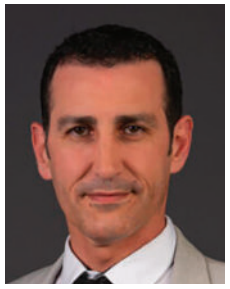


DAVID DURAN

DIRECTEUR OFFRE SÛRETÉ, IT
ET SÉCURITÉ ÉCONOMIQUE

formind

Voir la présentation détaillée de cette entreprise en **page 187**

# LA SÛRETÉ DES LIEUX : **QUELS FUTURS ENJEUX** POUR LA VIDÉOPROTECTION ?

STRATÉGIE

## INTRODUCTION

La vidéoprotection, ou surveillance vidéo, joue un rôle essentiel dans la sécurité publique et privée. L'intégration de l'intelligence artificielle (IA) et des technologies avancées dans les systèmes de vidéoprotection représentent une transformation majeure de la surveillance, améliorant l'efficacité, la précision et l'efficience des opérations de sécurité. Alors que les technologies continuent de progresser à un rythme rapide, les enjeux futurs de la vidéoprotection se dessinent avec clarté, révélant des défis d'envergure et des opportunités significatives.  Voici une analyse des principaux enjeux auxquels cette industrie devra faire face dans les années à venir.

## POURQUOI S'ÉQUIPER D'UN SYSTÈME DE VIDÉOPROTECTION ET DE SÛRETÉ EN GÉNÉRAL ?

La sûreté électronique, et plus particulièrement la vidéoprotection, est un moyen efficace pour assurer une sécurité supplémentaire. Celle-ci est un élément incontournable des politiques de sûreté publiques et privées, la brique de détection et de levée de doute d'un système de sûreté.
La vidéoprotection est ainsi devenue une nécessité et permet une assistance électronique de rigueur pour l'ensemble des forces exploitants ces solutions. La protection des biens et des personnes par le biais de la vidéoprotection est aujourd'hui l'affaire de tous et fait partie intégrante de la vie de chacun avec les systèmes de vidéoprotection urbains.
Elle peut toutefois être intrusive et perturber le droit à la vie privée des citoyens si elle est mal utilisée.
D'où l'intérêt de s'adresser à un professionnel qui saura prendre en considération les besoins de visualisation, les besoins et les contraintes d'exploitation sans oublier les exigences règlementaires et normatives.



## QUELS SONT LES ENJEUX (installation, autorisation d'installation, cybersécurité, protection de la donnée personnelle, autres…) ?

Au-delà d'une réponse opérationnelle et organisationnelle, l'implémentation d'un système de vidéoprotection requiert obligatoirement une attention sur les prérequis de l'ensemble de la chaîne.
En effet, des questions techniques des services DSI et RSSI, en passant par le service DPO, devront impérativement être prise en compte dès la conception du système.

### Les mesures critiques

Parmi ces enjeux de mesures critiques, nous pouvons citer la cybersécurité, qui engage les OIV (Organisme d'Importance Vitale), les sites sensibles mais aussi les collectivités, ainsi que la protection des données personnelles (RGPD).
Dans ces cas majeurs, les menaces et les vulnérabilités pèsent sur le fonctionnement direct du système, sur une prise de contrôle des caméras par une personne mal intentionnée et sur la compromission des données personnelles et sensibles.

### Les mesures de sécurité techniques

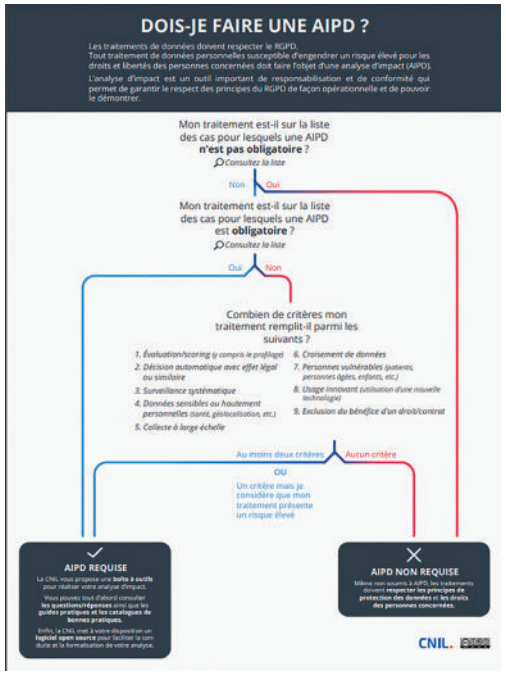
Des mesures de sécurité techniques doivent être prises en compte dès la conception pour palier aux vulnérabilités terrain et logicielles.
Le chiffrement des données, l'authentification et le contrôle d'accès réseau en passant par la segmentation de celui-ci sont des pratiques qui empêchent les attaquants d'accéder facilement à l'ensemble du réseau en cas de compromission d'un dispositif ou d'un segment.

### Les mesures de sécurité organisationnelles

De même que les mesures de sécurité techniques, les mesures de sécurité organisationnelles sont des points prépondérants à l'intégration d'un système de vidéoprotection pour sa pérennité.
Des politiques de sécurité et des sessions de formation et sensibilisation seront à mettre en œuvre pour aider à prévenir les erreurs humaines qui pourraient compromettre cette sécurité.
Des audits réguliers et des évaluations de sécurité permettront de détecter et de corriger les failles de sécurité avant qu'elles ne soient exploitables et exploitées. Ces audits et ces évaluations peuvent être menés en interne ou par des tiers pour garantir une appréciation objective.

### Protection de la vie privée

Anonymisation et pseudonymisation permettent de minimiser les risques pour la vie privée des individus et des citoyens visualisés. Ces techniques rendent les données moins identifiables tout en conservant leur utilité pour l'analyse et la surveillance. La collecte et le stockage des données doivent être limités à ce qui est strictement nécessaire pour les objectifs de la vidéoprotection.




De même, clarté, communication et éventuellement consentement sont essentiels pour garantir la transparence et la confiance du public. Les politiques de confidentialité doivent être clairement communiquées et facilement accessibles.

## COMMENT S'INTÉGRER SUR UN SYSTÈME D'INFORMATION (SI) ET ÊTRE INTEROPÉRABLE ?

**Intégration d'un système de vidéoprotection**

L'intégration des systèmes de vidéoprotection sur un(des) système(s) d'information est l'un des aspects essentiels pour sécuriser les infrastructures de l'entité et ainsi maximiser l'efficacité, la coordination et la valeur ajoutée des technologies de surveillance. Ces concepts permettent aux divers éléments de fonctionner ensemble de manière cohérente et efficace, facilitant ainsi la gestion centralisée, l'analyse des données, la maintenance et la réponse aux incidents.

**Intégration des éléments d'un système de vidéoprotection**

Au-delà de la complexité de conception sur l'intégration des éléments de la chaîne de vidéoprotection avec le partage de certains services (antivirus, authentification réseau, etc.), les éléments suivants doivent être prévus en fonction des exigences et des contraintes globales.

Caméras et Capteurs : les systèmes de vidéoprotection modernes utilisent une variété de caméras (fixes, PTZ, thermiques) associées à des applicatifs d'analyse d'images. L'intégration de ces dispositifs permet de couvrir un large éventail de scénarios de surveillance et de répondre à différents besoins de sécurité.

Des obligations de MCS (Maintien en Conditions de Sécurité) pourraient avoir une incidence majeure sur les investissements si le LTS (Long Term Support) n'est pas pris en compte dès la conception.

Serveurs et Stockage : les dispositifs de capture doivent être intégrés avec des solutions de stockage robustes et évolutives. Les serveurs doivent être capables de traiter et de stocker de grandes quantités de données vidéo en temps réel, tout en garantissant l'accès rapide aux enregistrements et la réponse aux règlementations (chiffrement, accès et traçabilité).

Logiciels de Gestion Vidéo (VMS) : ces systèmes de gestion vidéo jouent un rôle central dans l'intégration des différents composants de vidéoprotection. Ils fournissent des interfaces utilisateur pour la surveillance en temps réel, la gestion des enregistrements, et l'analyse des données. Un VMS efficace doit être capable d'interagir avec divers types de caméras et capteurs, ainsi que de s'intégrer dans une politique de maintenance standardisée et pérenne.

**Interopérabilité entre différents systèmes**

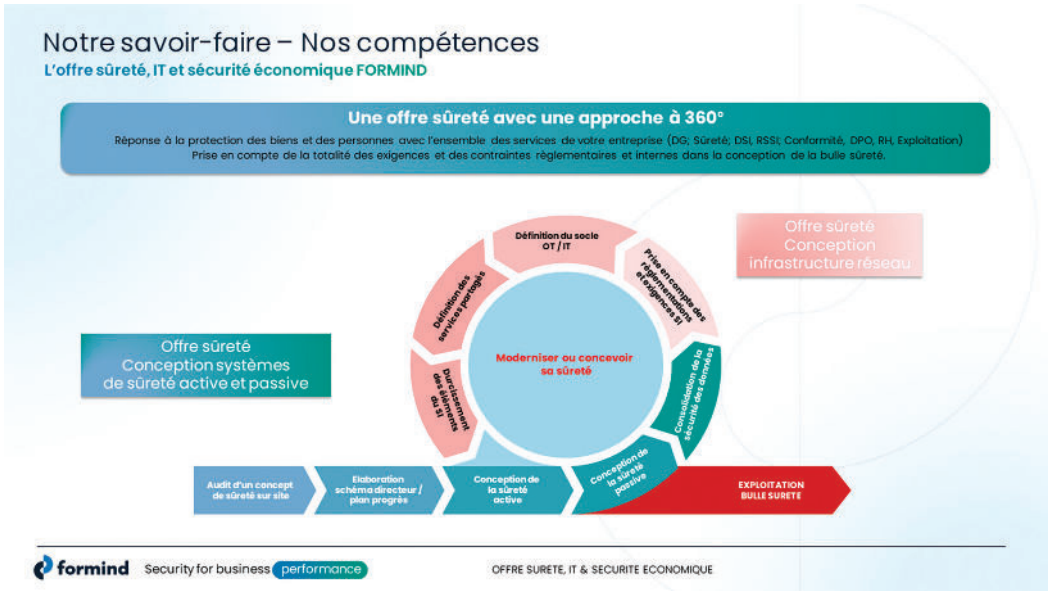
L'utilisation de protocoles de communication standardisés et de systèmes interfacés nativement est cruciale pour assurer l'interopérabilité entre les différents composants et systèmes de sûreté.

Ainsi, les interfaces de programmation d'application permettent aux systèmes de vidéoprotection de s'intégrer avec d'autres systèmes de sécurité et de gestion, tels que les systèmes d'hypervision et de supervision, de contrôle d'accès et autres systèmes de gestion des bâtiments.

**Avantages de l'intégration et de l'interopérabilité**

Une intégration conçue en amont du déploiement permet d'obtenir à la fois un système robuste en termes de cybersécurité, un taux de disponibilité haut et, de ce fait, une exploitation répondant aux besoins.






Les solutions intégrées permettent une gestion centralisée et simplifiée des systèmes de sécurité. Les opérateurs peuvent surveiller et contrôler plusieurs systèmes à partir d'une interface unique, réduisant ainsi la complexité et les erreurs humaines.

L'intégration des systèmes de vidéoprotection avec d'autres systèmes de sécurité permet de créer des solutions complètes, homogènes et cohérentes.

**Défis de l'intégration sur un SI**

La compatibilité entre les dispositifs de différents fabricants et les procédures et attentes informatiques de l'entité peut poser plusieurs défis. Il est essentiel de s'assurer que les composants choisis respectent les standards de communication et de sécurité exigés par les services DSI et RSSI (exigences règlementaires ou internes).

Il est indispensable de s'assurer dès la conception du système de vidéoprotection et autres systèmes de sûreté que les différents points d'intégration répondent aux normes et attentes en vigueur et soient protégés contre les actes malveillants.

L'intégration de systèmes sur un socle SI, existant ou à créer, peut introduire des vulnérabilités de sécurité. Il est primordial que les systèmes choisis respectent les normes et règlements en vigueur et soient sécurisés de toutes failles et vulnérabilités connues et éventuellement à venir.

Il est donc obligatoire de s'assurer de disposer de compétences techniques et de ressources adéquates (internes ou externes avec un professionnel) pour gérer et concevoir les systèmes de manière efficace, sécurisée et pérenne.

## CONCLUSION

Les enjeux futurs de la vidéoprotection sont vastes, complexes et d'envergure, nécessitant une expertise complète et minutieuse pour répondre aux défis technologiques, sécuritaires, éthiques et sociaux.

L'évolution de cette industrie dépendra de la capacité des acteurs à innover tout en respectant les régulations et en gagnant la confiance du public. En somme, la vidéoprotection de demain pourra être plus intelligente, plus sécurisée, et plus respectueuse des droits individuels, jouant un rôle central dans les scénarios de sécurisation des lieux installés.

FORMIND peut vous accompagner sur l'ensemble de la chaîne de valeur, de la conception au durcissement des éléments en passant par la sensibilisation et la formation.

## QUESTIONS LES PLUS FRÉQUENTES

**Quels sont les futurs investissements en sûreté dans les années à venir ?**
Les investissements programmés en termes de sûreté pour les entités se concentrent sur le contrôle d'accès, la vidéoprotection, les outils liés à la cybersécurité et enfin la détection d'intrusion.

**Quelles sont les règlementations étroitement liées à la sûreté ?**
L'évolution de la sûreté liée à la cybersécurité ouvre la porte à certaines règlementations qui doivent s'appliquer de façon obligatoire. Chaque entité, suivant son activité, peut être assujettie à ces règlementations :
LPM ; II901 ; NIS & NIS 2 ; ISO 27001 ; Guides de l'ANSSI ; Directive Police & justice (RGPD appliqué aux supplétifs de police).

**La sûreté peut-elle être associée à des mesures RSE ?**
Oui.
Certains points, plus particulièrement en sûreté passive, ont évolué et permettent aujourd'hui de réaliser des économies d'énergie.
La sûreté, et plus particulièrement la vidéoprotection, peut s'associer / s'interfacer avec des systèmes de smart building / smart city et être fédérée avec un système BOS (Building Operating System) pour mutualiser les flux d'informations entre les capteurs du terrain et les applications systèmes.