WHITEPAPER

SIRAM OCR7 LPR AND CYBERSECURITY IN MODERN PR SYSTEMS

Cybersecurity in an LPR system is not about isolating it from the network. It is about designing it to connect securely, be updated in a controlled manner, manage vulnerabilities effectively, and maintain availability throughout its entire lifecycle.

CONTENTS

1. INTRODUCTION

LPR systems have evolved from simple license plate recognition engines into critical components of parking infrastructures, smart cities, industrial facilities, ports, airports, and logistics centers. In all of these environments, service availability is just as important as recognition accuracy..

For many years, selecting an LPR system was driven almost exclusively by recognition rates, reading speed, nighttime performance, and reliability under challenging conditions. These factors remain essential—no one wants a system that fails to read license plates accurately. However, the market is now asking questions that, until recently, rarely arose in technical discussions: How are camera firmware updates managed? What happens when a vulnerability is discovered? How are communications secured? How long will the system be supported? Who ensures that the installation remains secure five or ten years from now?

The answer is straightforward. A modern LPR system is no longer just a camera or an OCR engine. It is a connected ecosystem of devices that controls physical access while exchanging information with management platforms, payment systems, cloud applications, and other enterprise services. As a result, it is no longer enough for an LPR system to perform well on the day it is commissioned. It must be designed to protect itself, receive secure updates, and remain operational throughout its entire lifecycle.

This white paper presents Innova's approach to cybersecurity for OCR7 and explains how the combination of OCR7, SCAP, Axis cameras, and Access and Alarm services provides an architecture designed to address this new landscape.

2. CYBERSECURITY IN LPR SYSTEMS

An LPR system controls physical access and interacts with barriers, parking management systems (PMS), payment platforms, video management systems (VMS), and enterprise services. A vulnerability no longer affects only license plate recognition—it can compromise business continuity, alter critical configurations, block a traffic lane, or become an entry point into other corporate networks.

The most significant risks include:

Risk	Description
Configuration tampering	Unauthorized changes to critical system settings.
Unauthorized opening or blocking of access points	Improper control of barriers or access points.
Device unavailability	Cameras or services out of service that disrupt operations.
Exploitation of known vulnerabilities	Exploitation of publicly disclosed vulnerabilities that have not been patched in time.
Camera as a network entry point	The camera is used as an entry point to other corporate systems.
Unauthorized firmware or software	Installation of unverified or malicious versions.

In distributed installations, these risks are further multiplied if there is no centralized view of device status.

Therefore, cybersecurity must be considered a functional requirement of the system rather than an additional feature. In parking, logistics, industrial, or critical infrastructure environments, service availability is part of security. A system that is perfectly protected from a cryptographic perspective ceases to provide value if an incident prevents access operations. Security should not be limited to protecting information; it must also help keep the service operational.

3. OCR7 DESING PRINCIPLES

OCR7 is developed following a Security by Design philosophy. This means that authentication, access control, communication protection, event logging, and update capabilities are part of the architecture from the very beginning of the development process. They are not added at the end as external elements but instead shape the way the system is designed, deployed, and maintained.

This approach is complemented by Secure by Default: default configurations designed to reduce risks, minimize unnecessary services, and enable a more controlled deployment. In practice, this helps integrators avoid common mistakes, such as leaving services exposed, sharing credentials between users, or keeping devices running outdated firmware versions.

The objective is not only to protect OCR7 on the day of installation, but also to ensure that the installation remains secure throughout its entire lifecycle. To achieve this, change traceability, profile management, the ability to update software versions, and reducing the attack surface are essential.

4. SECURE CONNECTIVITY: ACCESS & ALARM

In the past, it was common to consider a secure system as one that was completely isolated from the Internet. Today, this is no longer true for many installations: remote management, centralized monitoring, continuous updates, and the use of cloud services provide significant operational value when implemented securely.

The question is no longer whether a system is connected, but how it is connected. Communications must take place over authenticated and encrypted channels, limiting access to only the services that are strictly necessary and applying the principle of least privilege. A camera securely connected to Access or Alarm is not the same as a camera exposed to the Internet without control.

Access Cloud enables centralized management of distributed installations and provides controlled remote access. Alarm Cloud complements this architecture by providing continuous visibility into the operational and maintenance status of devices. Together, these platforms enable the transition from an isolated, difficult-to-maintain installation to a securely connected infrastructure that can be managed over the long term.

5. CONTINUOUS SECURITY WITH SCAP AND ALARM

SCAP, the SIRAM Camera Application Platform module, enables the standardized deployment and maintenance of applications on Axis cameras. Its value lies not only in simplifying installation, but also in reducing operational variability: fewer manual procedures, fewer improvised configurations, and greater control over which software version is installed on each device.

Security does not end when commissioning is complete. Over the following years, new firmware versions, OCR7 updates, known vulnerabilities, expiring certificates, network changes, and devices reaching end of support will all arise. Keeping an installation secure requires continuous management, not just an initial configuration.

In this context, Alarm evolves from a monitoring platform into a continuous lifecycle management tool. Its planned capabilities include:

- Centralized device inventory.
- Identification of Axis firmware versions.
- Tracking of OCR7 versions.
- Detection of devices that are out of support.
- Assistance with update deployment.
- Generation of useful information for responding to known vulnerabilities.

This approach transforms cybersecurity management into an operational process. It is not only about knowing whether a camera is connected, but also whether it is up to date, whether it is running a supported version, whether it requires intervention, or whether it is part of an installation that requires preventive action.

6. THE VALUE OF OCR7 ON AXIS CAMERAS

The platform on which the software runs is also a determining factor. OCR7 can run embedded on Axis cameras, taking advantage of a network platform designed to operate in professional environments and maintain an active security lifecycle.

Axis Capability	Security Benefit
AXIS OS	Maintained platform through updates and supported releases.
Signed firmware and Secure Boot	Help ensure that the device runs authorized software.
Axis Edge Vault	Device identity protection and secure storage of cryptographic keys.
HTTPS, digital certificates, and IEEE 802.1X	Facilitate integration into corporate networks with advanced security requirements.

Another key aspect is vulnerability management. The fact that a manufacturer publishes security advisories and patches does not remove the responsibility of the integrator or operator, but it provides a transparent basis for taking action. An update only provides protection if it is applied; therefore, the combination of the Axis platform, SCAP, and Alarm helps close the loop between detection, patch availability, and controlled deployment.

Running OCR7 on Axis does not mean that security is automatically solved. It means starting from a solid foundation on which Innova can develop LPR capabilities, cloud integration, and continuous maintenance with lower exposure and greater traceability.

7. ZERO TRUST APPLIED TO LPR

The Zero Trust philosophy is based on a simple idea: never implicitly trust any user, device, or service. Being inside the network should not be sufficient to gain access. Every request must be verified, authorized, and limited according to the actual function it is intended to perform.

Applied to OCR7, this means network segmentation, least privilege, strong authentication, the use of certificates, and continuous monitoring of device status. For example:

Role / Componente	Access It should have
Operator	View events, without being able to modify critical configurations.
Maintenance technician	Temporary access to a specific camera, not to other systems.
Application / Integration	Communication only with the services that are strictly necessary.

Zero Trust should not be understood as a product, but as a way of designing the architecture. In a modern LPR system, it helps reduce the attack surface and limits the impact of a compromised credential, a misconfigured device, or an overly permissive integration.

8. AVAILABILITY AND OPERATIONAL RESILIENCE

In cybersecurity, confidentiality and integrity are often discussed, but in LPR systems, availability carries particular importance. A ticketless parking facility, an industrial access point, or a port cannot depend on a single element if a service interruption blocks daily operations.

For this reason, resilience must be part of the architecture. TwinPlate P2P Master/Master is an example of how a distributed architecture can reduce single points of failure: if one camera stops operating due to a malfunction, a disconnection, or an incident, the other can help keep the lane operational and minimize the impact.

It is not only about increasing technical availability, but also about reducing the operational impact of failures or incidents. In this sense, resilience is also a dimension of cybersecurity.

9. RECOMMENDATIONS FOR INTEGRATORS & CUSTOMERS

A secure architecture requires good deployment practices. In many installations, the administrator account is created once, shared among multiple users, and remains unchanged for years. This practice eliminates traceability and makes it difficult to determine who modified a configuration or performed a critical action.

It is advisable to define separate profiles according to the actual role of each user. An operator who reviews events should not modify camera settings. A maintenance technician should have sufficient permissions for the assigned task, but not permanent administrative access. Whenever possible, integration with corporate directories or identity providers helps avoid forgotten local accounts and simplifies user deprovisioning.

Network and maintenance measures should also be applied:

- Segment cameras and services.
- Use HTTPS and deploy certificates.
- Disable unnecessary services.
- Keep firmware and OCR7 up to date.
- Review configurations periodically.
- Protect backups.

Updates are not an operational inconvenience, but an essential part of system security.

Responsibility is shared:

Actor	Responsibility
Innova	Design secure products and publish updates that facilitate the deployment, integration, and maintenance of the LPR system.
Integrator	Install the system following best practices.
Customer	Operate the infrastructure with clear user, network, and maintenance policies.

10. NIS2 AND THE CYBER RESILIENCE ACT

Cybersecurity is playing an increasingly important role in the management of connected infrastructures. In this context, the NIS2 Directive and the Cyber Resilience Act (CRA) set the direction the market will follow in the coming years.

While NIS2 strengthens the security requirements for organizations operating essential infrastructures and services, the Cyber Resilience Act establishes new requirements for manufacturers of connected digital products. These include vulnerability management, the publication of security updates, and product maintenance throughout its entire lifecycle.

CRA Implementation Timeline

- 10 December 2024: Entry into force of the Cyber Resilience Act.
- 11 September 2026: Obligations to report actively exploited vulnerabilities and severe incidents begin.
- 11 December 2027: Full application of the requirements related to product support, security updates, and vulnerability management.

Source: European Commission – Cyber Resilience Act.

For end users, the message is simple: an LPR system should no longer be evaluated solely on its recognition accuracy. It is equally important that it can remain secure over time through regular updates, proper vulnerability management, and an architecture designed to reduce operational risks.

Ultimately, a system's ability to evolve securely will become an increasingly important decision criterion, on the same level as its performance and reliability.

11. CONCLUSIONS

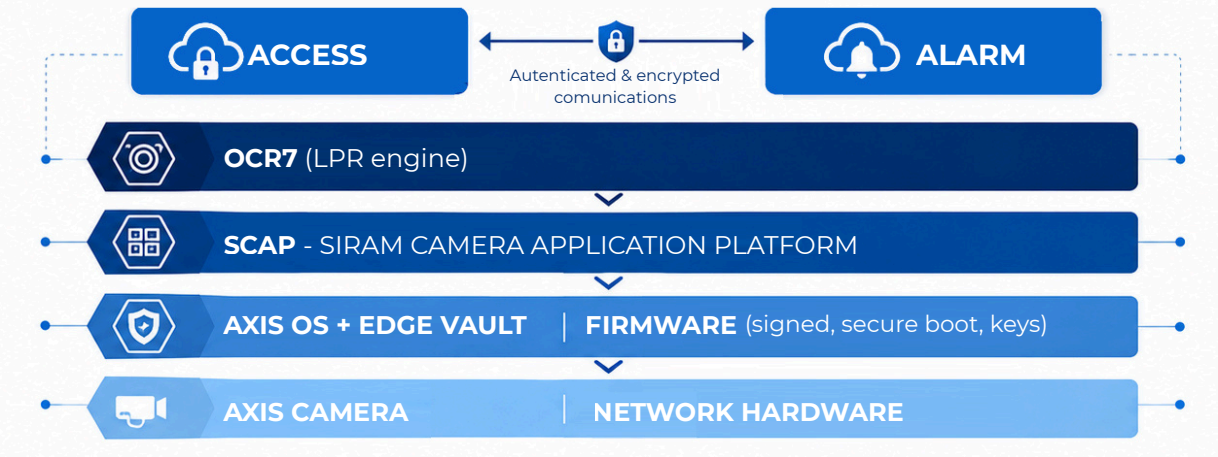
Cybersecurity is no longer a differentiating factor; it is becoming an essential requirement for any professional LPR system. Recognition accuracy will remain a key factor, but increasing importance will be placed on the system's ability to remain secure over time through software updates, protected communications, vulnerability management, and a resilient architecture.

With OCR7, Innova adopts a Security by Design approach, integrating security mechanisms from the outset of the solution's design. This strategy combines a secure architecture, encrypted communications, continuous software lifecycle management, and the use of the cybersecurity capabilities built into Axis cameras. Solutions such as SCAP, SIRAM Access Cloud, and SIRAM Alarm complement this strategy, enabling more secure operations and centralized management of installations.

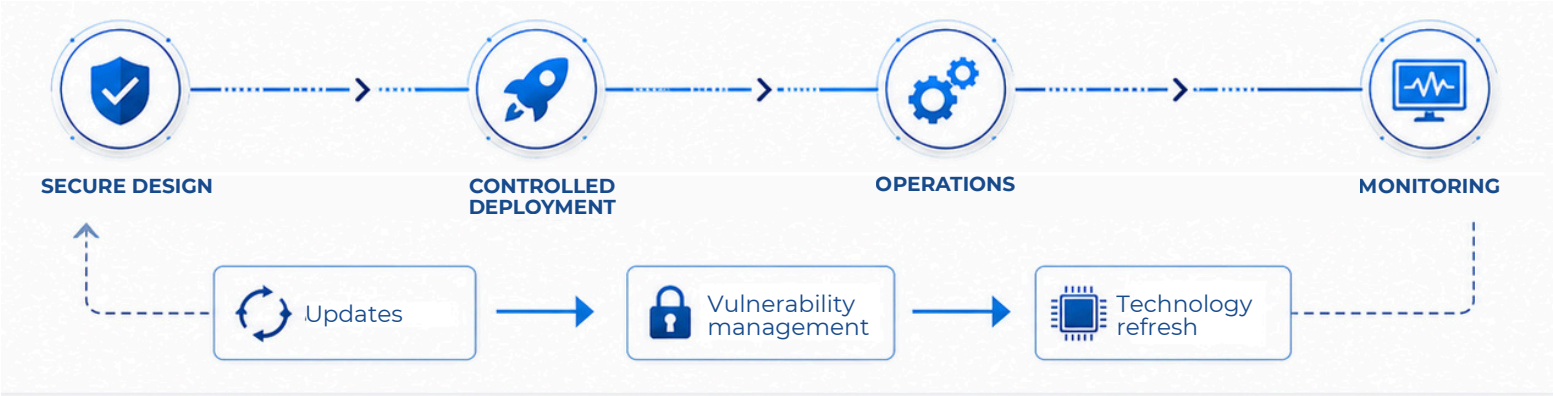
The security of an LPR system does not end when it is commissioned. On the contrary, this marks the beginning of a phase in which keeping the software up to date, monitoring the status of the infrastructure, and proactively managing potential vulnerabilities become essential. Only through a continuous strategy of maintenance and improvement is it possible to ensure the availability, resilience, and protection of the system throughout its entire lifecycle.

12. APPENDIX: DIAGRAMS AND ASSESSMENT QUESTIONS

Secure Architecture: OCR7 + Axis + Alarm



Operational Security Lifecycle



Five questions to ask before choosing an LPR System

How are camera firmware and OCR software updated?
Through SCAP (SIRAM Camera Application Platform), which standardizes the deployment and maintenance of applications on Axis cameras, and Alarm, which assists with update deployment and tracks the OCR7 and Axis firmware versions installed on each device. The firmware platform is based on AXIS OS, maintained through updates and supported releases, with signed firmware and Secure Boot to help ensure that the device runs authorized software.

How are known vulnerabilities managed?
Axis publishes security advisories and patches; Alarm generates useful information to help respond to known vulnerabilities by identifying affected devices; and SCAP facilitates the controlled deployment of patches. Innova summarizes this approach as "closing the loop between detection, patch availability, and controlled deployment"—publishing a patch is not enough; it only provides protection once it has been applied.

What mechanisms protect communications between devices and cloud services?
Authenticated and encrypted channels to Access and Alarm, with access limited to the services that are strictly necessary (least privilege). At the platform level, Axis provides HTTPS, digital certificates, IEEE 802.1X, and Axis Edge Vault for device identity protection and secure storage of cryptographic keys. All of this follows a Zero Trust philosophy: no request is trusted simply because it originates from within the network.

How is the installation monitored throughout its lifecycle?
With Alarm, which evolves from a monitoring platform into a continuous lifecycle management tool, providing centralized device inventory, identification of Axis firmware versions, tracking of OCR7 versions, and detection of devices that are out of support.

What happens when a device reaches end of support or becomes unavailable?
Alarm Cloud detects devices that reach end of support so that renewals can be planned (the final stage of the lifecycle: "technology refresh"). If a camera stops operating due to a malfunction, a disconnection, or an incident, architectures such as TwinPlate P2P Master/Master allow another camera to keep the lane operational, minimizing the impact. Resilience is treated as part of cybersecurity, not only as a matter of technical continuity.

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