WHITEPAPER

SIRAM OCR7 LPR ET LA CYBERSÉCURITÉ DANS LES SYSTÈMES LPR MODERNES

La cybersécurité d'un système LPR ne consiste pas à l'isoler du réseau, mais à le concevoir pour qu'il puisse se connecter de manière sécurisée, être mis à jour de façon contrôlée, gérer les vulnérabilités et maintenir sa disponibilité tout au long de son cycle de vie.

SOMMAIRE

1. INTRODUCTION

Les systèmes LPR ont évolué, passant de simples moteurs de reconnaissance de plaques d'immatriculation à des composants critiques des infrastructures de parkings, des villes intelligentes, des installations industrielles, des ports, des aéroports et des centres logistiques. Dans tous ces environnements, la disponibilité du service est tout aussi importante que la précision de la reconnaissance.

Pendant de nombreuses années, le choix d'un système LPR s'est presque exclusivement fondé sur son taux de reconnaissance, sa vitesse de lecture, ses performances de nuit ou son comportement dans des conditions difficiles. Tous ces critères restent essentiels : personne ne souhaite disposer d'un système incapable de lire correctement une plaque d'immatriculation. Toutefois, le marché commence désormais à poser des questions qui, il y a encore peu de temps, étaient rarement abordées lors des discussions techniques : comment le firmware des caméras est-il mis à jour ? Que se passe-t-il lorsqu'une vulnérabilité est découverte ? Comment les communications sont-elles protégées ? Pendant combien de temps le système sera-t-il pris en charge ? Qui garantit que l'installation restera sécurisée dans cinq ou dix ans ?

La raison est simple : un système LPR moderne n'est plus seulement une caméra ni uniquement un algorithme OCR. Il s'agit d'un ensemble de dispositifs connectés qui contrôlent les accès physiques et échangent des informations avec des plateformes de gestion, des systèmes de paiement, des applications cloud et d'autres services d'entreprise. C'est pourquoi il ne suffit plus aujourd'hui qu'un système fonctionne correctement le jour de sa mise en service : il doit être conçu pour se protéger, être mis à jour et rester opérationnel tout au long de son cycle de vie.

Ce document présente la vision d'Innova en matière de cybersécurité appliquée à OCR7 et explique comment la combinaison d'OCR7, de SCAP, des caméras Axis et des services Access et Alarm permet de construire une architecture prête à relever les défis de ce nouvel environnement.

2. CYBERSÉCURITÉ DES SYSTÈMES LPR

Un système LPR contrôle les accès physiques et interagit avec des barrières, des plateformes PMS, des systèmes de paiement, des solutions VMS et des services d'entreprise. Une vulnérabilité n'affecte plus uniquement la lecture des plaques d'immatriculation : elle peut compromettre la continuité des opérations, modifier des configurations critiques, bloquer une voie de circulation ou devenir un point d'entrée vers d'autres réseaux.

Parmi les risques les plus importants figurent les suivants :

Risque	Description
Manipulation des configurations	Modifications non autorisées des paramètres critiques du système
Ouverture ou blocage non autorisé des accès	Contrôle non autorisé des barrières ou des points de passage
Indisponibilité des dispositifs	Caméras ou services hors service interrompant le fonctionnement de l'installation
Exploitation de vulnérabilités connues	Exploitation de failles déjà publiées et non corrigées à temps
La caméra comme point d'entrée vers le réseau	La caméra est utilisée comme point d'accès à d'autres systèmes d'entreprise
Firmware ou logiciel non autorisé	Installation de versions non vérifiées ou malveillantes

Dans les installations distribuées, ces risques se multiplient en outre en l'absence d'une visibilité centralisée sur l'état des équipements.

C’est pourquoi la cybersécurité doit être considérée comme une exigence fonctionnelle du système et non comme une caractéristique supplémentaire. Dans un environnement de parking, de logistique, d’industrie ou d’infrastructure critique, la disponibilité du service fait partie intégrante de la sécurité. Un système parfaitement protégé d’un point de vue cryptographique perd toute valeur si un incident empêche le fonctionnement des accès. La sécurité ne doit pas se limiter à la protection des informations ; elle doit également contribuer à assurer la continuité opérationnelle du service.

3. PRINCIPES DE CONCEPTION D’OCR7

OCR7 est développé selon une approche Security by Design. Cela signifie que l’authentification, le contrôle des accès, la protection des communications, la journalisation des événements et la capacité de mise à jour font partie intégrante de l’architecture dès le début du développement. Ces mécanismes ne sont pas ajoutés a posteriori comme des éléments externes, mais déterminent la manière dont le système est conçu, déployé et maintenu.

Cette approche est complétée par le principe Secure by Default : des configurations initiales conçues pour réduire les risques, limiter les services inutiles et faciliter une mise en service plus maîtrisée. En pratique, cela aide l’intégrateur à éviter des erreurs courantes, telles que laisser des services ouverts, partager des identifiants entre plusieurs utilisateurs ou maintenir des équipements avec des versions obsolètes du firmware.

L’objectif n’est pas uniquement de protéger OCR7 le jour de son installation, mais de permettre à l’installation de rester sécurisée tout au long de son cycle de vie. Pour cela, la traçabilité des modifications, la gestion des profils, la possibilité de mettre à jour les versions et la réduction de la surface d’attaque sont des éléments essentiels.

4. CONNECTIVITÉ SÉCURISÉE : ACCESS & ALARM

Par le passé, il était courant de considérer qu'un système sécurisé était un système totalement isolé d'Internet. Aujourd'hui, cette affirmation n'est plus valable pour de nombreuses installations : la gestion à distance, la supervision centralisée, les mises à jour continues et l'exploitation des services cloud apportent une valeur opérationnelle considérable lorsqu'elles sont mises en œuvre de manière sécurisée.

La question n'est plus de savoir si un système est connecté, mais comment il l'est. Les communications doivent s'effectuer au moyen de canaux authentifiés et chiffrés, en limitant l'accès aux seuls services strictement nécessaires et en appliquant le principe du moindre privilège. Une caméra connectée de manière contrôlée à Access ou Alarm n'est pas comparable à une caméra exposée à Internet sans aucune protection.

Access Cloud permet de centraliser la gestion d'installations distribuées et d'offrir un accès distant sécurisé. Alarm Cloud complète cette architecture en assurant une supervision continue de l'état opérationnel et de maintenance des équipements. Ensemble, ces plateformes permettent de faire évoluer une installation isolée et difficile à maintenir vers une infrastructure connectée de manière sécurisée et administrable sur le long terme.

5. SÉCURITÉ CONTINUE AVEC SCAP ET ALARM

SCAP, le module SIRAM Camera Application Platform, permet de standardiser le déploiement et la maintenance des applications sur les caméras Axis. Sa valeur ne réside pas uniquement dans la simplification de l'installation, mais aussi dans la réduction de la variabilité opérationnelle : moins de procédures manuelles, moins de configurations improvisées et un meilleur contrôle des versions logicielles installées sur chaque équipement.

La sécurité ne s'arrête pas une fois la mise en service terminée. Au cours des années suivantes apparaîtront de nouvelles versions du firmware, des mises à jour d'OCR7, des vulnérabilités connues, des certificats arrivant à expiration, des évolutions de l'infrastructure réseau ainsi que des équipements atteignant leur fin de support. Maintenir une installation sécurisée nécessite donc une gestion continue, et non une simple configuration initiale.

Dans ce contexte, Alarm évolue d'une plateforme de supervision vers un outil de gestion continue du cycle de vie. Ses fonctionnalités prévues comprennent :

- Inventaire centralisé des équipements.
- Identification des versions du firmware Axis.
- Suivi des versions d'OCR7.
- Détection des équipements hors support.
- Assistance au déploiement des mises à jour.
- Génération d'informations utiles pour répondre aux vulnérabilités connues.

Cette approche transforme la gestion de la cybersécurité en un processus opérationnel. Il ne s'agit plus seulement de savoir si une caméra est connectée, mais aussi de vérifier si elle est à jour, si elle exécute une version prise en charge, si elle nécessite une intervention ou si elle fait partie d'une installation nécessitant une action préventive.

6. LA VALEUR D'OCR7 SUR LES CAMÉRAS AXIS

La plateforme sur laquelle le logiciel est exécuté est également déterminante. OCR7 peut être exécuté de manière embarquée sur les caméras Axis, en s'appuyant sur une plateforme réseau conçue pour fonctionner dans des environnements professionnels et garantir un cycle de vie de sécurité actif.

Capacité d'Axis	Bénéfice en matière de sécurité
AXIS OS	Base maintenue grâce aux mises à jour et aux versions bénéficiant d'un support.
Firmware signé et démarrage sécurisé	Contribuent à garantir que le dispositif exécute uniquement des logiciels autorisés.
Axis Edge Vault	Protection de l'identité du dispositif et stockage sécurisé des clés cryptographiques.
HTTPS, certificats numériques et IEEE 802.1X	Facilitent l'intégration dans les réseaux d'entreprise répondant à des exigences avancées en matière de sécurité.

Un autre aspect essentiel est la gestion des vulnérabilités. Le fait qu'un fabricant publie des avis de sécurité et des correctifs ne supprime pas la responsabilité de l'intégrateur ou de l'exploitant, mais fournit une base transparente pour agir. Une mise à jour ne protège que si elle est effectivement appliquée ; c'est pourquoi la combinaison de la plateforme Axis, de SCAP et d'Alarm permet de boucler le cycle entre la détection, la disponibilité des correctifs et leur déploiement maîtrisé.

Exécuter OCR7 sur les caméras Axis ne signifie pas que la sécurité est automatiquement garantie. Cela signifie s'appuyer sur une base solide sur laquelle Innova peut développer des fonctionnalités LPR, des intégrations cloud et une maintenance continue, avec une exposition réduite aux risques et une meilleure traçabilité.

7. ZERO TRUST APPLIQUÉ AU LPR

La philosophie Zero Trust repose sur une idée simple : ne faire confiance implicitement à aucun utilisateur, équipement ou service. Le simple fait d'être connecté au réseau ne devrait pas suffire pour obtenir un accès. Chaque requête doit être vérifiée, autorisée et limitée en fonction du rôle réel qu'elle doit remplir.

Appliqué à OCR7, cela implique une segmentation du réseau, l'application du principe du moindre privilège, une authentification forte, l'utilisation de certificats et une supervision continue de l'état des équipements.

Par exemple :

Rôle / composant	Accès autorisé
Opérateur	Consulter les événements, sans pouvoir modifier les configurations critiques.
Technicien de maintenance	Accès temporaire à une caméra spécifique, sans accès aux autres systèmes.
Application / intégration	Communication uniquement avec les services strictement nécessaires.

Le Zero Trust ne doit pas être considéré comme un produit, mais comme une manière de concevoir l'architecture. Dans un système LPR moderne, cette approche contribue à réduire la surface d'attaque et à limiter l'impact d'un identifiant compromis, d'un équipement mal configuré ou d'une intégration excessivement permissive.

8. DISPONIBILITÉ ET RÉSILIENCE OPÉRATIONNELLE

En cybersécurité, on évoque souvent la confidentialité et l'intégrité, mais dans les systèmes LPR, la disponibilité revêt une importance particulière. Un parking ticketless, un accès industriel ou un port ne peuvent pas dépendre d'un seul élément lorsque l'interruption du service bloque l'exploitation quotidienne.

C'est pourquoi la résilience doit faire partie intégrante de l'architecture. TwinPlate P2P Master/Master est un exemple de la manière dont une architecture distribuée peut réduire les points uniques de défaillance : si une caméra cesse de fonctionner à la suite d'une panne, d'une déconnexion ou d'un incident, l'autre peut contribuer à maintenir la voie opérationnelle et à minimiser l'impact.

L'objectif n'est pas seulement d'améliorer la disponibilité technique, mais aussi de réduire l'impact opérationnel des défaillances ou des incidents. À ce titre, la résilience constitue également une dimension essentielle de la cybersécurité.

9. RECOMMANDATIONS : INTÉGRATEURS ET CLIENTS

Une architecture sécurisée repose sur de bonnes pratiques de déploiement. Dans de nombreuses installations, le compte administrateur est créé une seule fois, partagé entre plusieurs personnes et conservé sans modification pendant des années. Cette pratique supprime toute traçabilité et rend difficile l'identification de la personne ayant modifié une configuration ou exécuté une action critique.

Il est recommandé de définir des profils distincts en fonction des responsabilités réelles de chaque utilisateur. Un opérateur chargé de consulter les mouvements ne devrait pas pouvoir modifier les paramètres de la caméra. Un technicien de maintenance devrait disposer des autorisations nécessaires à sa mission, sans bénéficier d'un accès administrateur permanent. Lorsque cela est possible, l'intégration avec des annuaires d'entreprise ou des fournisseurs d'identité permet d'éviter les comptes locaux oubliés et facilite la désactivation des utilisateurs.

Il convient également d'appliquer des mesures relatives au réseau et à la maintenance :

- Segmenter les caméras et les services.
- Utiliser HTTPS et déployer des certificats.
- Désactiver les services inutiles.
- Maintenir le firmware et OCR7 à jour.
- Vérifier régulièrement les configurations.
- Protéger les sauvegardes.

Les mises à jour ne constituent pas une contrainte opérationnelle, mais une composante essentielle de la sécurité du système.

La responsabilité est partagée :

Acteur	Responsabilité
Innova	Concevoir des produits sécurisés et publier des mises à jour facilitant le déploiement, l'intégration et la maintenance du système LPR.
Intégrateur	Installer le système conformément aux bonnes pratiques.
Client	Exploiter l'infrastructure en appliquant des politiques claires en matière de gestion des utilisateurs, de réseau et de maintenance.

10. RELATION AVEC NIS2 ET LE CYBER RESILIENCE ACT

La cybersécurité joue un rôle de plus en plus important dans la gestion des infrastructures connectées. Dans ce contexte, la directive NIS2 et le Cyber Resilience Act (CRA) définissent l'orientation que suivra le marché au cours des prochaines années.

Alors que la directive NIS2 renforce les exigences de sécurité applicables aux organisations exploitant des infrastructures et des services essentiels, le Cyber Resilience Act introduit de nouvelles exigences pour les fabricants de produits numériques connectés. Parmi celles-ci figurent notamment la gestion des vulnérabilités, la publication de mises à jour de sécurité et la maintenance du produit tout au long de son cycle de vie.

Calendrier d'application du Cyber Resilience Act

- 10 décembre 2024 : entrée en vigueur du Cyber Resilience Act.
- 11 septembre 2026 : début des obligations de notification des vulnérabilités exploitées et des incidents graves.
- 11 décembre 2027 : application complète des exigences relatives au support, aux mises à jour de sécurité et à la gestion des vulnérabilités.

Source : Commission européenne – Cyber Resilience Act.

Pour les utilisateurs finaux, le message est simple : un système LPR ne doit plus être évalué uniquement en fonction de sa précision de lecture. Il est tout aussi important qu'il puisse rester sécurisé dans le temps grâce à des mises à jour régulières, à une gestion appropriée des vulnérabilités et à une architecture conçue pour réduire les risques opérationnels.

En définitive, la capacité d'un système à évoluer de manière sécurisée deviendra un critère de décision de plus en plus important, au même titre que ses performances ou sa fiabilité.

11. CONCLUSIONS

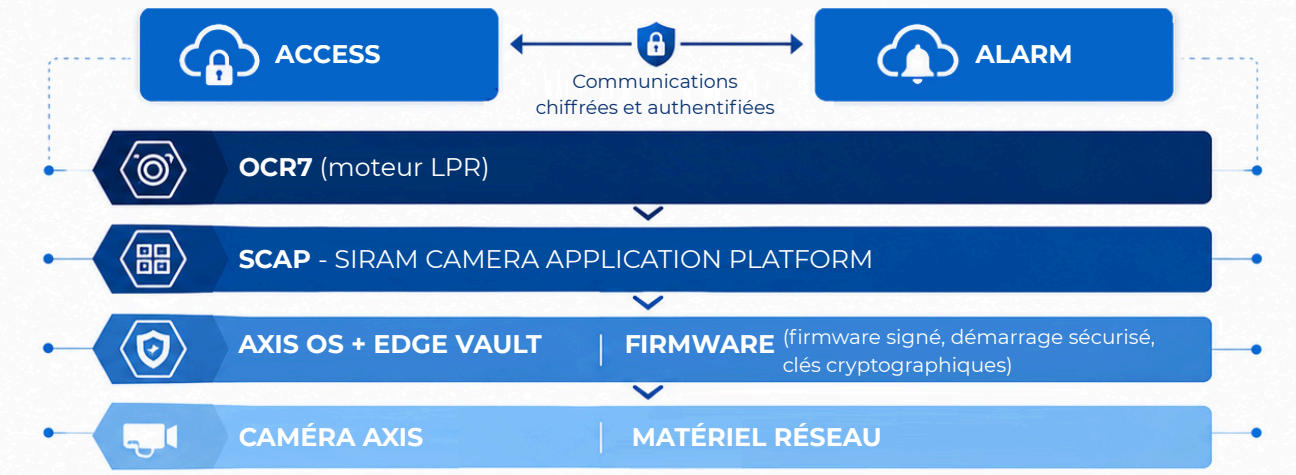
La cybersécurité est en train de cesser d'être un élément différenciateur pour devenir une exigence indispensable de tout système LPR professionnel. La précision de la reconnaissance restera un facteur essentiel, mais la capacité du système à demeurer sécurisé dans le temps grâce aux mises à jour, aux communications protégées, à la gestion des vulnérabilités et à une architecture résiliente prendra une importance croissante.

Avec OCR7, Innova adopte une approche Security by Design, en intégrant les mécanismes de protection dès la conception de la solution. Cette stratégie associe une architecture sécurisée, des communications chiffrées, une gestion continue du cycle de vie du logiciel et l'exploitation des fonctionnalités de cybersécurité intégrées aux caméras Axis. Des solutions telles que SCAP, SIRAM Access Cloud et SIRAM Alarm complètent cette stratégie en facilitant une exploitation plus sécurisée et une administration centralisée des installations.

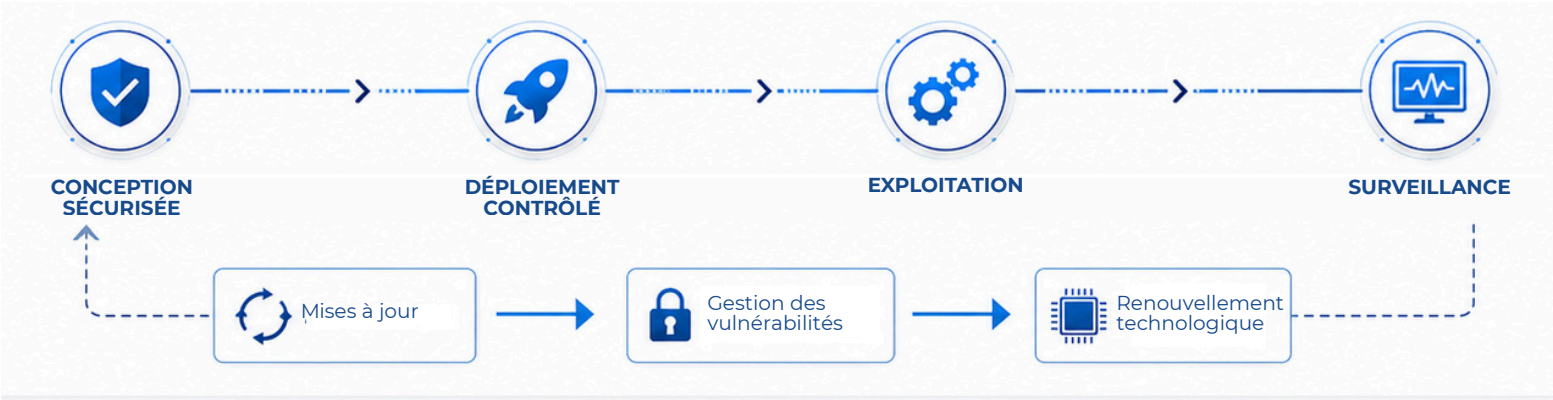
La sécurité d'un système LPR ne s'arrête pas à sa mise en service. Au contraire, une phase commence durant laquelle il est essentiel de maintenir le logiciel à jour, de superviser l'état de l'infrastructure et de gérer de manière proactive les vulnérabilités potentielles. Ce n'est qu'au moyen d'une stratégie continue de maintenance et d'amélioration qu'il est possible de garantir la disponibilité, la résilience et la protection du système tout au long de son cycle de vie.

12. ANNEXE. SCHÉMAS ET QUESTIONS D'ÉVALUATION

Architecture sécurisée OCR7 + Axis + Alarm



Cycle de vie de la sécurité opérationnelle



Cinq questions à se poser avant de choisir un système LPR

Comment le firmware des caméras et le logiciel OCR sont-ils mis à jour ?
Grâce à SCAP (SIRAM Camera Application Platform), qui standardise le déploiement et la maintenance des applications sur les caméras Axis, et à Alarm, qui facilite le déploiement des mises à jour et assure le suivi des versions d'OCR7 et du firmware Axis installées sur chaque équipement. Le firmware repose sur AXIS OS, une plateforme maintenue au moyen de mises à jour et de versions bénéficiant d'un support, avec un firmware signé et un démarrage sécurisé garantissant que le dispositif exécute uniquement un logiciel autorisé.

Comment les vulnérabilités connues sont-elles gérées ?
Axis publie des avis de sécurité et des correctifs ; Alarm génère les informations nécessaires pour répondre à ces vulnérabilités connues en identifiant les équipements concernés ; et SCAP facilite le déploiement contrôlé des correctifs. Innova résume cette approche comme le fait de « boucler le cycle entre la détection, la disponibilité des correctifs et leur déploiement maîtrisé » : publier un correctif ne suffit pas, il ne protège que s'il est effectivement appliqué.

Quels mécanismes protègent les communications entre les équipements et les services cloud ?
Des canaux authentifiés et chiffrés sont utilisés pour les communications avec Access et Alarm, avec un accès limité aux seuls services strictement nécessaires, conformément au principe du moindre privilège. Au niveau de la plateforme, Axis fournit HTTPS, des certificats numériques et IEEE 802.1X, ainsi qu'Axis Edge Vault pour protéger l'identité du dispositif et assurer le stockage sécurisé des clés cryptographiques. L'ensemble repose sur une approche Zero Trust, selon laquelle aucune requête n'est considérée comme fiable du seul fait qu'elle provient du réseau interne.

Comment l'état de l'installation est-il supervisé tout au long de son cycle de vie ?
Grâce à Alarm, qui évolue d'une plateforme de supervision vers un outil de gestion continue du cycle de vie : inventaire centralisé des équipements, identification des versions du firmware Axis, suivi des versions d'OCR7 et détection des équipements arrivés en fin de support.

Que se passe-t-il lorsqu'un équipement arrive en fin de support ou devient indisponible ?
Alarm Cloud détecte les équipements arrivant en fin de support afin de permettre la planification de leur renouvellement (dernière étape du cycle de vie : le « renouvellement technologique »). Par ailleurs, si une caméra cesse de fonctionner à la suite d'une panne, d'une déconnexion ou d'un incident, des architectures telles que TwinPlate P2P Master/Master permettent à une autre caméra de maintenir la voie opérationnelle, réduisant ainsi l'impact. La résilience est considérée comme une composante de la cybersécurité, et non uniquement comme une question de continuité technique.

Innova Systems Group
C/ Joaquim Mir 55
08100 Mollet del Vallès
Barcelona (SPAIN)
Tel. +34 93 5797238
www.innovagroupbcn.com