CHeKT
Intelligent Visual Monitoring

Visual Monitoring
INSTALLATION - *Best Practices*

Introduction

For decades, central station operators have responded to potentially critical events without the ability to see or understand what exactly is happening at the protected premises. The CHeKT solution allows an installing company to install a security system the same way it has for years; and, when needed, can pair an intrusion detector and camera together to provide video to the operator of whatever caused the alarm to occur. This solution allows an operator to respond quickly and accurately when a signal is received in a central station. This solution is also flexible and can scale into large visual monitoring opportunities for your company. From small commercial and residential to large commercial and industrial, this solution has you covered. This technology allows you to go into new or existing infrastructure and pair the intrusion system and video system into a single, powerful solution. Using the same cameras and alarm systems you have deployed for years, CHeKT seamlessly ties everything together into a single solution. This *Installation-Best Practices* document will provide suggestions on how to deploy comprehensive video systems to transform your business.

Visually monitored systems that are installed and monitored following the *Installation-Best Practices* in this document are capable of obtaining a much higher apprehension rate. When visual evidence is provided to the responding agency, they tend to respond much faster. The principles described in this document are to provide an understanding of the integrity and effectiveness of a visually monitored system, as well as explain how to best design a visually monitored system so that it meets the client's expectations. As the central station operator depends on the surveillance system to respond correctly, it is important to understand that the system must always be maintained in all environments.

When a detector (intrusion sensor or analytics) senses a change in the environment, (intrusion sensor or analytics) video is transmitted to and displayed at a central station, where it is presented to the central station operator. Prior to contacting emergency contacts or law enforcement, central station operators view these images for a period of time to confirm the exact details of the situation. Under normal circumstances, an emergency response is only requested by the central station if there is both positive video evidence of unauthorized access to the secure area and of actual criminal intent.

Scope

The purpose of this document is to provide installation best practices for deploying the CHeKT visual monitoring solution. This document will provide recommendations for the design, installation, commissioning, maintenance, operation, and central station monitoring of detector activated and analytic surveillance systems. This document will also include information about the CHeKT monitoring portal, which allows users to leverage cameras with edge-based analytics and AI. When analytics are active, the CHeKT portal will send signals into a central station just like an alarm panel. (Signals are transmitted from the CHeKT cloud to the central station in Contact ID format.) These principles apply to all systems that are visually monitored. This document will provide recommendations to security companies for the design, installation, commissioning, maintenance, and operation of detector-activated and edge-based analytic activated surveillance systems.

Contents

Site Light Levels

Secure Site or Area/Unsecure Site or Area/Dual Site

System Proposal

System Equipment & Configuration

Arming and Disarming the Site

Audio or Talk-Down Functionality

Relay Control

Cabling Recommendations

Walk Test

Post-Installation

System Maintenance

Legal Concerns

Terms and Definitions

Activation
An intrusion system utilizing CHeKT triggers an event resulting in the transmission of video to the central station.

Alarm/with Video
Positive evidence in the delivered video that there is an unauthorized access to the protected premises of actual criminal activity requiring a response from the central station.

Alternative Power Source
Additional power may be required to provide needed power to both the Bridge hardware and possibly the surveillance system.

Arming & Disarming
The Bridge is commonly armed and disarmed with an alarm panel's voltage output. When the Bridge is in a disarmed state, it will not send video clips unless the zone on the Bridge is programmed as a 24-hour zone.

Avoidable Alarm Activation
An event that could have been avoided; generally, a result of user error, poor system design, etc.

Central Station
A location where concurrent alarm signals and video events are received, processed and responded to by the operator.

Central Station Operator
A person located in the central station who is trained and authorized to monitor security systems.

Control Equipment
In this document, this term pertains to the intrusion equipment, as well as the visual monitoring equipment and surveillance equipment.

Data
Information provided by the surveillance systems, including alarm signal, video clips, audio talk down, and other associated information concerning the intrusion.

Dealer Portal
The CHeKT portal that allows for the setup, configuration, supervision and remote management of the Bridge and connected devices.

Design Document
A document that details the system design for present and future use of the surveillance system.

Detector
Intrusion sensors or camera analytics that detects a change in the in the environment causing the system to initiate.

Dual Site
Some protected premises may contain areas that are considered both secure and unsecured. Noting these areas during the initial installation is vital as it allows the supervising station personnel how to properly respond in each area.

End-User
The person or organization using the visual monitoring services and has the authority to utilize the system at the protected premises.

Event
Activity within a secure area after the system is armed.

False Positive
An activation where there is not positive evidence in the delivered video of unauthorized access to the protected property or of an actual crime in progress.

Fault
A condition that exists when an interruption in one or more components or connections could prevent the intrusion system or video system from operating normally.

Illumination
Infrared illumination visible to the camera.

Terms and Definitions

Integrator
Company that provides installation and/or servicing of the visually monitored site.

Isolation
A device status threat prevents the detector from operating alarm activity. The device will remain in this status until the detector is restored, replaced, or repaired.

Monitoring Portal
The monitoring portal is primarily used by the operator at the central station to provide the subscribed service but can also be accessed by installing and/or service companies to ensure that the system is functioning properly.

Omission
A detector or camera status which prevents an alarm activity from occurring. The device will remain in this status until the detector is restored, replaced, or repaired.

Overlay
The CHeKT dealer portal allows the installer to overlay the detection pattern of the detector with the associated camera. This assists the operator to better understand where the detector is located when an alarm occurs.

Power Supply
A device that provides, modifies, and isolates power for the Bridge and/or video system.

Primary Power Source
A power source used to provide power to systems under normal working conditions.

Receiver
A device that receives data from wireless sensors.

Remote Connection
The CHeKT dealer portal allows dealers to remotely connect to the web interface of connected cameras, allowing for remote configuration of network appliances.

CHeKT Site Map
Downloading a Google Image of the property and placing it in the CHeKT dealer portal allows the installer to place cameras directly on top of the map. This functionality will provide the operator a better understanding of the protected premises and camera locations.

Secure Site or Area
An area at the protected premises in which unauthorized access is intended to be detected. A secure site or area should have walls, fencing, or a natural barrier that should prevent persons from accessing that area without effort.

Surveillance System
A system consisting of camera equipment, recorder, detectors, display monitor and associated surveillance equipment.

Tamper
A deliberate attempt to defeat the intrusion system, surveillance system, or video monitoring equipment.

Uninterruptable Power Supply
Equipment designed to maintain power for a specific period of time if the primary power source is interrupted.

Unsecured Site
A site or specific area at a site not entirely enclosed on all sides and allows individuals unrestricted access to the property.

Visual Monitoring
General Principles

When providing visual monitoring with intrusion detection indoors, ensure that a camera overlooks the entire detection pattern of the motion detector, glass break detector, panic door contact, etc.(Example A)

Note: Indoor visually monitored systems will not increase signal traffic into the monitoring station. Design your intrusion system as you would normally. Ensure that cameras used for video monitoring can see the entire detection pattern of the detector or multiple detectors.

When providing visual monitoring outdoors, position the proper number of cameras so that an operator can understand what is happening around the entire property and is able to assess the threat level. (Example B)

Note: Visually monitored systems with exterior detection warrant a higher cost for both the installation and the monthly recurring fee. Visually monitored systems can provide a much higher level of service because potential intruders can be detected before a crime occurs.

Note: Because the outdoors is an uncontrolled environment, detection is generally set up as a silent zone. Text-to-speech talk-down or an operator-controlled siren (using the on-board relay) can be activated while the operator views the site.

When using an intrusion system to arm and disarm a visually monitored system with outdoor detection, it is also important to clearly understand how the user will enter and exit the protected premises. It is recommended that the user do not enter through a detector to access the system. This potentially generates unwanted alarms each time the end user enters the property. (It is recommended that a camera be placed overlooking the area where a user will enter the property.)

Note: When using exterior detection, it is recommended that the end user clearly understand how to enter the property without activating an alarm. Alternatively, the end user may access the intrusion system using the alarm manufacturer's mobile application to arm and disarm the system before entering and exiting the property.
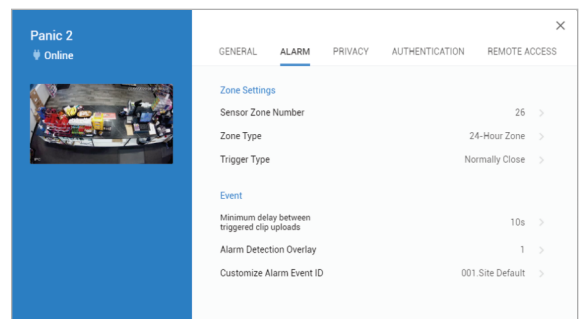
Overlap Interior Detection/Camera Patterns

Critical Exterior Camera Placement

Note: The Visual Verification Bridge can be configured to delay the alarm signal to the central station to allow the end user to enter the property without an alarm activation. This should be understood clearly by the installing company and by the end-user.

Dealer Portal Camera/Zone Settings

Once installation is completed, document the camera's correct field of view. Changing a camera's field of view after the initial installation may prevent the operator from seeing the detector's detection pattern at a later time. When possible, cameras should focus on the secure areas at the protected property. Cameras facing a public area can cause confusion and possible delay in the central station; or create an unwanted response. (Remember, the operator has never been to the site. His or her ability to understand the site is based on your system design.)

Visual Monitoring
General Principles

It should be understood by the client that, while video monitoring generally provides monitoring and detecting, it is generally unable to recognize and identify a person on the protected premise. Although the possibility of identifying a person with this equipment exists, it is unlikely; and this should be understood clearly by the installing company, central station, and end-user.

Video viewed by the central station at night can be difficult to view. Poor quality images may result from poor camera choice, dust on the lens, inclement weather conditions, spiderwebs, and poor lighting. Understanding these limitations is important during system design and installation.

Areas where detectors are installed or video analytics are utilized should have proper lighting or illumination. An operator must have the ability to accurately determine if there is a human present when an alarm is activated. Placement of detectors outside the camera's illuminated range or in poorly lit areas may cause uncertainty in the operator's response.

When infrared illumination is used, understand that the ability for the operator to provide an accurate description of the person is greatly diminished. Infrared illumination may create an environment in which an operator detects a person, but may not be able to accurately describe that person. This may lead to inaccurate or inadequate information communicated to the end-user or responding agency. *(See Thermal Detection pg.10,11)*

After the initial installation is completed, if significant changes are made to the system, those changes should be understood and notated by the installing company, central station, and end-user.

Trouble conditions, such as power outages or camera disconnects, can prevent the central station operator from seeing the video feed. Understanding trouble signals and conditions from the site where visual-monitoring is performed is vital to ensures the operator that the trouble conditions are restored.

CAM 1

Insufficient lighting

CAM 6

Dust, spiderwebs, etc.

Inclement weather

West Perimeter
CAM 4

East Lot
CAM 12

Thermal images

Visual Monitoring
General Principles

To assist in managing these trouble conditions, the Bridge hardware and CHeKT cloud will monitor the video stream of all connected cameras. If a camera is disconnected, after a pre-programmed amount of time expires, a "camera disconnect" signal will be sent to the central station. It is important to understand how the end-user would like the central station to respond to these trouble signals if they occur. If a disconnected camera is paired with an intrusion detector, the detector will continue to create the alarm signal, but video will not be accessible to the operator.

Note: If available, other cameras on the site should be viewable by the operator.

If you are using edge-based analytics or AI and a camera disconnects from the Bridge, the video stream and the detector will become offline. A camera with analytics disconnecting from the network immediately impacts the system's integrity. This limitation should be understood clearly by the installing company, central station, and end-user.

It should also be understood by the installing company, central station, and end-user how and when the service provided will respond when trouble or failure of the system occurs. When installing outdoor intrusion detection, it is recommended that the detectors utilize anti-masking technology as this will minimize the possibility of system tampering while the system is disarmed.

Zone Bypassing
End-user's expectations for a visually monitored system typically differ from those for a traditional intrusion systems. To ensure an acceptable service level, it should be understood clearly by the end-user that when a zone is bypassed, this can affect the system's ability to detect intruders and the operator's ability to receive video. This type of detection error is more prevalent in outdoor detection systems than in indoor systems.

Head-end equipment should be installed in areas that restrict the possibility of system tampering. The location of the equipment should be clearly documented by the installer. This information should also be known by both the central station and the end user.

The CHeKT visual monitoring solution utilizes the premise internet connection to communicate with the CHeKT cloud. The installing company, central station, and end-user should understand how to determine whether a second connection is necessary.

End-User Bypassed Zone

General Camera Installation
Guidelines

It is recommended to use bullet or turret cameras when possible, as these cameras isolate the lens from the infrared. The lenses in dome cameras tend to reflect infrared energy back into the lens, reducing nighttime video quality. Install dome cameras using a bracket to shield the dome from rainfall. When a dome camera is mounted sideways on a building, the image can worsen on rainy days. In hotter climates, improperly mounted cameras often show discoloration that impairs nighttime image quality.

Note: Most lenses on vandal-resistant dome cameras are made of polypropylene, that is a plastic material that tends to yellow as it ages.

Thermal imaging surveillance cameras are a great choice when monitoring large outdoor areas in difficult or unique environments, where obstructions can make viewing difficult. Thermal imaging cameras use the heat signature generated by an object or person to determine their approximate location. The leading advantage of thermal imaging cameras is that they do not require any visible or external light source to detect movement.

Guidelines for proper camera installation:

- Camera placement should be based on achieving the best field of view, not on ease of installation.

- Consider the effects of daily and seasonal variations of light, especially at night.

- Consider possible changes in foliage growth.

- Consider protection from vandalism or camera repositioning.

- Consider protection from environmental weather events(e.g.,driving rain).

- Be aware of temporary, new, and existing structures that may obstruct the camera's field of view.

- Place the camera where it can be serviced safely.

- Ensure that the camera is fixed firmly to the structure to prevent movement due to high winds. Instability can impact the detection capabilities of cameras with analytics.

Site Light Levels

It is important to maintain acceptable light levels over an area to ensure that video feed will be detailed and accurate enough that the system functions correctly. The minimum light level required for proper functioning depends on the type of camera and the type of activity being monitored. It is recommended to choose a camera that performs well in low-light conditions.

Note: Just because a camera has an infrared illumination function, this does not necessarily mean it will provide an adequate low-light picture.

When providing video monitoring services, the minimum light level should be determined both before and after installation. As with human vision, cameras struggle to detect colors and details in low-light environments. During the day, light levels are generally acceptable; at night, however, this is not the case. Artificial light may be required to provide acceptable visibility for the operator responding to an alarm.

Note: The light level will likely alter the color range detected by the camera.

Example:
The color of a vehicle or article of clothing may appear differently in natural light than it does using artificial light at night. This is important to keep in mind when an operator is communicating details to the responding agency.

In cases where artificial light is not available, cameras can be installed with infrared illumination. Using infrared illumination complicates the operator's ability to accurately identify if a human is present. Infrared camera picture deteriorates at longer distances away from the camera. Because cameras in night-mode are often displayed in black and white, an operator may have difficulty describing a suspected intruder to the end-user or responding agency.

Example: A person in dark clothing can easily blend into a black background, particularly when the person is at a long distance from the camera.

General Camera Installation
Guidelines

The placement of a camera during the day should also be considered. On a sunny day, the light level can become excessive. This often occurs in the morning or evening time, when the sunlight shines directly into a camera. Excessive light levels can cause the image to flair, preventing the camera from being viewed by the operator. Flair can also be caused by light reflecting off of other surfaces, such as windows, flashlights, or vehicle headlights. Lighting conditions can also affect the operation of a system that uses analytics or AI, and excessive light levels potentially preventing these operations from functioning properly at these times.

Camera testing should be performed both during the day and at night to account for these factors. Testing should also be performed six months following installation, to take seasonal changes into consideration.

Secure Site or Area &
Unsecure Site or Area/Dual Site

EXPLANATION
Visual monitoring adds complexity to the operator response. If someone is present in a live or recorded video clip, this does not necessarily mean that a crime has occurred. Most false alarms are caused by employees or family members entering a protected site or property. To simplify the operator response, it is recommended that a supervising station classify separate areas when providing video verification and video monitoring services. For the purpose of this document, the phrases "Secure Area" and "Unsecure Area" will be referenced. Where possible, be sure to provide specific instructions for each area so that an operator has a clear understanding of the environment while viewing the video camera.

Secure Site/Area
A secure site is an area at the protected site in which unauthorized access is intended to be detected. A secure site or area should have walls, fencing, or a natural barrier that would prevent persons from accessing that area without effort.

Unsecure Site/Area
An unsecure site is an area that is not fully enclosed by a securely constructed barrier. An example of an unsecure site would be an automotive dealership without a fence surrounding the entire property.

Even if an area is surrounded by a fence, if the barrier is damaged, the area should be considered unsecure. When providing visual monitoring, a person seen in an unsecure area is not necessarily committing a crime. Some protected premises may have areas that are both considered secure and unsecure. Noting these areas during the initial installation provides the required information for the central station personnel to know how to respond in each area.

When the central station views an event video, an operator should understand whether the area is classified as secure or unsecure. This information will aid the operator in responding to the event accurately. Operator access to documentation that includes response instructions is also recommended.

Note: A Talk-down or operator controlled audible is recommended in unsecure areas to audibly remove intruders from the property.

Visual Monitoring
Site System Planning

CHeKT
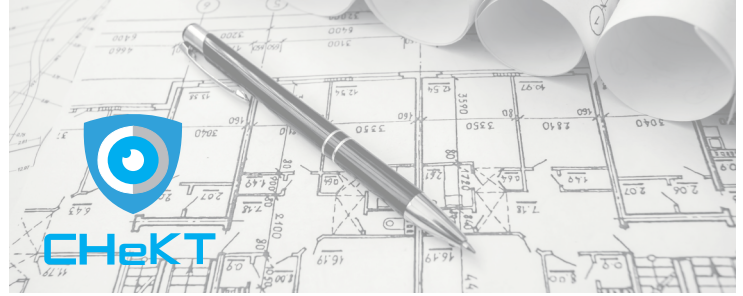
Site Analysis
A site visit should be performed to determine how the system will be designed to meet the client's objectives and provide the necessary service(s).

Design Document
A design document for the system should be created so that the end-user, central station, and installing/servicing companies have all necessary information about the visually monitored system. The end-user should also be made aware of any system threats and limitations.

System Proposal
The system proposal should include the following:

- Positions of all cameras and detectors and what the cameras are designed to view or detect.

- Location and mounting height of cameras.

- When using intrusion detectors, labels describing which cameras are paired with a specific detector.

- Location and display of audio devices, if used.

- A lighting plan (natural , artificial or infrared).

- A comprehensive list of equipment being installed.

- A list of maintenance services to be provided and who is responsible for providing them.

- If the end-user is required to perform maintenance (i.e., clean cameras or remove foliage), this should be understood clearly by the user.

System Equipment and Configuration
Detectors should be installed to provide necessary detection in a secure area while minimizing false or unwanted alarms. When pairing intrusion detectors with a camera, it is important that the detection pattern fall within the paired camera's field of view. When designing a system, imagine the operator; he or she must understand with certainty what caused the detector to trigger. (Example A)

Prior to completion of installation, the detectors should be walk tested to ensure that the detectors meet the system requirements. Detector's patterns should not extend into areas that do not require detection. (This is a frequent cause for unwanted alarms.)

The rising and setting of the sun should also be considered when placing intrusion detectors and cameras. When deploying cameras with analytics. Direct sunlight can impair detection in systems with cameras that use analytics. With certain cameras, this can also be a cause of unwanted alarms. (Example B)

When multiple detectors are paired with a single camera, walk-test each detector to ensure that the correct camera is populating in the CHeKT monitoring portal and that the camera's field of view clearly covers all detection patterns. Place the detection pattern on the camera in the dealer portal to further ensure an accurate and effective response from the operator.
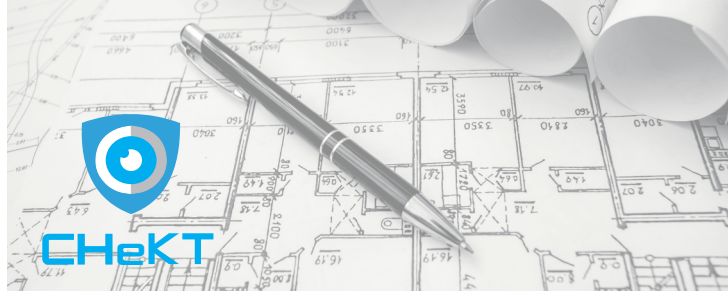

A

Overlap Interior Detection/Camera Patterns

B

CCTV Image Affected by Sunlight

Visual Monitoring
Site System Planning

Arming and Disarming the Site

The Bridge contains a voltage input that allows the user to arm and disarm the Bridge with an existing alarm panel. This is the recommended way to arm a site. With this method, thought should be given to how the end user will access the property.

Note:The alarm manufacturer's mobile app is the recommended method of arming.

Many alarm manufacturers provide programmable relay boards that can be installed on an alarm panel and configured via intrusion panel programming. Triggering events on the Bridge with this method provides the simplest means of delivering video to the central station. With this configuration, program the associated zones to a relay and wire the relay directly to the Bridge zone input. Using this method will require you to place the Bridge in the "armed always" state in the dealer portal.

Note: A relay is not supervised, so it is recommended that the Bridge be located near the relay output board and the wiring be protected to avoid tampering or disconnection.

Future:
In late 2020, users will be able to arm the Bridge by schedule, as well as directly through a mobile app. This functionality will allow an integrator to design systems that may not require a traditional intrusion system to be installed at the protected premises.

Zones on the Bridge itself can be configured with various features including an alarm panel (delay, instant, 24 hour). It is recommended that, if exterior detection is used, an exit delay be programmed in the CHeKT dealer portal to allow the user to arm the system and exit safely without triggering the system.

Note: Be sure to understand how to configure these applications in the dealer portal.

Exterior Light

If you are using the armed output of the alarm panel to arm and disarm the Bridge, the same wiring method can be used to activate a light that provides a visual indication that the property is either armed or disarmed. This is an effective way to alert employees as they approach the property so that they can determine whether the system is activated.

Note: Intruders are provided with the same indication.

Allowing the end-user to access the protected premises without generating an unwanted alarm requires a clear plan that must be understood by the end-user. This method proves more challenging when the intrusion detection is outdoors, as the end-user passes through the area of detection to access the system to disarm it.

Audio or Talk Down Functionality

Audio or talk-down functionality is an important surveillance feature. This function can be used to remove intruders from a protected property without contacting the end user or notifying the responding agency. The Bridge has an 1/8" audio output that broadcasts pre-recorded or custom text-to-speech messages form the operator. An installer should understand that a speaker must be amplified and that different amplifiers and speakers have varying performance levels. An amount of time should be spent choosing the appropriate speaker and amplifier for each specific site.

Many large commercial properties already have an existing PA system. If an additional input option is available on the PA system, the Bridge can broadcast the audible warning through the existing infrastructure. Again, the quality of the audio should be tested to ensure that the system meets the end-user's expectations.

Commercially Rated PA System

Visual Monitoring
Site System Planning

Relay Control

Depending on the Bridge type purchased, a relay control may be available to the operator in the monitoring portal. It is important that a relay be paired with a camera. When a relay is activated, the Bridge will communicate a signal to the central station indicating that the relay was activated. When this action occurs, a video clip will be generated and stored in the CHeKT cloud.

This information allows the central station and end user to understand which service was provided and when. The purpose of the relay is to allow for a higher level of service to the end-user. With the relay, an operator can control sirens, lights, exterior gates, or an access-controlled door. These are low-voltage relays and users and operators must understand the limitations of these devices. Refer to the electrical code to determine if the relays can be used to control devices that require high voltage.

Cabling Recommendations

Cables should be installed in a professional manner.

- When using exterior intrusion detection, efforts should be made to prevent cable tampering.

- Because of the increased possibility of tampering when cables are installed outdoors, EOLs should be installed at the device and the detector itself should be tampered.

- When cable runs are long, consider the current draw of the device and the wiring distance of the detector being installed.

- It is recommended that cables be labeled at both ends to avoid mistakes during service and maintenance.

- Cable splices should be secured and protected from weather and tampering to ensure system integrity.

- Detectors and connected cameras should be installed in accordance with manufacturer specifications.

Walk Test

A walk test of all devices should be performed by the installation company. This test should, when possible, be confirmed by the central station.

During the walk test, carefully check for the following:

- Ensure the detectors are paired with the appropriate camera, the intrusion system is communicating properly with the central station, and the CHeKT portal is correctly populating cameras.

- Once the detectors and cameras have been tested, enter the detection overlay into the CHeKT dealer portal.

- Ensure that when a detector is triggered, an operator can clearly determine if a human is present.

- The walk test should be performed outside the detection area to ensure that unwanted alarms are not generated.

- If the CHeKT SMS verification is utilized by the end-user, send verification texts to the users and instruct them on how to respond when the notification is received.

- After installation is complete, review daytime and nighttime images to ensure that the operator can see and identify human activity when a detector is triggered.

- Once system installation is complete, the central station should review the entire site to confirm that the cameras provide a quality image both during the day and at night. If the images are not of acceptable quality, additional lighting, illumination, or cameras are recommended.

- Methods of communication should be established between the end user and the central station personnel.

Visual Monitoring
System Completion

The following information should be provided to the central station and kept by the installation and service companies for future reference.

- The System Design Plan.

- An equipment list detailing part numbers and part placement.

- Site address and point of contact for the company where system was installed.

- Installing company and technician, if the installation is subcontracted.

- When possible, provide the schedule of operation that includes when the system is commonly armed and disarmed.

- A Response Plan.

Important: A specific response plan for each camera or detector should be included. THIS RESPONSE PLAN SHOULD BE UNDERSTOOD CLEARLY BY THE INSTALLING COMPANY, CENTRAL STATION, AND END USER. Failure to provide a clear understanding of how to process a received video signal will likely result in false dispatches and customer frustration.

Recommendation: When system installation is completed at a protected site, an installing company should consider temporarily monitoring the site for a few days to ensure that the system is stable and properly designed & installed. During and following installation, the systems video events are stored in the cloud and are accessible to the installing company. This allows the installer to view events the following day and take corrective action if needed to address any equipment errors that may cause false positives. After it is determined by the installing company that the system is stable and the correct response from the central station is confirmed, the site can be commissioned and brought online.

Additional Consideration / Post Installation
Go over your completion documents to ensure that the end user and central station have a clear understanding of system capabilities and limitations. Have the central

station check the lighting or illumination levels at night to ensure that human presence and criminal activity can be accurately detected. Understand clearly how to communicate to the central station any faults or trouble conditions for system performance. Also, understand how repair services will be provided to fix any issues that occur. Talk to the end-user so that they clearly understand their responsibilities if present on the protected premises when an alarm occurs (An operator may not know if this person is authorized to be on the property). If numerous unwanted alarms occur, determine who will be responsible for correcting or eliminating the unwanted alarms.

Note: A customer may have let foliage become overgrown, or moved something in a detector's field of view, causing unwanted alarms. Correcting this problem may be their responsibility.

All installed equipment should be maintained according to manufacturer recommendations. There should be a response document agreed upon by the installing company, central station, and end-user. This document should detail the action(s) to be taken upon incidence of an alarm, fault, or trouble condition.

It is recommended that the central station and end-user be familiar with this document before commissioning the system. It is also recommended that the installing company create a completion document and that the document be completed before the system is fully commissioned.

System Maintenance
Video verification/video monitoring requires the video system to function for the operator's ability to respond appropriately to the received signal. Periodic maintenance should be provided to ensure the camera's proper operation. Examples: dirty camera lens or globe, IP address change, or camera angle/tilt changes, causing the camera to no longer cover the desired area.
Note: Visual monitoring is the ideal application for selling the client a maintenance agreement.

Legal Concerns
A supervising station should understand what laws apply to storing and accessing information. A company providing video verification/video monitoring should be aware of the requirements placed on them by these laws and should have procedures in place to enable them to comply. Note that laws can be amended, new ones introduced, and old ones superseded; so it is recommended to seek up-to-date legal advice.

Suggested
Exterior Sensors

OPTEX HX-40AM Detector

The HX-40AM is a high mount outdoor detector with Anti-Masking for mid-level to high-end applications where reliability and performance are a must. The unique pyro-element developed by Optex provides a multiple pattern detection with 94 high density detection zones an accurate discrimination function for spot temperature changes in moving objects. These features drastically reduce false and missed alarms caused by severe outdoor environmental changes and provide a wide range of applications in visual security systems.

Ideal application: Plumbing or electrical contractors; businesses where inventory or merchandise is kept outdoors.

OPTEX BX Shield

The BX Shield (BXS) Series is a range of quad PIR sensors ideal for protecting windows and the immediate boundaries of a building or site.

The BXS also excels in environments where the temperature difference between the human body and the background is very small, due to its extreme high detection mode increasing the PIR sensitivity, preventing any missed alarms.

UNDERSTANDING VISUAL LIMITATIONS
The client should understand that video monitoring generally provides monitoring and detecting. Video monitoring does not always allow operators to recognize and identify a person on the protected premises. Although the possibility of identifying a person exists, it is unlikely and should be clearly stated by the security company.

OPTEX AX Series Photobeam

The AX-100TF short range photoelectric detector is compact in design with selectable beam frequencies. The selectable beam frequencies allows users to avoid unwanted crosstalk that may occur when using multiple photo beams over long distances or for beam stacking applications.

The AX-100TF is built with the IP65 high durable structure, which prevents water, dust, or bugs from getting into the unit. The ideal optical pitch design also reduces false alarms due to accidental beam interruption by falling leaves, birds, or other environmental factors. These features deliver performance in severe outdoor environmental condition with greater reliability.

OPTEX HX-80N Detector

The HX-80N is a high mount, outdoor passive infrared detector that provides the stability and reliability required of an outdoor PIR sensor. The most important element in a reliable outdoor detector is the ability to distinguish a human from a small animal. The exclusive pyro element on-board allows the HX to project an ideal detection pattern, providing improved accuracy in detecting of humans and producing fewer false alarms.

The HX detection length can be limited to avoid unwanted detection, and it's short range zones can be masked if needed. By limiting the detection range, false alarms due to unwanted movement by cars, persons, or animals outside the protected area can be eliminated.

OPTEX VXS Detector

Building upon features inherited from the VX-402 series, VX Infinity presents infinite possibility with the power of detection designs. The VX Infinity demonstrates long & stable performance in typical outdoor environments. The VX Infinity Series is manufactured to excel in its performance whether as a perimeter detection solution, spot / area detection solution, or as an immediate perimeter/boundary solution directly on a structure (walls and rooftops).

Digital Double Layer Detection: Both upper and a lower detection areas must be crossed simultaneously in order to generate an alarm. The detections are independently analyzed so that misleading events can be filtered out. This technology virtually eliminates detections of smaller animals on the premises.

OPTEX Fit Curtain Detector

The OPTEX Fit is a cost effective sensor that creates a 16 foot curtain detector.

The FTN-AM offers the perfect solution for outdoor areas where false alarms caused by environmental disturbances and small animals are frequent. The FTN-AM comes with a built-in bracket that enables horizontal rotation of 190° and the device's compact size and flexible detection area allow the sensor to 'fit' into a variety of both residential and commercial applications. The FTN-AM also includes the added security of Anti-Masking technology.

Online Product Catalog

click HERE

Visual Monitoring
Thermal Detection

While non-thermal methods of surveillance depend on visual light for detection, thermal imaging requires only a heat signature. Heat signature detection illiminates interference by weather, shadows, lighting, and other outdoor factors. With visible light cameras, all of these variables create the potential for excessive events in the monitoring center. This detection ability makes thermal devices optimal for outdoor surveillance and detection. Many customers would have a vested interest in thermal detection methods as they provide improved outdoor detection and imaging. There are a variety of vertical markets in which the majority of inventory is kept outdoors, requiring outdoor intrusion detection to prevent theft and damage. Automobile dealerships and boat or RV dealers often use outdoor lots to store and display inventory. A variety of distribution companies use outdoor storage facilities to store products and equipment. When a customer's inventory is stored outside, the customer is primarily concerned about protecting their inventory from theft and damage. In addition, in many instances, inventory is relocated or moved. Providing complete detection over an outdoor area is necessary to maintain a visual on the inventory at all times.

In contrast to many traditional surveillance methods that depend on visual light for detection, thermal imaging depends on heat for detection. The heat detection capability of thermal surveillance devices allows for a visual at all times on any humans on the protected property. When storing inventory outdoors, deploying cameras with video analytics or artificial intelligence may seem logical. However, understanding the limitations and potential for nuisance alarms should not be underestimated. Intelligent cameras have improved in recent years and will continue to improve, however it should be understood that the algorithms these cameras use to determine if a threat exists ultimately depend on pixels changing on the camera itself. Inclement weather, poorly lit areas, and other variables may cause excessive signals into the central station an even higher concern is missing a real event. Alternative surveillance methods, including thermal imaging technology, can improve security outdoors by eliminating dependence on direct video visual from a camera.

The advantages of thermal imaging cameras allow for a wide variety of applications in visual monitoring and outdoor security. Because thermal imaging cameras see heat rather than light, and human bodies radiate a significant amount of heat, these devices can be thought of as direct human-detectors. A thermal imaging camera is able to avoid many of the things that impacts the detection of a visible light camera. While the detection capability of a visible light camera immediately deteriorates in inclement weather or shaded areas, thermal cameras perform well in these conditions. Because thermal cameras rely only on heat detection, these devices are able to filter out disturbances such as rain and shadows. Thermal devices can accurately and distinctly detect a person moving several hundred feet away, even when there is no natural light available. When conditions compromise or complicate the detection of a visual light camera in an outdoor area, thermal imaging directly detects human presence in the area.

Despite the many advantages of thermal imaging devices, this equipment inherently contains a number of limitations. One limitation is that thermal cameras provide no means by which to describe the exact details of a person. As thermal cameras provide only a heat signature, an operator viewing the video would not be able to provide a detailed description of an intruder. In an outdoor storage lot such as a car dealership, this information would be useful to determine which products may have been affected by theft or damage.

Thermal Image

East Lot
CAM 12

Visual Monitoring
Thermal Detection

If a customer requires the detection of details and objects, thermal imaging devices will not be enough. It is therefore recommended that thermal imaging devices be used together with other monitoring devices to provide the maximum clarity possible to operators and emergency responders.

Certain measures should be followed when mounting and installing a thermal camera to prevent damage to the device and ensure maximum surveilling capability. It is vital when installing all cameras with analytics to ensure that the camera is mounted to a surface that is not susceptible to movement or shaking. A camera mounted outside may vibrate from passing cars, trucks, or wind. Vibration and movement can impact the device's detection ability by distorting detected heat signatures. When possible, use a camera with image stabilization, as is important to ensure that the field of view allows for maximum detection. Thermal cameras often have a relatively narrow field of view. Mounting a thermal camera high on a building will create a blind spot directly beneath and in front of the camera. The specific area where the camera is unable to detect should be clearly understood by the installer, central station, and the end-user. Following these guidelines when installing thermal imaging equipment allows for a higher probability of detection and greater security against intrusion.

While thermal cameras provide consistent and reliable detection, they lack the ability to provide exact details that an operator or responding agency needs. The addition of visible light cameras can play an important role in ensuring a complete visual and maintaining constant detection. A dual image camera provides both thermal and visible light in the same housing.

In these two-in-one devices, the thermal camera provides general detection, and the visible light camera provides color and other specific details for camera operators and emergency responders. Taking this one step further, some dual-image cameras run detection analytics on both imagers, which provides the best of both worlds, because there are some conditions that can be detected better by visible, and others detected better by thermal.

With dual-sensor analytics, the images are synchronized and provide accurate detection while validating alerts from both sensors. This is the recommended way of delivering a highly trusted security result in virtually all conditions. By combining two technologies into a single housing, this minimizes cost in complexity of mounting multiple devices.

The improved detection and outdoor surveillance capabilities of cameras that contain thermal imaging software reduces the risk of intrusion and improves response to security threats. Thermal imaging cameras provide the most cost-effective outdoor detection coverage by providing heat signature information to the operator. The additional visual provided by thermal devices can reduce the risk of property damage or theft and reduce detection and response times. Thermal imaging devices are also relatively straightforward to mount and integrate into existing systems, reducing installation fees. While the price point of these devices may appear high, the ability of thermal monitoring devices to detect broad areas of detection, minimize interference, and provide immediate signaling to the central station makes these devices well worth the price.

Thermal imaging information was provided by Sight Logix. For help designing an area with thermal detection, a site survey tool can be found at:http://www.sightlogix.com/sightsurvey-tool/

Online Resources

Exterior Visual Monitoring [click here]
Design Solutions

Interior Design Solutions [click here]
Design Solutions

Interior Industrial
Designing Visual Monitoring for Warehouse Environment

- Installing a traditional 10 zone intrusion alarm panel with 2 Bridges, and an 8-channel HDCVI recorder, interior video monitoring service is quickly provided to this client.

- Using a photobeam, an industrial motion detector in the warehouse to protect sensitive chemicals and an interior office motion detector, the monitoring center has visual alarm verification of each zone.

- Because all zones are interior, the monitoring center does not have any increased alarm signals.

Introduction to the CHeKT
Dealer Portal [click here]

Remote Configuration Of All Chekt Devices

Viewing Real-Time Status Of Online & Offline Devices

Remote Add/Remove Cameras From A Site

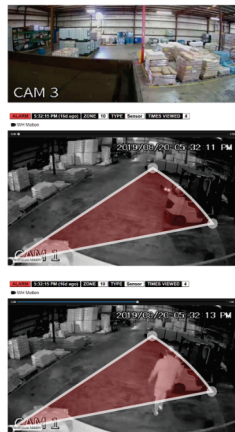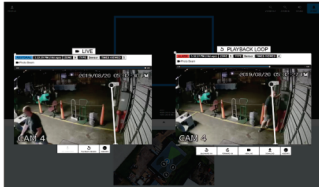Customizable Site-Map Setup For Central Station

Billing Feature

Introduction to the CHeKT
Operator Portal [click here]

Residential Sites | **Commercial** Sites

Automation XML Integration

Pre & Post Video Of Alarm Events

On-Demand Playback of Cameras

Talk-Down Feature

Interactive Site Map

End-User SMS Verification

Dealer Launch Site

Visual Verification Bridge
Powered by CHeKT

www.chekt.com/launch

[click here]

Everything You Need To Successfully Deploy Visual Monitoring

CHeKT

www.chekt.com
224-44-chekt
support@chekt.com