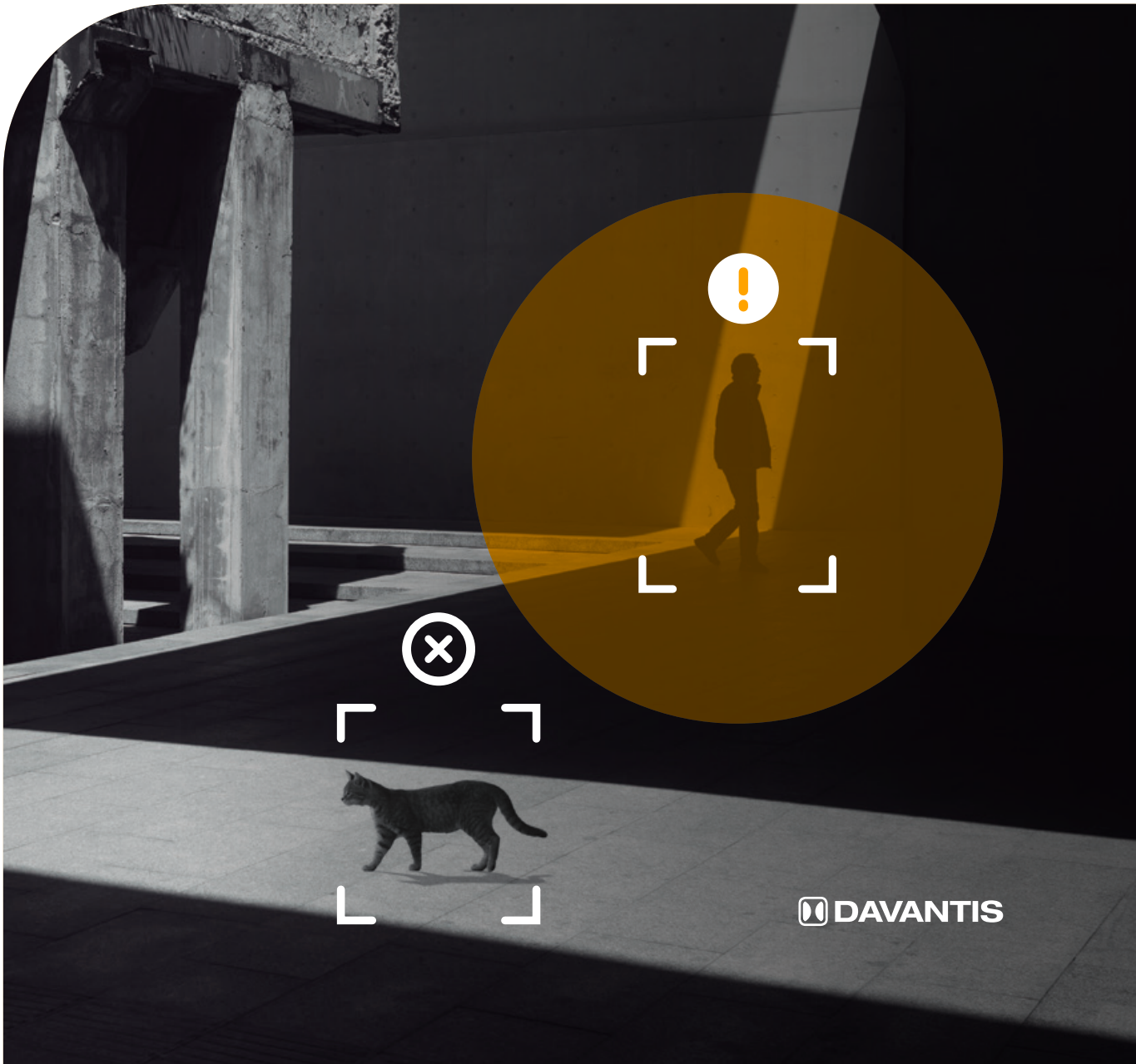
Perimeter security and video analytics /

Complete guide



Index

01_

Perimeter security

What Is Perimeter Security? _

Definition
Perimeter security is a set of measures and technologies designed to protect the physical and virtual boundaries of a property, facility, or asset.

Purpose
To prevent unauthorized access, detect intrusions, and respond to threats.

Components
It includes physical barriers such as fences, walls, and hedges, along with technologies like cameras and various types of sensors, all designed to protect the perimeter and trigger intrusion alerts in secured areas.

Role
It serves as the first line of defense within a comprehensive security system.

02_

Perimeter Security Systems

What are the most common perimeter security systems? _

The most common conventional systems for perimeter protection include sensor cables, IR beams, microwave sensors, pressure sensors, radar, and PIR detectors. However, **the most modern, effective, and efficient system is video analytics**.

Why is video analytics recommended? _

In short, many traditional perimeter protection systems have a limited detection range and typically only trigger alarms without showing what caused them. This makes it necessary to send patrols, police, or security guards, increasing costs—or to install additional cameras, which complicates and raises the cost of the project, without guaranteeing fast or accurate verification.

With the **DFUSION** product range, the camera acts as both a sensor and a visual alarm. This enables immediate detection and verification, generating real-time alerts with a snapshot and a video clip that includes a bounding box highlighting the cause of the alarm—**delivering greater speed, accuracy, and efficiency**.

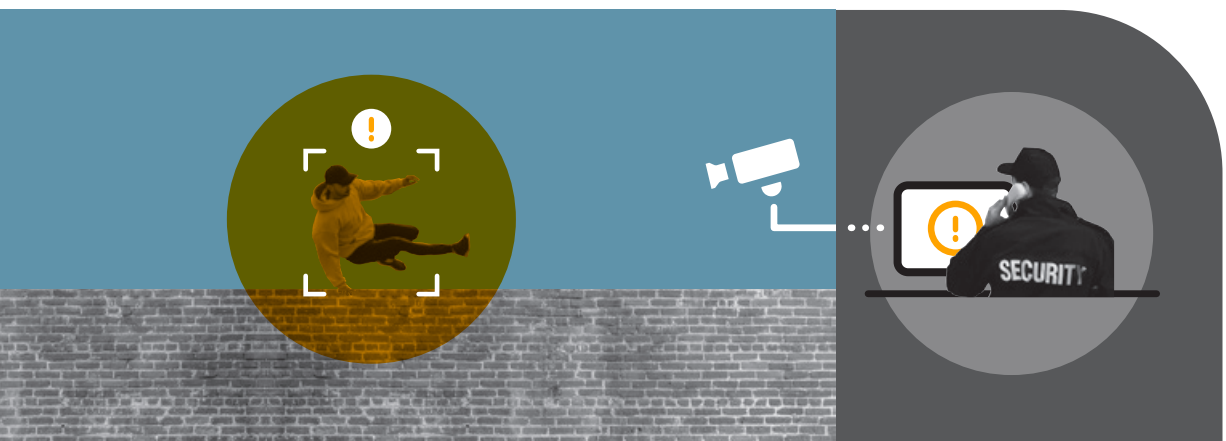
Verified visual alarms ensure that only real threats are reported to users, eliminating false alarms and improving both safety and peace of mind.

A camera connected to **DFUSION can cover large areas and detect at long distances** when installed at a sufficient height to prevent tampering without triggering a sabotage rule.

The secure area can be clearly defined, even using the camera's full image as the detection zone if necessary, **while public or external areas can be treated as pre-analysis zones** that do not generate alarms.

Maintenance is simple, and immediate assistance is available via remote access—eliminating the need for long, costly travel.

With **DFUSION**, the user benefits from a virtual security guard at a much lower cost.



03_

Identifying Ideal Clients for Perimeter Security Through Video Analytics

Ideal clients include those with perimeter security needs, such as individuals or organizations exposed to multiple risks and threats, experiencing frequent theft or vandalism, requiring personal protection at their residence, aiming to reduce physical surveillance costs, relying solely on cameras for monitoring, or dissatisfied with their current perimeter protection system. These profiles are perfect candidates for our solution.

Critical Infrastructure
These sites require high security standards to ensure operational continuity and protection against sabotage, terrorism, and vandalism. Examples include power plants and substations, water treatment facilities, food production plants, gas and chemical facilities, refineries, government buildings and facilities, data centers, ports, and prisons.

Industrial Sites
Businesses, warehouses, factories, logistics centers, and outdoor storage areas—such as lots for cars, trucks, RVs, machinery, and construction materials, as well as car dealerships—need to protect valuable assets from theft and damage.

Residential Properties

Focused on protecting residents from home intrusions and safeguarding personal property to ensure a secure living environment.

Open Areas

Locations such as solar farms, quarries, scrapyards, construction sites, and large properties where surveillance is only possible via security cameras often have insufficient protection measures, leaving them vulnerable to theft and damage.

Educational Institutions

Schools, universities, and sports centers, where the risk of theft and damage is high, require effective solutions for proper perimeter protection.

Sites with Obsolete or Insufficient Systems

Facilities using older technologies like sensor cables, IR beams, microwave sensors, pressure sensors, radar, or PIR need significant upgrades to reach optimal security levels. Similarly, transitioning from a passive 24/7 recording CCTV system to an active system with real-time alarms is essential.

04_

Perimeter Protection with Security Cameras and Video Analytics

Designing a perimeter protection system for a facility using security cameras requires a prior assessment of the perimeter and its surroundings to choose the right cameras.

Day/night cameras and thermal cameras are both excellent options.

Which is better? _

Day/night cameras with appropriate lighting are more suitable for standard ranges up to 70 meters.

Their higher resolution, color, and texture details provide more information for Artificial Intelligence (AI) algorithms.

Video analytics can detect intruders even under the most challenging conditions with a low false alarm rate.

What About Thermal Cameras?

Thermal cameras are ideal for long distances, as they do not require additional lighting.

While they are more expensive, they can reduce the number of cameras needed.

We strongly recommend day/night cameras for video analytics over standard distances, as well as dual-sensor cameras that integrate both a day/night sensor and a thermal sensor in a single device.

-

However, on a perimeter where 2 or 3 consecutive cameras can be replaced, thermal cameras can help reduce overall costs.

When to Use PTZ Cameras as Support

PTZ cameras support fixed cameras by recording additional video with enhanced zoom and detail in the intrusion area.

When controlled by the DFUSION**PRO** range, they can track intruders in real time—ideal for open areas or large, unobstructed perimeters.

They can cover multiple points from a single location, complementing the detection zones of several fixed cameras.

How to Position the Camera Optimally

Install the camera between 4 and 6 meters high to minimize blind spots and reduce the risk of tampering.

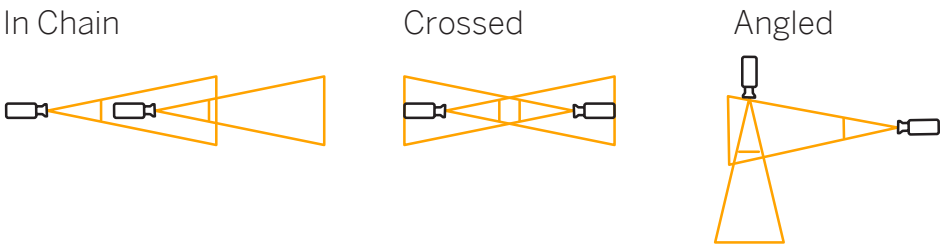
Ensure the field of view fully covers the security area, using appropriate lenses based on the space and distance to be monitored.

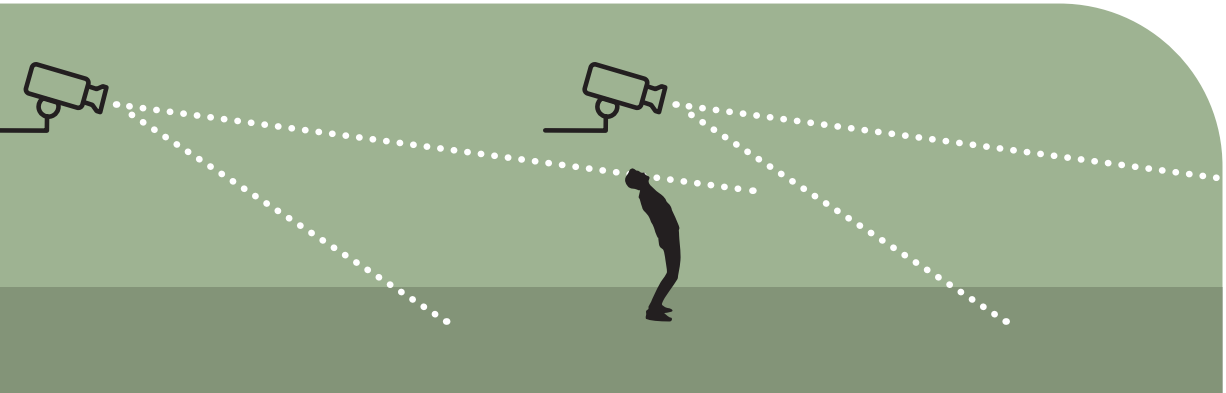
Adjust placement to avoid any elements that might obstruct the view, such as trees, poles, or other potential blockages, ensuring a clear view of the defined security zone.

Make sure the size of people near and far from the camera matches the perspective required for video analytics.

Design continuous coverage to eliminate blind spots, using simulation tools to optimize camera placement—such as our free Site Planning Tool: https://siteplanning.davantis.com.

Camera Placement to Avoid Blind Spots





05_

Key Pillars for Effective and Long-Term Video Analytics

What are the essential elements for effective and sustainable video analytics over time? _

1. Project Design

Use tools like our Site Planning Tool to accurately plan projects, ensuring cameras are placed at the correct position and height. This allows you to verify the maximum detection range as well as the horizontal and vertical field of view based on the camera model, also considering the blind spot directly below the camera.

2. Proper Camera Selection

Use day/night or thermal cameras with the appropriate lens, resolution, pixel size, or image sensor for the environment to ensure effective detection under various lighting conditions and distances.

3. Camera Installation

Cameras must be mounted securely on walls or poles to prevent movement caused by strong winds, which could lead to excessive false alarms.

4. Defining Areas of Interest

Define specific security zones within the camera's field of view so the video analytics system can focus on critical areas, reducing false alarms and increasing accuracy.

5. Use of Advanced Algorithms

Employ video analytics with **intelligent algorithms**, such as the **DFUSION** range, which enables intrusion detection and real-time verification. This solution integrates **two analytics engines**, combining traditional **Machine Learning (ML)**-based analytics with the most advanced AI technology.

6. Sensitivity and Parameter Adjustment

Allow easy and quick configuration of detection parameters, such as detection sensitivity and object size, taking environmental conditions into account to minimize false alarms and improve system reliability.

7. Visual Verification Capability

Ensure that the video analytics system provides instant images or video clips with a highlighted box around the cause of the alarm, enabling fast and accurate verification.

8. Remote Monitoring and Alarms

Capability to send real-time alarms to Alarm Receiving Centers (ARCs), allowing for a quick response to any detected intrusion.

9. Integration with Other Security Systems

Open video analytics system that integrates easily with third-party security solutions such as VMS, PSIM, or alarm management platforms in ARCs, both in new and existing installations.

10. System Arm/Disarm

It is important to define how the video analytics system is armed or disarmed, as using scheduled times can trigger false alarms if the user accesses the system outside of the set hours. More effective options include using the alarm panel's keyboard, its mobile application, or the video analytics app, such as our app compatible with Android and iOS, allowing the user to easily arm or disarm the video analytics system whenever needed.

11. Deterrent Devices

Since patrols or the police often arrive too late, after intruders have already caused damage or fled, it is important to have a quick way to deter the intruder as soon as possible. Server-based video analytics, like DFUSION, allow remote deterrence of intruders from a Centralized Monitoring Station (CMS) or App using sirens, lights, pre-recorded audio, or direct voice communication via VoIP.

12. Fast Deployment

Server-based video analytics offer a centralized setup that unifies the adjustment method for all camera manufacturers, eliminating the need for individual processes for each model or brand. This standardization speeds up installation, minimizes errors, saves resources, and ensures an efficient and agile setup, even in large projects or those with multiple devices.

13. Future Expansions

A video analytics system must be prepared for future expansions. It should be scalable, compatible with installed security systems (VMS, PSIM, cameras), and updatable so it can evolve over time.

14. Maintenance

Easy maintenance, and if possible, remote maintenance, is essential to ensure optimal performance and to make sure the cameras and system are functioning under ideal conditions.

15. Technical Support

DAVANTIS technical support stands out for its speed, specialization, and personalized attention, offering assistance from initial setup to solving complex issues. Its trained team provides training resources, software updates, and detailed guides, ensuring efficient, effective, and reliable perimeter video analytics systems.

06_

Challenges in Perimeter Security with Video Analytics

Can video analytics prevent false alarms caused by moving trees, spider webs, car headlight reflections, and also protect against sabotage? _

False Alarms

DFUSION technology, equipped with a **dual engine of next-generation AI-based analytics**, prevents false alarms caused by factors such as plants, trees, animals, insects, spiders, vehicle lights, heavy rain, wind, and more.

Protection Against Sabotage

It also **detects camera tampering**, such as rotation or lens obstruction, which can result from vandalism or natural causes like strong winds or tree branches hitting the device. It includes **technical alarms** as well, such as video signal loss, system arm/disarm status, and loss of communication with the installation, among others.

Can Video Analytics Detect Intrusions in Adverse Environmental Conditions? _

False Alarms

Traditional sensor systems can generate many false alarms due to factors like wind or animals. DFUSION video analytics, with its dual analytics engine, can distinguish between real and false events, significantly reducing false alarms without missing actual detections.

Variable Lighting Conditions

With day/night cameras and intelligent algorithms, DFUSION video analytics can operate effectively in low-light conditions—something many other video analytics systems struggle to achieve with the same level of accuracy.

Missed Detections – AI Alone Is Not Enough

AI is effective at detecting people in clear, well-lit environments, and can classify objects such as people, bicycles, or vehicles. However, it has limitations when dealing with tactical intrusions (running, crawling, crouching), brief appearances, partially covered individuals, or those carrying large objects (ladders, boxes, umbrellas, etc.), as well as in low-light, vegetated, or harsh weather conditions.

Detection in These Situations Is Key for Perimeter Security. While standard AI offers high precision with few false alarms,

it often suffers from low recall—missing actual detections. DFUSION, with its dual analytics engine, combines high detection precision with high recall, ensuring **minimal false alarms** and maximum intrusion detection.

But **what happens in real-life scenarios when an intruder jumps the fence in the farthest area from the camera, at night, and in poorly lit zones?** AI alone is not enough to detect these intrusions.

Is the Video Analytics System Tested by an Independent External Entity?

The DFUSION range is certified by the UK government's NPSA (formerly i-LIDS), **confirming its compliance with the highest quality standards** and its suitability for critical applications—such as protecting critical infrastructure and other sensitive environments where security is a top priority.

Both DFUSION and DFUSIONPRO are listed in the UK's Catalogue of Security Equipment (CSE), which helps security professionals identify the right security equipment—in other words, products that have been **evaluated against NPSA's rigorous security standards.**

National Protective Security Authority

How to Choose a Good Video Analytics System and Avoid an Inadequate One?

Choosing the right video analytics system is key to effective perimeter protection. Here are some tips to help you make an informed decision:

Detection in Adverse Conditions

A good system must accurately detect intruders even in complex environments or under challenging weather conditions.

False Alarm Rate

Look for systems with a very low false alarm rate to avoid operational issues for security personnel.

High Detection Rate

Choose systems that combine a low false alarm rate with a high detection rate, ensuring that important events are not missed.

Compatibility and Functionality

The system should offer all the necessary features for perimeter protection and be compatible with existing security infrastructure.

Open Integration

Select a system that easily integrates with platforms like VMS, PSIM, or alarm management systems at a Central Monitoring Station (CMS), providing flexibility for future expansions or the use of existing CCTV infrastructure.

Beware of Unrealistic Promises

Be cautious of systems that claim 0% false alarms or 100% detection rates. No system is perfect, and such claims are often misleading.

Independent Certification
Look for systems certified by trusted third parties, such as the UK's CPNI, which ensure proven performance in real-world perimeter protection scenarios.

Real-World Testing
Before purchasing, it's recommended to request a free demonstration and test the system in a real environment. This allows you to evaluate its practical performance.

By following these steps, you can identify a professional video analytics system and avoid options that fall short of your security needs.

Is It Possible for a User to Enter and Exit a Facility with Video Analytics Activated Without Triggering an Alarm? _

Cameras connected to a video analytics system typically operate in the following modes:

Standard Mode
Cameras immediately respond to any detected threat by triggering an alarm.

This mode does not allow users to exit the perimeter after arming the system or enter to disarm it without setting off an alert.

Entry/Exit Mode – Available in the DFUSION Range
This mode allows for configurable delays when entering or exiting a facility, enabling users to access or leave the premises without triggering alarms.

How Does Entry Delay Work?

1. The user enters the perimeter of their home, property, or business monitored by security cameras.

2. The system detects the entry and starts a programmable countdown.

3. During this time, the user must disarm the system to prevent an alarm.

4. If the system is not disarmed before the countdown ends, an alarm is triggered and a notification is sent to the Central Monitoring Station (CMS), Control Center (CC), or local security personnel.

How Does Exit Delay Work?

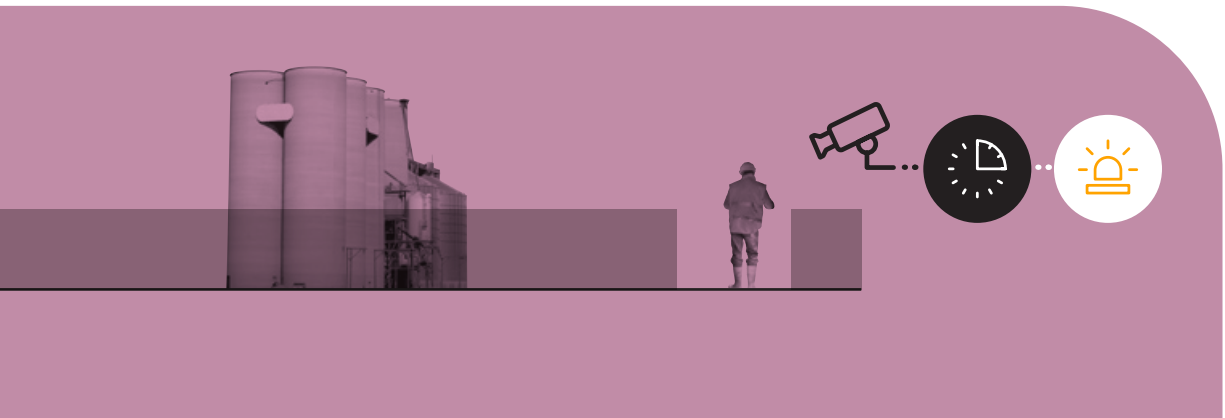
1. The user arms the system and leaves the monitored perimeter.

2. Upon exit, the system starts a programmable countdown.

3. During this time, no alarm will be generated for the person leaving the monitored area.

4. Once the countdown ends, the cameras return to active surveillance mode and will detect intrusions.

By configuring the entry/exit mode and adjusting the delay times, unnecessary false alarms when arming or disarming the video analytics system can be avoided.



Can a Real Intruder Be Identified at Long Distances in Open Areas or Large Perimeters Using Thermal Cameras?

Intruder Detection with Thermal Cameras

Thermal cameras excel at **detecting intruders over long distances** by sensing temperature differences. However, they may have limitations in clearly identifying individuals or intruders due to their reliance on thermal contrast.

Integration with PTZ Cameras

When combined with day/night PTZ cameras, detection is enhanced. **The PTZ camera can automatically zoom in on the detection area**, providing a clearer visual verification of the intrusion.

Enhancements with DFUSION**PRO** and ATK**PRO**

The DFUSION**PRO** range can record detailed zoomed video using PTZ cameras at the point of intrusion, while the ATK**PRO** **auto-tracking module** enables real-time tracking of the intruder—even after they are no longer visible in the thermal image.

ATK**PRO**

Is It Possible to Integrate Video Analytics Alerts with Maps Easily, Without Requiring an Additional VMS or PSIM?

The "MAPS IN ACTION" feature in DFUSION video analytics offers a visual and efficient way to monitor the perimeter through an interactive map-based system.

Site Planning Tool
It uses Google Maps to display perimeter-monitoring cameras on an interactive map.

Real-Time Notifications
Cameras that detect activity flash on the map and can automatically display the live video feed within the same interface.

Remote Access
Maps are accessible from any location—whether directly in the video analytics system, a Central Monitoring Station (CMS), a VMS, or a PSIM.

Benefits
Real-time visualization of incidents.
Fast, intuitive identification of intrusion zones.
Improved response capabilities and enhanced security

The "Maps in Action" feature enables efficient and visual perimeter control.

Maps
in Action

Is It Possible to Quickly Adapt Video Analytics to Different Threat Levels That Vary in Critical Infrastructure Facilities?

Factors Affecting Threat Levels in Critical Infrastructure

· Changes in the geopolitical environment
· Activities of malicious groups
· Technological vulnerabilities
· Fluctuations in internal security

Threat Levels Feature Available in the DFUSION Range

Automatic Adaptation

Video analytics automatically adjusts settings based on the threat level.

Flexible Activation

Selectable threat levels through external hardware, such as buttons that trigger inputs to a DFUSION server.

Instant Adjustments

Immediate changes to camera configurations and rules.

High Threat Level Scenario

High Sensitivity
Enhances detection and behavior analysis in high-risk situations, such as individuals crawling.

Additional Zones
Configure detection areas for early warnings.

Custom Rules
Define active security measures only at specific threat levels.

-

Objective
Quickly and accurately adjust the response based on the identified risk level.

Can Surveillance Cameras in Perimeter Security Be Manipulated?

The camera tampering detection function is also critical in critical infrastructure facilities.

Common Intrusion Method
Turning or tampering with security cameras is a common technique used to avoid detection by camera-based alarm systems.

Consequence
If a camera is rotated to face another direction, intruders can cross the perimeter without being detected.

DFUSION Solution

DFUSION uses Deep Learning technology to analyze images and detect tampering attempts.

It triggers an alarm if someone rotates the camera or covers the lens.

Tampering Rule
An automatic alert is generated in case of tampering and notifies the CMS, Control Center (CC), or local guard for immediate response.

How to Solve Perimeter Camera Movements Due to Wind That Hinder Detection? _

Problem
Perimeter surveillance cameras can experience movements due to wind, causing blurry or unstable images that make analysis difficult.

Image Stabilization

More Accurate Recognition
Stabilization reduces blur and distortion caused by movement, allowing algorithms to effectively identify objects.

Reduction of False Alarms

Unstable images can trigger false alarms, as sudden movements are misinterpreted as threats. Stabilization improves system reliability by minimizing this issue.

Implementation

Image stabilization can be achieved through advanced software, such as DFUSION, eliminating the need for costly electronic systems.

Stabilizer

How Can the Possible Low Contrast of Thermal Cameras in Summer, High Temperatures, or Fog Be Solved?

Thermal cameras are an excellent option for **long-distance** perimeter security, but both **fog and heat can reduce the contrast** of thermal images.

This can lead to **low contrast**, making it difficult for the camera to distinguish the temperature differences between a person and their surroundings. This reduction in contrast poses a **risk to detecting intruders** at long distances.

Advanced video analytics functions, such as **Virtual IR** in the DFUSION**PRO** range, **automatically enhance the scene and increase the contrast** in a defined area of the image. This **improves the detection of intruders**, as higher contrast leads to better detection.

Can a Local Guard Receive Information About an Intrusion During Their Patrol?

The lack of active monitoring and mobile notifications allows intruders to take advantage of moments when the guard is conducting their patrol and not at their fixed post. This gives them the opportunity to enter the facility, hide, and act without

Virtual IR

being immediately detected, increasing the risk of damage or theft before any action is taken.

The free DAVANTIS App, compatible with Android and iOS, can be a key tool to prevent these situations by offering:

1. Real-Time Notifications
Notifies the guard of any suspicious alarms during their patrol, ensuring they are always aware of potential intrusions.

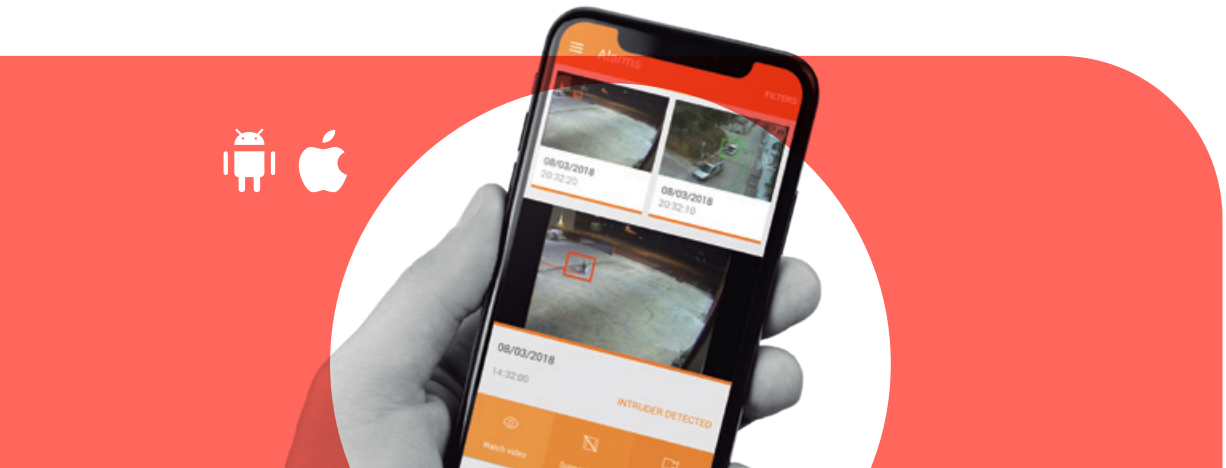
2. Remote Access to Alarms and Cameras
Allows the guard to view alarm images and videos with highlighted areas and live images to review events from anywhere, even outside the guard booth.

3. Alarm Confirmation
Facilitates immediate alarm verification to determine whether it is a real threat or a false alarm.

4. Direct Interaction with the System
Provides control over deterrent devices that can be activated remotely.

5. Increased Efficiency
Reduces reaction times and allows for quick, informed decision-making, making it more difficult for intruders to act without being detected.

This ensures that the guard is always connected to the security system, even when they are not physically at their fixed post.



For more information about our products and services, we invite you to visit our website at

www.davantis.com, where you'll find details about our solutions and how we can help enhance the security of your business.

If you have any questions or would like to receive personalized advice, please don't hesitate to contact us by email at **info@davantis.com**.

You can also call us at **+34 93 220 33 33**, and we'll be happy to assist you and provide all the information you need.

DAVANTIS TECHNOLOGIES

info@davantis.com
www.davantis.com

GVA_120525_EN