



BOSCH

Invented for life

Application Note

Improve the level of security
by adding video analytics

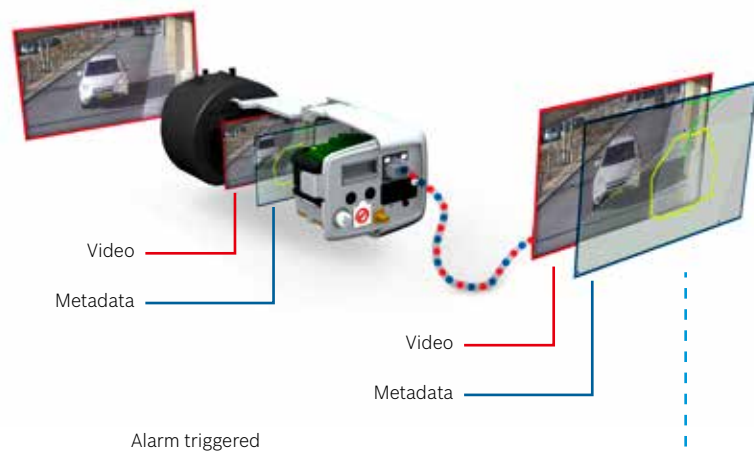
Video analytics integrated into
B/G Series Intrusion Alarm Systems

B Series and G Series control panels intelligently link each security and life safety domain for highly reliable intrusion detection and security you can trust. Bosch offers a unique level of intrusion detection by directly integrating Bosch IP cameras built-in video analytics with standard detection points and B Series and G Series intrusion control panels.



Detection you can depend on: Bosch video analytics integration with intrusion panels

Each IP camera supports up to 8 built-in video analytics rules in parallel and they can be assigned to 8 unique detection points on the intrusion panels. Each video analytics alert triggered by the camera is monitored and managed via the keypad and control panel. If an alarm is triggered, the control panel can give a command to the camera, for example to move (pan-tilt-zoom), or send the recording to an email address.



Metadata adds sense and structure to your video footage. This in turn enables your network video cameras to understand what they're seeing and alert you to any potential threats the moment they happen.

Video analytics scans each image and then triggers an alert on the intrusion panel as soon as one of the pre-defined alarm rules are met.



Professional Monitoring Station



Notification via the app/SMS/email



More powerful

B Series and G Series intrusion control panels support up to 16 Bosch IP cameras, and each IP camera supports up to 8 video analytics alerts in parallel. Each video analytics rule set in the camera is assigned to a unique detection point, and is programmed like any other intrusion point. The Bosch B Series and G Series control panels also support 4 outputs per IP camera, that can trigger the IP camera to perform functions such as pan-tilt-zoom (PTZ) controls, recording profiles, or any other IP camera function. For example, video motion detection can be used to activate points on the panel, triggering the camera to send video snapshots via email.

More accurate

While offering a very high degree of sophistication, video analytics is very easy to implement, set up and control. Fine-tuning of sensitive areas, detection fields, object shapes and movements lets you configure the system the way you want, quickly and accurately.

More reliable

To help ensure alarms are only triggered for real events, camera features such as camera calibration and perspective correction greatly enhance video analytics accuracy and reliability. Statistical analysis of the captured images makes the system highly weather resilient. Rain and snow is filtered out and image stabilization ensures that only movement within the captured areas is detected, and not movement caused by the camera swaying in the wind. Special filters for size, speed, direction and aspect ratio minimize false alert rates while allowing for flexibility in video analytics alert programming.

More intelligent

Any video analytics alert triggered by the camera that fits the preprogrammed video analytics criteria immediately faults the corresponding point on the B and G Series control panels until the video analytics alert clears.

Video analytics intrusion port can be configured as:

- ▶ Interior Follower when the video analytics alert is 'motion detection', 'line crossing', or 'object in field'
- ▶ 24 hour for critical video analytics alerts such as 'object removed' or 'camera tampering'
- ▶ with point attributes such as cross zoning or monitor delay for alarm verification purposes.



As soon as a person or object enters the pre-defined loitering zone, and the loitering timer is set for 60 seconds, the camera will trigger a loitering alarm.

The loitering alarm will be reported to the control panel, from which then the information flows to the keypad, alerting the users of the loitering alarm.

Video analytics alert Description

Line Crossing

Someone has passed into a restricted area and crossed a defined line. Multiple lines can be used to customize the detection alert.



Loitering

The video analytics alert faults a detection point when someone has lingered for too long in an area. This can prevent crime in a parking area, lobby, or ATM vestibule.



Idle Object

Whether it's a car parked illegally or an object left behind, video analytics can fault a detection point and immediately notify a responder of the threat.



Object Removed

If an object disappears from its usual position, video analytics automatically faults an intrusion point. Access control systems could immediately lock down the site's parameter, preventing the object from leaving the building.



Crowd Detection

The video analytics will generate an alarm if a number of objects are located within a certain area. Applications include vandalism, rioting, terrorism, and maximum occupancy.



Object in Field Entering Field Leaving Field

Video analytics alerts can fault a point when an object enters a restricted area, leaves an area, or if an object is in an area. All alerts can be used together to detect unique or specific sequence of video analytics events.



Camera Tampering

An intrusion input point is triggered when the camera is being tampered such as if the camera has been moved, covered, masked, or tampered with.



Object Filters

You can program video analytics detection characteristics for an object such as aspect ratio, speed, size, direction, and object color. All object filters can be combined to provide fully customizable alerts.



Bosch Security and Safety Systems

Protecting lives, buildings and assets is our aim. Our product portfolio includes video security, intrusion detection, fire detection and voice evacuation systems as well as access control and management systems. Professional audio and conference systems for communication of voice, sound and music complete the range.

Visit [boschsecurity.com](https://www.boschsecurity.com) for more information.