SIQURA®
SURVEILLANCE SOLUTIONS

White Paper

Safeguarding Your Surveillance System

An introduction to the Siqura camera health monitoring VCA solution

Optelecom-nkf

Safeguarding Your Surveillance System

An introduction to the

Siqura camera health monitoring VCA solution

Kate Huber, *Technical Writer*

Peter de Konink, *Product Line Manager, Codec/Analytics*

Armand Wemelsfelder, *Senior Hardware Engineer/Software Architect*

Siqura Camera Health Check
White Paper v1.0 (100303-1)
AIT5.2-MW07SP2

Brand names

Any brand names mentioned in this document are registered trademarks of their respective owners.

More information

If you have any comments or queries concerning any aspect related to this document, please do not hesitate to contact:

USA
Corporate Headquarters
Optelecom-NKF, Inc.
12920 Cloverleaf Center Drive
Germantown, Maryland 20874, USA

General : +1 301 444 2200
Fax : +1 301 444 2299
E-mail : sales.us@optelecom-nkf.com
WWW : http://www.optelecom-nkf.com/

The Netherlands
European Corporate Offices
Optelecom-NKF B.V.
Zuidelijk Halfrond 4
2801 DD Gouda, The Netherlands

General : +31 182 592 333
Fax : +31 182 592 123
E-mail : sales.nl@optelecom-nkf.com
WWW : http://www.optelecom-nkf.com/

Top-notch surveillance system leaves company in the lurch after break-in

There were cameras everywhere, so no one expected that the burglars would ultimately get off scot free. After the perpetrators broke the front window and stole no fewer than ten PCs, the police and office personnel expected justice to be had from the recordings made by three cameras in the vicinity of the vandalized window. It was supposed to be an easy open and shut case.

In the end, however, the promising footage only revealed that one of the cameras was out of focus at night, the other had been turned to face the wall, and the last divulged the blatant blooming effect of the full moon. The injured company ended up having to bear the loss itself despite having already invested heavily in a state-of-the-art video surveillance system.

Is this just a case of bad luck?

Introduction: Safeguarding your surveillance system

Every year, hundreds of millions of dollars are spent on video surveillance equipment. Most of these purchases are preventative: Systems are set up to register problems as they occur and to keep calamity from compounding. Once a system is set up, most expect it to work. Yet, despite high-tech surveillance systems receiving regular maintenance inspections, every system is at risk of failing at just the wrong time.

In an effort to combat potential pitfalls, Optelecom-NKF (manufacturer of Siqura®) recently introduced the Camera Health Check, which is composed of two video content analysis components: the Siqura Image Quality Monitor (IQM) and the Siqura Tampering Detector. It offers the CCTV and video surveillance industry a solution that monitors every system's most failure-prone part, namely, the camera.

By making sure that an alarm triggers the moment a camera stops working properly, operators can request the right kind of maintenance, the moment it is required. As a result, camera configurations utilizing extra cameras to ensure duplicates in the event of a breakdown (such as that in the figure below) become superfluous, ultimately cutting the cost of the overall surveillance system. Furthermore, system owners, end-users, and service level agreement (SLA) holders can be confident that the images they need are there the moment they need them.

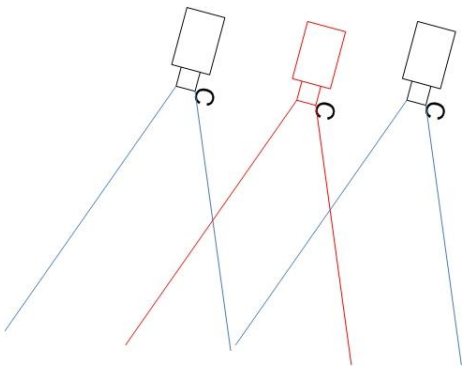

Figure 1 The Camera Health Check makes the center (red) camera superfluous.

Exposing stoppages

True to its name, the IQM uses a variety of intelligent VCA algorithms to keep a constant and close watch on the camera image, using an alarm to alert operators within seconds of malfunction. In order to maintain a complete overview of the quality of the camera image, the IQM observes four elements: focus, exposure, contrast, and the signal to noise ratio (SNR), each of which is discussed in more detail in the following sections.

Figure 2 Users can configure and view the IQM via an access-controlled browser-based user interface.

Confirming a clear vision

Naturally, you need to be able to see clearly when you're supervising a surveillance situation. The focus monitor regularly measures the detail in an image, or how sharp the edges of the pixels in an image are, making sure that the parts of the camera scene that you need to see are clear. This entails sampling the luminance, or perceived brightness, of the picture, taking into account certain known sensitivities of the human eye.

Figure 3 Unfocused image (left); focused image (right). The focus measurement alerts operators the moment pictures start to look blurry.

Although at a technical level it's inevitable in digital imaging that video is never completely void of any obscurities, the parameters of the focus algorithm guarantee that operators are warned as soon as indistinct areas start to impede the surveillance situation. To ensure the success of this application and for the focus algorithm to work correctly, it is imperative to specify exactly what it is you need to see in detail.

Specifying what you need to see

All four image quality components use a single so-called region of interest (ROI) image, which is a one bit per pixel bitmap image. Since it usually doesn't matter if the whole picture is in focus, users define the important areas of a camera scene by masking the parts of the ROI that are *not* of interest. The system then compares its results with the ROI to generate a meaningful measurement and notify operators when user-configured thresholds are crossed.

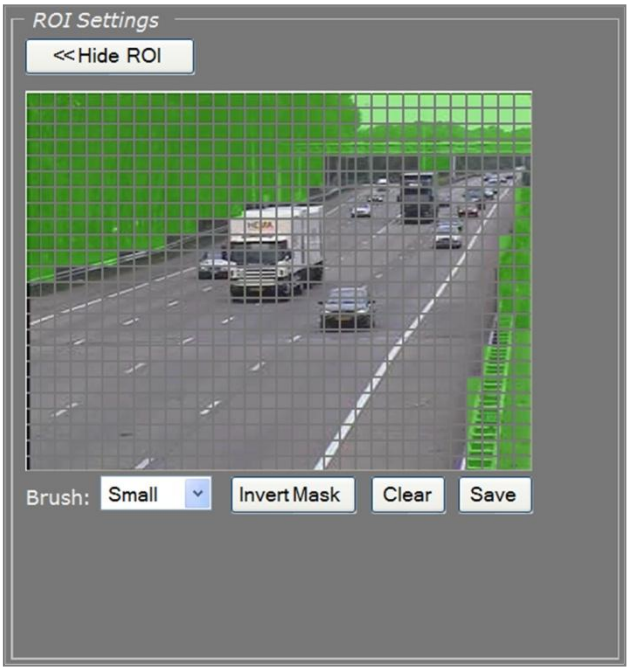

Figure 4 The IQM algorithms examine the region of interest (ROI) to produce meaningful measurements.

Illuminating inadequate exposure

No one can see in the dark and driving on a sunny day after a rainy squall can sometimes make the road unbearably bright. Similar extremes in lighting conditions affect cameras just as they do people. Anything from a failed iris control or a poorly positioned camera to someone pointing a flashlight at the camera can cause an over- or underexposed image. Therefore, the exposure monitor warns operators the moment a situation gets too dark or too light.

Figure 5 An overexposed image (left); an underexposed image (right)

It does this by first measuring the luminance of the pixels populating an image and then calculating an average. The exposure algorithm compares this average with parameters that are configured to conform to a user's personal preference for the brightness of a picture. The result of this comparison determines whether or not an alarm will alert operators of an under- or overexposed camera image.

Keeping a balanced contrast

Similarly to the exposure monitor, the contrast monitor also looks at the brightness of an image. However, unlike the other quality monitors, the contrast algorithm measures the difference between the light and dark pixels, which indicates the extent to which objects in the camera scene are visible; for example, the setting sun in the background might veil essential images in the foreground in the same way that it's never a good idea to take your friend's picture with the president when there is a bright light behind them.

Figure 6 Too much contrast (left); not enough contrast (right)

In general, the contrast monitor deems a camera view to have just enough contrast when there is an equal number of dark, light, and gray pixels. Depending on the parameters set by the surveillance system personnel, the contrast monitor will inform operators when there are either too many gray pixels (low contrast) or too few (high contrast).

Detecting signal disturbances

Every electronic device that receives or transmits information, from surveillance cameras to car radios, incurs some “noise” in the signal. Under normal circumstances, the signal to noise ratio (SNR) is high (>45 dB) and unnoticeable to the human eye. However, when too much noise enters a picture, it can, of course, hinder the surveillance situation. For example, in low-light conditions, the noise level can rise above acceptable levels. Likewise, flaws in older cameras may produce additional noise, consequently obscuring images. Moreover, in IP systems, noise in video greatly complicates the encoding process.

Figure 7 Too much noise (left); a balanced signal to noise ratio (right)

Curbing crime

Since cleaning, mechanical vibrations, or even vandalism can reposition cameras and a lens can become contaminated by elements, such as spiders and dust, the Tampering Detector compares the actual camera scene with the intended one and alerts you of any unexpected changes. Therefore, despite the normal wear and tear of everyday operation, users can rest assured that their video surveillance system is recording what it needs to, when it needs to.

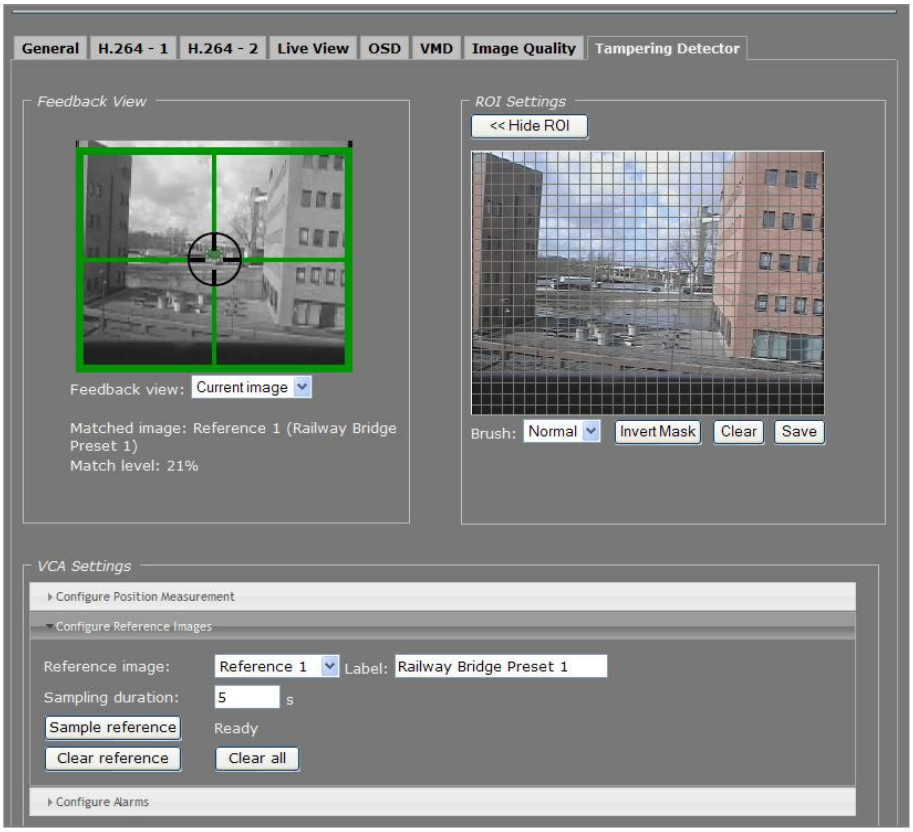

Figure 8 Users can configure and view the Tampering Detector via an access-controlled browser-based user interface.

A steady position and stable pixels

The Tampering Detector uses two methods to verify the quality of the video stream, either of which can trigger an alarm if certain user-configured thresholds are traversed. The first way is through regularly comparing the video with a reference image and checking if the pixels are the same. The Tampering Detector also perceives any shifts in how the camera is situated by comparing a picture's current location to configured values for the horizontal and vertical position of the reference image.

An option for nearly every occasion

Uniquely, the Tampering Detector can automatically select the applicable reference image for a specific situation. This means that users don't need to worry about checking on the Tampering Detector's settings if the position of the camera changes to one of the established reference images.

Since up to 16 reference images can be configured in the system, it is possible, for example, for the Tampering Detector algorithm to maintain an overview of the camera image in both day and nighttime lighting conditions for eight different PTZ preset positions. This, as well as its ability to observe changes over both long and short periods of time, makes the Tampering Detector an invaluable tool in securing virtually any surveillance system, from trains and other vehicles to corporate or government campuses.

When an alarm triggers

Alarm: Sanding tunnel road blurs camera images

It's been a cold winter and the roads have been icier than usual. Municipal trucks are out in force to frequently sand and salt the busiest motorways. Unfortunately for operators in a tunnel traffic control room, these efforts have made it hard to see clearly: The sand and salt have covered the surveillance cameras overseeing the tunnel road with a layer of dirt and grime, making it virtually impossible for operators to safely assess automatic incident detection (AID) alarms.

Fortunately, the IQM focus measurement is configured to sound an alarm the moment dirt starts to blur the camera image, notifying operators before the AID application is no longer able to work properly. After an alarm sounds, operators can call the appropriate maintenance personnel to clean the camera cover and prevent false - or worse, missed - AID alarms.

Alarm: Metro car no longer monitored

Last year, a metro system in a mega-metropolis installed video surveillance cameras in its trains after a rash of late-night muggings beleaguered riders. The system has made a world of difference: Perpetrators are caught red-handed and passengers feel it is safe once more to venture out after hours.

Recently, however, a number of the newly installed cameras have triggered Tampering Detector alarms. Security personnel examining the camera images noticed that various scenes supervised by all these cameras appear to have shifted.

The system is owned by the integrator, who has a service level agreement (SLA), guaranteeing that each camera will record 24 hours per day and that the footage shot between 11 p.m. and 6 a.m. will be available for 99.9% of the time in a given calendar year. Once the integrator has assessed the situation, they realize that the trains' vibrations have jiggled the cameras away from the areas they were intended to monitor. Measures are taken to reposition the cameras and fasten them so that they will better resist the tremors of daily metro operation in the future. Since the integrator was alerted in time and the system was up and running again in no time, not a single hour of the SLA was breached.

Alarm: Nesting pigeons block camera view

A national railway network comprises a vast network of tracks and trains that are all registered year round by CCTV cameras. On a warm spring day, one of the cameras supervising the area around the main station in the capital triggers an alarm. The image is occluded by pigeons that are building a nest on top of the camera's housing cover. Maintenance personnel are alerted and measures are taken to make the birds move elsewhere.

While the pigeons might have had a bad day, the railway authorities are happy to have the full faculties of the camera when later that same day, youngsters come to flatten pennies on the tracks, putting themselves in a very dangerous situation. However, railway security is able to keep the trains running on time despite having to escort the children to a more appropriate playground.

Alarm: Vandals play paintball with city center surveillance cameras

On a dark Monday night, an alarm triggers indicating to the city police that something is amiss with three cameras outside a bank on the edge of town. On-duty officers receive the alert on their PDAs and go to the cameras' location.

Upon arriving, they see a group of teenage boys playing paintball and making various cameras in the vicinity their targets. The lads are arrested for vandalism and the police contact the network owner and SLA holder, who come to replace the cameras before the night is out. While the law may have been infringed upon, the availability of this surveillance system and, consequently, the general safety of this city center have hardly been violated at all.

Alarm: Parking garage attendant can't see the main entrance at sunset

Parking garages are notorious for crime. Due to the fact that attendants can rarely oversee the entire situation and parking garages are often open to all who pass by, potential perpetrators may view many lots as easy targets. Despite disturbing facts and figures, technological advancements are helping to make the world a safer place. That's why a city center parking garage recently installed a state-of-the-art CCTV system capable of recognizing license plates and detecting specified incidents.

Yet, the day after deploying the new system, an IQM alarm indicated that one of the cameras monitoring the main entrance of the facility was producing extremely overexposed images, consequently putting the license plate recognition and incident detection applications out of commission. The parking garage management contacted the SLA holder and owner of the system who, in turn, investigated the problem.

It turned out that the windows on the office building opposite the garage were reflecting the sun at dusk directly at the camera in question. Some settings and the position of the camera were adjusted, and the network is once again able to accurately and effectively protect people and their possessions at the parking garage.

Alarm: Snow occludes view of bridge over port's primary waterway

It has been the snowiest winter in over a decade. At a traffic control center supervising the main water- and motorways surrounding one of the busiest ports in the world, visibility is hampered by all the hailstones and snowflakes.

Yet, it is only after a Tampering Detector alarm triggers that operators notice that snow is blowing up against the PTZ camera providing an overview of an important bridge, across which a major highway traverses and under which seagoing freighters must pass to gain access to the port. While operators can pan and tilt the camera to shake the snow off it, this procedure causes delays and the problem persists, and the system owner is notified.

By repositioning the camera to a slightly different angle, snow isn't able to collect on the camera housing and occlude the camera's view. As a result, drivers and sea captains no longer have to wait as long for operators to ensure that it is safe to open the bridge, ultimately streamlining the flow of traffic both by land and by sea.

Conclusion: Every image at your beck and call

Routine checks cannot always catch everything that might hinder image quality and something as harmless as a maintenance inspection or lens cleaning can shift a camera to supervise a superfluous area. In sum, myriad things can go wrong without you knowing about it regardless of how up-to-date or well-kept your surveillance system is. This can lead to disappointing results at the moment you most need on a positive outcome. Dealing with these needs is now absolutely necessary to the video surveillance industry so that businesses and our safety can continue to depend on video surveillance systems.

Maintenance on demand

By developing two unique new VCA tools, Optelecom-NKF counters unexpected breakdowns and provides video streaming technology with an invaluable aid in ensuring system performance and securing the safety of any surveillance situation. The IQM and Tampering Detector immediately let operators know when something is wrong with a specific image. As a result, these applications make sure that the upkeep you pay for fixes exactly what's needed, when it's needed.

Guaranteeing availability

For those relying on or accountable for service level agreements (SLAs), the IQM and Tampering Detector can function as the perfect companion to confidently combat elusive technical failures. Whether changes in lighting conditions require refocusing, the iris control gets stuck, or vandalism occludes an image, the IQM and Tampering Detector are there to warrant that your system is functioning up to par and that you know right away if something is amiss with the picture of a particular camera. As a result, these innovative applications guarantee the availability of quality images you can count on.

Version 1.0 (100303-1)
Siq. CHM white paper (MW07SP2)