Perimeter Security False Alarms

The Definitive Guide

DAVANTIS

False Alarms in Perimeter Security

Causes, types, real costs and how to eliminate them with AI video analytics.

A guide for CMSs, installers and security managers, organised by sector.

76%

of alarms received by a CMS are false alarms. Only 24% require a genuine response.

95%

reduction in false alarms achieved at real installations using DFUSION /3 video analytics.

25 fps

fps vs 2–6 fps with cloud-based filtering. The difference in the data available to determine whether an alarm is genuine.

This guide is for CMS Managers, Installers and System Integrators, Security Managers / CISOs, and Critical Infrastructure Managers.

Guide Contents

1. What is a false alarm in perimeter security?

A false alarm — also known as a false positive — is an alert generated by a security system in response to an event that does not represent a genuine threat. The system detects something, interprets it as an intrusion or incident, and reports it accordingly. However, when the event is verified, no intruder or security risk is found.

In CCTV perimeter security, false alarms are the biggest operational challenge faced every day by Central Monitoring Stations (CMSs) and security teams. This is not a minor or occasional issue: in installations using conventional motion detection technology, more than 76% of the signals received by a CMS are false alarms. Operators spend three quarters of their time and resources dealing with noise rather than genuine threats.

Industry terminology

False positive (FP): the system raises an alarm for an event that is not a genuine threat. The system says “intruder detected” when there isn’t one.

False negative (FN): the system fails to raise an alarm for an event that is a genuine threat. The system says “no threat detected” when

there is one. In CMS environments this is known operationally as a missed detection.

False positive rate: the percentage of alarms generated that prove to be false, measured against the total number of alarms.

2. **False alarms vs false negatives:** the visible and the invisible problem

A great deal is said about false alarms, but far less attention is given to their opposite: the false negative or missed detection. This is a critical blind spot. They are different problems, with different causes, different costs and different solutions — and the second is more dangerous precisely because nobody sees it happen.

Dimension	False alarm (false positive)	False negative (missed detection)
What happens?	The system detects a threat that does not exist. Alarm without a real intrusion	The system DOES NOT detect a threat that does exist. Intrusion without an alarm
Who is affected	CMS operators, response guards, CMS manager, end customer	End customer (victim of theft/intrusion), installer, CMS (legal responsibility)
Immediate consequence	Protocol activation, unnecessary dispatch, wasted time, direct cost	Intrusion completed without response. Real damage: theft, vandalism, sabotage, injury
Legal consequence	Fines for repeated false alarms (Private Security Act). Contractual penalties	Civil liability for the installer and CMS due to system failure
Economic cost	Direct and measurable: operator time + dispatch + penalties	Hard to quantify but potentially much higher: theft, damage, litigation, loss of client
Visibility	**High — the operator always sees it**	**Invisible — only becomes known once the damage has occurred**
Cumulative effect	"Alarm fatigue": operators become desensitised and stop treating alarms seriously	Total loss of trust in the system. The client cancels the contract or takes legal action
Priority of resolution	**High**	**Critical — irreversible consequences**

How missed detections occur

A missed detection does not always happen because the system is poor. It occurs more often than expected in seemingly controlled situations:

- **External alarm filtering:** A third-party platform outside the video surveillance process filters the alarms, but typically receives only a fraction of the original video frames. If the intrusion occurs in a frame that is not analysed, it does not exist for the system. This also creates direct legal exposure for both the CMS and the installation company. (Why frame rate matters is covered in depth in Section 6.)
- **Operator alarm fatigue:** An operator who has processed 500 consecutive false alarms has reduced responsiveness to alarm 501. Cognitive overload is a well-documented cause of human missed detection in high-volume CMS environments.
- **Intrusion during a technical window:** Cloud-based processing with latency or connectivity interruptions creates time windows in which images are not analysed. An experienced intruder can exploit these gaps.

Key conclusion _

False alarms are the visible problem: we see them, we count them, they are a nuisance. False negatives are the invisible problem: we do not know how many occur until it is too late.

Any solution that reduces false alarms by introducing missed detections is making the real problem worse, even if it appears to improve CMS operational metrics.

3. Why do false alarms occur?

The causes of false alarms in perimeter security can be grouped into four categories. Understanding each one is the first step towards selecting the right solution.

Installation-related causes

Many false alarms originate not from the technology itself, but from how the system has been installed and configured:

Incorrect camera angle: framing that includes high-movement vegetation, roads or areas outside the perimeter.

Poorly configured exclusion zones: areas of legitimate movement (staff access routes, adjacent roads) not excluded from analysis.

Insufficient or excessive lighting: installations without proper IR illumination, or with lighting that creates glare and image saturation.

Camera vibration: poor mounting structures on PTZ cameras or installations near heavy machinery.

Uncontrolled vegetation growth: trees and shrubs growing into the camera's field of view over time.

Environmental causes

The most common source of false alarms in outdoor installations. The natural environment is unpredictable and constantly changing, and basic motion detection cannot distinguish an intruder from environmental motion:

Rain and water: droplets on the lens, reflections on wet surfaces, puddles creating movement when disturbed.

Wind: moving vegetation, displaced objects, flags or tarpaulins flapping.

Light changes: abrupt transitions from night to day, streetlights switching on/off, moving shadows.

Fog: reduced visibility and visual artefacts interpreted by motion algorithms as objects.

Reflections: vehicle headlights sweeping across the field of view, sun glare on metallic surfaces.

Snow: sudden contrast changes and accumulation on the lens or detection surface.

Biological causes

Insects: spiders, mosquitoes and other insects passing in front of the lens or building webs — one of the most frequent causes in outdoor night-time installations.

Birds: pigeons, sparrows and birds of prey crossing the field of view or sitting within the frame.

Small animals: cats, foxes, rabbits, dogs, rodents — especially in industrial sites, warehouses and rural perimeters.

Medium-sized animals: wild boar, deer and other animals in solar/wind farms or agricultural sites in peri-urban environments.

System-related causes

Basic motion detection: systems that only analyse pixel changes cannot distinguish a person from a falling leaf.

Poorly calibrated sensitivity thresholds: too sensitive leads to false alarms; too insensitive leads to missed detections.

Lack of object classification: without AI classifying whether movement is a person, vehicle or animal, any motion triggers an alarm.

Low-frame-rate filtering: systems analysing only a few frames per second lose critical information needed to assess whether an alarm is real (see Section 6)

4. What false alarms cost, by role

The problem changes depending on who suffers it. This section concentrates all the cost and impact figures of the guide — one authoritative reference for each profile.

CMS_

Central Monitoring Station Manager. Your problem is volume (operational and economic)

For a CMS, false alarms are not a nuisance — they are the business model in reverse. A medium-sized CMS receives thousands of signals per day. If 76% are false alarms, operators are processing noise 76% of the time:

Operational cost: each false alarm consumes 1–5 minutes of operator time in verification, coordination with the client and event closure.

Dispatch cost: false alarms that escalate generate the deployment of a guard or patrol — €30–€120 per unnecessary dispatch depending on the market.

Capacity saturation: a CMS with a high false alarm rate cannot scale its portfolio without adding operators — it breaks the scalability of the business model.

Alarm fatigue: operators saturated with false alarms have reduced responsiveness to real alarms, increasing the risk of human missed detection.

Regulatory risk: Spanish and European regulations govern response performance and may sanction CMSs with systematically high false alarm rates.

Contract renewal impact: clients experiencing repeated false alarms (sirens, unnecessary calls) are less likely to renew contracts.

Putting a number on it_

A medium-sized CMS with 500 installations and an average of 20 signals per installation per day, at a 76% false alarm rate, handles 7,600 unnecessary verifications per day.

At an average of 3 minutes each, that is 380 operator hours per day spent on noise rather than real security. If a fraction of these signals escalate to dispatch (typically €30–€50 each), the annual direct cost can exceed €100,000 in a mid-sized CMS.

The model that AI video analytics changes for the CMS_

With conventional motion detection, the CMS receives all signals and the operator filters them manually. With on-premises AI video analytics (DFUSION), the AI filters at the installation before reporting: the CMS only receives verified real-threat alerts.

The operator shifts from handling 100 signals/hour to managing 5–10 qualified real events. This does not only reduce cost — it changes scalability: the same team can manage a much larger portfolio.

Metrics a CMS should measure

False alarm rate per installation (% FP over total signals); dispatch ratio per installation and per month; average verification time per event; missed detection rate (requires cross-audit with reported incidents); total cost per managed installation.

INS_

Installer & Security Integrator. Your problem is responsibility (technical and commercial)

When the system you installed generates false alarms, the call comes to you. The installer is the first point of contact for any operational issue, and a deployment with a high false alarm rate quickly erodes the commercial relationship with both the client and the CMS.

Seven common installation mistakes causing false alarms

- Installing cameras facing trees or bushes without configured exclusion zones.
- Positioning cameras where vehicle headlights sweep across the field of view at a direct angle.
- Failing to calibrate sensitivity thresholds according to the specific conditions of the site.
- Mounting cameras on walls shared with vibration sources (compressors, HVAC systems).
- Not accounting for vegetation growth: a clear zone in January becomes a problem in July.
- Leaving authorised staff or vehicle access routes within the analytical area.
- Not performing a night-time stress test: many installations have radically different day and night lighting conditions.

What to ask the client before installation

- Are there animals on-site or in the surrounding area? What type?
- What are the authorised access schedules for staff?
- Are there company vehicles that will circulate within the perimeter, and at what times?
- Are there variable light sources nearby (adjacent roads, timer-controlled streetlights, third-party facilities)?
- What SLA response level is agreed with their CMS? How many false alarms are acceptable per month?

How AI video analytics protects the installer_

A deployment with DFUSION shifts filtering capability to the system, not the installer or the operator. When the system is correctly configured with dual-engine AI (motion + appearance), the false alarm rate drops dramatically from day one — reducing support calls and increasing customer satisfaction with no additional maintenance cost.

CISO_

Security Manager.
Your problem is exposure (strategic and regulatory)

For a Security Manager or CISO, especially in critical infrastructure, a high false alarm rate is not just an operational issue. It is a sign that the system has low accuracy — and a low-accuracy system also implies missed detections that you are not seeing.

The NIS2 Directive and the National Security Framework (ENS) set explicit requirements for reliability and response in critical infrastructure security systems. A system generating 76% false alarms can hardly demonstrate the level of control required by these regulations.

How to justify investment in false alarm reduction to senior management

- **Current measurable cost:** number of false alarms per month × cost per dispatch = avoidable expenditure.
- **Regulatory risk:** exposure to penalties due to inadequate response rates under NIS2/ENS.
- **Missed detection risk:** if the system has 76% FP, it statistically also has unrecorded FN.
- **AI ROI:** 95% reduction in false alarms with the same number of cameras and no need to increase staffing.

Metrics for internal reporting: Monthly false alarm rate per zone/ perimeter; average response time from detection to verification; number of real incidents detected vs total alarms; active camera coverage and uptime without technical incidents; cross-audit of physical incidents reported vs system detections.

NIS2 and perimeter security_

The European NIS2 Directive (transposed in Spain in 2024) raises security requirements for operators of essential services and critical infrastructure. It includes the obligation to deploy incident detection systems with verifiable response capability. A system with a high false alarm rate may compromise compliance if it creates operational fatigue leading to missed detections.

5. False alarms by sector: specific causes and how to address them

Not all installations generate the same type of false alarms. The causes vary significantly depending on the environment. Identifying the specific causes in your sector is the starting point for an effective solution.

Sector 01 /

Central Monitoring Stations (CMSs)

#Signal volume
#Operational fatigue
#Multi-site installations

- Signals from PIR detectors or volumetric sensors connected to systems without video analytics — no visual context means everything is reported as an alarm.
- Integrations across multiple system types (CCTV, intruder alarms, access control) with heterogeneous configurations that create signal overlap.
- Incorrectly configured opening/closing schedules: the system triggers alarms because it "does not know" that staff are working outside standard hours.

- Clients forgetting to disarm the system before accessing the premises: one of the main causes of avoidable calls.

Specific solution for CMS_

Integration of DFUSION directly into the alarm management software (compatible with leading VMS and CMS platforms). The AI filters at source — at the client's installation — before reporting. The CMS receives verified events, not raw signals. With ClickThru, the operator can access event footage in seconds without switching platforms. (See Section 8 for the full integration picture.)

“

Compatible with leading VMS and CMS platforms

Sector 02 /

Logistics and Warehousing

#Constant movement
#Authorised personnel
#Multi-shift operations

- Forklifts and loading vehicles operating across perimeter areas over extended time windows — their lights and movement continuously trigger basic detection systems.
- Night-shift or weekend staff accessing areas marked as “protected” outside configured schedules.
- Delivery trucks and trailers manoeuvring in loading bays — slow, unpredictable and large-scale movements that generate multiple activations.
- Loading/unloading zones with frequent object changes: pallets, containers and boxes being rearranged, creating “new” scenes that motion-based systems interpret as change.
- Driver supervision in loading areas: the need to distinguish between drivers waiting (legitimate) and drivers accessing unauthorised zones.

Specific solution for logistics_

Smart exclusion zones configured by schedule and object type. DFUSION classifies whether what is moving is a person, a vehicle, or both — and applies different rules depending on zone and time. The system learns the legitimate patterns of the site and only triggers alerts in response to truly anomalous behaviour.

Sector 03 /

Critical Infrastructure

#NIS2 compliance
#Maximum requirements
#Challenging environments

- Airports and ports: constant vehicle and pedestrian traffic across large perimeter areas, making it difficult to distinguish between authorised access and intrusion.
- Power plants: industrial environments with moving machinery, steam emissions, thermal fluctuations and vibrations that affect sensors and cameras.
- Water and wastewater facilities: peri-urban or rural locations with frequent wildlife (wild boar, foxes, large birds) and insufficient perimeter lighting.
- Transport hubs: high volumes of authorised pedestrian flow during peak hours, making threshold configuration difficult — too sensitive during operations, too insensitive during closures.

Specific solution for critical infrastructure_

DFUSION is certified by the CPNI (Centre for the Protection of National Infrastructure) in the United Kingdom — one of the most demanding security technology certifications in the world. This accreditation ensures the detection standards and false alarm reduction levels required by critical infrastructure regulations across Europe.

> DFUSION holds one of the most demanding security technology certifications in the world

Sector 04 /

Solar and Wind Energy

#Remote installations
#Active wildlife
#No human presence

- Medium and large wild animals: wild boar, foxes, rabbits, deer and birds of prey roaming installations in natural or peri-urban areas.
- Extreme light variations: solar plants have reflective surfaces that create glare and flashes depending on the sun angle — a common source of false alarms in basic systems.
- Wind turbine vibration and machinery movement: in wind farms, ground and structural vibrations affect cameras mounted on poles or masts.
- Sites without stable connectivity: reliance on 4G or satellite connections introduces latency in cloud-based filtering systems, increasing the risk of missed detections.
- Unplanned maintenance access: technical teams entering outside standard hours without prior notification to the security system.

Specific solution for energy_

On-premises (edge) analysis, with no dependency on connectivity. DFUSION processes video directly at the installation — if the internet connection fails, the system continues to operate. This is especially critical in solar and wind farms located in rural areas with limited or unstable connectivity.

Sector 05 /

Industrial Parks

#Multi-company
#Loitering
#Complex perimeters

- People loitering at night: loitering — reconnaissance prior to theft — is difficult for basic systems to detect because there is no actual access, only prolonged presence near the perimeter.
- Multiple companies with different access schedules: what is an intrusion at 3am may be a legitimate night shift in the adjacent facility.
- Vehicles parked in perimeter areas: staff cars, waiting trucks or abandoned vehicles interpreted by the system as “new” objects in the scene.
- Urban and peri-urban wildlife: cats, stray dogs, rats and birds attracted by waste and machinery heat in industrial zones.

Specific solution for industrial parks_

Active loitering detection — DFUSION detects not only access but also pre-intrusion behaviour: a person circling the perimeter for more than X minutes without entry, or repeatedly appearing at the same point on consecutive nights. The AI distinguishes between occasional presence and reconnaissance patterns.

“

DFUSION detects even pre-intrusion behaviour

Sector 06 /

Retail and Commercial Premises

#Exclusion zones
#Staff and customers
#Mixed operating hours

- Pedestrian and vehicle traffic during opening hours that triggers the system if exclusion zones are not correctly configured by schedule.
- Bins, shopping trolleys or urban elements moved by wind or by passers-by outside operating hours.
- Decorative plants in shop windows or entrances moving due to ventilation or air currents when doors are opened.
- Waiting customers: people standing at the entrance before opening hours, interpreted by the system as potential intrusion.

Specific solution for retail_

Custom detection rules that distinguish between presence (a person waiting) and anomalous behaviour (a person attempting to access through a restricted zone). Time-based exclusion zones that automatically activate and deactivate according to the opening schedule.

6. Identify the real alarm at source, or filter it later in the cloud?

This is the most important technical debate in video analytics for perimeter security. There are two radically different architectures for reducing false alarms, and the difference between them is not only technical — it has direct consequences for detection reliability and the risk of missed detections. Everything this guide says elsewhere about cloud filtering points back to this section.

On-premises analysis (edge)	Cloud filtering (third-party platforms)
25 fps — analysed —	2-6 fps — analysed —
✓ Processes the full video stream: 25 fps. Maximum available information for decision-making	✗ Analyses only 2–6 fps out of the original 25 fps: 76–92% of the information is discarded before analysis
✓ Zero latency: detection occurs within milliseconds at the installation itself	✗ Added latency: image upload time to the cloud + processing time + response delay
✓ No connectivity dependency: continues to operate even if the internet goes down	✗ Connectivity dependency: if the network fails, the filtering system does not work
✓ No risk of image loss due to network issues	✗ Risk of image loss due to network issues at the moment of the event
✓ The system filters at source — the CMS only receives qualified events	✗ The CMS receives the original signal first — the filter arrives afterwards, once the operator has already acted
✓ Privacy: images do not leave the installation unless a real alarm is triggered	✗ Images are uploaded to third-party servers — privacy and GDPR considerations

Which is faster at identifying a real alarm?

Identification speed has two components: detection speed (how quickly the system recognises that an event is occurring) and qualification speed (how quickly it determines whether it is a real or false alarm).

Parameter	On-premises (DFUSION)	Cloud filtering (third-party)
Initial detection	Milliseconds — processed directly in the camera/ local device	Seconds — upload time to cloud + processing queue delay
Qualification (is it real?)	At the point of detection — the local AI decides before reporting	After detection — the cloud filter receives an already generated signal, then decides whether to confirm it
Available information	25 fps — full stream, complete temporal context of the movement	2–6 fps — partial snapshot, without full temporal context
Connectivity failure	Fully autonomous operation	**Filtering is interrupted — all signals reach the CMS unfiltered**
Total time to CMS operator	Qualified event is sent directly to the operator	Raw signal > operator starts verification > cloud filter receives > confirms or discards

The double-filter problem_

When a 25 fps video analytics system is combined with a cloud filtering platform operating at 3 fps, the detection process ends up relying solely on the 3 fps analysed by the cloud. The filtering AI makes decisions using less than 12% of the available information.

If those few frames do not correctly capture the intrusion, the risk of missing a real threat increases significantly. The "double filter" introduces a bottleneck that can compromise security rather than improve it.

> The double filter introduces a bottleneck that can compromise security

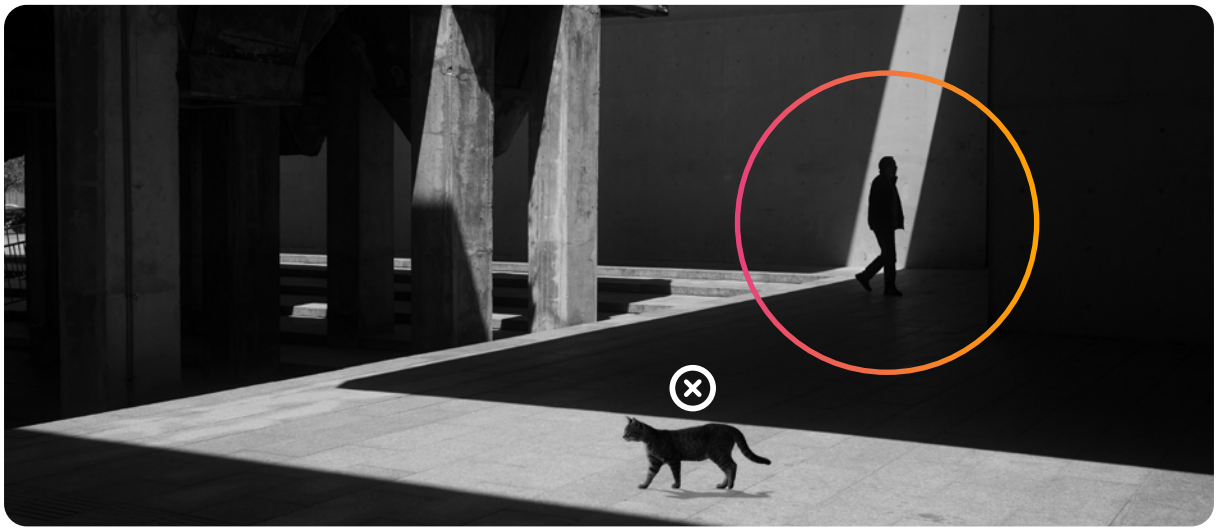
Technical verdict _

On-premises analysis is faster, more reliable and more secure than cloud filtering in the context of perimeter security.

Not because cloud AI is inferior — in ideal conditions it can perform very well — but because the perimeter CCTV environment is not ideal: images under adverse conditions, small objects at long distances, and situations that require movement to be analysed in full temporal context.

That requires 25 fps, not 3.

7. **DFUSION vs embedded analytics:** camera AI, VMS modules and cloud platforms



"AI video analytics" has become a label that covers very different things. A CMS or integrator evaluating options today will typically encounter four architectures. They are not equivalent — they differ in where the analysis runs, how much information it uses, and who controls the detection quality.

The four architectures

- AI embedded in the camera: the analytics run on the camera's own chipset. Convenient (no extra hardware), but constrained by the camera's limited compute: models are smaller, typically appearance-only, and performance varies from one camera model and firmware to another. Detection quality is tied to the camera brand and its refresh cycle, and a mixed camera estate means mixed (and unpredictable) analytics quality.

- VMS analytics modules: detection add-ons inside the video management system. They centralise configuration, but the analytics are generic modules serving many use cases, not specialised perimeter engines; performance depends on the VMS server sizing, and the CMS is locked to that VMS ecosystem.

- Cloud filtering platforms: filtering after the fact on a fraction of the frames, with the latency, connectivity and privacy limitations described in Section 6.

- Dedicated on-premises analytics (DFUSION): a purpose-built perimeter detection system running at the installation on dedicated hardware, analysing the full 25 fps stream with a dual-engine AI (appearance + motion), independent of camera brand, working with the cameras already installed.

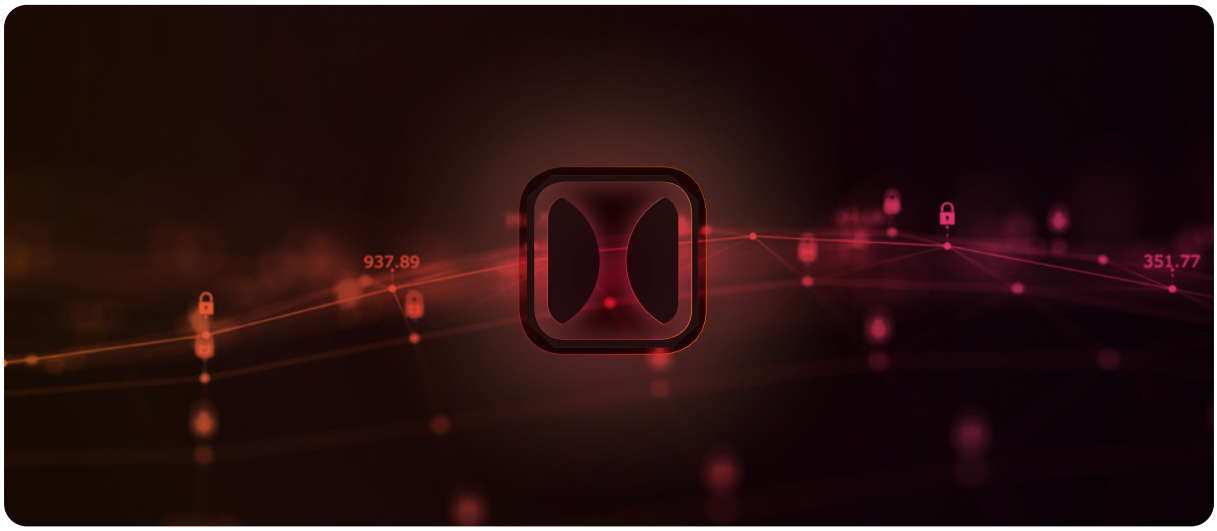
The practical difference_

Camera-embedded AI answers the question “can this camera also detect people?”. A dedicated perimeter system answers a different question: “can I certify the detection performance of this perimeter, on any camera, in any conditions, and stand behind it contractually?”

For a CMS or integrator, the second question is the one that determines liability, SLA compliance and scalability. [Note for product team: please review this section’s competitive claims before publication.]

	Camera-embedded AI	VMS module	Cloud filtering	DFUSION (dedicated edge)
Where it runs	Camera chipset	VMS server	Third-party cloud	Dedicated device at the installation
Frames analysed	Full stream, but with reduced model capacity	Depends on server load	2–6 fps	25 fps, full stream
AI approachinformation	Typically appearance-only, lightweight models	Generic detection modules	Appearance on sampled frames	Dual engine: appearance + motion
Long distance / partial occlusion	Limited — small objects exceed lightweight model capability	Variable	Weak — few frames, no temporal context	Designed for it: full temporal context + classification
Camera independence	No — tied to brand, model and firmware	Partial — tied to VMS ecosystem	Yes	Yes — works with existing cameras of any brand
Consistency across a mixed estate	Low — quality varies per camera model	Medium	Medium	High — same engine on every channel
Works without internet	Detection yes; delivery depends on link	Yes (on site)	No	Yes — fully autonomous
Perimeter certification	No	No	No	CPNI-certified
Who tunes detection quality	Camera manufacturer	VMS vendor	Platform provider	Perimeter specialist, per site

8. **Integration with CMS alarm platforms:** filtering is only half the job platforms



Reducing false alarms at source only pays off if the qualified events reach the CMS operator inside the tools they already use. A detection system that requires the operator to switch to a separate interface adds friction, training cost and response time — and in practice, alarms end up being handled outside protocol.

What a real CMS integration looks like

- **Qualified events, not raw signals:** alarms arrive in the CMS alarm management software as qualified events with classification (person/vehicle), zone and priority — not as raw camera signals to be re-verified.
- **Instant video verification:** with ClickThru, the operator opens the event footage in seconds, directly from the alarm queue, without switching platforms or hunting through a VMS timeline.

- **Native connectivity:** DFUSION integrates with the leading VMS such as Genetec, Milestone, exacq, Desico, Hikvision among others. As well as CMS alarm management platforms like Manitou, MasterMind, Immix, Sentinel and Evalink. This way the CMS keeps its existing workflow, protocols and reporting. See all integrations here

- **Audit trail included:** events carry the evidence (clip, snapshot, metadata) needed for dispatch decisions, client reporting and — where required — police response protocols under the Private Security Act.

Why this remains a differentiator

Camera-embedded analytics and VMS modules typically deliver events inside their own ecosystem: the camera brand's platform or the VMS client. Getting those events into the CMS's alarm automation software — with video attached, correctly prioritised, across a mixed camera estate — is where integrations break down. A dedicated system designed around the CMS workflow delivers one consistent event format from every site, regardless of the cameras installed there. See all our partners here

9. **How to reduce false alarms:** four levels of intervention

Reducing false alarms is not only a technological decision — it is a process that combines installation, configuration, technology and protocol. The four levels are applied in order: first resolve installation issues, then invest in more advanced technology.

Level	What it involves
Level 1 — NO COST / Installation and correct positioning	30–40% of false alarms in new installations can be eliminated by correcting positioning: reorienting cameras facing vegetation, increasing installation height to avoid small animals, improving mounting stability to eliminate vibration. No system changes required.
Level 2 — CONFIGURATION / Exclusion zones and thresholds	Configure exclusion zones for authorised access areas, adjust sensitivity thresholds by time and zone, and define detection rules that distinguish between presence and suspicious behaviour. Requires time but no additional investment.
Level 3 — TECHNOLOGY / Dual-engine AI video analytics	Replace or complement basic motion detection with AI that combines appearance (object classification: person, vehicle, animal) and motion (pattern: intrusion, loitering, presence). This delivers the most significant reduction in false alarms — up to 95%.
Level 4 — PROCESS / Measurement and audit	Audit false alarm and dispatch rates monthly per installation and zone, cross-audit reported incidents against system detections to surface missed detections, and review rules as the site evolves (vegetation, schedules, works).

Why dual-engine AI (appearance + motion) makes the difference_

AI based solely on appearance is excellent at distinguishing a person from non-person objects — but it requires high-quality, well-lit images where the object is relatively large. In outdoor CCTV environments, these conditions are rarely met. AI based solely on motion detects any pixel change — including insects, rain and leaves.The combination of both — appearance AND motion — enables detection of small objects at long distances, partially occluded or in adverse conditions, with a radically lower false positive rate.

10. Checklist: does your system have a false alarm problem?

Answer these 20 questions about your current installation. Each “yes” in the problem column indicates a potential source of false alarms or missed detections.

Installation and positioning

- ☐ Is there visible vegetation within any camera’s field of view?
- ☐ Is any camera facing a road or external vehicle access route?
- ☐ Are cameras mounted on structures with nearby vibrating machinery?
- ☐ Are there lights or streetlamps within the frame that switch on/off automatically?
- ☐ Does any camera receive direct sunlight at any point during the day?
- ☐ Are there areas without adequate night-time lighting for the installed technology?

System configuration

- ☐ Are authorised staff access routes excluded from analysis?
- ☐ Are staff access schedules configured in the system?
- ☐ Have sensitivity thresholds been specifically adjusted for this installation?
- ☐ Has a night-time stress test been performed after installation?
- ☐ Do system schedules match the client's current operational reality?
- ☐ Have different rules been configured for external perimeter zones and internal access areas?

Detection technology

- ☐ Does the system distinguish between people, vehicles and animals?
- ☐ Is analysis performed on-premises or dependent on permanent cloud connectivity?
- ☐ Does the system analyse the full video stream (25 fps) or only selected frames?
- ☐ Can the system detect intruders at long distances or when partially occluded?
- ☐ Does the system continue to operate autonomously if the internet connection is lost?
- ☐ Are missed detections recorded and analysed, or only false alarms?

Operational process

- ☐ Does the CMS receive qualified events or raw signals that require manual verification?
- ☐ Is the false alarm rate per installation and zone audited monthly?

11. Questions professionals ask about false alarms

01 /

How many false alarms are normal in a perimeter security system?

There is no universally accepted “normal” number, but the industry benchmark is clear: with conventional outdoor motion detection systems, the false alarm rate systematically exceeds 70–80% of total signals. In environments with high environmental density (vegetation, wildlife, frequent lighting changes), it can exceed 90%. With properly configured AI video analytics, the rate can be reduced to below 5–10%, which in real installations corresponds to a 95% reduction compared to baseline conditions.

02 /

Can AI completely eliminate false alarms in perimeter security?

Complete elimination is not a realistic goal in complex outdoor environments. The achievable target with current systems is a drastic

reduction — in real installations with DFUSION, 95% reductions are common. This does not mean zero false alarms, but that out of 100 signals previously generated, only about 5 remain. These residual cases are typically edge scenarios (unusual animal sizes, extreme weather conditions) that even advanced systems may struggle to classify definitively. The key point is that these remaining signals do not hide missed detections: the system continues to detect all real threats.

03 /

How do rain, fog or night conditions affect AI video analytics?

These are the most demanding conditions for any video analytics system. Basic motion detection systems are especially vulnerable to rain (which creates movement across the entire image) and night-time lighting changes (IR illumination creating shadows and reflections). AI video analytics systems trained on adverse conditions have higher resilience, but are not immune. The most effective approach is combining dual-engine detection (reducing dependency on perfect image conditions) with properly configured time-based thresholds: more permissive during heavy weather and more restrictive under optimal conditions.

04 /

What regulations govern false alarms in Spain?

Organic Law 4/2015 on the Protection of Citizen Security and Law 5/2014 on Private Security regulate obligations for security companies and users regarding false alarms. Regional governments also have regulatory authority. In practical terms, law enforcement agencies may apply penalty systems for installations with repeated high false alarm rates, and contracts between installers, CMSs and clients typically include specific clauses regarding acceptable false alarm and dispatch thresholds. In critical infrastructure contexts, the EU NIS2 Directive adds reliability and response requirements that indirectly impact false alarm management.

12. **Conclusion:** false alarms are not an unavoidable industry cost

Throughout this guide we have seen that false alarms are not an isolated failure or a minor nuisance: they are a structural problem that affects each profile in the sector differently, but which shares a common root cause. Whether it is a CMS manager handling thousands of signals per day, an installer receiving calls from frustrated clients, or a security director justifying investment to senior management, the origin of the problem is the same: systems that cannot distinguish a real threat from environmental, biological or technical noise.

And false alarms are not, by far, the most serious issue. That is the missed detection — the invisible false negative that no operator sees until it is too late. Any strategy for reducing false alarms that does not place this at the centre of its design is not solving the security problem: it is simply shifting the noise elsewhere.

The problem, in one paragraph_

False alarms are the largest operational cost in perimeter security — more than 76% of the signals reaching a CMS are false — and false negatives are its largest hidden risk: undetected intrusions with real damage and legal liability for installer and CMS alike.

How DFUSION solves it_

DFUSION resolves the problem at source: on-premises video analysis of the full 25 fps stream, a dual-engine AI (appearance + motion), and filtering that sends only real, qualified events to the CMS — inside the alarm management platforms operators already use.

The results at real installations: false alarm reductions of up to 95%, with the risk of missed detections minimised, no dependency on cloud connectivity, and reliable detection even in complex environments — long distances, partial occlusion, adverse weather, active wildlife.

In short_

DFUSION does not just reduce false alarms. It transforms the security operation: it protects the installer's liability and reputation, restores the CMS's scalability and operational efficiency, and increases the real security of the end customer.

What to do next, depending on your role

If you work in a CMS

Audit your real rate. Calculate how many of your monthly signals are false alarms and how much operator time they consume. Without that baseline figure, there is no way to measure improvement or justify investment.

If you are an installer

Check before you calibrate. Most false alarms originate in installation, not in the technology itself. Use the checklist in this guide before adjusting sensitivity thresholds.

If you are a security director

Ask for the missed detection metric. Do not settle for the false alarm rate. Ask your provider how they measure and report false negatives — this is the question that separates a mature system from one that only appears to perform well.

The core conclusion of this guide_

Reducing false alarms without increasing the risk of missed detections requires two things at the same time: analysing the maximum amount of information possible (25 fps locally, not 2–6 fps filtered in the cloud) and classifying what is moving, not just detecting that something is moving (dual-engine appearance and motion, not basic motion detection).

Any system that sacrifices either of these principles to improve the other is addressing the wrong problem.

About this guide

This content combines data from real installations using DFUSION /3 with general technical knowledge from the perimeter security sector. It is intended as a reference resource for any security professional — installer, integrator, CMS manager or security director — regardless of the technology currently in use.

DAVANTIS

davantis.com

GFA_030726_EN