tyco | Illustra

Illustra Video Intelligence Analytics

Illustra **(ISIN-P02Z321-N)** has powerful video intelligence analytics automatically analyze captured video and alert users of specific motion detected activities. Available on the Illustra IP camera series, Illustra creates a cost-effective solution for onboard video analytics without the need for a dedicated analytics server.

Benefits of Video Analytics: -

- Automatically detect and notify security personnel of suspicious events
- Streamline security operations to see relevant video evidence immediately
- Minimize search time with configured video analytic alarms
- Save expenses and network load with intelligent analytics on the edge

  Choose analytic alarms including: Motion detection/video tampering alarm/Line crossing detection/ intrusion detection/ region entrance detection/ region exiting detection/unattended baggage detection, object removal detection/Face Capture.
- Configure multiple analytic rule types to trigger at once.

These features can meet a wide range of surveillance requirements in various settings. The feature set includes fixed dome, bullet, and fisheye cameras to accommodate a variety of installation locations. They can be utilized to monitor office buildings, retail outlets, and industrial assets that are less frequently patrolled by security personnel. VCA Events are integrated into the Illustra camera, allowing for quick searches via the preserved film. The rapid video prompts allow security staff to respond promptly to any issues.

Minimized No. of False Alarms: A human silhouette database and quick reactions using VCA technology are key components of the Smart VCA. Human appearances in a video monitoring area are promptly recognized by the smart engine. Because most video surveillance involves people as the objects of interest, the People identification feature allows customers to easily customize their installation.

Traditional video content analysis is mainly reliant on the detection of pixel changes or motion vectors, and false alarms might be produced by swaying trees, passing clouds, or even the sight of small animals. Smart VCA detection, with comprehensive

identification rules and an adjustable temporal filter, can overcome the flaws of standard video detection and make setting easier at a monitoring location.

Smart VCA Individual Features: -

Motion Detection -

Motion detection enables you to define a region of interest in the camera's field of view which can be used to trigger an Event Action. Multiple areas of interest can be selected in the field of view but only one Event Action may be triggered.

Motion detection through advanced motion detection technology

- Illustra Camera combines the commonly used motion detection capability with advanced learning algorithms that distinguish people and vehicles from other moving objects.

- Advance Motion Detection allows them to concentrate their security efforts on actual dangers by reducing false flags brought on by animals, falling leaves, and heavy rain, as well as by keeping watchful alarm triggering.

How Advance Motion Detection work?

- Illustra Camera advance Motion Detection features person & vehicle target classification, easy configuration, and efficient playback.

Person and vehicle target classification

- Illustra Cameras algorithms are trained to categorize objects in movies into three categories: people, vehicles, and other. Users can further tune the algorithms to automatically recognize people, automobiles, or both based on their individual needs, and then notify them in real time.

People/Person

Vehicle

- Watch the motion on screen and adjust the sensitivity until the motion cells correspond to the on-screen human figures. The same is true if you want to identify bigger objects, like cars. Adjust the sensitivity so that the motion cells' appearance more closely matches the appearance of the objects you are interested in.
- The comparison of the same object found using various sensitivity levels is displayed below. Excessive motion cells are visible at sensitivity level high, but inadequate motion cells are detected at level low.

Sensitivity: High

Sensitivity: Low

Motion Detection Best Practices –

To ensure you get the highest quality results when using Motion Detection on the camera it is recommended that you adhere to the following:

- An object exhibiting motion needs to be at least 8x8 pixels in size to be detected.
- The colour of the object (in gray scale) should be approximately 10-15% different than the background.
- Exclude the Time Stamp region from motion detection, because the time stamp changes constantly and could register as motion.
- Try not to point cameras into sunlight, because high brightness prevents detection of movement of bright objects such as a person with a white shirt.

Video Tampering –

Video tampering is a feature that detects and recognizes when the camera is covered or obscured by a person's hand or an object. It is possible to send an alert notification email as soon as the camera is obstructed or vandalized, allowing you to react quickly and contact the police or someone else who can assist you prevent a crime from occurring.

Detecting sabotage on PTZ (Pan-Tilt-Zoom) cameras involves identifying signs of intentional tampering, covering, or misalignment of the camera, which are often intended to obstruct surveillance. Implementing an effective PTZ camera sabotage detection system generally involves a mix of software and hardware techniques, here are key methods to achieve this:

Video Tampering Detection –

- **Blur Detection:** Algorithms can detect if the camera view is abnormally blurry, which could indicate someone has sprayed or covered the lens.
- **Scene Change Detection:** Analyze frames for abrupt, persistent changes in the camera angle or zoom level, suggesting forced redirection of the PTZ lens.
- Algorithms can detect if the camera view is blocked by cloth/Spray etc.
- **Immediate Notifications:** Upon detecting any tampering or sabotage attempt, the system should trigger an alert to security personnel for real-time response.
- **Redundant Backup Recording:** Use on-board SD cards to keep a backup feed in case the primary stream FOV is compromised.

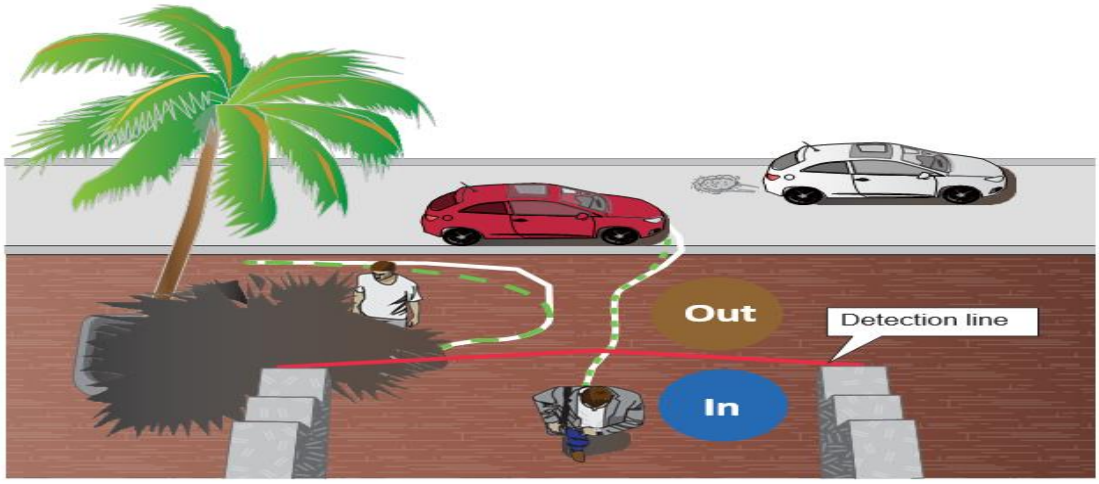
Some examples of video camera sabotage. (a) No-sabotaged image. (b) Partial occlusion/Hide view example. (c) Defocus example. (d) Scene example

Line Crossing –

Used to detect when objects enter a protected area through a perimeter area, or detect when an object is in the perimeter area. Draw line of interest to define the protected area. Once the virtual plane is detected being traversed according to the configured direction, a set of alarm action is triggered.

Line Crossing Detection-

- The Line Crossing detector identifies one or more people crossing a virtual tripwire. The traffic direction can be assigned on the screen for people crossing the line in one or both directions.
- Detects entry/exit through virtual lines.
- Detects and sounds an alarm in a certain direction.
- The detection line can be used as a fence border to determine whether someone has passed an articulated line around a perimeter.



- **People walking direction:** By default, a detection line will appear on screen, use your cursor to change its shape and location.

  Out → In
  In → Out
  Out ⟷ In

  Choose the line direction that is most appropriate for your purpose. Please see the image below.

- **Sensitivity:** The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

- **Detection Target:** You can select Human, Vehicle, or Other as the detection target. If Human is selected, only human beings will be identified as detection objects and as well as Vehicle and Other.

- Linkage Method tab to select the linkage method taken for the region entrance alarm, Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable

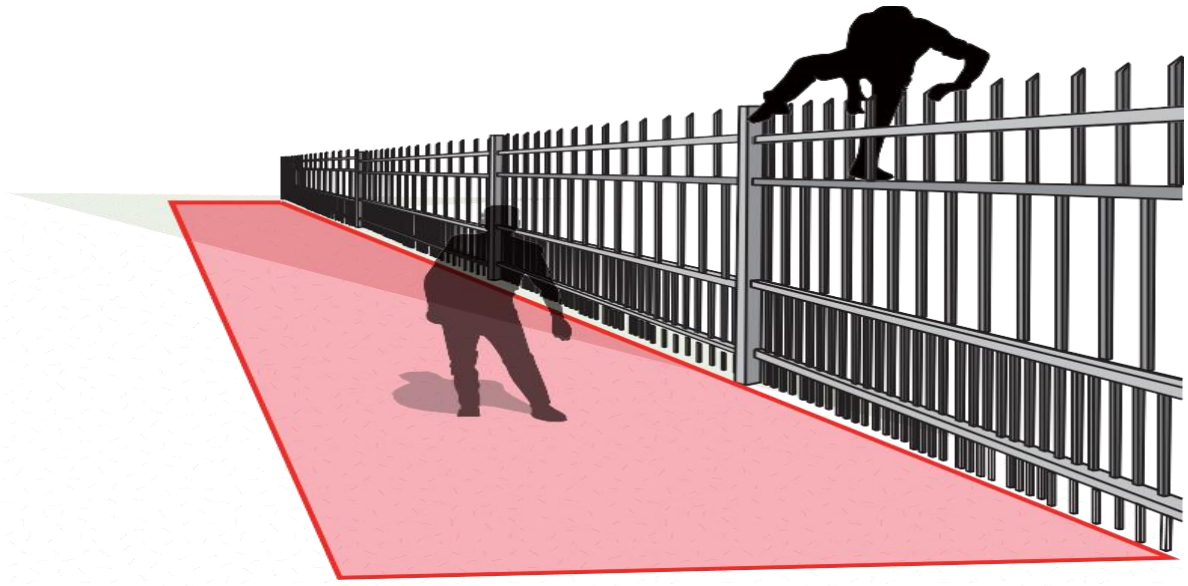
Intrusion Detection –

Illustra camera intrusion detection is a security technology that combines PTZ cameras with intelligent analytics to monitor and respond to unauthorized entry or unusual activities within a surveillance area.

The user can utilize intrusion detection if there is a location in the surveillance image that requires extra care or that is entirely sensitive. To cover the entire sensitive area or location, the user must set an enclosed polygon area (a rectangle or an irregular shape) in the surveillance image. Two kinds of events that the user is worried about can be handled by intrusion detection. One kind occurs when the target moves into or out of the space. The other is when the target shows up in the vicinity. This feature is employed to identify people and/or vehicles. Lawns, entrance/exit, guarded areas, and areas where driving is prohibited are among the application scenarios. Beyond the bare minimum of safety precautions .It can be utilized to address the missed alarms problem. Like the warning line, a specific area of target movement must be set aside at the area line's boundary in order to detect an entry or leave event.

The applicable scenarios of this feature can be Intrusion Detection -

- Detects after-hours entry into bank vaults and schools or any critical area.
- Detects unauthorized entry to emergency exits, fire escapes, and restricted areas.
- **Automatic Alerts:** When an intrusion is detected, the system can automatically send alerts to security personnel or trigger alarms. PTZ systems allow users to customize alert criteria based on the Threshold(s) ,sensitivity, Target Type.
- **Threshold:** The threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
- **Sensitivity:** The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
- **Detection Target:** User can select human, vehicle, or other object as the detection target. If Human is selected, only human beings will be identified as detection objects, so as the other two options.
- Linkage Method tab to select the linkage method taken for intrusion detection, Notify Surveillance Canter, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output, Trigger Recording, Smart Tracking are selectable.



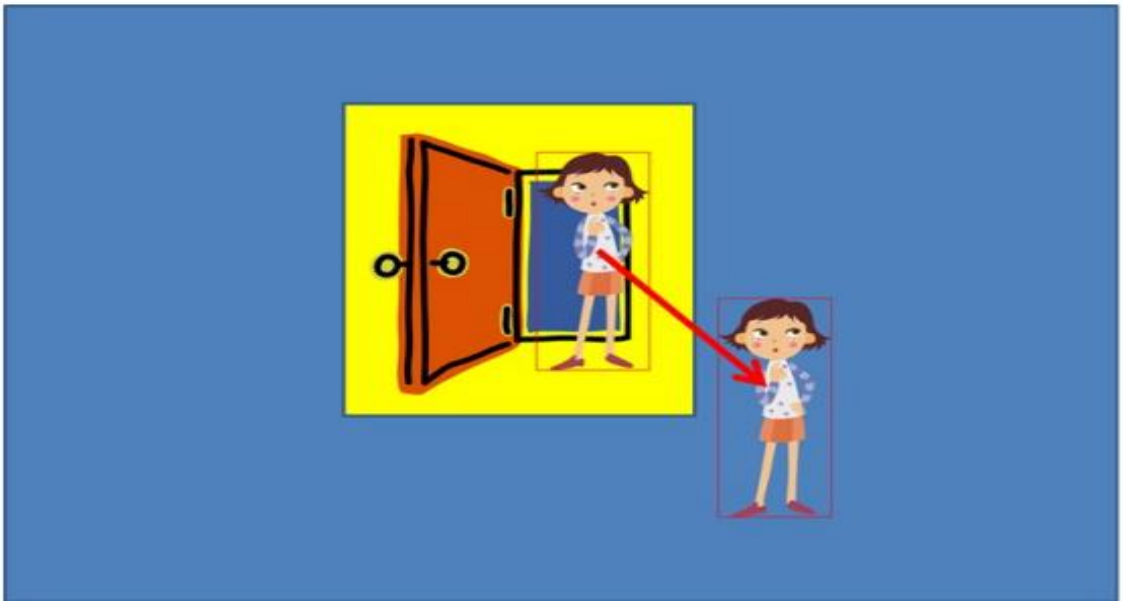
Region Entrance/Exit Detection –

Region entrance/Exiting detection function detects people, vehicle or other objects which enter/exit a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Region Entry -
Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

Region Exit -
Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

Overlap (%): The amount of detected object that must be in the region of interest when the object leaves the scene for an alarm to be triggered. The object must appear in the scene while being outside the region of interest by the same amount. For best results select a higher overlap setting.



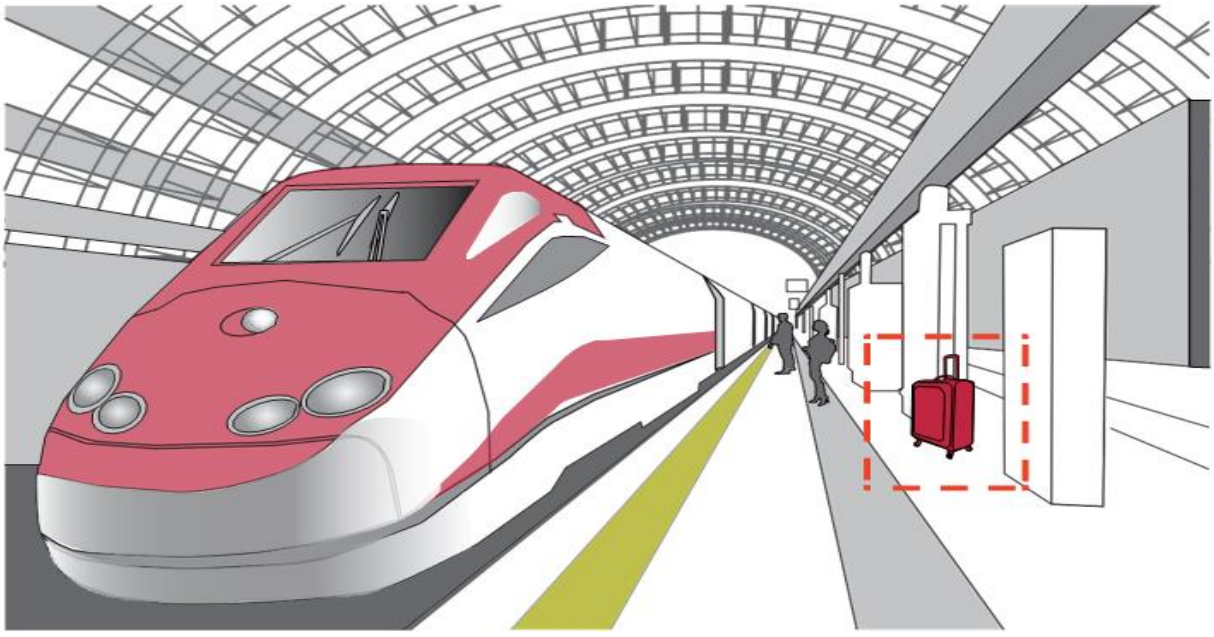
The yellow ROI complete contains the door

Unattended Object Detection –

The Unattended Object detection can be used to detect objects intentionally orunintentionally left in scene. Illustra camera in surveillance and security systems supports the cover large areas with adjustable viewing angles and zoom capabilities. Position the camera in an area where it can monitor the expected zones for objects detection. Object detection in cameras involves using various algorithms and techniques to identify the objects in the video feed:

Object Detection Techniques -

- **Deep Learning:** Object detection based on Object size, Threshold(s), Sensitivity, Detection area etc.
- **Linkage Method:** Alarm can be linkage with Email, FTP/SD Card, Alarm centre etc . Calibration: Configure the camera's pan, tilt, and zoom settings to optimize the field of view for detecting objects
- **Detection:** The system will continuously analyze the video feed for objects, distinguishing between normal movements .
- Alert System: When an object meets the criteria, trigger an alert for security personnel or record the event for further investigation.
- **Unattended objects appeared:** Select a Sensitivity Leve before triggering an event after an object is left in scene.
- **Object maximum/minimum size**: Use these size parameters to determine the size of the objects to be detected in the area

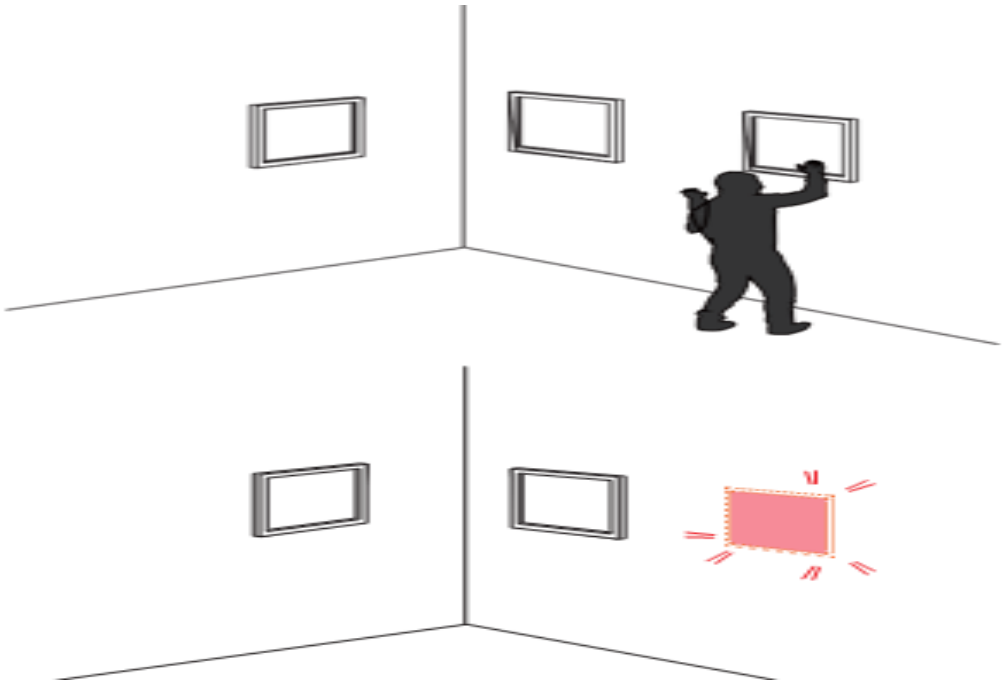


Object Removal Detection –

The Object removal detection can be used to remove objects intentionally or unintentionally remove in scene. Illustra camera in surveillance and security systems supports the cover large areas with adjustable viewing angles and zoom capabilities. Position the camera in an area where it can monitor the expected zones for objects Removal. Object removal in cameras involves using various algorithms and techniques to identify the objects in the video feed, Alert detects when object theft occurs in storage areas or warehouses or critical areas . It is helpful when there aresecurity personnels monitoring the scene, yet their attention went down through time:

Object Detection Techniques -

- **Deep Learning:** Object removal based on Object size, Threshold(s), Sensitivity, Detection area etc.
- **Linkage Method:** Alarm can be linkage with Email, FTP/SD Card, Alarm centre etc . Calibration: Configure the camera's pan, tilt, and zoom settings to optimize the field of view for detecting objects
- **Removal:** The system will continuously analyze the video feed for objects, distinguishing between normal movements .
- Alert System: When an object meets the criteria, trigger an alert for security personnel or record the event for further investigation.
- **Object maximum/minimum size**: Use these size parameters to determine the size of the objects to be detected in the area



Face Capture –

The next level up from detection is face capture. At this stage, the NVR,VMS, or camera will identify a face in the picture or video and record that specific face image for subsequent analysis. An alarm will also be sent. Face capture detects the presence of human faces in the field of view.

The applicable scenarios of this feature can be:

- By tagging the video frames which contain facial features, the administrator can later search for the video clips with presence of these faces in a more efficient manner.
- Instead of searching through hours of recordings, face detection can facilitate the process of forensic search in recorded videos. Objects irrelevant to facial features will be filtered out.