

VIDÉO PROTECTION L'INTERO- PÉRABILITÉ EST UNE LONGUE ROUTE

“ L' ”

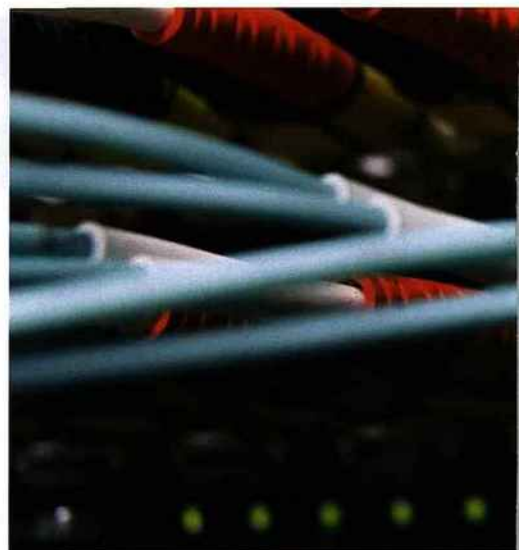
époque des systèmes analogiques de vidéoprotection, où on pouvait brancher n'importe quelle caméra sur n'importe quel autre équipement, et cela fonctionnait, rappelle Sylvie Gauthier, responsable des ventes chez Honeywell France. Bref, la vidéoprotection était ouverte, compatible et interopérable... Mais dans un circuit en boucle fermée. Depuis près de dix ans, les technologies Internet Protocol (IP) ont transformé caméras, enregistreurs et systèmes de stockage en véritables ordinateurs communiquant sur les réseaux Ethernet. Bonne nouvelle « on peut partager l'information en mutualisant les équipements. Ainsi, une même caméra peut-elle être visualisée par des centaines d'utilisateurs », souligne Laurent Scetbon, responsable marketing Europe du distributeur Aasset Security. Mauvaise nouvelle, la vidéoprotection tombe dans les mêmes travers que l'informatique. Formats de données propriétaires incompatibles entre eux, incessantes mises à jour logicielles, obsolescence accélérée des équipements... Il en résulte un réel manque d'interopérabilité.

OBJECTIF : FACILITER LE TRAVAIL DES ENQUÊTEURS

Ce qui ne fait l'affaire ni des grands comptes (ADP, RATP, SNCF...), ni des forces de l'ordre ni de la justice. Autrement dit, les utilisateurs réclament l'interopérabilité entre la caméra, le Network Video Recorder (NVR), le Video Management System (VMS), la baie de stockage et les logiciels spécifiques (pilotage de murs d'écran, analyse et traitement d'images). « S'il survenait un grave accident ou un attentat à la station de RER Châtelet-les-Halles ou à la gare du Nord à Paris, les forces de l'ordre et de la justice récupéreraient de longues heures d'enregistrements provenant de nombreuses caméras de marques différentes », indique Dominique Legrand, président de l'Association nationale de la vidéoprotection (AN2V). « Soit autant de formats de fichiers vidéo propriétaires réclamant visionneuses et codecs spécifiques installés sur l'ordinateur. » Pourtant, en France, un arrêté d'août 2007 impose que les vidéos collectées par l'État puissent être exploitées par les enquêteurs. « Cette exigence porte sur la qualité des images et sur les détails de la localisation de la scène. En pratique, on s'aperçoit que les systèmes de vidéoprotection produisent des données dans des formats différents », confirme Jean-François Sulzer, coordinateur du groupe de travail WG5 au sein du comité technique TC223 de l'International Standard

LE PASSAGE DE L'ANALOGIQUE AU NUMÉRIQUE A CRÉÉ DES FORMATS PROPRIÉTAIRES DE DONNÉES ET DE MÉTADONNÉES. CE QUI GÊNE LE TRAVAIL DES FORCES DE L'ORDRE DURANT LEURS ENQUÊTES. DES ALLIANCES INDUSTRIELLES, COMME L'ONVIF ET LA PSIA, ONT COMMENCÉ À Y REMETTRE DE L'ORDRE. TRÈS PARTIELLEMENT.

PAR ERICK HAEHNSEN



Organisation (ISO) qui développe la norme internationale, ISO22311 en la matière, dont la promulgation est prévue en 2013. « Bien sûr, cette hétérogénéité met des bâtons dans les roues des enquêteurs. »

LA CACOPHONIE DES FORMATS

On s'en doute, les services de vidéoprotection s'organisent pour gérer l'hétérogénéité des systèmes. Notamment en mettant à jour tous les logiciels et drivers de périphériques nécessaires. « Mais il manque toujours quelque chose », reconnaît le président de l'AN2V. Par exemple, l'encodage de l'horodatage de telle caméra sera dans l'image. Tandis qu'avec la génération suivante, cet encodage peut soudain se retrouver dans les métadonnées. Dont les formats sont, à leur tour, susceptibles de subir des modifications à l'occasion d'une mise à jour du logiciel... Ce qui pénalise considérablement la relecture, le traitement et l'analyse non seulement des images mais de plus en plus des métadonnées. Pourquoi une telle cacophonie? « Les fabricants sont des développeurs de matériels, pas de logiciels, contrairement à Mobotix », estime Patrice Ferrant, directeur commercial et développement de MobotixG pour la France, le Maghreb et l'Afrique francophone.

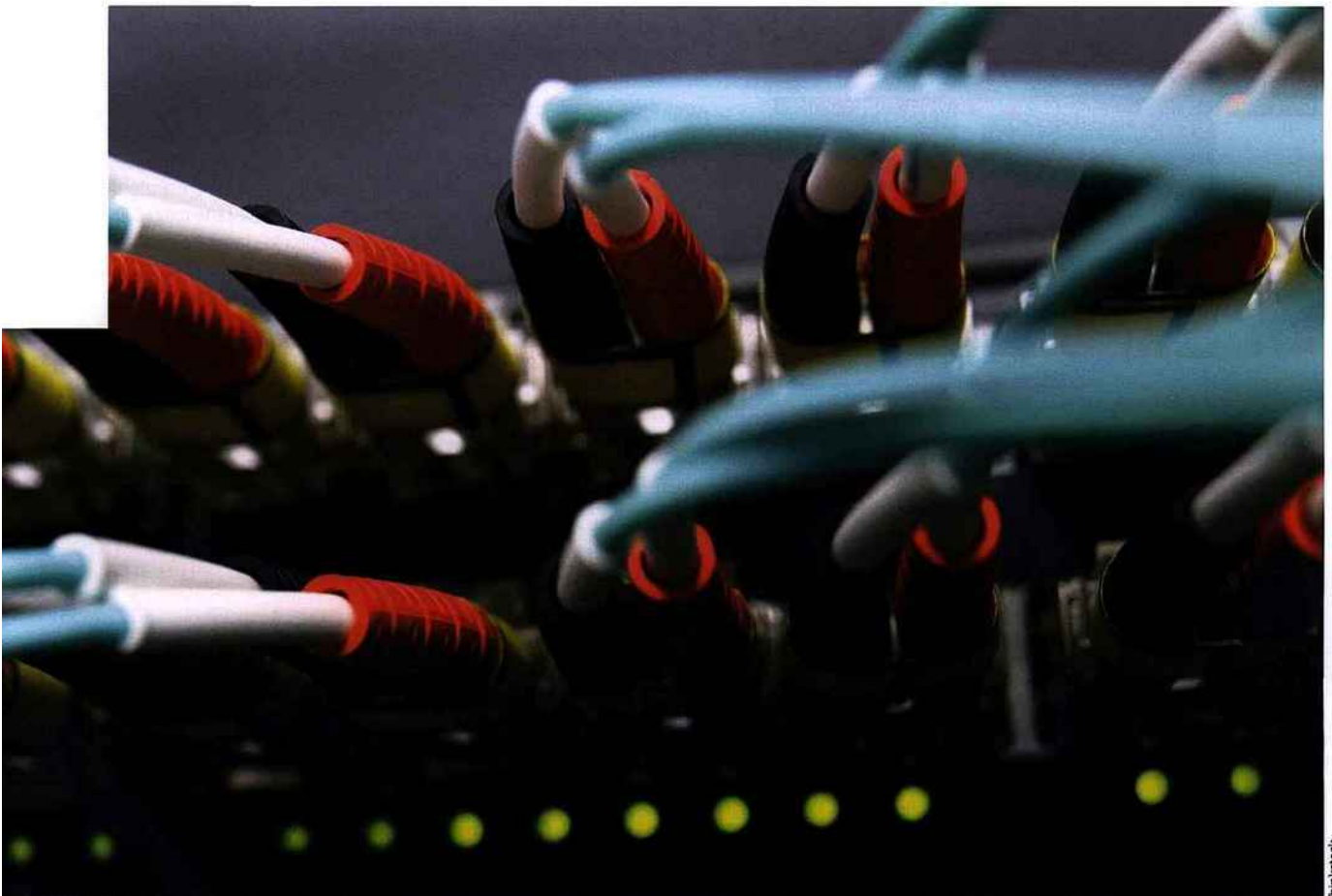
VERS DES STANDARDS INTERNATIONAUX

Cependant, MobotixG montre, depuis 1999, la voie de l'interopérabilité en misant sur le standard de connectivité RFC93 (Request for Comments), qui définit le dialogue inter-équipement au sein du protocole TCP/IP. Ainsi que sur les protocoles Common Internet File System (CIFS) et Server Message Block (SMB) pour le transfert de données et

le partage de fichiers sur le réseau. « Avec ces trois protocoles, n'importe quel ordinateur, serveur ou disque Network Attached Storage (NAS) peut dialoguer en connectivité et en transfert de données avec une de nos caméras », reprend Patrice Ferrant. « La plupart des constructeurs respecte également les standards du streaming vidéo », explique Jean-François Sulzer qui, à cet égard, pense aux protocoles Real-time Transport Protocol (RTP) et Real-time Transport Control Protocol (RTCP). En fait, les enjeux de l'interopérabilité varient considérablement selon le point de vue des différentes parties prenantes. Côté forces publiques, l'interopérabilité devrait s'appuyer sur une base technologique permettant de connecter deux produits de marque différente et d'échanger données et métadonnées afin de les exploiter facilement et de retrouver délinquants, criminels ou terroristes.

DU COUP, LES ETATS VOUDRAIENT SE REPOSER SUR DES NORMES INTERNATIONALES

« Quant aux constructeurs, ils se veulent compatibles afin de décrocher de nouveaux marchés – ou de s'accaparer les extensions de marchés jusqu'ici tenus par leurs concurrents. Ensuite, ils rajoutent des innovations "propriétaires" (tracking, renvoi d'alarme, métadonnées spécifiques...) pour verrouiller leurs marchés », décrypte Dominique Legrand de l'AN2V. « Généralement, il faut installer des caméras supplémentaires quelques mois après un grand déploiement. Evidemment, ce ne sont plus les mêmes », commente Garry Goldenberg, président d'Open IP Vidéo, un laboratoire de test d'interopérabilité qui, avec une trentaine d'acteurs, travaille sur l'acquisition des images et du son



ainsi que sur le transfert, le traitement, la visualisation, le stockage et l'analyse des données. Sans oublier les relations avec les environnements connexes (contrôle d'accès, alarme, incendie). « Dans ce contexte, la norme est le seul organe stabilisateur. » Enfin, de leur côté, « les éditeurs de logiciels applicatifs sont également pénalisés car ils sont obligés d'intégrer la librairie de spécifications techniques de chaque équipement », précise Pierre-François Verbecque, directeur commercial de l'activité VideoSecurity de Sony Professional France. « En même temps, ils ont peur de voir se développer la concurrence. Il est vrai que l'interopérabilité facilite l'accès des nouveaux venus sur le marché. De fait, depuis 2008, on compte deux fois plus d'éditeurs. »

DES ALLIANCES INDUSTRIELLES

Reste qu'Axis, Bosch et Sony ont voulu rationaliser le secteur dès 2008 en lançant l'initiative Open Network Video Interface Forum (Onvif). Laquelle réunit 350 constructeurs et éditeurs de logiciels. « Avant l'Onvif, chaque acteur devait prendre le Software Development Kit (SDK) d'un constructeur pour exploiter le flux de la caméra. Avec l'Onvif, deux produits labellisés se reconnaîtront sur le réseau », poursuit Pierre-François Verbecque. Le constructeur japonais pratiquait déjà une stratégie de compatibilité. « Depuis longtemps, nous envoyons les SDK et les prototypes des caméras aux acteurs de notre écosystème, soit environ 200 entreprises trois à six mois avant la sortie de chaque nouveau produit. De cette manière, nos nouveautés sont déjà reconnues, dès qu'elles sortent sur le marché. Pour cette raison, nous avons remporté de très gros projets », confie Pierre-François Verbecque. Parmi les initiatives industrielles de standardisation, signalons également la PSIAlliance (PSIA). « L'Onvif et PSIAlliance travaillent au niveau mondial. Néanmoins l'Onvif est plus reconnue au niveau européen tandis que PSIA l'est dans d'autres pays. Bien sûr, nous sommes dans les deux consortiums », indique Sylvie Gauthier, de Honeywell France.

Dominique Legrand (à gauche), président de l'Association nationale de la vidéoprotection (AN2V). Garry Goldenberg (à droite), président d'Open IP Vidéo.



Le but de ces forums industriels vise à ce que tous les futurs équipements intègrent, en plus de leur couche propriétaire, la couche PSIA ou Onvif (100 produits seraient ainsi labellisés). Cette dernière contient plusieurs protocoles de reconnaissance de matériel sur le réseau, de réglage de la caméra (PTZ, balayage, élévation, zoom), du codage audio et vidéo de la caméra, de télémétrie (pilotage de la caméra à distance)... « Il y a aussi des sous-protocoles d'analyse intelligente de la caméra ou de l'encodeur qui permettent d'interpréter l'apparition ou la disparition d'objets, le franchissement d'une frontière virtuelle, le comptage des personnes dans une scène, la détection d'une personne qui reste trop longtemps dans une scène » précise le représentant de Sony. « Les détections restent propriétaires, mais une solution d'enregistrement aura les moyens d'accéder à l'intelligence de la caméra. »

DE SIMPLES LISTES DE COMPATIBILITÉ

Mais alors où en est l'interopérabilité en vidéoprotection ? « Elle est toute relative ! A l'Onvif, par exemple, il y a des listes de compatibilités entre une caméra (Axis, Bosch, Cisco, Honeywell, LG, Panasonic, Siemens, Sony...) et un NVR [Cossilys] Milestone, Indigo Vision...) ou un logiciel de VMS installé sur PC (Aimetis, CASD, Genetec, eProcess, Honeywell, Milestone, Teleste, Thales...), détaille Patrice Ferrant. « Plus exactement, l'interopérabilité se fait entre une caméra et un NVR. Ou bien une caméra et un logiciel. Elle ne concerne pas les caméras entre elles ni les NVR entre eux ni les logiciels entre eux. » On parle alors de « listes d'interopérabilités » qui, en fait, sont des « listes de compatibilités ». « En associant une caméra IP Honeywell à un système vidéo Honeywell, l'utilisateur peut gérer toute l'intelligence offerte par la caméra comme la détection de mouvement, la fonction sabotage (masquer la caméra avec la main ou un spray envoie une alarme à l'enregistreur) », souligne Sylvie Gauthier qui plaide pour l'interopérabilité au sein du même constructeur, lequel pense la concrétiser grâce au superviseur Win-Pak, associé à la centrale d'alarme Galaxy. « Si on utilise une caméra tierce, on n'intègre que les flux vidéos. »

Au final, l'Onvif, la PSIA et même la norme Iso 22311 ne répondront que très partiellement aux besoins d'interopérabilité. « 30% à 40% des fonctionnalités avancées resteront propriétaires car il sera trop complexe de normaliser les fonctions les plus avancées », complète Pierre-François Verbecque. A cela s'ajoute le manque de maturité du secteur. « A l'Onvif, les spécifications sont passées de la version 1.0 à la version 2.1 en à peine dix-huit mois », rappelle Garry Goldenberg. « Et encore ! Si une caméra et un enregistreur sont labellisés Onvif 1.2, il est vraisemblable qu'ils seront compatibles et interopérables sur les fonctions de base. Il faudra quand même vérifier cette compatibilité par des tests. » Sage recommandation.

UNE NORME ISO POUR 2013

► Ce projet de norme internationale porte sur les données vidéo et certaines de leurs métadonnées. Le texte, en cours de traduction, va bientôt faire l'objet d'une enquête publique par l'Afnor en France.

Les constructeurs préparent les normes internationales IEC 2676-1 et 2 qui regroupent les standards de l'Onvif et de la PSIA. Objectif remplacer un équipement de vidéoprotection par un autre qui présente à peu près les mêmes fonctions. « Pour autant, ces normes ne garantissent pas le format des données et métadonnées enregistrées », souligne Jean-François Sulzer, coordinateur du projet de norme de vidéoprotection ISO 2311. Laquelle cherche à faciliter le travail d'enquête des forces de l'ordre et de la justice.

« Le projet ISO 2311 reprend le format H264 d'échange de données vidéo de la norme MAF (en cours de révision). Et côté métadonnées, des formats de la SMPTE (organisme de normalisation de la vidéo et du cinéma du broadcast) pour définir avec précision la localisation de chaque scène », précise Jean-François Legendre, responsable de développement à l'Afnor. « Même en sous-sol, renchérit Jean-François Sulzer. Il faudra que tous les systèmes utilisent la même horloge de temps universel. Aujourd'hui, ce n'est pas le cas. Par ailleurs, la norme veut s'assurer que chaque source d'image est bien définie de façon unique pour éviter que deux caméras s'appellent de la même manière. » Enfin, dans les systèmes comportant un grand nombre de caméras de marques différentes, la norme veut proposer de décrire sous forme d'arborescence XML la façon avec laquelle sont rangés les flux vidéo dans les enregistrements... « La norme en est au stade de Draft of International Standard (DIS). Nous la traduisons afin de lancer, au travers de l'Afnor, une enquête publique en France auprès de tous les acteurs concernés », poursuit Jean-François Sulzer. « Le texte en français sera disponible dans les prochains jours. Quant à la norme, elle devrait être promulguée en 2013. »



En matière d'interopérabilité, 30 à 40 % des fonctionnalités avancées restent propriétaires. © Thinkstock

L'interopérabilité se fait entre une caméra et un NVR. Ou bien une caméra et un logiciel. Elle ne concerne pas les caméras entre elles, ni les NVR entre eux, ni les logiciels entre eux.



Le système Win Pak Galaxy de Honeywell.
© Honeywell