



# DES USINES À MIEUX PROTÉGER

Face à la menace terroriste et aux actes de malveillance, l'État veut renforcer la protection des 2500 sites industriels les plus sensibles. Au-delà de l'urgence, les entreprises doivent développer une nouvelle culture de la sûreté industrielle.

PAR HASSAN MEDDAH

#### MODE D'EMPLOI

- **La sûreté** regroupe l'ensemble des mesures de protection pour lutter contre les actes de malveillance.
- **La sécurité** industrielle vise un fonctionnement sans danger des installations pour les employés et les populations avoisinantes.

Les usines ne sont pas à l'abri des actes de malveillance ni du terrorisme. Au contraire ! Les équipements coûteux et les matières dangereuses qui y sont manipulées en font des cibles de choix. Depuis 1992, 850 actes de malveillance contre des sites industriels ont été dénombrés par le Bureau d'analyse des risques et pollutions industriels (Barpi), rattaché au ministère de l'Écologie, du Développement durable et de l'Énergie. Ces accidents entraînent

dans la plupart des cas des pertes économiques significatives, une fois sur deux des dégâts environnementaux et, dans près de 15 % des cas, des blessés dans les entreprises concernées. Ces actes prennent parfois une tournure encore plus tragique, comme l'ont montré les attaques de type terroriste survenues l'été dernier. Le 26 juin, dans l'usine d'Air Products à Saint-Quentin-Fallavier (Isère), un prestataire a projeté son véhicule sur des bonbonnes de gaz industriels pour les faire exploser. Quelques semaines plus tard, le 14 juillet, deux explosions criminelles touchaient un site pétrochimique à Berre-L'Étang (Bouches-du-Rhône), sans faire de victime.

« Dans les deux cas, il y avait des failles », analyse Alain Juillet, le président du Club des directeurs de sécurité et de sûreté des entreprises [lire l'entretien page 34]. Au som-

En France, plus de 2500 sites font l'objet d'une vigilance particulière.





L'usine Air Products de Saint-Quentin-Fallavier (Isère), attaquée le 26 juin, était pourtant considérée comme un site à risque et classée Seveso.

met de l'État, l'heure de la mobilisation a sonné. Il devenait urgent de renforcer la protection des sites sensibles. Au cœur de l'été, les hauts fonctionnaires de défense des ministères concernés (Intérieur, Économie, Écologie), le directeur du Secrétariat général de la défense et de la sécurité nationale, chargé notamment de la lutte contre le terrorisme, ainsi qu'une trentaine d'industriels opérant des sites Seveso se sont mobilisés autour de Ségolène Royal, la ministre de tutelle, pour mettre en place un plan d'action. Plus de 2 500 sites en France font l'objet d'une vigilance particulière [lire page 28]. Il s'agit des 1 370 points dits d'importance vitale (PIV), comme les aéroports, les gares, les centrales nucléaires..., essentiels au bon fonctionnement du pays; et de 1 200 sites répondant à la réglementation Seveso. Plus globalement, environ 500 000 sites sont soumis à la législation des installations classées pour la protection de l'environnement (ICPE). Ils sont susceptibles de générer des risques pour les personnes, les biens...

« Tous ces sites seront inspectés avant la fin de l'année et un bilan sera tiré. On simule des scénarios de malveillance.



**« Les prestataires n'ont pas besoin d'avoir accès à toutes les zones. Il faut définir des accès restreints pour les zones névralgiques. »**

Patricia Blanc, directrice générale de la prévention des risques

On teste les plans d'action et de continuité, les réactions en cas d'intrusion», précise Patricia Blanc, la directrice générale de la prévention des risques. Une instruction gouvernementale datée du 30 juillet 2015 définit précisément le plan de l'État pour améliorer la sécurité des sites vulnérables. Les entreprises concernées doivent renforcer les conditions d'accès à leurs sites, par la voie du gardiennage ou de systèmes de badge. La gestion des sous-traitants est devenue un sujet critique. « Les prestataires n'ont pas besoin d'avoir accès à toutes les zones. Il faut définir des accès res-

treints pour les zones névralgiques», précise Patricia Blanc. Le nouveau texte demande également aux préfets de se rapprocher des industriels afin d'identifier les responsables de la sûreté et les dispositifs mis en œuvre pour réagir plus vite en cas de besoin.

Le résultat des audits révélera, à coup sûr, nombre de vulnérabilités. Si les directeurs de sûreté des entreprises se montrent très frileux pour s'exprimer sur le sujet, les professionnels du secteur (auditeurs, fabricants et distributeurs d'équipements de sécurité, consultants...) font état d'une réalité du terrain... pas très rassurante. À l'exception notable des opérateurs d'importance vitale, la sûreté n'a jamais été la priorité des entreprises. Celles-ci concentrent avant tout leurs efforts sur la sécurité industrielle de leur site, c'est-à-dire les procédures à mettre en œuvre pour qu'il n'y ait pas de conséquences sur les populations et l'environnement en cas d'accident industriel. « Hormis dans les industries de défense, les entreprises industrielles ont une culture historiquement orientée HSE (hygiène, sécurité, environnement) liée à la prévention des accidents. Elles sont souvent moins préparées à faire face aux actes de malveillance, par manque de culture et d'expérience sûreté. Or une faille de sûreté est une faille de sécurité», souligne Sébastien Mauqué, le directeur général du groupe Partenaire sécurité, une société de conseil et d'ingénierie dans le domaine de la sécurité.

#### Identification des technologies prioritaires

D'autres constats sont encore plus sévères, comme celui résumé par les trois « A » : angélisme, aveuglement et amateurisme. « Les entreprises passent successivement par ces trois phases. Elles s'estiment toujours bien protégées et considèrent qu'elles ne sont pas une cible. Enfin, il leur arrive de choisir des solutions qui ne correspondent pas à la réalité de la menace et d'opter pour des solutions low cost peu dignes des véritables enjeux», estime Gilles Goubin, le chef du pôle de formation sûreté-malveillance du Centre national de prévention et de protection (CNPP), qui forme 150 cadres sûreté par an. Les optimistes verront le verre à moitié plein, mettant en avant les progrès réalisés. « Il y a dix ans, des grands groupes comme Peugeot et Lafarge n'avaient pas de directeur de la sûreté. Leur internationalisation et leurs développements dans des régions du monde où les risques sont plus grands les ont sensibilisés à cette question, observe Olivier Hassid, le directeur général du Club des directeurs de sécurité et de sûreté des entreprises (CDSE). Sur les 75 membres du CDSE, une poignée ont rejoint le comité exécutif. En 2009, il n'y en avait aucun. »

L'État veut aller plus loin que les mesures d'urgence. Il veut profiter des audits pour identifier les bonnes pratiques de sûreté et élargir sa réflexion avec des comparaisons internationales, notamment avec les autres pays européens et les États-Unis. Un exercice de crise impliquant un site Seveso sera organisé dans chaque grande zone de défense (on en compte sept en France) avant la fin de l'année. Le but : éprouver l'efficacité des mesures prévues par le plan de protection de l'entreprise. Dans son plan d'action, l'État mise également sur les nouvelles technologies.

MARIUS BECKERDPA - D. R.

### 4 % DES ACCIDENTS SONT CAUSÉS PAR DES ACTES DE MALVEILLANCE

850

accidents liés à la malveillance depuis 1992, soit 4 % des accidents intervenus dans les ICPE (installations classées pour la protection de l'environnement)

13,5%

C'est le pourcentage de ces accidents ayant causé des blessés, souvent légers

85%

d'entre eux ont eu des conséquences économiques sérieuses (frais de réparation, pertes d'exploitation)

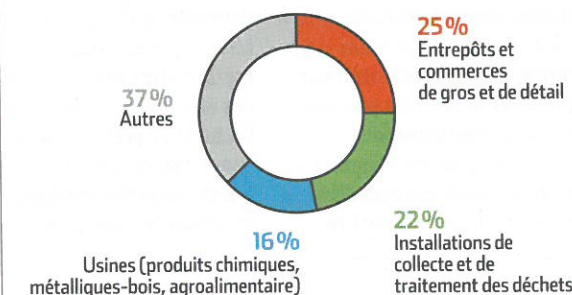
50%

Près d'un cas sur deux a occasionné des dégâts environnementaux (pollution des sols, des eaux...)

77%

de ces cas ont entraîné un incendie dont 49 % avec rejet de matières dangereuses ou polluantes

Les activités les plus touchées par type d'établissement



SOURCE: ÉTUDE DU BUREAU D'ANALYSE DES RISQUES ET POLLUTIONS INDUSTRIELLES (BARPI), OCTOBRE 2015

Le Comité de la filière industrielle de la sécurité (Cofis) identifie les technologies prioritaires. Deux pistes sont déjà privilégiées : la détection d'armes et d'explosifs à l'entrée des sites sensibles ainsi que le repérage et la localisation d'individus dans une zone sous contrôle afin de déceler des comportements anormaux [lire page 32]. Toutefois les experts préviennent : la technologie seule ne résoudra pas les problèmes de sûreté. Il ne sert à rien de mettre des caméras partout s'il n'y a personne pour regarder les écrans, tout comme il est vain d'investir dans des technologies sophistiquées de détection d'intrusion sans un système de badges rigoureux. La fameuse cohérence de la chaîne de sûreté ! « La vidéo-surveillance n'empêchera jamais un braquage ni une attaque »





QUATRE DISPOSITIFS POUR GARANTIR LA SÉCURITÉ DES SITES INDUSTRIELS

LA DIRECTIVE SEVESO  
**La réglementation historique**



**PÉRIMÈTRE** EUROPE, 1211 SITES CONCERNÉS EN FRANCE

Cette directive européenne a été mise en place à la suite d'un accident grave de rejet de dioxine qui a frappé la commune italienne éponyme en 1976. Les sites dits Seveso font partie des installations classées pour la protection de l'environnement, les ICPE, présentant le plus haut niveau de risque. Leur destruction ou leur mauvais fonctionnement pourrait causer un danger grave pour les populations voisines. Selon la quantité de matières à risque déposées sur le site, la directive

distingue les sites Seveso seuil haut et seuil bas (respectivement 656 et 515 sites en France, au dernier recensement datant de fin 2014). L'exploitant doit faire une demande d'autorisation avant toute mise en service de son installation et démontrer qu'il maîtrise les risques. La bonne application de la directive est du ressort de l'inspection des installations classées, sous l'autorité du préfet. Le texte prévoit une obligation d'information à destination des populations en cas d'accident majeur. ■

LA RÉGLEMENTATION DES ACTIVITÉS D'IMPORTANCE VITALE  
**Un statut à part pour des activités vitales**



**PÉRIMÈTRE** FRANCE, 1370 SITES

Il existe des activités qui, si elles subissaient une attaque ou une avarie, mettraient en danger le fonctionnement de l'État et la vie de ses citoyens. Il s'agit d'activités qualifiées d'importance vitale par le Code de la défense et définies par le décret du 23 février 2006. L'État, à travers le secrétariat général de la Défense et de la Sécurité nationale, a identifié 235 opérateurs d'importance vitale (OIV), des entreprises appartenant au secteur privé comme au secteur public, dont la liste est classifiée.

Ces OIV opèrent dans douze secteurs d'activités, dont l'énergie, la défense, les transports, l'industrie, la pharmacie, l'espace et la recherche ou encore la gestion de l'eau... Ces derniers exploitent 1370 points d'importance vitale qu'ils doivent impérativement sécuriser en respectant un plan particulier de protection. Ce dispositif, qui décrit les vulnérabilités du site et les moyens mis en œuvre pour le protéger, doit être approuvé par le préfet du département. ■

des différentes fédérations régionales. Il s'appuie pour cela sur le guide de l'Institut national de l'environnement industriel et des risques (Ineris) qui vient d'être réactualisé. Celui-ci permet aux entreprises d'auto-évaluer leur niveau de vulnérabilité face aux menaces de malveillance et de terrorisme. « Dans le public, on trouve tout type de profils : des directeurs d'établissement, des responsables de la sûreté, des responsables HSE », explique Philippe Prudhon, qui en profite pour rappeler les questions de base à son auditoire. Existe-t-il une politique de sûreté rédigée et accessible dans l'entreprise ? Quels en sont les objectifs affichés ? A-t-elle été communiquée aux personnels ? Quelle est la nature des contrats avec les prestataires ?

L'UIC se veut également force de propositions. Parfois très simples. Comme la révision des fiches Seveso. À travers

VINCENT MEYER/GET IMAGES; PASCAL GUITTET; BINTA/AP/SIPA

LE PLAN VIGIPIRATE  
**Des mesures contre le terrorisme**



**PÉRIMÈTRE** FRANCE ET SITES FRANÇAIS À L'ÉTRANGER, TOUS LES SECTEURS D'ACTIVITÉ SONT CONCERNÉS

Quand la menace terroriste est jugée élevée et durable, le plan Vigipirate est l'outil de prévention et de protection privilégié par le gouvernement pour sécuriser les citoyens et les intérêts de la nation. Le nouveau plan de 2014, qui a succédé à ceux de 2003 et 2006, s'applique à des domaines d'activités très transverses (alerte et intervention, bâtiments et installations, cybersécurité...). Il a été simplifié passant de quatre à deux niveaux

de vigilance (simple et renforcée). Mis en place en 1978 pour la première fois, le plan Vigipirate est composé d'environ 300 mesures qui s'appliquent à tous les grands domaines d'activité (transports, santé, alimentation, réseaux d'énergie...). Ce dispositif est complété par des mesures spécifiques en cas de menaces sur des cibles particulières (avion, centrale nucléaire, navire, site de production chimique...). ■

ces documents, la loi oblige les entreprises à communiquer, dans un souci de transparence vis-à-vis des populations voisines, des données très précises sur la nature, la quantité et même la localisation des produits stockés sur leurs sites. « La plupart de ces informations se retrouvent sur internet. Au point que cela va à l'encontre de la sûreté », déplore Philippe Prudhon.

Les services de l'État étudient, par ailleurs, l'opportunité de classer des établissements Seveso points d'importance vitale, c'est-à-dire répondant à des contraintes de sûreté encore plus drastiques. Ce qui déplaît à certains industriels. « Les investissements pour se conformer à ce dispositif sont très élevés pour un gain commercial nul », s'insurge l'un d'eux. Au ministère du Développement durable, on estime que le rapprochement à long terme

L'INSTRUCTION GOUVERNEMENTALE DU 30 JUILLET 2015  
**Les derniers développements**



**PÉRIMÈTRE** FRANCE, TOUS LES SITES SEVESO

Adressée aux préfets de zones de défense et de sécurité, de police, de région et de département, cette circulaire vise à renforcer la sécurité des sites Seveso contre les actes de malveillance, à la suite de l'attentat contre le site de Saint-Quentin-Fallavier (Isère) le 26 juin et aux deux explosions criminelles survenues sur le site pétrochimique de Berre-l'Étang (Bouches-du-Rhône) le 14 juillet. Un plan d'action prévoit notamment que chaque site Seveso devra être inspecté avant la fin de l'année 2015

et qu'une série d'établissements fera l'objet d'audits interministériels approfondis en matière de sûreté. Elle contraint les forces de l'ordre à acquérir une meilleure connaissance des installations et de leurs dispositifs de sûreté. La directive rappelle par ailleurs que le secrétariat général de la Défense et de la Sécurité nationale doit étudier l'opportunité de classer de nouveaux établissements Seveso comme point d'importance vitale au regard de leurs activités. ■

des réglementations sur les activités d'importance vitale et les activités Seveso apportera une réponse prometteuse pour renforcer la protection des sites industriels. Selon le Secrétariat général de la défense et de la sécurité nationale, une telle convergence donnerait une vision d'ensemble aux exploitants aussi bien sur les risques de malveillance ou de terrorisme que sur les risques technologiques ou pandémiques.

Quelque 75 sites Seveso sont déjà classés comme points d'importance vitale. À quel rythme ira la convergence entre les deux réglementations ? Les résultats des audits des sites Seveso, qui seront connus au début de l'année prochaine, donneront le nouveau tempo. ■

SUITE DE NOTRE ENQUÊTE P. 30

→ terroriste. Pour des terroristes comme les frères Kouachi, déterminés à aller jusqu'au bout, être filmés ou pas n'est pas la question. Élever le niveau de sûreté globalement exige de réunir trois ingrédients indispensables : le matériel, les procédures et l'homme », estime Éric Davoine, le porte-parole en France d'Asis International, l'association internationale des professionnels de la sûreté.

**Des contraintes drastiques**

Les industriels se montrent d'ores et déjà réceptifs au plan d'action initié par l'État. L'Union des industries chimiques (UIC), qui représentent plus de 50 % des sites Seveso, est en première ligne. Son Monsieur sûreté, Philippe Prudhon, le directeur du département technique, multiplie les séminaires pour répondre aux sollicitations





Reportage

# DES DONNÉES SOUS HAUTE PROTECTION

Agents de sécurité, détecteurs d'intrusion, contrôle d'accès biométrique, vidéosurveillance, badges personnalisés... Pour accéder au datacenter d'Interxion, il faut montrer patte blanche.

PAR HASSAN MEDDAH



Toute tentative sauvage de pénétration dans le site est repérée par les détecteurs de mouvement. Et déclenche une alarme et l'activation des caméras.

**S**on architecture moderne tranche avec les petits pavillons voisins. À La Courneuve (Seine-Saint-Denis), l'imposant centre de données d'Interxion héberge des serveurs web pour le compte de grandes entreprises. « Pour que nos clients puissent bénéficier de la meilleure offre de connectivité, nos datacenters doivent être proches des grands réseaux internet. Il n'était pas question de nous exiler à la campagne », explique Fabrice Coquio, le président de la filiale française d'Interxion, qui gère pas moins de huit datacenters. L'installation tente toutefois de se faire discrète. Sur la grande façade du bâtiment comme sur le portail d'entrée, nulle trace de pancarte, de publicité ou de logo qui indiqueraient qui est le propriétaire des lieux ou ce qui s'y fait. Seule l'adresse confirme au visiteur qu'il se trouve au bon endroit. « Cela ne sert à rien de s'afficher. On attire moins la malveillance », assure Fabrice Coquio.

### Une barrière infrarouge autour du bâtiment

Une clôture de 2,20 mètres, la hauteur maximale prévue par le plan local d'urbanisme, a été préférée à un mur. Et pas seulement pour mieux s'intégrer au quartier. Le stationnement de véhicules et les comportements suspects aux abords du site sont ainsi plus facilement repérables. « Voir, c'est le premier élément de sécurité », assure le responsable. Avec plus d'une centaine de clients et une surface de salles informatiques qui va bientôt doubler, à quelque 9 600 mètres carrés, le datacenter de La Courneuve est une infrastructure critique. Il garantit une disponibilité proche du 100 % grâce à des équipements électriques et de refroidissement des serveurs ultra-redondés. Interxion, qui a son siège à Amsterdam, aux Pays-Bas, assure une sécurité optimale. « Celle-ci repose avant tout sur des process. Ils sont identiques dans l'ensemble de nos quarante datacen-



Le sas d'entrée est équipé de caméras thermiques pour dénombrer les personnes présentes et de lecteurs biométriques des paumes de main.



Dans la salle informatique, les serveurs sont protégés dans des espaces grillagés, accessibles par clé et par reconnaissance biométrique.

STÉPHANE JAYET

ters en Europe. Depuis leur arrivée sur le site jusqu'à la salle des serveurs, les clients devront franchir au minimum cinq niveaux de sécurité », précise Fabrice Coquio.

Rien n'échappe aux 200 caméras disposées sur la façade et à l'intérieur des locaux. Elles surveillent le parking, les abords du bâtiment, l'entrée principale et l'accès à l'accueil. Le datacenter est cerclé par une barrière infrarouge. Si un mouvement est détecté, les caméras s'orientent, zooment automatiquement vers la zone en question et les images s'affichent sur les écrans des gardiens. Les vidéos en haute définition permettent de lire la plaque d'immatriculation des véhicules ou de reconnaître le visage d'un individu à plusieurs centaines de mètres de distance. Ce suréquipement permet aussi de ne faire appel qu'à deux agents de sécurité pour l'ensemble du site.

### Un contrôle permanent des déplacements

L'intérieur de l'enceinte est encore plus protégé que l'extérieur. Les quelques clients venus ce jour-là pour accéder à leurs serveurs informatiques sont habitués au protocole à suivre. Il doivent d'abord se présenter aux deux agents du poste de sécurité, assis derrière une vitre blindée. Ces derniers leur fournissent, en échange de leur pièce d'identité, un badge électronique et les clés dont ils auront besoin. La gestion des 160 clés, soigneusement accrochées sur un tableau mural qui permet de repérer rapidement celles qui sont sorties, est doublée par un logiciel de suivi informatique. En un coup d'œil, les badges permettent d'identifier l'activité des personnes présentes sur le site. Les équipes d'Interxion en portent un bleu, les prestataires un gris, les clients un orange et les visiteurs un vert. Si un visiteur se déplaçait seul dans les locaux, ce qui est interdit, il serait très vite repéré.

Avant-dernier rempart avant d'accéder aux salles des serveurs, le sas de sécurité avec son double jeu de portes en verre permet de faire entrer deux personnes à la fois. Il combine trois systèmes de contrôle ! Les visiteurs doivent badger pour attester de leurs droits d'accès. À l'intérieur, des caméras thermiques situées au plafond repèrent le nombre de personnes présentes pour éviter les accompagnateurs frauduleux. Enfin, pour sortir, l'individu doit s'authentifier en posant la paume de sa main sur un capteur biométrique. Les couloirs à la décoration minimaliste, dans lesquels les caméras et les détecteurs scrutent les moindres recoins, ressemblent à ceux d'un hôpital, l'activité et le passage en moins. Ils mènent aux salles informatiques, froides et impersonnelles à souhait. Là, les serveurs sont placés dans une cellule grillagée... pour davantage de sécurité.

« La sécurité est également une question de coût. Elle représente environ 10 % de nos investissements et de nos coûts d'exploitation. Mais cet investissement est à mettre en rapport avec le coût d'une éventuelle défaillance de sécurité », estime Fabrice Coquio. Le centre de données aura coûté près de 130 millions d'euros. En quinze ans d'exploitation, Interxion n'a déploré aucun accident significatif de malveillance. ■

SUITE DE NOTRE ENQUÊTE P. 32 ➔

Collectivités

Opérations

Grande distribution

SALONS

# STMP

Location

Retrouvez tous nos produits sur

[www.stmp-location.fr](http://www.stmp-location.fr)



01 43 89 06 00



STMP France  
100 avenue de Choisy - 94 190 Villeneuve Saint Georges  
01 43 89 06 00  
contact@stmp-location.com





# Sûreté LES TECHNOLOGIES, OUI, MAIS PAS SEULEMENT...

Pour protéger les sites industriels, les parades technologiques sont de plus en plus perfectionnées et quasi autonomes. Mais l'homme doit rester dans la boucle.

PAR HASSAN MEDDAH

**F**ace aux problèmes de sûreté rencontrés par les entreprises, la réponse est-elle technologique ? Certains ont tendance à le croire. Ainsi Alain Juillet, le président du Club des directeurs de sécurité des entreprises (lire l'entretien page 34), souligne-t-il la supériorité de la machine sur l'humain pour la réalisation de tâches répétitives. Deux domaines sont révélateurs de cette tendance : les drones et la télésurveillance.

Les entreprises s'intéressent de plus en plus aux mini-drones de surveillance terrestres ou aériens. « Sur notre site de démonstration, une ronde complète prend une heure et demie à deux heures à un gardien. On regarde de près ce que les drones pourraient nous apporter dans ce domaine », explique Gilles Goubin, le chef de service Pôle de formation sûreté-malveillance du CNPP, un groupe spécialisé dans la prévention des risques. Ni l'offre ni l'innovation ne font défaut. Tecdrone et Nexter proposent des petits robots capables d'effectuer des levées de doute en cas de détection d'intrusion. Pour leur part, Fly-n-Sense, ECA Group, Bertin Technologies... commercialisent des mini-drones aériens permettant d'acquies rapidement de l'information sur une zone donnée. Avec un argument de poids : écarter l'homme du danger.

Dans la télésurveillance, la tentation du tout technologique est aussi présente. Au salon de la sécurité APS qui s'est tenu fin septembre à Paris, de nombreux exposants présentaient des caméras capables de distinguer, de jour comme de nuit, des détails toujours plus fins. Gare, toutefois, au mirage technologique. « À quoi cela sert-il de déployer des dizaines de caméras si l'on n'a pas défini les procédures et les moyens de réponse en cas d'intrusion ? interroge Sébastien Mauqué, le directeur général du Groupe Partenaire Sécurité, une société de conseil et d'ingénierie spécialisée en sécurité globale. En amont, l'entreprise doit développer une politique de sûreté cohérente et définir une cartographie de ses risques opérationnels pour savoir de quoi et comment elle se protège. » ■



## LA VIDÉOSURVEILLANCE INTELLIGENTE

La vidéosurveillance n'est pas seulement une affaire de pixellisation et de qualité d'image. Komanche se distingue en misant sur l'intelligence artificielle. Sa solution Visiomind permet ainsi d'analyser et de reconnaître des formes dans les flux vidéo. Dès qu'une personne ou une forme inconnue pénètre dans une zone déterminée, la caméra « s'accroche » et la suit. Elle distingue si un individu est debout, assis ou allongé. Afin d'alléger le travail des télésurveillants, Visiomind peut aussi sélectionner une zone de traitement spécifique sans prendre en compte l'intégralité du champ de l'image enregistrée par la caméra vidéo. Selon son fabricant, Visiomind permet de réduire d'un facteur 10 le taux d'erreur (fausses alertes) lié aux systèmes de vidéosurveillance. ■



## LA CLÔTURE ÉLECTRONIQUE

La clôture qui dissuade d'entrer sauvagement sur un site, c'est bien. Celle qui alerte lorsqu'un individu malveillant passe à l'acte, c'est mieux. La société Hymatom a conçu une panoplie de capteurs s'intégrant aux systèmes de protection périmétrique. Si une personne tente de découper ou d'arracher la clôture, de l'escalader ou de la franchir sans appui, une alarme est déclenchée. La solution Detect 4 U intègre quatre technologies : un capteur de vibrations en surface réagissant aux coupures, un détecteur de rupture de faisceaux infrarouges signalant toute tentative de franchissement, un système sensible aux contraintes mécaniques subies par les poteaux et enfin une caméra vidéo haute définition. En cas d'intrusion, la caméra transmet la vidéo sur le poste du télésurveillant en précisant l'endroit où elle s'est produite. ■



## LE RONDIER INCROYABLE

Les robots s'apprentent à révolutionner la surveillance des sites industriels et des entrepôts. La start-up EOS Innovation a mis au point le robot rondier e-vigilante. Le télésurveilleur peut programmer des rondes prédéfinies ou laisser le robot se déplacer aléatoirement. Monté sur trois roues et haut d'une cinquantaine de centimètres, il se déplace à une vitesse allant de 5 à 10 km/h, en évitant les obstacles grâce à ses capteurs embarqués. S'il détecte des personnes en mouvement ou des objets déplacés, il déclenche une alarme par Wi-Fi. Le télésurveilleur peut alors prendre la main sur la caméra embarquée pour effectuer une levée de doute et piloter l'engin manuellement. Sa caméra thermique détecte les points chauds, notamment une présence humaine. Après dix heures en continu, il se recharge automatiquement. Incroyable. ■

## LA BALISE GPS ANTIVOL

Elle est compacte, discrète et peut se dissimuler sous les palettes ou dans un véhicule pour lutter contre le vol de marchandises au sein des entrepôts ou des sites industriels. La balise GPS-GSM antivol LocBox a été conçue par la société Geotracer, spécialiste des technologies de géolocalisation. Le boîtier trace en continu à la fois les malfaiteurs et la marchandise. Sa version industrielle affiche une autonomie de dix ans. En mouvement, cela correspond à 20 000 transmissions GPS par réseaux GSM-GPRS. L'enveloppe



en polycarbonate renforcé offre une résistance aux chocs et une étanchéité totale. Le PC de télésurveillance réceptionnant les données de position pourra être alerté en cas de mouvement non autorisé ainsi que d'entrée ou de sortie dans des zones géographiques prédéfinies. ■



## LE DISPOSITIF ANTI-VOITURE BÉLIER

L'attentat commis dans l'usine d'Air Products à Saint-Quentin-Fallavier (Isère) l'été dernier, qui a vu l'employé d'un fournisseur projeter sa camionnette contre des bonbonnes de gaz, montre l'utilité de disposer de solutions d'interception de véhicule. La société Rigomer, spécialiste des obstacles anti-franchissement, notamment pour les bases militaires et les checkpoints, a mis au point un dispositif pour les sites industriels. Le prototype Ratel stoppe un véhicule de deux tonnes lancé à 60 km/h en huit mètres environ. Le produit est immédiatement réutilisable : il suffit de changer sa cartouche, une structure en aluminium architecturée en nid-d'abeilles qui lui confère sa résistance. Contrairement à un mur de protection, ce dispositif, qui pèse moins de 50 kg, peut être déplacé. ■



## LA DÉTECTION LOINTAINE

Détecter suffisamment tôt un véhicule menaçant s'approchant d'un site industriel sensible pour pouvoir réagir... Les responsables de la sûreté en rêvent. Thales a mis au point une solution combinant des caméras thermiques avec des radars terrestres de moyenne portée. Opérationnelles de jour comme de nuit, les caméras thermiques séduisent par leur performance et leur robustesse, notamment les militaires. Elles permettent de détecter un véhicule jusqu'à environ dix kilomètres de distance et d'en reconnaître le modèle à deux kilomètres. L'armée française utilise de tels équipements pour détecter, reconnaître, identifier et localiser des cibles, même dans des conditions dégradées (brouillard, vent de sable, face au soleil). ■

SUITE DE NOTRE ENQUÊTE P. 34 →





Entretien

# « LE NUMÉRIQUE CHANGE LA FACE DE LA SÉCURITÉ »

Selon **Alain Juillet**, le président du Club des directeurs de sécurité des entreprises, celles-ci ne mesurent pas les risques liés à leur sûreté. Et il déplore la baisse des budgets en situation de crise.

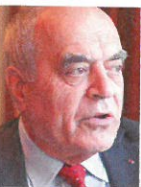
PROPOS RECUEILLIS PAR PASCAL GATEAUD ET HASSAN MEDDAH

Les attaques contre l'usine d'Air Products à Saint-Quentin-Fallavier (Isère) et la raffinerie LyonDellBasell de Berre-l'Étang (Bouches-du-Rhône) ont montré que les sites industriels peuvent être des cibles. Sont-ils suffisamment protégés en France ?

Le risque zéro n'existe pas. Quoi que vous fassiez, il peut toujours y avoir une faille. Qu'elle soit technique ou humaine... Quand de tels accidents surviennent, il faut s'interroger, savoir si cela aurait pu être empêché ou s'il n'y avait pratiquement rien à faire. Dans les deux cas, il y avait des failles. Qu'un ou plusieurs individus aient pu accéder à des cuves d'hydrocarbures pour y placer des explosifs, cela pose de vraies questions. C'est grave. Il y a un problème de sécurité à repenser. Dans l'affaire de l'usine d'Air Products, le contrôle à l'entrée a bien été effectué et le prestataire était habilité à entrer. Ensuite, il a eu un comportement imprévisible. Cela pose néanmoins le problème de la circulation interne dans l'entreprise.

Comment relever le niveau de sécurité des installations industrielles ?

L'entreprise doit se poser les bonnes questions et d'abord identifier les zones à risque. Est-ce que la sécurité de son site exige de protéger chacun de ces points sensibles ou le contrôle à l'entrée suffit-il ? Ensuite, elle doit définir le degré de sécurité à appliquer pour ces zones et le dispositif qui y répond : un portail, un système de contrôle d'accès par badge, des gardiens... Pour les organisations les plus critiques, il faut



**« Face à la menace terroriste, seuls les opérateurs d'importance vitale sont réellement préparés car ils ont été sensibilisés par l'État. »**



même envisager plusieurs contrôles d'accès ou des systèmes de blocage à l'intérieur du site pour prévenir et stopper les attaques. La contrepartie, c'est que cela va forcément coûter des moyens humains et matériels supplémentaires.

Peut-on réellement se prémunir des attaques terroristes ?

Il est quasiment impossible d'arrêter un type qui a fait le sacrifice de sa vie. Face à la menace terroriste, seuls les opérateurs d'importance vitale sont réellement préparés car ils ont été sensibilisés par l'État. Ils savent qu'ils sont des cibles et ont prévu les moyens de faire face à des attaques menées par des professionnels, même de type commando. La plupart des autres entreprises n'ont absolument pas conscience de ce type de risque et se satisfont généralement de mesures de base comme un contrôle d'accès, une clôture... En France, en période de crise, les investissements en matière de sécurité diminuent.

Faut-il s'alerter d'une telle situation ?

Paradoxalement, je suis optimiste car les nouvelles technologies, portées notamment par le numérique, sont en train de changer la face de la sécurité. Avant, dans une usine, des gardiens faisaient une ronde, en passant par des points précis, à des horaires précis. Ce système comportait des failles du fait des habitudes. Aujourd'hui, il y a des petits robots qui font des rondes aléatoires, qui regardent tous les recoins sans accuser la fatigue. Dans ce cas, la machine est bien plus efficace que l'individu.

La menace qui pèse sur les sites industriels a-t-elle changé de nature ?

Clairement. Aujourd'hui, les organisations criminelles peuvent gagner beaucoup plus ou faire beaucoup plus de dégâts avec beaucoup moins de risques. Mieux vaut s'emparer de l'ordinateur portable d'un ingénieur qui contient des secrets d'entreprise que braquer une banque. Il y a également un changement d'échelle. Dans les années 1980, les terroristes agissaient en petite équipe. Avec Al-Qaïda et Daesh, les soi-disant loups solitaires sont formés par centaines dans des camps d'entraînement puis téléguidés par internet. Avec les moyens techniques actuels, cela va plus vite et plus loin.

Le gouvernement a pris des mesures supplémentaires pour renforcer la protection des sites Seveso. A-t-il eu raison ?

C'est évident. Faire sauter un tel site peut avoir des conséquences importantes. Le gouvernement a donc très bien fait d'en renforcer la sécurité. On attend les résultats des audits lancés pour l'ensemble de ces sites. En théorie, les entreprises doivent être capables d'identifier seules les risques réels sur leurs activités et d'y apporter des réponses adaptées. Dans la pratique, certaines, pour des raisons économiques, ne vont pas faire les investissements nécessaires ou vont les différer dans le temps. C'est le rôle de l'État de faire pression pour qu'elles se mettent en ordre de bataille par rapport à ces problématiques.

Directive Seveso, plan Vigipirate, points d'importance vitale... N'y a-t-il pas trop de lois dans ce domaine ?

La sûreté n'échappe pas au mille-feuille juridique avec des lois qui s'ajoutent aux précédentes. Or ces lois ne prennent pas en compte la réalité d'aujourd'hui et s'opposent même parfois les unes aux autres. L'État n'a plus suffisamment de moyens ni de policiers pour assurer la sécurité des sites Seveso. Pourtant, il n'autorise pas les entreprises ou leurs prestataires à assurer la sécurité dans l'espace public autour de leur site. Il faut faire évoluer la loi. En Grande-Bretagne et aux États-Unis, on fait appel à des sociétés privées pour assurer la sécurité des sites à l'intérieur comme à l'extérieur. Ça marche très bien et ça coûte moins cher. Il va falloir que l'État délègue un certain nombre de responsabilités régaliennes aux entreprises spécialisées pour mieux répondre aux attentes de sécurité et de sûreté. Le consensus est général à ce sujet.

Au-delà des moyens financiers et de la technologie, la sûreté est surtout une question d'hommes...

Le profil des directeurs de sûreté a évolué du fait d'exigences plus fortes. Dans les grandes entreprises, certains siègent au comité de direction. Au départ, c'étaient d'anciens militaires ou gendarmes recrutés pour leurs facultés à gérer des équipes. La sûreté se limitait alors essentiellement à du gardiennage. Depuis quelques années, on assiste à la montée en puissance d'ingénieurs recrutés en interne comme responsables de sûreté. Ils sont les mieux armés face aux menaces liées aux nouvelles technologies, notamment les cyberattaques à des fins de sabotage industriel. C'est un risque majeur dans les années qui viennent. ■

PAGE SUIVANTE  
DCNS en lice pour  
le contrat du siècle

PASCAL GUITTET



SECURISEZ VOS ECHELLES FIXES !

Matériels conformes aux normes NF E 85-012 et EN 14122-4



Version acier galvanisé et aluminium Verrouillage cadenas ou serrure

- TOITURES
- MACHINES
- PONTS ROULANTS
- GALERIES TECHNIQUES
- PORTIQUES
- SIGNALISATIONS ROUTIERES
- RESERVOIRS
- SILOS
- CHATEAUX D'EAU
- PYLONES



Système à fermeture automatique et déverrouillage d'urgence en issue de secours



Les échelles fixes représentent des accès à des zones de danger dont vous devez interdire l'utilisation au public et à toute personne non habilitée (art. R.4224-20 et R.4224-4 du Code du Travail).

COUTIER INDUSTRIE vous propose toute une gamme de solutions industrielles et normalisées adaptables sur tout type d'échelle.

Dominique LANG  
☎ 03 82 86 84 00  
☎ 03 82 86 04 44  
✉ coutierindustrie@coutier-industrie.fr

COUTIER INDUSTRIE  
Parc d'activités Unicom - Rue Ampère  
57970 BASSE-HAM  
www.coutier-industrie.fr



L'INFORMATION DE RÉFÉRENCE  
DES PROFESSIONNELS DE L'INDUSTRIE

ABONNEZ-VOUS  
**285** € TTC  
1AN



PRINT  
L'HEBDOMADAIRE  
+ LES NUMÉROS  
SPÉCIAUX  
+ LE GUIDE  
DE L'INGÉNIEUR

DIGITAL  
L'HEBDOMADAIRE  
SUR IPAD, MAC ET PC  
+ ACCÈS À LA BASE DE  
DONNÉES INDUSTRIE  
EXPLORER  
+ LE WEB ABONNÉ  
+ CHAQUE SEMAINE  
PAR E-MAIL L'ACTUALITÉ  
DES USINES EN RÉGIONS

Retrouvez toutes nos offres sur  
[www.usinenouvelle.com](http://www.usinenouvelle.com)