

Key elements of an Effective Perimeter Security System



Speedy detection of security breaches is a priority in all types of perimeter security projects



Outdoor perimeter security systems must be technologically advanced enough to guarantee the high levels of control and protection that installations need and be flexible enough to adapt to all technical specifications.

When protecting critical infrastructures like power stations, petrochemical plants, prisons, museums, or residential properties, the goal is always to provide efficient, cost-effective protection from intruders with a low rate of false alarms. At DAVANTIS, we specialise in developing smart video analytics technologies based on artificial intelligence (deep learning) to conquer your surveillance, control, and perimeter protection goals.

CCTV video surveillance system installers must consider the many variables that come into play when analysing and designing a perimeter security strategy. The goal is clear: maximum detection precision with few security breaches. That's why the following points must be considered when determining the essentials of an effective perimeter security system:

Speedy detection allows operators to analyse the situation immediately and take appropriate actions:

- Real-time alarm activation
- Permanent detection
- Triggering measures to deter intruders
- Ultra-precise detection to keep false alarms to a minimum
- Adaptation to the surroundings for a well-calibrated, precise security system.
- Single-layer, double layer, or multi-layer detection strategy
- Anti-sabotage systems

Detect - Dissuade

A perimeter control security system must dissuade, detect, delay, allow assess and respond to all potential threats to the site perimeter.

One efficient way to stop unauthorised access to your site and prevent theft, sabotage, vandalism, and other undesirable events is to install a combination of integrated perimeter protection systems with deterrent technologies. Our video analytics systems integrate seamlessly with

The goal is clear: maximum detection precision with few security breaches

all kinds of deterrents, such as IP loudspeakers and high-intensity floodlights, among others, adding a layer to any perimeter security installation. According to studies conducted by our technical team, integrating deterrents and video analytics systems reduces security breaches by 73.4%.

Early detection is the key to success

Smart video analytics systems detect intruders and foreign objects quickly, **keeping unwanted visitors out of your site and protecting property from theft and damage.**

All perimeter security projects should include an intruder detection system, while more demanding systems can be installed with a two-layer design.

Critical infrastructure security can even consist of multi-layer systems that ensure the highest level of perimeter security. It stands to reason that stacking complementary technologies such as fence

sensors and AI video analytics software strengthens perimeter security by boosting alarm and security systems.

In addition, systems made up of several layers of new generation technologies - such as DFUSION - are ideal for maximum security sites because installing this equipment improves the effectiveness of any perimeter intrusion protection system.

And now you have detected your intruder...

Instant access to real-time images of the cause of the alarm allows the Alarm Receiving Centre (ARC) or Control Centre (CC) to analyse and assess the situation before activating security protocols, sending out guards and taking other appropriate action.

Video analytics systems can easily be integrated with alarm

Our video analytics solutions ensure that real incidents never go undetected

management software such as CRA, VMS and PSIM. With DFUSION, you can have an integrated perimeter security system with CCTV alarm communication and analysis, giving security staff access to the images captured by the

system. Our video analytics solutions use algorithms that combine the appearance and movement of the images for precise detection, ensuring

DFUSION uses sabotage detection algorithms based on Deep Learning and combines our extensive database with real cases gathered through our expertise in perimeter security

that real incidents never go undetected. We continuously analyse massive numbers of images per second, while a false alarm filter optimises costs and lightens the load for your security staff.

Anti-tampering mechanisms

Outdoor perimeter alarm systems with CCTV are exposed to all types of tampering and sabotage risks. Technical interference in image transmission by the CCTV camera system should trigger an alarm at the Alarm Receiving Centre to solve the problem quickly.

A good perimeter protection system is essential to detect camera sabotage or manipulation, including cutting cables, blocking cameras,

and many other types of tampering.

DFUSION uses sabotage detection algorithms based on Deep Learning techniques combined with an extensive database with real cases gathered through effective perimeter management.

Need an effective video analysis system for perimeter control and protection? Contact our technical team and learn how to transform your CCTV installation into a smart perimeter security system!

info@davantis.com