Video Analytics

Guide

MARCH networks

TRANSFORMING THE WAY YOU VIEW YOUR BUSINESS

About March Networks

March Networks® (TSX:MN) is a global provider of intelligent IP video solutions. For close to a decade, the company has helped some of the world's largest commercial and government organizations transition from traditional CCTV to networked video surveillance used for advanced security, loss prevention and risk mitigation. VideoSphere®, the company's enterprise-class video management portfolio, includes open-platform VMS software complemented by high-definition IP cameras, encoders, video analytics and recording platforms, as well as outstanding professional and managed services. March Networks systems are delivered through an extensive distribution and partner network and currently support over one million channels of video in more than 50 countries.
www.marchnetworks.com.

Our Commitment to a Green Tomorrow

March Networks takes pride in its commitment to social responsibility and environmental sustainability. Our employees, suppliers and valued partners are passionate about designing environmentally friendly solutions for our customers and minimizing the company's carbon footprint.

We embrace environmental sustainability as part of our overall strategy and business values with multiple initiatives to ensure that we do our part to create a cleaner, healthier environment for future generations. The steps we have taken affect all aspects of our organization and involve our senior management team, employees, suppliers, partners and customers. You can receive further details at:
Company General: http://www.marchnetworks.com/resources/default.aspx?id=81
Product Specific: http://www.marchnetworks.com/Files/RoHS-WEEE_Compliance_Statement_EN.pdf

Customer Support and Assistance

North America

Telephone — 613 591 1441
Toll Free (US & Canada) — 1 800 472 0116
Fax — 1 613 591 1858
E-mail — techsupport@marchnetworks.com

EMEA

Telephone — +39 0362 17935 extension 3 (CET)
Fax — +39 0362 17935 90
E-mail — milantechsupport@marchnetworks.com

APAC

For former March Networks Products:

Telephone — 1 613 591 1441
Fax — 1 613 591 1858
E-mail — techsupport@marchnetworks.com

For former Cieffe Products and VMS:

Telephone — +39 0362 17935 extension 3 (CET)
Fax — +39 0362 17935 90
E-mail — milantechsupport@marchnetworks.com

Providing Documentation Feedback

At March Networks, our goal is to produce documentation that is technically accurate and informative. If you have comments or suggestions about our online Help and documentation, you can e-mail us at: techwriters@marchnetworks.com.

Trademarks

Notice of Rights

Part Number

22748 R2.0 Most Recent Revision: May 18, 2010

Table of Contents

Chapter 1

Welcome to Video Analytics

The March Networks video analytics provide you with the ability to monitor your environment more effectively by allowing you to configure alarms for specific events.

The following topics are covered in this chapter:

Understanding Video Analytics

The March Networks suite of video analytics are enhanced surveillance tools which detect and track actions or events captured in live video. You can use video analytics to alert you to unusual incidents or potential threats in your monitoring environment, or to gain information about employee or customer behaviors, or other operational activities.

March Networks video analytics are available on specific cameras and encoders and on March Networks recorders running R5 software. For a list of supported cameras, encoders, and recorders, consult your March Networks representative.

Available Video Analytics

You can configure video analytics using the Administrator Console software. The Live Monitoring Console then allows you to be notified of alarms as they occur, view the live video, and respond to alarms in real-time. Some video analytics are detected by the device, such as a recorder, while others are detected by the camera or encoder.

For more information about configuring analytics, see the *Administrator Console User Manual* or online Help, available on the March Networks software CD.

Table describes the March Networks video analytics.

Table 1: March Networks Video Analytics

Analytic	Description
Field of View Monitoring	Detects and notifies you when the camera's field of view changes. A field of view alert occurs when the camera is no longer recording its intended field of view, due to being moved, losing focus or experiencing decreased signal quality.
Camera Obstruction Detection	The device can automatically detect when a camera's field of view has been obstructed by an object. For example, the device can notify you when a jacket is placed over the camera lens or an object such as a display sign is placed in front of a camera.
Area Obstruction Detection	Detects when any part of an object of specified size remains in the camera's defined area of interest for a defined duration, for example, a suspicious package that has been left behind or a large crate that is blocking a fire exit, and generates an alarm.
People Counting	Lets a camera that has been mounted over a doorway count people who enter and exit through the doorway. You can enable people counting on one or more cameras.
Queue Length Monitoring	March Networks cameras and encoders have built-in queue length monitoring abilities that allow them to detect when a certain percentage of a waiting area is occupied by a queue of stationary people.
Facial Detection	Detects faces in a scene and triggers an alarm when the camera detects a fully exposed face. This alarm can be used to ensure that the camera has a clear image of each person entering a secure area, by using the face alarm to trigger a door to unlock.

Table 1: March Networks Video Analytics (Continued)

Analytic	Description
Loitering Detection	Detects when an individual remains in an area for longer than a specified length of time. When loitering detection is enabled and configured, the live video displays boxes around any individuals in the specified area and a counter displays the length of time they have been in the area. If a person remains in the specified area for longer than the configured time, a loitering alarm is triggered.
Perimeter Protection	Detects when an individual or object crosses a certain point in the camera's field of view. Optionally, you can specify that you only want to detect when an individual crosses the line and is moving in the direction you specify. This analytic is also known as a wire cross alarm.
Occupancy Detection	Detects and follows the movement of people or vehicles and raises a tracking alarm when a person or vehicle moves from one specified zone to another.

What Does This Guide Provide?

This guide provides you with the physical setup and usage guidelines to maximize the video analytics features available on March Networks devices, cameras, and encoders, as well as the information required to avoid the generation of false alerts.

Further information on setting up video analytics is available in the *Administrator Console User Manual* or online Help, available on the March Networks software CD.

Chapter 2

Field of View Monitoring

The field of view monitoring feature is a licensed tool that lets the device monitor connected cameras and alert you when the camera's view changes. This feature is useful when you are monitoring several cameras at different organizations and want to be automatically notified when changes occur.

When the camera's field of view changes, and the change lasts for at least 24 hours, the device generates an alert to notify you. For example, the camera's field of view can change when a camera is moved from its original position. It can also change when a camera failure occurs, such as a change in camera focus or decreased signal quality.

You cannot configure an IP camera or a People Counting camera for field of view monitoring.

Although a change must last for at least 24 hours before an alert is generated, the device does not count any periods of time during which there is very low or no interior or exterior light source as part of this 24 hours. So, if there are 12 hours of darkness at night, an alert actually takes between 36 to 48 hours to generate (depending on when the field of view change occurs relative to the period of darkness)

The following topics are covered in this chapter:

Field of View Monitoring

Further to the field of view monitoring information provided in the *Administrator Console User Manual* and the online Help, please review the following guidelines for setup and use, and the potential causes of field of view alerts.

Field of view monitoring is not supported by the 4516 C NVR.

Field of view monitoring is only available on recorders running release 5.2 and later.

Setup and Usage Guidelines

To ensure proper setup and use of the field of view monitoring feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable field of view alerts for PTZ cameras.
- Indoor scenes are recommended. We recommend that you disable field of view alerts for outdoor cameras.
- This feature works best in areas where the majority of the scene remains constant over time. For example, the lobby in an office building or a hallway in a shopping mall are both appropriate for field of view monitoring. Permanent changes to major portions of the scene may cause the device to generate a field of view alert.
- Avoid scenes where windows take up more than half of the camera's view. This also includes scenes that reflect outdoor conditions, such as mirrors and swimming pools.
- Ensure that sufficient lighting is provided for at least 56 hours over one week so that the device can properly learn the scene in the period required. Scenes that remain in complete darkness for much of the time are not appropriate for field of view monitoring; the device fails to learn.

Possible Causes of Field of View Alerts

The following situations cause the device to generate field of view alerts:

- The camera has been disconnected and replaced.
- The camera has been moved and is now showing a completely different scene.
- A 24-hour period of video sync loss has occurred.

Chapter 3

Camera Obstruction Detection

Camera obstruction detection allows a device, such as a recorder, to automatically detect when a camera's field of view has been obstructed by an object. This licensed feature is useful when you are monitoring several cameras at different organizations and want to be notified of an obstructed camera within five to 30 minutes. Once you enable this feature, you can set up camera obstruction detection by specifying how long the obstruction must last before you receive an alert. For example, the device can notify you when a jacket is placed over the camera lens or an object such as a display sign is placed in front of a camera.

When the device detects that the camera is severely obstructed, it generates an alert to notify you. You can then respond to these alerts.

You cannot configure an IP camera or a People Counting camera to detect camera obstructions.

No calibration period is required for camera obstruction detection. The device starts alerting you of camera obstructions as soon as you choose a camera obstruction duration.

The following topics are covered in this chapter:

Camera Obstruction Detection

Further to the camera obstruction detection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for setup and use, and the potential causes of camera obstruction alerts.

Setup and Usage Guidelines

To ensure proper setup and use of the camera obstruction detection feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Indoor scenes are recommended. We recommend that you disable this feature on outdoor cameras.
- Avoid scenes where windows take up more than half of the camera's view. This also includes scenes that reflect outdoor conditions, such as mirrors and swimming pools.
- Ensure some lighting is always present. At a minimum, security lighting is sufficient. A sudden drop in lighting levels may cause the device to generate a camera obstruction alert.

Possible Causes of Camera Obstruction Alerts

The following situations cause the device to generate camera obstruction alerts:

- The camera has been disconnected and replaced.
- The camera has been moved and is now showing a different scene.
- Prolonged periods of video sync loss have occurred.

A camera obstruction alert may not be generated in any of the following circumstances:

- A camera is obstructed by a translucent object, for example, water or other liquids, but it still possible for the device to detect the original scene through the object.
- A camera is obstructed by an object that continues to move. For example, the camera is covered by a piece of paper that flaps in the wind. The camera obstruction algorithm assumes that no motion will occur in an obstructed field of view.

Chapter 4

Area Obstruction Detection

The area obstruction detection feature is a licensed tool that allows a device to automatically detect when any part of an object of specified size remains in the camera's defined area of interest for a defined duration, for example, a suspicious package that has been left behind or a large crate that is blocking a fire exit, and an alarm occurs.

You cannot configure an IP camera to detect area obstructions.

You cannot configure a people counting camera to detect area obstructions.

The following topics are covered in this chapter:

Area Obstruction Detection

Further to the area obstruction detection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for setup and use.

Setup and Usage Guidelines

To ensure proper setup and use of the area obstruction detection feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Indoor cameras are required. We recommend that you disable this feature on outdoor cameras.
- Ensure some lighting is always present. At a minimum, security lighting is sufficient. As well, lighting must be consistent. We recommend locating the camera where streams of sunlight or reflected sunlight are not present. Note that if an object has a prominent shadow, the shadow is interpreted as part of the object.
- High contrast is required. We recommend using professionally installed/focused cameras with high resolution and no transmission noise.
- A consistent background is required. Ensure that the camera's field-of-view does not largely contain any of the following:
  - Frequently opening/closing doors
  - Large passing objects/vehicles
  - Reflective surfaces
  - A group of moving objects (i.e. people) that may collectively and persistently consume the area of interest

  An object that is placed within the camera's area of interest must remain unobstructed by other objects for at least five consecutive seconds before it is considered an obstruction. For example, if a bag is dropped in a crowd of people, the bag is not detected until the area remains clear (the crowd disperses) for five consecutive seconds.
- If a complex scene is generating unwanted alarms, we recommend you increase the amount of time that must elapse before an alarm occurs. For information about configuring this delay, see the "Configuring Alarms" section of the *Administrator Console User Manual*.
- Ensure you specify the minimum area of interest. The area of interest should only include the specific region that you want to monitor for obstructions. It may be necessary to draw multiple areas of interest to omit any regions that could generate unwanted alarms.
- Ensure you set the area obstruction sensitivity to a suitable level. If the sensitivity level is too high, obstructions that may be too small to be of interest will generate alarms.

- An object is not detected as an obstruction and does not cause an alarm if:
  - The object is not at least partially within the specified area of interest.
  - The object is too small for the algorithm (less than 8 pixels in width or height for a CIF-sized image.
  - The object is large enough to be considered a camera obstruction, rather than an area obstruction. For information about camera obstruction detection, see the *Administrator Console User Manual*.

Chapter 5

People Counting

The people counting feature is a licensed tool that lets a camera that has been mounted over a doorway count people who enter and exit through the doorway. You can enable people counting on one or more cameras.

You cannot configure an IP camera to count people.

If you enable a camera to count people, you cannot enable any other video analytics functionality on this camera. If other video analytics were enabled on this camera before you enabled people counting, they are disabled, and these other video analytics are not automatically re-enabled when you disable people counting.

The device does not record video from a people counting camera. In order to access people counting data (counts and when they occurred), you must be working in an ESM-managed environment so that you can use the people counting reporting tool, which queries the ESM for this information.

When a camera is configured as a people-counting camera, it does not appear in the Investigator or Live Monitoring Console, and users cannot access video from the camera.

The following topics are covered in this chapter:

People Counting

Further to the people counting information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for camera installation and setup, as well as configuration and usage.

Camera Installation and Setup Guidelines

For the people counting feature to function accurately, please install people counting cameras using the following guidelines:

- The camera's auto-iris must be disabled.
- The camera must be mounted inside the doorway in such a way that the lens is pointing directly towards the floor (in other words, the camera is perpendicular to the floor).
- Indoor doorways with good lighting conditions are required. Shadows or fluctuations in light levels due to outdoor lighting changes must not occur within the camera's field of view.
- The base of the camera's field of view should be positioned where the doorway meets the floor.
- The camera's field of view should include the entire exit/entry area; otherwise, counts will not be accurate. It should include an area in which people walk vertically through the field of view and then through the doorway (or vice versa).
- We recommend that the camera's field of view not include areas of motion not related to entry and exit, for example, where automatic doors or cashier stations are located. If areas of motion exist at the edges of the field of view, you can mask the field of view to isolate an area of interest. For information about isolating an area of interest for a people counting camera, see the "Configuring People Counting" section of the *Administrator Console User Manual*.
- Floors within the camera's field of view should not be highly reflective, as they may produce noticeable shadows.
- We recommend that the camera's field of view should accommodate two to four people walking in single file through the entrance/exit. This allows the camera adequate time to count. For more accurate installation parameters, refer to Table 2, Table 3, and Table 4.

Accurate coverage of the traffic flowing through a selected doorway requires proper selection of the camera lens, CCD/CMOS, and camera installation height. In general, a single person entering or exiting through the doorway must be smaller than the isolated area of interest; however, if a person is too small within the area of interest, it may be difficult for the camera to distinguish individuals within a group of people. As well, a camera with a fish eye lens that has been mounted too low causes distortion. Refer to Table 2 for information on varying installation parameters that allow coverage of different doorway widths based on a 1/2" CCD/CMOS, Table 3 for similar information based on a 1/3" CCD/CMOS, and Table 4 for similar information based on a 1/4" CCD/CMOS.

Table 2: 1/2" CCD/CMOS - Doorway Width Coverage for Different Camera Installation Parameters

	9.5 ft Height	15 ft Height	20 ft Height	25 ft Height
2.9 mm Lens	23 ft width			
3.6 mm Lens	19 ft width	29 ft width		
4.0 mm Lens	16 ft width	26 ft width		
5.0 mm Lens		20 ft width	27 ft width	
6.0 mm Lens		17 ft width	23 ft width	29 ft width

Table 3: 1/3" CCD/CMOS - Doorway Width Coverage for Different Camera Installation Parameters

	9.5 ft Height	15 ft Height	20 ft Height	25 ft Height
2.9 mm Lens	17 ft width			
3.6 mm Lens		21 ft width	29 ft width	
4.0 mm Lens		20 ft width	26 ft width	
5.0 mm Lens		16 ft width	20 ft width	26 ft width
6.0 mm Lens			17 ft width	21 ft width

Table 4: 1/4" CCD/CMOS - Doorway Width Coverage for Different Camera Installation Parameters

	9.5 ft Height	15 ft Height	20 ft Height	25 ft Height
2.9 mm Lens	17 ft width			
3.6 mm Lens		21 ft width	29 ft width	
4.0 mm Lens		20 ft width	26 ft width	
5.0 mm Lens		16 ft width	20 ft width	26 ft width
6.0 mm Lens			17 ft width	21 ft width

To further understand these tables, note that:

- Empty cells within the table indicate that these configurations are not supported by the people counting feature.
- Any camera lenses or CCD sizes not included in these tables are not supported by the people counting feature.

- Ceiling heights lower than 9.5 feet and higher than 25 feet are not supported by the people counting feature. If you are working with a ceiling height that falls within the range of 9.5 feet and 25 feet, but the exact height is not listed in the tables, follow these steps first to determine that your ceiling height is supported, and then to calculate the doorway width:

  a) Determine whether your ceiling height is supported for the camera lens you are using by referring to the table that corresponds to the CCD/CMOS being used, and ensuring that doorway widths display for the two heights between which your ceiling height falls. For example, if you are using a 1/2" CCD/CMOS and a 3.6 mm lens, and your ceiling is 12 feet high, you can verify that this ceiling height is supported because doorway widths are available in the **9.5 ft Height** column (**19 ft width**) and the **15 ft Height** column (**29 ft width**).

  b) If your ceiling height is supported, estimate the doorway width by performing linear interpolation between the two existing doorway widths using the following formula:
  $W=W1+[(W2-W1)*(H-H1)/(H2-H1)]$
  Where
  W is the width of the doorway supported for your ceiling height,
  W1 is the width of the doorway associated with *H1* in the table that corresponds to the CCD/CMOS you are using,
  W2 is the width of the doorway associated with *H2* in the table that corresponds to the CCD/CMOS you are using,
  H is your ceiling height,
  H1 is the supported ceiling height in the table that corresponds to the CCD/CMOS you are using, which is lower than *H*, and
  H2 is the supported ceiling height in the table that corresponds to the CCD/CMOS you are using, which is higher than *H*.
  For example, you would use the following calculation to determine the doorway width for a 12 foot high ceiling if you are using a 1/2" CCD/CMOS and a 3.6 mm lens:
  19 ft+[(29 ft-19 ft)*((12 ft-9.5 ft)/(15 ft-9.5 ft))]=23.5 ft

Configuration and Usage Guidelines

To ensure proper configuration and use of the people counting feature, please follow these guidelines:

- The isolated area of interest should be cleared of temporary objects and should not include any areas where people typically loiter.
- We recommend that you isolate an area of interest that focuses on the entry and exit of traffic that is vertical to the camera's field of view. Otherwise, counts may be inaccurate.
- Ensure the isolated area of interest meets the following requirements:
  - The area of interest must be high enough to accommodate a minimum of two people walking in single file through the entrance/exit area.
  - The area of interest must be wide enough to accommodate one person walking through the entrance/exit area without "touching" the edges of the masked area.

  Otherwise, calibration and/or counts may be inaccurate.
- Ensure that the traffic flow during the calibration period is typical; otherwise, the system may not count accurately. For example, if the traffic during calibration consists mainly of adults and very few children, the system may not count children once the calibration is complete.

How People Counting Affects Recording Frame Rates

Each recorder model has a maximum aggregate frame rate at which it can record video (for information, see Table 5 on page 18).

When you configure an input for people counting, the recorder no longer records video, but a portion of the recorder's maximum aggregate frame rate is still consumed. This frame rate consumption is equal to the amount that would be consumed if the camera was still recording video at the recorder's average camera frame rate. In other words,

$$\text{Cost to enable people counting on a camera} = \frac{\text{Recorder's maximum aggregate frame rate}}{\text{Recorder's average camera frame rate}}$$

For example, a 4416 NVR has a maximum aggregate frame rate of 240 fps for use with its 16 video ports, resulting in a cost of 15 fps for each people counting sensor (CIF, NTSC).

For certain recorder models, when you enable people counting on cameras, you may be required to disable other inputs. For information, see the procedure, "To enable people counting" in the *Administrator Console User Manual*.

Table 5 on page 18 details how the people counting feature affects the maximum allowable aggregate frame rates of recorders and the cost per people counting camera.

Table 5: How People Counting Affects Maximum Aggregate Frame Rates

Series	Model	Maximum Aggregate Frame Rate (CIF)	Max. # of People Counting Cameras Allowed	Cost per People Counting Camera (CIF)
3000 Series DVR*	3108 DVR	30 fps (NTSC), 25 fps (PAL)	4	8 fps (NTSC), 6 fps (PAL)
	3204 DVR	60 fps (NTSC), 50 fps (PAL)	4	15 fps (NTSC), 12 fps (PAL)
4000 Series DVR*	4116 S (first generation)	60 fps (NTSC), 50 fps (PAL)	16	4 fps (NTSC), 3 fps (PAL)
	4210 DVR (first generation)	60 fps (NTSC), 50 fps (PAL)	16	4 fps (NTSC), 3 fps (PAL)
	4116 S (second generation)	60 fps (NTSC), 50 fps (PAL)	8	4 fps (NTSC), 3 fps (PAL)
	4210 DVR (second generation)	60 fps (NTSC), 50 fps (PAL)	8	8 fps (NTSC), 6 fps (PAL)
	4310 DVR	120 fps (NTSC), 100 fps (PAL)	16	8 fps (NTSC), 6 fps (PAL)
	4410 DVR	240 fps (NTSC), 200 fps (PAL)	16	15 fps (NTSC), 12 fps (PAL)
4000 C Series NVR	4216 C NVR	60 fps (NTSC), 50 fps (PAL)	8	8 fps (NTSC), 6 fps (PAL)
	4316 C NVR	120 fps (NTSC), 100 fps (PAL)	16	8 fps (NTSC), 6 fps (PAL)
	4416 C NVR	240 fps (NTSC), 200 fps (PAL)	16	15 fps (NTSC), 12 fps (PAL)
	4516 C NVR	480 fps (NTSC), 400 fps (PAL)	This model does not support people counting.	

* People counting is only available on these models after the software running on the recorder has been upgraded to release 5.3 or later.

The cost per people counting camera is not the actual frame rate at which the people counting feature analyzes video frames.

You can differentiate between a first generation and a second generation 4116 S or 4210 DVR by the fan vent location on each device. First generation units can be identified by the vents located at the top and sides of the unit. Second generation units can be identified by the vents located at the front left and right of the unit, beside the handles.

Chapter 6

Queue Length Monitoring

March Networks cameras and encoders have built-in queue monitoring abilities that allow them to detect when a specified percentage of a waiting area is occupied by a queue of stationary people.

After this feature is enabled and configured, security staff and investigators can use the Live Monitoring Console to alert them to changes in the number of people in the waiting area, or they can use the Investigator to review alarms that have already occurred.

For a list of cameras and encoders that support this feature, contact your March Networks representative.

The following topics are covered in this chapter:

Queue Length Monitoring

Further to the queue length monitoring information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for setup and use.

Setup and Usage Guidelines

To ensure proper setup and use of the queue length monitoring feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Ensure the scene has adequate light levels. Low lighting conditions may cause problems in the details evaluation.
- Ensure that there are no objects in the scene that can partially obscure the image.
- Mount the camera above the scene and select a camera angle that can evaluate queue formations or waiting areas.
- Avoid scenes with frequent lighting changes or blinking lights, such as televisions, large windows, or blinking neon signs.

Possible Causes of Queue Length Monitoring Alerts

The following situations cause the device to generate queue length monitoring alerts:

- Changes in the scene, such as lighting fluctuations, or the opening and closing of doors.
- Static objects have partially obscured the image.
- People were continuously moving in the queue.
- Video acquisition problems occurred.
- Power supply problems occurred.

Chapter 7

Facial Detection

March Networks cameras and encoders have built-in facial detection abilities that allow them to distinguish human faces from other objects. This feature is useful when you are monitoring a secure area, such as a bank entrance, and want to capture images of the faces of people entering the building. When the camera detects a full frontal image of a face, it generates a face alarm which can then be used to trigger the bank door to unlock.

For a list of cameras and encoders that support this feature, contact your March Networks representative.

The following topics are covered in this chapter:

Facial Detection

Further to the facial detection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for camera installation and setup, as well as configuration and usage.

Setup and Usage Guidelines

To ensure proper setup and use of the facial detection feature, please follow these guidelines:

- Ensure the scene has adequate lighting. Daylight or the equivalent level of artificial light is recommended.
- Mount the camera at a height and angle that will capture a clear view of faces.
- Adjust the camera's view so that the face comprises one-fifth of the scene.
- The 'Min/Max size' and the 'Confidence' settings must be configured accurately on the Camera Web page. For more information about configuring the settings, see the *Administrator Console User Manual*.

Possible Causes of Facial Detection Alerts

The following situations cause the device to generate facial detection alerts:

- Oval objects were detected in the scene.
- Masks reproducing human faces were detected in the scene.
- The lighting was insufficient for detecting faces.
- A face that was partially hidden, for example by a scarf, hat, or helmet, was detected in the scene.
- Video acquisition problems occurred.
- Power supply problems occurred.

Chapter 8

Loitering Detection

March Networks IP cameras and Edge encoders have built-in loitering detection abilities that allow them to detect when an individual remains in an area for longer than the amount of time you specify.

For a list of IP cameras and encoders that support this feature, contact your March Networks representative.

When loitering detection is configured and enabled, a loitering alarm is triggered if a person remains in the specified area for longer than the configured time.

The following topics are covered in this chapter:

Loitering Detection

Further to the loitering detection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for camera installation and setup, as well as configuration and usage.

Setup and Usage Guidelines

To ensure proper setup and use of the loitering detection feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Ensure there is adequate lighting, since low lighting can prevent detection of details.
- Configure the camera to ignore zones with large amounts of persistent movement.
- Configure the camera to ignore zones with lighting changes, such as blinking neon signs and televisions.
- Ensure that the camera's perspective is properly configured.
- Ensure that objects or people moving in the selected zone are large enough to be detected.

Possible Causes of Loitering Detection Alerts

The following situations cause the device to generate loitering detection alerts:

- There were moving objects on the camera lens, such as insects.
- There were too many moving objects in the scene.
- Two or more moving objects were overlapping in the scene.

The following situations may prevent the generation of loitering detection alerts:

- Inclement weather such as rain, snow, or mist.
- Moving objects temporarily disappeared from the scene, for example behind a wall.
- There were too many moving objects detected in the scene.
- Two or more moving objects in the scene were overlapping.
- Video acquisition problems occurred.
- Power supply problems occurred.

Chapter 9

Perimeter Protection

March Networks cameras and encoders have built-in perimeter protection abilities that allow them to detect when an individual or object crosses a certain point in the camera's field of view. Optionally, you can specify that you only want to detect when an individual crosses the line and is moving in the direction you specify.

After this feature is enabled and configured, security staff and investigators can use the Live Monitoring Console to alert them of alarms in real-time, or they can use the Investigator to review alarms that have already occurred.

For a list of cameras and encoders that support this feature, contact your March Networks representative.

The following topics are covered in this chapter:

Perimeter Protection

Further to the perimeter protection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for camera installation and setup, as well as configuration and usage.

Setup and Usage Guidelines

To ensure proper setup and use of the perimeter protection feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Ensure there is adequate lighting, since low lighting can prevent detection of details.
- Configure the camera to ignore zones with large amounts of persistent movement.
- Configure the camera to ignore zones with light changes, such as blinking neon signs and televisions.
- Ensure that the camera's perspective is properly configured.
- Ensure that objects or people moving in the selected zone are large enough to be detected.

Possible Causes of Perimeter Protection Alerts

The following situations cause the device to generate perimeter protection alerts:

- There were moving objects on the camera lens, such as insects.
- There were too many moving objects in the scene.
- Two or more moving objects were overlapping in the scene.

The following situations may prevent the generation of perimeter protection alerts:

- Inclement weather such as rain, snow, or mist.
- Moving objects temporarily disappeared from the scene, for example behind a wall.
- There were too many moving objects detected in the scene.
- Two or more moving objects in the scene were overlapping.
- Video acquisition problems occurred.
- Power supply problems occurred.

Chapter 10

Occupancy Detection

March Networks cameras and encoders have built-in occupancy detection abilities that allow them to detect when people or vehicles move from one specified zone to another and generate a tracking alarm.

The occupancy detection feature follows the movement of people or vehicles and stores the information in a real-time database. This information can be used to develop an understanding of activities in the field of view, or to raise a tracking alarm. You can easily view the movement of people or objects through the field of view because they are outlined with colored boxes and their progress is traced by a corresponding colored line.

For a list of cameras and encoders that support this feature, contact your March Networks representative.

The following topics are covered in this chapter:

Occupancy Detection

Further to the occupancy detection information provided in the *Administrator Console User Manual* and online Help, please review the following guidelines for camera installation and setup, as well as configuration and usage.

Setup and Usage Guidelines

To ensure proper setup and use of the occupancy detection feature, please follow these guidelines:

- Stationary cameras are required. We recommend that you disable this feature on PTZ cameras.
- Ensure there is adequate lighting, since low lighting can prevent detection of details.
- Configure the camera to ignore zones with large amounts of persistent movement.
- Configure the camera to ignore zones with lighting changes, such as blinking neon signs and televisions.
- Ensure that the camera's perspective is properly configured.
- Ensure that objects or people moving in the selected zone are large enough to be detected.

Possible Causes of Occupancy Detection Alerts

The following situations cause the device to generate occupancy detection alerts:

- There were moving objects on the camera lens, such as insects.
- There were too many moving objects in the scene.
- Two or more moving objects were overlapping in the scene.

The following situations may prevent the generation of occupancy detection alerts:

- Inclement weather such as rain, snow, or mist.
- Moving objects temporarily disappeared from the scene, for example behind a wall.
- There were too many moving objects detected in the scene.
- Two or more moving objects in the scene were overlapping.
- Video acquisition problems occurred.
- Power supply problems occurred.

Glossary

Action The activity you want the device to perform when a particular activity occurs. For example, during scheduled hours you want the device to retain video from a camera for an extended period of time. In this example, the action refers to the **Retention** action.

Alarm Source A camera or alarm input for which you can set up alarm monitoring in Live Monitoring Console.

Area of interest The portion of the camera's field of view that you want to monitor.

ESM Enterprise Service Manager. A server application that lets you monitor and maintain devices on your network, at one or more sites. The ESM can be made up of one or more servers, which form a cluster.

Event The activation of a trigger. An event can be the activation of a physical peripheral, such as a door contact. Or, an event can refer to activity occurring during a scheduled time period.

Evidence Data captured by a device, including video, audio, and text captured from an external peripheral, such as an ATM or POS register.

Field of view The area that is visible through the camera lens.

Frame rate The measurement of the frequency (rate) at which a video camera produces unique, consecutive images (frames).

Live Monitoring Console A tool that allows security personnel to monitor video and alarms in real time, and respond to alarm events.

Trigger Something that prompts the device to perform an action. A trigger can be a physical peripheral, such as a door contact. A trigger can also be a scheduled time period. For example, during scheduled hours you want the device to retain video from a camera for an extended period of time. In this example, the trigger is the schedule time period.

Video analytic Technology that analyzes video for specific actions or events.

Index