Fike Video Analytics®
FVA-IP Camera

Installation and Operation Manual

P/N: 06-523
Rev: 8, 04/20

Fike®
Video Analytics
Corporation

DEVELOPED BY	**Fike Video Analytics Corporation** 704 SW 10th Street Blue Springs, Missouri 64013-0610 U.S.A. Phone: 844-345-3843
COPYRIGHT NOTICE	
TRADEMARKS	

Table of Contents

1.0 Introduction to Fike Video Analytics....2
1.1 FVA-IP Camera....2
1.2 Video Management Software User Interface....3
1.3 Scalable System Architecture....4
2.0 Fike Video Analytics System Design....5
2.1 System Design....5
2.2 Field of View (FOV)....6
2.3 Detection Range....7
2.4 Environmental Considerations....8
2.5 Selecting Cable....8
2.6 Powering Up the System....9
2.7 Network Configuration....9
2.7.1 Network Requirements....9
2.7.2 Typical Configurations....10
3.0 Installation....11
3.1 IP Camera Setup....11
3.2 Power & Computer connections....14
3.3 IP Camera Communications....16
3.4 Operator Features....17
3.5 Administration Features....19
3.6 Finishing Camera Setup....29
4.0 Video Management System....31
5.0 Fike Video Analytics Video Management Software....31
6.0 Commissioning....31
7 Inspection, Testing, and Maintenance Recommendations....32
7.1 NFPA 72, Chapter 14 recommendations....32
7.2 Inspections....32
7.3 Testing....32
7.3.1 Difference in Functional and Operational conformance....33
7.3.2 Factors affecting Functional Conformance....33
7.3.3 Factors affecting Operational Conformance....33
7.4 Testing for Operational Conformance....34
7.4.1 Fault Condition....34
7.4.2 Communication failure / Analytics failure....34
7.4.3 Simulated response....34
7.5 Maintenance....35
7.6 Camera Replacement....36
Appendix A – FVA-IP Camera Specifications....39
Appendix B - Dry Contact Diagram....43
Appendix C – Fike Video Analytics System FM approved Computer Requirements....45
Appendix D - Commissioning Paper Work....47
Appendix E - Approved Fire Test Results....53

Table of Figures

Figure 1 - Snapshot of the Video Management Software User Interface. 3
Figure 2 – Typical installation of a Fike Video Analytics system with 8 FVA-IP cameras, an FSM-IP video management system, and a LAN network connected to monitoring workstation and remote monitoring of the site. 4
Figure 3 - The camera is positioned high in the space, and the FOV covers both the floor and ceiling, maximizing the area covered. The camera was mounted 15 ft. (4.6 m) high with a 70 ft. (21 m) unobstructed view down the length of the warehouse. 6
Figure 4 - Typical Fike Video Analytics Network setup for small installation: FVA-IP Cameras, Video Management system; Network hub /LAN; Guard station; Internet. 10
Figure 5 – Back plane of the FVA-IP camera showing the layout of the LED's, and dry contact, Ethernet, BNC, power in, power out, and audio connections. Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24 volt power supply. 12
Figure 6 – Front Plane of the FVA-IP camera showing location of the C/CS Lens mount and Front panel LED. Also the dimensions of the lens are shown. 12
Figure 7 – Local Area Connection Properties 14
Figure 8 – IP Properties 15
Figure 9 – POE switch 15
Figure 10 – Required user name (admin) and password (axonx) to establish connection to the FVA-IP camera. 16
Figure 11 – Administration Home page 16
Figure 12 – Camera algorithm status and override features 17
Figure 13 – Live video though either Java Applet or Multipart Stream (FireFox only). 17
Figure 14 – Live video from the camera at the default 2 fps. 18
Figure 15 – Relay Control provides the operator the functionality to confirm, delay, or reset an event. 18
Figure 16 – Snap shot taken from the camera. 19
Figure 17 – Configure option under the administrator section has a number of sub menu features. 19
Figure 18 – Access control with default password (axonx). 20
Figure 19 – Date & Time set. 20
Figure 20 – General settings used to configure the Network settings and Camera settings. 21
Figure 21 – Relay settings are configurable. 22
Figure 22 – Sensitivity settings 23
Figure 23 – Camera report provides a list of the configured variables. 24
Figure 24 – Camera restart 24
Figure 25 – Camera restore 25
Figure 26 – Load Factory Defaults 25
Figure 27 – Firmware upgrade window 26
Figure 28 - Upgrade Firmware page 26
Figure 29 - Camera Report page-showing program version 27
Figure 30 – Creating a schedule. 27
Figure 31 – Schedule inputs 28
Figure 32 – Zone window pane 28
Figure 33 – Create a zone by providing a zone name, type, action, and zone size defined by points 29
Figure 34 – FVA-IP Camera Back View 30
Figure 35 - Ferrite Bead Installation 30
Figure 36 – Camera web interface 36
Figure 37 - Restart Camera 37
Figure 38 – Example of a page from an audit report for a specific camera 38

Table of Tables

Table 1 – Detection times in seconds of IP camera models to various sources. 7
Table 2 - Color and State of the three LED's located on the IP camera. 13
Table 3 - Fire Size to Distance 34

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions. Keep these instructions
2. Head all warnings. Follow all instructions
3. Do not use this camera near water. Clean only with a dry cloth.
4. Install in accordance with the manufacturer's instructions
5. Do not install near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
6. Only use attachments/accessories specified by the manufacturer.
7. Refer all servicing to qualified service personnel. Servicing is required when the camera has been damaged in any way.
8. WARNING: To reduce the risk of fire or electric shock, do not expose this camera to rain or moisture.
9. Installation should be done only by qualified service personnel and conform to local codes.
10. Ensure that the camera is securely mounted. Use installation methods and materials capable of supporting four times the maximum specified load.
11. Only power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.
12. Please thoroughly familiarize yourself with the information in this manual prior to installation and operation.
13. This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operations.
14. This Class A digital apparatus complies with Canadian ICES-003. *Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.*

Approvals:

1.0 Introduction to Fike Video Analytics

Fike Video Analytics is a software-based technology that uses analytics to continuously monitor video—frame-by-frame, pixel-by-pixel -- to detect anomalies characteristic of smoke, fire, and motion. With the Fike Video Analytics video management software user interface, Fike Video Analytics' early fire and smoke detection capabilities are unmatched by any traditional smoke detection technology.

Fike Video Analytics, located within a Texas Instruments chip onboard the FVA-IP camera, can detect a flaming fire in a 7 by 7 pixel area, as well as both ambient and plume-like smoke patterns. The Fike Video Analytics system is also capable of detecting reflected firelight off walls or objects so that a fire can be detected even if the flames are not in the camera's line of sight.

NOTE: The reflected fire algorithm is not an FM approved detection method.

Unlike spot-type smoke detectors or temperature sensors, The FVA-IP camera is a volume sensor, which observes and identifies the fire condition within the entire observed space of the CCTV camera. This fundamental difference results in faster fire and smoke detection and, most importantly, provides a visual picture of the situation to responding personnel. In the event of a fire or the production of smoke, the FVA-IP camera "sees" the event and issues a warning signal.

Each Fike Video Analytics system includes:

- At least one FVA-IP Camera.
- The video management software user interface.
- A Video Management System.

1.1 FVA-IP Camera

The FVA-IP camera is a color camera with a micron 1/3-inch CMOS MT9M11 Imager, Texas Instruments TMS320DM642 chip, Digital Media Processor, 128 MB RAM, and battery backed-up real-time clock. All cameras accept a fixed Iris and fixed Field Of View (FOV) CS mount lens supplied by the manufacturer for 2.8 mm and 8 mm FOV. Each lens allows for focus adjustments. The FVA-IP Camera processes video in real-time, transmitting the video using unicast protocol through coax or a network to the management system and the Fike Video Analytics video management software. When an early warning condition does occur, the Fike Video Analytics creates an event file and sends it to the video management software operating on a remote PC workstation in the system. The on-duty operator or remote monitoring center receives an early warning notification along with live video from the location.

1.2 Video Management Software User Interface

With the Fike Video Analytics video management software user interface, you can use an approved workstation for video surveillance, fire safety monitoring, and configure any number of cameras. The software provides the tools to monitor your facilities, build an organization tree and import plant site drawings, build schematics, and photos. Figure 1 is an image of the video management software user interface.

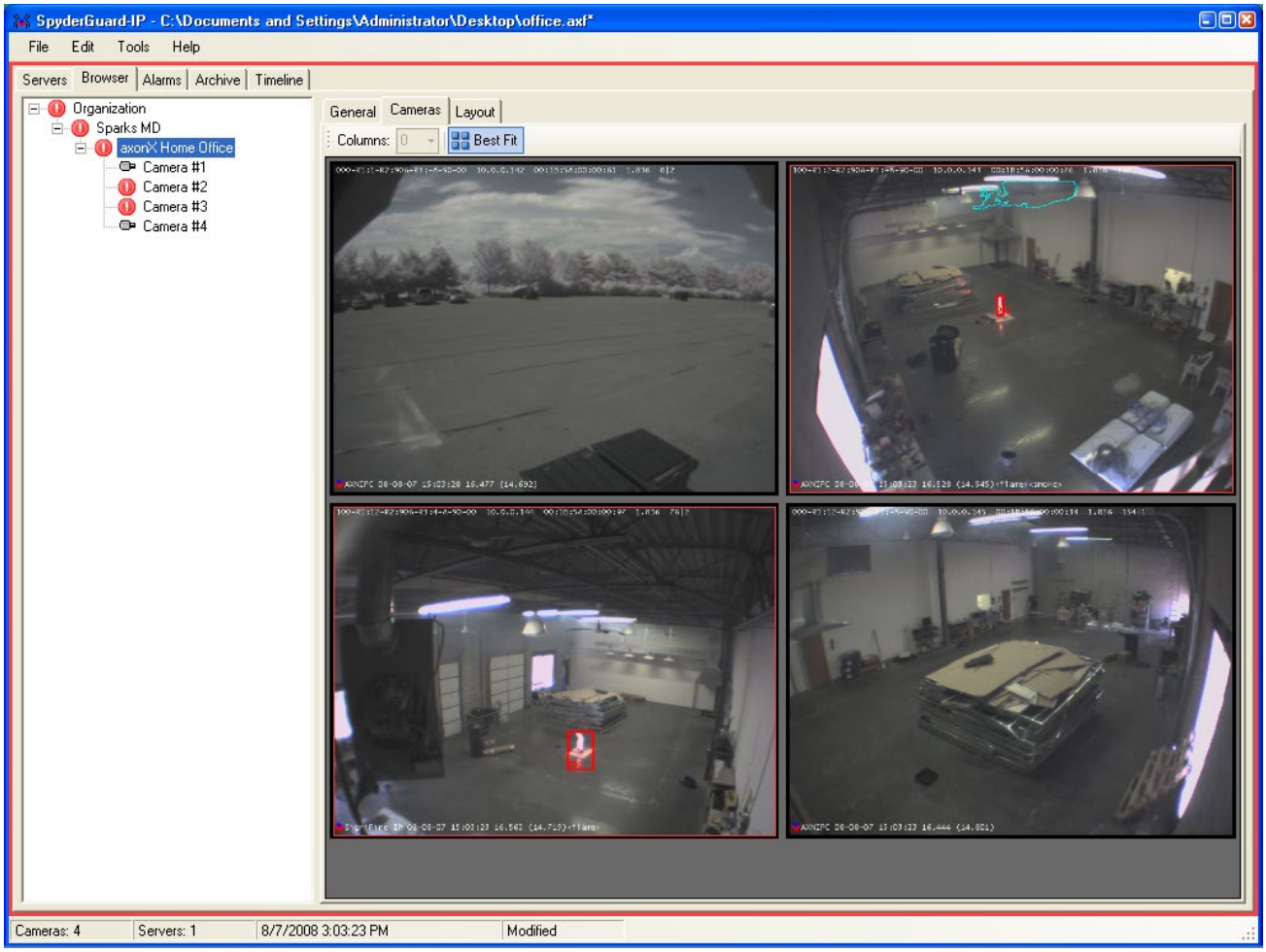


Figure 1 - Snapshot of the Video Management Software User Interface.

1.3 Scalable System Architecture

A Fike Video Analytics system is comprised of at least one FVA-IP camera, a video management system, and a monitoring solution. The system components must be connected to a common local network that is dedicated to fire protection use only. The components must be on the same subnet, and must not be separated by routers or gateways. The connection of the system components to a non-dedicated LAN is not recommended or supported by Fike Video Analytics. You can connect any number of FVA-IP cameras and event management servers to the network to expand the system to meet end-user needs (limit of 32 cameras per network recorder). FVA-IP cameras can be powered by an FM approved fire alarm control panel (FACP), an approved power supply listed for fire alarm use with battery backup, or as a supplemental means a Power-Over-Ethernet (POE) switch with battery backup. With the Fike Video Analytics video management software, any approved PC workstation can be used as a monitoring system so long as it is connected to the same dedicated LAN. Figure 2 is an example of scalable enterprise architecture.

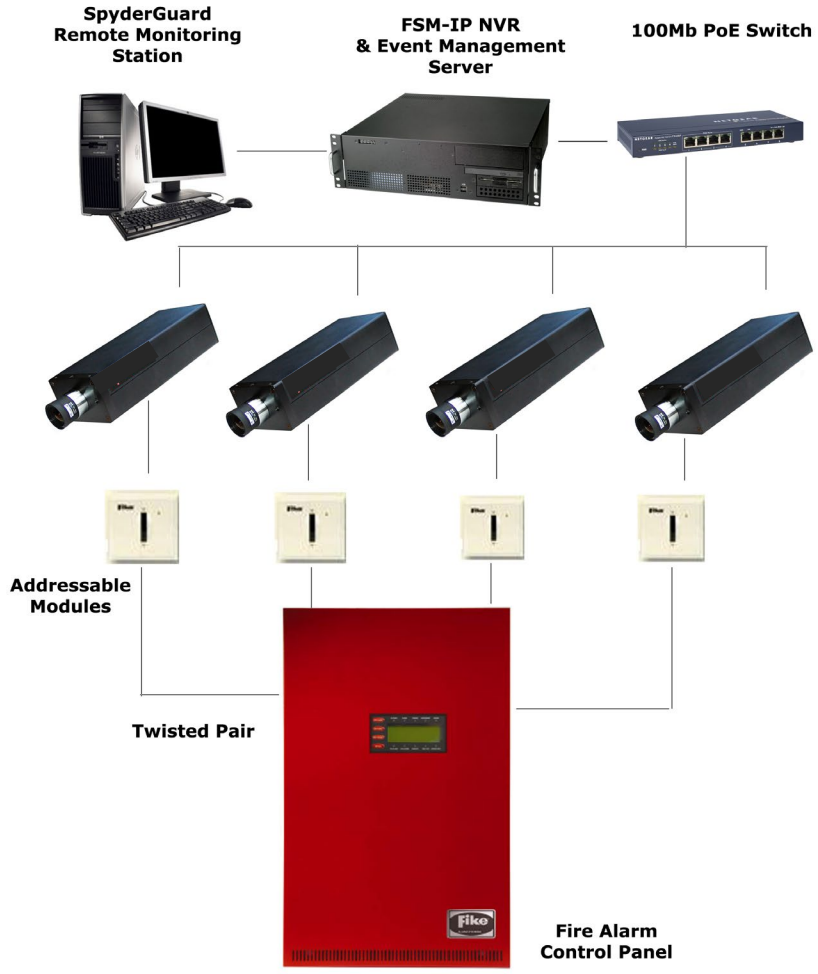


Figure 2 – Typical installation of a Fike Video Analytics system with 8 FVA-IP cameras, an FSM-IP video management system, and a LAN network connected to monitoring workstation and remote monitoring of the site.

Fike Video Analytics comes with a video management system called FSM-IP Network Video Recorder (NVR). The NVR provides a storage point for video alarms from the FVA-IP Cameras and acts as an information conduit between the video management software monitoring station and the cameras themselves. The number of FVA-IP cameras that can be supported in any Fike Video Analytics installation is dependent on the speed and robustness of the network to which the cameras are attached. It is this flexibility of the number of cameras, NVR platforms, and video management software monitoring stations that makes Fike Video Analytics systems scalable to any size application.

2.0 Fike Video Analytics System Design

The system design should include the proper coverage of the hazard area as well as monitoring of the events recorded by the FVA-IP cameras. The monitoring can be done by an on-site PC workstation or a remote monitoring facility. The system architecture is very flexible to suit the end-users needs, and care should be taken when designing the system layout to meet the needs of the end-user. Some examples of the varying architectures include:

- Wiring the cameras directly to the dry contacts of an FM approved FACP
- Connecting the cameras to on-site monitoring using the coax or the LAN connection
- Configuring the cameras to be remotely monitored by a third party or corporate site
- Using a video management system to record events for post-event analysis

Any combination of architecture can be combined to produce the desired results.

2.1 System Design

NOTE: All the requirements of *NFPA 72, including but not limited to, back-up power requirements, maintenance requirements, and performance-based installation criteria* should be followed.

NOTE: Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.

The FVA-IP camera should be connected to either Power-Over-Ethernet (POE) or a 12/24 VDC 1A, Class 2 power supply certified for use with fire alarm applications only. Both can be used together for redundancy. Electrical ratings can be found on the FVA-IP cameras. If you are unsure of camera placement, you may want to perform a Fire Hazard Analysis (FHA) and or a performance-based design analysis to determine the proper placement and number of cameras to adequately protect the area. It is important to consider the desired performance and prevention of nuisance alarms. Take into account predicted smoke flow, ceiling obstructions, the configuration of contents, lighting, and desired fire size at detection.

The location and spacing of cameras should be the result of an engineering evaluation that includes:

- Size and type of fire to be detected
- Fuel involved
- Detector sensitivity
- Camera Field of View (FOV)
- Distance between fire and camera
- Purpose of the detection system
- Response time required
- Sources of light
- Obstructions

The FVA-IP camera relies on “seeing” smoke and flames. The presence of intervening structural members and/or intermittent opaque objects or materials in front of the cameras can compromise its ability to respond to the fire. Obstructions in the cameras FOV are acceptable, as long as the obstructions do not compromise the ability of the system to detect the desired fire size and type in the allotted response time. Mount cameras to ensure objects that will appear large to it will not pass in front of or through its FOV; for example, a person standing closer than 5 ft. (1.5 m) past the camera or a vehicle parking in front of the camera.

Cameras should be mounted high and away from interferences so they can overlook the area of protection. The camera should be mounted so that large sources of light (glass walls, large bay doors, or directional spotlights) will not compromise the image quality by saturating the image sensor with light. Ideally, the FOV will include both the ceiling and floor of the facility, as shown in Figure 3 below.

Figure 3 - The camera is positioned high in the space, and the FOV covers both the floor and ceiling, maximizing the area covered. The camera was mounted 15 ft. (4.6 m) high with a 70 ft. (21 m) unobstructed view down the length of the warehouse.

2.2 Field of View (FOV)

The most significant factor affecting system performance is the camera positioning and the resulting FOV. It is important to position cameras to maximize the FOV as well as the area covered by the cameras. A performance-based design should be used to determine the number of cameras needed to properly cover the space from the determined fire threat. Table 1 shows the response times to various fire sources. Cameras should be placed high in the space so as to overlook the hazard area and avoid objects within 7 ft. (2 m) of the camera.

Table 1 – Detection times in seconds of IP camera models to various sources.

Fuel Source	Distance to detector	2.8 mm FOV	6 mm FOV	8 mm FOV	EX 8 mm FOV
1 ft pan of Heptane	100 ft	18	9	9	9
1 ft pan of JP-8	100 ft	18	10	10	10
1 ft pan of Ethyl Alcohol	100 ft	21	10	11	11
1 ft pan of Isopropyl Alcohol	100 ft	16	9	9	10
1 ft pan of Unleaded Gasoline	100 ft	8	8	8	9
4 min Smoke Emitter	100 ft	301	94	52	63
4 min Smoke emitter	75 ft	43	24	22	48
6 in pan of Heptane	100 ft	100	10	9	10
Cardboard boxes and paper 4 ea. 10 x 10 x 4-in. boxes	100 ft	278	83	101	97
6 in diameter pan of Heptane/toluene 75/25	28 ft	19	19	20	18
Shredded newspaper	28 ft	127	150	102	151
Smoldering wood	28 ft	3062	3279	3027	2927
Wood Crib 6 x 6 x 2.5-in.	28 ft	142	192	145	194

NOTE: Known nuisance sources include: Welding, grinding, modulated light sources, and directional light sources.

2.3 Detection Range

After proper camera positioning, the detection range is the second most important consideration. The most sensitive detection algorithm to distance is flame detection because it relies on direct flame image pattern analysis. To detect a flame, the pattern must be at least 7 by 7 pixels in size. You can perform calculations to determine a relationship between the distance and lens angle to the fire size at detection. The range of potential smoke sources and their corresponding optical densities makes it difficult to theoretically estimate the exact distance at which a threshold of smoke detection will be reached. The Offsite detection method depends on a variety of factors, such as the presence and properties of reflecting surfaces, the type of combustible, and the lighting conditions. The offsite algorithm is not FM approved because of these many variables.

Cameras should be placed so that coverage will detect the desired fire size and type consistent with the hazard area. The number of cameras needed should be determined on the basis of the camera position. Unlike many radiant energy-sensing fire detectors, flames that are obstructed or outside the FOV may be detected, depending on the number of obstructions and the reflective properties of the surrounding surfaces. Video flame and smoke detector performance is relatively uniform across the plane intersecting a source's optical axis. Unlike fire detectors that sense radiant energy, corrections for fire size vs. distance need not be given for fires that may occur away from the optical axis of the detector. You can also assume that smoke starting outside the FOV of a camera may drift into the FOV. While these features provide extra detection, the primary objective is to ensure that all regions requiring detection coverage are within the FOV of at least one camera. Cross zoning cameras also provides an opportunity to reduce nuisance alarms caused by directional light sources.

2.4 Environmental Considerations

To maximize the fire detection potential of the Fike Video Analytics system, the camera lenses should be properly set up to ensure sharp images. Using a portable TV with the BNC connection attached to the back of the IP camera will allow localized adjustment to optimize the image focus. Lenses should be clean and free of scratches. Camera positioning should consider light saturation and consistency, mounting integrity, humidity, airborne particulates, and other potentially damaging ambient conditions. Bright light sources should be located behind the cameras.

The area to be protected should be uniformly illuminated; fluctuations caused by natural light should be limited. Cameras should be securely mounted to prevent vibration, swinging, and other camera motion. Excess humidity may cause fogging of the lenses that may trigger the system.

Make provision to sustain camera lens clarity in applications where airborne particulates and aerosols may coat the camera lens between maintenance intervals and affect sensitivity. Cameras should be protected either by design or installation to ensure that performance is not compromised. When used in conditions that will expose the camera to extreme conditions, the cameras should be shielded or otherwise arranged to maintain performance when exposed to those extreme conditions. The cameras should not be installed in a location where ambient conditions are known to exceed the extremes for which they have been listed (see specifications Appendix A). Nuisance sources include but may not be limited to welding, modulated light sources, and localized fluctuations in lighting. The area to be protected should be uniformly lit at the UL minimum of 1 foot-candle (10 lux) measured at the floor level for the hazard area, or the FM approved 4.8 Fc (~48 lux) at 30 inches (76 cm) above the floor surface. General lighting shall meet the minimum emergency lighting requirements of NFPA 101 (1 Fc (10 Lux)) and shall not produce a low light camera fault.

2.5 Selecting Cable

There are several classifications of cable used for twisted-pair networks. We recommend Category 5 (or CAT 5) cable for all new installations. There are several fire code classifications for the outer insulation of CAT 5 cable. CMR cable, or "riser cable," is the most common. However, CMP or plenum cable is also available and may be required by local, state, or national codes if it will be running through suspended ceilings, ducts, or other areas, that are used to circulate air or act as an air passage from one room to another. Stranded wire patch cables are often specified for cable segments running from a wall jack to a PC and for patch panels. They are more flexible than solid core wire.

CAT 5 cable has four twisted pairs of wire for a total of eight individually insulated wires. Each pair is color-coded with one wire having a solid color (blue, orange, green, or brown) twisted around a second wire with a white background and a stripe of the same color. The solid colors may have a white stripe in some cables. Cable colors are commonly described using the background color followed by the color of the stripe; e.g., white-orange is a cable with a white background and an orange stripe.

The straight-through and cross-over patch cables are terminated with CAT 5, RJ-45 modular plugs. RJ-45 plugs are similar to those you'll see at the end of your telephone cable, except they have eight versus four or six contacts on the end of the plug, and they are about twice as big. Make sure they are rated for CAT 5 wiring. (RJ means "Registered Jack"). Also, there are RJ-45 plugs designed for both solid core wire and stranded wire. Others are designed specifically for one kind of wire or the other. Be sure you buy plugs appropriate for the wire you are going to use.

2.6 Powering Up the System

The system and all its electrical components should be supplied with power from an uninterrupted power source. This will ensure that the cameras, guard station, and network will remain functioning over the course of power loss. The amp-hour for the system to maintain power will vary depending on the number of cameras used. Calculations should be conducted to ensure adequate backup power is available to maintain the system for 24 hours.

NOTE: Backup power supply for cameras should adhere to the requirements of NFPA 72 and be NRTL certified for fire.

NOTE: Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.

The voltage required to operate the camera is clearly marked on the rear panel of the camera. The green power LED on the rear and front of the IP camera indicates that power is connected. Power consumption is approximately 5.0 Watts. The IP Camera is fitted to automatically switch between low voltage power supply and POE if one is to fail.

NOTE: All wiring should be done according to NEC 70 practices.

2.7 Network Configuration

NOTE: If your organization uses static IP addresses (i.e., does not use DHCP services), you must provide specific IP addresses to complete the following steps. Contact your IT representative or system administrator.

Consider the following when configuring the network connections:

- Type of network currently in place within the organization
- IP and DNS configuration options (automatic or manual)
- Number of cameras residing on the same network
- Future expansion plans (how many cameras may be added)
- Who will access the system and from where (local networks, Internet)

2.7.1 Network Requirements

Typical bandwidth to transfer video from the IP camera to the Video Management System is minimal. Each frame is approximately 40 to 60 kb in size. Therefore, one camera at 2 frames per second (fps) results in 120 kbps. An operator displaying 48 cameras at once, (48 x 120 x 8) results in 46,080 kbps (46.0 Mbps), which is less than 50% capacity of 100 MB network or less than 5% capacity of a 1 GB network. However, it is highly unlikely that an operator would view 48 cameras at once on one Fike Video Analytics video management workstation, nor would they need to do so.

2.7.2 Typical Configurations

NOTE: By default, the Ethernet connection is factory-preset for a fixed IP configuration. If your organization uses DHCP, do not connect the camera to the network until the Network setup has been completed. Refer to section 3.5 for details.

The typical Fike Video Analytics setup will be similar to the one shown in Figure 4 and includes the following components: FVA-IP Camera(s) connected by CAT-5 cable to a network hub or LAN, connecting the monitoring workstation running the Fike Video Analytics video management software and the FSM-IP NVR. In addition, dry contact connections are provided one each FVA-IP camera so the system can be tied into an FM approved FACP. A BNC connection is provided, so a coax connection can be used with legacy systems. Appendix B provides a diagram for identifying and attaching the dry contact outputs.

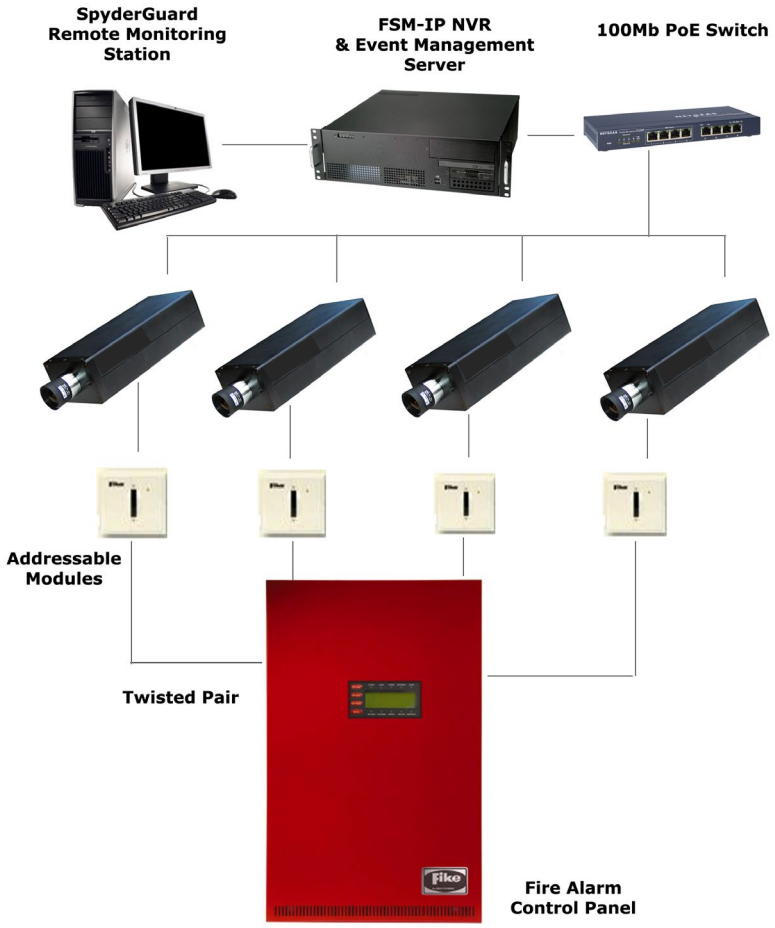


Figure 4 - Typical Fike Video Analytics Network setup for small installation: FVA-IP Cameras, Video Management system; Network hub /LAN; Guard station; Internet.

NOTE: This section provides information for configuring a basic system. For more information, contact your IT representative or system administrator.

3.0 Installation

Typical Fike Video Analytics installation is completed in four basic steps:

- Configure, and install FVA-IP Cameras
- Install the video management system
- Install and configure Fike Video Analytics video management software on the workstation
- Configure and commission the Fike Video Analytics system.

Complete instructions to perform each step are presented in the following sections and within the video management software User manual.

NOTE: All wiring should be done according to NEC 70 practices.

NOTE: Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.

NOTE: It is important to create a permanent record of all camera settings upon installation (see section 3.5) and when any changes are made. These records will be useful for regular system maintenance and any future incident investigation.

NOTE: The Fike Video Analytics detection system shall comply with all applicable requirements of NFPA 72, including but not limited to, back-up power requirements, maintenance requirements, and performance-based installation criteria.

NOTE: The system maintains a supplemental status to enhance fire detection and protection of assets and property.

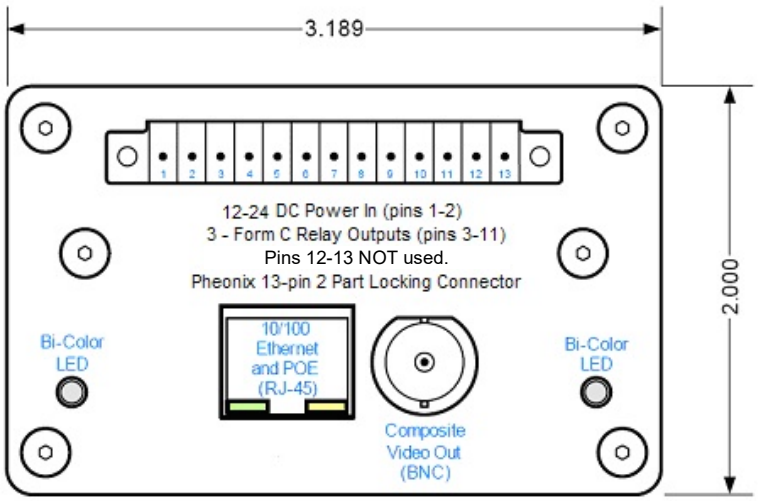
NOTE: Only personnel trained and certified to install the FVA-IP Camera should install and commission a Fike Video Analytics system. Installation should be in accordance with the instructions within this manual and NFPA guidelines.

3.1 IP Camera Setup

Once the camera locations have been selected, the entire procedure will consist of the following steps:

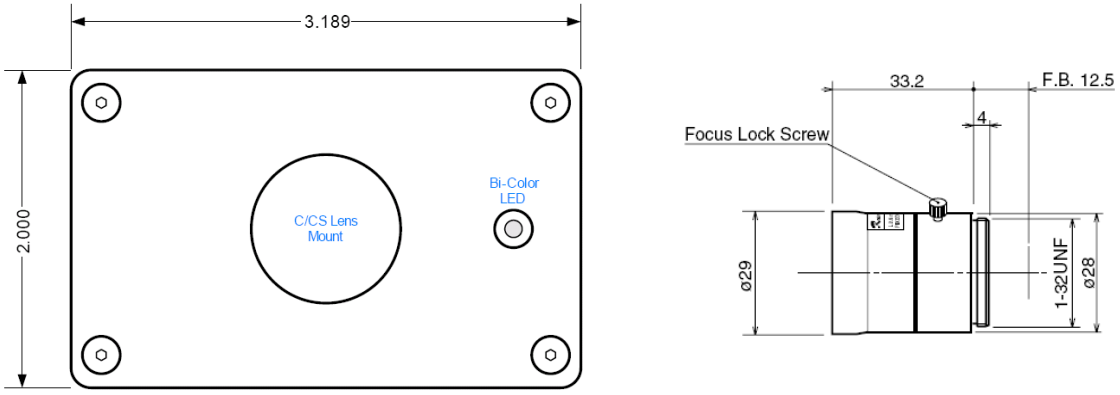
- Unpack and inspect IP Cameras
- Power up and connect to the IP camera
- Configure camera
- Install the camera and set focus.
- Commission cameras

Unpack the camera. Inspect both cameras and attached lens for defects or damage. Familiarize yourself with the camera layout and all of its connections, Figures 5 and 6. The FVA-IP camera offers standard power and coax video connectors as well as an RJ45-10 connector that accepts POE, three configurable dry contact closers, and a power out connection for approved accessories.



Back View

Figure 5 – Back plane of the FVA-IP camera showing the layout of the LED's, and dry contact, Ethernet, BNC, power in, power out, and audio connections. Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.



Front View

Figure 6 – Front Plane of the FVA-IP camera showing the location of the C/CS Lens mount and Front panel LED. Also, the dimensions of the lens are shown.

There are three LEDs located on the FVA-IP camera; front, right rear, and left rear. The color of the pulse and the resulting state are listed in Table 2. The Front LED provides the alarm condition of the camera. The left rear LED indicates the condition of the network connection for troubleshooting purposes. The right rear LED indicates the state of the image collection and internal processing of the images by the analytics.

Table 2 - Color and State of the three LED's located on the IP camera.

Front LED	
Color	State
Green Pulse (1-sec interval)	Normal
Green Pulse rapid	Motion
Yellow Pulse	Trouble
Red Pulse	Alarm
Left Rear LED (ref from the rear)	
Green Pulse	Network normal
Red Pulse	Network Failure
Yellow Pulse	HTTP server Failure
Right Rear LED (ref from the rear)	
Green Pulse	Every 15th frame (Image task)
Yellow Pulse	Camera Control Task Failure
Red Pulse	Image Task Failure

To run the FVA-IP camera interface and configure the camera, a computer with either Firefox or Internet Explorer is required. If Internet Explorer is used, Java must be properly installed and up to date in order to see the video feed. Firefox can be easily downloaded and will run both Java and multipart stream video feed options.

In addition to the web browser, a network connection with a fixed IP configuration must be established. **The FVA-IP camera comes pre-configured with a Fixed IP address of 192.168.0.100.** This requires the computer used to configure the camera be set to a fixed IP to initially communicate with the camera, for example 192.168.0.1. Once the initial communication is acquired, the camera can be configured to function on a DHCP or a Fixed IP Network, and its IP address can be changed to specifically identify the camera.

3.2 Power & Computer connections

To set your computer to a fixed IP:

1. Select ***Start>Control Panel>Network and Internet Connections***.
2. Click the ***Network Connections*** icon.
3. Right-click the ***Local Area Connection*** icon and select ***Properties***. The Local Area Connection Properties dialog box opens.

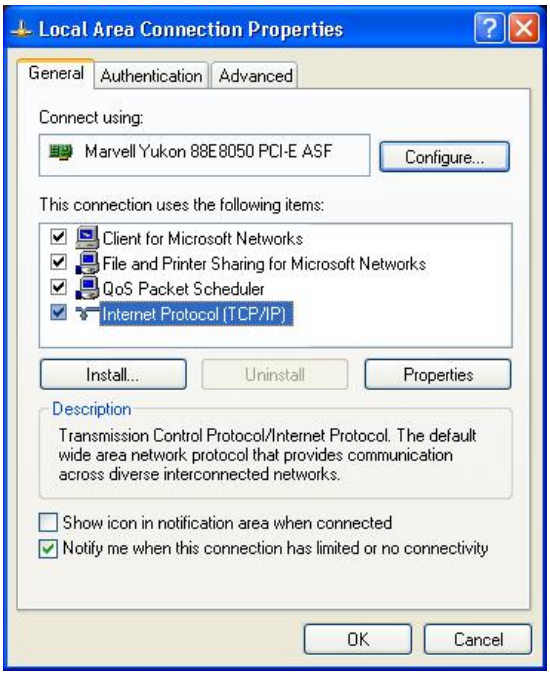


Figure 7 – Local Area Connection Properties

4. Select Internet Protocol (TCP/IP) and click the Properties button. The Internet Protocol (TCP/IP) Properties dialog box opens at the General tab.

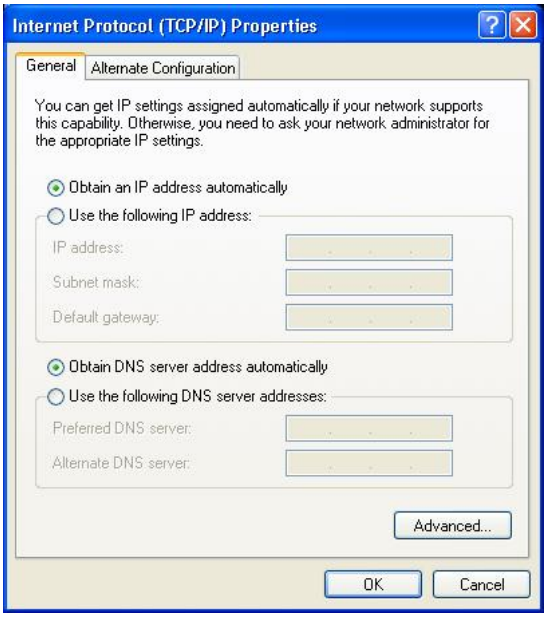


Figure 8 – IP Properties

5. Select ***Use the following IP Address*** and enter the IP address in the correct range (192.168.0.1 to 192.168.0.255, subnet mask 255.255.255.0.
6. Connect the computer to a HUB and the IP camera to the same HUB using CAT-5 cables.

You are now ready to power up and connect to the IP Camera. Note the cameras by default are set to 192.168.0.100, so you cannot use this address for the NVR, or you will create an IP address conflict.

NOTE: Power with 12-24 VDC (UL), 12 VDC (FM) from UL listed Class 2 power supply listed for fire alarm use should be used. POE may be used as supplemental to the listed 12 or 24-volt power supply.

Connect the Ethernet cable to a hub and attach the laptop or workstation used to configure the camera to the hub.

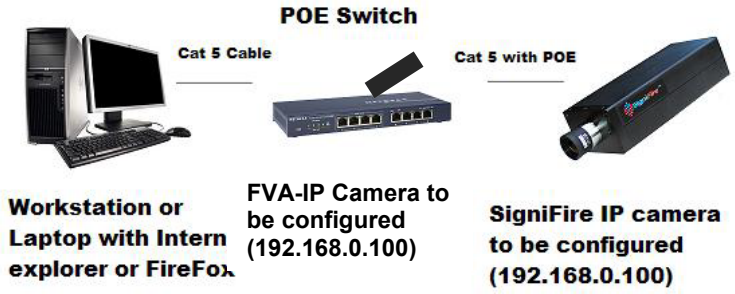


Figure 9 – POE switch

3.3 IP Camera Communications

Open the preferred internet browser (Firefox or Internet Explorer) and type http://192.168.0.100/admin in the address bar. If the connection is successful, you will be prompted for a user name and password, Figure 10. The factory default user name and password are **admin** and **axonx**, respectively.

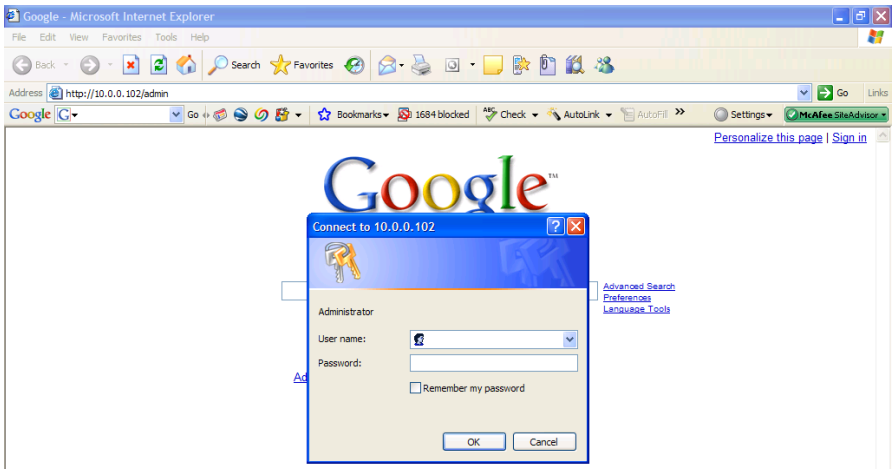


Figure 10 – Required user name (admin) and password (axonx) to establish a connection to the FVA-IP camera.

Once you have entered the user name and password, the Administration Home page will appear, Figure 8. You are now connected to the FVA-IP camera, and the configuration of the settings can commence. The page is broken into two sections; one for an operator the other for the administrator. Although the operator features are present, it is suggested that all monitoring by the operator be done using the Fike Video Analytics video management software or the host fire alarm panel. Both sections, administrator and operator, are secured from the other by a user name and password. The factory default user name and password for each section is:

Operator section: User Name: operator
Password: axonx

Administrator section User Name: admin
Password: axonx

These passwords can be changed by the administrator in the administration section under **configure>access control**.

The operator has access to the camera status, live video, relay control, and snapshot features. The administrator can configure the camera, including schedules and zones, print a report of the configuration, as well as restart and update the FVA-IP camera. Each of these features will be discussed in the following sections.

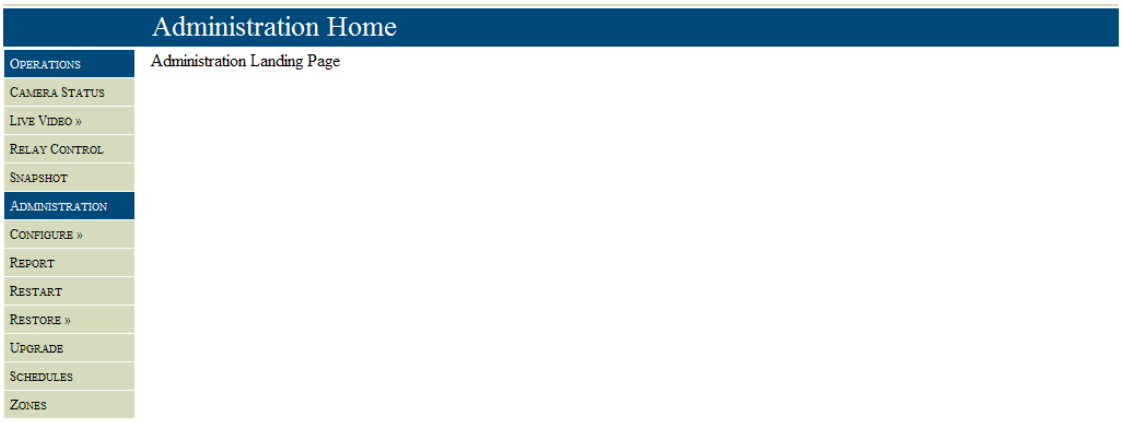


Figure 11 – Administration Home page

3.4 Operator Features

The first feature on the operator list is the **Camera Status**, Figure 12. This table provides the operator with the state of each alarm and trouble condition. It also allows the operator to switch the state and turn on any of the alarm or trouble states for testing purposes. Turning any of the states "on" results in an event file being created and recorded and any dry contacts that are set to close on the event type would close. The override will continue until the operator returns the function to off.

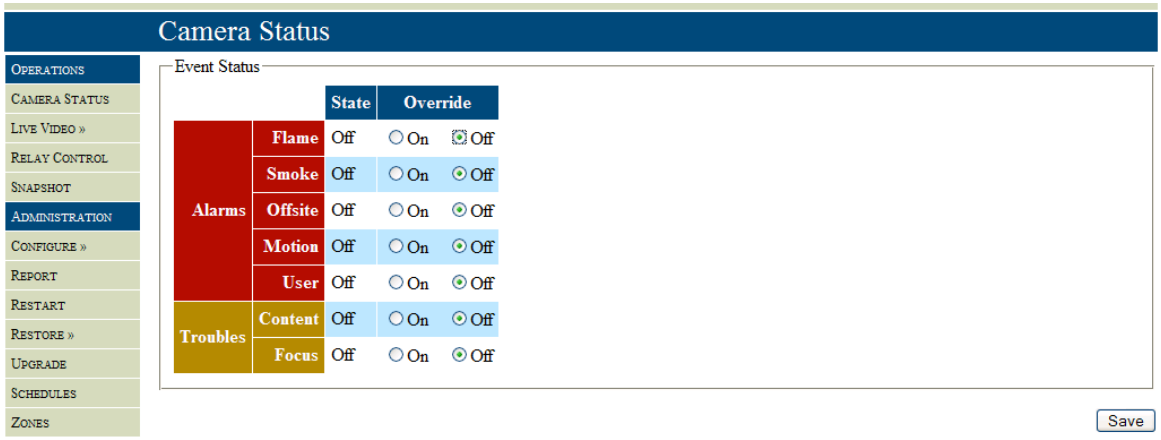


Figure 12 – Camera algorithm status and override features

The **Live Video** feature allows the operator to view the video feed produced by the FVA-IP camera. The video can be seen using the JAVA Applet or Multipart Stream (Firefox only), Figure 13.

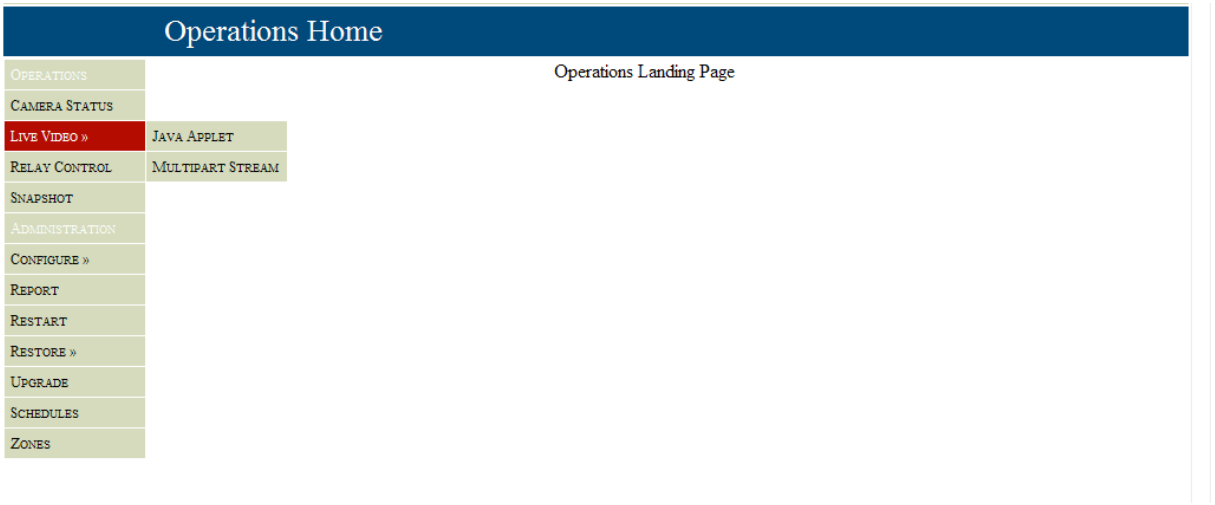


Figure 13 – Live video though either Java Applet or Multipart Stream (Firefox only).

Figure 14 displays the video feed from the camera using the JAVA Applet. By default, the frame rate is set to two frames per second (fps). The frame rate is configurable to between 1 and 15 fps to limit bandwidth usage or provide a smoother image feed, respectively. Once the desire frame rate is chosen, click the **update** button, and the video will run at the desired frame rate.

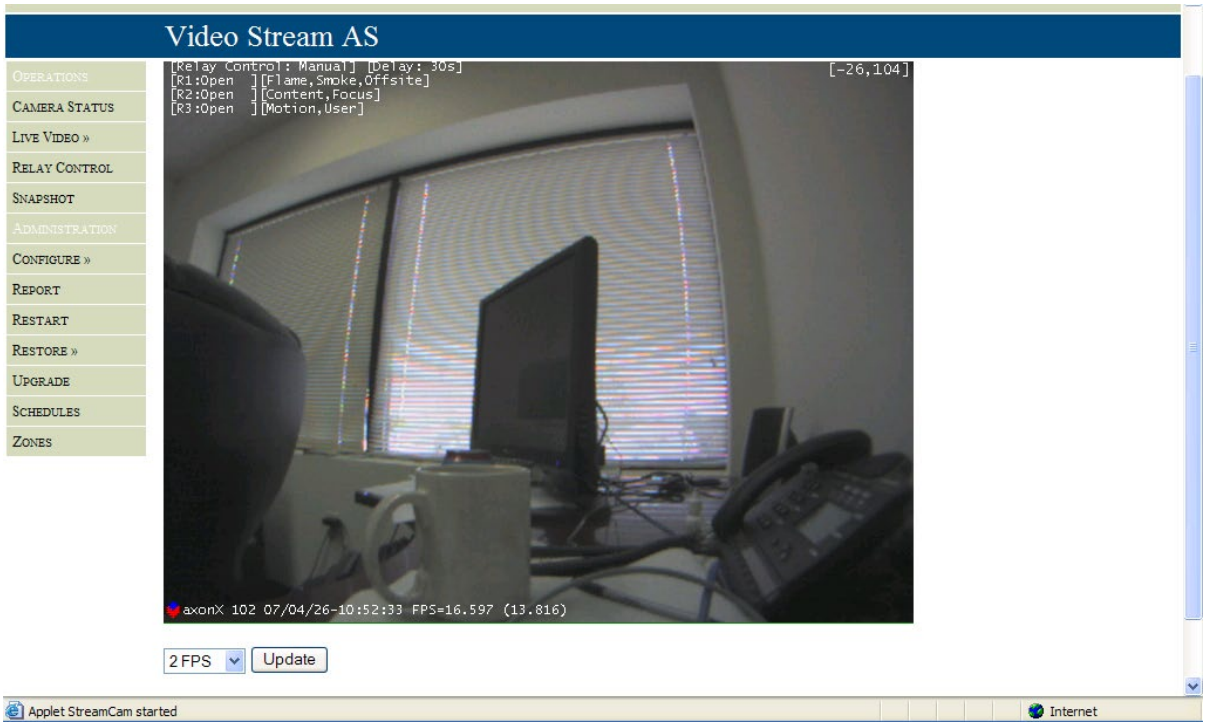


Figure 14 – Live video from the camera at the default 2 fps.

Returning to the **Operations** menu, **Relay Control** identifies the state of the relay, what event types are associated with a given relay, and provides the operator the functionality to confirm, delay, or reset an event, Figure 15. Each relay is configured with event types and can be given a countdown to delay contact closer, so onsite or remote monitoring personnel have time to see and confirm the event before action is taken by the camera. The monitoring personnel can then **confirm** the event, which instantly closes the dry contact, **delay** the event which resets the countdown, or **reset** the event, which resets the background image and closes the event file.

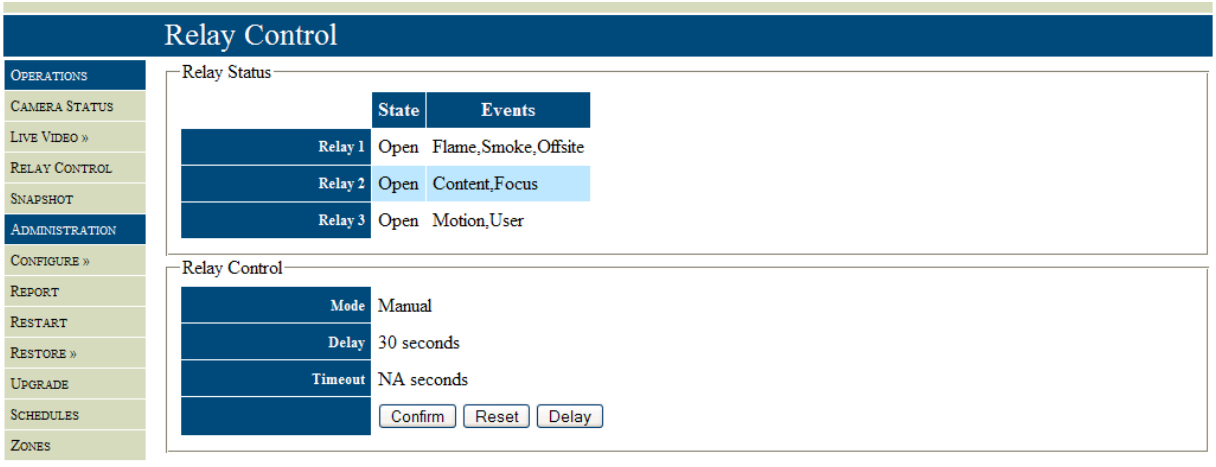


Figure 15 – Relay Control provides the operator with the functionality to confirm, delay, or reset an event.

The final feature available to the operator is a **Snapshot** feature, which provides a current frame to the operator, Figure 16.

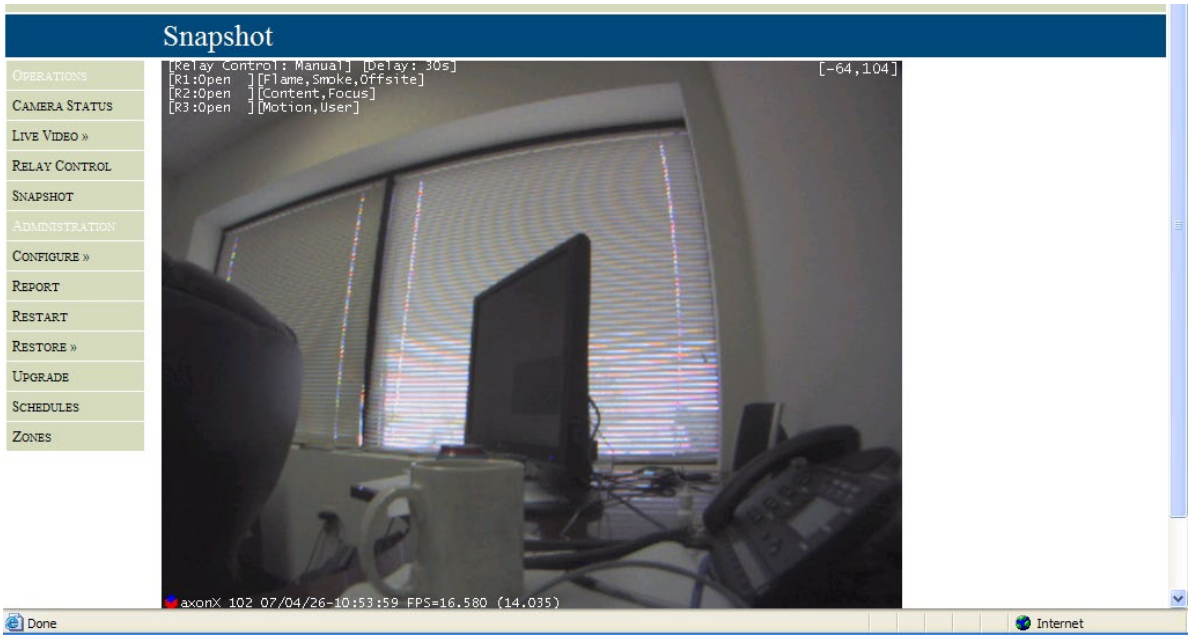


Figure 16 – Snapshot taken from the camera.

3.5 Administration Features

The administrator (a trained and certified authority having sole control of the settings) of the system has a number of features he/she should be familiar with and will have to configure to fit the architecture and design of the system. This includes network configuration, sensitivity settings, relay closures, schedules, zones, and passwords. The first feature on the administrator menu is the configuration tab that contains a number of sub-menu items, Figure 17.

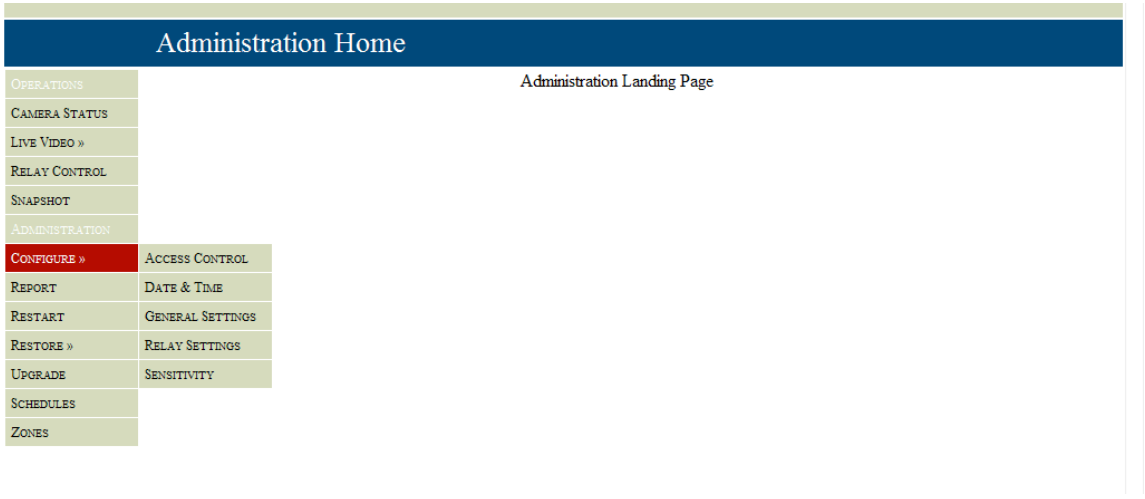


Figure 17 – Configure option under the administrator section has a number of sub-menu features.

The first submenu item is **Access Control**, Figure 18. This allows the administrator to change the manufacturer pre-set passwords for both the operator and administrator.

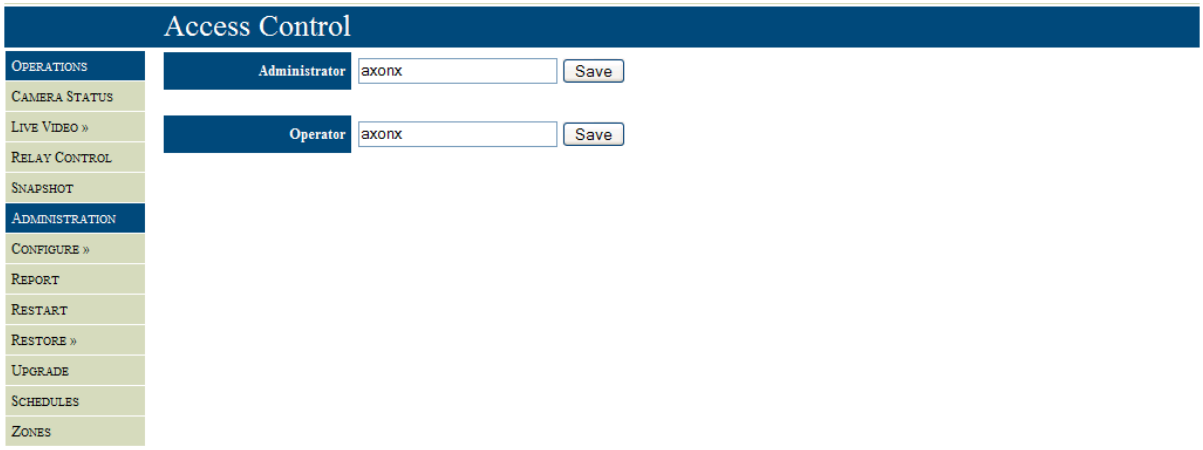


Figure 18 – Access control with the default password (axonx).

The next submenu item is the **Date & Time,** Figure 19. This allows the administrator to set the date (mm/dd/yyyy) and time (hh:mm:ss) in order to synchronize the camera with other systems.

Figure 19 – Date & Time set.

The **General Setting** is a sub-menu found in the **Administration Section** under the **Configure** selection, Figure 20. This is where the mode (static IP or Dynamic Host Configuration Protocol (DHCP)) of the camera is set. If the camera is on a static network, the IP address, Subnet Mask, Gateway, DNS server, and the domain name must be filled out. If DHCP is selected, the fixed IP settings can be left in their default setting. The IP cameras can work on both a fixed and DHCP network. However, due to the fact that any physical location will be tied to the IP address, care should be taken in setting up a DHCP network so the physical location can be determined, and the camera location can be identified by the IP address. When using a DHCP configuration, the best way to ensure a camera gets the same address is to fix the given IP address to the cameras MAC address and give the camera an appropriate name. Contact the IT personnel to assist in configuring the network setup.

After the network setup comes the camera setting, which defines the camera name, flicker control, frame time, and video format (NTSC or PAL). The camera can be given a name of up to 24 characters. It is best to name the camera after the physical location to expedite the response to the event scene.

The flicker control is used to set the frequency and mode of the flicker control. The frame time is used to increase or decrease the rate at which images are captured by the camera. A value of 60 represents a frame rate of approximately 16 fps (1000/60); at 30, the frame rate would increase to 32 fps (1000/30). The video format should be set depending on the standard in use in the country of installation. For North America, it is NTSC and PAL for European countries.

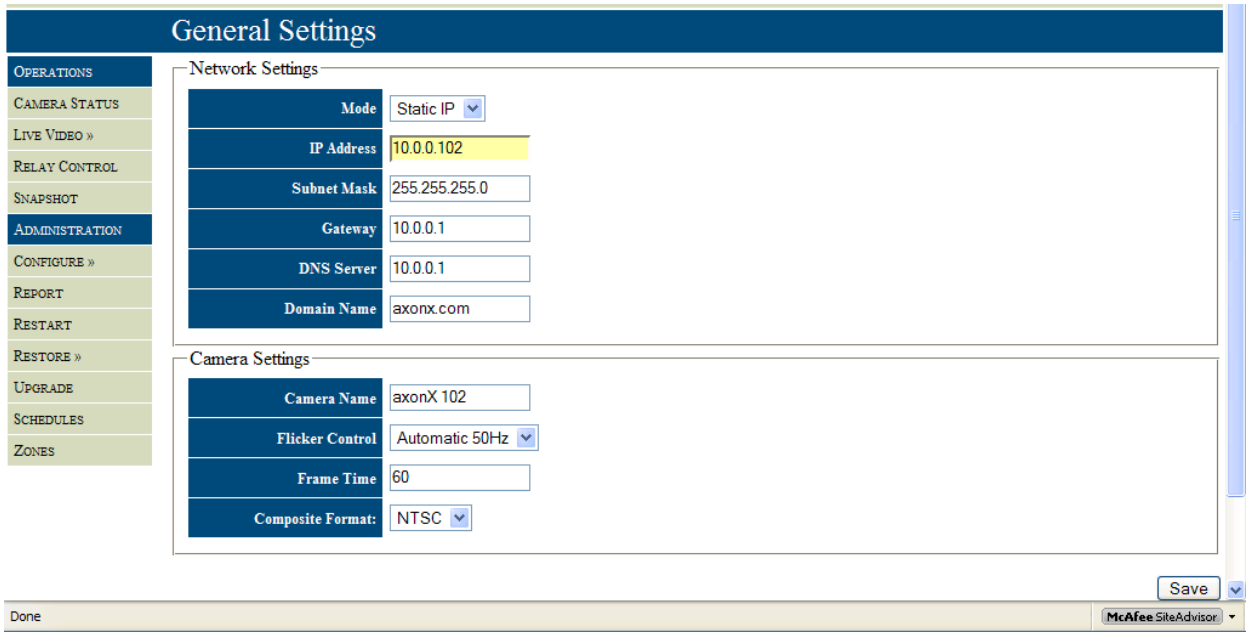


Figure 20 – General settings used to configure the Network settings and Camera settings.

Once proper operation of the camera is confirmed and the appropriate communication scheme (static IP or DHCP) is selected, all further steps for camera configuration may be completed after the camera is physically installed. However, further set-up may be continued at this point.

The **relay settings** page defines when, under what event types, one of the three relays will close as well as if the relay will be automatic (no delay) or manual (with delay), Figure 21. If manual is chosen, a delay can be set in place to provide time for the monitoring personnel to confirm, delay, or reset the event. The delay time can be set from 0 to 250 seconds. To initiate a relay, select the desired event you wish the relay to activate on. The selected events will cause the relay to switch states. This can be tested using the operator feature Camera status. The default setting is relay one: smoke and fire alarm, relay two: trouble, and relay three auxiliary (left blank). Relay two is reversed so as to close on loss of power and should remain a trouble contact.

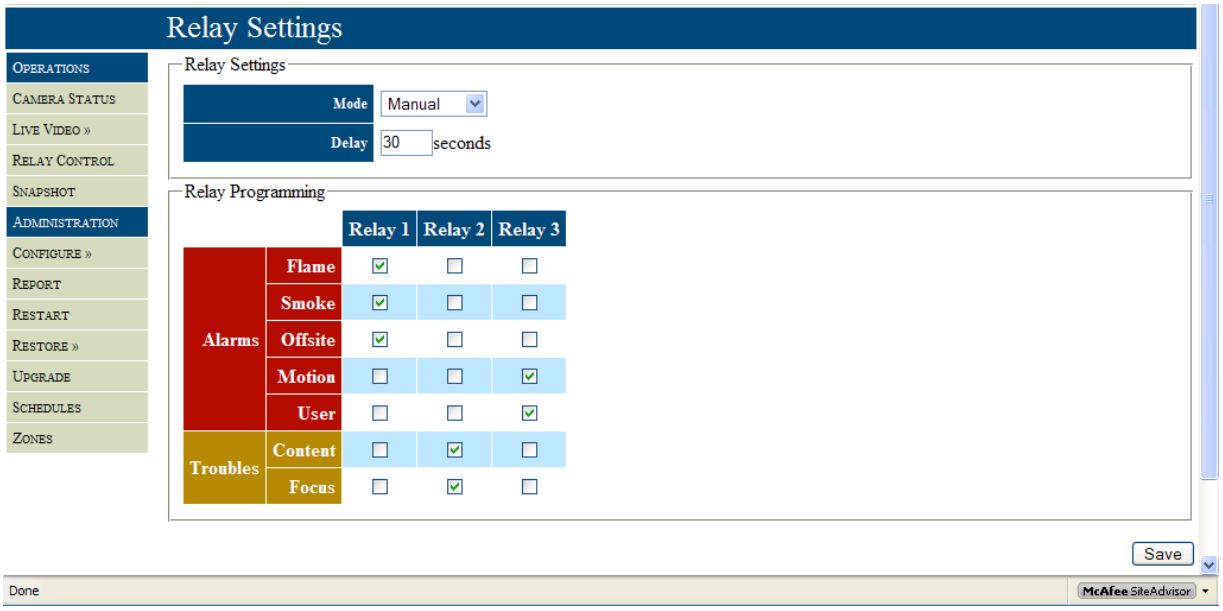


Figure 21 – Relay settings are configurable.

The final sub-menu feature is the cameras **Sensitivity Settings,** Figure 22. All three algorithms are by default set to medium, and the dynamic function is set to off. The system is FM approved for a sensitivity setting of medium for both flame and smoke.

NOTE: The Offsite algorithm is not an FM approved detection method.

The fire, smoke, and offsite (reflected firelight) algorithms can be set to low medium or high. The smoke also has an ultra-sensitivity setting used for very clean and stable environments. The dynamic setting is used in applications that have light fluctuations due to windows, large doors, or processes that make the background image unstable and may cause nuisance alarms. The system is for indoor applications only.

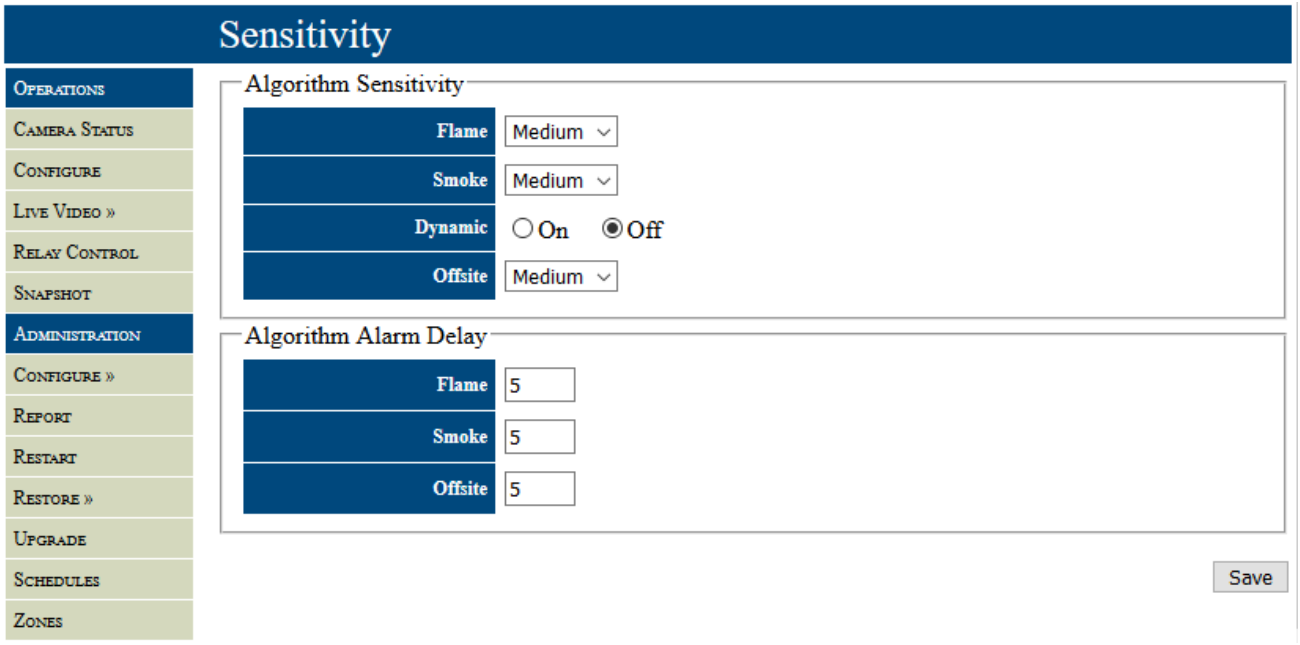


Figure 22 – Sensitivity settings

The **Camera Report** feature, Figure 23, is a useful tool for installers, AHJ's, and for maintenance purposes. The button provides all the selected variables in a format that can be saved to a text file and printed out for record-keeping.

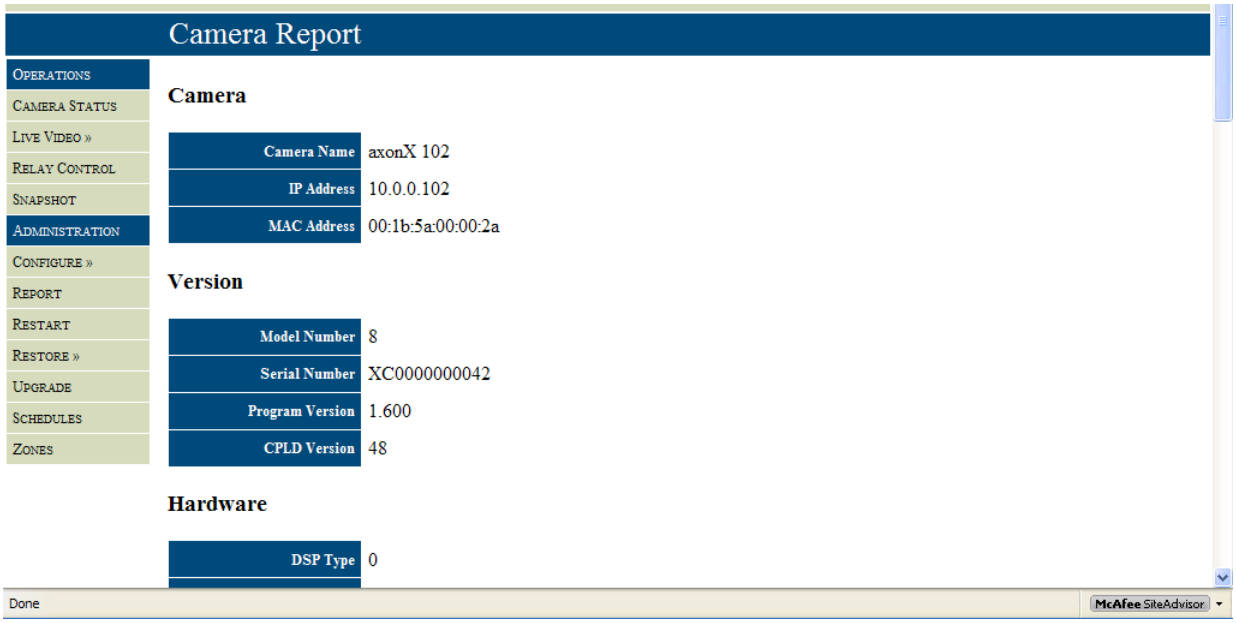


Figure 23 – The camera report provides a list of the configured variables.

The **Restart Camera** button, Figure 24, reboots the camera. You will be asked if you are sure you wish to restart the camera to avoid an accidental restart. Whenever changes are made to the camera setting within the camera interface, it is good practice to save and restart the camera.

NOTE: If you restart the camera after changing communications settings, you will lose communication with the camera until you enter the same settings on the computer. Powering down the camera also performs a restart. It is recommended that the restart function be used with caution.

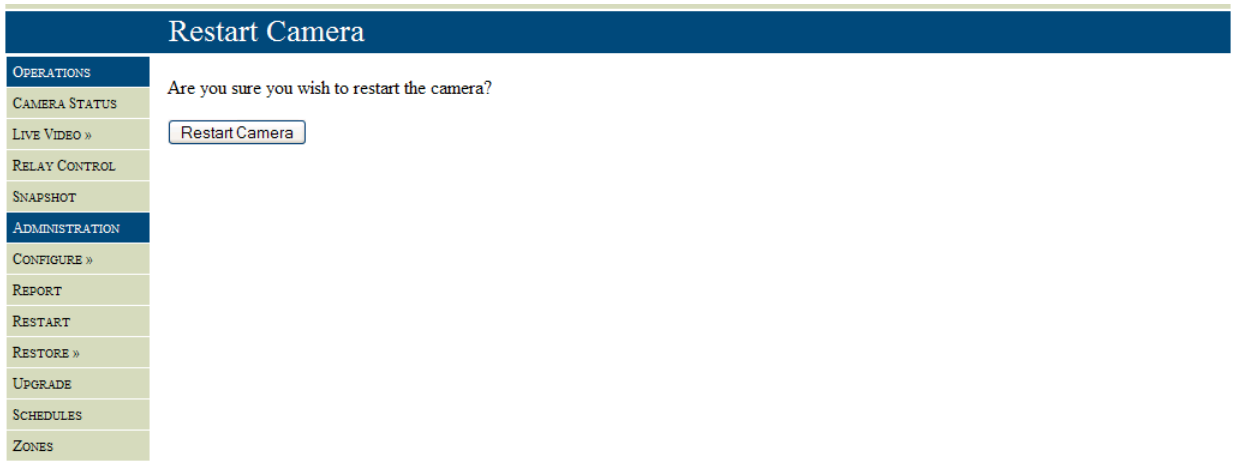


Figure 24 – Camera restart

The **Restore** sub-menu option provides two options: **Reset Camera** and **Factory Defaults**. The **Reset Camera** button, Figure 25, reboots the camera and sets the configuration to the default settings; however, it does not change the network settings.

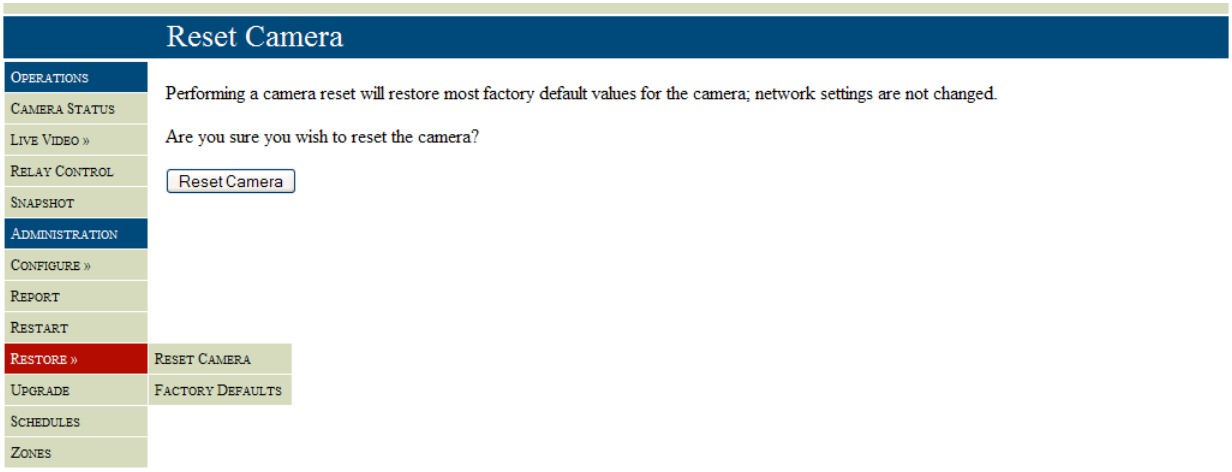


Figure 25 – Camera restore

The **Restore Factory Defaults** sub-menu option, Figure 26, resets all the settings to the default value; this includes clearing all schedules and zones.

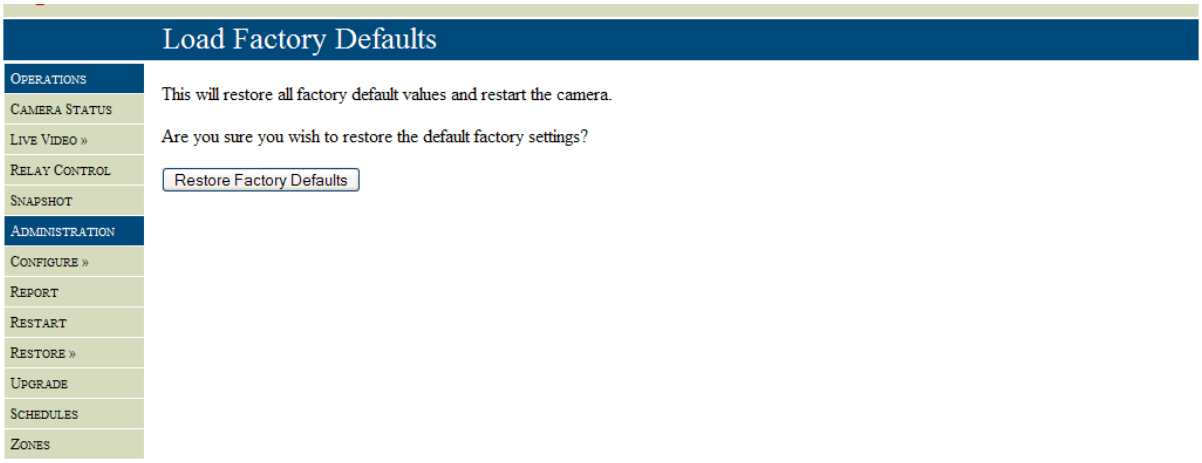


Figure 26 – Load Factory Defaults

The **Upgrade Firmware** feature allows the end-user to upgrade the software on the FVA-IP camera when it is suggested by the manufacturer, Figure 27.

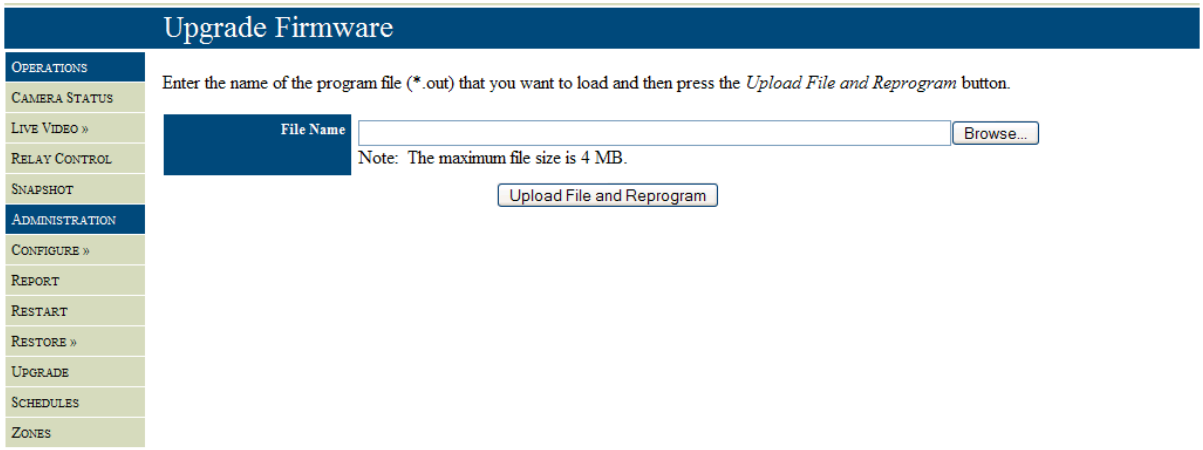


Figure 27 – Firmware upgrade window

To upgrade the firmware:

1. Select **Upgrade** from the administrator section of the menu bar on the left-hand side.

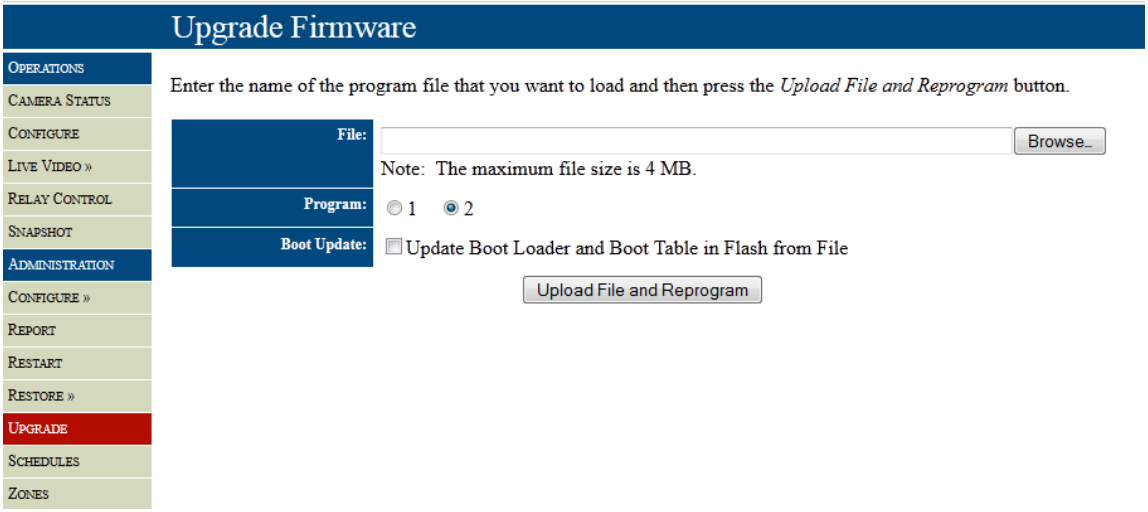


Figure 28 - Upgrade Firmware page

2. Select **Browse** to find the new firmware version that was supplied to you.
3. Leave the options of Program and Boot Update settings at the default. See Figure 28.
4. Click **Upload File and Reprogram**. This might take several minutes, do not disconnect the camera during this process. You will then be prompted to Restart the Camera.
5. Select **Restar**t from the left-hand side menu bar and click restart.
6. Once the camera restarts, you can check the program version by selecting **Report** on the menu bar. Under Version, the Program Version will be listed. See Figure 29.

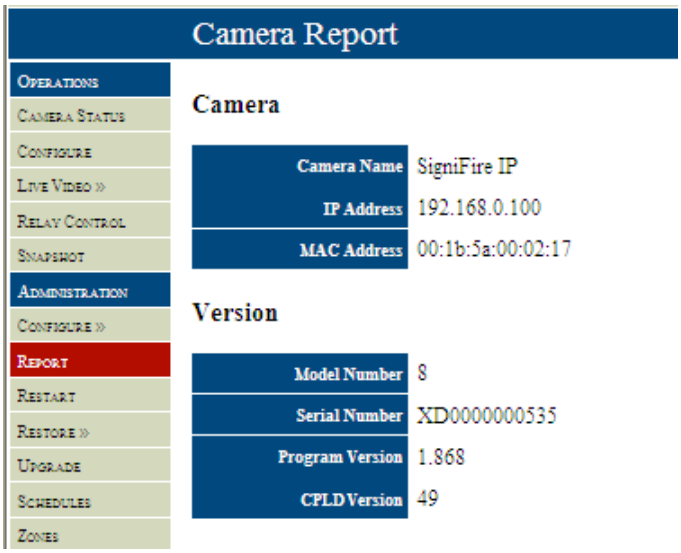


Figure 29 - Camera Report page-showing program version

The **Schedules** feature is used to create a reoccurring or single time period that is then attached to a zone to activate or deactivate that zone for the allotted time period. It is suggested that the Fike Video Analytics video management software be used to set all schedules and zones once the system is in place and being commissioned. It is significantly easier to make these changes in the video management software interface.

To create a schedule, select *Create Schedule* from the top of the Schedules window pane, Figure 30. You will then be asked to set the schedule by first providing a name then defining the time period, Figure 31. The name should reflect the schedule type, so it is intuitive when attaching it to a zone. You then select:

- The frequency (once, daily, weekly, monthly, yearly)
- The days of the week (Monday to Sunday)
- The days of the month (0-31)
- The months of the year (January to December)
- And the time (0 – 1439 minutes)

If multiple days of the month or multiple time slots are needed, they should be separated by commas. For example, "1,15,30" in the days of the month slot would mean the 1st, 15th, and 30th of the month or 0,60,360,960 in the time slot would mean from midnight to 1 in the morning and then from 6 am to 4 pm in the afternoon.

Figure 30 – Creating a schedule.

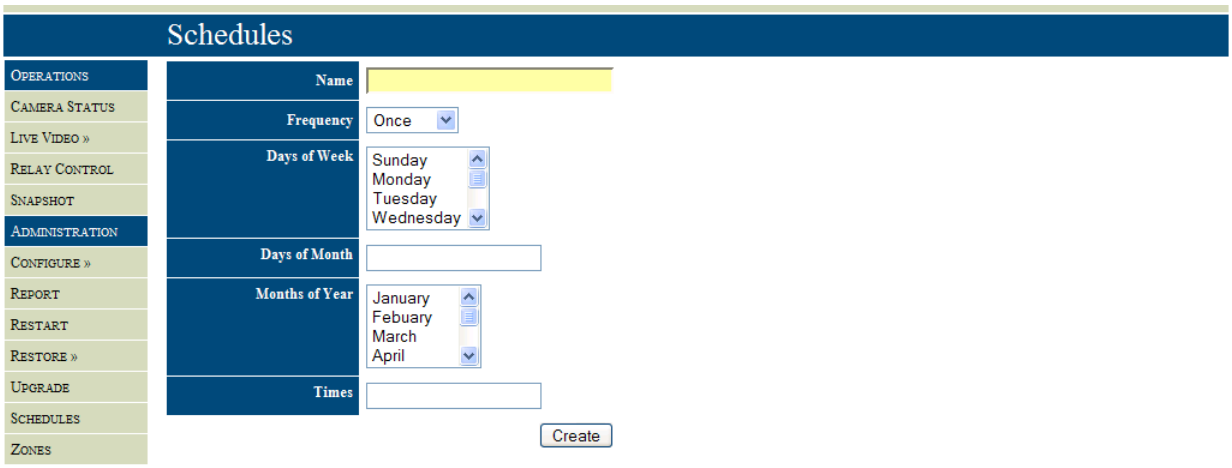


Figure 31 – Schedule inputs

To create a zone, select the **Zone** button and Create Zone from the top of the zones window pane, Figure 32. You will then be prompted, as in Figure 33, to provide:

- A zone name
- The type of zone (Flame, Smoke, Offsite, Motion)
- The action (Block or Detect)
- Sensitivity (0-307,200)
- Points (x,y,x,y)
- Attach a schedule, if desired.

Again, it is suggested that the Fike Video Analytics video management software be used to set all schedules and zones once the system is in place and being commissioned. The zone name should be descriptive in nature and describe the purpose of the zone. The user must define the type of zone and the action taken by the zone. Generally, you will be blocking the ability to detect fire, smoke, and offsite analytics and detecting motion within a zone. The sensitivity parameter is only applicable to a motion zone and represents the amount of pixel shift expected by the intruder (large or small in the FOV). The points define the zone shape and size with a needed input of four points to define the x,y pixel coordinates of the square zone.

Figure 32 – Zone window

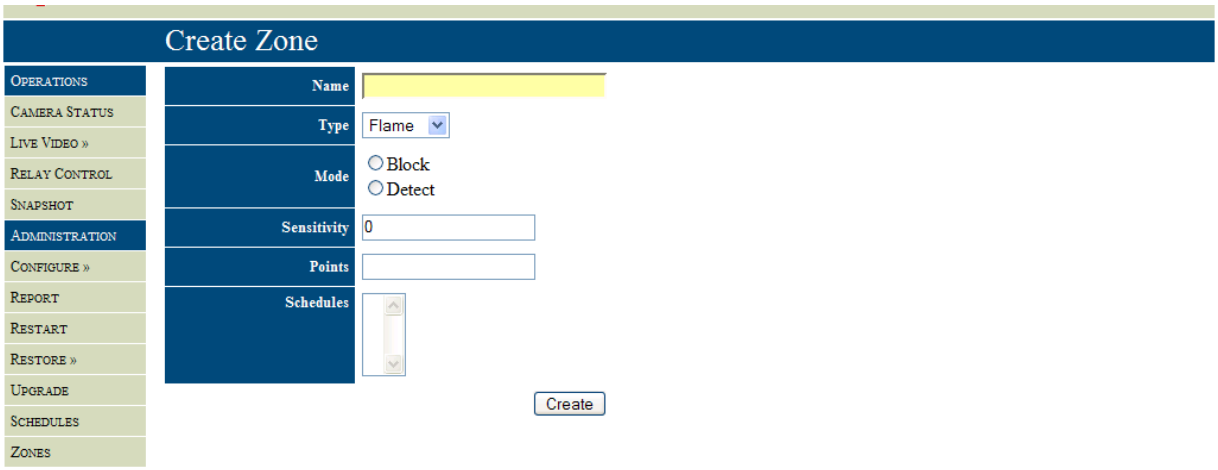


Figure 33 – Create a zone by providing a zone name, type, action, and zone size defined by points

3.6 Finishing Camera Setup

Now that the software interface to the camera has been solidified, it is time to mount the cameras properly.

Installing Cameras

When installing the cameras, point the camera horizontal with no more than a 5 or 10-degree downward angle, so the camera looks out into the space. Do not point the camera down**,** as the patterns the camera identifies as flame and smoke look different when looking down onto a fire rather than out at it. Pointing the cameras downward will cause increased nuisance alarms and may diminish the ability of the camera to detect fire and smoke.

Focus the Cameras

It is extremely important that you get a proper focus that produces a sharp image, as the camera uses image contrast as a factor in identifying smoke. A fuzzy, out of focus lens will produce nuisance alarms.

Maximize Cameras Field of View

When installing the cameras, ensure there are no obstructions directly in front of the camera. And mount the camera to look out at the hazard area to cover the most space possible.

For further setup information, see section 5 of Fike Document 06-529, IP Smoke, and Fire Detection Camera Applications Guide.

CE Installation Requirements

To meet the emission requirements established by the European Union (CE), ferrite beads, P/N 02-14682, must be installed on the 12-24VDC low voltage input power line (terminals 1 and 2), and on the incoming cables connected to the dry contacts (terminals 3 through 11) located on the back of the Fike FVA-IP camera, Figure 34.

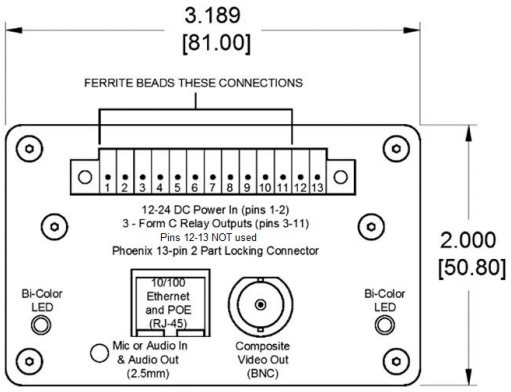


Figure 34 – FVA-IP Camera Back View

Ferrite Bead Installation

Three (3) ferrite beads are provided with each camera. A separate bead must be installed on the low voltage input power line in order to maintain separation between non-power-limited and power-limited wiring. The remaining two (2) beads are provided for the dry contact circuit wiring. The incoming circuit wires must be looped through and around the ferrite bead, Figure 35.

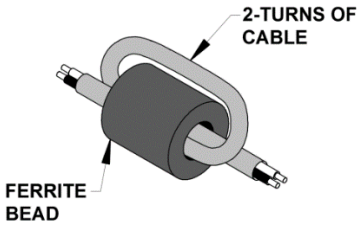


Figure 35 - Ferrite Bead Installation

NOTE: Beads must be located as close to the IP camera as physically possible.

NOTE: The Ethernet and Coax Cable connections do not require ferrite beads.

4.0 Video Management System

FVA-IP cameras do not have any storage capacity on board to capture and replay video images of alarm conditions. This must be done through the use of a video management system. In addition, the video management software user Interface does not communicate directly to FVA-IP cameras, but rather through the Fike Video Analytics server software installed on the FSM-IP NVR.

If the Fike Video Analytics system is not using the FSM-IP hardware/software package, then an alternative third-party video management system must be used. A Software Development Kit (SDK) is available that allows such third-party systems to use software modules to gain access to data from Fike Video Analytics FVA-IP network cameras and to act as a conduit for control commands from the Fike Video Analytics video management software to the cameras. If your installation is using a third-party video management system, contact Fike Video Analytics Corporation for further information on the SDK.

5.0 Fike Video Analytics Video Management Software

Now that the cameras are installed, and the FSM-IP video management system has been placed on the local area network (LAN), the video management software can be installed on an approved PC workstation. The VMS software is used to create the organization structure, configure the camera settings, and monitor the cameras. The VMS software should be installed on at least one local workstation located on the same LAN as the cameras. However, additional copies of the VMS software can be installed on other computers that have network access to the video management system being used. See appendix C for VMS software system requirements. For more detailed information on the Fike Video Analytics video management software and its plethora of functions, please see the Fike Video Analytics video management software manual.

6.0 Commissioning

It takes approximately 30 days to properly install, commission, and fill out commissioning paperwork. It is important to contact the local Authority Having Jurisdiction (AHJ) or the facility manager in charge of monitoring the fire protection system prior to application to ensure all required paperwork has been completed.

At a minimum, commissioning includes:

- Testing and stability period – where the system is subjected to fire and nuisance sources to demonstrate stability and performance.
- Documentation - Documentation of the organizational structure, camera settings, sensitivity settings, zones, schedules, and events archive. (see Appendix D)
- Preliminary Maintenance and service check - The system should be checked according to the service and maintenance requirements to establish the system's condition upon installation.

Once the system is in place and settings adjusted as necessary to ensure optimum performance, the system can be handed over to the end-user (on-site security or a remote monitoring facility). The system owner should record any changes up to one year after the commissioning of the system.

NOTE: During the commissioning period, the cache file and memory storage on the video management system should be regularly checked to ensure that adequate memory is available to store events for 30 days.

7 Inspection, Testing, and Maintenance Recommendations

7.1 NFPA 72, Chapter 14 recommendations

NFPA 72, section 14.4.3.3 dictates that video image smoke and flame detectors shall be inspected, tested, and maintained in accordance with the manufacturer's published instructions. Fike Video Analytics Corporation, as the manufacturer of the FVA-IP video image flame and smoke detector, has detailed these procedures to aid end-users, AHJs, and Fike Video Analytics distributors in establishing an inspection, testing, and maintenance program. It is in the interest of all parties to ensure that a functional system is provided and maintained.

7.2 Inspections

Inspections should be done on a semi-annual basis (twice a year); however, camera(s) and associated equipment that are inaccessible for safety considerations (e.g., continuous process operations, energized electrical equipment, radiation, and excessive height) shall be inspected during scheduled shutdowns if approved by the authority having jurisdiction. These extended intervals shall not exceed 18 months. The inspection should ensure no obstructions are between the detector and protected area, that lenses are clean and free of contaminants, that the cameras do not have mechanical damage, and that the unit is directed toward the intended hazard.

Obstructions within 10 ft. (3 m) of the camera that obstruct the line of sight to the hazard area are to be removed, or the camera location is to be adjusted to ensure that the hazard area is covered.

The video feeds at the monitoring station (Fike VMS software) can be checked for clarity to ensure that a buildup of dust, grease, or other debris has not obscured the lens. Reference images produced from the Fike VMS software report (see VMS manual) can be used as a reference.

A visual inspection of the camera should be made to identify mechanical damage. LED’s on the front and rear panel indicate a camera state of alarm, processing, and communication.

The cameras field of view (FOV) should be checked to ensure that it matches the Fike video management software Audit report and that the cameras have not been moved or miss-aligned. An audit and audit verification should be conducted every six months.

7.3 Testing

Testing should be done on an annual basis; however, camera(s) and associated equipment that are inaccessible for safety considerations (e.g., continuous process operations, energized electrical equipment, radiation, and excessive height) shall be tested during scheduled shutdowns if approved by the authority having jurisdiction. These extended intervals shall not exceed 18 months. Testing can be broken down into two sections; functional and operational conformance. Tests are performed by Fike Video Analytics Corporation as part of the Quality Control (QC) process. All FVA-IP cameras undergo extensive testing before being shipped to a customer as part of Factory Mutual (FM) approval conformance. These tests include live-fire tests, communication tests, and a burn-in of the cameras.

Cameras located on-site should be visually inspected quarterly for operational conformance. This is done by observing the user interface video stream and the front faceplate of the camera. If an image is present and the overlay text added by the software is updating (time and frame rate will progress and fluctuate respectively), then the cameras are functioning and they have the ability to detect at the prescribed sensitivity levels.

7.3.1 Difference in Functional and Operational conformance

Functional conformance is defined by the method of detection being valid and applicable for the given conditions and is determined primarily by a systems specification. Operational conformance is affected by the deterioration of the system performance over time due to such issues as the long term applicability of the system and the environmental and natural factors surrounding the camera.

7.3.2 Factors affecting Functional Conformance

The FVA-IP camera-based system should only be applied in ways that conform to our manufacturers' recommendations. Those include:

- Minimum/Maximum detection range
- Minimal size of flame to be detected
- Minimal size of the smoke plume to be detected

7.3.3 Factors affecting Operational Conformance

Among factors affecting Operational Conformance are the environmental and natural factors.

1. Environmental factors directly affect the integrity of optics (lenses), resulting in deterioration of image quality beyond the limits prescribed by the manufacturer.
2. Natural factors are caused by the aging of the components of the system, causing deterioration in overall performance or catastrophic failure of the entire system.
3. Man-made factors such as alteration of lens focus, capping the lenses, alteration of camera position and direction.

The FVA-IP camera detects fire and smoke by applying sophisticated image analysis algorithms to digitized video images acquired by the CMOS sensor. One can divide this process into 2 stages. The first stage is the formation of the image and acquisition into the digital form. The second stage is the processing of the sequence of digitized images. The first stage is analog in nature, while the second stage is digital. The implication of this division is very important for how one will address the conformance testing mainly because the second stage cannot deteriorate gradually over time. **If components of the system in the second stage degrade beyond the acceptable limit, the system simply fails, resulting in an off-line condition.** For the first stage, such deterioration, primarily optical integrity or degeneration of the sensitivity of the sensor will result in significant degradation of the acquired image quality and will be detected by the second stage as fault condition and reported accordingly.

The Fike Video Analytics built-in self-diagnostics will address most accidental man-made factors and will report faults if the camera is out-of-focus, covered, or has been turned towards the wall. Minor alterations of the camera's field of view are addressed by the semi-annual inspection.

It is important to note that self-diagnostics of the image quality is an integral part of the detection analytics. The image acquisition, alarm algorithms, diagnostic process, and communication are all interconnected. Therefore, the detection part of the analytics cannot fail without the diagnostics part, as well as the image processing chain, and communication is left unaffected. As in any digital computer system, it will be an all-or-nothing failure with any failure resulting in a closure of the trouble dry-contacts and a loss of signal to the user interface.

7.4 Testing for Operational Conformance

The goal of this testing is to assure that the entire system will register and properly report the following:

1. Deterioration of the image quality (contrast, focus, brightness) will cause a fault condition
2. Communication failure of the camera
3. Simulated response

7.4.1 Fault Condition

A fault condition can be tested by simply applying the cap or covering the lens of the camera with your hand or lowering the light level below the alarm threshold. The system will respond by reporting a fault in approx 30 sec.

7.4.2 Communication failure / Analytics failure

A fault can also be achieved by disconnecting the camera from the network switch. The fault relay will close immediately, and the Fike video management software will report a loss of the camera in less than 10 seconds.

7.4.3 Simulated response

There are three ways in which to test whether event reporting is operational. These should be discussed between the end-user, AHJ, and distributor as to which is applicable for the installation.

The first method is to temporarily introduce a motion detection zone and configure the relays to close on the detection of such motion. Introducing motion into the observation area will cause a closure of the relay, and an alarm response will propagate to the user interface. On completion of this test, the motion zone can be removed, and the relay disengaged. This scenario verifies that all camera functions are working properly and ensures that image capture, software, and communication are functioning.

The second method is to initiate a user alarm after configuring the relays to close on the user-initiated alarm. This will cause a closure of the relay, and an alarm response will propagate to the user interface. On completion of this test, the user alarm can be stopped, and the relay can be disengaged. This scenario ensures that communications are functioning, and a visual inspection of the video ensures software integrity.

The third method is to initiate live fires within the cameras field of view. This can be done using safe smoke (Regin smoke emitters) and low shooting flames (Isopropyl alcohol or heptane) or a properly configured propane torch (air inlets must be covered to create a diffusion flame). These live fire tests will initiate an alarm much like a motion or user event and close the respective dry contact and send an alarm response to the user interface. The distance the testing can occur from the camera will be based on the size of the smoke emitter or flame used. Below is a table of fire size to distance.

Table 3 - Fire Size to Distance

Source	Distance (ft)
Plumbers propane torch	<20 ft
6 in pan fire	<30-50 ft
1 ft pan fire	<100 ft
90-second smoke emitter	<30 ft
3 min smoke emitters	<50-60 ft
4 min smoke emitters	<100 ft
Theatrical smoke	Varies based on equipment

After finalizing testing, an Audit should be created for verification purposes using the FVA video management software.

7.5 Maintenance

This section deals with preventive maintenance, describes possible faults in camera operation, and indicates corrective measures. Ignoring these instructions may cause problems with the detector and may invalidate the warranty. Whenever a unit requires service, please contact the manufacturer or its authorized distributor for assistance.

Maintenance should be done on an annual basis; however, camera(s) and associated equipment that are inaccessible for safety considerations (e.g., continuous process operations, energized electrical equipment, radiation, and excessive height) shall be maintained during scheduled shutdowns if approved by the authority having jurisdiction. These extended intervals shall not exceed 18 months. The FVA-IP camera is designed to provide years of trouble-free operation with little to no attention; however, the periodic maintenance steps described below will allow for reliable fire protection.

Maintenance records should be kept on each detector and stored in a logbook. The record should include the name, affiliation, business and telephone number of the person(s) performing inspection, maintenance test, etc. Also, an ID of the unit, test frequency, name of the property, address, the installation date, and entries for every maintenance operation performed, including the description of the operation, date, and personal ID should be included. If a unit is sent to the manufacturer or distributor for service, a copy of the maintenance records should accompany it.

Before working on the IP camera, inform all appropriate personnel of your intention to work on the camera and the duration of which you expect the maintenance interval to last. Disable any automatic systems that may be activated by the cameras' alarm signals. This may include audio and visual alarms or dialers, extinguishing agents, and building controls.

Check the fault log on the Fike video management software to ensure that that the detectors are functioning properly. Note any faults and the cause (low light, blurred image, content, loss of communication, etc.). Fault conditions with their probable cause and corrective action are listed below

Low light – The camera may have been covered, or the area is too dark for proper smoke detection. If the camera is covered, remove the obstruction and take preventative measures to ensure it does not occur again. If the area is too dark, inform the end-user that more lighting is necessary for the smoke detection algorithm to function properly.

Out-of-Focus – The camera’s lens has become too dirty, or the lens itself has moved, resulting in bad focus. Clean the lens and/or readjust the focus to provide a clear image.

Content – an obstruction is too close to the camera, or the camera has become misaligned and is facing a wall or other large object. If possible, remove the obstruction and take preventative measures to ensure that it does not occur again or/and re-align the camera so that the FOV matched that of the previously recorded image.

Communication – A loss of communication from the camera to the end-user interface has occurred. If these are short in duration (less than 5 seconds), they can be due to dropped informational packets on the network, and will not affect system performance. If the loss is greater than 5 seconds, check the condition of the LAN network both physically and operationally. Ensure that the switches are properly powered and in good working order, ensure that all RJ-45 connections are secure and that no mechanical damage has occurred to the network. Finally, ensure that the network bandwidth is large enough for the number of cameras and their frame rate settings.

Inspect the video image feed to the user interface (Fike VMS software) for a build-up of dust, debris, or out of focus lens. There may not be enough to cause a fault condition yet, but cleaning may still be necessary. If necessary, clean the lens with a cotton wipe and commercial liquid glass cleaner. Rinse the lens with clean water and dry with a clean cloth.

Ensure that the camera still has a clear line of sight to the hazard area and compare the previously recorded image report with the current image to ensure that the camera has not been misaligned.

Check to ensure that the camera is securely mounted to the wall.

Re-initiate and disabled automatic systems and inform all appropriate personnel that you now have completed the maintenance and that the system is back online.

That concludes the inspection testing and maintenance of your Fike Video Analytics fire and smoke detection system. By implementing a service and maintenance program, you are ensuring the uninterrupted operation of your system, keeping your assets secure and safe. If you have any questions, please contact Fike Video Analytics Corporation.

7.6 Camera Replacement

In the event a camera is damaged, or the camera itself fails, the camera should be replaced to ensure coverage. The replacement of a camera is a simple process if a current audit report of the system has been maintained. The audit report that is generated by the video management software is a documented record of all the camera settings. This audit report allows the camera's sensitivities, delays, zones, and schedules to be reconfigured onto a new camera. Without the audit report, the camera will have to go through the commissioning cycle, which requires time to collect all the nuisance events and re-configure the settings. **It is very important to have a copy of the audit report.**

Step 1 – Ensure the connection to the fire alarm control panel (FACP) has been disabled while the camera is being replaced and reconfigured. Whenever work is done on a camera or within 2-3 meters of a camera, the camera should be detached from the FACP to prevent false alarms.

Step 2 – Using the IP camera's web interface, set the IP address of the replacement camera to the IP address of the camera it will be replacing. To access the camera's web interface, a small system needs to be set up with a laptop and the replacement camera connected to a network switch with Cat5 cable. The camera can be powered with Power over Ethernet (PoE) using a PoE switch or with 12 or 24 VDC on the rear of the camera. Once a laptop, the camera, and switch are connected and powered, the user can access the web interface with an internet browser such as Internet Explorer or Firefox by typing http://192.168.0.100/admin in the address bar. You will be prompted for a user name (admin) and password (axonx).

Once the username and password have been accepted, you will be able to access the camera web interface. You will then select **Configure** and **General Settings** from the **Administrator** section of the menu bar on the left-hand side, Figure 36. You can then enter the new IP address (make sure the Gateway and DNS Server address match the camera you are replacing) and click the save button located in the bottom right of the page. Then select **Restart** from the administrator menu and click on the Restart Camera button to restart the camera. Figure 37.

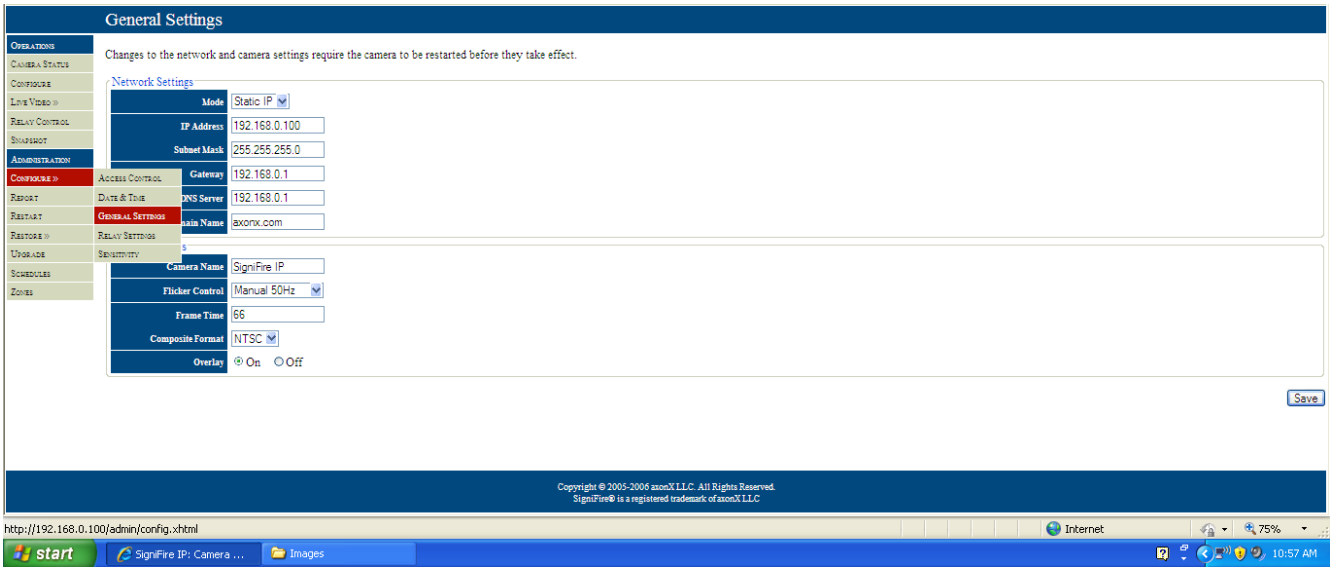


Figure 36 – Camera web interface

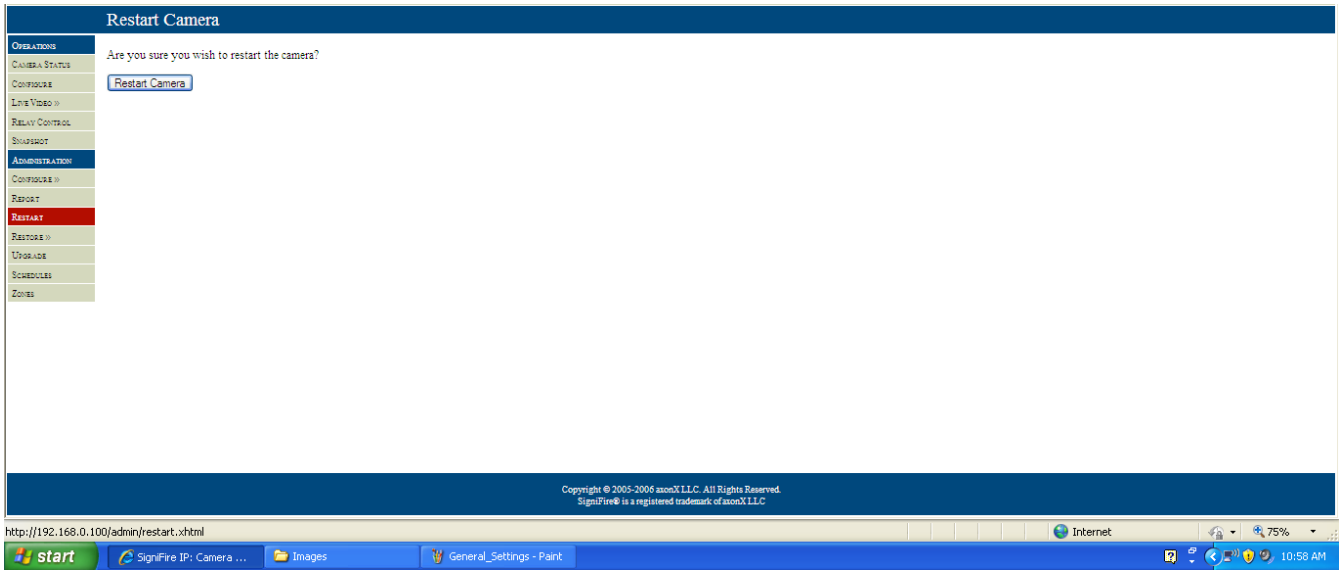


Figure 37 - Restart Camera

Step 3 – With the IP address changed, the camera can be put out in the field and replace the broken and/or damaged camera. The dry contact strip on the back of the broken camera can be removed from that camera without removing the wiring and will fit into the replacement camera, so no wiring will need to be done. Due to the identical IP address, the FSM-IP NVR and the Fike video management software will recognize the new camera.

Step 4 – Using the audit report that shows an image of the camera's field of view, the camera field of view should be lined up to match the original field of view horizontally and vertically. Figure 38 is an example of one page of an audit report. Each camera in a system is given one page that shows its field of view, zones, and settings.

Step 5 – Using the audit report, the camera's sensitivity settings, delays, schedules, and zones should be configured. This is done using video management software and accessing the camera's properties window. Once the settings have been configured, the audit report in the video management software should be regenerated. The two pages should be identical (old audit and new audit) except for the camera serial and MAC address numbers. Adjustments to the zones may be necessary to get an identical match to the original audit.

Channel: 4 Date: 4/6/2011

Address	10.0.0.147	Serial	XD0000000535
Version:	1.847	Name:	SigniFire IP

Detectors	Sensitivity	Delay
fire:	medium	10
smoke:	medium	15
offsite:	medium	5

Relay mode: manual

Relay	flame	smoke	offsite	motion	user	content	focus	network	bright	dark
1	•	•	•	○	○	○	○	○	○	○
2	○	○	○	○	○	•	•	•	○	○
3	○	○	○	•	○	○	○	○	○	○

Zone	Type	Mode	Schedules	Points
m1	motion	detect		464:162,497:242
smokeIII	smoke	block		0:247,78:265,163:262,364:258,539:258, 639:214,639:2,0:2
Flame	flame	block		142:308,295:412

Inspector name_____ Signature_____

Figure 38 – Example of a page from an audit report for a specific camera

Appendix A – FVA-IP Camera Specifications

Fike®
VIDEO ANALYTICS CORPORATION

DATA SHEET

Fike Video Analytics IP Camera

Description

The Fike Video Analytics IP camera combines the enhanced resolution and picture clarity of a standard analog/network camera with built-in fire, smoke and motion detection capabilities. The camera's proprietary onboard analytics is used to continuously monitor the video, frame-by-frame, pixel-by-pixel to detect anomalies characteristic of fire, smoke and motion. The camera video processing algorithms include:

Flaming Fires - looks for a specific fire pattern consisting of a bright core of the flame and a flickering corona.

Smoke Plumes - identifies the anomalies that are caused by smoke and analyzes the progression over a period of time to identify a growing smoke plume.

Ambient Smoke - monitors the light diffusion from light sources and bright objects in the video images to detect the pattern consistent with the slow accumulation of smoke.

Intrusion Detection - can monitor multiple areas of the video image for the presence of moving objects at different times. This can be used to detect and record wanted or unwanted persons.

The software and user defined settings are stored within the camera in non-volatile memory so that the camera automatically starts functioning once power is applied. Each camera is provided with a web interface for communication and camera configuration. The camera connects to a Local Area Network (LAN) using the Ethernet plug on the rear of the camera and must be given its own IP address (static recommended).

Operation

Unlike traditional spot-type smoke detectors or temperature sensors that rely on the transmission and buildup of smoke or heat to initiate an Alarm, the Fike Video Analytics IP camera is a volume sensor which observes and identifies the fire condition within the entire observed space of the camera using video image analysis. It does not rely on the transmission of smoke or heat for Alarm activation. This fundamental difference results in faster smoke and fire detection. In the event of a fire or the production of smoke, the camera issues a warning signal through its onboard contact closures and by digitally streamed transmissions over IP to a monitoring PC running the Fike Video Management Software (VMS).

Approvals

- UL
- FM
- CE
- CSFM

Features and Benefits

- Detection algorithms embedded on camera
- Intelligent edge device
- Benefits of IP network camera security system
- Remote monitoring with Fike Video Management Software (VMS)
- Connect up to 32 cameras per network video recorder (NVR)
- Relay contacts provided on each camera for interface with compatible Fire Alarm Control Panels (FACP)

Ordering Information

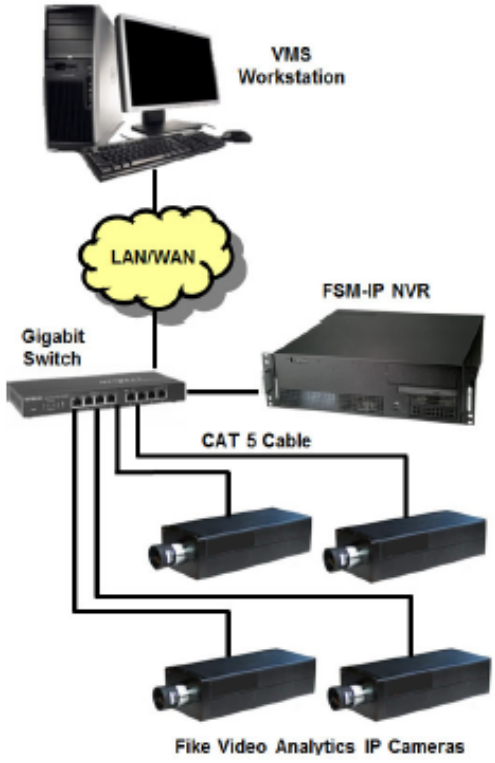
Fike P/N	Description
28-001	Fike Video Analytics IP Camera 2.8mm, 82° Total Field of View Lens
28-024	Fike Video Analytics IP Camera, 8mm, 34° Total Field of View Lens
28-006	Lens-2.8mm, 82° Total Field of View
28-007	Lens 8mm, 34° Total Field of View

Specifications

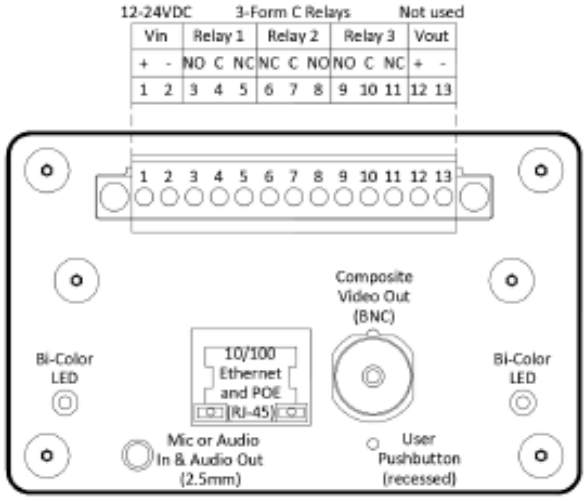
Processor		Texas Instruments TMS320DM642 Digital Media Processor
Memory		128 MB RAM
Clock		Battery backed up real time clock
Imager		Micron CMOS MT9M11
Video Format		Color NTSC
Video Resolution		640 x 480 (NTSC)
Video Compression		MJPEG
UL Minimum Illumination		1 Foot-candle (10 Lux)
Events Notification Medium		http network based communications, Alarm, Trouble and Auxiliary Dry Contacts
Detector Performance	Flame	1 ft. pan fire at 100 ft. (30.5 m)
	Smoke	Indoor detection verified at 100 ft. (30.5 m)
	Motion	Confirmable motion detection based on zones and schedules
Detection Zones		User defined, including detect/non-detect logic. Each zone may be linked to multiple detection schedules (daily, weekly, monthly, yearly, single occurrence)
Weight		1.7 lbs. (771 g)
Temperature Limits		32-120°F (0-49°C) *Must be installed within an enclosure where not in installed in a temperature controlled environment.*
Humidity		5 to 95% relative humidity, non-condensing
Power		• Power over Ethernet (PoE) • 24 VDC
Power Consumption		< 5 Watts, 0.2 amps at 24 Volts 0.4 amps at 12 Volts
Video Management Software		Spyder*Guard* API available for video management integration
Connectors		• RJ-45 Ethernet Jack • Terminal block for three relay outputs • DC power connection • BNC for coaxial analog output
Lenses		2.8mm and 8mm lenses (fixed Iris, fixed FOV, adjustable focus, CS mount)

System Architecture

In its basic configuration, the Fike Video Analytics system will consist of at least one Fike Video Analytics IP camera, FSM-IP network video recorder (NVR), and a Windows based PC running the Fike Video Management Software (VMS) all connected to the same high-speed local area network (LAN). Remote VMS workstations can be located on a different network and will communicate normally as long as the NVR is accessible over a TCP connection.



Where Alarm annunciation is required, three Form-C dry contact relays connections are provided on the back of each Fike Video Analytics IP camera. These connections can be tied into an FM Approved Fire Alarm Control Panel (FACP) to signal individual camera activation.



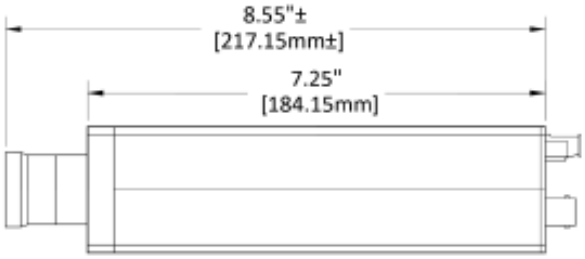
Camera Rear View

Network Requirements

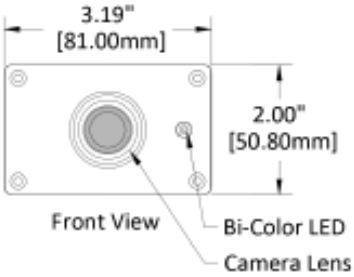
In order for the Fike Video Analytics cameras to communicate with the FSM-IP NVR, they must all share the same high-speed local area network (LAN).

If integrating the Fike Video Analytics components into an existing LAN, consult with your IT representative or system administrator to ensure that adequate capacity is available to handle the camera(s) bandwidth. Contact your Fike Video Analytics distributor for additional information regarding network requirements.

Camera Dimensions



Side View



Appendix B - Dry Contact Diagram

V_{in}		Relay 1			Relay 2			Relay 3			V_{out} (Not used)	
+	-	NO	C	NC	NC	C	NO	NO	C	NC	+	-
1	2	3	4	5	6	7	8	9	10	11	12	13

Appendix C – Fike Video Analytics System
FM approved Computer Requirements

Minimum requirements - Pentium III 600 MHZ, 128MB RAM, 10GB HDD
800x600 pixel screen resolution, true color video adapter,
Windows 2000, Microsoft Speech, Microsoft .NET runtime v.1.5

Recommended – 2 GB RAM, 1024x768 pixel, true color video, sound card, Windows 7

Appendix D - Commissioning Paper Work

System Audit:

Client version: 1.3.2.36
Inspection Date: 6/22/2009 10:39:43 AM

Servers:

Address	Channels	Version
DEV	4	3.2.2.832

Cameras:

#	Name	Address	Server	Serial#	Version
1	AXNIPC	10.0.0.142:80	DEV	XC0000000097	1.841
2	AXNIPC	10.0.0.143:80	DEV	XD0000000118	1.841
3	SigniFire IP	10.0.0.144:80	DEV	XC0000000151	1.841
4	AXNIPC	10.0.0.145:80	DEV	XD0000000052	1.840

Inspector Name: _____

Channel #1 Date: 6/22/2009 10:39:43 AM
Address: 10.0.0.142:80 Serial: XC0000000097
Version: 1.841 Name: AXNIPC

Sensitivities			Delays (seconds)
Flame:	medium		9
Offsite:	off		7
Smoke:	medium	dynamic	6

Relay mode: auto Relay Delay: 90 sec.

Relay	Flame	Offs	Smoke	Motion	User	Cont	Focus	Netwk
1	X		X					
2						X	X	X
3				X	X			

Schedules:
daytime daily Minutes(244:1321)
nightly daily Minutes(0:398,1212:1439)

Zones:

Name	Type	Mode	Points	Sens	Schedules
ml	motion	detect	11,197 614,369	50	none
smk_block	smoke	block	0,212 640,480	50	none
sky	smoke	block	0,0 640,230	50	none
motionII	motion	detect	491,271 630,470	50	none

Person performing inspection _____

Channel #2 Date: 6/22/2009 10:39:43 AM
Address: 10.0.0.143:80 Serial: XD0000000118
Version: 1.841 Name: AXNIPC

Sensitivities

Flame: medium
Offsite: medium
Smoke: medium dynamic

Delays (seconds)

5
5
5

Relay mode: auto Relay Delay: 90 sec.

Relay	Flame	Offs	Smoke	Motion	User	Cont	Focus	Netwk
1	X		X					
2						X	X	X
3				X	X			

Schedules:

everday daily Minutes(119:1398)

Zones:

Name	Type	Mode	Points	Sens	Schedules
motion	motion	detect	319,78 377,170	50	everday
motion1	motion	detect	494,133 637,311	50	everday
smk_block	smoke	block	0,180 640,480	50	none
smk_wall	smoke	block	315,27 444,160	50	none
smk_wall2	smoke	block	445,20 640,225	50	none
smk_wall3	smoke	block	79,59 160,146	50	none

Person performing inspection _____

Channel #3 Date: 6/22/2009 10:39:43 AM
Address: 10.0.0.144:80 Serial: XC0000000151
Version: 1.841 Name: SigniFire IP

Sensitivities			Delays (seconds)
Flame:	medium		5
Offsite:	medium		5
Smoke:	medium	dynamic	5

Relay mode: auto Relay Delay: 90 sec.

Relay	Flame	Offs	Smoke	Motion	User	Cont	Focus	Netwk
1	X		X					
2						X	X	X
3				X				

Schedules:
everyday daily Minutes(480:1020)

Zones:

Name	Type	Mode	Points	Sens	Schedules
smk_block	smoke	block	0,242 253,480	50	none
fire	flame	block	218,165 569,209	50	none
ml	motion	detect	410,373 639,480	50	none
smk2	smoke	block	277,308 640,480	50	none
sm33	smoke	block	374,249 640,480	50	none

Person performing inspection _____

```
Channel #4                              Date: 6/22/2009 10:39:43 AM
Address: 10.0.0.145:80                  Serial:  XD0000000052
Version: 1.840                          Name:    AXNIPC
Sensitivities                           Delays (seconds)
Flame:   medium                         5
Offsite: off                            5
Smoke:   medium    dynamic              5

Relay mode: auto                        Relay Delay: 90 sec.
Relay       Flame  Offs   Smoke  Motion User   Cont   Focus  Netwk
1           X
2                                          X      X      X
3                         X

Schedules:
everyday daily Minutes(600:840)

Zones:
Name          Type   Mode   Points                Sens   Schedules
mtion         motion detect 0,155 130,292         50     everyday
smk_block     smoke  block  0,180 640,480         50     none
SmokeII       smoke  block  441,26 640,480        50     none
wall          smoke  block  225,36 358,150        50     none
smoke3        smoke  block  0,8 183,141          50     none
```

Person performing inspection _____

Appendix E - Approved Fire Test Results

Fuel Source	Distance to detector	2.8 mm FOV	6 mm FOV	8 mm FOV	EX 8 mm FOV
1 ft pan of Heptane	100 ft	18	9	9	9
1 ft pan of JP-8	100 ft	18	10	10	10
1 ft pan of Ethyl Alcohol	100 ft	21	10	11	11
1 ft pan of Isopropyl Alcohol	100 ft	16	9	9	10
1 ft pan of Unleaded Gasoline	100 ft	8	8	8	9
4 min Smoke Emitter	100 ft	301	94	52	63
4 min Smoke emitter	75 ft	43	24	22	48
6 in pan of Heptane	100 ft	100	10	9	10
Cardboard boxes and paper 4 ea. 10 x 10 x 4-in. boxes	100 ft	278	83	101	97
6 in diameter pan of Heptane/toluene 75/25	28 ft	19	19	20	18
Shredded newspaper	28 ft	127	150	102	151
Smoldering wood	28 ft	3062	3279	3027	2927
Wood Crib 6 x 6 x 2.5-in.	28 ft	142	192	145	194

Known nuisance sources include: Welding, grinding, modulated light sources.

For further information on the impact of illumination, refer to Fike Document 06-774.

Revision History

Revision	Date	Revision Description
4	1/15	Company name change from AxonX to Fike Video Analytics Corporation.
5	03/19	Revised document to replace SigniFire references with Fike Video Analytics. Replaced all Fike Video Analytics IP references with FVA-IP.
6	06/19	Revised document to replace SpyderGuard references with Fike Video Analytics video management software.
7	03/20	Revised document to integrate information from six guides (06-766, 774, 776, 782, 783, 784, and 789).
8	04/20	Revised document to standardize all content and fix minor errors.

Fike®

Video Analytics Corporation

CONTACT US

Fike Video Analytics Corporation
704 SW 10th Street
Blue Springs, Missouri 64013-0610 USA
Tel: +001 844-345-3843
www.Fike.com

For a list of contact information for Fike offices around the world, visit the Global Locations section of Fike.com