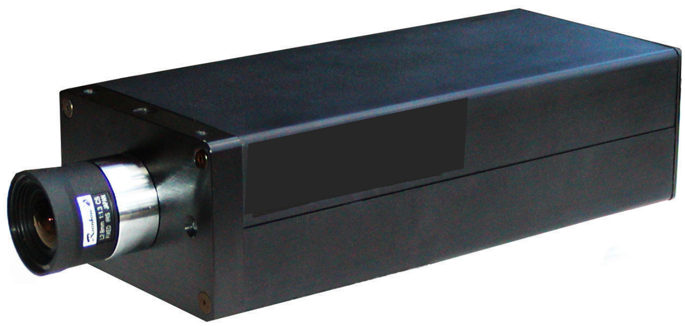
Fike Video Analytics®
IP Smoke & Fire Detection Camera



Applications Guide

P/N: 06-529
Rev: 3, 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

Introduction

This document provides a review of applicable codes and standards, design practices, system components, system commissioning and maintenance.

The move to intelligent Internet Protocol (IP) based video systems that combine the benefits of networking, digital video, and camera intelligence results in a more effective means of smoke and fire detection than has ever been available before in the fire industry. A Fike Video Analytics system provides a wide range of innovative functions and features that are only possible with Video Image Detection (VID) and IP technology.

Section 1 – Standards that Apply

Fire detection systems are governed by codes and standards to ensure safety and reliability. Video Image Detection (VID) is a supplemental system. Supplemental refers to equipment or operations not required by the code and designated as such by the Authority Having Jurisdiction (AHJ). VID systems are installed to provide early warning detection that yields a cost benefit and safety that go beyond code mandated systems that are currently installed in these facilities. Even when a supplemental fire alarm system is installed in addition to the mandatory life safety system, it should conform to local codes and be listed or approved for the purpose of the application. This section highlights some of the applicable codes and standards addressing Video Image Detection (VID).

1.1 NFPA Codes and Standards

The National Fire Protection Association (NFPA) publishes standards for the proper application, installation, and maintenance of smoke detectors. The mission of the NFPA is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. Throughout this document code requirements will be cited where applicable. A system designer should review and interpret the code for themselves to ensure conformance if required. Codes that address the implementation of VID systems are:

NFPA 72 – The National Fire Alarm Code covers the application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, fire warning equipment and emergency warning equipment, and their components. NFPA 72 2007 and later define video image smoke detection (VISD) and video image flame detection (VIFD) and provide installation, design, and maintenance guidance.

NFPA 502 – The Standard for Road Tunnels, Bridges, and Other Limited Access Highways provides fire protection and fire life safety requirements for limited access highways, road tunnels, bridges, elevated highways, depressed highways, and roadways that are located beneath air-right structures. This standard establishes minimum requirements for each of the identified facilities. This code allows for the use of VID systems as part of the smoke and fire detection method in tunnel applications.

NFPA 70 – The National Electric Code covers the installation of electrical conductors, equipment, and raceways; signaling and communications conductors, equipment, and raceways; and optical fiber cables and raceways for the following: (1) Public and private premises, including buildings, structures, mobile homes, recreational vehicles, and floating buildings (2) Yards, lots, parking lots, carnivals, and industrial substations (3) Installations of conductors and equipment that connect to the supply of electricity (4) Installations used by the electric utility, such as office buildings, warehouses, garages, machine shops, and recreational buildings, that are not an integral part of a generating plant, substation, or control center. The wiring practices in NFPA 70 apply to all detectors including VID.

1.2 Testing Laboratories

Factory Mutual (FM) Global is an international property insurance and loss-prevention engineering leader in both capacity and coverage. FM works in partnership with clients to reduce threats to their property and maintain operating reliability through property loss prevention research, engineering and comprehensive insurance products.

Authorities Having Jurisdiction (AHJ's) serving industrial and commercial companies rely on products and services that are FM Approved and specification tested to protect their properties from loss. The FM APPROVED mark, Fig 1, which is backed by scientific research and testing is a sign that the product conforms to the test standards that apply. The Fike Video Analytics IP camera is tested to two standards:

FM 3260 – Optical Flame detector standard
ANSI / UL 268 – Smoke detector for fire protection signaling systems

Figure 1 – FM approved mark

1.3 Manufacturer's Publications

Fike Video Analytics Corporation produces a number of documents that detail the use of the components needed for a video image system as well as highlight significant system traits. Literature includes user manuals, specification sheets, brochures, articles, white papers, case studies and boiler plate specifications. Many of these can be found on the Fike website (www.Fike.com) or by contacting an Fike office or a distributor directly.

Section 2 – How Video Image Detectors Work

This section is for informational purposes and is not required in order to design, install, or maintain a VID system. The section provides a brief overview of the principles of VID systems detection. Video Image Detection (VID), whether it is Video Imaging Smoke Detection (VISD) or Video Image Flame Detection (VIFD), is the application of artificial intelligence to analyze video images, also known as Machine Vision, to detect smoke and fire. The main proposition of VISD or VIFD is that if one can see fire and smoke, then one can formalize the process similar to what occurs in the human brain. The process is then put in the form of computer software, or more generally, a device that can do the same function as a human observing the space.

As stated in its name, VID systems use video images as the only source of data, applying specific computational algorithms to identify flames, and smoke though pixel changes within the images. Functionally, VID systems always consist of video imaging acquisition, processing, and notification. Early VID systems used ordinary analog CCTV cameras for image acquisition and processing was done on a computer that hosted the detection algorithms. With the advancement of specialized Digital Signal Processing (DSP) chips, a second generation of systems are capable of hosting algorithms embedded onboard the camera. Such an arrangement has major advantages such as eliminating long transmission lines, distributed intelligence, and consolidating the VID system into one low power device. Fike Video Analytics IP is a second generation VID system with a Texas Instrument processing unit embedded inside the camera enclosure. Fike Video Analytics IP uses form C dry contact relays as a means of alarm notification. In addition, Fike Video Analytics IP can provide digital IP based notification to one or more remote video monitoring workstation(s) providing guards with a first hand view of the area that caused the alarm. Video content, as well as more extensive information on the alarms is delivered to a digital video network management system using local area networks.

2.1 Video Image Analysis Challenge

VID systems, unlike more traditional detection methods, do not operate in contexts of familiar physical parameters (i.e. temperature, obscuration). Data entering a VID system represents light intensities arriving at the video camera lens from all directions within a Field Of View (FOV). A VID system knows nothing about the origins of this light, whether it’s coming directly from a radiating source, reflected from other objects, or scattered by smoke. The decision that a VID system has to make is not based on the measurement of a particular intensity coming from a particular direction, but rather by not so obvious changes of those intensities over time and their spatial relations to each other. While assumptions and ideas behind the VID systems may be expressed in simple intuitively understandable forms, precise implementation presents a challenge. For example, instructions that seem to be very simple and obvious for humans such as “look for a *cloud shape* that is growing *upwards”* are difficult to put in form of precise prescriptive algorithmic steps. As an input, Fike Video Analytics receives massive streams of real-time data. For example, the Fike Video Analytics IP camera uses images of 640 x 480 pixels that are processed at the rate of 16.7 frames per second. That amounts to over 5 million data readings (pixels) per second. Consider that processing one pixel takes approximately 500 machine instructions: it will require processing power of 2.5 billion instructions per second (2,500 MIPS) which would be unthinkable 10 years ago. VID implementations follow the evolution of the images over some period of time to analyze changes in search of specific patterns. This is why Pan Tilt and Zoom (PTZ) cameras will not work with video smoke and fire detection system. What exactly are the patterns? Flame-specific flicker and intensity of grouped together pixels, forming a region within the image may be a good indicator of open fire. However, flicker alone does not provide sufficient selectivity, so systems rely on additional hints such as color, bright static radiation and geometric configuration of the radiating source. Particular systems may rely on a more comprehensive set of characteristics combing data stream with a series of temporal DSP filters to produce transformed images with smoke and flame, producing spatial patterns that are identifiable and unique. The alternative approach is to analyze the changes in illumination and color/intensity of the images over time. Assuming that smoke makes colors attenuated, while flames make colors shifted towards yellow/red regions. In addition, some algorithms rely on loss of high frequencies in spatial Fast Fourier Transform (FFT), Fast Hadamard Transform (FHT) or Wavelet transforms over time as an artifact indicating the presence of smoke. As an example and to gain a better understanding of how VID systems detect we will look at the Fike Video Analytics flame detection.

2.2 Flame Detection

Flame in open air has certain properties that allow visual identification. There are specific physical processes that determine some of the flame features that can be observed and recognized. These physical processes are well defined in the SFPE handbook and modeled through the use of Fire Dynamic Simulator (FDS). First of all, flame has an area of intense heat where oxidation reaction takes place. The heat combined with gravity causes the upward draft of gaseous products of combustion. At some degree of intensity this draft becomes turbulent which causes the flame to flicker chaotically, constantly changing the configuration of the flame and intensity of light it radiates. Most of the VID systems for flame use flicker property as one of the criteria, combining it with other specific properties that make detection more reliable.

2.2.1 Stage 1: Preprocessing

The goal of the first step is to reduce the data flow to a manageable size. That can be done by considering only pixels that fit certain criteria with additional processing only those parts of the image reducing the pixel count. Flames are constantly changing, thus the simplest approach is to examine only pixels that undergo changes. The changes can be detected as absolute difference in brightness from one video frame to another (or time-average background) using a DSP filter. Adjacent pixels that pass the selection criteria are grouped together for future processing. A well designed first stage should leave only few cases, greatly reducing the amount of information for further processing.

2.2.2 Stage 2: Normalization

Each case is further examined to determine if it is associated with flame. Varying in size, cases usually undergo normalization so each case will be represented by a set of data entries of a standard size. Other than being a technical necessity, normalization eliminates any sensitivity dependency in VID systems to the geometric size of the flame relative to the image. Events that are too small to produce the data set of the required size are ignored. The size limit also helps determine the maximum distance to size ratio of detection. Using geometry and knowing the minimum pixel size needed for detection as well as the cameras resolution and FOV, one can calculate the minimum fire size to be detected at a given distance. For example, Fike Video Analytics' minimum detection size is 7 by 7 pixels, the processed image resolution is 640 by 480 pixels, and encompasses a 90 degree FOV. The resulting fire size at 100 feet would encompass 1.88 square feet or the area encompassed by a 1 ft pan fire.

2.2.3 Stage 3: Decision

The decision to categorize a case as flame can be based on the geometry of a pattern, color/brightness, and consistency over time. Implementations may vary in particular methods used to do the determination such as decision trees, neural networks, fuzzy logic or linear estimators. Remaining important, is that some methods use training (neural network, linear estimators) while others rely on the designers ability to define the rules that govern the decision making. Training is an operating mode where the system is presented with a large number of data samples (flames and nuisances) and provided with the correct classification of alarm state by a human trainer. Training is performed at the design stage of the system and no alteration to the neural network is done after or during installation. As a result, a well designed decision engine is able to generalize and classify correctly any arbitrary samples in the future. Rule-based systems requires a very good understanding on the part of the designer how particular elements of data relate to a decision the engine is attempting to make. Applicability of these approaches is a matter of the kind and size of input data: rule based systems are applicable when data entries are relatively small and well understood, while trained systems are better with larger sets having no clear definition on how individual entries relate to each other and to classification phenomena.

2.2.4 Case study: Flame

The discussion would be incomplete without the example of a particular implementation of a flame detection system (Fike Video Analytics) to illustrate the above-mentioned concepts. Stage 1 of the algorithm constantly transforms the original image using time-domain DSP applied to each pixel to calculate two values: static, slow changing brightness (RED) that is achieved by a lo-pass filter and dynamic flicker factor (BLUE) using a hi-pass filter. Flames on the image produced by this transformation have distinctive characteristics: red *core* and blue *corona*, Fig 2. Nuisances produce different kinds of patterns: computer screens have blue and red pixels distributed uniformly; flashing and blinking lights create circular patterns.

At Stage 2, the algorithm searches the image for the representative anomalies with high values of both RED and BLUE channels overlapping each other, extracts and scales them to a standard size of 7x7 with each entry containing RED and BLUE values.

Finally, Stage 3 uses a feed-forward neural network to recognize the pattern representative of flames. The network was pre-trained with a large number of flame (over 5,000) and nuisance (over 10,000) samples to accommodate all variations that can be encountered in real life. That includes extreme cases when flame is subject to wind which can significantly tilt the pattern sideways. Nuisances include varieties of light sources such as flashing lights, strobes, moving lights, computer monitors, reflection on aluminum foil, etc. In addition, nuisances were collected using prototypes installed in the field with intensive human or vehicle traffic. As more usable data is gathered the algorithms can be refined and uploaded to existing systems in revision cycles.

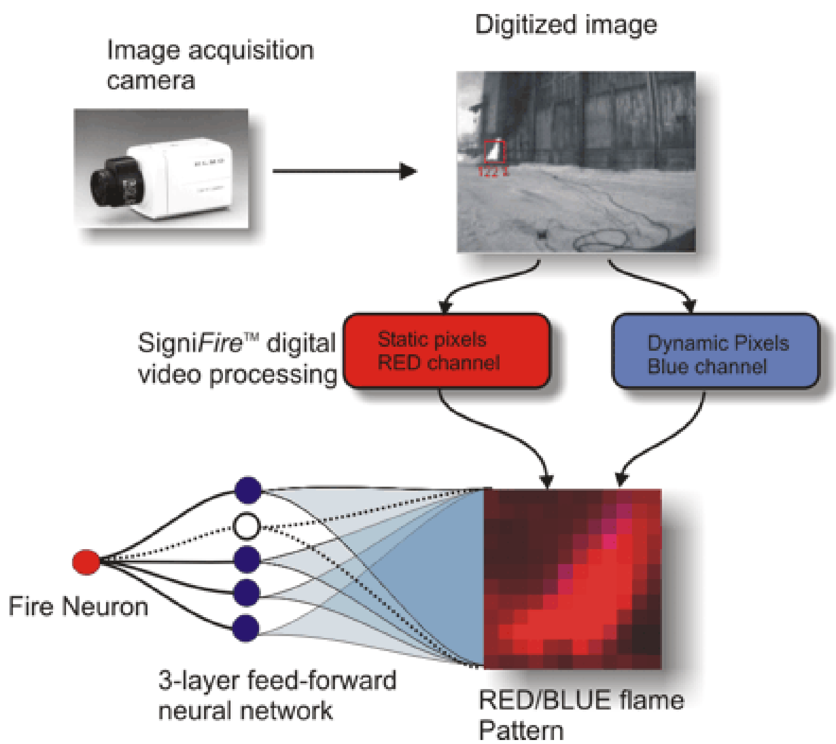


Figure 2 - DSP-based VID for flame. Video images are processed by DSP calculating two values for each pixel each assigned pretended colors. RED color is representing slow-changing brightness acquired by lo-pass filter and BLUE color representing flicker factor acquired by hi-pass filter. Method is color insensitive. Final identification can be accomplished by feed-forward neural net or any other decision making engine.

For more information of how VID systems work and standardized testing of VID systems see “Video Image Detection Systems for Fire and Smoke” by George Privalov and James A Lynch, which can be accessed on the Fike website under the “reports” tab (www.Fike.com)

Reserved for future use.

Section 3 – VID System Applications

Video image detection systems are best suited for large volume and or high asset protection. In addition, it can be implemented in areas were there is a desire to provide situational awareness and security. Because of the duel use and system flexibility a wide range of hazards, occupancies, and situations have benefited from the use of VID systems. Below are some of the applications. You can see below there is a wide range of applications for this new and unique technology. Because of its ability to cover large areas, provide video, and its early warning capability, it is an ideal tool for areas that had no solution previously. In addition to identifying the appropriate application, system implementation and layout is equally important. These systems are best when monitored and an early response can be initiated to extinguish the fire during the early growth stages.

3.1 End User Applications

Retail

Warehouses, big box stores, and distribution centers have implemented video image detection to monitor larger areas and provide early warning smoke and flame detection. These facilities are ideal for VID because of the large volume and high amount of assets per square foot. Cameras are generally placed looking over loading and unloading docks, packing areas, battery and forklift maintenance areas, high hazard areas such as aerosol rooms, and over the tops and down aisle ways.

Utilities

Coal, hydro, and nuclear plants benefit from implementing VID through early detection and situational awareness. Most fires in power plants originate at the lube oil system on large rotating turbines and generators. Early detection and video verification will limit loss of assets as well as avoid a plant shutdown. Fike Video Analytics IP cameras have been installed in turbine halls, battery rooms, tripper rooms, over nuclear fuel rod pools, and compressor stations.

Marine

Ship applications consist of installing Fike Video Analytics in generator rooms, propulsion rooms, turbine rooms, pump rooms and other general machinery spaces. VID systems have been tested by the US and Royal Navy’s and is implemented on large ships using networked systems to provide command and control with video and alarm information.

Manufacturing and Industrial

Plant fires spread quickly when combustible material is readily available. VID has been successfully installed in areas where expensive machinery that is vital to day to day operations is located and also cover entire facilities that due to the operation and environment could not be covered by conventional methods.

Education

In schools and universities arson is the single greatest cause of fires; water damage from sprinklers does the rest. With the growing implementation of cameras and mass notification in educational institutions, VID also provides value through intrusion detection and situational awareness in addition to smoke and fire detection on one system. Large corridors or open entry ways, arenas, gymnasiums, auditoriums as well as labs and libraries are suitable for VID.

Airports

The cost of an airplane hangar is minimal compared to the loss of the potential aircraft inside which may add up to hundreds of millions of dollars, plus loss of revenue due to disruption of service. VID provides early detection and the opportunity for early suppression or nuisance rejection before an expensive AFFF dump.

Museums and Cultural Properties

Priceless, irreplaceable contents are easily damaged by smoke. VID is ideal for these properties because many museums were built with high ceilings that render conventional detection ineffective. An additional benefit is utilizing motion detection algorithms to add an additional layer of protection.

Transportation

In addition to airport and marine installations mentioned above tunnels, subway and train stations benefit from the early detection and video features supplied by VID systems.

Outdoor
Applications such as car dealerships, lumber yards, construction sites, and wildland-urban interfaces can use VID to provide early warning where no other detection technology could be used.

3.2 System Benefits

A Fike Video Analytics system provides a host of benefits and advanced functionality. The advantages include remote accessibility, high image quality, event management, intelligent video capabilities, easy integration, scalability, flexibility and cost-effectiveness.

Remote Accessibility – A Fike Video Analytics system can be configured and accessed remotely enabling multiple authorized users to view live and recorded video any time and from anywhere in the world.

Image Quality – Analog camera systems deliver an NTSC signal resulting in an image that contains 320 by 240 pixels or 76,800 total pixels. The Fike Video Analytics network camera processes 640 by 480 pixels or 307,200 total pixels providing a clearer image and better performance than analog systems.

Event Management and Intelligent Video – Event management and intelligence in the form of analytics at the edge limits the potentially large amount of video information that would have to be transferred and stored within the network. For example, if the video feed were processed at the server at least 15 frames a second would have to be sent across the network. Many networks do not have the bandwidth to handle this amount of data. With processing done on the camera only enough images are transmitted over the network to provide a smooth video to the end user (~5 frames a second). Also when there is no motion within the image, the cameras throttle down to as low as 1 frame every 5 seconds. This maximizes the use of the network and storage space providing video and network capacity when it is needed. Within the video management server, video is constantly recorded so any time period from any camera can be watched. In addition, events are marked which allows them to be searched using an archive or a timeline feature within Spyder*Guard* for easy retrieval.

Scalability and Flexibility – A Fike Video Analytics system can be expanded as the user needs grow. Network based systems share the same wired or wireless network for communication so more cameras can be added without significant or costly impacts to the infrastructure. Each FSM-IP NVR can handle 32 IP cameras with Spyder*Guard* capable of handling multiple FSM-IP NVRs to allow for a completely scalable architecture.

Cost Effective – A Fike Video Analytics system has a low cost of ownership and with network infrastructure often already in place attaching Fike Video Analytics IP Network cameras onto that existing network can be an easy solution. Network cabling is less expensive than an alternative analog system. Also, IP access to the cameras allows for cost effective monitoring and storage. Maintenance is reduced by placing the cameras in easy to reach locations rather than at the ceiling level (where traditional detection is placed) that may require a lift or scaffolding. The POE capability of the cameras also helps reduce installation cost since power does not need to be run in addition to the communication lines. Because each system is a self contained detection device with lower power consumption, supplying the sometimes mandatory backup battery power is substantially reduced what compared to the older analog systems.

Section 4 – Typical System Layout

When selecting a particular VID system architecture, the designer and end user must identify the goals of the system. There are many acceptable ways to configure the system architecture. The most basic and most implemented method is the networked system in, Fig 3. This architecture uses only network cable and consists of the cameras, an NVR, and the Spyder*Guard* user interface. This architecture is used when 24 / 7 monitoring is present and personnel can respond quickly to a fire for suppression purposes. The advantage of this system architecture is that the system can be set with maximum sensitivity to provide the earliest possible warning. Another architecture possibility is to use the dry contacts to transmit an alarm to the fire alarm control panel. This is not as widely used because you limit the capabilities of the system by not using the video supplied for verification purposes (nuisance mitigation). However, combining the two architectures Fig. 4 provides an added level of protection and is suitable for installations that may not have 24 / 7 guards and want to ensure a response.

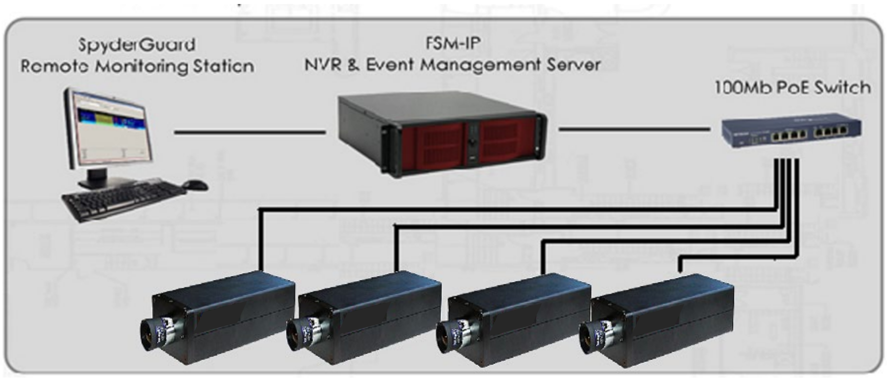


Figure 3 - Standard Network architecture.

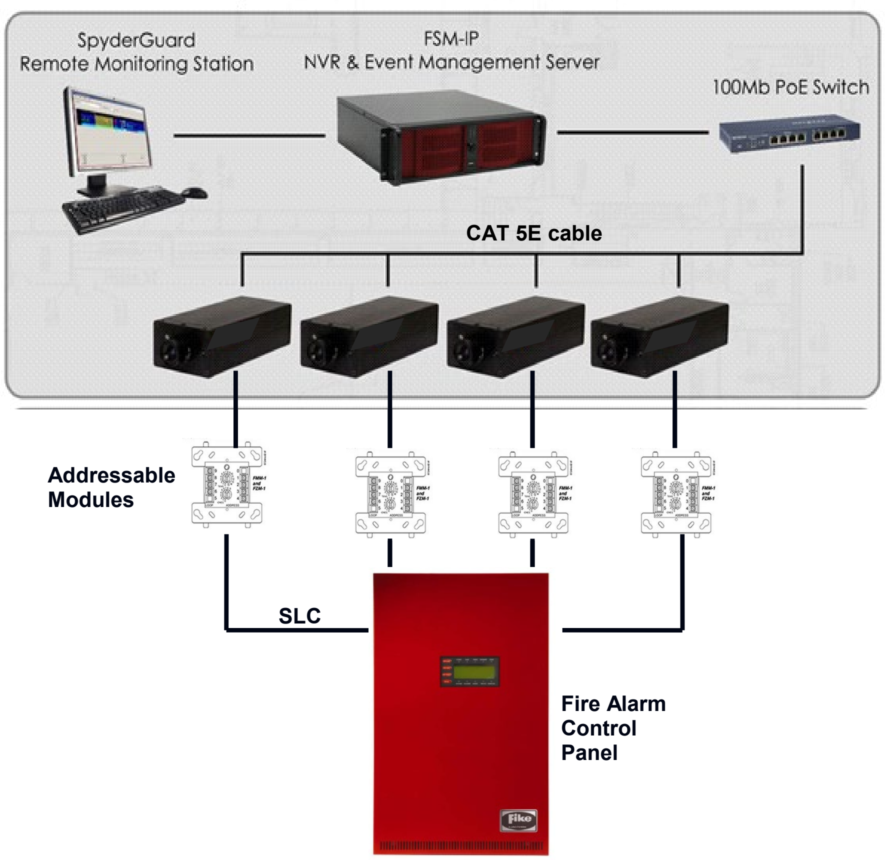


Figure 4 – Network architecture with dry contacts attached to addressable modules to the fire alarm control panel.

A Fike Video Analytics IP camera is a device that integrates a digital video camera and processing computer to detect fire, smoke, and motion. The camera includes a fixed iris, fixed field of view (FOV) lens, a CMOS imager, network interface, three internally controlled relays, and DSP-based embedded computer (Texas Instrument (TI) DM642). The DSP is used for running the video smoke fire and motion analytics, video compression, and network functionality. The software and user defined settings are stored internally in non-volatile memory so that cameras automatically start functioning once power is turned on. The Fike Video Analytics camera, being a network device is given it own IP address and connects to the network using an Ethernet plug on the rear of the camera. The camera provides a web interface for communication. In addition to sending live video, the Fike Video Analytics camera provides event data for event management and intelligent video functionality such as fire and smoke detection, motion detection, reflected fire light detection, and trouble conditions such as low light, dirty or out of focus lens, blocked image, loss of network and loss of power. Beyond the network capabilities the camera can be attached to external devices such as a fire alarm control panel (FACP) through Form C dry contacts using an addressable module, Fig 5. Contacts 1 and 2 are for power. Contact 3 through 11 are configurable Form C Dry Contacts. 6 through 8 is by default the trouble, when power is supplied the state will change and will close on loss of power, loss of network connection or a content or focus trouble. 3 through 5 and 9 through 11 are configurable and by default 3 through 5 is set to close on a fire or smoke alarm.

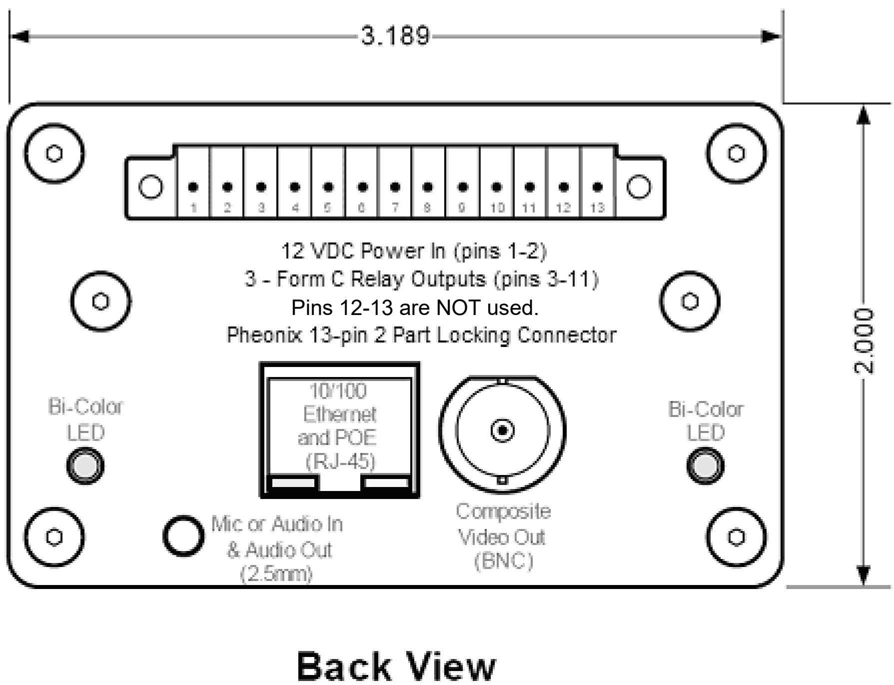


Figure 5 – Back plane view of Fike Video Analytics IP camera

4.1 Components

A Fike Video Analytics system at its most basic architecture includes an IP camera, network, video management system, and user interface. Other components can include housings and mounts, addressable modules and fire alarm control panels, and suppression systems. The following sections will detail some of the system components that may be required.

4.1.1 Housings

The Fike Video Analytics IP cameras have been environmentally tested to FM standards. The cameras are often placed in environments that are very demanding and go beyond the extremes tested by FM. If the coverage area is going to be exposed to unusual or extreme temperature, humidity, rain, corrosive substances, vibration, vandalism or air born particulate, precautions should be made to protect and clean the camera. This usually consists of installing the cameras in outdoor sealed enclosures and may even require an explosion proof housing. CCTV housings are usually made of either metal or plastic and can be fitted with heaters, blowers, wipers, chillers, air curtains and can be water tight and/or dust proof. When selecting a housing, you should consider access, mounting, cabling, temperature and other ratings, power supply and resistance to tampering. The window of an enclosure is usually made of high-quality glass or durable, polycarbonate plastic. Glass should be used in areas subject to corrosion and cameras should be positioned as close to the window as possible to limit reflections and glare from the window. A cleaning regiment may need to be executed which consists of wiping down the housing to ensure a clear FOV. Figure 6 shows various mounting options including explosion proof, outdoor and indoor mounting.

Figure 6 – Fike Video Analytics IP Camera inside explosion proof housing, outdoor housing, and an indoor IP camera mounting bracket.

4.1.2 Network/ Network Cables

A network consists of multiple devices in this case Fike Video Analytics IP cameras, FSM-IP NVRs and user interface workstations connected using network wiring. Each device is supported by network software that provides the server or client functionality. The hardware used to transmit data across the network may include copper cable or fiber optic cable. The standard cabling used is 10Base-T category 5 Ethernet cable also known as CAT5. This is twisted copper cabling which appears at the surface to look similar to TV coaxial cable. It is terminated on each end by a connector that looks much like a phone connector. When this equipment is used together to build a network within a facility it is known as a LAN. A local area network (LAN) is a group of devices that are connected together in a localized area to communicate with one another and share resources. Data is sent in the form of packets. The most common LAN technology is the Ethernet which defines a number of wiring and signaling standards and it is specified in a standard called IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting devices to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. It has been in use from around 1980 to the present, largely replacing competing LAN standards.

Ethernet uses a star topology in which the individual devices are networked with one another via active networking equipment such as switches. Physical transmission for a wired LAN involves twisted pair or fiber optics. A twisted pair cable consists of eight wires, forming 4 pairs of twisted copper wires and is used with RJ-45 plugs and sockets. The maximum length before another switch has to be installed for the twisted pair is 328 ft (100 m) while fiber optic lengths range from 6 .2 to 43.5 miles (10 km to 70 km). Data transfer rates can range from 100 Mbits/s to 10,000 Mbits/s depending on cabling. It is always a good idea use cabling with greater capacity than is required. A fast Ethernet can transfer data at a rate of 100Mbit/s. Fike Video Analytics cameras are equipped with 100BASE-TX Ethernet to support this data transfer speed. The type of twisted pair cable that supports this Ethernet is called CAT-5 Cable and can be purchased at most hardware stores or online. A Gigabit Ethernet, which can use twisted pair of fiber optic cable delivers a rate of 1,000 Mbit/s (1Gbit/s) and is quickly becoming the standard network speed. The type of twisted pair cable used to achieve the high data rate is CAT-5e or higher cable. For transmissions over longer distances, fiber cables such as 1000Base-SX transfer up to 1,639 ft (550 m) and 1000BASE-LX up to 14,900 ft (5,000 m). A 10 Gigabit Ethernet is the next step up with data rate deliveries of 10 Gbit/s (10,000 Mbits/s). It is mainly used for backbones in high end applications that require the high data rates. A high quality cable such as Cat-6a or Cat 7 is required and fiber optic cable rated for the use can transfer data up to distances of 6.2 miles (10,000 m).

4.1.3 Switches

To network multiple devices in a LAN, a network switch is required. The main function of a network switch is to forward data from one device to another on the same network. This is done efficiently by directing data from one device to another without affecting other devices on the same network. This is done using the Media Access Control (MAC) address. Each networked device including each Fike Video Analytics camera has a unique MAC address, which is made up of a series of numbers and letters produced by the manufacturer and is listed on the device product label. The switch automatically registers the MAC addresses of all the devices and when it receives data, it forwards it only to the port that is connected to a device with the appropriate destination MAC address. Switches typically indicate their performance in per port rates, indicating the maximum rates on specific ports. For example, a switch that indicates a speed of 100Mbits/s is referring to the performance of each port. A switch can handle different data rates simultaneously with rates being determined through auto negotiation between the switch port and the connected device. The highest common data rate and best transfer mode are used with data being sent and received at the same time resulting in increased performance. Switches may also come with other features such as Power over Ethernet (PoE) or Quality of Service (QoS) which controls bandwidth used by different applications.

Figure 7 – Industrial POE switch

4.1.4 Power over Ethernet (PoE)

The PoE option allows power to be supplied to devices connected to the Ethernet LAN network utilizing the same cable as the one used for data and video communication. This lowers installation cost by reducing the equipment and wiring required. PoE is widely used to power IP Phones, wireless access points and network cameras. PoE conforms to the IEEE 802.3af standard published in 2003. The standard is used for cable CAT-5 and higher and ensures that data transfer is not affected. The standard includes a method for automatically identifying if a device is PoE capable, so power will only be supplied to the port when connected to a PoE enable device. This means that the installer does not need to worry about electrical shock or shocking a non-PoE network device. The main benefit of this feature is the cost savings. The installation is simpler because power does not have to be supplied to every device, just the PoE Switch which reduces labor and material costs. Because of PoE capabilities there is no need to run a separate power line to the device. Having PoE also makes it easier to move a camera or add a camera to the system. If the PoE feature is utilized, the power supplied will often originate in a server room or server closet that is often backed up with a UPS (Uninterruptible Power Supply) allowing the system to remain operational even during a power outage. If the backup power supply is sized to last 24 hours it also fulfills an NFPA 72 requirement. Due to these benefits it is recommended that Fike Video Analytics cameras be powered with PoE whenever possible. When a switch is needed we suggest an industrial POE switch, Fig 7. These switches are rugged and their power is supplied by screw down terminals rather than plugs that can become removed over time.

According to the IEEE 802.3af standard 48VDC with a maximum wattage of 15.4 W per port is supplied. The standard also defines various performance categories for the receiving devices based on the maximum power level used measured in wattage. The classification is divided into 4 classes (0 through 3). Class 0 is the full range from 0.44W to 12.95 (15.4 after losses due to the copper twisted pair). Class 1 range is 0.44W to 3.84W, Class 2 is 3.84W to 6.49W, and Class 3 is 6.49W to 12.95W. The Fike Video Analytics camera is a Class 2 device. If POE is not used the camera can be powered by 12-24 VDC using the first two contacts on the dry contact strip in the rear of the camera, Fig 5. For redundancy the camera can be powered by 12-24 VDC and POE. If one were to fail, it will use the remaining supply.

4.1.5 Video Management System (FSM-IP NVR)

An important aspect of the Fike Video Analytics fire and smoke detection system is managing video for live viewing, recording, playback and storage. Fike Video Analytics Corporation offers a Network Video Recorder (NVR) which is a piece of hardware with pre-installed video management software know as FSM-IP. The video management system resides in the FSM-IP NVR. The rack mount computer acts as a conduit to the user interface (Spyder*Guard*) storing video and alarm data recorded continuously for up to a month or more. Each FSM-IP server can handle 32 cameras with configurable storage, swappable drives, and two Ethernet ports for connection and isolation from the rest of the network. The NVR is specifically designed for video management and is dedicated to recording and playing back network video as well as storing event data to identify specific alarm conditions associated with the stored video. The NVR allows scalability, with the user interface handling multiple NVRs to suit the end users demand.

4.2 Network Wiring

Network camera wiring differs from both fire alarm detector wiring and analog CCTV wiring. Fire alarm devices are usually connected in a loop starting and ending at the fire alarm control panel, Fig 8. These systems provide power to the devices from the panel and the devices supply a state alarm or condition. Analog CCTV systems require a coax cable run from the camera all the way back to the Digital Video Recorder (DVR) and power supply, Fig 8. These systems can supply video for recording purposes but do not have alarm capabilities. IP camera systems usually use a CAT5 cable run from the camera to the closest switch then only one run to a Network Video Recorded (NVR), Fig 8. With Fike Video Analytics IP cameras the single cable network wire supplies power and transmits data and video. There can be multiple switches in the field connected together forming a web for scalability and redundancy if needed.

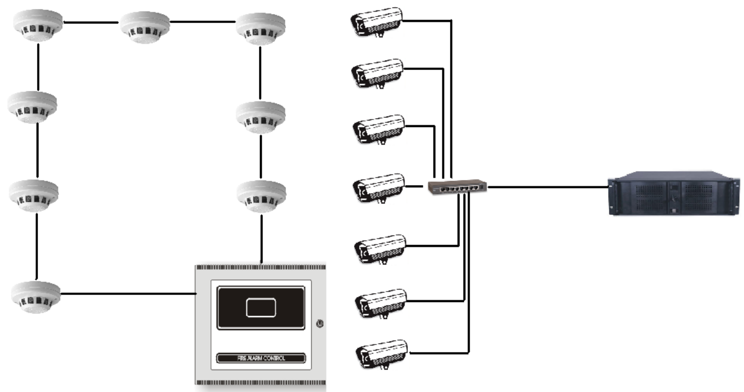


Figure 8 – Differing system wiring Fire alarm panel, analog CCTV system and IP camera system.

4.2.1 The Internet

To send information from one LAN to another LAN you must use IP addressing and the protocols for communicating over the internet. The internet is a global system of interconnected computer networks. To forward the data from one LAN to another via the internet a network router must be used. A router directs information from one network to another based on the IP addresses. The routers connect to the internet via an Internet Service Provider (ISP). The rate at which the service provider can transfer data to and from the internet is referred to as the upstream and downstream transfer speed. Upstream is the transfer rate to the internet, downstream is from the internet. To prevent unauthorized access to and from the internet and LAN firewalls are created. These firewalls can be implemented in both hardware and software. The firewalls examine the data coming and leaving the LAN and block those packets that do not meet the specified security criteria. Any device that wants to communicate with other devices via the internet must have a unique IP address. IP addresses are grouped into four blocks and each block is separated by a dot (.). Each block represents a number between 0 and 255, for example: 192.168.0.100. Certain blocks of IP addresses are for private internal use within the LAN. These blocks are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255. Devices that want to communicate over the internet need IP addresses outside this range and are allocated by an ISP. Contact your IT representative or system administrator.

4.2.2 Setting Ipv4 Address

The Fike Video Analytics IP camera is exactly like any network device and must be assigned an IP address to function on a LAN. The IP camera has two IP camera numbering methods. First the camera can be set to automatically receive an address from the server using DHCP (Dynamic Host Configuration Protocol). The second method is to manually assign a static IP number into the camera web interface along with subnet mask and the IP address of the gateway and DNS server. It is best to assign a static IP address that will remain the same for the life of the camera rather than using the DHCP option where the IP address will change over time. This is because the IP address of the camera is used to identify physical locations on the user interface and this information will be lost as the addresses changes. For more information on Fike Video Analytics Camera setting see the IP Camera Manual.

4.2.3 Network Security

If the camera system is on an existing network used for other purposes the cameras and SpyderGuard software both have password protection capabilities that can be used to limit or restrict access to unauthorized users.

4.2.4 Bandwidth and Storage Considerations

Network bandwidth and storage requirements are important considerations when designing a Fike Video Analytics system. Factors include the number of cameras, type and duration of recordings, image resolution, compression, scenery and frame rates. The amount of network bandwidth and storage space utilized will be based on the configuration of these variables.

Fike Video Analytics systems are designed to continuously record video at an image resolution of 640 by 480 using MJPEG compression. The cameras do throttle down the frame rates to send only 1 frame every 5 seconds when no motion is seen and 2 frames per second when motion is occurring, and 5 frames a second if an alarm event has been identified. The camera continuously processes around 16 frames per second at the camera. Each image streaming through the network is approximately 60 KB. At 5 frames a second for 3,600 seconds yields 1080000 KB or 1080 Mb of data per hour. For one day (24 hours) recording 5 frames per second generates ~26 GB of data per day. If you wanted to store video for 30 days you would need 778 GB or just less than 1 TB of data storage. A single FSM-IP NVR can be configured with 8 TB of storage and additional storage can be attached to the network in the form of a NAS (network area storage) or SAN (Storage area network).

Section 5 – System Design

Currently video image detection systems by code are designed using the performance-based design approach in the form of an engineering evaluation similar to optical flame detectors. This is in place of prescriptive requirements that would not be possible due to the range in system performance between different manufacturers and the variables involved in designing for proper coverage. Performance-based design is the engineering approach to fire protection design based on (1) established fire safety goals and objectives, (2) analysis of fire scenarios, and (3) quantitative assessment of design alternatives against the fire safety goals and objectives using engineering tools, methodologies, and performance criteria (SFPE, 2000). The design of a single video system will not require the extensive depth that a full building performance based design would require but the same basic methodology should be used.

Most buildings will be designed using prescriptive codes with conventional detector technologies. However, video image detection systems and the use of performance-based design offers opportunities to achieve the desired detection in areas that conventional systems do not fit due to ceiling height, aesthetics, functionality, or the desire for early detection and situational awareness in the building.

Because a full performance based design can be excessive and an exhaustive exercise, video image detectors are usually employed consistent with the approval, and detector quantity is determined based on an engineering evaluation with the intent that the detectors are positioned adequately to protect the hazard area. When conducting the engineering evaluation it is important to consider the desired performance and prevention of nuisance alarms. What should be taken into account is: predicted smoke flow, ceiling obstructions, configuration of contents, lighting, and desired fire size for 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
- Smoke output of fuel
- Fuel involved and quantity of fuel exposed
- Detector sensitivity
- Camera Field of View (FOV)
- Distance between fire and camera
- Purpose of the detection system
- Response time required
- Sources of light
- Obstructions

As mentioned above, the first step in the design of a video image detection system is to determine the fire size and potential sources to be detected. VID systems are generally installed as supplemental, early warning detection systems. They are capable of detecting fires in the smoldering and incipient stage when flaming fire sizes are small (~100 kW). Because of the capability of these systems to detect small fires in large spaces, and the end users desire to mitigate losses, these systems are usually required to detect and notify when the fire size is small so that localized suppression efforts can be made prior to sprinkler activation. As discussed earlier, VID systems rely on a pixel analysis to determine if a fire is within the cameras field of view. The Fike Video Analytics IP camera can detect a flaming fire that occupies 7 by 7 pixels on a 640 by 480 pixel image. Smoke must occupy 34 by 34 pixels. If we examine the pixel size to fire size at detection the result would be that a 100 kW pan fire (1ft by 1ft) would occupy enough pixels at 100 – 150 ft to cause an alarm. The Fike Video Analytics camera has been FM tested and approved for this distance and fire size. If the fire was to be moved 50 ft closer to the camera the system would detect a 6in pan fire (10kW) and inversely if the fire was to move to 200 ft the pan size would need to double to 2 ft (640 kW).

The ability to determine the time of smoke detection is more difficult due to many variables associated with smoke (color, obscuration, buoyancy and movement). Fire models such a FDS or CFAST or hand calculation from Principles of Smoke management by Klote and Milke or the SFPE Handbook could be used to provide smoke production rates that can then be compared to test data to provide a reasonable time of detection. Generally, if the camera coverage design is adequate to detect a flaming fire it will be adequate for smoke detection due to the fact that the visible smoke output will spread significantly faster and encompass a greater area than the flaming fire itself for most commodities.

Once the desired fire size at the time of detection has been determined, it is up to the designer to place cameras in such a way that the fire will be detected in the allotted time and the number of cameras is cost beneficial to the end user. Camera systems are three dimensional systems with the camera FOV and the starting point being at the camera and radiating outward, Fig 9. They do not need the smoke or heat from a fire to reach the detector like conventional methods (heat, ion, photo, aspiration detectors) but rather propagate/ be visible in the field of view. Smoke will travel and expand with time rapidly when compared to the movement of a flame.

Fike Video Analytics cameras are fixed network cameras which means the FOV must be fixed once it is mounted (no PTZ systems). A fixed camera system is a traditional camera type where the camera and the direction in which it is pointed are clearly visible. These cameras are sometimes installed in housings designed for indoor or outdoor installations. It is important that they remained fixed and the FOV should be checked semi annually to ensure that the coverage area has remained the same to that of the design and at system commissioning. Spyder*Guard* produces a report (see Spyder*Guard* manual) with system settings and camera images for easy comparison.

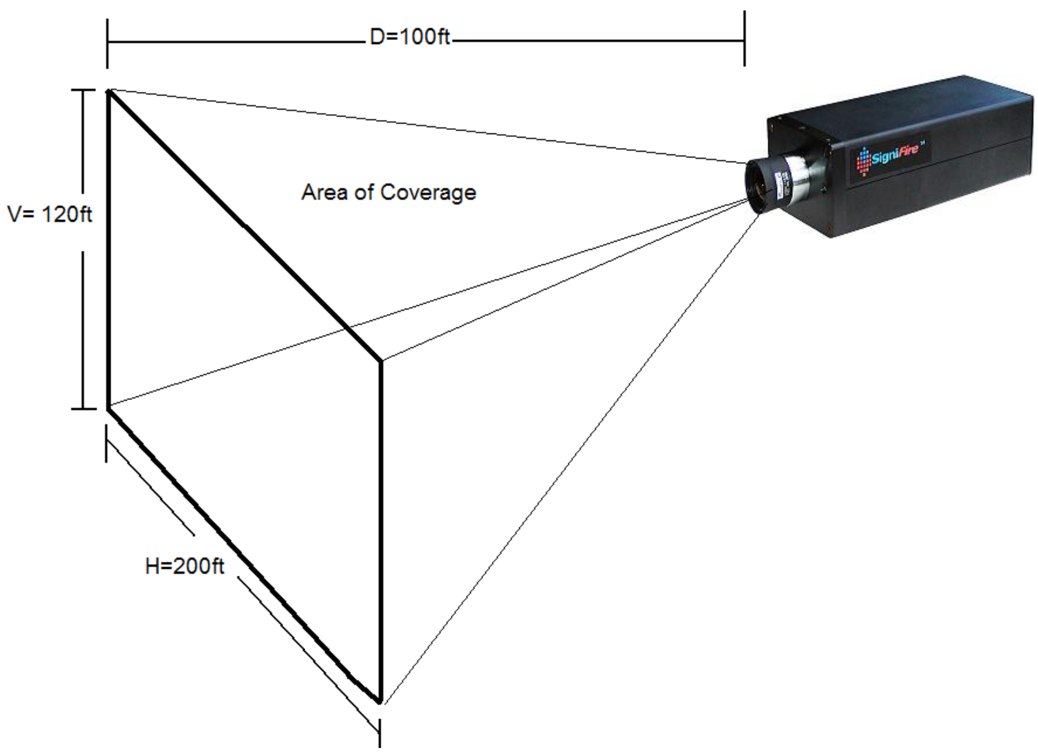


Figure 9 – Depiction of a Fike Video Analytics camera FOV radiating outward from the camera.

Being a volume detector also means that the camera does not need to be mounted at the ceiling like most conventional detectors. The cameras should be mounted above human interference (12 feet or greater) but still reachable by a ladder which allows for easy access during maintenance. Camera locations should also take into account any obstructions that could hamper detection. For very high ceiling spaces, multiple camera levels may be needed based on the desired design outcome. One can calculate the camera FOV using simple trigonometry and understand the horizontal and vertical camera coverage based on distance of the camera to the source. For example, if you had a Fike Video Analytics camera and lens that provided a 90 degree horizontal field of view and a 67 degree vertical field of view and your camera coverage (distance to anticipated source from camera) was 50 feet, your horizontal coverage would be approximately 100 feet and your vertical coverage would be about 60 feet. At 100 feet, the location of our 1 ft pan fire, the cameras horizontal coverage would expand to 200 feet and the vertical coverage would be 120 feet. These easy calculations can be used to identify, based on where a camera is placed and how high the ceiling is, when the camera coverage will begin to intersect the floor and ceiling. This assumes that the camera is perfectly horizontal so adjustments may have to be made to compensate for any angle due to downward tilt of the camera. You do not want to be looking down on a fire or smoke source rather out at it so camera tilt should be minimized You also want to cover both the floor and the ceiling as that is where fire and smoke are most likely to occur, Fig 10.

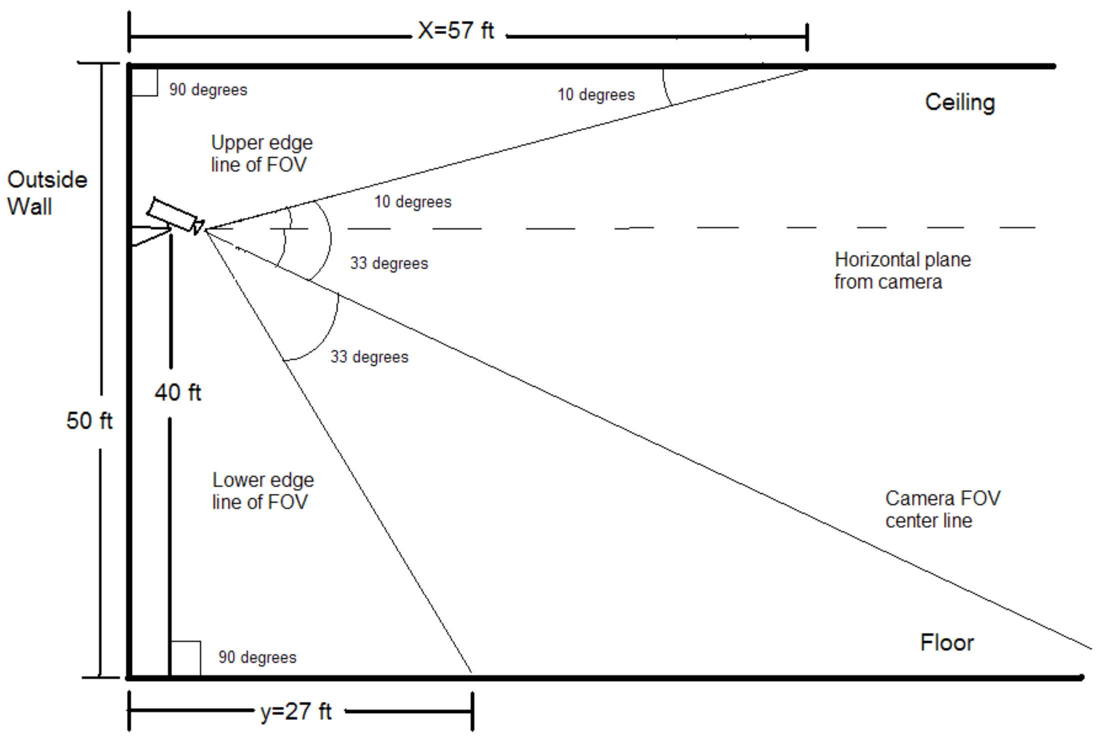


Figure 10 – Vertical camera coverage

The cone of coverage from the camera does result in a "blind" spot at the camera so systems are usually designed so that another camera will cover the blind spot by either facing two cameras opposite each other or creating a pattern were cameras overlap. General CCTV camera practices also apply. These include not pointing the camera at a light source that will saturate the imager (for example a spot light), not placing the camera behind an object that will obscure the field of view and protecting the camera from physical and environmental damage, Fig 11.

Figure 11 – bad camera placement.

5.1 Light sensitivity

A flaming fire radiates significant amounts of light, a Fike Video Analytics camera can detect this light even when the rest of the room is completely dark. However, smoke can only be detected by the effects it imposes on the residual light so detection requires illumination to function. The level of illumination required is usually measured in terms of lux or foot-candles (Fc) which corresponds to a level of illumination in which the camera will produce an acceptable image. 1 foot-candle is equivalent to 10.76391 lux. Normally 200 lux or 19 Fc is needed to illuminate an object so that a good quality image can be obtained. Generally, the more light present the better the image. With too little light, focusing can be difficult and the image will begin to get dark and noisy. The camera has been tested to 1 Fc (10.76 lux) detecting the UL 268 smoke room tests and is FM approved for 4.8 Fc (51.7 lux). Some camera systems are designed to work with no visible light. They use IR illumination and IR sensitive cameras to detect smoke. This method of detection conflicts with the ability to detect flame, as a flame contains very high IR illumination and has a tendency to blind IR-sensitive cameras. Any VID system design should take lighting into consideration and many locations have varying illumination, with both shadows and high light areas that give different levels of illumination. It is important to take multiple readings with a light meter, averaging the readings to provide an overall light condition for the whole area. Light measurements are taken using a light meter at floor level. The following is a chart with illumination levels under various conditions.

Illuminance	Foot-candles	Example
0.27 lux	0.025 Fc	Full moon on a clear night[1,2]
1 lux	0.093 Fc	Full moon overhead at tropical latitudes[3]
3.4 lux	0.32 Fc	Dark limit of civil twilight under a clear sky[4]
10.7 lux	1 Fc	Emergency Light Level (NFPA)
50 lux	4.7 Fc	Family living room[5]
80 lux	7.5 Fc	Hallway/toilet[6]
100 lux	9.3 Fc	Very dark overcast day[1]
320 lux	30.0 Fc	Recommended office lighting (Australia)[7]
400 lux	37.4 Fc	Sunrise or sunset on a clear day. Well-lit office area.
500 lux	46.7 Fc	Lighting level for an office according to the European law UNI EN 12464.
1,000 lux	93.5 Fc	Overcast day[1]; typical TV studio lighting
10,000–25,000 lux	935 – 2,336 Fc	Full daylight (not direct sun)[1]
32,000–130,000 lux	2990 – 12,150 Fc	Direct sunlight

1. Paul Schlyter, Radiometry and photometry in astronomy FAQ (2006)
2. "Petzl reference system for lighting performance" . http://en.petzl.com/petzl/frontoffice/Lampes/static/referentiel/present_referentiel_en.jsp. Retrieved on 2007-04-24.
3. Bunning, Erwin; and Moser, Ilse (April 1969). "Interference of moonlight with the photoperiodic measurement of time by plants, and their adaptive reaction". *Proceedings of the National Academy of Sciences of the United States of America* **62** (4): 1018–1022. doi:10.1073/pnas.62.4.1018. PMID 16591742. http://www.pnas.org/cgi/reprint/62/4/1018. Retrieved on 2006-11-10.
4. "Electro-Optics Handbook" (pdf). *burle.com*. p. 63. http://www.burle.com/cgi-bin/byteserver.pl/pdf/Electro_Optics.pdf.
5. Pears, Alan (June, 1998), "Chapter 7: Appliance technologies and scope for emission reduction" (PDF), *Strategic Study of Household Energy and Greenhouse Issues*, Australian Greenhouse Office, p. 61, http://www.energyrating.gov.au/library/pubs/pears-ago1998.pdf, retrieved on 2008-06-26.
6. Australian Greenhouse Office (May, 2005), "Chapter 5: Assessing lighting savings" ([*dead link*] – Scholar search), *Working Energy Resource and training kit: Lighting*, http://www.greenhouse.gov.au/lgmodules/wep/lights/training/training9.html, retrieved on 2007-03-13.
7. "How to use a lux meter (Australian recommendation)". http://www.energy-toolbox.vic.gov.au/energy_toolbox/summer_push/how_to_use_a_lux_meter.html.

5.2 Lenses

A lens performs three main functions:

1) Defines the Field Of View (FOV), how much of a scene and level of detail are captured.
2) Defines the amount of light passing through to the image sensor so that an image is properly exposed.
3) Focuses the image by adjusting the elements within the lens assembly or the distance between the lens and the image sensor.

Fike Video Analytics cameras come with a choice of four lenses. Three of the lenses are FM approved fixed field of view, fixed iris lenses. The purpose of the camera is to detect fire and smoke so fixed field of view and fixed iris lenses were chosen to optimize the performance and provide ease of installation. An end user or installer is only required to focus the camera and does not have to attempt to set the FOV or iris for detection purposes. The lenses come in sizes of 2.8 mm, 6.0 mm and 8.0 mm which corresponds to a FOV of approximately 82, 44 and 34 degrees respectively, Fig 12. The fourth lens is for non FM special circumstances that require a specific field of view or telescopic capabilities.

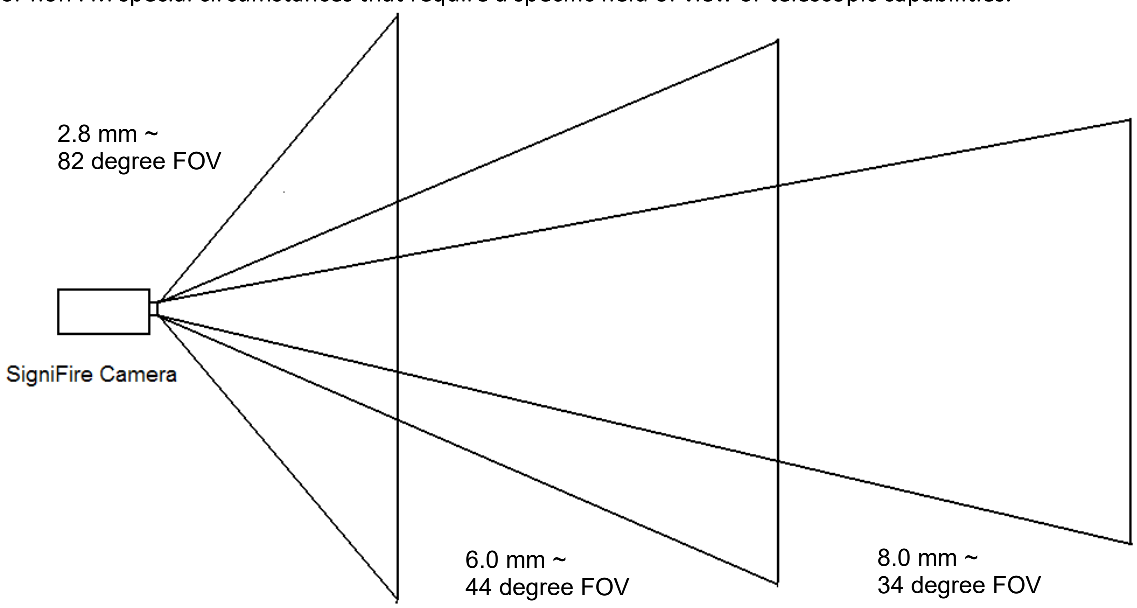


Figure 12 – Horizontal camera coverage

5.3 Installing a Fike Video Analytics System

Once a VID system application has been designed and all equipment purchased it is time to install the system. Not every aspect of the system can be thought through at the design stage so installation should proceed in accordance to the guidelines to assure proper function of the system. Below are recommendations on how to achieve the best performance, based on camera positioning and environmental considerations.

Camera objective – The aim is to get an image of the area of interest in order to detect smoke and or fire. Make sure that the design location meets the goals of these objectives once the camera is physically installed. A camera mounted looking at a small area such as a door way or cash register will not see and identify the progression of smoke or build up of fire outside the FOV. Over looking small areas and trying to use the camera for license plate or face recognition conflict with the goal of the camera.

Add light if needed – It is normally easy and cost-effective to add lighting indoors to provide the necessary light conditions for capturing good images.

Avoid direct sunlight and large contrasts in lighting – The Fike Video Analytics camera contains a IR filter so this is not as significant a problem as in other cameras but in general you want to avoid creating areas of intense light (spot light) that will create contrast between two areas of the image or backlight an object. It is best if the area protected is uniformly lit.

Section 6 – Commissioning and Trouble shooting of system

The purpose of this section is to outline the steps taken to reduce nuisance alarms during the commissioning of a Fike Video Analytics system. A properly installed system should have a trial run period of at least one week to accumulate nuisance event data with the goal of further eliminating those alarms in the future. At the conclusion of the week the cameras will be given zones, delays, sensitivities, and schedules. This information along with the events used should be recorded and kept for later analysis, if necessary. This process is then repeated until all nuisance alarms are eliminated. Commissioning tests can then be conducted to ensure that the system will identify the desired fire size. For more information on setting zones, delays, sensitivities, and schedules see the Spyder*Guard* and Fike Video Analytics IP camera manuals.

When camera commissioning begins generally the questions to be addressed are: What is the system architecture (ie. tied to a fire panel, guard interface) and what is the resulting acceptable number of nuisance alarms? The acceptable number of events will be based on the system as a whole, and the design objectives, while this methodology will work on a camera by camera basis. To identify or even accept a nuisance alarm based on only a week of data is very unlikely. So for the purposes of this outline we will assume a goal of zero events. The camera variables to be configured are;

Zones – This process will look at blocking zones opposed to detecting zones which maybe necessary.

Schedules – This process will look at daily schedules and identify the day of the week, specifically weekends.

Sensitivities – This process will look at High, Medium, Low, and Off

Alarm delay – This process will look at delays up to 30 seconds for fire and 60 seconds for smoke.

The first step is to examine all events for a week noting the information in a file. For each event a record of the;

event type (fire, smoke, offsite)
event location
duration (seconds) and
time of day (24:00:00) should be kept.

The events are then sorted and trends are identified so a mitigation strategy can be deployed. A diagram of the overall process is contained in Figure 13 and discussed below in further detail.

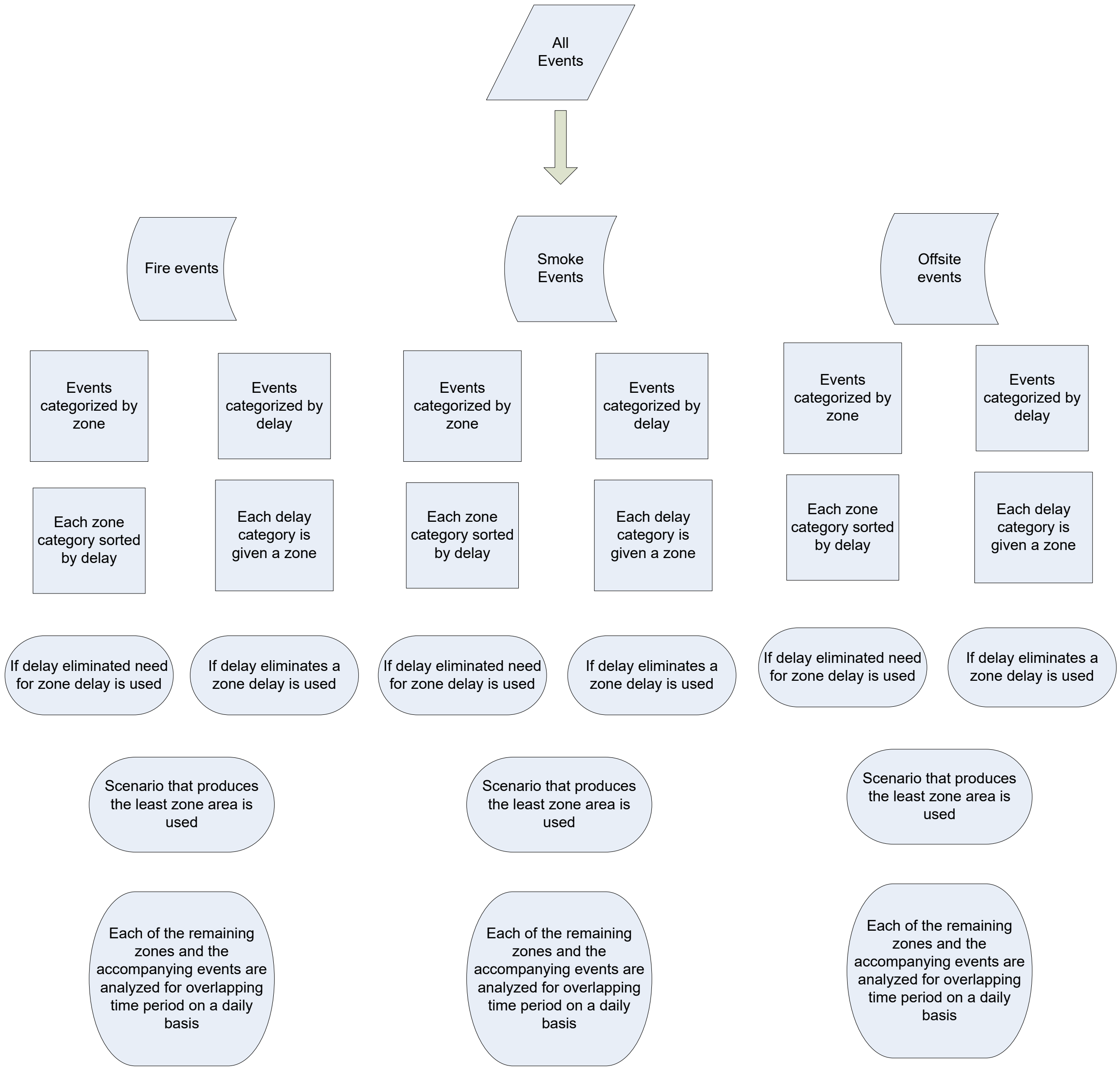


Figure 13 – Diagram of commissioning process

The second step in the process is to sort all the alarms by event type so the analysis can be conducted on an event type basis. Each algorithm (fire, smoke, offsite) is independent of the other therefore zones, delays, and schedules are also independent and set for each detection method.

Each series of events is then run through two branches that identify a zone and a delay that would mitigate that event. During this process it is important to identify what events are affected by a given delay or zone in each branch. Specifically it is important to be able to identify all events within a given zone so a schedule can potentially be made. When the final zones and delays are set all events will be able to be filed under either a delay or a zone.

Branch 1 organizes all the events into zones based on event location specifically overlapping event areas. This may result in many separated zones, large overlapping zones, or one large zone depending on the number and scattering of events.

For example purposes, after the collection of events you may have a small singular event (Fig 14) resulting in one small zone, a large singular event (Fig 15) resulting in one large zone, small individualized events (Fig 16) resulting in many small zones, strings of connected events (Fig 17) resulting in a few zones that cover the overlapping individualized strings, many individual events connected by one large event (Fig 18) resulting in one large zone, two large events that slightly overlap resulting in two large zones (Fig 19), a small event overlapping a large event resulting in either two zones or one large zone, or a combination of scenarios.

Fig 14 – Singular event small

Fig 15 – Singular event large

Fig 16 – Many small singular events

Fig 17 – Many small events strung together

Fig 18 – Many small singular event connected by large event

Fig 19 – two large event slightly overlapping

A single small event results in a single zone
A single large event results in a single large zone
Scattered single small events non overlapping results in scattered single zones
Overlapping small single events results in one zone encompassing all overlapping events
Single small scattered events connected by large event results in one large zone
Two large events that overlap by less than 50% results in two separate zones
A large event that overlaps a small event by less than 25% results in two separate zones

Each zone is then identified with a delay that corresponds to the duration of the longest event within that zone. If the delay is below 30 seconds the zone can be eliminated and the delay time is used to block the events that would cause a need for the zone. The delay on each zone is determined by the longest alarm duration for an event within the given zone. The delay is not to exceed 30 seconds (user configurable). For example a zone area is comprised of three events, event 1 is 75 seconds, event 2 is 5 seconds, and event 3 is 23 seconds. The delay is 75 seconds. The delay is unusable because it is greater than 30 seconds so the zone remains. If each event created its own zone a delay of 23 seconds would be used eliminating the need for zone 2 and zone 3. Zone 1 would remain.

When Branch 1 is complete you have a set of zones and a delay for a given event type. However, a second Branch that identifies and categorizes all events by duration is needed.

Branch 2 would categorize all events of a given type by duration in 5 second intervals 0-5, 2-10, 10-15, 15-20, 20-25, 25-30 and 30+. Each interval would then be given a zone encompassing all events with in the interval. The zones could then be eliminated by time interval until the zone area is equal to or below the zone area identified in Branch 1 or the 30 second interval is reached.

The two branches are needed to identify separate cases that could exist. Branch 1 emphasizes the zones, limiting and therefore lowering the delay time needed. Branch 2 emphasizes the delay potentially creating smaller zones. Fig 20 and 21 demonstrate a scenario where Branch 2 would be more applicable than Branch 1 and vice versa.

Fig 20 – Two 60 second events connected by a string of four 15 second events. Branch 1 results in a single zone (Green) encompassing all events with no delay. Branch 2 results in two smaller zones (light blue) encompassing the 60 events with the string of 15 seconds events eliminated due to a 15 second delay. The zone area of Branch 2 is smaller so that is the chosen solution.

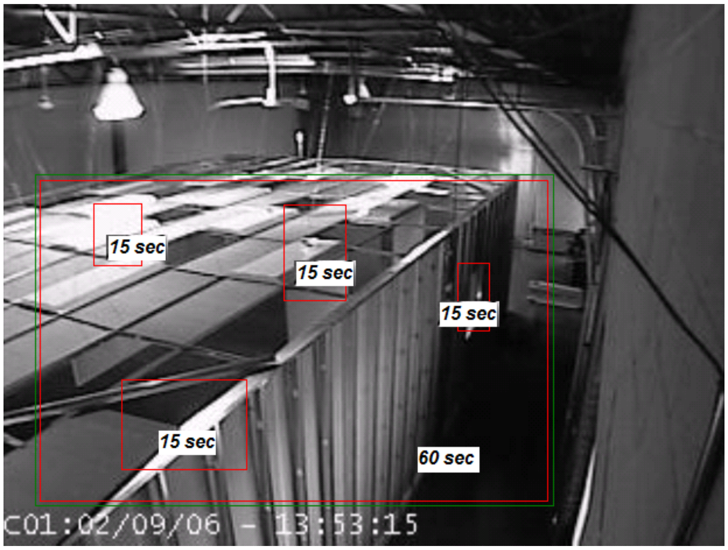


Fig 21 – Four smaller 15 second events encompassed in a larger 60 second event. The resulting zone area of both branches is the same however Branch 2 would have an unnecessary 15 second delay.

Once Branch 1 and Branch 2 are complete each branch will result in a zone area and delay for the event type. If Branch 1's zone area is equal to or less than Branch 2, Branch 1 results are taken. Otherwise the results from Branch 2 are taken.

Now that the zone and delays have been identified it is advantageous to identify if any of the zones can be placed on a schedule. All events eliminated by a delay should be removed from this analysis and all events should be organized by what zone they are encompassed within. Only zones with a minimum of 2 events can be included in this analysis. For each zone the events can be sorted by time of day and duration. If there is an obvious connection between events and time of day or day of week then a schedule can be attached to the zone. Zone and schedule combinations that are used to mitigate alarms caused by sunset and sunrise should allow for seasonal changes. For example in Washington DC the sunrise can vary by 3 hours and 25 minutes and the sunset by 3 hours and 32 minutes. Consulting a sunrise sunset table and catering the schedule to the time of year and location on the planet will ensure that seasonal changes do not affect these zones.

The final step in the process would be to identify if a lower sensitivity is needed. This would be due to over zoning the image resulting in poor detection capabilities. Identifying a change in sensitivity is done by conducting commissioning tests and ones engineering judgment in the form of a sanity check. You should ask yourself, if a fire started in the hazard area would the spread of smoke or flames result in an alarm that would meet the goals of the system implementation? If the answer is "no" a lower sensitivity should be used and zoning, delays, and schedules should be identified using data collected at the new lower sensitivity level.

This commissioning process should be done by someone who is familiar with a Fike Video Analytics system, has been trained on the equipment, and understands the limitations. Understanding how the zones function and the zone size and placement in relation to smoke and fire spread will provide the installer with the fundamentals needed to identify if the zone scheme is adequate. Fire zones should remain small or at the very least it should be understood that a fire will have to grow beyond the fire zone boundaries before being detected. Smoke zones on the other hand can be large and encompass large areas as well as overlap. One commonly used zoning scheme is to create a large smoke zone covering the bottom of the image and a smaller zone covering the top of the image meeting in the middle. This turns the three dimensional FOV into a plane looking for smoke to break the plane as if hundreds of beam detectors had been place side by side. Two additional zones can be added and placed running vertically. This further limits the FOV to a point turning the camera for all practical purposes into a beam detector.

Reserved for future use.

Section 7 – Testing, Maintenance and Service of Detectors

7.1 NFPA Chapter 10 recommendations

NFPA section 10.4.3 dictates that video image smoke and flame detectors shall be inspected, tested, and maintained in accordance with the manufacturers published instructions. Fike as the manufacturer of the Fike Video Analytics 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 and include a physical check of the cameras and a commissioning report confirmation. However, camera(s) and associated equipment that is inaccessible for safety considerations (e.g. continuous process operations, energized electrical equipment, radiation, and excessive height) can forgo the physical inspection until scheduled shutdowns, if approved by the authority having jurisdiction. These extended intervals shall not exceed 24 months.

The inspection should ensure no obstructions are between the detector and protected area, that lenses are clear and free of contaminants, that the cameras do not have mechanical damage, and that the unit is directed toward the intended hazard. The cameras field of view (FOV) should be checked to ensure that it matches the Spyder*Guard* generated audit report and that the cameras have not been moved or misaligned. Everything but physical damage to the camera can be checked by comparing the audit report generated on the day of commissioning to an audit report generated on the day of inspection. The two reports should be identical. Obstructions within 3 meters of the camera that obstruct the line of site 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 (Spyder*Guard*) can be checked for clarity to ensure that a build up of dust, grease or other debris has not obscured the lens. Images produced from the audit report (see Spyder*Guard* 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 camera state of alarm, processing and communication (see IP camera user manual)

7.3 Testing

Testing should be done at commissioning and system checks on a semi-annually basis. Testing can be broken down into two sections; functional and operational conformance. Tests are performed by Fike as part of the Quality Control (QC) process. All Fike Video Analytics 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 can be visually inspected for operational conformance. This is done by observing the user interface video stream and the front face plate 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. 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. The Fike Video Analytics IP based system should only be applied in ways that conform to our manufacturers’ recommendations.

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

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

The Fike Video Analytics 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 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 second stage is digital. The implication of this division is very important for how one will address the conformance testing mainly because 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 a fault condition and reported accordingly.

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 to the cameras field of view is 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 being 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 dry-contacts and a loss of signal to the user interface resulting in a fault event.

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)
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. The system will respond by reporting a fault in approx 30 sec.

7.4.2 Communication failure / Analytics failure

Such conditions can be achieved by disconnecting the camera from the network switch. The fault relay will close immediately and Spyder*Guard* 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.

7.4.3.1 Simulated response motion

The first method is to temporarily introduce a motion detection zone and configure the relays to close on 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.

7.4.3.2 Simulated response user alarm

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.

7.4.3.3 Simulated response live fires

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 soot flames (Isopropyl alcohol or heptane) or a properly configure plumbers 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.

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 is 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 24 months. The Fike Video Analytics 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 and security protection.

7.5.1 Maintenance records

Maintenance records should be kept on each detector and stored in a log book. 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 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.

7.5.2 Maintenance Procedures

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 Spyder*Guard* to ensure 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 as follows:

> 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 measure 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 properly function.

Out-of-Focus – The cameras 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 measure to ensure that it does not occur again or/and re-align the camera so 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 does 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 (Spyder*Guard*) 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 with clean water and dry with a clean cloth.

Ensure that the camera still has a clear line of site to the hazard area and compare the previous 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 the disabled automatic systems and inform all appropriate personnel that you now have completed the maintenance and that the system is back on line.

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

Revision History

Revision	Date	Revision Description
2	06/19	Revised document to replace SigniFire references with Fike Video Analytics. Replaced all Fike Video Analytics IP references with FVA-IP.

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