gares prévoyant un doublement des agents de sûreté ferroviaire, qui passeront de 80 à 160, la gratuité des TER pour les forces de l'ordre, élargie le mois dernier aux 2 500 policiers municipaux). ■

SÉCURITÉ PRIVÉE

Nouveau DU à l'université Paris-Descartes

L'université Paris-Descartes propose désormais un DU dédié à la sécurité privée. D'ici la fin de l'année, une douzaine de personnes seront retenues pour suivre ce diplôme universitaire, dont les cours s'étendent sur une semaine par mois, de janvier à juin (150 heures au total). Intitulé « Gestion de la sécurité-sûreté dans l'espace ouvert au public », il se compose d'un tronc commun autour de thèmes sur le fonctionnement de la sécurité privée comme son régime, la gestion des services ou encore les contrats et les responsabilités... Une attention particulière est notamment portée à la coopération entre les acteurs de la sécurité.

Public cible

• Titulaires de la licence professionnelle « Sécurité des biens et des personnes » de l'université Paris-Descartes ou d'un autre diplôme de 3e année de l'enseignement supérieur ;
• Professionnels de la défense ou de la sécurité publique ou privée ayant au moins trois ans d'expérience en matière de direction ou d'encadrement. ■

© Getty Images

➔ www.scfc.parisdescartes.fr/index.php/descartes/formations/droit/du-gestion-de-la-securite-surete-dans-l-espace-ouvert-au-public

À NE PAS MANQUER

La Nuit de l'AN2V

© DR

Le 29 janvier, l'association présidée par Dominique Legrand organise, dans le cadre du musée des Arts forains, à Paris, la Nuit de l'AN2V. Son thème : *Quelles perspectives et quels enjeux pour le secteur de la sécurité en 2029 ?*
Lors de l'événement, l'AN2V organisera un exercice de prospective unique : un brain storming de 400 spécialistes du secteur de la sécurité qui définiront les perspectives et les enjeux de la sécurité en 2029.
Il faut aussi souligner que la soirée sera marquée par les interventions de trois invités prestigieux : Alice Thourot, députée et co-auteure du rapport de la mission parlementaire *« D'un continuum de sécurité vers une sécurité globale »,* Luc Ferry, ancien ministre de la Jeunesse, de l'Éducation nationale et de la Recherche et Philippe Gabilliet, professeur de psychologie du comportement et de leadership. ■

➔ La Nuit de l'AN2V
29 janvier 2019 de 18 h 30 à 23 h 45
Musée des Arts forains
53, avenue des terroirs de France, 75012 Paris
Contact : Rémi Fargette
rf@an2v.org
https://an2v.org

FORMATION

DU de coordinateur de cellule de crise

L'université technologique de Troyes propose un DU (10 jours en temps partagé) pour former les cadres de management intermédiaires et stratégiques d'entreprises, d'administrations et de collectivités à la préparation et à la coordination d'une cellule de crise. La formation propose une approche événementielle permettant de considérer :
- le suivi des activités planifiées (festivités, manifestations) et la réaction aux événements inattendus (accident, etc.) ;
- l'anticipation et le traitement des situations complexes, de l'incident inhabituel à la gestion d'événements de haute intensité ;
- le traitement en parallèle d'un événement exceptionnel et la continuité des activités nécessaires au quotidien.

Le contenu de la formation s'appuie sur la plate-forme de crise virtuelle Presages (plateforme de recherche d'expérimentation et de simulation des activités de gestion des événements de sécurité), un dispositif pédagogique innovant créé par l'UTT.
La première session de formation DU Coordinateur de cellule de crise ouvre au mois de mai 2019. Les candidatures sont ouvertes. ■

➔ https://entreprises.utt.fr/

À NE PAS MANQUER

AccesSecurity ouvre ses portes début mars à Marseille

Les 6 et 7 mars prochains, le parc Chanot, à Marseille, accueillera la troisième édition d'AccesSecurity, le salon euro-méditerranéen de la sécurité globale. L'édition 2017 avait été un succès avec plus de 120 exposants et 3000 visiteurs, dont une délégation marocaine.

Cette année, exposants et visiteurs devraient être au rendez-vous d'un salon qui est devenu une véritable réunion d'affaires (que vous pourrez pré-organiser) et un colloque de haut niveau marqué par les participations de directeurs sécurité comme Christophe Merlin, directeur sûreté Transpole-Keolis-Lille pour lequel *«l'intérêt d'être présent à ce rendez-vous est de pouvoir y rencontrer de nouveaux partenaires qui présentent leurs innovations technologiques. La technologie évolue très rapidement. C'est aussi l'occasion d'y retrouver nos partenaires actuels qui sont très attentifs à nos besoins, afin qu'ils nous présentent leurs évolutions technologiques, notamment en matière d'intelligence artificielle.»** À noter que Christophe Merlin interviendra sur le salon lors d'une conférence le 7 mars sur *«La sécurité numérique – quels nouveaux développements, quelles ruptures ? Quelles synergies entre la sécurité physique et cybersécurité ? Véhicules connectés, drones, robots».*

Par ailleurs, des associations et groupements bien connus de nos lecteurs participeront également au salon, à l'instar de l'AN2V, dont le président, Dominique Legrand, reconnaît *«qu'avec 3000 visiteurs attendus et son positionnement de rendez-vous méditerranéen des professionnels de la sécurité, AccesSecurity est devenu en 2019 un rendez-vous incontournable.»** Avant d'ajouter, *«pour cette troisième édition, deux sujets qui seront traités lors du salon attirent tout particulièrement notre attention : le rapport Fauvergue-Thourot* «D'un continuum de sécurité vers une sécurité globale» *qui propose un élargissement du périmètre d'intervention des polices municipales et des sociétés privées de sécurité, et également les questions qui se posent entre DSI et directeurs sécurité dans le cadre précisément de cette sécurité globale.»**

Au sujet de la l'AN2V, il faut noter que La Nuit AN2V, le 29 janvier 2019 au musée des Arts forains, réunira les acteurs du secteur de la sécurité pour un exercice de prospective unique : un brain storming de 400 spécialistes pour définir les perspectives et les enjeux de la sécurité en 2029. Trois intervenants experts partageront leurs expertises : Alice Thourot, députée et co-auteure du rapport de la mission parlementaire *«D'un continuum de sécurité vers une sécurité globale»,* Luc Ferry, ancien ministre de la Jeunesse, de l'Éducation nationale et de la Recherche et Philippe Gabilliet, professeur de psychologie du comportement et de leadership. ■

© AccesSecurity

** Interviews réalisés par Stéphane Gérard, Labo Créatif.*

ACCESSECURITY
Du 6 au 7 mars 2019
Mercredi 6 mars de 9 h à 18 h 30
Jeudi 7 mars de 9 h à 18 h
Parc Chanot, Marseille
➔ **http://accessecurity.fr**

© Getty Images

RGPD

Un logiciel gratuit pour les analyses d'impact

Le logiciel open source PIA (Privacy Impact Assesment), que propose la Cnil, facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données (AIPD) telles que prévues par le RGPD. Cet outil s'adresse principalement aux responsables de traitement n'étant pas ou étant peu familiers avec la démarche d'analyse d'impact relative à la protection des données (AIPD). Il s'agit d'une version «prêt à l'emploi», se lançant facilement sur un poste de travail. Il s'articule autour de trois axes afin d'aider les utilisateurs à suivre la méthode AIPD développée par la CNIL : une base de connaissances juridique et technique ; un outil modulaire qui s'adapte à vos besoins ; une interface didactique pour vous guider pas à pas. ■

➔ **www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**

SALON

Beau succès pour Expoprotection

Le 8 novembre dernier, le salon Expoprotection fermait ses portes à Paris. Durant trois jours, le salon a rassemblé 785 exposants – dont 300 nouveaux participants – 6700 visiteurs par jour en moyenne (pour environ 20100 visiteurs uniques sur les trois jours). Par ailleurs, son programme de conférences et ateliers a lui aussi rencontré le succès puisqu'un peu plus de 6000 personnes y ont assisté. Deux thématiques phares se sont confirmées tout au long de l'événement : l'impact du digital sur la prévention des risques et la sécurisation en cas d'attaque terroriste notamment celle des établissements de soins. Vitrine d'un marché estimé à 28,2 milliards d'euros*, Expoprotection 2018 a offert pendant trois jours le reflet d'une offre innovante, riche et exhaustive en matière de prévention et de gestion des risques. Parmi les 785 sociétés exposantes, 300 nouveautés produits, solutions et services ont été dévoilées et présentées, en parallèle des lauréats des trophées et des Villages start-up et experts. Ainsi, le salon a permis à chacun de trouver des réponses, technologiques ou stratégiques, adaptées à leurs problématiques de risque actuelles ou à venir. Un salon d'un grand intérêt donc.

© Stéphane Laure

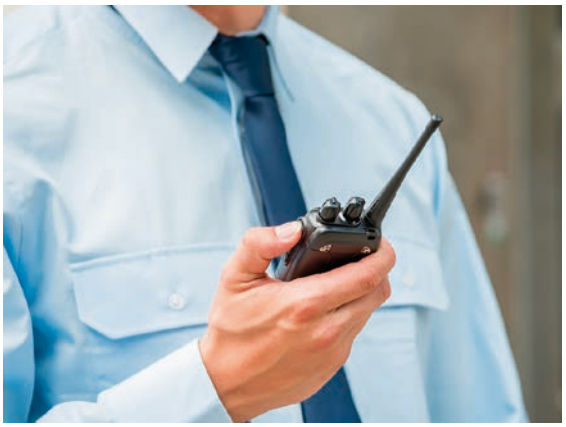
Intérêt que confirment d'ailleurs des exposants comme Niccuza Covaraln, marketing manager chez Risco Group France : *« Nos ambitions, en revenant à Expoprotection, étaient de rencontrer les installateurs de systèmes de sécurité. Globalement, nous avons atteint nos objectifs, nous avons reçu des visiteurs de qualité… et parce que nous souhaitons en accueillir plus encore, nous reviendrons probablement en 2020. »* Ou encore Alex Ossokine, DG de Neutronic Sécurité Incendie : *« Expoprotection reste à ce jour le plus grand événement auquel Neutronic participe. Ce rendez-vous nous semble essentiel et nous avons déjà prévu notre participation en 2020. »* ■

** Chiffres Atlas de la Sécurité 2018.*

SÉCURITÉ PRIVÉE

Le Snes veut la création d'un Opco

Le Snes souhaite la création d'un Opco (opérateur de compétences) auquel seraient rattachées les branches de la sécurité privée, du travail temporaire et de la propreté. Cet Opco n°11 réunirait donc des branches (intérim, propreté) aux problématiques similaires à celles de la filière de la sécurité privée, en termes de formation, de certification, de recrutement, d'attractivité, d'ancrage au plus près des territoires et des besoins de proximité des entreprises de toutes tailles. Cette opportunité contribuerait à faire émerger un partenaire centré sur les services, ce dont a besoin la branche sécurité privée.
Comme le souligne le Snes dans un communiqué, *« Si le Snes fait son choix en faveur de l'Opco n°11, c'est pour permettre à la branche prévention-sécurité d'être plus forte et moins isolée, dans une structure plus cohérente qu'actuellement ou que d'autres options possibles, associant des métiers très différents les uns des autres. Ainsi, il s'agit de gagner en marges de manœuvre en termes de gouvernance paritaire comme de recherche de financement et de partenariats. »* ■


© Getty Images

© Getty Images

COMMERCES

La présence d'agents de sécurité rassure les clients

Une étude réalisée par Opinionway pour Perifem, la fédération du commerce, montre que les Français ont une bonne opinion de la sécurité de leurs commerces. Et que la présence d'agents de sécurité les rassure encore plus.

Alors que 49 % estiment que ces derniers ne sont pas différents du reste des espaces publics en matière de sécurité et que 32 % déclarent même s'y sentir en sécurité, seulement 16 % affirment se méfier de leur environnement et des personnes y gravitant. Dans le détail, ce sentiment se confirme lorsqu'Opinionway se penche sur les différentes formes de commerces. En l'espèce, seulement 25 % des Français éprouvent un sentiment d'insécurité sur un marché, 24 % dans un hypermarché, 24 % dans un commerce de proximité et 22 % dans un supermarché.

Notons cependant qu'en général, 60 % des femmes interrogées déclarent éprouver régulièrement ou de temps en temps un sentiment d'insécurité dans au moins un type de commerce contre 51 % des hommes. Au regard des 4 % de Français déclarant ressentir de l'insécurité en pénétrant dans un commerce ou en y cherchant un article, le sentiment de sécurité semble primer à l'intérieur du point de vente.

La peur des parkings et des agressions

À l'inverse, les espaces autour des grandes surfaces sont beaucoup plus craints que les commerces en eux-mêmes. De fait, le parking couvert d'un centre commercial inspire pour 39 % des Français un sentiment d'insécurité, tout comme les parkings découverts d'une grande surface (29 %) ou encore les galeries d'un centre commercial (29 %). Mais au-delà des lieux, certaines périodes sont plus propices au sentiment d'insécurité que d'autres…

Concernant les agressions verbales, 63 % des Français hissent cette forme de violence au rang de crainte, tout comme 59 % pour le vol sans agression physique et 56 % pour l'agression physique.

Enfin, 85 % des personnes âgées de plus de 65 ans craignent d'être confrontées à une scène de violence dans un commerce tandis que les personnes âgées de moins de 35 ans déclarent qu'il en va de même pour 63 % d'entre eux.

La présence humaine rassure

Si des équipements techniques peuvent faire preuve d'efficacité pour amoindrir le sentiment d'insécurité des Français à l'image d'un bon éclairage (79 %), d'un dispositif de caméras de vidéosurveillance (73 %) ou d'une alarme (59 %), le facteur humain demeure le plus important.

Ainsi, 75 % des Français déclarent que la présence d'agents de sécurité à l'entrée ou à l'intérieur du commerce ainsi que sur le parking contribue à renforcer leur sentiment de sécurité. ■

À RETENIR

- 49 % estiment que les commerces ne sont pas différents du reste des espaces publics en matière de sécurité
- Le top 3 des lieux où les Français se sentent en insécurité : parkings couverts des centres commerciaux (39 %), galeries d'un centre commercial (30 %) parkings ouverts d'une grande surface (29 %)
- 28 % des Français ressentent un sentiment d'insécurité lorsqu'ils rangent leurs achats dans le coffre de leur véhicule
- 75 % des Français déclarent que la présence d'agents de sécurité les rassurent
- 73 % se disent également rassurés par la présence de caméras.

Agenda

JANVIER 2019

La Nuit de l'AN2V
29 janvier 2019 – Paris
https://an2v.org

FÉVRIER 2019

Securidays
Du 20 au 21 février 2019 - Deauville
www.securi-days.fr

MARS 2019

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

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

MAI 2019

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

JUIN 2019

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

Carnet

PWC

Thierry DELVILLE


© DR

Ancien délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, Thierry Delville a rejoint les équipes « Cyber Intelligence » de PwC. Il participera au développement du pôle « Cyber Intelligence » qui rassemble toutes les expertises du cabinet liées à la gestion des nouvelles menaces. En 2014, il devient délégué ministériel aux industries de sécurité, puis par Décret paru le 24 janvier 2017, il voit ses attributions étendues avec la création de la délégation aux industries de sécurité et à la lutte contre les cybermenaces. Au sein de PwC, Thierry Delville aura notamment pour objectif de bâtir une solution ambitieuse de gestion des crises avec l'appui de l'ensemble des expertises concernées.

CSF INDUSTRIES DE SECURITE

Marc DARMON


© DR

Le 22 novembre, Marc Darmon a été nommé par le gouvernement président du comité stratégique de filière (CSF) des industries de sécurité. Diplômé de l'École polytechnique et de telecom ParisTech, Marc Darmon a débuté sa carrière chez Alcatel en 1988. Il rejoint le groupe Thales en 1998 au sein de l'entité Thales Communications en tant que directeur du département « réseaux d'infrastructure ». De 2006 à 2008, il est directeur général de Thales Communications et, depuis 2013, directeur général adjoint, systèmes d'information et de communications sécurisés de Thales. Marc Darmon est également, depuis septembre 2014, président du Conseil des industries de la confiance et de la sécurité (CICS).

« La filière industries de sécurité a ceci de particulier qu'elle porte sur un secteur sensible, avec des enjeux forts, sur le plan stratégique et sociétal. »

© Thales

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

MARC DARMON

Président du CSF industrie de sécurité

« La création du CSF montre l'importance qu'accorde l'État à la sécurité. »

Marc Darmon est le président du nouveau CSF industrie de sécurité créé tout récemment, le 22 novembre dernier, par le gouvernement. Marc Darmon est également directeur général adjoint du groupe Thales. Il a accepté de répondre aux questions de *PSM* pour nous présenter le rôle du CSF et les grands dossiers sur lesquels il va devoir se pencher.

En quoi la création du CSF est-elle une étape importante pour la filière ? Pourquoi vient-elle « couronner » le travail accompli par le CoFis depuis sa création ?

La filière des industries de sécurité est une filière d'avenir pour la France, dont tous les acteurs – PME/ETI, secteur public, grands groupes leaders mondiaux – pourront renforcer la portée nationale et internationale au sein du CSF. Chaque acteur apportera sa pierre à une démarche collaborative et structurante en faveur de la sécurité, dans toutes ses dimensions : cybersécurité, protection des infrastructures et des réseaux, sécurité du transport, secours aux personnes, lutte contre le terrorisme et la grande criminalité, gestion de la crise. La création du CSF montre l'importance qu'accorde l'État à la sécurité dans un monde toujours plus connecté et vulnérable face aux risques. Il va également permettre aux acteurs de la filière de proposer des projets structurants et des plans d'actions pertinents, développés ensuite en conditions réelles.

Que représente la filière française industries de sécurité ?

La filière industrielle de sécurité pèse 25 milliards d'euros au plan national dont 50 % sont réalisés à l'export. Cela représente 130 000 emplois. Cette filière industrielle se caractérise aussi par une croissance annuelle mondiale de 6 % et représente plus de 15 % des publications scientifiques mondiales. C'est dire son importance. Par ailleurs, la filière de sécurité, dans son sens le plus large, représente, quant à elle, un chiffre d'affaires de 34 milliards d'euros et 285 000 emplois dans le secteur marchand. Auxquels s'ajoutent 700 000 emplois publics.

La sécurité représente également un marché international très porteur qui couvre des sujets très divers, que l'on peut diviser en trois segments de solutions technologiques. Tout d'abord, les produits et solutions de sécurité physique (véhicules, plates-formes dont solutions robotiques, contrôle d'accès, équipements de protection, etc.). Viennent ensuite les produits électroniques et numériques : identification et authentification, systèmes de détection, communications sécurisées, systèmes de commande et contrôle, solutions d'observation, de géolocalisation et de vidéoprotection. Enfin, s'y ajoutent les produits et solutions de cybersécurité.

Comme tous les comités de filière soutenus par le gou- ● ● ●

« Les JO 2024 à Paris permettront de démontrer et promouvoir à l'export les solutions françaises. »

MARC DARMON

Président du CSF industrie de sécurité


© Thales

« Comme tous les comités de filière soutenus par le gouvernement, le CSF aura à cœur de développer la compétitivité des PME/ETI et de nos groupes leaders mondiaux. »

vernement, le CSF aura à cœur de développer la compétitivité de PME/ETI et de nos grands groupes leaders mondiaux, qui occupent sur le marché de la sécurité une place de premier plan avec cependant une concurrence qui s'affermit.
Pour autant, la filière industries de sécurité a ceci de particulier qu'elle porte sur un secteur sensible, avec des enjeux forts sur le plan stratégique (garantir notre autonomie dans les secteurs les plus critiques), mais également sociétal (proposer des solutions conciliant harmonieusement sécurité et respect de nos libertés individuelles et collectives).

Quels seront les axes de travail et projets de CSF dans les mois et années à venir?

Les comités stratégiques de filière (CSF), correspondant chacun à une filière stratégique de l'industrie française, ont pour mission d'identifier de façon convergente, dans des « contrats de filière », les enjeux clés de la filière et les engagements réciproques de l'État, des grands groupes et des PME/ETI, d'émettre des propositions d'actions concrètes et de suivre leur mise en œuvre.
Dans la lignée des travaux engagés par le CoFIS, le CSF industries de sécurité aura donc à cœur de répondre à l'ensemble des enjeux liés à la sécurité physique, aux solutions numériques et à la cybersécurité, en s'appuyant sur la recherche et développement et sur des projets d'envergure.
La filière des industries de sécurité portera ainsi des projets structurants comme la sécurité des prochains Jeux Olympiques 2024, la cybersécurité, les territoires de confiance (comprenant la sécurité de la ville connectée), la souveraineté en matière de sécurité ou encore l'identité et la confiance numérique.

Quelles seront les actions stratégiques du CSF pour aider et soutenir le développement à l'international des entreprises françaises?

Le CSF permettra de coordonner l'action des services de l'État et des industriels pour assurer le succès des offres françaises à l'export et établir à l'international une marque France puissante dans le domaine de la sécurité. L'opportunité des JO sera exploitée pour démontrer et promouvoir à l'export les solutions françaises. Des plans seront mis en place pour viser un leadership sur la cybersécurité de l'IoT et des territoires de confiance.

Comment les industries de sécurité peuvent-elles s'inscrire dans la politique plus vaste de sécurité de la France? Comment peuvent-elles ou doivent-elles collaborer avec les pouvoirs publics, les entreprises de la sécurité privée?

Le dialogue engagé par le CoFIS entre les utilisateurs publics et privés et l'industrie sera poursuivi et renforcé dans le cadre du CSF. L'industrie apporte ainsi des solutions pour faciliter le continuum de sécurité, souhaité par les pouvoirs publics et les acteurs de la filière sécurité, ou répondre aux problèmes qui ne sont pas réglés par les effectifs. Au sein du Conseil national industrie (CNI), la filière sécurité apportera aux autres filières la protection de l'industrie à travers la sécurité du numérique, des sites, des entreprises.

Quels sont les enjeux et défis que doit relever la filière : cybersécurité, intelligence économique, évolutions des menaces? Pourquoi?

Ils sont multiples. Ainsi, à l'heure où les menaces sont toujours plus nombreuses, et toujours plus présentes, le développement du comité de la filière industrielle de sécurité répond avant tout à des enjeux de protection des entreprises, des citoyens et de la Nation. Tout en assurant un espace d'échanges et de prises de décisions entre tous les acteurs de la filière. Le CSF doit répondre à des missions aussi diverses que la protection des grandes infrastructures publiques ou privées, la sécurité du transport, le secours aux personnes, la lutte contre le terrorisme et la grande criminalité, la gestion de crise ou encore la cybersécurité, telle est l'ambition du comité stratégique de filière industries de sécurité. Pour répondre à ces objectifs, notre filière possède et peut compter sur des leaders mondiaux de la sécurité en biométrie, sécurité urbaine, radiocommunications sécurisées, sécurisation des transports terrestres, systèmes d'information et de commandement, cryptologie et sécurité des systèmes d'information... Pour porter à l'international et en France, les technologies et le savoir-faire français. ■

LES INDUSTRIE DE SÉCURITÉ EN QUELQUES CHIFFRES

- 130000 emplois en France
- Plus de 25 milliards d'euros de chiffre d'affaires annuel
- 6 % de croissance annuelle mondiale
- Plus de 15 % des publications scientifiques mondiales.

ultraSync

Passerelle de communication IP Ultra Sécurisée

Pour votre entreprise

Les systèmes **UltraSync Smart Building** et **UltraSync Smart Home**

offrent sur tous produits compatibles un niveau inégalé de cybersécurité aux:

- utilisateurs
- prestataires de service
- centres de télésurveillance

En immotique comme en domotique, ils vous permettent de configurer vos systèmes de sécurité avec souplesse et précision: ils s'adaptent à vos besoins et à leurs évolutions, où que vous soyez.

De plus, l'hébergement est naturellement conforme au RGPD UE.

fr.firesecurityproducts.com

et votre domicile

interlogix
United Technologies

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

dossier

Sécurité et smart cities

Avec le développement des nouvelles technologies, les villes peuvent de plus en plus envisager de se servir de la masse des données collectées pour proposer des applications permettant de les rendre plus sûres pour ses habitants et de faciliter le travail des forces de sécurité.

© Getty image

SOMMAIRE

La safe city doit permettre de remonter les données collectées par les différents réseaux de la ville afin d'accroître l'efficacité des agents sur le terrain.

© DR

Les technologies au service de la safe city

La gestion intelligente de la sécurité est un des enjeux majeurs de ce qu'on appelle la «ville intelligente» ou la smart city. Mais se lancer dans un tel projet ne s'improvise pas et doit se faire en respectant un certain nombre de prérequis. Car les solutions pour tendre vers la safe city existent et les entreprises françaises proposent des outils très pertinents.

Souvent portés par les maires, les projets de smart city ont longtemps pâti – et pâtissent encore – d'une certaine forme de flou artistique. Ce que confirme Emmanuel François, président de la Smart Building Alliance for Smart Cities (SBA): *«Encore aujourd'hui, l'expression "ville intelligente" est vague et mal comprise des citoyens. On y met un peu tout et n'importe quoi. Souvent les projets de smart city sont réduits à des outils marketing à des fins électoralistes ou pour vendre des solutions techniques. Un peu à l'image de ce qui s'est produit dans le cas de la domotique.»* Pour le président de la SBA, il serait dommage d'en rester là. *«Mais on en n'est pas loin car les fondamentaux nécessaires à l'élabora-*

LE POINT DE VUE D'UN INTÉGRATEUR

THIBAULT BOULLÉ
Ingénieur commercial smart city chez Sogetrel


© DR

« LA VIDÉO EST LA COLONNE VERTÉBRALE DES RÉSEAUX SMART D'UN TERRITOIRE. »

« La vidéoprotection est un outil puissant dont certaines données peuvent intéresser et être utiles pour différents services de la ville et offrir de nouveaux services digitaux aux citoyens. De nombreuses villes de taille moyenne, qui cherchent à garder leur population et à attirer des entreprises, réfléchissent à l'élaboration de nouveaux services pour se rendre plus attractives. Le prérequis d'une vidéoprotection efficace est la présence d'un réseau fibre parcourant les axes stratégiques d'un territoire. Pour peu qu'il ait été dimensionné en amont pour permettre d'autres usages, ce réseau peut servir de support pour le déploiement d'objets connectés. On ne peut aussi que conseiller aux villes périurbaines et rurales de mutualiser leurs moyens techniques, ne serait-ce que pour en répartir le coût et bénéficier de solutions techniques homogènes. C'est ce qu'a fait Chartres métropole dont le CSU profite également à des communes de très petite taille qui n'auraient pas eu les moyens d'investir seules. Un réseau bien dimensionné sera aussi capable d'évoluer plus facilement, on pourra venir y greffer d'autres capteurs et d'autres usages. On réfléchit par exemple à la manière dont on pourrait utiliser les systèmes de contrôle d'accès installés dans les bâtiments gérés par la Ville et qui donnent une visibilité sur leur occupation. Cette information peut avoir un impact sur la consommation énergétique dudit bâtiment. Nous ne sommes qu'aux prémices d'une multitude de cas d'usages pour se faciliter la vi(ll)e ! »

tion d'un projet de ville intelligente sont loin d'être maîtrisés et connus des acteurs concernés. »

Tout doit commencer par une vision, un projet clair. *« On doit s'appuyer sur la technologie mais il n'est pas toujours aisé, quand on est un homme politique, d'être les deux à la fois. C'est-à-dire être en même temps visionnaire et perméable à la technologie »*, constate Emmanuel François. Or, il est impératif de maîtriser les fondamentaux posés en préalable par le président de la SBA. À savoir qu'une ville intelligente, et *a fortiori* sûre, repose sur de la technologie, du numérique, un système intelligent et évolutif. Mais cela ne suffit pas. *« Il faut aussi savoir par quoi commencer,* ajoute-t-il. *Quels sont les prérequis de la smart city ? Elle doit disposer de réseaux connectés et communicants, évolutifs et pérennes, c'est-à-dire ouverts et interopérables, et donc non liés ou dépendants d'une seule application. Toute infrastructure déployée dans le cadre de ce type de projet doit donc reposer sur du numérique et de la technologie ouverte. Si les réseaux ne communiquent pas entre eux, on reste dans une logique de silos. À l'heure où nos concitoyens sont informés en temps réel de tout, de la qualité de l'air ou des ondes, il devient indispensable de casser ces silos et de créer des écosystèmes vertueux pour les territoires connectés. »*

> *« La smart city implique de disposer de réseaux connectés, communicants et pérennes. »*
>
> **EMMANUEL FRANÇOIS, PRÉSIDENT DE LA SBA**

Une initiative locale

Les maires sont en première ligne en matière de sécurité. Comme l'expliquait dans le cadre des Universités de l'AN2V, en janvier 2018, Caroline Pozmentier-Sportich, adjointe au maire de Marseille, déléguée à la sécurité et à la prévention de la délinquance et vice-présidente de la région Paca, qui a fait installer 1 000 caméras de vidéoprotection et développer un centre de supervision urbain de dernière génération : *« Les maires doivent mettre en place des solutions sur trois ans qui auront des effets*

DU CÔTÉ DU FABRICANT

THIERRY OROSCO
Axone


© DR

« Notre solution OODA (pour Observ, Orient, Decide & Act) est un hyperviseur 3D qui vient tout simplement coiffer les grands systèmes verticaux d'un territoire connecté (caméras, gestion des feux de signalisation, contrôle d'accès…), pour offrir à l'opérateur devant son écran de la data qualifiée pour qu'il agisse le plus efficacement et rapidement possible. Cette capacité à remonter une information en temps réel et à la délivrer, via une interface très intuitive et simple d'usage, est très appréciée dans la cadre de la safe city, la principale préoccupation actuelle des villes. Notre solution permet également, dès lors que l'on dispose de cette plate-forme, d'y ajouter d'autres applications métier en dehors de la sécurité, le pas vers la smart city. OODA se caractérise par une capacité à intégrer très facilement tous les sous-systèmes existants du marché pour valoriser les équipements déjà installés. Il permet aussi de tirer les enseignements d'un incident en retrouvant l'état de chaque capteur à un même moment passé, de faire de la simulation, de planifier une opération en plaçant sur la carte 3D les avatars des forces qui seront engagées et surtout de faire du prédictif immédiat, c'est-à-dire une aide à la décision en temps réel. OODA permet donc à l'autorité de réagir très vite en intégrant ce que fait l'adversaire et ce qu'elle est en mesure de faire sur le terrain. Tout l'enjeu consiste à fournir un minimum d'éléments simples, élaborés à partir d'une multitude d'informations pour faciliter le travail de l'opérateur. »

● ● ● *sur vingt ans. Cela passe par de l'audace, des partenariats et des investissements. Notamment en demandant des financements auprès du fonds interministériel de prévention de la délinquance (FIPD) ainsi que des fonds européens, notamment pour financer les applications de big data dans la sécurité.»*

En matière de smart cities, les mairies partent souvent du même constat. *«Elles ont face à elles deux choses. D'une part, les Villes disposent sur le terrain de systèmes historiques – capteurs de flux, signalisation, vidéo… – construits en silos,* explique Laurent Rochette, DG délégué du syndicat mixte ouvert Yvelines numériques. *Et d'autres part, elles souhaitent mettre l'usager, le citoyen, au centre de leur préoccupation. Elles veulent lui donner des indicateurs lui permettant, par exemple, de faire des choix en matière de mobilité. Or, quand elles décident de se lancer dans un projet qui permettrait de faire travailler ensemble les données collectées, par leurs systèmes historiques, et les services qu'elles souhaitent mettre à la disposition des usagers, elles se rendent compte que cela est difficile, voire impossible. Certaines décident donc de mettre les choses sur la table : de combien de capteurs disposent-elles sur le terrain ? En général, beaucoup. Elles comprennent que pour les exploiter au mieux, il va leur falloir rationnaliser le tout et mener une réflexion globale afin d'éviter de multiplier les capteurs ou de superposer différentes couches de capteurs.»*

Comment faire ?

«Il faut mettre tous les acteurs concernés autour d'une table et discuter. On ne se lance pas dans un tel projet sans avoir claire-

DU CÔTÉ DU FABRICANT

XAVIER FÉRY

Gérant de Komanche

© DR

« En matière de safe city, le savoir-faire français est réel. Mais, à l'inverse de ce qui se fait dans d'autres pays, il nous est très difficile d'expérimenter nos solutions. Dans le cas de Komanche, nous travaillons sur un hyperviseur natif 3D qui va permettre aux villes de générer des requêtes en temps réel et faire remonter automatiquement toutes les informations de tous leurs différents réseaux et capteurs. Or, comment en valider l'efficacité sans tests sur le terrain ? C'est pourquoi, le FrenchShield, avec certains de ses partenaires comme Overall Security, Affinis, Alcéa, Kopp, Heure & Contrôle, Mextor et Komanche, se sont rapprochés du Campus de l'espace, à Vernon, afin de pouvoir tester, sur un site privé, et en grandeur réelle, les technologies applicables à la safe city : reconnaissance de visages, lecture de plaques, détection automatique d'incident, reconnaissance de couleurs, d'objets, gestion des flux, contrôle d'accès, protection mécanique anti-intrusion, Audit, cyber, etc., en interagissant avec l'environnement vidéo et ses couches d'intelligence. Pour que notre hyperviseur puisse fournir à l'opérateur les informations utiles dans le cadre de tel ou tel scénario prédéfini. »

2 QUESTIONS À

DENIS HAMEAU

Vice-président du conseil régional de Bourgogne Franche-Comté, conseiller ESRI Dijon métropole chargé du projet OnDijon

© DR

Comment se lance-t-on dans un projet aussi vaste que OnDijon ?

Il y a trois ans, à partir de la vision stratégique de notre territoire autour de l'environnement, de l'inclusion sociale et du développement économique, nous avons voulu repenser la façon de gérer les grandes fonctions urbaines et l'espace public. Évidemment, ce vaste projet incluait les usages des citoyens et une remise à plat complète, dans le cadre de notre vision de la ville de Dijon demain, des manières de fonctionner de nos différents postes de contrôle sécurité : PC police municipale, CSU, PC circulation, PC sécurité, Allo mairie...Tout cela fonctionnait en silo, plutôt bien, mais avec une coordination et une transversalité perfectible. Il nous fallait donc revoir le dispositif avec une méthode différente. Nous avons d'abord réfléchi à une échelle plus large, celle de la métropole : 260 000 habitants et 24 communes. Nous avons ensuite étudié très attentivement ce qui se faisait en France et dans le monde en matière de « ville intelligente » pour nous inspirer des meilleures pratiques notamment en matière d'éclairage public et d'économies d'énergie.

Cela fait, nous nous sommes tournés vers les entreprises. Quatre consortiums pilotés chacun par Bouygues Énergie Services, Engie, Eiffage et Vinci ont répondu à notre appel d'offres.

Justement, vous avez été retenu, parmi plus de 470 dossiers, en finale d'un concours organisé dans le cadre du Smart City Expo World Congress de Barcelone. Cela démontre la qualité de votre projet…

Cela montre surtout que nous sommes allés bien au-delà de la vision la plus simple de ce qu'on appelle communément la smart city, qui souvent se limite à ses aspects sécuritaires ou technologiques dans un domaine. Nous avons voulu avec Bouygues Énergies Services, Citelum, Suez et Cap Géminiez conjuguer un leadership public fort et le meilleur de l'innovation privée.

Ainsi, grâce à la meilleure utilisation des données générées par la Ville, nous pourrons réinventer, avec le personnel sur le terrain, nos services (police, voirie, propreté, etc.). Cela débouche aussi sur une gouvernance locale des données à construire. Elles seront mises à disposition de nombreux acteurs et sur le campus de l'université, une rue permettra aux start-up de tester grandeur nature leurs solution. Ce partage des données – qui restera sous le contrôle de la Ville – se fera avec le monde universitaire, les écoles d'ingénieurs, les laboratoires, les entreprises de l'économie numérique, contribuera à l'attractivité du territoire et à inventer les services de la ville de demain.

ment défini les objectifs du projet et ce qu'on souhaite, précise Laurent Rochette. *Ainsi, dans le cas de la mise en place de notre CDSI (Centre départemental de supervision des images), nous avons constitué un comité de réflexion qui devait mener la réflexion sur la smart city : les freins à dépasser, les leviers à utiliser, les sujets imposés comme la mobilité, la régulation du trafic… tout cela pour coordonner les choses.»*

Concrètement, les villes qui souhaitent se lancer dans un projet smart ou safe city, ont deux briques principales à leur disposition : la vidéoprotection et la mobilité/régulation de trafic. Dans la première, elles ont installé plusieurs centaines, voire milliers de capteurs – dont les caméras – dans un certain nombre de lieux publics (écoles, collèges, lycées, casernes de pompiers, gymnases, hôtel de ville…) dont les villes doivent assurer la sûreté. En ce qui concerne la mobilité/régulation de trafic, certaines collectivités disposent d'un système élaboré.

«Tout l'intérêt de la concertation entre les différents acteurs et les départements limitrophes, ajoute Laurent Rochette, *est de pouvoir étudier la possibilité de mutualiser certains réseaux et outils. C'est par exemple, ce que l'EPI78-92 (établissement public interdépartemental) fait en ce moment avec une étude en cours pour étendre le système Siter aux Yvelines.»*

Sortir de la logique des silos

La démarche exposée par Laurent Rochette implique que les réseaux à disposition des villes et pouvant éventuellement servir à la mise en place d'une approche safe city puissent commu- ●●●

PAROLE D'EXPERT

EMMANUEL FRANÇOIS

Président de la Smart Buildings Alliance for Smart Cities (SBA)

© DR

«IL FAUT DES RÉSEAUX NUMÉRIQUES OUVERTS ET INTEROPÉRABLES.»

«La smart city, et *a fortiori* la safe city, ne peuvent pas se bâtir sans des réseaux numériques, ouverts, communicants et interopérables. Il faut en outre que la Ville soit propriétaire de ses données, qu'elle ne soit pas contrainte de devoir passer par un tiers pour en disposer. Ceci posé, il est évident que la sécurité est une des "portes d'entrée" pour ce type d'infrastructure car les villes disposent souvent de réseaux de vidéoprotection qui peuvent permettre d'envisager d'en exploiter les données dans une démarche "intelligente". Mais, selon moi, on ne peut pas envisager la smart city sans des bâtiments intelligents qui, non seulement permettront de piloter l'énergie, la sécurité ou la mobilité à l'échelle du bâtiment, mais aussi de fournir – le cas échéant – une partie de ces données aux services de la ville. Il faut penser continuum des données entre la ville et ses bâtiments. Mais cela va évidemment impliquer une évolution du cadre législatif.»

L'usager doit rester au cœur de tout projet de smart ou de safe city.

© Getty image

niquer entre eux. Ce qui est loin d'être le cas. *«Les villes, lorsqu'elles ont déployé leurs réseaux de vidéoprotection, de gestion du trafic ou autres… n'ont pas toujours travaillé dans une logique d'interopérabilité de ces systèmes,* regrette Emmanuel François. *Leurs réseaux, actuellement, ne communiquent pas entre eux ou ont du mal à le faire. Pour construire une safe city, il faut donc impérativement sortir de la logique du silo.»*

Autre écueil à éviter : la logique propriétaire. «Par ailleurs, continue le président de la SBA, *les villes ne sont pas forcément propriétaires de leurs infrastructures et donc maîtres de leurs données. La smart city ou la safe city pose donc un problème de gouvernance. C'est-à-dire qu'elles doivent absolument pouvoir disposer des données générées par leurs divers réseaux, pour les exploiter.»*

Cette exploitation des données et réseaux par les villes est donc un des enjeux majeurs de la safe city. Elle doit leur permettre de proposer de nouveaux services aux usagers de la ville et de rentabiliser les installations existantes…

Rentabiliser les systèmes

«Les villes se demandent comment rentabiliser les systèmes déjà déployés, et en particulier ceux de vidéoprotection, constate Thibault Boullé, Business Developper Smart City chez Sogetrel. *Par exemple, environ 80 % des villes moyennes disposent d'une installation de vidéoprotection. Et cherchent à rentabiliser cette installation. Se lancer dans un projet smart city est un bon moyen de se servir autrement d'une installation de sécurité pour mettre à disposition certaines données et informations collectées par le réseau de caméras à la disposition d'autres services de la Ville.»*

Les villes disposent aujourd'hui, avec leur réseau de vidéoprotection, d'un outil puissant et parfois intelligent, doté de capacités de stockage importantes, supervisé par des agents dans un PC. Or, les villes utilisent une faible partie du potentiel de ces réseaux. Et les opérateurs devant leurs écrans de contrôle sont souvent réduits à la simple visualisation des images fournies pour, le cas échéant, alerter les équipes sur le terrain. *«De nombreux autres métiers et services de la Ville, notamment la voirie, gagneraient à bénéficier d'une réactivité temps réel,* ajoute Thibault Boullé. *Les agents devant leurs écrans peuvent leur fournir des informations provenant des différents capteurs posés sur la*

PAROLE D'EXPERT

PHILIPPE GENDREAU
Délégué général adjoint du Gicat

© DR

«PROPOSER DES APPLICATIONS DIGITALES AUX CITOYENS.»

«Quand on parle de safe city, on est face à deux sujets qu'on a tendance à mélanger. Le premier concerne la sécurité intrinsèque des systèmes de la Ville (eau, éclairage public, feux de signalisation…) et la plupart des gens s'arrêtent là. Le second, plus complexe, concerne la réflexion qu'on doit mener pour offrir une meilleure sécurité "perçue" aux citoyens et usagers de la ville. En déployant mieux sur le terrain les forces de sécurité et en proposant aux citoyens des outils et services digitaux leur permettant d'être informés en temps réel d'un événement, de la présence de pickpockets dans un tramway, d'un incident dans le trafic urbain… La safe city doit donc permettre de concevoir des applications allant bien au-delà de la surveillance de la population. Et les entreprises françaises jouissent d'un vrai savoir-faire en la matière. Mais il est dommage que la réglementation en vigueur les empêche de tester, en grandeur réelle, le bien-fondé de leur approche, l'efficacité et la validité de leur application. Il faut leur permettre d'expérimenter sur le terrain…»

2 QUESTIONS À

LAURENT ROCHETTE

Directeur général délégué du syndicat mixte ouvert Yvelines numériques


© DR

Quels sont les prérequis à respecter pour engager un projet de smart ou de safe city ?

Il faut tout d'abord garder à l'esprit que l'usager doit être au cœur de la démarche. Sans cela, tout ce qu'on pourra mettre en place risque de rester lettre morte et susciter des réactions négatives. Une fois cela posé, il faut évidemment engager une vaste concertation avec tous les acteurs concernés et bien identifier qu'elles sont les responsabilités de chacun, les différents opérateurs selon les prestations assurées pour la ville… Car nous sommes souvent confrontés à un morcellement et un empilement des responsabilités sur un même territoire qui peuvent nuire à la possibilité d'avoir une vision par le haut. Par exemple, le département des Yvelines n'a pas hésité à se rapprocher du département des Hauts-de-Seine dans le cadre de son projet de smart city afin d'étudier comment nous pouvions mettre en commun nos moyens respectifs pour les mutualiser ou les intégrer dans la smart city pour éviter de multiplier des systèmes qu'il n'est pas toujours évident de faire collaborer. C'est de cette réflexion approfondie qu'est né notre CDSI ou centre départemental de supervision des images qui centralise, en un seul système, les images fournies par les 3000 caméras du département, pour les stocker, les exploiter, en lien avec les forces de sécurité.

En quoi ce système centralisé vous permet de mieux gérer les flux des caméras ? Cela vous permet-il d'envisager de faire profiter de cette exploitation des données d'autres services du département ?

Pour que tout cela fonctionne correctement, il faut mettre de l'intelligence dans le système. Et cela suppose que ce soit possible, c'est-à-dire que votre système ait été conçu pour être évolutif. Notre CDSI peut compter sur l'IA pour faire de la détection automatique d'anomalies dans les flux des 3000 caméras du réseau : un incident, la détection d'un cri, une personne qui appuie sur un bouton… Et comme le système est ouvert, nous pouvons raisonnablement envisager d'y greffer demain d'autres applications comme la détection de température, de fumée… Nous travaillons d'ailleurs déjà à l'interconnexion du système de gestion du trafic avec celui de la vidéo. Mais il faut rappeler qu'on ne se lance pas dans un tel projet sans un élément déclencheur, un besoin réel économique ou politique. Pour répondre à la seconde partie de votre question, d'autres services de l'État sont très intéressés par notre démarche. La police et la gendarmerie évidemment qui y voient un moyen très efficace pour avoir de l'information en temps réel et qualifiée. Les services de l'Éducation nationale également qui souhaiteraient s'en servir pour faire intervenir les personnels compétents en cas d'incident et disposer d'un élément de preuve…

ville. Par ailleurs, les données remontées par les caméras pourraient permettre d'apporter du service aux citoyens (flux de circulation, fréquentation des guichets...) et de sortir de la seule logique d'exploitation sécuritaire du réseau de vidéoprotection.»

Point de vue que partage Philippe Gendreau, délégué général adjoint sécurité du Gicat : *«En gros, les villes disposent de réseaux de vidéoprotection utilisés à des fins de pure surveillance et qui occupent un grand nombre d'agents. Il faut que les villes – et c'est tout l'intérêt de se lancer dans une réflexion smart city – se demandent ce qu'elles pourraient faire d'original avec ces réseaux afin d'en optimiser le potentiel. Comment se servir des nouvelles technologies, des algorithmes, de l'intelligence artificielle… pour faire autre chose (gestion du trafic, suivi de la pollution urbaine…) et afin de faire en sorte que la partie veille, pendant laquelle il ne se passe rien, soit gérée de manière automatique par des outils intelligent avant de réserver à l'homme la prise de décision et l'intervention. Et surtout de participer à la mise à disposition de nouveaux services aux usagers.»*

Quelle porte d'entrée ?

Il semble bien qu'à l'heure actuelle le réseau qui soit à même de permettre aux villes de s'engager dans un projet smart et safe city soit celui de la vidéoprotection. *«Le réseau de caméras, lorsqu'il a été bien conçu et câblé, est tout à fait à même de servir de support à d'autres services»*, confirme Philippe Gendreau. Constat que partage Thibault Boullé : *«De nom-*

DU CÔTÉ DU FABRICANT

AUGUSTIN MARTY

Directeur général de Deepomatic


© DR

« Depuis sa création en 2014, Deepomatic travaille sur la manière de rendre les caméras intelligentes. Aujourd'hui, notre solution permet, sans qu'il soit nécessaire d'intervenir sur les caméras installées dans les villes, de les rendre intelligentes en installant tout simplement, parallèlement au système existant, un serveur d'analyse à côté des serveurs vidéo. Le tout étant piloté à partir d'une interface dans le cloud. Avec notre solution il est tout à fait possible, et très aisément, de permettre au système de caméras sur le terrain de remonter de l'info pour savoir, par exemple, si les gens font du covoiturage, si les conducteurs respectent les couloirs réservés aux cyclistes... Notre solution permet donc de transformer un système de vidéoprotection, dont les données sont très souvent sous-exploitées, en un système intelligent, fournissant à l'exploitant de l'information utile. »

PAROLE D'EXPERT

DOMINIQUE LEGRAND

Président de l'AN2V et président de la commission safe city de la SBA

© DR

« FOURNIR EN TEMPS RÉEL LA MEILLEURE INFORMATION POSSIBLE. »

« Je me demande si on peut encore parler de smart cities, de safe cities… Je crois qu'il faut plus raisonner en termes de "smart territories" ou "territoires de confiance". Cela permet d'aller plus loin que la simple smart city et donne bien une idée du fait que pour assurer la sécurité de nos concitoyens dans le cadre de la "ville sûre" ou "intelligente", il faut raisonner à l'échelle du territoire car, dans une approche d'une sécurité globale, il faut que les différents systèmes et réseaux dont ils disposent puissent être connectés entre eux afin de fournir en temps réel la meilleure information possible aux citoyens et personnels chargés d'assurer leur sécurité. Tout doit concourir à ce que les technologies déployées sur le terrain soient à même de remonter de manière très fluide et rapide les informations avant et après un incident évidemment, mais surtout pendant. On doit tendre vers le temps réel et c'est d'ailleurs ce que réclament de nombreux représentants des forces de l'ordre. La safe city doit être conçue pour permettre de refermer autour de lui, le champ d'action d'un délinquant, le plus rapidement possible, grâce aux moyens technologiques et humains. »

● ● ● *breuses villes, métropoles ou pas, disposent d'un réseau suffisamment ambitieux et bien conçu pour permettre à d'autres applications de venir se greffer dessus. En revanche, lorsque les réseaux urbains ont été construits service par service, sans réflexion globale, on peut avoir du mal à connecter d'autres usages et cela génère des surcoûts importants. »*

Ici nous en revenons à une problématique évoquée plus haut : la nécessaire concertation entre les différents acteurs et services concernés par un projet smart city. *« Pour élaborer de nouveaux services et applications à partir d'un système ouvert, il faut organiser des réunions afin de faire émerger les besoins différents des services concernés »,* ajoute l'expert de Sogetrel. Avant de regretter *« qu'il soit très rare que les villes aient un réflexe collaboratif afin d'étudier la manière dont il possible de faire travailler entre eux les différents systèmes de la commune. »* Or, la mutualisation des systèmes, comme nous l'a expliqué Laurent Rochette, est importante car elle permet de disposer d'une certaine homogénéité des dits systèmes pour leur permettre d'évoluer.

« La safe city doit permettre de concevoir des applications allant au-delà de la surveillance de la population. »

PHILIPPE GENDREAU, DÉLÉGUÉ GÉNÉRAL ADJOINT DU GICAT

Une ville « Big Brother »

La safe city n'est pas la mise en place d'une ville qui surveillerait tout le monde, tout le temps. Et cela doit être expliqué.

« Il s'agit de proposer non seulement de nouveaux services aux citoyens, mais aussi d'accroître l'efficacité des forces de l'ordre déployées sur le terrain, tient à souligner le délégué général adjoint du Gicat. *Le but est de proposer aux usagers des services à valeur ajoutée mais aussi d'offrir aux citoyens une meilleure sécurité "perçue", de manière harmonieuse, non anxiogène. La safe city, bien conçue et pensée, permet de mettre à disposition du citoyen – et même des forces de l'ordre – des applications qui vont bien au-delà du simple contrôle des foules et de la population. »*

Il ne s'agit aucunement de copier des modèles étrangers. *« La safe city n'est pas l'occasion pour le pouvoir de surveiller tout le monde et de le verbaliser tout le temps dès qu'il sort des clous. On ne souhaite pas copier l'exemple chinois. Et les lois en vigueur en France nous en préservent heureusement »*, ajoute le président de SBA, Emmanuel François.

« On ne doit pas laisser les débats éventuels suscités par la safe city à ceux qui en dénoncent les dérives éventuelles ou la dangerosité potentielle pour les libertés publiques. Nous devons communiquer, expliquer et informer nos concitoyens sur les objectifs de la safe city et en quoi elle nous permettra d'améliorer leur sécurité et de leur offrir de nouveaux services », conclut Philippe Gendreau. ■

DU CÔTÉ DU FABRICANT

ÉRIC CHAU

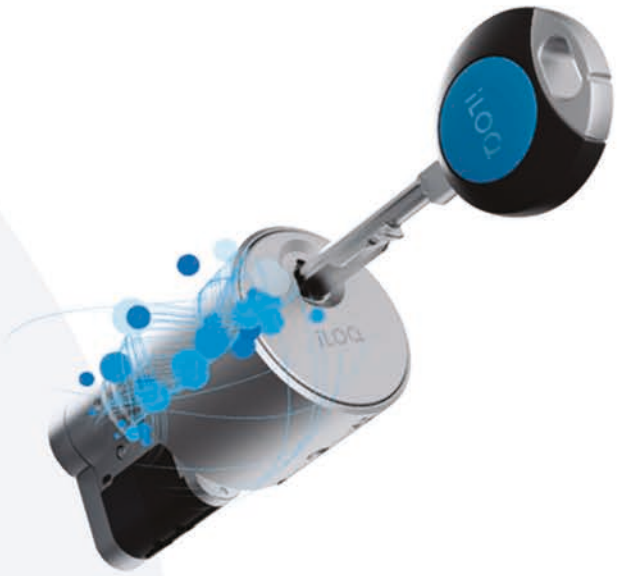
Directeur produit de Datategy

© DR

« Datategy est une start-up spécialisée dans l'analyse des données. Notre plate-forme collaborative Octocity permet de gérer les flux de données des personnes, de l'énergie, du trafic… Nous sommes capables d'utiliser les flux de la vidéosurveillance ou du contrôle d'accès afin de fournir à tout instant les informations nécessaires à l'opérateur. Par exemple, en cas d'incident, comment gérer les flux de personnes ou comment modéliser les déplacements des personnes dans l'infrastructure ? Nous utilisons aussi des données de fréquentation et de verbalisation pour aider les opérateurs de mobilité à gérer leur activité et lutter efficacement contre la fraude… Notre solution vient aisément se greffer sur n'importe quel type de capteurs, n'importe quelle source de données… afin de les analyser et les exploiter de manière pertinente. »

iLOQ

Making life accessible



Système de verrouillage auto-alimenté

iLOQ S10 est le système de verrouillage unique au monde pouvant s'auto-alimenter en récupérant l'électricité nécessaire lors de l'insertion de la clé. Ses serrures et clés programmables peuvent donc fonctionner sans batteries ni câbles.

Gestion des accès mobiles Remplacer les clés classiques par une technologie NFC

L'iLOQ S50 révolutionne la façon dont la gestion des accès mobiles sert le secteur des services publics et privés. iLOQ s'est totalement affranchi des clés physiques et des cylindres de serrure en confiant à des smartphones le pouvoir d'ouvrir tout un monde de possibilités.

01 81 80 14 30
france@iloq.com
www.iloq.com

Publi reportage

Les grands utilisateurs et certains bureaux d'études ont vraiment pris conscience de l'importance de la cybersécurité en matière de vidéosurveillance.

© DR

Pensez à vous protéger contre les cybermenaces !

Bien que les choses progressent en matière de cybersécurité dans la vidéosurveillance, les utilisateurs finaux, les BE, les intégrateurs, installateurs… sont encore démunis. Certains fabricants peuvent vous aider. Et les certifications existent.

Un constat que nous pouvons tous faire : la vidéosurveillance et ses réseaux sont partout. Sur la voie publique, sur nos lieux de travail, dans les transports… Et, compte tenu de cette présence sans cesse croissante, elle est – comme tous les objets connectés au réseaux informatiques – exposée aux cyberattaques. Les caméras de surveillance sont aujourd'hui, pour certains hackers et autres malfrats, les « portes » et outils idéaux pour préparer des attaques et actes délictueux. Les réseaux de vidéosurveillance et de vidéoprotection doivent donc être protégés contre la menace cyber.

Si, il y a encore quelques années, voire mois, les choses étaient loin d'être satisfaisantes en la matière, elles sont en train de changer. L'entrée en vigueur du fameux règlement RGPD y est sans doute pour quelque chose. Mais pas uniquement. Il semble bien que les fabricants, les utilisateurs finaux, les bureaux d'études, les intégrateurs et autres installateurs… aient enfin compris qu'au même titre que les ordinateurs que nous utilisons tous les jours, les réseaux de caméras doivent être protégés. *« Depuis moins d'un an, les choses ont véritablement changé côté utilisateurs finaux dès que l'installation vidéo est reliée au réseau informatique à la demande des DPO,* confirme ainsi Patrice Ferrant, Regional Sales Manager France et Afrique chez Mobotix. *Les grands utilisateurs et certains bureaux d'études ont vraiment pris conscience de l'importance de la cybersécurité en matière de vidéosurveillance. C'est devenu pour eux un vrai sujet et de nouveaux critères de choix dans les cahiers des charges imposés aux installateurs et bureaux d'études. »* Un avis que ne partage pas Philippe Bénard, ingénieur avant ventes chez Axis Communications : *« Contrairement à certains de mes confrères que je trouve un peu optimistes sur le sujet de la prise en compte de la cybersécurité dans la vidéosurveillance, je pense qu'il reste beaucoup à faire et que nous sommes encore loin d'une réelle prise de conscience. Et ce malgré la mise en place du RGPD. »*

On ne rigole pas avec la cybersécurité !

Toutes les installations de vidéo peuvent être la cible d'une attaque cyber, d'une tentative d'intrusion. Qu'il s'agisse des sites sensibles et autres OIV, des collectivités locales, des entreprises… *« Les installations vidéo sur des espaces ouverts au public visualisent et enregistrent des données à caractères personnels,* tient à rappeler Ronan Jézéquel, ingénieur développement au CNPP. *La prise en compte du RGPD est donc primordiale et il faut absolu-*

ment y sensibiliser les acteurs concernés. Et la Cnil est très tatillonne sur le sujet. Les installateurs et les exploitants d'un système de vidéosurveillance doivent prouver qu'ils ont mené une analyse de risque et mis en œuvre des solutions de prévention et de protection contre une cyberattaque en cohérence avec cette analyse. Pour cela, on peut notamment leur conseiller de recourir à des produits certifiés cybersécurité.»
De son côté, Patrice Ferrant insiste sur un point très important, dont ne semble pas toujours conscients certains installateurs: *«C'est le respect du RGPD qui fait désormais foi. L'installateur et le bureau d'études devient coresponsable face à ce règlement. Il déploie un système de vidéo. Si le client final est victime d'un vol de données, il pourra transférer sa responsabilité à l'installateur. Ce dernier se doit donc de déployer et installer des systèmes respectant le RGPD et la norme EN 50 132.»*

Quelles failles? Quels risques?

Le risque en matière de cyberattaque dépend du type d'installation. Si le réseau est dédié à la vidéosurveillance, qu'il n'y a aucune connexion vers internet et aucun câble réseau accessible, le risque provenant de l'extérieur est impossible. *«Cependant nous constatons souvent,* regrette Philippe Bénard, *que la multitude de mots de passe et leur complexité peuvent inciter les utilisateurs à moins de rigueur. L'accès au système est donc réalisé de l'intérieur, par l'utilisation d'un compte opérateur. Le risque est alors la capture d'images.»* Avant d'ajouter: *«Néanmoins un réseau multiservices voix, données, images, contrôle d'accès connecté à internet et avec des câbles réseau à l'extérieur du bâtiment peut être par l'utilisation de techniques connu et reconnu difficilement pénétrable. La mise en place de séparation logique par l'utilisation de VPN, l'utilisation du protocole 802.1X, de mots de passe, et de firewall sur IP et cryptage Https permettra de se prémunir des intrus.»*
«Pour un constructeur, l'accompagnement de l'installateur dans la démarche de cybersécurité est primordial, explique Matthieu Lucas, Product & Marketing Manager chez Bosch Security and Safety Systems. *Malgré la mise en œuvre du RGPD et les recommandations de l'Anssi, il y a encore beaucoup à faire en matière de cybersécurité. Même si la sensibilisation à cette question progresse. Chez Bosch, nous mettons en place des outils qui obligent à respecter certaines règles de sécurité et certains prérequis. Nous sommes, par exemple, très vigilants sur l'authenticité de nos logiciels et firmwares. Par ailleurs, nous fournissons beaucoup d'efforts pour sensibiliser les utilisateurs et les bureaux d'études sur les problématiques de cybersécurité. Nous leur proposons des guides de bonnes pratiques en matière de sécurité. Nous* ● ● ●

NOTE TECHNIQUE DE L'ANSSI

L'Anssi a rédigé une note technique de «Recommandation de sécurité pour la mise en œuvre de dispositifs de vidéoprotection.» Ce document décrit un ensemble de mesures et de principes d'architecture, dont la mise en œuvre vise à contrer ces vulnérabilités potentielles, ou du moins à en limiter l'impact. Les recommandations qu'il formule portent sur l'ensemble des composants d'un dispositif de vidéoprotection: déploiement physique des capteurs, architecture du réseau support, configuration des équipements et du centre de supervision.
→ **www.ssi.gouv.fr/uploads/IMG/pdf/**

LE POINT DE VUE DU CNPP

RONAN JÉZÉQUEL
Ingénieur développement


© DR

«LA CYBERSÉCURITÉ N'EST PAS UNE CONTRAINTE POUR TOUS LES MARCHÉS.»

«La vidéosurveillance est très en retard en matière de cybersécurité. Les raisons de ce retard sont multiples. La principale résidant dans le fait, selon moi, que le marché de la vidéo est un marché mondial: globalement, les fabricants fournissent de gros efforts en matière de résolution, de qualité d'images, de coût… mais il faut reconnaître que, contrairement au marché français, la cybersécurité n'est pas toujours une contrainte pour tous les marchés. De ce fait les contraintes «locales» ne sont pas toujours comprises. C'est dommage car cela permet de rassurer les utilisateurs finaux, les installateurs, les BE… qui recherchent des produits dont la protection contre les cybermenaces soit digne de ce nom.»

renforçons nos liens avec des partenaires comme Genetec autour de l'axe de la cybersécurité. Enfin, nous mettons à disposition de nos utilisateurs et installateurs des outils comme le "Configuration Manager" qui permet de s'assurer du niveau de sécurité des communications avec nos équipements dès la phase d'installation et de mise en service. »

Des minima requis

Tous les éléments constituant un réseau de vidéosurveillance, dès lors qu'ils sont connectés à un réseau, doivent être protégés et sécurisés. Il faut, par exemple, séparer le réseau caméras du réseau interne, en particulier si les caméras sont installées à l'extérieur. C'est d'ailleurs ce que préconise la note technique de l'Anssi du 14 février 2013 relative aux recommandations de sécurité pour la mise en œuvre de dispositifs de vidéoprotection.
D'autres mesures s'imposent. Il faut mettre à jour les micrologiciels des caméras pour corriger les failles de sécurité. On doit aussi filtrer les MAC adresses autorisées sur les switchs (Media Access Control, sorte de numéro de sécu réseau). Il faut en outre impérativement accroître la compléxité des mots de passe et le cryptage des documents. On doit aussi veiller à n'utiliser que des réseaux dédiés et non mutualisés ou, à défaut, se servir des Vlan sécurisés.

PAROLE D'EXPERT

PATRICE FERRANT

Regional Sales Manager France et Afrique chez Mobotix

© DR

« S'APPUYER SUR LES CRITÈRES COMMUNS. »

« De plus en plus de BE, d'intégrateurs… sont conscients des problématiques cyber en matière de vidéosurveillance. Et de plus en plus demandent à ce que nos solutions répondent aux "critères communs" définis en Europe, aux États-Unis ou au Canada et appliqués par des bureaux de contrôle comme le Bsi en Allemagne ou l'Anssi. Les critères communs sont un ensemble de normes (ISO 15408) internationalement reconnues dont l'objectif est d'évaluer de façon impartiale la sécurité des systèmes et des logiciels informatiques. Également dénommés Common Criteria, ce référentiel est né d'un partenariat entre le Canada, les États-Unis et l'Europe. Grâce au cadre offert, les utilisateurs de technologies de l'information vont pouvoir utiliser des profils de protection pour spécifier les exigences fonctionnelles de sécurité attendues et les évaluateurs pourront vérifier que les produits sont bien conformes au niveau d'assurance requis. Chez Mobotix, nous avons parfaitement intégré cette approche depuis deux ans et avons été le premier à obtenir cette certification en Europe répondant aux exigences de BSI (office fédéral allemand de la sécurité des technologies de l'information) reconnus par l'Anssi via les critères communs. Pour le marché français, grâce à notre concept Cactus, nos solutions sont en cours de certification par le CNPP et passent actuellement des essais de robustesse aux attaques numériques. »

3 QUESTIONS À

KARIM ABID-RAHMANE

RSM France

© DR

La vidéosurveillance n'est pas toujours très bien protégée contre les cyberattaques. Et tout ce qui tourne autour du cloud inquiète. Comment sécurisez-vous votre solution sur le cloud ?

Premièrement, les applications VMS dans le cloud refusent toutes les connexions provenant d'internet et du réseau professionnel de l'entreprise. Elles utilisent une authentification basée sur un certificat numérique pour sécuriser leurs connexions au cloud VMS. Que les pirates informatiques et les programmes malveillants se trouvent à l'extérieur ou à l'intérieur du réseau d'entreprise, ils ne peuvent pas accéder à cloud VMS. Deuxièmement, le cloud VMS bloque les tentatives de connexion sortantes provenant de caméras infectées et les mettent en quarantaine contre les réseaux de robots.
Enfin, les applications sur site gérées via le cloud sont automatiquement mises à jour en matière de cybersécurité, sans qu'aucune action de la part du client ou de l'installateur ne soit requise.

Pourquoi est-il mieux protégé que certaines solutions de vos concurrents ?

Les VMS des concurrents enregistrent généralement des vidéos sur site ou dans une salle de serveur gérée par le client. Cela nécessite une assistance, une réparation et une maintenance préventive du service informatique. Eagle Eye Networks cloud VMS est fourni en tant que service, permettant à l'utilisateur final ou à l'intégrateur de ne pas exécuter ces tâches. Cela permet d'économiser de l'argent. Par ailleurs, Eagle Eye VMS comprend des applications mobiles entièrement fonctionnelles. Un installateur et un intégrateur n'ont pas besoin d'un ordinateur pour l'installer.
Le VMS cloud de Eagle Eye Networks est conçu pour être cybersécurisé contre les pirates informatiques. Eagle Eye dispose d'une équipe de sécurité experte qui surveille le système à tout moment. La vidéo est cryptée à tout moment, même lorsqu'elle est stockée.

Quels conseils donner à un utilisateur qui veut protéger son système de surveillance ?

Il faut d'abord que les problématiques de cybersécurité soient traitées et prises en considération comme elles devraient l'être. Il ne faut pas les négliger lors du choix de telle ou telle solution hardware ou software.
En outre, il convient d'examiner en particulier la manière dont la cybersécurité est organisée dans une solution sur site et de la comparer à la cybersécurité d'une solution cloud, à la fois en termes de coûts et d'efficacité. Un VMS cloud bien conçu crypte les données vidéo lorsque son dispositif de mémoire tampon sur site les reçoit de la caméra, en utilisant le cryptage AES à 256 bits. Il le transmet ensuite en toute sécurité au cloud VMS. Il peut aussi fournir une authentification à deux facteurs pour l'accès des utilisateurs à l'application VMS, ainsi qu'une authentification pour les appareils mobiles.

PAROLE D'EXPERT

PIERRE SANGOUARD
Directeur général de Provision-ISR France


© DR

« PROPOSER LES BONS OUTILS À NOS PARTENAIRES. »

« En matière de cybersécurité, nous sommes confrontés à deux problèmes : la protection des systèmes et le facteur humain. Il faut faire monter en compétence les installateurs et autres intégrateurs sur ce sujet. Il faut ensuite proposer à nos partenaires des outils qui leur permettent de protéger les différents éléments d'une installation vidéo. Tout commence par le durcissement des mots de passe pour ne serait-ce que les protéger contre les robots cyber. Nous avons conçu une solution qui bloque le système après un certain nombre de tentatives échouées. Il faut protéger les communications en utilisant des protocoles de sécurité avancée et en désactivant par défaut tous les protocoles ouverts, durcir les systèmes grâce à des switches durcis pour isoler le réseau des caméras et les protéger des intrusions, sécuriser les NVR, et effectuer les mises à jour de sécurité des firmwaresles BE. »

LIVRES BLANCS ET AUTRES MANUELS

• **AXIS** met à votre disposition un livre blanc (en anglais) sur les firmwares : **www.axis.com/files/whitepaper/wp_firmware_mgmt_72339_en_1809_lo.pdf**

• **BOSCH** : **http://resource.boschsecurity.com/documents/Data_Security_Guideb_Special_frFR_9007221590612491.pdf**

• **EAGLE EYE NETWORKS** met à disposition un livre blanc sur la cybersécurité : **www.een.com/cyber-security-cloud-video-surveillance/**

• **GENETEC** propose son centre de confiance : **www.genetec.com/fr/soutien-et-services/centre-de-confiance/%C3%A9tablir-une-relation-de-confiance.** Un grand nombre de ressources sur les problématiques cyber dans la vidéosurveillance.

• **MOBOTIX** propose un *Guide de cyberprotection. Comment protéger votre système vidéo Mobotix ?* : **www.mobotix.com/sites/default/files/2018-02/Mx_Guide_de_cyberprotection_fr_20180220.pdf**

• **PROVISION-ISR** propose sur son site des bonnes pratiques et conseils de paramétrages sécurité : **www.provision-isr.com/index.php?option=com_content&view=article&id=170:notification-of-vulnerabilities&catid=45&Itemid=58**

LE POINT DE VUE D'UN FABRICANT

PHILIPPE BÉNARD

Ingénieur avant ventes chez Axis Communications

© DR

« NOUS SOMMES TRÈS VIGILANTS QUANT À LA PROTECTION CYBER DE NOS PRODUITS. »

« L'OS de nos produits est un noyau Linux. Cet OS est utilisé dans des équipements aussi variés que l'ordinateur de bord de voitures, routeur IP, serveur... Il est développé par une communauté qui aujourd'hui représente des milliers de programmeurs et docteurs en cybersécurité. Il est arrivé que des travaux de recherche autour du Kernel Linux mettent à jour des failles de sécurité comme CVE-2017-9765 qui a été corrigé immédiatement, Axis délivrant un patch sur l'ensemble des produits dans le mois suivant (information sur www.axis.com/fr-fr/support/product-security) a contrario des OS propriétaires qui ne sont pas exempts de failles de sécurité et sur lesquelles le nombre de développeurs est limité. Nous permettons, via la technologie Acap, le téléchargement d'applications comme la détection périmétrique, le comptage, la détection de fumées, la lecture de plaque d'immatriculation. Ces applications installées dans le cœur de la caméra utilisent les mêmes ressources cyber que celle-ci soit l'intégration dans un VPN, le 802.1X, mots de passe, firewall, cryptage HTTPS. L'ensemble des outils cité 802.1X, mots de passe, firewall, HTTPS sont intégrés nativement dans l'environnement Linux et donc parfaitement fiables et opérationnels. Nous disposons d'un outil Axis Device Manager qui permet entre autres de diffuser les certificats 802.1X, de façon globale et centralisée. »

Exigez des matériels testés

Le CNPP teste les solutions de vidéosurveillance pour vérifier leur protection réelle contre les cyberattaques. *« Il faut être très exigeant en matière de cybersécurité. Nous avons élaboré un certain nombre d'exigences fermes pour les matériels de vidéosurveillance,* insiste l'expert du CNPP. *Nous testons les matériels selon une méthode d'essais spécifique aux objets connectés, la ST DEC 1704, applicable aux matériels de vidéo comme les caméras, les NVR... Nous avons intégré cette méthode à nos spécifications techniques sur lesquelles s'appuient nos certifications de produits qui couvrent aujourd'hui ce sujet de la cybersécurité. Cela nous permet de définir et de vérifier que les produits testés sont, un minimum, protégés intrinsèquement contre les menaces cyber, qu'ils sont robustes "by design". »*

« Malgré la mise en œuvre du RGPD, il y a encore beaucoup à faire en matière de cybersécurité. Même si la sensibilisation à cette question progresse. »

LUCAS MATTHIEU, PRODUCT & MARKETING MANAGER CHEZ BOSCH SECURITY

Lors de ses essais, le CNPP teste la caméra elle-même, mais aussi les protocoles de communication et les applications logicielles qui permettent de se connecter au système, de le piloter, de visualiser à distance... *« Nous imposons dans le cadre de nos certifications que les produits testés satisfassent le premier des trois niveaux du référentiel cyber. Cela correspond à vérifier qu'il n'existe pas de vulnérabilité de criticité haute, c'est-à-dire que les failles éventuelles ne sont pas facilement exploitables et que leur exploitation ne permet pas un impact maximum... C'est la garantie d'un niveau minimum pour les caméras. »* Le CNPP teste aussi la sécurité des protocoles associés aux communications (wi-fi, Bluetooth, Lora, Lora1...), et contrôle le niveau de protection des données, leur confidentialité, la manière dont est assurée leur intégrité, leur disponibilité... *« Il faut reconnaître que si on appliquait nos exigences aux solutions actuellement déployées sur le marché, 95 % des caméras n'y satisferaient pas... »*, conclut Ronan Jézéquel.

DU CÔTÉ DES VMS

LAURENT VILLENEUVE

Product Marketing Manager cybersécurité chez Genetec

© DR

« IL FAUT FAIRE SIMPLE ET BÂTIR UNE RELATION DE CONFIANCE AVEC NOS PARTENAIRES. »

« Compte tenu des difficultés que connaissent les utilisateurs pour prendre en considération la cybersécurité de leurs installations, il nous faut la rendre la plus simple possible. Leur mâcher le travail en quelque sorte… Il faut être pratique et faire simple. Pour cela, chez Genetec, nous nous astreignons, dès la conception de nos solutions, et en particulier notre VMS Security Center Omnicast, à y intégrer un haut niveau de sécurité, avec plusieurs couches de protection qui évoluent au gré des technologies et des menaces. Nous protégeons les données avec de la cryptographie, et multiples méthodes de vérification d'identité et d'autorisation… afin de limiter les accès aux données. Par ailleurs, nous soumettons plusieurs fois par an nos produits à des firmes externes pour des tests de pénétrabilité. Enfin, nous sommes très sensibles à la certification qui rassure nos partenaires. Notre solution Omnicast, certifiée UL 2009-2-3, respecte les directives de l'Anssi.»

HIKVISION

TECHNOLOGIE ACUSENSE

INTÉGRATION DE FILTRES D'ALARME INTELLIGENTS ET DE FONCTIONNALITÉS DE RECHERCHE CIBLÉE POUR LES PETITES ET MOYENNES ENTREPRISES

Filtrer les fausses alarmes

Déclenchement d'alarme

Filtrer tout en enregistrant en vidéo

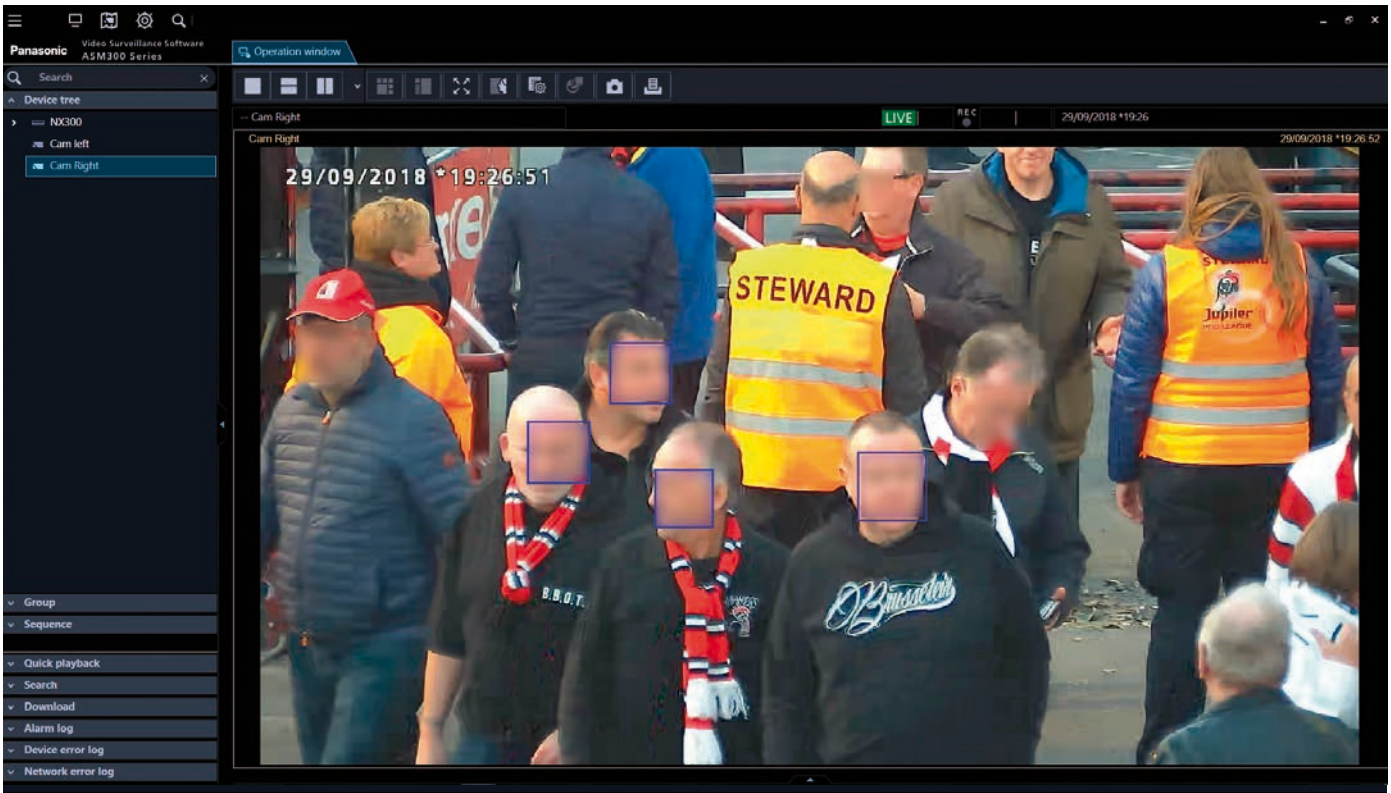
Recherche rapide de cible

Avec la technologie AcuSense de Hikvision, les PME bénéficient désormais des dernières avancées en matière de technologie Deep Learning, directement incorporées dans leurs systèmes de sécurité existants, via une seule caméra AcuSense ou un Acusense DVR/NVR.

Hikvision France
6, rue paul cézanne
93360
Neuilly Plaisance
France
Tél +33 (0)1 85 33 04 50
marketing.fr@hikvision.com

@HikvisionFrance @hikvisionfr @Hikvision France

AcuSense
www.hikvision.com/fr



Contrôler l'accès à des stades et équipements sportifs, une nouvelle application de la reconnaissance faciale qui suscite un intérêt croissant.

© Panasonic

Reconnaissance faciale, la biométrie qui monte

Avec à peine 4 % du marché des lecteurs biométriques vendus dans le monde, la reconnaissance faciale semble une niche, loin derrière les lecteurs d'empreinte digitale qui représentent plus de 92 %. Mais la révolution de l'intelligence artificielle associée à des outils de capture d'image de plus en plus qualitatifs pourrait changer la donne.

La reconnaissance faciale gagne du terrain. Pas une semaine sans qu'une banque, un aéroport ou un stade ne communique sur de nouvelles modalités d'accès à ses locaux par la reconnaissance faciale. Les états ne sont pas en reste, et le contrôle aux frontières utilisent de plus en plus ces technologies. L'Europe, va encore plus loin sur ses frontières Schengen, puisqu'elle teste actuellement sur des voyageurs volontaires le programme IBorder Ctrl, un système automatique de contrôle qui allie la vérification des documents d'identité, la reconnaissance faciale et signes de tentative de fraudes (basée sur les expressions du visage). Difficile de faire l'impasse sur cette technologie qui, dès à présent, permet de déverrouiller son téléphone ou d'effectuer des paiements bancaires. Le cabinet de recherche Crone Consulting LLC estime que la reconnaissance faciale devrait concerner plus de la moitié des identifications sur les smartphones d'ici les trois à cinq prochaines années. De leur côté, les acteurs de la vidéosurveillance développent des logiciels vidéos d'analyse de l'image de plus en plus puissants et performants. Le contrôle d'accès échappera-t-il à cette vague de fond ?

La vidéosurveillance, premier outil de reconnaissance faciale

Walid Maadan, directeur commercial de Safe Security, installateur de solutions de sécurité, estime qu'il faut distinguer la reconnaissance faciale dans deux types de configuration, la reconnais-

3 QUESTIONS À

BAUDOUIN BENOUVILLE

Directeur du développent commercial région EMEA, Suprema

© DR

Le marché du contrôle d'accès par reconnaissance faciale a-t-il de l'avenir ?

Selon IHS Markit, le contrôle d'accès par reconnaissance faciale n'a compté que pour 3 % des lecteurs biométriques vendus dans le monde en 2017. Cependant, ce type de produit est celui qui présente la plus forte croissance annuelle (+ 22 %). Grâce à la baisse de certains composants électroniques, le prix du FaceLite de Suprema pour le contrôle d'accès par reconnaissance faciale sera désormais identique à celui des lecteurs d'empreintes digitales 2D.

Quel est l'intérêt de l'infrarouge ?

Pour une application de «Black Listing» telle qu'identifier un vandale dans un stade de foot, la technologie par camera optique (Axis, Pelco, Bosch, Honeywell, Hikvision) suffit. Pour une application de «White Listing», ou le système doit donner à un individu l'autorisation de pénétrer dans une zone restreinte (contrôle d'accès), l'infrarouge (Near-Infra-Red, NIR) est bien plus fiable que les caméras optiques. Le NIR n'est pas perturbé par les variations de luminosité ou de couleurs, les reflets, les taches d'ombre ou le maquillage. Un lecteur comme la FaceStation2, dispose d'un processeur quatre-cœurs qui permet le traitement quasi instantané de la donnée infrarouge. De plus, aucune image brute (sensible, car du domaine de la donnée privée) n'est stockée. Seul un gabarit biométrique est stocké en base.

Qui vous demande ce type de lecteurs ?

En France, où le marché de la biométrie est un peu moins développé que chez ses voisins, nous avons installé le FaceStation2 dans des banques, des data centers, des bureaux (protection des données sensibles ou du cash), des casinos (protection de cash et de jetons), des hôpitaux (protection de médicaments sensibles), des bureaux de police (casier à effets personnels ou armes à feu) ou des chantiers.
À l'horizon 2022, nous pensons qu'elle a des chances de devenir la première technologie de reconnaissance biométrique utilisée dans le monde (smartphone, contrôles d'identité aux aéroports, systèmes de sûreté/sécurité).

sance via la vidéo, ou celle effectuée par un lecteur biométrique : *« Lorsqu'elle est intégrée dans le système de vidéosurveillance, l'analyse des visages se fait via les images de la caméra. Dans ce cas de figure, elle sert généralement à faciliter à l'utilisateur la relecture de ses enregistrements en effectuant une recherche par visage. Le système trouve ainsi seulement les séquences vidéos du – ou des – visage recherché et constitue une aide complémentaire dans la gestion d'un système de vidéosurveillance. Cela peut concerner la détection de personnes recherchées dans un espace public, ou encore la détection de personnes ayant déjà commis un acte répréhensible comme un vol ou une dégradation dans un centre commercial, par exemple. Les limites de la reconnaissance sont liées à la qualité de l'image et aux conditions de prises de vue : obscurité, éloignement du visage de l'objectif de la caméra, port d'une capuche ou autre… »* La qualité de la reconnaissance faciale dans le cas de lecture à la volée, par exemple dans un espace public, doit encore progresser. *« Si l'image capturée par la caméra est de mauvaise qualité,* explique Philippe Henaine, Key Account Manager de Panasonic, *l'analyse par le logiciel sera médiocre et le taux de reconnaissance insatisfaisant. Chez Panasonic, nous pouvons faire tourner un logiciel qui prépare l'image dans la caméra avant transmission au logiciel de reconnaissance : détection du visage, réglage des contrastes, transmission uniquement de la zone visage pour accroître la rapidité. Cette combinaison améliore fortement le taux de reconnaissance. C'est un produit qui intéresse grandement les centres commerciaux, aussi bien pour la recherche de personnes perdues que pour suivre le parcours de personnes suspectes. Les images sont automatiquement détruites au bout d'une durée déterminée, lorsque la personne est retrouvée ou si elle quitte les lieux. Les hôpitaux sont aussi très intéressés, notamment pour être alertés en cas de tentatives de sorties de personnes désorientées. L'intérêt de notre système de reconnaissance faciale* ● ● ●

SOLUTION PRODUIT

Facelite, la reconnaissance faciale au prix d'un lecteur d'empreinte digitale

Une des raisons principales de la prédominance de l'empreinte digitale, dans le contrôle d'accès biométrique, est le prix accessible de la technologie, environ trois fois supérieur à un lecteur RFID standard. Jusqu'alors, un lecteur de reconnaissance faciale coûtait en moyenne quatre fois le prix d'un lecteur d'empreinte, soit douze fois plus qu'un lecteur à cartes RFID, un frein avéré pour les structures désireuses de passer à un contrôle biométrique sans contact. Le tout nouveau lecteur FaceLite de Suprema, présenté en avant-première au salon Intersec de Dubaï, se positionne au même prix qu'un lecteur d'empreintes digitales tout en gardant des spécifications similaires à la FaceStation2 (à savoir une reconnaissance Faciale de haute précision par infrarouge). *«Pour les utilisateurs qui souhaitent un contrôle d'accès biométrique autre que par empreinte digitale, le FaceLite permet de rendre la reconnaissance faciale à un prix accessible, sans faire de concession sur la performance, la sécurité et la protection des données privées»*, a déclaré Baudoin Genouville, directeur du développement EMEA, Suprema.

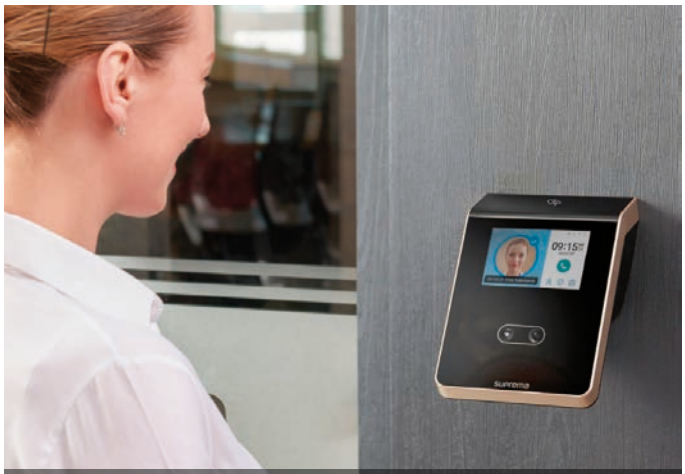
© Suprema

● ● ● *est qu'il s'implémente facilement sur nos caméras. Et la vidéo est très présente, aussi bien dans les centres commerciaux que dans les centres hospitaliers.* »

Équipements sportifs : les whitelistés et les blacklistés

Les équipements sportifs sont eux aussi très demandeurs de solutions pour le contrôle d'accès avec reconnaissance faciale. Zetes, filiale de Panasonic a annoncé la mise en place d'un système de contrôle d'accès pour le Racing White Daring de Molenbeek, basé sur le logiciel de serveur de reconnaissance faciale Panasonic WV-ASF950. Lorsque les membres s'inscrivent en ligne pour leur billet de saison, ils fournissent une photo pour accéder facilement au stade les jours de match. Lorsque les détenteurs de billets de saison RWDM arrivent dans leur stade, les caméras installées sur place, combinées au logiciel Panasonic, peuvent capturer et analyser leurs visages et les comparer à leur base de données. La base de données contiendra des images fournies par ceux qui ont commandé un abonnement en ligne via la plate-forme ZetesFastrace. « *La technologie de reconnaissance faciale est un moyen de nous assurer que seules les personnes autorisées ont accès aux stands,* a expliqué Thierry Dailly, le président du RWDM. *La très grande fiabilité du système de reconnaissance, combinée à un traitement rapide des données, nous a permis de fluidifier les accès. Ce système est aussi peu intrusif que possible pour nos membres et accélère les contrôles à l'entrée.* »

Dans le cas de Molenbeek, la reconnaissance faciale est circonscrite aux contrôles d'accès. Les photos téléchargées par les supporters sont stockées sur un serveur du RWDM, qui n'est pas raccordé à internet ni à aucun autre réseau. Seul le personnel habilité du RWDM y a accès. Par ailleurs, les images prises par les caméras à l'entrée ne sont pas enregistrées afin de protéger la vie privée des supporters. Le test de cette « white list » (liste de personnes autorisées) suscite beaucoup d'intérêt de la part de stades de foot et de rugby de l'Europe entière.



Le contrôle d'accès par reconnaissance faciale trouve sa place dans les établissements qui souhaitent une haute sécurité.

© Suprema

« *Des caméras placées aux entrées d'un stade, en contrôle d'accès sont dans des conditions idéales pour une excellente fiabilité,* assure Philippe Henaine, Key Account Manager de Panasonic. *Les personnes se placent face caméra et le taux de reconnaissance avoisine les 98 %. Les équipements sportifs, dans certains pays, souhaitent également mettre en place des « black lists » pour la reconnaissance de hooligans interdits de stade. La fonctionnalité peut être mise en place lorsque la législation le permet, et notre logiciel peut reconnaître jusqu'à 30 000 personnes "blacks listés".* »

PAROLE D'EXPERT

LAURENT LEPETIT

Responsable valorisation technologique & partenariats, ID3

© DR

« LE DEEP LEARNING CONSTITUE UNE VRAIE RUPTURE TECHNOLOGIQUE. »

« Jusqu'à peu, la reconnaissance s'appuyait sur des mesures biométriques. Les algorithmes mesuraient un certain nombre de points sur le visage et les comparaient aux mesures de références pour la personne à identifier ou à authentifier. Plus le nombre de points comparés était élevé, plus le logiciel était considéré comme performant et fiable. Avec le deep learning, on vit une vraie rupture technologique. Les performances ont explosé. Le logiciel que nous avons développé se base sur un système dit neuronal d'auto-apprentissage. Au départ, le logiciel est alimenté avec des dizaines de millions de visages triés et peu à peu « apprend » à reconnaître les personnes et développe un « mode de raisonnement » qui lui est propre. Au fur et à mesure, le logiciel améliore ses capacités de reconnaissance et peut prendre en compte des modifications volontaires ou non : port de lunettes, coupe de cheveux, maquillage, vieillissement... Nos résultats de reconnaissance sont exceptionnels. L'avantage est de pouvoir capter des visages à la volée, extrêmement rapidement avec un temps de comparaison de quelques nanosecondes en authentification (1:1) et 6 millions de matches à la seconde en identification, (1:N). Nous travaillons avec les intégrateurs et nous leur fournissons un SDK (kit de développement logiciel) qui va s'interfacer entre les caméras et le serveur de leurs clients. Notre logiciel est déjà utilisé pour des accès d'entreprises en Allemagne (avec une carte d'accès). Il suscite le plus grand intérêt d'opérateur d'importance vitale et est en cours de validation dans un environnement aéroportuaire. Notre logiciel est également utilisé en vidéosurveillance aux États-Unis avec une fonctionnalité toute particulière : outre la reconnaissance faciale, il est couplé à un logiciel de reconnaissance d'armes à feu et permet de lever une alarme. »

La Cnil réservée

Alors que les logiciels de reconnaissance faciale se multiplient et peuvent s'adapter à toute une gamme d'équipements dotés de caméras, on trouve assez peu de lecteurs biométriques à reconnaissance faciale dédié au contrôle d'accès. Les principaux sont Idemia, Suprema, Anviz... *« Dans cette configuration,* reprend Abdelilah Attaf, directeur général de Safe Security, *la personne qui a été enrôlée dans la base, se présente, volontairement devant le lecteur. Le visage de la personne qui se présente à la porte est détecté. Le logiciel consulte une base de données et autorise ou non l'accès en déverrouillant la porte. La reconnaissance est proche de 100 %. Le système est économique, si on considère qu'il évite la gestion de badges et le problème des pertes ou des vols. Cependant, son utilisation est limitée en raison de la réglementation. »* En effet, la CnilL estime que *« les enjeux de protection des données et les risques d'atteintes aux libertés individuelles que de tels dispositifs sont susceptibles d'induire sont considérables. Tout projet d'y recourir devra à tout le moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD). »* Cette analyse peut être menée par le fournisseur d'un produit (matériel, logiciel ou service) pour évaluer l'impact sur la protection des données de son produit. Les différents responsables de traitement qui utilisent ensuite ce produit doivent mener leurs propres AIPD mais, le cas échéant, ceux-ci peuvent être alimentés par l'AIPD du fournisseur. La Cnil vient d'ailleurs de publier des guides pour aider à effectuer cette analyse. Procédure récente issue du RGPD, l'avenir dira si l'AIPD favorisera le déploiement du contrôle d'accès par reconnaissance faciale ou le limitera.

AMERICAN AIRLINES TESTE LA RECONNAISSANCE FACIALE

Gemalto a annoncé un projet pilote avec American Airlines pour offrir aux voyageurs un embarquement biométrique sécurisé à l'aéroport international de Los Angeles. *« Être en mesure d'utiliser son visage au lieu d'une carte d'embarquement permettra non seulement de renforcer la sécurité, mais aussi d'embarquer plus facilement et rapidement »*, a déclaré Neville Pattinson, vice-président en charge des programmes gouvernementaux chez Gemalto. Ce pilote offre une grande flexibilité.
Le système d'identification de visages en direct Gemalto Cogent est un système de reconnaissance faciale vidéo qui reconnaît automatiquement les visages dans une foule, même dans des environnements dynamiques et incontrôlés. Le système peut être intégré dans une large gamme d'équipements vidéo, et des algorithmes avancés augmentent la précision des correspondances. Dans le cas de l'aéroport de Los Angeles, les passagers s'approcheront de la porte d'embarquement et, à la suite d'une vérification faciale effectuée par les services de contrôle des voyageurs du CBP, ils recevront une confirmation sur un écran.
Une fois vérifiées, les images saisies seront effacées du système pour garantir la confidentialité des passagers.

Les caméras thermiques : voir tout le temps

Les caméras thermiques vous assurent de voir et détecter une anomalie, quels que soient leur environnement et les conditions de luminosité.

SÉRIE FC-S – FLIR SYSTEMS

QUELLES QUE SOIENT LES CONDITIONS ATMOSPHÉRIQUES

L'imagerie thermique vous permet de voir les intrus dans l'obscurité totale, dans pratiquement toutes les conditions atmosphériques. Les modèles de la série FC-S sont extrêmement robustes. Leurs organes sont bien protégés, jusqu'à IP66. Ils fonctionnent (en continu) sur une plage de températures unique de –50 °C à +70 °C. Il existe plusieurs canaux pour le flux de vidéo numérique, aux formats H.264, MPEG-4 et M-JPEG. Il est possible d'obtenir simultanément une sortie vidéo composite et numérique. Chaque caméra série FC-S est livrée avec la version mono capteur du logiciel Sensor Manager de FLIR. Ce logiciel intuitif permet aux utilisateurs de gérer et de commander une caméra série FC-S dans un réseau TCP/IP.

→ CARACTÉRISTIQUES : • Les caméras thermiques série FC-S sont proposées en deux modèles : un de 320 × 240 pixels, l'autre de haute résolution, de 640 × 480 pixels. Afin qu'il existe une caméra série FC-S pour chaque application de sécurité, Flir Systems propose une grande variété d'objectifs. Ceux de grande focale possèdent un champ de vision plus étroit et permettent de repérer les intrus de plus loin. Les objectifs proposés vont du grand angle pour un champ de vision de 90° en horizontal X 69° en vertical au téléobjectif pour un champ de vision de 9° en horizontal X 7° en vertical.

La série FC-S est une caméra hybride. Avec la fonction PoE (Power over Ethernet), un seul câble assure la communication et l'alimentation. La série FC-S peut être intégrée à tout réseau TCP/IP existant, et être commandée par ordinateur. Aucun câble supplémentaire n'est nécessaire. La série FC-S est conforme à la norme ONVIF 2.0 et peut donc être facilement raccordée à un réseau d'autres capteurs.

© Flir Systems

CAMÉRAS IR IP – GEUTEBRUCK

SURVEILLER EN TOUTE DISCRÉTION

Ces caméras infrarouges IP professionnelles permettent d'assurer une vidéosurveillance discrète 24 h/24, que ce soit en pleine obscurité ou avec du brouillard ou de la fumée. Grâce au système d'analyse vidéo G-Tect/VMX, ces caméras permettent non seulement d'optimiser la sécurisation des périmètres de zones de surveillance mais réduisent également le taux de fausses alertes. Avec des distances focales comprises entre 7,5 mm et 35 mm et un angle de vision horizontal entre 40° et 9°, elles conviennent tout particulièrement pour la surveillance de vastes terrains.

→ CARACTÉRISTIQUES : • Les objets et les personnes qui dégagent de la chaleur peuvent être détectés à un stade précoce sur de longues distances: les personnes jusqu'à 1 450 mètres et les véhicules jusqu'à 3,4 km. La fonction d'optimisation du contraste fournit des images nettes tandis que le procédé de compression H264CCTV optimisé pour les systèmes de vidéosurveillance garantit une lecture avant et arrière fluide et sans interruption des images d'enregistrement.

© Geutebruck

DÔME TCX PTZ – FLIR SYSTEMS

ANALYSE DE MOUVEMENTS INTÉGRÉE

© Flir Systems

Flir Systems propose la TCX PTZ (orientation, inclinaison, zoom), caméra thermique PTZ compatible avec les normes vidéo les plus élevées du secteur qui comporte également une fonction d'analyse intégrée des mouvements sur les vidéos (VMD). La TCX PTZ est compatible avec les systèmes de sécurité existants, y compris les systèmes MPX de Flir, ou HDCVI, IP et analogiques. Elle est également compatible avec la norme Onvif Profil S qui lui permet de facilement s'intégrer aux technologies existantes de détection des intrusions (détecteurs de mouvements, fils piège et protection périmétrique).

→ CARACTÉRISTIQUES :

• La TCX PTZ associe une fonction d'analyse des mouvements sur les vidéos (VMD) à une technologie vidéo propriétaire de Flir, la grande plage de mesure dynamique des données thermiques (WDR), pour afficher des images d'avant-plan et d'arrière-plan riches en contrastes qui améliorent les performances d'analyse vidéo. Disponible dans une résolution de 640 x 480 avec un objectif de 32 degrés ou de 320 x 240 avec un objectif de 25 degrés, les deux étant dotés d'un zoom électronique continu x4 et d'une fonction panoramique continue à 360 degrés, la TCX PTZ capture les séquences vidéo sous plusieurs angles et perspectives.

© Hanwha

WISENET T - HANWHA FRANCE

DÉTECTION DANS LES ENVIRONNEMENTS DIFFICILES

Ces cinq nouvelles caméras thermiques anti-vandales de la gamme Wisenet T, capables de filmer des vidéos jusqu'à une résolution de 640 x 480, ont été conçues pour détecter les objets et les personnes en environnement difficile, par exemple à travers la fumée, la neige, les fortes pluies et le brouillard, ce dont les caméras traditionnelles ne sont pas toujours capables. Elles représentent également une solution efficace pour les projets dans lesquels la pollution visuelle peut poser des problèmes.

→ CARACTÉRISTIQUES : • Les capteurs gyroscopiques intégrés assurent une stabilisation fiable pour assurer que les images restent fixes en cas de vent ou de vibration.

M15D – MOBOTIX

MESURER LE RAYONNEMENT THERMIQUE

© Mobotix

Les nouveaux modules de la caméra thermique M15D mesurent le rayonnement thermique d'objets, de véhicules ou de personnes, et fonctionnent donc même dans une obscurité absolue. Combinés avec le logiciel de détection de déplacements MxActivitySensor de Mobotix, ils détectent les mouvements dans l'image, de jour comme de nuit. En revanche, seuls les déplacements d'humains ou de véhicules déclenchent un événement. Les objets qui bougent mais ne se déplacent pas ne déclenchent pas d'alarme. Même de jour, les modules thermiques détectent les objets ou individus en déplacement situés dans l'ombre, dans la pénombre ou derrière des buissons.

→ CARACTÉRISTIQUES : • La combinaison des deux images d'une caméra double M15 équipée d'un module thermique et d'un capteur de lumière diurne permet, d'une part, de fournir des enregistrements 5 mégapixels HR de jour ou au crépuscule et, d'autre part, de détecter les déplacements de manière fiable de nuit. Les modules thermiques Mobotix sont certifiés résistants aux intempéries (norme IP65) et sont disponibles en diverses distances focales, tout comme les modules diurnes.

La sécurité de demain ? Le robot O-R3 d'Otsaw Digital est capable de collaborer avec un drone.

© Otsaw Digital

Robotisation : vers la collaboration robots-drones ?

L'utilisation de robots dans la surveillance de site et la lutte contre l'intrusion est plus que jamais d'actualité. Les tests se multiplient. Mais il semble bien que les professionnels du secteur et leurs clients envisagent de plus en plus d'associer robots terrestres et drones. Voici pourquoi.

Le monde de la sécurité développe aujourd'hui des offres techniques et des prestations que certains appellent déjà le cyberguarding. Les drones et les robots terrestres font partie de cette nouvelle offre. Ils patrouillent déjà sur certains sites et volent au-dessus d'autres. Mais des entreprises de sécurité et des donneurs d'ordres envisagent sérieusement de faire collaborer les drones terrestres, des véhicules autonomes et autres drones. Un exemple que nous avons déjà rapporté dans notre précédent numéro : des chercheurs hongrois de l'Académie des sciences de Hongrie, de l'université Eötvös Loránd et de l'université d'Amsterdam, ont réussi à faire voler en essaim trente drones, sans que ces derniers soient pilotés, programmés à l'avance ou dirigés depuis le sol par un ordinateur. Comme l'explique notre confrère *Le Figaro* : *« Le groupe de quadricoptères s'adapte et évite les obstacles grâce à l'intelligence collective, comme celle d'un banc de poissons ou d'un nuage d'étourneaux. […] Chaque fois qu'un drone rencontre un obstacle, il en transmet l'information à ses collègues et le groupe s'y adapte. »* Autre exemple : à Singapour, Otsaw Digital a développé O-R3, un robot patrouilleur autonome qui peut collaborer avec un drone de surveillance et ainsi créer un système mobile capable de lancer l'engin volant pour suivre les intrus et indiquer leur position. Enfin, le gyropode Segway pourrait bientôt avoir des applications dans la sécurité. La société Turing Video a ainsi conçu Nimbo qui, grâce à l'IA, est capable d'apprendre à reconnaître les situations à risque et de patrouiller en équipe pour prévenir toute menace !

Une place évidente dans le marché

Les robots – terrestres ou volants – auront toute leur place dans le paysage de la sécurité de demain. Associés à des hommes ou pas. *« Les robots sont d'ores et déjà d'actualité dans nos métiers,*

LE POINT DE VUE D'UN FABRICANT

MATHILDE BRAVAIS

Directrice marketing de TBC France

© DR

«IL FAUT INTÉGRER DE L'IA AUX ROBOTS.»

«On parle beaucoup des applications possibles des drones et des robots terrestres dans la sécurité. Elles existent mais on doit, selon moi, passer par une phase de tests afin de définir avec l'utilisateur final ses besoins réels et cela de manière précise. Associer un drone à un robot terrestre peut être pertinent car les drones et les robots ont chacun des avantages et des inconvénients. Cette association peut permettre de pallier ces inconvénients. Un robot seul peut remplacer efficacement un agent de terrain ou compléter sa mission sur le terrain. Le robot terrestre est capable de surveiller de grands espaces, en extérieur et en intérieur, de protéger un site vide, et ce, 24 h/24. Il permet donc de réduire les coûts de gardiennage. Il peut aussi communiquer avec un agent en lui envoyant des images ou des alarmes. Mais il faut aller plus loin. Nous devons intégrer à nos robots, et c'est ce à quoi nous travaillons pour notre robot Jack, de l'intelligence artificielle associée à de l'analyse d'image afin de lui permettre de reconnaître un être humain, une voiture, un animal… Pour être capable d'alerter, à bon escient, l'opérateur ou l'agent de sécurité et, ainsi, limiter les fausses alarmes. Les robots vont devenir ainsi, à terme, les yeux des gardiens sur le terrain. Par ailleurs, pour en faire une solution à réelle plus-value, nous allons devoir réfléchir à l'intégration d'autres capteurs dans les robots : capteurs de chaleur, capteurs thermiques, détecteurs de fumée… ce qu'on ne peut pas encore faire avec un drone qui est limité en matière de charge utile.»

confirme Servan Lépine, président d'Excelium. *La sécurité privée est et sera impactée par ces innovations, associées à des moyens humains car, outre leurs atouts en matière technique, ils permettront de proposer aux clients des prestations mieux adaptées à leurs budgets. Par ailleurs, si nous avons d'abord réfléchi en silo, en séparant les robots terrestres et leurs possibles utilisations, et les drones, aujourd'hui, il est indéniable que ces deux types de robots sont totalement complémentaires.»*

Les robots intéressent donc de plus en plus les entreprises qui souhaitent protéger leurs sites et infrastructures contre les intrusions et tout autre acte de malveillance. *«L'intérêt suscité par les robots est évident. Et nous réalisons de nombreux tests avec des utilisateurs finaux afin de définir au mieux, en étroite collaboration avec eux, les fonctionnalités de notre robot Jack et les besoins réels de l'utilisateur final,* explique Mathilde Bravais, responsable marketing chez TBC France. *Ces tests, que nous menons actuellement avec une entreprise du CAC 40, concerne non seulement l'utilisation de notre robot, seul sur site, mais aussi en association avec des drones afin de voir lequel est le plus efficace et si la collaboration des deux plates-formes apporte un plus à la démarche sécurité de notre partenaire.»*

© Azur Drones

Stéphane Morelli, directeur général d'Azur Drones, considère que ses drones pourraient, à terme, tout à fait «collaborer» avec des robots terrestres.

Drone/robot : on y réfléchit

Chez Azur Drones, spécialiste du drone de surveillance, l'association robot terrestre/drone est à l'ordre du jour. Ce que nous confirme Stéphane Morelli, son directeur général : ●●●

DU CÔTÉ DES DRONES

STÉPHANE MORELLI

Directeur général d'Azur Drones

© DR

«UNE ASSOCIATION PAS SI SIMPLE…»

«Le drone, malgré ses atouts, reste essentiellement à ce jour un outil d'observation, et pas d'intervention puisqu'il n'emporte pas de masse importante. Ce que peut faire le robot terrestre. À l'inverse, le drone se déplace rapidement et sa position haute permet de mieux voir ce qui se passe sur le site. Tout l'intérêt de l'association drones-robots terrestres réside dans le fait que leur collaboration permet de combiner leurs atouts respectifs et donc de fournir des informations plus qualifiées à l'opérateur ou l'agent de sécurité, de limiter les fausses alarmes, de récupérer les bonnes données afin de déclencher la bonne action. Mais attention, la combinaison de ces deux outils est complexe car ils ne font pas appel aux mêmes technologies. Il faut donc, pour ces fournisseurs de plates-formes aériennes et terrestres, travailler étroitement avec les intégrateurs de solutions afin de définir au mieux, avec eux, la bonne combinaison technique et opérationnelle de ces deux plates-formes, via un hyperviseur de sécurité digne de ce nom. Il faut travailler sur la mise en œuvre cohérente du robot et du drone afin que les informations de l'un profitent à l'autre, et réciproquement, via l'hypervision qui traite ces informations.»

PAROLE D'EXPERT

RENATO CUDICIO
Global Robotics


© DR

« FAIRE DU ROBOT AUTRE CHOSE QU'UN DÉTECTEUR SUR ROUES… »

« Au sein de la société canadienne Global Robotics, nous travaillons sur toutes les applications possibles de l'intelligence artificielle (IA) et son intégration dans des robots dont, évidemment, les robots et autres drones utilisés aujourd'hui et demain dans la sécurité. Le but est de faire en sorte d'intégrer de l'IA aux robots et drones pour en faire autre chose que des simples détecteurs de mouvements mobiles… L'avenir de la robotisation de la sécurité sera dans l'IA embarquée afin de permettre aux robots d'apprendre, d'agir par rapport à la menace identifiée. Tout l'enjeu est de permettre aux robots, à partir de ce qu'ils voient ou détectent, d'interagir avec un environnement complexe. Par exemple, lorsqu'ils rencontrent un être humain afin de limiter, entre autres, les fausses alertes. Il faut donc apporter de la capacité de discernement aux robots terrestres et aux drones pour en faire des outils vraiment utiles aux utilisateurs finaux et pas uniquement une couche supplémentaire de détecteurs, mobiles certes, mais sans réelle valeur ajoutée et se limitant à la réalisation de tâches répétitives. Faire du robot, quel qu'il soit, autre chose qu'un simple détecteur sur roues ou volant… »


© TBC France

Le robot Jack de TBC est capable de surveiller de grands sites industriels. TBC France travaille à y intégrer de l'intelligence artificielle pour lui permettre de reconnaître un être humain, un véhicule, un animal… afin d'alerter, à bon escient, le service de sécurité.

● ● ● *« Nous réfléchissons sérieusement à la collaboration possible entre les robots terrestres et nos drones. Elle a un vrai intérêt opérationnel. Car ce que fait le drone, le robot ne le fera pas obligatoirement. Et réciproquement. »*

Cette complémentarité entre les robots terrestres et les drones est confirmée par Mathilde Bravais : *« Ces outils sont évidemment complémentaires car, qu'il s'agisse du robot terrestre ou du drone, ils ont certaines limites que l'autre solution peut pallier. La vitesse de déplacement du robot terrestre est moins élevée que celle du drone. Mais le robot est capable d'emporter une charge utile plus importante que le drone, pour lequel le poids et l'autonomie sont encore des contraintes réelles. »*

Demain, si les acteurs de la sécurité souhaitent construire une offre globale de surveillance, ils devront sans doute associer robot terrestre et drone. *« La vitesse de déplacement du drone et le fait qu'il fournisse un point de vue en hauteur en font un outil très utile pour des missions de surveillance et d'observation,* reconnaît Stéphane Morelli. *Par contre, il possède une capacité d'emport qui ne lui permet que rarement d'embarquer d'autres charges utiles que celles de ses capteurs, alors que dans certains cas, l'emport d'"effecteurs" serait nécessaire. À l'inverse, le robot terrestre peut plus facilement transporter ces "effecteurs", ainsi que des moyens de détection, d'observation, d'interpellation du ou des intrus… Mais il se déplace beaucoup moins vite que le drone et n'offre pas la même vision de la situation à l'opérateur ou l'agent de sécurité. »*

Une association complexe

Cependant, il ne faut pas croire que la collaboration entre les drones et les robots terrestres ira de soi et se fera facilement. *« La collaboration entre les robots et les drones est en effet une piste que nous devons étudier,* concède Renato Cudicio de Global Robotics. *Faire travailler ensemble des choses complexes est toujours difficile. Si le drone est assez bien maîtrisé aujourd'hui, le robot est plus complexe en soi. »*

Par ailleurs, se pose aussi la question de la plus-value apportée par cette collaboration entre les drones et les robots terrestres. Que va-t-elle permettre de proposer aux utilisateurs finaux ? *« Si on ce contente d'associer des capteurs comme les caméras,* ajoute Renato Cudicio, *cela n'a pas grand intérêt. L'intérêt de la démarche collaborative doit résider, selon moi, dans notre capacité à doter les robots terrestres et les drones d'intelligence artificielle afin de leur permettre d'interagir, entre eux, et avec leur environnement. Pour permettre, par exemple, au robot qui sera*

2 QUESTIONS À

CHRISTOPHE MERLIN — Directeur sûreté Transpole – Keolis-Lille


© DR

À l'ère de l'innovation, du big data et de l'IA, à quoi correspond la sécurité chez Keolis ?

D'une manière générale, la sécurité peut encore être basée sur un très vieux concept d'un humain qui appuie sur un bouton pour ouvrir une barrière et qui, accessoirement, regarde 30 caméras pour voir s'il se passe quelque chose dans le périmètre. Avec l'innovation et l'IA, nous sommes au cœur du projet de la nouvelle DSP de Kéolis-Transpole Lille. Nous allons mettre en place un pilote. Nous avons déjà des caméras intelligentes sur le réseau, ce sont les premières. Nous en avons notamment cinq dédiées à la détection de la fraude sur les portiques de contrôle. Nous développons également le contrôle d'accès dans les sites. Je suis en train d'élaborer un schéma pour protéger les sites de maintenance et de stockage de nos moyens roulants (bus, métros et trams) avec des caméras intelligentes, détecteurs infrarouges et des microprocesseurs pour faire de la détection d'intrusion, de mouvement, du tracking. Le but est que les caméras détectent et alertent tout en mettant du son et de la lumière adaptée en phase d'alerte. Ces caméras vont devenir notre première barrière de vigilance. On va démultiplier ce type de dispositifs également dans le transport, je pense notamment aux bus avec des systèmes de comptage, dans les stations de métro pour faire de la détection de certains mouvements, par exemple des phénomènes de foule, des gens qui courent, tombent dans les escalators, ou qui transportent une planche de surf ou un pistolet mitrailleur... Nous avons décidé de trouver des partenaires internationaux sur le sujet, pour mettre en place des preuves de concept, des POC (Proof of concept), démonstrateurs de faisabilité. On réfléchit en ce moment à la mise en place d'un POC pour la reconnaissance faciale ou biométrique sur l'accès à un local extrêmement sensible et sécurisé.

Vous travaillez aussi sur ce qu'on appelle désormais le cyberguarding...

Nous sommes sur un terreau très fertile dans le domaine, on sait qu'on peut progresser énormément grâce à l'IA couplée toujours à l'humain bien sûr, et qu'on va gagner en efficience face à des phénomènes nouveaux de délinquance, de malveillance, de terrorisme. Cela permet une plus grande facilité de détection en amont, ou de rapidité d'intervention en cas de détection de phénomène. On veut gagner ce temps précieux d e la détection et d'alerte. Pour préparer notre site pilote sous couverture complète en cyberguarding, nous avons réalisé des tests : on a testé des drones attachés à un câble, en position stationnaire ou libres avec des parcours sur GPS avec des bornages et des ballons dirigeables. Il y a encore aujourd'hui trop de contraintes réglementaires et hexogènes pour être totalement efficient. Nous souhaitons aussi également tester des robots patrouilleurs avec Sécuritas qui a fait des démonstrations assez intéressantes au salon de Las Vegas. Certains sites ont jusqu'à 15 km de grillage, donc une patrouille humaine n'est pas capable de tout faire, alors qu'un patrouilleur peut faire une première couche sur un chemin de ronde, et avec une caméra qui peut aller chercher les événements. Nous ne sommes pas pour un remplacement de l'humain par la technologie mais dans une complémentarité de ressources qui permet à la fois d'accroître la couverture et de gagner du temps. Nous ne pouvons être tributaire d'un seul moyen. Si une panne technologique est détectée, nous devenons vulnérables. Notre action et notre stratégie répondent à une logique de complémentarité. Nous avons déjà testé dans les agences commerciales des robots pour renseigner et orienter les usagers. L'ensemble pourra être couplé à la caméra intelligente avec microprocesseurs, pour nous aider à améliorer la protection du terrain, la rapidité de détection et d'intervention.

***Interview** réalisé par Stéphane Gérard, Labo Créatif, dans le cadre d'AccesSecurity*

amené à rencontrer un humain d'interagir avec le langage naturel, de parler avec l'individu, de lui demander un mot de passe, un code... C'est-à-dire de travailler dans un environnement complexe. Et le drone devra aussi être capable de cela. » Avant de poursuivre : « *Sans cette capacité d'interaction avec leur environnement, les robots et les drones, associés ou pas, se contenteront d'êtres des machines assez efficaces pour effectuer des tâches répétitives, dans un environnement contrôlé. Est-ce réellement ce qu'attendent les utilisateurs de ce type de solutions ?* »

Une fois tout cela dit, une question demeure : qu'elle sera la place de l'homme dans tout ça. « *La situation actuelle du marché de la sécurité n'est pas satisfaisante. Les prestations de surveillance ne se caractérisent pas toujours, loin de là, par une véritable plus-value opérationnelle et sont pénalisées par un modèle économique exangue. Les drones et les robots s'imposeront car ils apportent une réponse à cette situation insatisfaisante pour toutes les parties : prestataires et donneurs d'ordres. Ils vont permettre d'accroître la qualité des prestations, leur efficacité... Les agents de sécurité se verront alors proposer des missions plus valorisantes* », conclut Stéphane Morelli. ■

PAROLE D'EXPERT

SERVAN LÉPINE
Président d'Excelium


© DR

« SORTIR DE LA LOGIQUE D'EMPILEMENT DES MOYENS TECHNO. »

« Les drones et les robots sont totalement complémentaires. Les drones jouissent d'une efficacité de déplacement importante mais sont soumis aux contraintes météo, par exemple. Le robot terrestre, quant à lui, bénéficie d'une plus grande facilité d'utilisation mais pâtit d'une vitesse de déplacement inférieure à celle du drone. En matière de robotisation de la sécurité, il faut sortir de la logique de l'empilement des différents moyens technologiques. On doit plutôt se concentrer sur les moyens de les faire travailler ensemble. On doit leur donner les moyens de communiquer entre eux, de remonter de l'information et de se "l'échanger". Mettre en place un modèle reposant sur la logique d'asservissement : je reçois une info, du drone ou du robot, et le robot ou le drone déclenche une action. »

Le CMSI joue un rôle primordial dans la lutte contre le feu. Il est demandé dans la plupart des ERP.

© Défense92

Le CMSI : élément central et incontournable !

Élément primordial de la sécurité incendie telle qu'on la conçoit en France, le CMSI a fait la preuve, depuis de longues années, de son efficacité dans la lutte contre l'incendie.

En France, la réglementation incendie impose dans la majorité des ERP l'installation d'un centralisateur de mise en sécurité incendie ou CMSI. *« Il s'agit,* comme l'explique Franck Lorgery, président du Gesi, un des groupements de la FFMI, *d'un équipement principal dans la mise en sécurité incendie, souvent relié à un système de détection incendie (SDI), l'ensemble constitue ce qu'on appelle un système de sécurité incendie de catégorie A ou SSI. »* Dans cette configuration, le CMSI reçoit du SDI les informations de la détection automatique d'incendie comportant l'identification de la zone sinistrée. *« Une fois ces informations reçues,* ajoute le président du Gesi, *le CMSI active automatiquement, suivant un scénario prédéfini, les actions à effectuer, entre autre, il actionne les dispositifs actionnés de sécurité (DAS) et les solutions permettant d'assurer l'évacuation des personnes du bâtiment. »*

Sécuriser le bâtiment

Les dispositifs actionnés par le CMSI permettent donc de mettre en sécurité le bâtiment selon les règles suivantes :

- compartimentage : cette fonction a pour objectif de faire obstacle à la propagation du feu (exemples de DAS : porte coupe-feu, clapet coupe-feu) ;

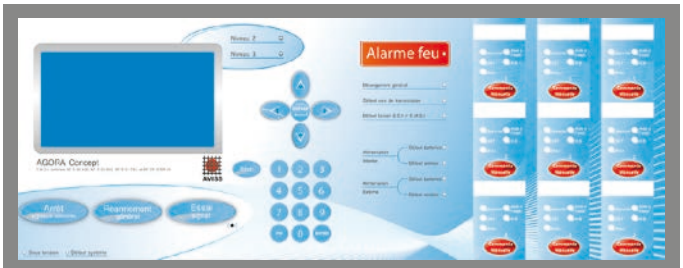
DU CÔTÉ DU GESI

FRANCK LORGERY
Président du Gesi


© DR

« LE CMSI PERMET DE GAGNER DU TEMPS. »

« La démarche française en matière de sécurité incendie, et plus particulièrement en ce qui concerne le CMSI, permet de gagner du temps. Par ailleurs, il faut souligner qu'on demande, impérativement, au CMSI de toujours fonctionner et d'être disponible. Même si on lui autorise de perdre une fonction, et une seule… Perte qui ne doit en aucun cas affecter son fonctionnement de base et la gestion des autres zones. Il doit donc toujours être opérationnel. Par conséquent, l'innovation technique ne doit pas se faire au détriment de cet impératif fonctionnel. On ne doit donc pas toucher au cœur du CMSI. Il est préférable que l'innovation se situe à la marge, autour du CMSI lui-même : par exemple sur les tableaux de report, gestion de graphiques, aide à l'exploitation… afin, qu'en cas de problème technique sur les périphériques, le CMSI reste toujours disponible et en état d'assurer sa mission. Par ailleurs, il ne faut pas oublier de s'assurer du bon fonctionnement du CMSI. On doit donc surveiller les lignes de communications entre les différents éléments du SSI, les tester et les maintenir. Il faut aussi vérifier une fois par jour le bon fonctionnement de la signalisation en face-avant. Enfin, comme beaucoup "d'objets", les CMSI peuvent renvoyer des informations vers des réseaux informatiques. Ils doivent donc se protéger si besoin contre les défaillances réseaux et les éventuelles cyberattaques. Nous y travaillons actuellement au sein du Gesi, en collaboration étroite avec le CNPP et l'Anssi. »



© Aviss

Aviss
Son CMSI Agora Concept conjugue technologie et économie. Il est intégralement adressable et peut gérer jusqu'à 256 fonctions/zones de mise en sécurité, 1024 DAS et 2048 DCT. Son architecture de puissance « intelligente » permet un gain économique substantiel, avec un impact sur la quantité de cuivre consommée par la réduction significative du nombre de câbles, de leur section et linéaire. La conception de son architecture peut permettre de s'affranchir de VTP avec des matériels déportés discrets. Matériel déporté universel, il permet le raccordement de tous types de DAS et matériels de diffusion du signal d'évacuation. Par ailleurs, il s'adapte à l'évolution d'utilisation de l'établissement sans impact notoire sur l'architecture déployée.

- désenfumage qui assure l'évacuation des fumées afin que les personnes ne soient pas asphyxiées (exemple de DAS : volet de désenfumage, coffret pour ventilateur d'extraction et de soufflage) ;
- évacuation : fonction qui signale aux occupants du bâtiment qu'il faut évacuer rapidement (exemple : diffuseurs sonores et lumineux) ;
- commandes d'équipements techniques : la commande de ces équipements (exemple : arrêt climatisation, non arrêt des ascenseurs au niveau de la zone sinistrée, remise en lumière) permet de garantir l'évacuation des personnes.

Élément central de la sécurité incendie

On le comprendra aisément : compte tenu de son rôle, le CMSI est un élément principal de la sécurité incendie. Ce que confirme Régis Cousin, président de la FFMI : *« Le CMSI est une spécificité française. Il constitue la pierre angulaire de la sécurité incendie telle que nous la concevons en France. Il est au cœur du concept même de la sécurité incendie "à la française". »*

« Le CMSI, ajoute Franck Lorgery, *était extrêmement*

UN CMSI : QU'EST-CE QUE C'EST ?

→ CMSI

Le CMSI est un ensemble de dispositifs qui permet, à partir d'informations de détection incendie ou d'ordres de commande manuelle, d'émettre des ordres électriques de commande des matériels assurant les fonctions nécessaires à la mise en sécurité d'un bâtiment ou d'un établissement en cas d'incendie : le compartimentage, le désenfumage et l'évacuation. Il se compose en général d'une unité de signalisation ou US, d'une unité de gestion d'alarme ou UGA, d'une unité de commande manuelle centralisée ou UCMC. Il peut comporter aussi une unité de gestion des issues de secours ou UGIS.

→ US

L'US assure la signalisation des informations nécessaires pour la conduite du système de mise en sécurité incendie ou SMSI.

→ UGA

L'UGA collecte les informations en provenance de déclencheurs manuels (DM) ou du système de détection incendie (SDI), les gère et déclenche le processus d'alarme.

→ UCMC

L'UCMC émet des ordres de télécommande par fonction et par zone à destination des DAS, par exemple. On regroupe en général sous la dénomination DAS les clapets et portes résistant au feu, les exutoires de fumées, les ouvrants de façade, les volets, les coffrets de relayage, les dispositifs de déverrouillage pour issues de secours.

2 QUESTIONS À

DAVID BERTRAND

Responsable équipe technico-commerciale et projets France Cooper Sécurité (Groupe Eaton)


© DR

Quel est l'intérêt du CMSI ?

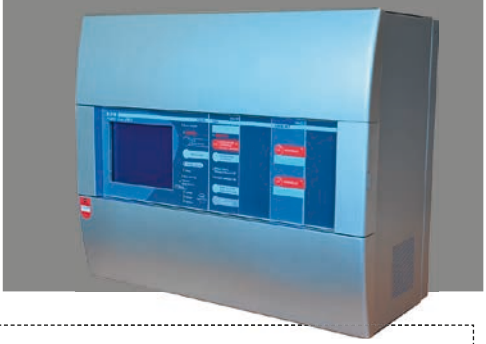
Élément central de la sécurité incendie, il permet d'agir de deux manières différentes en cas de départ de feu dans un ERP. De manière automatique d'une part. Il actionne les dispositifs constituant le SSI afin de mettre en sécurité le bâtiment et permettre l'évacuation du site. D'autre part, on peut intervenir manuellement sur le CMSI pour, là encore, déclencher certaines actions de mise en sécurité.

Les CMSI sont très encadrés et normés. On ne fait pas ce qu'on veut pour les concevoir. Dans ces conditions, comment peut-on innover ?

L'innovation est en effet très contrainte en matière de CMSI. Mais elle n'est pas impossible. Par exemple, nous avons lancé il y a quelques années, une gamme de CMSI dotés d'un écran tactile fournissant des informations complémentaires au responsable d'établissement : maintenance et son historique, aide à l'exploitation, à la programmation de premier niveau… L'innovation concerne donc principalement les outils d'aide à l'utilisation et à la maintenance. On peut aussi innover pour les câblages ou sur les bus de communication. L'innovation doit se limiter à la périphérie du système afin de ne pas nuire à son fonctionnement et à son appropriation par ses différents utilisateurs.

Eaton

La gamme Sensea regroupe les fonctions de détection incendie et de mise en sécurité en deux centrales principales (Sensea.EC et Sensea.CM) dans le plus strict respect des exigences réglementaires et normatives. Par exemple, le CMSI de type B à boucles adressables avec UGA et 2 lignes à Manque de Tension équipé d'un écran tactile. Le CMSI de type B Sensea.CM B a été conçu spécifiquement pour les bâtiments de taille petite à moyenne nécessitant un SSI de type B avec des boucles de détection manuelle adressable. L'unité de gestion d'alarme intégrée (UGA 2) permet de gérer l'évacuation d'une zone d'alarme. Le CMSI à 2 lignes à Manque de Tension (2MT) permet de gérer deux zones de mise en sécurité.


© Eaton


© DR

« Le CMSI est une spécificité française. Il constitue la pierre angulaire de la sécurité incendie telle que nous la concevons en France. »

RÉGIS COUSIN, PRÉSIDENT DE LA FFMI

● ● ● *en avance sur son temps car il permet de mettre, de manière automatique, le bâtiment en sécurité d'après les informations issues de la détection incendie. Grâce à ce système, on n'attend pas que l'être humain mette en sécurité le bâtiment. Le système le fait automatiquement. Les actions déclenchées sont signalées sur le CMSI. Ainsi, lors de leur intervention, les secours peuvent savoir comment évolue le feu et quels sont les problèmes éventuels. »*

Grâce au CMSI, le pompier a à sa disposition des commandes manuelles dans un lieu unique et peut gérer la sécurité du bâtiment, en l'adaptant aux nécessités de l'intervention des secours. Le CMSI a fait la preuve de son efficacité. Et, bien que spécificité française, d'autres pays ont été convaincus de son intérêt. *« Ainsi, en Suisse, Belgique ou au Luxembourg, des CMSI sont installés dans certaines installations à hauts risques ou, en Afrique du Nord, dans de grands hôtels »*, précise Franck Lorgery.

Dans les autres pays, les alarmes sont directement reliées aux postes des pompiers. Ce sont eux qui interviennent, décident de ce qu'il faut faire et se chargent de la mise en sécurité du bâtiment et de lutter contre le feu. En France, c'est le chef d'établissement qui est responsable de la phase de mise en sécurité. La raison d'être du CMSI est de l'y aider.

LE POINT DE VUE D'UN FABRICANT

MANUEL PINHEIRO

Responsable produits détection chez Tyco Johnson Controls


© DR

« NOUS AVONS LANCÉ RÉCEMMENT UN NOUVEAU CONCEPT DE TRE. »

« Chez Johnson Controls, nous avons situé l'innovation au sein même du terrain en privilégiant les outils de mise en service et de maintenance mais aussi l'exploitation distante des informations. Ainsi, associé à notre CMSI ZXA nous proposons notre 850EMT, un outil d'aide à la mise en service à distance qui permet de simplifier et accélérer l'installation du CMSI associé à des modules déportés configurables en fonction des besoins de chaque zone de sécurité. Par ailleurs, et ce en conformité avec la dernière norme NF S61-94, nous avons lancé un nouveau produit le PR1DF: un tableau répétiteur d'exploitation (TRE) qui permet, comme la réglementation l'exige, de maintenir sous surveillance humaine permanente un CMSI lorsque celui-ci n'est pas toujours visible des personnels de sécurité sur site. Notre solution se caractérise par un TRE unique ECS & CMSI disposant d'un écran tactile couleur dont la couleur de fond varie en fonction des informations : rouge pour une alarme, jaune pour un dérangement. »

La même chose pour tout le monde

« L'intérêt du CMSI, explique David Bertrand, responsable équipe technico-commercial et projets France Cooper Sécurité (Groupe Eaton), *repose donc sur un concept de départ assez simple : mettre à disposition de toute personne habilitée – chefs d'établissements, pompiers, etc. – un système que tout le monde puisse comprendre, avec les mêmes informations, quelle que soit la marque du CMSI, afin de faciliter le travail des secours et des pompiers. De ce fait, l'interface homme/machine est assez figée. Afin de ne pas faire perdre du temps aux pompiers. »*

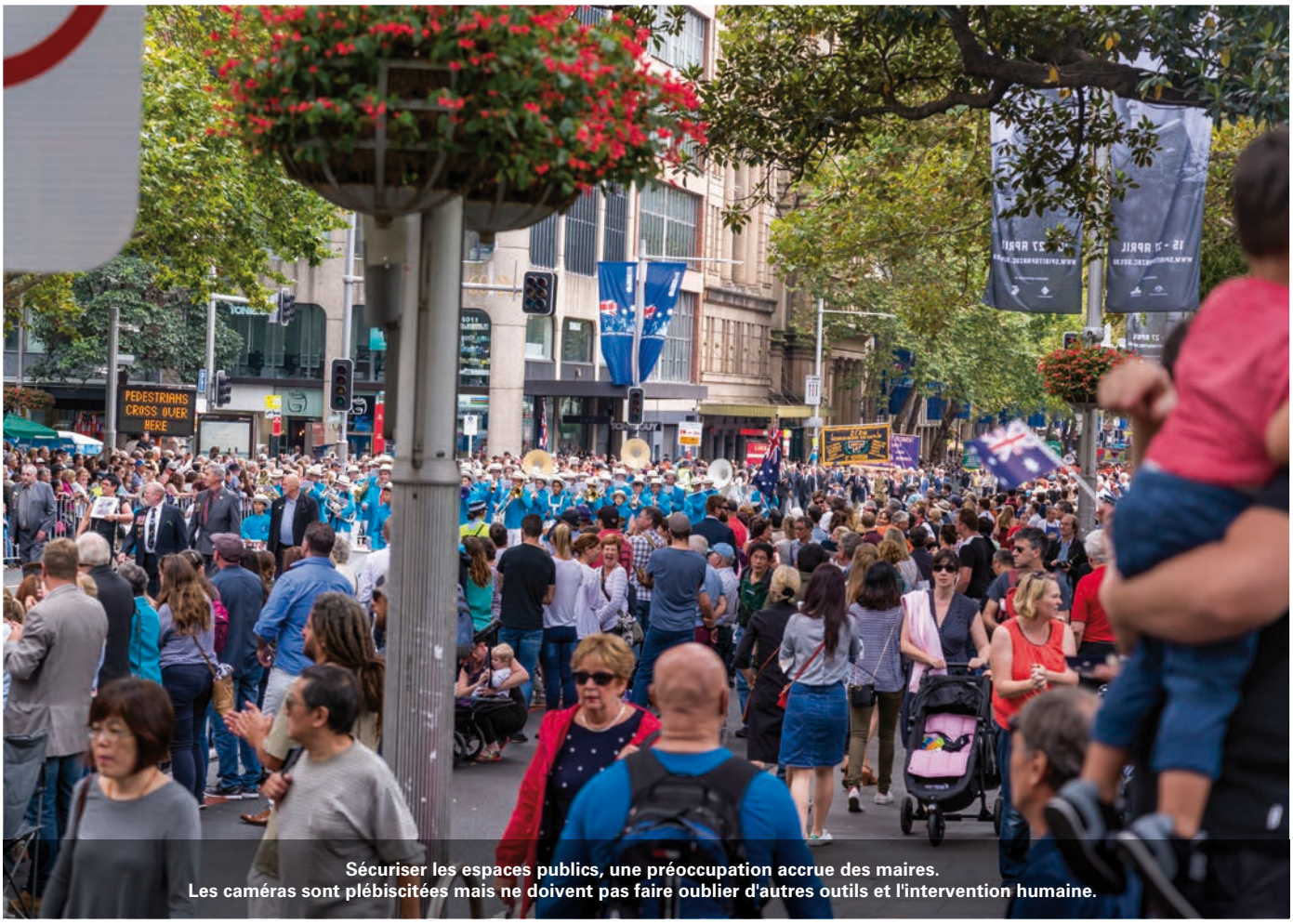
En effet, la norme, en l'occurrence les NFS 61 930 à NFS 61 940, a défini les caractéristiques principales du CMSI. Et impose certaines limitations : 256 fonctions maximum, gestion de 1 024 DAS maximum (portes coupe-feu, volets, trappes, etc.), gestion de 2 048 dispositifs de commande terminal maximum. Cette limitation de la capacité d'un CMSI peut amener, lors de la mise en œuvre, l'emploi de plusieurs CMSI sur un même site. *« Les normes ont donc fixé ce qu'on est en droit d'attentre d'un CMSI et de la gestion des défauts, de sa performance »*, insiste le président du Gesi.

Un CMSI doit donc comporter une face avant afin de permettre son exploitation. Face avant qui comporte les boutons de commandes manuelles pour effectuer une mise en sécurité du bâtiment sous décision humaine. Elle intègre aussi tous les voyants permettant de lire l'état des différents organes commandés.

« Cette volonté de normaliser l'ensemble se comprend aisément, ajoute le président du Gesi. *Si les informations, d'un CMSI à l'autre, d'un site à l'autre, différaient, les pompiers ou les personnes en charge de la première intervention sur le feu, risqueraient de perdre un temps précieux à décrypter et comprendre ce qu'il y a en face d'eux. C'est aussi simple que ça. Et ça marche… »*

© Siemens

Siemens
Le centralisateur de mise en sécurité incendie STT20 offre une architecture très flexible et modulaire. Il est constitué d'un matériel central (MC20) et de matériels déportés (MD20 – classe AC1 et MEA20xx – classe AC2) permettant la gestion de dispositifs actionnés de sécurité (DAS) et de commandes terminaux (DCT). Le matériel central (MC20) peut gérer 16 matériels déportés (MD20) qui eux-mêmes permettent de gérer sur chacune des 2 voies de transmission rebouclées, jusqu'à 32 modules électroniques adressables (MEA). La liaison MC20/MD20 s'effectue par deux voies de transmission distinctes d'une longueur maximale chacune de 1 200 mètres, assurant la disponibilité du système.



Sécuriser les espaces publics, une préoccupation accrue des maires. Les caméras sont plébiscitées mais ne doivent pas faire oublier d'autres outils et l'intervention humaine.

© Getty Images

Espace public sous l'œil des caméras

Équiper l'espace public de caméras ne fait aujourd'hui plus débat et la vidéo s'insère naturellement dans le paysage urbain. Toutefois, de simples caméras ne suffisent pas à prévenir les actes délictueux ou malveillants. La sécurisation de l'espace public passe aussi par les hommes et un aménagement judicieux de l'espace pour réduire les risques.

L'espace public est sous-tension. Les récents événements l'ont rappelé, la sécurisation de l'espace public est devenue une priorité des élus et des pouvoirs locaux, et ceux-ci se tournent naturellement vers la vidéoprotection. Si cette dernière est un outil remarquable, ce n'est qu'un outil. Comme le souligne Dominique Legrand, président de l'AN2V, *« les maires sont submergés par leurs tâches, et bien souvent ne prennent pas le temps de s'arrêter sur leurs besoins en vidéo. Nous essayons de leur apporter du conseil et sommes à leur disposition pour les aider, mais les élus manquent de temps pour s'approprier un sujet essentiel. Or la mise en place de la vidéo doit être l'aboutissement d'une réflexion complète menée sur la ville, ses objectifs en matière de sécurité, si on veut de l'efficacité. »*

Même constat, chez Pascal Bouvignies, Business Development Manager chez Bosch Security : *« Les collectivités locales se répartissent en deux catégories : ceux qui ont déjà de la vidéo et ont pu en tester les avantages, les contraintes et les limites. Pour ceux-là nous pouvons dialoguer sur des éléments concrets, et ils perçoivent ce que peut apporter nos systèmes d'analyse de la métadonnée. En*

revanche les "primo-accédants", souvent de plus petites communes, sont peu informés et il faut vraiment les accompagner dans la mise en place. Pour les petites villes qui souhaite s'équiper de 15 à 32 caméras, nous fournissons un VMS de façon à harmoniser l'équipement. Nous alertons aussi souvent les collectivités sur la pérennité de solutions comprenant un mix de matériels et logiciels : le risque est de perdre le savoir-faire lorsque les personnes partent. La pérennité d'une solution passe par les entreprises qui peuvent suivre le parc et les systèmes et assurer le suivi en cas d'évolution technologique, législative ou autre. »

Des hommes derrière les écrans

La vidéo a conquis les villes mais l'exploitation des images, notamment en direct, reste un sujet brûlant. L'intelligence artificielle vient au secours de ceux qui sont chargés de la visionner. *« En 2019, toutes nos caméras bénéficieront d'un système d'intelligence artificielle embarquée. Soit Essential Video Analytic soit Intelligent Video Analytic avec un processeur dédié,* indique Pascal Bouvignies. *La caméra va transmettre en temps réel des images et leur interprétation. Par exemple, nos caméras sont en mesure de trier les objets en fonction de leur forme, taille, couleur, et grâce au flux de métadonnées de donner l'interprétation immédiate et de lever des alertes sur la base de scénarios prédéterminés : véhicule circulant à contresens ou dans un espace piétons, personne à terre et immobile, attroupement, objet abandonné… »* Encore faut-il que ces alarmes soient traitées. C'est aujourd'hui là que le bât blesse pour Dominique Legrand de l'AN2V qui note la faible conver-

SOLUTIONS

UN RALENTISSEUR ANTI-INTRUSION POUR SÉCURISER LES ÉVÉNEMENTS

© © ville de Caspestang

Dalitub propose une solution brevetée innovante, entièrement conçue et fabriquée en France : le ralentisseur anti-intrusion. Cet équipement modulaire ferme et sécurise tous types de voies. En position haute, il constitue un obstacle infranchissable pour les véhicules de taille moyenne (résistance au choc d'un véhicule bélier de 7,5 tonnes lancé à 48 km/h). En position basse, il fait fonction de ralentisseur. Les positions actives et inactives sont sécurisées par un système de verrouillage, et le passage de l'une à l'autre est très rapide. Sans entretien, ce dispositif s'installe et se retire facilement et peut aussi être implanté de manière permanente grâce à des points d'ancrage. Une solution qui trouve sa place pour sécuriser les accès de marchés et manifestations locales.

3 QUESTIONS À

FRANCK DENION

Coordonnateur - correspondant agglomération justice, Melun-Val de Seine

© DR

En termes de sécurité de l'espace public, quelles sont vos préoccupations sur votre communauté d'agglomération ?

Située à 25 minutes de Paris, la communauté de Melun-Val de Seine compte 130 000 habitants et couvre vingt communes de 235 à 40 000 habitants, avec une très grande disparité de besoins et de moyens, mais aussi des préoccupations identiques. Le conseil intercommunal de sécurité et de prévention de la délinquance intervient essentiellement comme conseil auprès des maires dans la conception de projets, pour tout ce qui concerne la vidéoprotection pour laquelle la demande est de plus en plus forte, mais aussi sur l'ensemble des questions liées à la sécurité publique et à la prévention de la délinquance.

Comment intervenez-vous pour la vidéoprotection ?

Les maires restent maîtres dans le positionnement des caméras et conservent leurs pouvoirs de police, mais nous intervenons comme conseil sur le type de vidéo : surveillance, élucidation, placement, nombres… Par exemple, sur les dépôts sauvages en milieu rural, nous avons orienté les maires vers des solutions de « photo-piège », déjà utilisés par l'ONF pour la surveillance du gibier et la prévention du braconnage. Ces dispositifs ne se déclenchent qu'au passage et présente l'avantage d'avoir des modalités réglementaires d'installation très allégées par rapport à la vidéo. À ce jour, nous n'avons pas de centre urbain intercommunal (CSUI), mais mutualiser les images et leur exploitation pourrait devenir un projet à terme, la vidéo prenant une place de plus importante dans la mise en sûreté et sécurité des espaces publics.

Quels autres dispositifs avez-vous mis en place ?

C'est très varié. L'idée est de s'adapter aux demandes des communes dans tout ce qui touche à la sécurité du territoire. Pour ne vous citer que quelques-unes de nos 29 actions concrètes, avec les bailleurs sociaux, nous avons organisé la mise à disposition pour chaque policier d'un badge Vigik personnel qui lui permet d'entrer dans tous les halls d'immeubles et parties communes des habitats collectifs de l'intercommunalité. Nous sommes également conseil en application numérique : nous aidons les mairies à diffuser auprès de leurs administrés une application d'évaluation comme « Cambrio Liste » sur le taux de « cambriolité ». Nous travaillons également pour les maires sur un logiciel de traitement du plan intercommunal de sauvegarde, avec visualisation en temps réel des moyens disponibles sur tout le territoire. Nous sommes partie prenante du DU de sécurité publique avec l'université de Créteil, qui a pour objectif de préparer les jeunes peu favorisés aux concours de la fonction publique : gardien de la paix, policier municipal… Enfin, nous sommes en train de mettre en place un réseau de correspondants locaux de prévention de proximité dont le rôle va être de décharger les référents sûreté de la police nationale et gendarmerie pour la réalisation de premières « Études de sûreté et sécurité publiques » à destination des maires.

PAROLE D'EXPERT

DOMINIQUE LEGRAND
Président de l'AN2V


© LA

« LA VIDÉO EST UN OUTIL PUISSANT MAIS IL FAUT LEVER LES FREINS À SON EXPLOITATION. »

« Depuis 2004, l'AN2V s'est donné pour mission de conseiller et de former à l'usage de la vidéo. Nous encourageons les élus à venir nous rencontrer afin de mieux comprendre les capacités de la vidéo et ce que l'on peut en attendre au regard de leur problématique locale. La réponse ne sera pas la même face à des cambriolages, des agressions ou des dégradations, ni selon les budgets, ou si le maire dispose d'une police municipale, de centre de surveillance... Pour aider à définir leur besoin, nous avons développé une méthodologie autour de six axes. Trois axes principaux recouvrent la stratégie (quel est l'objectif ?), l'organisation (qui fait quoi ?) et la technique (caméra, réseau, stockage, etc.). Les trois axes transverses s'articulent autour des cadres juridiques (quelle législation et suis-je en conformité ?), des coûts globaux et de l'éthique. Lorsque les six éléments sont bien établis, alors on peut passer à une seconde phase de définition de l'implantation de la vidéo, en gardant à l'esprit que la réponse technique ne sera pas la même pour des caméras de dissuasion, de protection ou d'élucidation. La demande du citoyen se porte de plus en plus vers une vidéoprotection avec retour d'action très rapide. C'est probablement la plus complexe et la plus coûteuse. Il faut avoir les outils et les hommes pour détecter, transmettre, analyser et intervenir le plus rapidement possible. À cet effet, dans notre manifeste pour une efficience, nous plaidons – entre autres – pour améliorer la convergence entre télésurveilleurs, polices municipales et forces de l'ordre. »

● ● ● gence entre télésurveilleurs, polices municipales et forces de l'ordre, qui est une entrave à l'efficacité de la réponse face à un acte répréhensible.

Des caméras sécurisées

Des caméras qui sécurisent, mais qui doivent également être sécurisées. *« 2017 a été une année néfaste, en ce qui concerne la sécurité des caméras dans le monde*, indique Pascal Bouvignies, Business de Bosch Security Systems. *De nombreux hackers ont profité de protection insuffisante des caméras dans l'espace public pour mener des attaques sur des serveurs et les saturer. Aujourd'hui, c'est un risque qu'un fabricant ne peut ignorer. Nous avons de décidé de définitivement supprimer les mots de passe sur l'ensemble de nos caméras. De même, pour tous les outils type Telnet, UNP qui sont* ● ● ●

SITES À RISQUES

Un réseau de sirènes pour alerter la population dans la vallée de la Seine

Comment prévenir simultanément l'ensemble des salariés d'un site et toute la population de l'imminence d'un danger dans une zone comprenant 12 sites Seveso et neuf communes ? Depuis plus de quarante ans, ae&t, spécialiste des solutions d'alerte, d'évacuation et de communication dans le cadre de risques majeurs, propose une gamme de sirènes d'alerte pour la gestion de la sécurité publique, notamment dans le cadre du PPI (plan particulier d'intervention). *« Nous avons été consultés dans le cadre du renouvellement du réseau d'alerte sonore,* explique François Peyroutet, chef de produit chez ae&t. *Il s'agissait de couvrir toute une zone comprenant douze établissements Seveso sur neuf communes de Caux vallée de Seine et Port-Jérôme, soit plus de 25 000 habitants. Forts de notre connaissance des solutions industrielles, nous avons conçu et déployé une solution globale d'alerte sonore en réseau. Ce réseau permet au niveau de chaque mât, de diffuser à la population le signal national d'alerte. La modularité d'un tel système peut également permettre la diffusion de messages voix, préenregistrés ou créés en direct afin de s'adapter à toutes situations d'urgence (évacuation, confinement, point de regroupement, etc.). Il s'agit d'une vraie personnalisation de l'alerte face aux risques. C'est aussi une installation prévue pour fonctionner en cas de situation dégradée : système en réseau numérique 100 % sécurisé en 3G avec VPN et réseau radio VHF, redondance des communications entre les équipements, déclenchement individuel des sirènes par téléphone filaire... Même après une coupure de secteur de 72 heures, le déclenchement d'alerte est toujours possible grâce à des batteries. »* Cette installation s'inscrit dans un partenariat novateur de gestion de la sécurité publique entre la communauté d'agglomération, les villes et les entreprises du secteur.


Les sirènes – du réseau d'alerte de Port-Jérôme conçu, fabriqué et mis en service par ae&t avec Spie comme installateur – peuvent être utilisées pour tout type d'accidents majeurs technologiques ou naturels.
© ae&t

3 QUESTIONS À

GUILLAUME VEUX

Directeur prévention sécurité de la communauté d'agglomération Grand Paris Sud

© DR

Comment s'organise la prévention sécurité dans la communauté Grand Paris Sud ?

La communauté d'agglomération Grand Paris Sud compte 356 000 habitants répartis sur vingt-quatre communes de taille très variable. Cela va de la commune rurale de 500 habitants à des zones de sécurité prioritaire Les Tarterets, la Grande Borne et Savigny-le-Temple, en passant par des villes de moyenne importance. Cela signifie des typologies de délinquance très différentes. La communauté d'agglomération a compétence sur trois centres de supervision urbains intercommunaux. Nous travaillons avec des observatoires de la sécurité de manière locale. L'objectif est de faire des analyses statistiques régulières des phénomènes recensés par territoire et de pouvoir apporter une réponse rapide. Le format que nous avons mis en place – des cellules de veille par thématique qui peuvent s'activer si besoin permet d'être réactif. Dès qu'un problème est soulevé par un élu ou un administré, aussi varié soit-il (dépôts sauvages, zone de prostitution, radicalisation, nuisance sonore, rodéo deux roues, etc.), nous sommes en capacité de déployer le réseau. Nous montons une cellule qui va rechercher une solution adaptée à la situation et mettre en place un plan d'action avec les forces présentes, police ou gendarmerie mais aussi les transporteurs, les bailleurs ou les médiateurs et l'administration judiciaire.

Qu'apportent les trois CSU ?

Les centres de supervision sont un support opérationnel à disposition des élus et des forces de l'ordre pour la transmission d'image. Sur la CA GPS nous avons 506 caméras. La CA met en place le réseau dans lequel toute commune peut se rattacher, et met à disposition des opérateurs. Aujourd'hui, nous sommes une plus-value pour les communes qui souhaite se raccorder : nous pouvons apporter notre expertise, sur le type de caméra (jour/nuit) leur implantation etc... Nous expérimentons aussi de nouvelles solutions. Par exemple, nous sommes en train de tester des solutions d'analyse vidéo.

Comment évaluez-vous l'efficacité de la vidéoprotection ?

La vidéoprotection dans l'espace public semble être incontournable et on peut mesurer son efficacité. Par exemple, sur les parkings communaux à proximité des gares, on a vu le nombre de faits délictueux, essentiellement les vols à la roulotte baisser de 35 à 45 %. C'est aussi flagrant avec les points de trafics de stupéfiants qui se déplacent dès que la vidéo est installée. La vidéo ne résout pas le problème, mais c'est un outil qui aide à l'identifier et c'est au pouvoir régalien (police, gendarmerie) de passer à l'action. Il faut aussi se garder de tout miser sur la vidéo : la sécurité de l'espace public repose aussi sur une coordination et des échanges entre tous les acteurs de la sécurité publique.

susceptibles d'être utilisés par les hackers pour installer des malwares. L'installation de tout logiciel tierce, non validé par Bosch est désormais interdite. Chaque caméra est équipée d'un coffre-fort électronique qui va permettre de sauvegarder les certificats de communication de cryptage pour dialoguer entre la caméra et le poste central. Non clonable, chaque caméra bénéficie d'un certificat unique. La sécurité des caméras devient un enjeu de sécurité publique, dans la mesure où le bon fonctionnement des caméras est indispensable pour enclencher une réponse appropriée.»

Aménager l'espace

Les caméras ne font pas tout. Les véhicules bélier, depuis les attentats de Nice et Berlin, sont devenus la hantise des maires. De nombreuses fabricants proposent des solutions fixes ou amovibles de barrières anti-intrusions, pour équiper des places publiques dévolues aux piétons. Pour Guillaume Veux, de la communauté d'agglomération de Grand Paris Sud, *«La sécurité dans l'espace public ne se limite pas à la vidéoprotection. Je rencontre les maîtres d'œuvre et les urbanistes pour les sensibiliser au mobilier urbain et à l'aménagement de l'espace pour améliorer la sécurité. Des bornes anti-véhicules béliers peuvent être design et placées de façon à protéger des espaces. De même pour l'éclairage, en installant des éclairages qui se déclenche au passage on peut arriver à concilier la volonté de développement durable (économie d'énergie et lutte contre la pollution lumineuse) et la demande sécurité du tout éclairé.»*

SOLUTIONS

SOUND-SCANNER, ET LES CAMÉRAS ENTENDENT


© DSensivic

Le Sound-scanner de Sensivic est un détecteur automatique directionnel d'anormalités sonores dans un rayon de 40 m. Équipé d'un système de prise de son intégré, il analyse en permanence l'activité sonore habituelle du site où il a été placé. Il peut alors détecter les événements sonores inhabituels et les signaler par une notification à un logiciel de vidéprotection. Grâce à son système d'apprentissage, le Sound-scanner s'adapte automatiquement aux variations de l'ambiance sonore (jour/nuit, heures de pointes, travaux...). Il détermine également la direction d'où provient le son anormal. Il s'interface à travers un réseau IP et en cas de chocs sonores, il peut déclencher des scripts tels que, orienter la ou les caméras vers la source de bruit, ouvrir ou fermer des barrières, allumer ou éteindre des lampadaires d'éclairage public... Avec le Sound-scanner, les caméras mobiles regardent la bonne scène au bon moment et le travail des téléopérateurs ou des enquêteurs est facilité.

DRONES

Avec son drone filaire, Elistair participe à la sécurisation du concert d'Orelsan

Pour assurer la sécurité des équipes organisatrices, des fans et des artistes lors du concert d'Orelsan, le 30 novembre dernier, la société de services par drones Adéole et la Ville de Floirac (33) ont décidé d'expérimenter une nouvelle forme de vidéosurveillance de la voie publique : un drone DJI Matrice 200, avec caméra Zenmuse Z30 full HD, relié à la station filaire Ligh-T v3 d'Elistair. Ainsi, connecté au sol par un micro-fil d'alimentation, le petit aéronef a survolé la zone pendant plusieurs heures avant, pendant, et après le concert sans rupture d'énergie. Accès, entrées, sorties, routes, flux de personnes et de véhicules… grâce à l'engin, les équipes de sécurité ont pu contrôler en continu une zone d'1,5km de rayon.


Le drone filaire parfaitement adapté à la surveillance d'événements en zone urbaine, de jour comme de nuit.
© Elistair

«Cette mission avait pour objectif la décongestion du flux de circulation avant et après le concert d'Orelsan à l'Arkéa Bordeaux Arena situé à Floirac (33). Nous avons effectué un vol de 2h45 avant le concert et 1h après le concert avec le système filaire d'Elistair. Cette innovation nous a permis d'augmenter considérablement notre durée de vol ! Les vols ont été réalisés à une hauteur maximale de 50 m permettant d'appréhender l'ensemble des axes de circulation proches du site», commente Alexandre Auger, CEO d'Adéole.

Une sécurité renforcée pour le grand public. Directement communiquées au poste de sécurité, les images de vidéosurveillance ont permis une gestion instantanée des informations et une prise de décision rapide, selon les situations. *«Notre objectif était d'assister la police municipale de la Ville de Floirac dans la décongestion du flux de circulation. L'utilisation de ce drone filaire a aiguillé les agents de police sur place et réduit les difficultés de circulation de 45 minutes. De plus, grâce à ce système, nous avons pu retrouver une personne recherchée pour état d'ivresse sur la voie publique»*, ajoute Alexandre Auger.

Conçue pour des conditions d'utilisation ultra-exigeantes, cette station est utilisable de jour comme de nuit et assure des vols sûrs, parfaitement adaptés, entre autres, à des déploiements en zone urbaine à proximité d'infrastructures et de public.

Depuis 60 ans, le Réseau DEF, réseau international et indépendant d'entreprises expertes en sécurité incendie, est un acteur majeur sur le marché européen. À travers ses entreprises aux expertises complémentaires, il propose une offre complète dans le secteur des Systèmes de Sécurité Incendie et fournit des produits et services pour des projets de toute complexité.

reseaudef

reseaudef.com

Guide ANNUEL d'Achat

www.protectionsecurite-magazine.fr

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

e-salon-protectionsecurite.fr

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

DÉTECTION - ALARME

AE&T
www.aet.fr/fr/

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

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

TIL TECHNOLOGIES
www.til-technologies.fr

ZENITEL
www.stentofon.fr

VIDÉOSURVEILLANCE

ACALBFI
www.acalbfi.fr

ALL PRODUCTS
www.all-products.com

ARECONT VISION
www.arecontvision.com

AVIGILON CORPORATION
www.avigilon.com

BOSCH
www.boschsecurity.fr

CISCO SYSTEMS
www.cisco.com

CITELUM
www.citelum.com/fr

COMPUTAR / GANZ
www.cbc-cctv.com

CONSORT NT
www.consortnt.com

D-LINK
www.dlink-com/fr

DAHUA
www.dahuasecurity.com/fr

DELTA SECURITY SOLUTIONS
www.delta2s.fr

DIGITAL BARRIERS
www.digitalbarriers.com

ECCTV
www.ecctv.fr

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

ERYMA SÉCURITÉ SYSTÈMES
www.eryma.com

EVITECH
www.evitech.com

EXAVISION
www.exavision.com

FOXSTREAM
www.foxstream.fr

FUJIFILM
www.fujifilm.eu/fr

GENETEC
www.genetec.com

GEUTEBRÜCK
www.geutebruck.com

HIKVISION
www.hikvision.com

HONEYWELL
www.honeywell.com/security/fr

HYMATOM
www.hymatom.fr

IDIS EUROPE
www.idisglobal.com

INDIGO VISION
www.indigovision.com

INEO
www.cofelyineo-securite.fr

IOTEO
www.ioteo.com

IZYX
www.izyx-systems.c

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

SEPTAM
www.septam.fr

SERVIACOM
www.serviacom.fr

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

STIM
www.stim.fr

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

SYNOLOGY
www.synology.com/fr-fr/

TAMRON FRANCE
www.tamron.fr

TEB
www.teb-online.com

TIFALI
www.tifali.com

TIL TECHNOLOGIES
www.til-technologies.fr

VEDIS
www.vedis.pro

VIDEOTEC
www.videotec.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

HOROQUARTZ
www.horoquartz.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

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

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

UNIACCESS
www.uniaccess.fr

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

INTRUSION

Hikvision lance un radar ultra-précis

Le fabricant bien connu de solutions de vidéosurveillance complète sa gamme produits avec un tout nouveau radar de détection d'intrusion dédié à la surveillance grand angle. Hikvision a donc lancé sa solution de détection des intrusions Security Radar. Celle-ci s'appuie sur la technologie d'Hikvision qui permet de déterminer l'emplacement précis et les mouvements d'un grand nombre d'intrus (jusqu'à 32) par radar. Security Radar est idéal pour la surveillance de grandes surfaces exposées soumises à des conditions climatiques difficiles, et dont l'environnement est trop complexe pour se contenter de déployer des caméras de vidéosurveillance. Grâce à sa fiabilité par tous les temps, à sa couverture grand angle et à sa détection fiable des intrus, il est parfaitement adapté aux zones de surveillance autour des bâtiments, des zones industrielles, etc.

Détection précise de zones larges

Les caméras traditionnelles ou les systèmes de détection des mouvements, comme les infrarouges actifs ou la détection de mouvements sur vidéo, sont limités quand il s'agit de déterminer l'emplacement exact d'un potentiel intrus dans l'espace surveillé. Mais Hikvision Security Radar assure une détection précise, avec un angle de vue de 100° et à une distance maximale de 60 m.

Moins de fausses alarmes

La nouvelle offre utilise une technologie numérique de formation de faisceaux ainsi que des algorithmes d'analyse intelligents pour détecter avec précision tous les mouvements de la cible, quelles que soient les conditions météorologiques, réduisant ainsi au minimum les fausses alarmes. En outre, sa certification IP67 vient garantir que le matériel lui-même est approprié pour une utilisation par tous les temps.

Autres caractéristiques

- Il peut également communiquer simultanément avec jusqu'à quatre caméras dômes PTZ de Hikvision.
- Dans cette configuration, la détection d'un intrus déclenche non seulement une alarme, mais aussi l'enregistrement vidéo, afin de vérifier de visu la présence de celui-ci.
- Les caméras et le radar peuvent en outre être installés dans des endroits différents. ■

→ **www.hikvision.com/**

3 QUESTIONS À

LAURENT SCETBON

Responsable d'équipe grands comptes & projets chez Hikvision.


© DR

En quoi ce nouveau radar vient-il compléter la gamme Hikvision ?

Jusqu'à maintenant, nous ne faisions de la détection d'intrusion qu'avec des caméras normales ou thermiques, ainsi que des détecteurs PIR. Désormais, avec ce nouveau radar, nous pouvons proposer à nos clients une solution, qui certes ne détecte pas aussi loin que les caméras thermiques, mais qui va leur permettre de surveiller un grand angle. Par ailleurs, notre radar est capable d'isoler les cibles et d'en faire assurer le suivi, via une fonction asservissement, par quatre dômes motorisés.

Quels sont les autres atouts de ce radar ?

Il s'agit d'abord d'un produit compact, moins fragile qu'une caméra. Par ailleurs, il n'a pas besoin d'être nettoyé comme une caméra. Il peut donc tout naturellement être installé dans des zones agressives.

Ce lancement veut-il dire qu'Hikvision veut diversifier son offre produits ?

Tout à fait. La vidéosurveillance ne peut pas tout faire. Il faut ajouter d'autres technologies à notre gamme pour être capables de proposer aux utilisateurs finaux la meilleure solution de détection possible, selon le site : thermique, radar, etc. Notre but est de fournir des solutions cohérentes et complètes. Nous n'allons d'ailleurs pas nous limiter à ce seul radar. Nous allons très vite en compléter la gamme durant cette année. Comme nous allons aussi nous pencher très sérieusement sur tout ce qui tourne autour de l'exploitation des métadonnées, tout en respectant la vie privée.

CONTRÔLE D'ACCÈS

Nouvelle génération de serrure intelligente

© DR

Nuki lance la Nuki Smart Lock 2.0, la serrure connectée nouvelle génération qui permet de se passer de clé. Parmi ses nombreuses nouvelles fonctionnalités, la Smart Lock 2.0 intègre le Bluetooth 5 pour une meilleure portée, une puissance de traitement interne améliorée offrant plus de rapidité d'utilisation ainsi qu'une compatibilité totale avec Apple HomeKit et Zigbee. Cette nouvelle version inclut également un capteur de porte, un petit aimant qui se colle sur le cadre de la porte ou se fixe au mur. Grâce à ce dernier, il est désormais possible de vérifier non seulement le statut de la serrure (verrouillée ou déverrouillée) mais aussi celui de la porte elle-même (ouverte/fermée), pour toujours plus de sécurité. Conçue par les designers autrichiens d'EOOS.com, fabriquée en Suisse, et dotée d'un logiciel de sécurité de niveau bancaire, la Nuki Smart Lock 2.0 est totalement compatible avec Android et iOS et peut être préconfigurée pour accorder des droits d'accès aux amis, à la famille et à des prestataires de services via l'appli associée, même si ces derniers ne possèdent pas de smartphone. ■

→ **www.nuki.io**

CARACTÉRISTIQUES

- La Smart Lock propose des options très pratiques comme la télécommande Nuki Fob et le clavier Nuki Keypad, qui constituent des solutions d'accès idéales pour les enfants, les livreurs et les soignants.
- La Smart Lock 2.0 s'installe toujours aussi facilement sur votre serrure existante en moins de trois minutes sans nécessiter de modifications sur la porte.
- Elle a aussi été mise à jour pour être compatible avec les serrures à cylindre ovale, tout en conservant sa facilité d'installation sur les serrures existantes.
- Elle s'intègre aux solutions Smart Home existantes telles que Ring ou Nest, ainsi qu'avec les assistants vocaux populaires comme Siri, Alexa, Google Assistant et maintenant Apple HomeKit.

SUPERVISION

Nouvelle version d'ARD Access à partir de la version 1.9.x

Dans cette version 1.9.x de la solution ARD Access d'ARD, l'interfaçage avec le dispositif anti-intrusion Galaxy Dimension a été entièrement remodelé : la déclaration du matériel et de la configuration Galaxy dans ARD Access est facilitée par l'import d'un fichier XML contenant les points d'intrusion, zones, centrale, etc. La supervision n'est pas en reste, la communication avec la centrale et les alarmes intrusion sont remontées, la mise sous et hors alarme et l'éjection de points sont désormais possibles ARD Access. La supervision des événements Aperio Online L100 a été améliorée : en complément à l'état des piles et à la communication, l'état de la porte (verrouillée, déverrouillée et ouverture trop longue) et les défauts mécaniques (effraction, blocage mécaniques) sont remontés en supervision. L'ouverture à distance depuis un écran de supervision est désormais opérationnelle. ■

Autres nouveautés

• Interfaçage avec Office 365 pour la gestion des visiteurs : le dispositif recense les réunions créées par les utilisateurs dans Outlook, ce qui engendre la création automatique des visites associées dans ARD Access puis l'envoi d'un QR code d'accès par email aux visiteurs invités à la réunion. • L'enrichissement de l'API de Webservice SOAP d'ARD Com : listes d'opposition, calendrier des jours spéciaux, accès à l'historique d'événements. • La création des groupes prédéfinis « Agent de sûreté », « Exploitant », « Responsable sûreté » ou « Administrateur ». • Des améliorations ergonomiques diverses, de nouveaux objets d'animation pour les synoptiques de supervision (portail coulissant, lecteur online, etc.), stabilisation de l'interface du terminal Oterm Touch. • Bibliothèque de connecteurs de provisioning enrichie : Heberg3 (système de gestion de l'hébergement pour les CROUS), Gestion des clés Traka, connecteur de synchronisation entre plusieurs instances d'ARD Access, etc. • Gestion d'un identifiant secondaire (ex : identifiant encodé dans une application de la carte et identifiant n° de série de la carte).

© DR

→ **www.ard.fr**

quoi de neuf ?

SURVEILLANCE

Spynel 360°, le nec plus ultra pour la surveillance maritime

Le capteur thermique Spynel 360°, présenté par HGH Infrared Systems, a été conçu pour assurer une surveillance optimale sur les mers les plus agitées. Avec son logiciel de tracking automatique Cyclope, ils assurent la surveillance asymétrique 24/7 la plus fiable pour faire face à tous types de scénarios. Le capteur thermique 360° fonctionne avec succès dans l'obscurité la plus totale à un niveau de mer très élevé, grâce à une stabilisation optomécanique et numérique unique et innovante. Grâce au puissant traitement d'images du logiciel Cyclope, le taux de fausses alarmes est très faible malgré les vagues, les vibrations et les reflets du soleil. Une technologie adaptée aux conditions les plus difficiles puisque les cinq modèles de caméras thermiques sont équipés d'une peinture anticorrosion et d'un gicleur lave-glace pour ôter l'eau de mer de l'objectif. Les caméras Spynel sont les plus fiables. Pour preuve, les capteurs Spynel livrés à la marine française, il y a près de dix ans, sont toujours opérationnels. ■

→ **www.hgh.fr**

VIDÉOSURVEILLANCE

Nouveautés IndigoVision

À l'occasion des salons GSX 2018 et Security Essen 2018, IndigoVision a lancé de nouveaux produits permettant aux clients de renforcer leur solution de sécurité. Tout d'abord, la dernière version de notre solution de gestion de la sécurité multiniveau, Control Center v15.3, contribue à améliorer la sécurité de votre système avec des améliorations prometteuses apportées à l'appareil CyberVigilant (notamment les fonctions d'effondrement de l'alarme), une fonction de réorganisation des clips de story-board et l'intégration de Federated License Server. Il n'a jamais été aussi facile de garantir une sécurité à toute épreuve. La seconde nouveauté était la caméra thermique BX dont le nouveau tube thermique BX offre : débit numérique supérieur de 30 trames/s, nouveau capteur amélioré, fonctions d'entrée et de sortie audio, analyse de détection incendie… ■

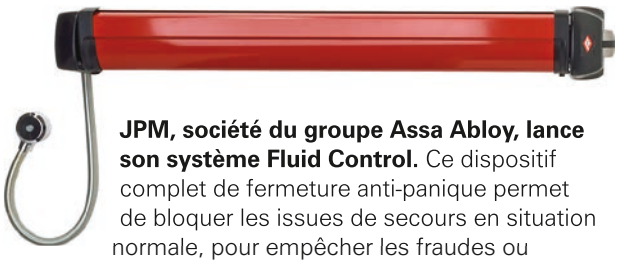
→ **www.indigovision.com**

CARACTÉRISTIQUES

- Control Center V15.3 est doté de la technologie de reconnaissance de plaque d'immatriculation (LPR) développée par InnoWare. Idéale pour les lieux d'entrée/sortie, comme les accès aux aires de stationnement qui nécessitent une carte ou de l'argent pour entrer et sortir.
- Cette technologie peut aussi être utilisée pour fluidifier la circulation à des vitesses allant jusqu'à 200 km/h.

LUTTE CONTRE LE FEU

Gamme innovante de fermeture anti-panique contrôlée chez JPM



JPM, société du groupe Assa Abloy, lance son système Fluid Control. Ce dispositif complet de fermeture anti-panique permet de bloquer les issues de secours en situation normale, pour empêcher les fraudes ou les sorties non-autorisées, tout en assurant une évacuation efficace en cas d'urgence. Fluid Control Exit permet de bloquer les sorties des issues de secours DAS en « situation normale » et en cas de besoin d'évacuation, de déverrouiller les portes pour assurer la sûreté des personnes. Outre son rôle classique d'évacuation des personnes en cas de mouvement de foule, la nouvelle fermeture anti-panique EXIT de JPM permet de contrôler les sorties en gestion locale ou £en raccordement à une unité de gestion centralisée du bâtiment. Elle protège les biens contre les vols dans les lieux de type musées, centres commerciaux, etc. Elle évite les fraudes dans les aéroports ou encore les salles concerts. De plus, du côté des entrées, les trois fonctionnalités du module de manœuvre extérieur permettent une gestion personnalisée :

- Entrée unique : le passage s'effectue uniquement grâce à la clé. Le système clé prisonnière oblige à reverrouiller le module après passage.
- Jour / nuit : par action de la clé, l'entrée est laissée libre en journée et condamnée en soirée.
- Entrée toujours libre : sans cylindre. ■

→ **www.jpm.fr/fr/site/jpm/**

VIDÉOSURVEILLANCE

NVR hautes performances chez Milestone

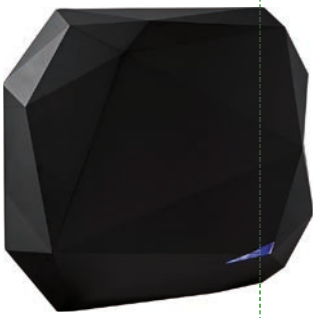
Milestone Systems a lancé sa nouvelle plate-forme matérielle NVR Milestone Husky X2 et X8 à VMS évolutif. Ces nouveaux produits vont permettre à la communauté Milestone de concevoir des solutions vidéo pour les petites comme les très grandes entreprises à l'aide du NVR Milestone Husky série X grâce à ses éléments de base évolutifs haute performance. Une solution qui permet de limiter le coût total de possession, car une installation donnée nécessite moins de matériel que les serveurs standard. La série NVR X peut atteindre ses performances grâce à son accélération matérielle qui permet d'améliorer les performances du système simplement en laissant le processeur graphique prendre en charge la plus grande partie du décodage vidéo, pendant que le système effectue d'autres tâches.

Deux modèles :
- Milestone Husky X2 – deux disques durs échangeables à chaud et un commutateur PoE + intégré. Ce modèle peut prendre en charge jusqu'à 133 caméras (720P @ 25 FPS, 2 Mbit/s).
- Milestone Husky X8 – huit disques durs échangeables à chaud et des interfaces réseau doubles 10 Gbit/s. Le stockage interne peut être étendu avec des unités de stockage externes connectées via une connexion à haute vitesse par ethernet (FCoE) ou iSCSI. Husky X8 peut prendre en charge jusqu'à 780 caméras, avec une vitesse d'enregistrement de 1,828 Mbit/s. ■

➔ **www.milestonesy.com**

CONTRÔLE D'ACCÈS

Spectre, le lecteur longue distance évolutif



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

➔ **www.stid-security.com**

CARACTÉRISTIQUES

- Fréquences porteuses : 865 – 868 MHz : 866 MHz ETSI (Europe), Maroc... 902 – 928 MHz : 915 MHz FCC Part 15 (USA)…
- Compatibilité puces : EPC Class 1 Gen 2 / ISO 18000 – 63.
- Lecture seule ou lecture écriture.
- 1 à 4 antennes.
- Distance de lecture : jusqu'à 13 m avec étiquette ETA et tage passif Teletag selon les conditions d'utilisation.
- Résistance aux intempéries IP66 – Structure renforcée antivandales IK10.

CONTRÔLE D'ACCÈS

Tel2Voice d'Urmet, un interphone 100 % connecté

Urmet France complète sa gamme d'interphonie 2Voice avec l'option Tel2Voice, une nouvelle solution 100 % connectée et hybride. Grâce à une application gratuite, Tel2Voice, système sans fil, permet aux résidents de l'immeuble, de visualiser, converser et autoriser l'accès aux visiteurs depuis leur smartphone. Le kit comprend une plaque de rue, une centrale, une alimentation, un lecteur Vigik, un modem et un abonnement mensuel ou prépayé adapté au nombre de logements à équiper. Tel2Voice fonctionne avec un modem 3G qui dialogue lui-même avec le logiciel en ligne Visiosoftweb pour une administration à distance simplifiée. Le gestionnaire, le bailleur ou le syndic peuvent contrôler les accès (création, modification, suppression des badges, portes, noms, passes, etc.), ouvrir à distance (donner des droits d'accès ponctuels pour des prestataires) et sécuriser les locaux (recevoir des alertes par mail : porte ouverte, panne de chauffage ou VMC, fuite d'eau, etc. Présentée au printemps dernier, la gamme d'interphonie 2Voice, simple à mettre en œuvre (2 fils seulement) présente un des plus grands choix du marché avec une large offre de plaques de rue, postes audio et moniteurs vidéo. ■

➔ **www.urmet.fr**

c'est vous qui le dites !

© DR

« Les technologies ne remplaceront pas l'homme en sécurité. »

ELIAS NAHRA
Président Groupe Triomphe Sécurité

À l'heure où les nouvelles technologies débarquent en force dans la sécurité privée, laissant augurer d'un possible remplacement de l'homme par la machine, Elias Nahra nous rappelle que le tout technologique est un leurre et que l'homme a toute sa place dans la sécurité.

Ce n'est pas un opérateur vidéo dans un centre de télésurveillance à Stockholm ou ailleurs qui assurera l'interpellation d'un voleur dans un grand magasin parisien. C'est un agent inspecteur du magasin en chair et en os et doté d'un savoir-faire et d'un talent personnel... Ce n'est pas un robot qui viendra porter secours et assistance à un client qui a un malaise dans une file d'attente après une bousculade... Ce n'est pas une caméra, même intelligente, qui fera preuve de tout son talent de médiation pour calmer une bande de jeunes lors d'un match de foot un peu chaud, mais bien une agente de sécurité bien formée et expérimentée... Voilà pourquoi je crois que si les technologies sont incontestablement partie prenante de l'avenir de la sécurité, rien ne remplacera l'homme en sécurité.

L'intelligence doit surtout être celle de nos hommes et femmes

L'utilisation des technologies est primordiale : la vidéosurveillance, la reconnaissance faciale, etc. Voilà pourquoi, nous formons nos agents à la pointe de la technologie. Il y a déjà et il y aura de plus en plus de recours à des technologies diverses tant pour la gestion, le suivi, le pilotage, la protection des agents, le contrôle, le reporting, l'assistance, l'inspection, la sûreté, la surveillance, la protection, l'incendie... c'est incontournable. Les tablettes, les téléphones intelligents... équipent de plus en plus nos agents sur site. Les agents en place manient des équipements technologiques de plus en plus fréquemment : portiques, raclettes, caméras...
Bien sûr que l'utilisation de l'IA pourra accompagner, aider les vidéos opérateurs en magasin pour agir le plus en amont, intervenir, profiler, mais l'intelligence doit être surtout celle de nos hommes et de nos femmes. Ce qui compte par-dessus tout, pour moi, ce sont la formation, les compétences, les certifications, les qualifications... Il est donc primordial de former nos agents à la pointe des technologies. Croire et miser sur les hommes, c 'est miser sur la formation. Mais il faut changer le système avec des formation plus courtes, plus opérationnelles, plus flexibles et polyvalentes. Et finançables ! C'est ainsi aussi que nous attirerons de nouveaux profils et renouvellerons nos équipes et améliorerons notre attractivité. Ce qui est nécessaire et indispensable.

Le tout technologique ne sera pas acceptable dans nos sociétés démocratiques

L'agent sera certes donc de plus en plus équipé et communiquant mais rien ne remplacera son esprit d'initiative, sa réactivité, son humanité. La sécurité humaine mérite bien son nom !
Par ailleurs, gardons la tête froide. Ne tombons pas dans l'illusion d'une sécurité totalement technologique. Cela provoquerait aussi un rejet de la société et des citoyens. Il faut que le niveau de sécurité et de surveillance reste humainement acceptable sinon nos sociétés démocratiques qui ont des capacités de révolte profonde – on l'a vu avec le mouvement des Gilets jaunes – la rejetteront.
Voilà pourquoi la sécurité humaine a de beaux jours devant elle à condition aussi d'évoluer, de se professionnaliser et de s'assainir en profondeur : garantie financière, maîtrise de la sous-traitance, etc. ■

ELIAS NAHRA ■ **2005** Création de Triomphe Sécurité. ■ **2007** Adhésion au Snes. ■ **DEPUIS 2011** Administrateur du Snes. ■ **2014** Élu vice-président du Snes

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

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

protectionsecurite-magazine.fr

Infos
Archives
Annuaires
e-salon
Dossiers techniques
...