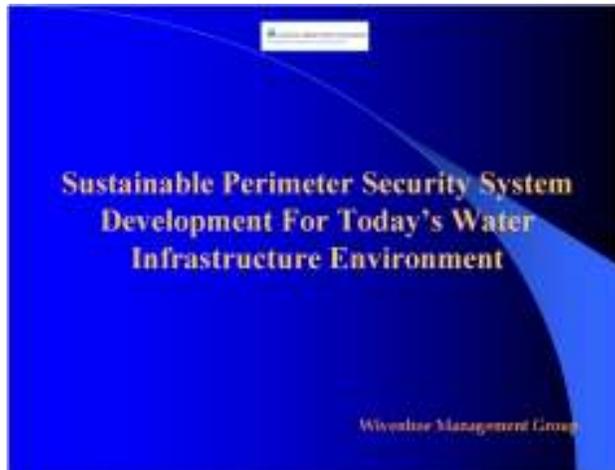


WIVENHOE MANAGEMENT GROUP

ONE PHEASANT RUN * MILLSTONE TOWNSHIP, NEW JERSEY 08510-1709
TEL: 609-208-0112 * FAX: 609-208-1295

EMAIL: dmccann@wivenhoegroup.com

SUSTAINABLE PERIMETER SECURITY SYSTEM DEVELOPMENT FOR TODAY'S WATER INFRASTRUCTURE ENVIRONMENT



Introduction:

This presentation given to the AWWA 2012 Water Security & Preparedness Conference in St. Louis in September, 2012 is in three parts:



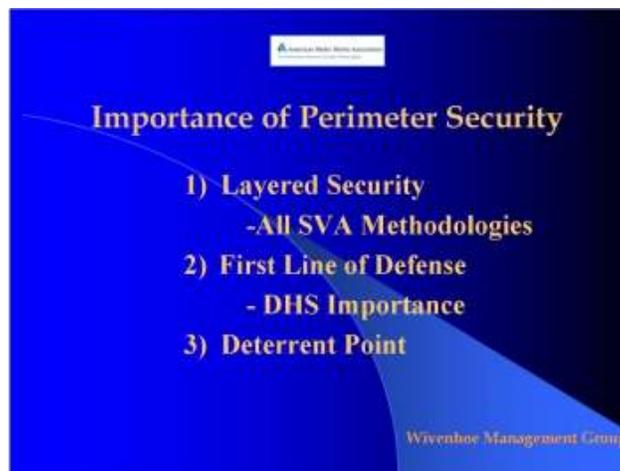
The first part relates to the importance of **Perimeter Security** in devising appropriate security measures to provide an adequate level of protection for a water or wastewater facility. This is in keeping with accepted Security Industry standards and practice.

It further meets SVA (Security Vulnerability Assessment) recommendations, and pending and future water security legislation and regulations, such as those being readied by the DHS (Department of Homeland Security) under the Water Security Act.

The second part of this presentation concerns **Sustainable Security Systems**, encompassing the strides that have taken place in the last few years to provide “off-grid” power sources for security systems and equipment, particularly in the wireless video and video motion detection areas that form the backbone to virtually every perimeter security system being installed today.

Part three of this presentation discusses the **New Security Technology** now available for perimeter security systems at water and wastewater facilities utilizing wireless equipment, stand-alone sustainable power sources and security systems with vastly improved camera surveillance equipment that can function in low power and low light conditions.

Part three also addresses new Deterrent Technology that is very applicable to water and wastewater facilities and the latest Remote Monitoring Services applicable to virtually any surveillance system. These new technologies significantly reduce the cost and manpower requirements that would otherwise be necessary for 24/7 monitoring.



The Importance of Perimeter Security:

Most SVA methodologies stress the need for **Layered Security**, providing a series of obstacles to an adversary attempting to access a specific area. The more layers and greater the difficulty, the longer it will take an adversary to reach their objective, and the more time local law enforcement has to neutralize the adversary before it can carry-out its goal.

A facility’s perimeter security is its **First Line of Defense**. This is where any intrusion system will first indicate that the perimeter has been breached by unauthorized parties. It is also the first point at which a planned response begins to take effect. Action cannot be taken to neutralize a situation if no one is aware of the security breach.

Perimeter security is also considered very important within the requirements of the DHS (Department of Homeland Security) and CSAT methodology and their corresponding Standards of Performance for the Chemical Industry. These same DHS standards are likely to be used under the proposed Water Security

Act, and are already being applied by NERC (North American Electric Reliability Corporation) for Energy Utilities.

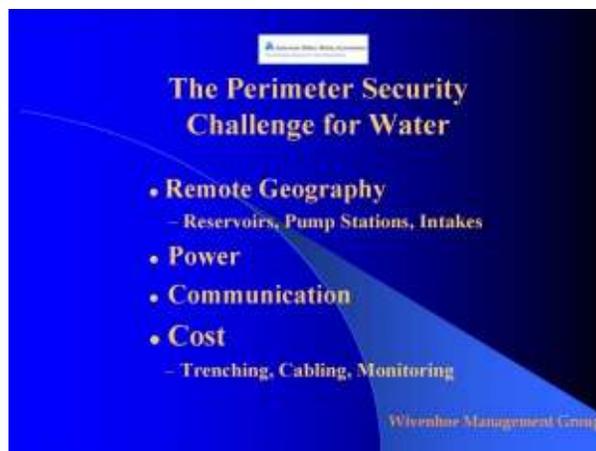
The most important point related to Perimeter Security may well be that of the **Deterrent Point**.



The Security Industry for many years has successfully deployed what is often called the Deterrent Approach to security, where solid, well thought-out perimeter security measures can act as a deterrent to adversaries and criminals, inducing such individuals to seek targets elsewhere, where security appears to be far less inhibitive.

Under the EPA mandated Water Industry SVA program, many security vulnerability assessments were carried-out under the RAM-W SVA methodology created by the Sandia National Laboratory section of the Department of Energy. (Sandia does not recognize the Deterrent Approach in their principle of **Detect, Delay, Respond**, which can reduce the cost of securing a Water or Wastewater facility by very significant amounts.)

The DHS does recognize the Deterrent Approach and employs the principle of **Deter, Detect, Delay, Respond**. Thus it is possible with good perimeter security to adequately protect water, and wastewater facilities and systems, meet budget constraints, and comply with current and pending security legislation and regulations.



The Perimeter Security Challenge for Water:

There are however, specific problems, particularly for the Water Industry in deploying good perimeter security, summarized as follows:

- 1). **Remote Geography** – Water systems include clean water and raw water reservoirs, pump stations, main intakes and other components that are often quite remote, and could be more difficult to cover from a perimeter security point of view due to sheer geography.
- 2). **Power** – In many cases, particularly the more remote components of a water system, there may be limited power resources, if any, necessitating difficult and expensive installation of same.
- 3). **Communication** – It is vital that there be communication of a breach in perimeter security, otherwise there can be no response from local law enforcement. In the case of more remote facilities and infrastructure it is not unusual to have no telephone or other form of communication, such as process control systems reporting back to a central point.
- 4). **Installation Cost** – Perhaps the most intimidating challenge is the cost of installing perimeter security systems where it may be necessary to run cabling via trenching, provide adequate power, install equipment, install some form of communication, and include ancillary components such as poles for cameras, etc. Monitoring of the systems also becomes a factor in cost.

Given developments in Security, Power, and Communication Technology, the Perimeter Security Challenge is no longer the “Goliath” faced by the Water Industry, and such security is now both practical and very affordable.



Sustainability:

What Has Changed?

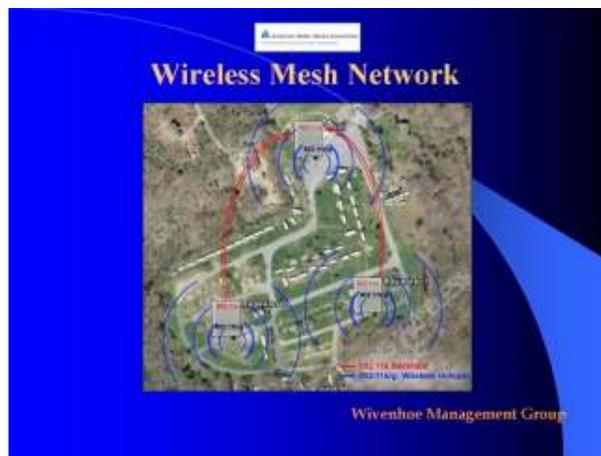
Several factors have changed the problems previously faced with Perimeter Security. They can be summarized as follows;



A. Wireless Networks and Technology

A major change in today’s perimeter security is the increasing use of **Wireless Networks** and **Wireless Mesh Networks**. Shown below is a typical Wireless Mesh Network, where three Backhaul Signal Repeaters (Items 802.11A) provide a Wireless Hotspot (WiFi area) that effectively covers the field of operation.

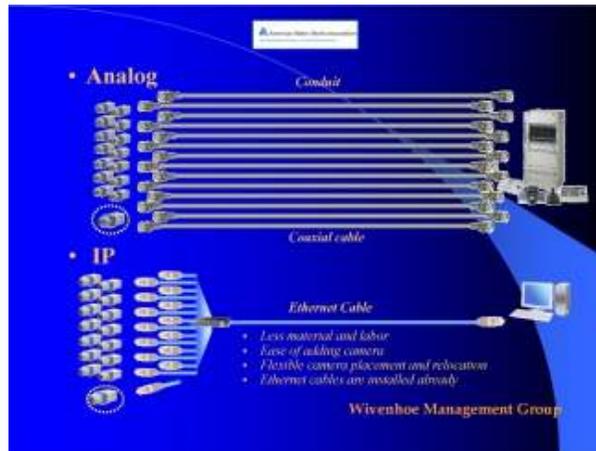
Utilizing this **Wireless Mesh Network** it would be possible to install a perimeter security system comprising wireless camera surveillance and detection units where the only installation requirement would be the need for suitable camera mounting locations, which could include the three Signal Repeater poles shown in the diagram below.



Wireless Mesh Network

Note: One element of Wireless Mesh Networks is that signals are multi-directional. Should there be a failure in signal transmission within the “Mesh,” the wireless system will find an alternative path to direct and transmit the signal.

Another new development is that of **IP (Internet Protocol) Addressable Devices**, particularly in the camera field, where it is now possible to connect cameras or other security devices via existing or new computer networks and view the results over the **Internet**. One important benefit in the use of IP addressable devices is that they can be **POE (Powered over Ethernet)**.



POE (Powered over Ethernet)

As seen in the diagram above, the benefits include less material and labor, where one Ethernet cable (CAT 5 or CAT 6), can act as a backbone for many cameras. (Previous analog cameras required a home run coaxial cable for each camera.) As stated above power for each camera can also be run over the same Ethernet cable. Analog cameras required a separate power cable either home run to each camera location or an individual power supply at each camera location.

Other benefits of IP Camera systems is the ease of adding cameras (plug-in to the network), and providing flexible camera placement and relocation. The cost savings can be very significant. In a wireless network, the use of wireless security equipment will eliminate the need for communication cabling.

B. Low Power Requirements for Security Equipment

SR Series features: Environmental friendly Eco design

Compared to current models, SR models cameras (box) can reduce up to 25% of the electric energy consumption.

Less energy consumption

Less electric energy consumption

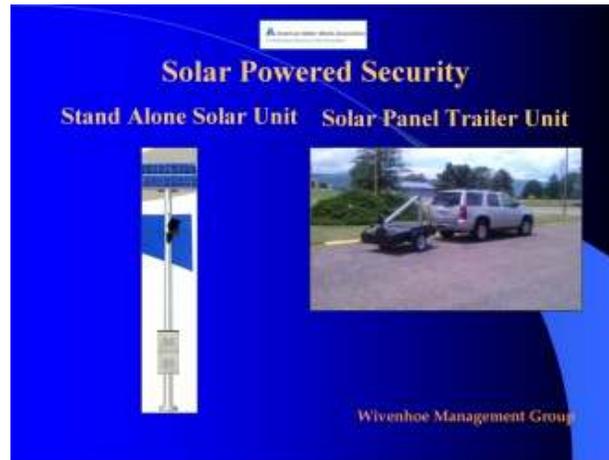
	Current	New
	WV-CF290	WV-CF310
AC220V	3.2W	2.3W
AC24V	2.9W	2.1W
DC12V	240mA	180mA
	Current	New
	WV-CF334	WV-CF344
AC24V	2.9W	2.1W
	Current	New
	WV-CF364	WV-CF374
AC24V	2.9W	2.1W

Wivenhoe Management Group

Low Power Camera Development Examples

In this diagram, it is possible to see the development of low power requirements for cameras with reductions of 25% - 28%. Many of the newer security devices employ green technology making such devices far more environmentally friendly.

C. Utilization of Sustainable Power in Security Systems



Solar Power Examples

From a water facility point of view, one of the most important changes that has taken place is in the area of Solar Powered Security Equipment providing “off the Grid” power for cameras and other security devices via solar panels, and wind driven turbines. (The solar panel or panels are mounted on a pole where there is wind driven turbine built-in to the middle of the same pole.) Seen above are photos of a standard pole mounted solar panel that is powering a complete **Deterrent Tracking Surveillance System**. Also shown is a mobile version of the same system. Thus, it would be possible and practical to set-up random camera surveillance systems in a wireless environment on a “stand-alone” basis.

These deterrent tracking surveillance systems are DHS approved and allow water facilities to meet perimeter security requirements at minimal cost and in the most rugged and remote sites.

Security Technology Development:



The primary developments in Security Technology that affect perimeter security as it applies to water and wastewater facilities are centered on the following:

A) Camera Technology

There has been a total evolution in camera technology ranging from a move away from Analog cameras to IP and Wireless cameras, HD (High Definition), Advanced Features such as Multiple H.264 compression streams, Improved DNR (Digital Noise Reduction) and ABF (Auto Back Focus), Progressive Scan, Face Detection, and Auto Dehumidification, to wider dynamic range.

Examples of camera technology are discussed in more detail commencing on **Page 10**.

B) Surveillance Deterrent Systems

The importance of being able to deter an adversary from a facility was discussed earlier. The latest development of this approach is that of new Surveillance Tracking Deterrent Systems. Future Sentry (www.futuresentry.com), an American manufacturer of the First Responder surveillance deterrent system has developed a unique system in this area.

The system is described commencing on **Page 19** of this presentation.

C) Video Motion

Developments here include the ability to mask specific areas around an object, differentiate between animals and humans, track directions, operate in extreme weather conditions, triggering zone, controlling flow, and matching patterns to name a few.

D) Low Light/Low Power Surveillance

It is almost standard with today's IP cameras to have a high sensitivity Day/Night function. In a 1.3 Megapixel mode using an F1.4, it is possible to have 0.03 fc lux (Color) and 0.008 fc lux (B/W).

E) Video Analytics/Recording

Tremendous strides have been made in Video Analytics, where it is possible to measure pixel movements that cannot be seen by the human eye that can detect breaches of security (such as human or other movement) by long range cameras at distances up to one to two miles.

Features include Motion Tracking, Target Size Filtering, Wrong Way Direction, Object Left Behind, Speed Alarm Detection and many others.

Video recording of one or more cameras can be digitally enhanced to enable zoom (pixel spreads) where there was no zoom lens on the camera, or provide camera coverage that was not visible on the camera monitor in live mode, but was captured within the camera focal view.

F) Remote Monitoring Management

It is now possible utilizing IP Digital Video Recorders and associated cameras, together with a separate IP address, to monitor all cameras on a system, either on a passive 24/7 basis, or via video events as they occur. This has great significance for water and wastewater facilities, where manpower is at a premium, and where many remote infrastructure elements are not manned at night or during weekends.

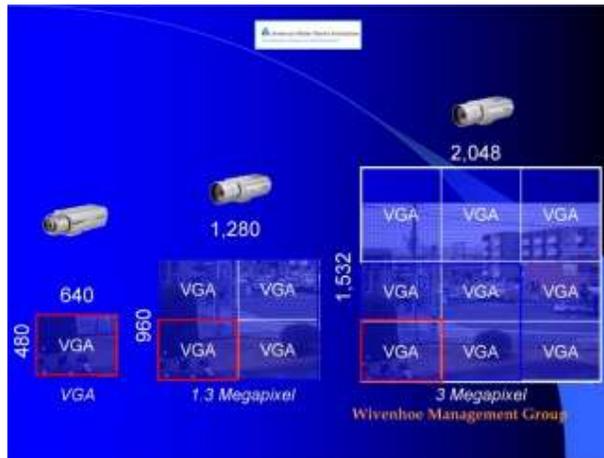


Camera Technology:

The most significant developments in camera technology include the following:

1) Megapixel Development

In IP camera systems, the advent of megapixel design can best be described in the diagram below.



The Megapixel Camera Difference

The view from a standard non-megapixel camera is measured in terms of its VGA (Video Graphics Array), an area of 480 by 640 pixels with that area being shown as a single rectangle at the far bottom left of the diagram.

1) Megapixel Development

The advent of Megapixel cameras which typically start at 1.3 Megapixel, provides four times the VGA area, or an area of 960 by 1,280 pixels, as demonstrated to the right of the standard camera in the diagram above. Using a 3 Megapixel camera, which within the last year has now become effectively the minimum megapixel level, expands a single camera VGA to 1,532 by 2,048 pixels.

With 10 and 20 specialty Megapixel cameras now available, the standard Megapixel camera will continue to increase in VGA area. It should also be noted that Megapixel cameras, even at the 1.3 level are able to read vehicle license plates at a distance.



Non-Megapixel Camera View

To put this into practical terms, the photo shown above is that from a standard camera with a VGA of 480 by 640 pixels. The photo shown below, is the same view, but using a 1.3 Megapixel camera. The difference in both clarity (resolution) and coverage is quite significant. The author has specified and implemented this type of camera into several diverse security applications, particularly perimeter security situations with considerable success.

It is now possible to design and implement perimeter security systems using a smaller number of cameras with greater efficiency and less cost.



Megapixel Camera View

2) **Low Light Capability**



Standard Megapixel Camera at Night

A major issue with perimeter security surveillance systems, has been the issue of lighting and how well camera surveillance systems work in remote areas where lighting is limited or non-existent. Remote pump stations, main intakes, water storage tanks, and particularly reservoir areas are notorious for having little or no lighting.

Some water treatment facilities that have lighting turn it off at night to reduce operating cost. There have been significant developments with both camera and associated equipment technology, that allow the latest cameras to provide reasonable video under low light conditions.

To demonstrate the low light developments, Slide 17 above shows a standard 3 Megapixel camera view at night utilizing existing street lights covering an intersection. The coverage from an area point of view is excellent, but the overall detail is less than perfect.



1.3 Megapixel Camera at Night with Technology Improvements

In the above view of the same intersection at night using a lesser cost 1.3 Megapixel camera with Digital Noise Reduction (the camera also had a better camera sensor and electronic), and minimum illumination of 1.5 lux, the difference is very substantial.

It should be stressed however, that where there is no light at all, such as at reservoirs or remote pump stations, even the best typical Megapixel camera is not going to detect an image. The answer for that environment is to use IR (Infrared) illumination, or infrared cameras either separately, or built into the camera itself.

This will be discussed in more detail on Page 15.

All Megapixel Cameras Are Not Alike:

As with many technologies, Megapixel cameras vary significantly in terms of cost and performance.



Reasonable Megapixel Camera View

The view above dramatically illustrates the advantages of Megapixel technology from a camera manufactured by Company A, and is considered a more than reasonable example of the difference between Megapixel cameras and analog cameras. However, note the greater coverage provided by a different camera from Company B, as shown in the photo below (Slide 20). This camera provides a better FOV (Field of View) due to camera sensor size and lens focal length, as well as utilizing better LDC (Lens Distortion Compensation) than Company A.

Of even more interest, the Company A camera is more expensive than the Company B camera and the warranty provided by Company B is three times that of Company A. It pays to have a qualified third party review your bids in terms of value and performance.



Another Company Megapixel Camera View – Same Location

3) **Functional Intelligence**

The latest camera technology includes features that can be referred to as Functional Intelligence, in the sense that these features can be turned on and off to provide greater performance for particular applications.

Examples include the following:



Megapixel Camera Demonstrating VIQS

VIQS (Variable Image Quality on Specified Area)

With certain cameras it is possible to not only “mask” a section of the view, but also apply high quality definition to one part of the view, and lesser quality definition to the rest of the view. As can be seen above, the designated area is the opening between the two rooms and people passing through the open area.

There is lesser interest in the roof and floor where there are no valuable exhibits.

LDC (Lens Distortion Compensation)



Compensation for Wide Angle Lens

There are occasions when it is necessary to cover as much area as possible with a single camera. Thus cameras are fitted with extreme wide angle lenses, also known as “Fish Eye” lenses. The problem with this type of coverage is the distortion induced by the Fish Eye lens.

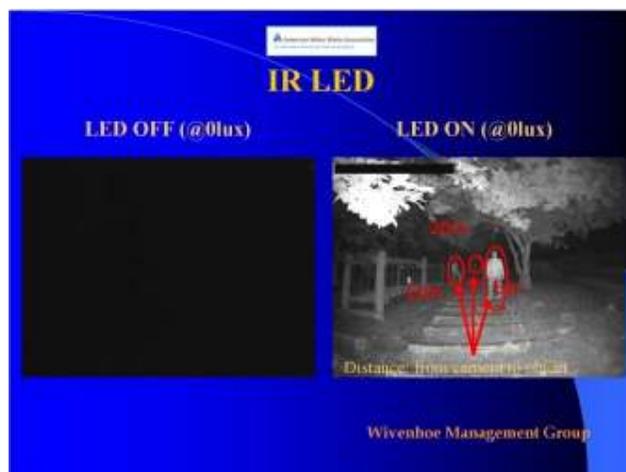
Utilizing LDC, it is now possible to significantly reduce that distortion as shown in the photo above.

4) Low Power Requirements

On Page 7, Slide #10 illustrated the dramatic reductions in power requirements achieved for new cameras. It is not just in the field of cameras that this has taken place. As already mentioned, where there is little or no light, it is necessary to consider infrared illuminators or infrared cameras, either built into the camera system or as free standing devices. The power consumption of such equipment has also seen low power development such that sustainable power sources (solar) are now able to power both the camera and associated equipment, including infrared illuminators at reasonable cost.

5) Low Sensitivity

As previously discussed IP Megapixel cameras can provide reasonable video in conditions of low light, but they cannot see in pitch darkness. To compensate for such conditions of no light, as found at many remote water and wastewater facilities, it is possible to deploy IR (infrared) illuminators. This can be built into the camera or installed as a separate device.



IP Megapixel Camera with Built-In IR

The photo shows a Megapixel camera operating in pitch darkness, and as can be seen, there is no image. However this camera also has built-in IR, and when the IR feature is switched on, figures can be seen up to 60 feet away, and quite clearly at distances of 15 to 30 feet or so.



IP Megapixel Camera & Separate Medium IR Illuminator

In the next slide above, a Megapixel camera is shown (bottom left hand corner) operating in pitch darkness, and as with the situation before, the camera generates no image. However, when a separate IR Illuminator is employed, it can be seen that the degree of IR generated light is greater than the camera with the built-in IR feature and the figure can be seen at greater range. There are infrared illuminators that can provide good illumination at hundreds of feet distance, but they are also significantly more expensive.

A further example, as illustrated below, using a separate medium distance IR Illuminator is shown in a warehouse environment. In pitch darkness the camera is unable to generate an image, other than that coming from outside distant lighting via a small panel in the overhead door. When the IR Illuminator is switched on, it is a very different situation and there is no question that an intruder is using a small flashlight to check cartons of equipment.



IP Megapixel Camera with Separate Medium IR in Warehouse Environment”

Yet another example of the use of separate IR illuminators is that shown below where a van is parked outside an entry point to a building and individuals are moving equipment from the building into the van. In pitch darkness the camera generates a limited image based on the light coming from the interior of the vehicle. However, when the IR illuminator is switched on, the van and its contents are clearly shown, as will be the individuals moving the equipment.



IP Megapixel Camera with Separate Medium IR in White Light Situation

Again, for a water industry environment, it is now possible to install sustainable perimeter systems that will operate in a wireless or IP network environment at moderate cost, with limited installation in terms of excavation and trenching, and yet provide very effective deterrent protection.

Network Video Recorder & Controller Developments

In almost every video surveillance situation, it is important to be able to record events as they unfold for later use in Court, or as an investigation tool. With IP camera systems there has been a corresponding technology advance similar to that of the cameras. Again, in the water industry an issue with perimeter security, especially at remote locations, is being able to record video events, and communicate them together by accessing and controlling any camera surveillance system from a central location.

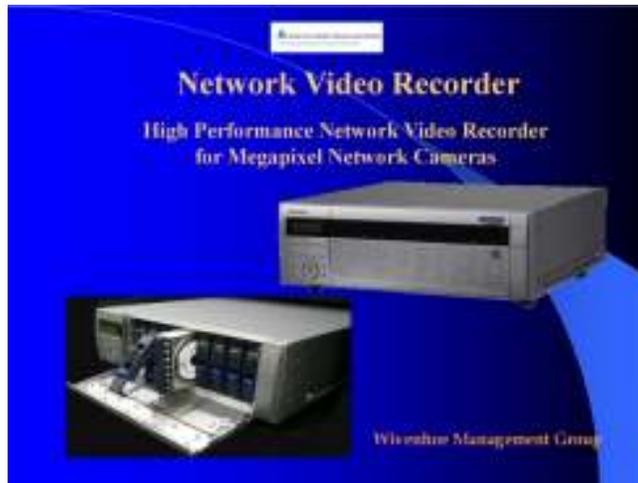
The technology has now evolved to where it is possible to transmit from a remote location via a network digital recorder with a separate IP address to a central control location with all cameras being monitored 24/7, either in a passive mode or in event mode.

In many cases, it is less expensive to have the surveillance system monitored on a passive 24/7 basis than via events.

Many security integrators also provide a Virtual Watch Tour arrangement whereby a central location can conduct monitoring of all cameras at a location, acting in a way similar to security officers walking around the perimeter.

Network Recorders have also developed in enhancement performance and capability. The Network Video Recorder and Controller shown below is able to handle up to 64 cameras and can be equipped with a total memory of 18 terabytes per unit with the ability of three units being used together for a combined memory of 54 terabytes. This particular device also has certain “analytic” features allowing management to enhance any video recording by a host of functions that include:

- Various Recording Modes
- 200 Mbps throughput
- Full Pan/Tilt, Zoom, Focus, Brightness Controls
- Audio from Cameras
- Group Browsing
- Filtered Search
- 2X 4X Digital Zoom
- SD Memory Card
- Disk Partitioning



Network Digital Recorder & Controller

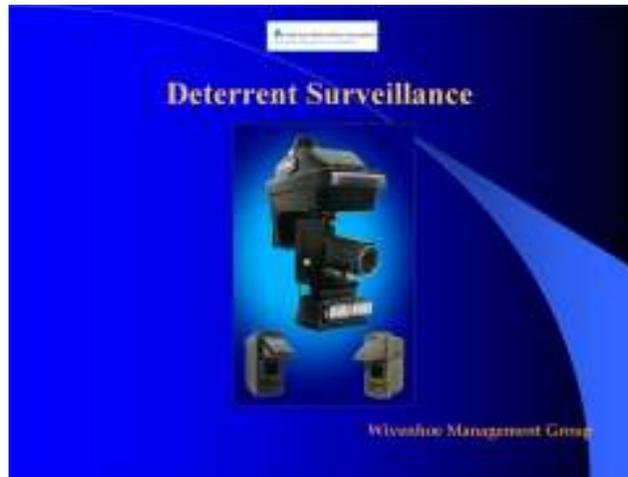
Deterrent Surveillance

Another technology development that has taken place is that of Deterrent Surveillance. The platform assembly shown below is very unique in that it can include virtually any IP or Analog camera type. It automatically reacts to any adversary intrusion (triggered by PIR wireless, sustainable sensors positioned along and throughout a perimeter area), by tracking and making the intruder aware of having been detected and now being recorded on video.

The method of operation is that an intruder sets-off a sensor somewhere along or within the perimeter which then causes the Deterrent Tracking Surveillance System to flash two sets of high intensity LED light units and then remain on as the platform tracks to the sensor area, the lights and camera pointing directly at the intruder.

The tracking system operates as a typical security guard would manually controlling a camera and following the intruder's path. The system operation tells the intruder that he or she has been detected, is now being identified and recorded by a camera, and that in all likelihood, a call has already gone out to local law enforcement and security to respond to the security breach.

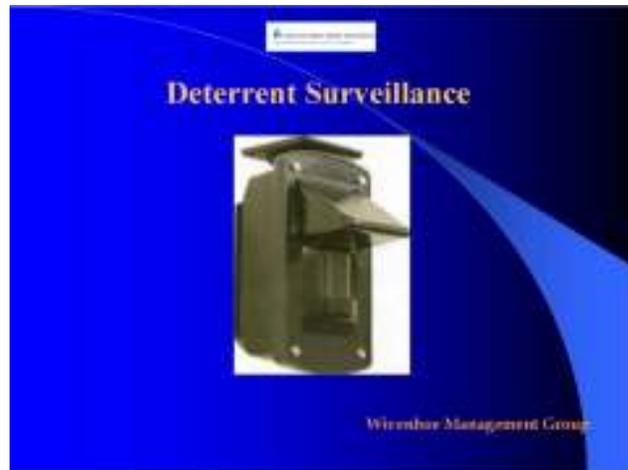
Criminals, terrorists, trespassers and other intruders share a common goal. They do not wish to be caught or identified and later apprehended. When spotted by a camera/light automatic tracking system the basic human instinct is to immediately leave the area.



Deterrent Surveillance Automatic Tracking Platform

The illustration below is a close-up of a wireless System Sensor utilized by the Deterrent Surveillance Automatic Tracking Platform which can be up to 500 feet away from the platform, is powered by a solar panel built into the top of the sensor. It is understood from the manufacturer that if the sensor has six (6) hours of sunlight exposure charging its battery, it can then operate for approximately eighty (80) days.

The author can confirm from having specified this system into a project that it works exceptionally well and in most cases where installed, the system will deter a “would be” trespasser.



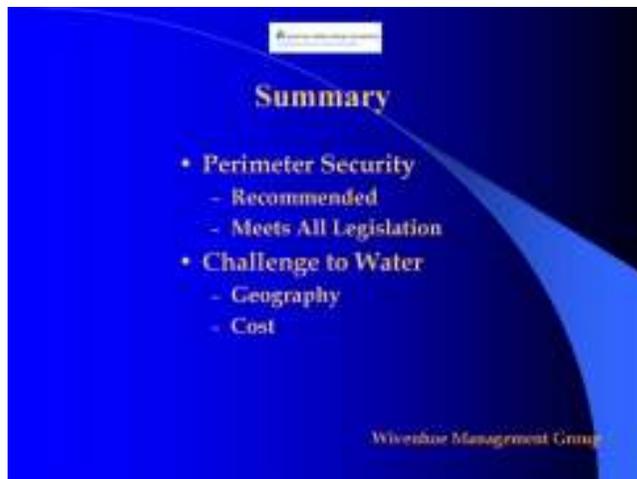
Deterrent Surveillance Automatic Tracking Platform Wireless Sensor



SUMMARY

In summary, the Perimeter represents the first line of defense in any security system. Layered security starts with the outer perimeter which is the earliest point to detect intrusion and respond. The DHS places significant importance on good perimeter security in their Standards of Performance.

Perimeter security has been a problem to the water industry for remote locations, due to the need for power and communication for perimeter security systems and an ability to respond.



To counter the issues of providing power to remote locations necessary for security surveillance and detection equipment, the corresponding high cost, as well as providing an effective communication system, it has been necessary to introduce an alternative arrangement to installing and powering remote perimeter security systems. There have been two important developments on this front, namely Wireless Networks and stand-alone Sustainable Power Sources, particularly Solar charging a battery source.

With Wireless Networks and security equipment that is IP addressable, and as such provides POE (Power over Ethernet), it is possible to set-up appropriate wireless and local IP surveillance networks utilizing sustainable power, not only reducing very significantly the cost of installation, but also making it a practical solution for Water Perimeter Security Systems.



New security technology is now available, concentrating on IP Camera Surveillance and Detection systems, including specific camera developments such as HD, Megapixel performance, Low Power, DNR, H.264 Multiple Streams, ABF, Progressive Scan, Face Detection, Wide Dynamic Range, Auto Dehumidification, and Low Sensitivity (Light) developments, LDC, and others.

All of these developments (as well as Video Motion, Video Analytics and Digital Video Recording, Deterrent Surveillance systems, IR Illumination, and Remote Monitoring Management) combine to allow water facilities to acquire and install Perimeter Security systems, at remote locations without the high cost of excavation and trenching to run cables for power and communication, utilizing camera surveillance as the most practical and least costly method of perimeter security, and able to be monitored from a third party central point at low to moderate cost.

The end result also leads to Environmental Friendly security that may well qualify for specific grant funding as a result.

For questions and further information, please see below:

