

WIVENHOE MANAGEMENT GROUP

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

EMAIL: info@wivenhoegroup.com

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

**A PRESENTATION PAPER FOR THE PENNSYLVANIA AWWA
CONFERENCE AT HERSHEY, PA., BY DAVID S. McCANN,
PRINCIPAL CONSULTANT WITH THE WIVENHOE
MANAGEMENT GROUP SECURITY CONSULTANTS**

Following the recommendations emanating from the multitude of Vulnerability Assessments (VA's) carried-out in the Water Industry, and mandated by the EPA in accordance with the Public Health Security Bioterrorism and Response Act (PL 107-188) June 2002, a number of water utilities have proceeded to implement those same recommendations.

In the majority of cases, the recommendations included the installation and implementation of new security systems, measures, and equipment that were considered necessary to reduce overall risk, particularly with respect to critical assets, to an acceptable risk level. **(Fig 1)** illustrates the Sandia Laboratory risk formula as prescribed in RAM-W VA methodology.

In a large number of cases security improvement recommendations included an array of security equipment and concepts. This includes Electronic Access Control, CCTV Camera Surveillance, Surveillance Monitoring and Recording, Perimeter Fencing, Intrusion Detection, and other security systems and equipment. The water utilities that installed security may have, without realizing so, **increased their Legal Liability as a result.**

Not only is this a real possibility, it may have also opened-up the precarious door known as "**Negligence**". Where Negligence is proven to be the fact, a company or utility is now facing more serious **Damages** awarded by a jury that is going to favor the plaintiff to a large extent of the time.

The reason for the increased liability may fall under several different categories as follows:

- 1). New security systems did not meet the necessary level of protection required

to counter VA identified **Threat Levels**

HAS YOUR NEW SECURITY SYSTEM INCREASED
YOUR FACILITY'S LIABILITY?

- 2). Security Equipment installed is considered inadequate or inappropriate to counter those same VA identified **Threat Levels**
- 3). The Security System has been incorrectly installed
- 4). Equipment such as cameras and motion detectors are incorrectly positioned
- 5). New Security Systems do not provide sufficient coverage of all key areas
- 6). The Security System(s) is not designed to Industry Standards
- 7). There are gaps in the Intrusion Detection Perimeter

We will look at the various reasons as to why your liability may have increased after installation of your new security systems and equipment in much greater detail shortly. The avoidance of such increased liability could have been achieved by applying **Good Security Design Criteria** before purchasing and installing equipment that you thought was the answer.

Many security professionals will advise any entity considering the installation and implementation of new security systems to first of all make sure that there are design objectives and defensible purpose to the systems, and more importantly, make sure that there is sound, appropriate, and consistent **Security Design Criteria supporting your systems**.

MANY SECURITY SYSTEMS ARE INSTALLED WITHOUT BEING PROPERLY DESIGNED, AND UNFORTUNATELY, WITHOUT HAVING PROPER DESIGN CRITERIA.

As illustrated in **(Fig 2)**, you do not want to be in the “hot” seat attempting to defend a law suit alleging that your security measures were inadequate and did not do the job when it was most needed.

The reasons that your new security systems may have now increased your liability can be summarized under the four main effects of not having good design criteria. These are:

- A. **Inadequate Security to Meet Threat Level**
- B. **Faulty Security System Design**
- C. **Inability to Support Installed Security System(s)**

D. **Omissions in the Security System(s)**

**HAS YOUR NEW SECURITY SYSTEM INCREASED
YOUR FACILITY'S LIABILITY?**

Industry Quote:

Many security consultants feel that implementing security systems without design criteria is unwise. As an example, Steven S. Wilder, President and C.O.O. of Sorensen Wilder & Associates, a noted authority in the security industry had this to say:

“In the security environment of “Post 9/11”, and given the Media scrutiny of all key infrastructure, it would be unwise if not reckless, to implement new security systems without adequate design, and good design criteria in keeping with industry standards”

Looking in more detail at the four main reasons for possible **Increased Liability:**

Inadequate Security To Meet Threat Level

Inadequate security may involve any of the following:

Failure to Detect:

If the installed security system(s) fail to detect an adversary entering the facility, there will be no response action set in motion. As such, the facility will be seen as having failed to adequately secure the property in accordance with industry standards, and in an acceptable manner. Such an allegation opens the door to **Negligence** as having already carried-out a VA, you were very aware of the security shortcomings.

Blind Surveillance Spots:

Depending on the design basis (also know as security functional concepts) of the security system(s), and the CCTV Camera Surveillance element of that system(s), it is very easy to miss important areas that should be under surveillance. It is also possible to have installed cameras where the overall field of view of a particular camera fell short of its target. Fixed cameras, as an example, rarely provide meaningful detail beyond 200 ft.

Inadequate Perimeter Security:

Perimeter security generally includes fencing, gates, CCTV camera surveillance, intrusion alarms, etc. If the facility encompasses an extensive perimeter, it may not be possible for a variety of reasons to secure the entire perimeter. (It is also possible in certain situations that it may not be practical or a requirement to secure the entire perimeter).

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Inadequate Security To Meet Threat Level

Inadequate Perimeter Security:

In the event that the perimeter security system fails to indicate a breach of security or there was a breach of security at a point where there was inadequate security measures in place, you are again facing possible grief including allegations of **Negligence**.

No Security at a Given Critical Asset:

If the critical asset was intentionally omitted in the security system countermeasures for appropriate reasons consistent with the security design criteria, then such an event can be defended but if the critical asset was simply missed or was passed-over for financial reasons, etc., then the situation will be difficult to justify in the event of an incident at that critical asset.

Inappropriate Equipment:

The security system includes a fence intrusion system as an example but the environment is such that any form of fence intrusion system will simply provide a myriad of false alarms. The result is that the system is either ignored or deactivated.

The author has seen many such instances. Your investment in at least part of your perimeter security system(s) is questionable, and worse, there is no detection at the perimeter of your property and an incident occurs that is directly related undetected unauthorized entry. That is a serious matter and may lead to allegations of **Negligence**.

Examples of Inappropriate Equipment include:

- a) **Exterior Door Hinge (Fig 3)**- These hinges are easily unscrewed leaving the door able to be removed from the frame.
- b) **2 Inch Wire Mesh on Fencing (Fig 4)** –Wide wire mesh is simply providing foot holds for an individual intent on climbing the fence. This is one of many items that can leave your fencing inadequate against the purpose for which it was installed (to prevent unauthorized entry into the site).

- c) **Alarm Wiring (Fig 5)** – In this example where the actual alarm point was not supervised, the wiring can be compromised by cutting thus providing an adversary with plenty of time to force the door.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY’S LIABILITY?

Inadequate Security To Meet Threat Level

Examples of Inappropriate Equipment include:

- d) **Door Contacts (Fig 6)** – Wherever possible, it is recommended that door contacts be of the concealed variety. Surface door contacts, particularly when the wiring is exposed and not protected by conduit is a target for mischief or deliberate cutting of the wires.
- e) **Difficult to Protect (Fig 7)** - In this example, a structure housing a main valve and access point to a facility’s Main Inlet stands alone on a public access beach area. Providing protection in this situation can be achieved, but at substantial cost.

An Example of Good Appropriate Equipment – (Fig 8)

In this situation where the intent was to provide a perimeter fence that would also prevent heavy vehicles from crashing through the fence but avoiding the high cost of High Security Fencing, “Jersey” barriers have been installed along the front of the fencing providing both an inexpensive vehicle restraint system and a powerful Deterrent.

Does Not Provide Adequate Protection to Meet Identified Threat Level:

Your VA identified the **Threat Level** in terms of the **Design Base Threat**, and further identified the most critical assets that would seriously jeopardize the continuing operation of your water system if those assets were destroyed or substantially damaged. Your new security system(s) may be the major means by which you will provide adequate security and counter measures to protect your systems operations, and critical assets.

In the event of an incident, particularly one that causes serious damage to a particular asset, the incident is likely to be viewed as a failure to provide adequate security to protect against the threat level. As a result, the facility will likely face legal consequences which may also include allegations of **Negligence**.

Faulty Security System(s)

The second major reason for increased liability is that of a Faulty Security System. Under this heading we have the following:

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Faulty Security System(s)

Does Not Work As Expected:

The Utility gave instructions to procurement to acquire a security system to meet the VA recommendations.

Procurement put together an RFP to local security contractors to provide a new security system with the contract going to the lowest bidder. The security contractor configured the new security system as best they could to meet the intent of the RFP with overall pricing playing a major role in their selection of systems and equipment.

All of this was based on the following:

- A. The Utility's interpretation of the necessary security improvements (new system (s) required to meet VA recommendations.
- B. Procurement's interpretation of the instructions from senior Utility managers on what type of new security system to acquire.
- C. The security contractors' interpretation of what they should put forward as the new security system that would appear to meet the Utility's requirements, and at the same time win the bid.

Unfortunately, in these circumstances, the end result is usually far from that originally envisaged by the Utility Management.

No Integration:

It is normally important that the various security systems deployed, i.e., alarm system, electronic access control system, security intercom system, CCTV camera surveillance, security data and video communications, and others be integrated together to allow a single operator to control all elements. This does not happen by accident but is designed into the system, and is an essential design criteria parameter. If an operator is required to try and control several non integrated security systems as well as their normal operator function, the likely result will be confusion at best.

Monitoring Inadequate:

This is very often the case with CCTV Camera Surveillance systems where a single operator is expected to monitor a multitude of video monitors which may have multiple camera views or which may be sequencing through a number of cameras on each screen.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Faulty Security System(s)

Monitoring Inadequate:

Great care should be exercised in the design of such systems both to intent and to configuration. There are many liability issues attached to CCTV Camera Surveillance, and to achieve effective results from such systems, it is necessary to do your homework, and make sure that your goals for such systems are based on design criteria formulated from the results of the VA, are feasible, sensible, and appropriate for camera surveillance that meet the functional objectives of the CCTV system.

Wrong Equipment:

As with many system applications, “garbage in, garbage out” is reflected in the Security Industry too. If you employ a camera with a focal length lens that is perfectly ok for reasonable identification of an object at perhaps 80 feet, and has high resolution, but then attempt to use that same camera at a distance of 120 feet, the identification of the object at that distance will be unsuccessful.

Likewise, issuing a proximity card to an individual to be used at a card reader point by that individual only, but where such cards can be passed between users (often the case at Colleges with students) will not do the job unless there is a further method to limit the use of that card to a particular individual such as a unique keypad ID to be used in conjunction with the card or where camera confirms that the person seeking entry is indeed the holder of that access card.

SECURITY PROFESSIONALS AGREE GOOD SECURITY DESIGN AND DESIGN CRITERIA IS ESSENTIAL TO SUCCESSFUL SECURITY SYSTEM OPERATION.

(Fig 9) provides a few examples of such consultants.

Examples of Good Security Design and Design Criteria:

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Examples of Good Security Design and Design Criteria:

Perimeter Detection:

Before deploying a Perimeter Detection system, first define the design criteria or functional objectives based on the identification of the vulnerabilities that the fence and fence detection system are suppose to defend against, then examine landscape elevations, obstructions, climbing aids, available setbacks on each side of the fence, etc., review weather conditions in the area to identify worst case environmental conditions, determine the perimeter length to be protected, identify the extent of interface with other systems, consider the best detection technology type for the application, review the method and location for system monitoring.

These and many other questions should be asked and answered before investing in a particular perimeter detection system, and above all, ensure that the system goal is feasible, and obtainable. Perimeter detection is of vital importance in a security system, and whatever detection system is chosen, it **has to work properly**.

CCTV Camera Surveillance:

Points that need to be considered carefully before implementing a CCTV Camera Surveillance system include the following:

1. What is the goal of the system? Is it broad perimeter surveillance; specific identification of individuals at particular locations; interior corridor coverage; exterior doorway coverage; covert surveillance, stairway coverage, etc. Knowing what you want to achieve with a surveillance system, and defining precise design criteria for such systems are vital for their success.
2. Do you require exceptional high resolution to achieve precise identification with your video system? The lower the resolution, the less able you are to identify what you are looking at. Low cost cameras offering limited resolution have resulted in many court cases against the owners of the surveillance system due to an inability to clearly identify an individual in an incident situation.
3. Field of View is important in positioning CCTV cameras. The field of view, resolution, and far field capability of cameras is very different from the capability of the human eye. Assuming a high resolution camera, the field of

view, resolution, and far field capability is determined, to a large extent, by the lenses quality and focal length.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Examples of Good Security Design and Design Criteria:

CCTV Camera Surveillance:

4. Wide-angle lenses help where it is necessary to obtain a wide field of view or large scene, however, scene objective size will be small (i.e., people and scene areas at the far field will be small), thus making identification difficult. Telephoto lenses, on the other hand, have a narrow field of view but scene objective size at the far field will be large thus providing a greater potential for identification of individuals and other objects.
5. It is also necessary to consider the positioning and quantity of cameras to avoid blind spots and obtain the desired coverage.
6. The issue of Fixed Cameras versus Pan-Tilt-Zoom (PTZ) Cameras can often be the difference between adequate and inadequate surveillance protection. Where contiguous perimeter coverage is required, it can be more effective to use sufficient fixed camera coverage as opposed to using conventional PTZ or High Speed Dome (PTZ) cameras. The reason being that PTZ cameras do not provide simultaneous contiguous coverage (full coverage all the time) Since a PTZ camera provides a limited coverage, if an unauthorized individual is attempting to get into a site, the PTZ camera may miss observing because the individual may be out the field of view of the camera (the camera is pointed in another direction at that moment
7. Many CCTV Camera Surveillance systems are not monitored live but are used to record events historically that can then be reviewed at a later date. In fact, the likelihood of someone monitoring live cameras, and actually looking at a particular camera view the instant that something starts to happen, and further recognizing that something is starting to happen, is extremely low.

Although digital video recording has replaced VHS recording in most situations, it is still important to ensure that your monitoring system is properly configured to record in the way that you wish and for an adequate time period, at a high resolution, and sufficient frame rate. The longer that you intend to maintain video recording such as 30 days before recording afresh, the higher the recorded resolution, and the higher the frame rate, the more hard disk space will be required for the system.

8. Lighting is a fundamental requirement in the use of CCTV camera surveillance.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Examples of Good Security Design and Design Criteria:

CCTV Camera Surveillance:

However, we have observed inadequate lighting at many sites that include CCTV surveillance. Any surveillance system is essentially worthless without adequate lighting. Good lighting for cameras is essential, and generally, it will require more than an average lighting level of two foot candles. It is recommended that a light meter be used to determine adequate lighting for the CCTV system. Without adequate light, there can be no clear picture.

7. In situations where site visible lighting would cause light intrusion to neighbors, non-visible infrared lighting can be employed. Also, technologies as infra-red cameras that will operate in total darkness can be used; but many forms of visible and non-visible lighting in the area will tend to create glare (blooming effects) on the infra-red image. Again, care has to be taken in designing such systems, and in defining the objective.

Alarm Systems:

1. All alarm systems should be supervised in the event that there has been tampering with a device or with any part of the wiring, and should also be equipped with two means of communication. If using a network for communication, it is important to have an alternate telephone link in the event that the network develops problems. Alarm panels should not be located in unsecured closets or unsecured rooms. An alarm system is of little value if the alarm panel is unprotected and can be compromised.
2. The positioning of devices such as motion detectors or acoustic sensors, etc., needs to be planned in advance, and to have proper design criteria that will support the particular positioning of such devices.
3. Motion detectors deserve special mention as many detectors are completely misused in systems. Correctly positioned detectors will pick-up movement at varying distances dependent on the detector design. However, elements, such as sunlight crossing the detector or proximity to heat vents, may cause false alarms.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Examples of Good Security Design and Design Criteria:

Alarm Systems:

Even if you are not having a security professional design the system for you, it would be a wise investment to have such a person look at your planned security system and offer comments before you proceed to purchase and installation.

Access Control:

1. **Electro-Magnetic Lock Devices** are one of several types of access controlled lock devices that can be used in conjunction with electronic access control systems. Electro-magnetic locks require fire alarm system interface to meet Fire Code requirements. Some States not only require an exit device such as an Egress Motion Detector but also require an emergency exit button adjacent to the access controlled door in the event that there is a problem with the electro-magnetic lock.

The author has also witnessed many instances of the electro-magnetic lock units being mounted on the outside of the door instead of the interior side. Mounted on the exterior side allows an adversary to simply unscrew the lock from the door. Certain types of doors require custom size electro-magnetic locks due to space constraints at the top of the door. It is possible to mount magnetic locks at the side of doors, but it is not recommended as the doors can be levered open.

2. **The Typical Access Control Reader Device** is used to identify the card holder, permit access and provide other functions. A good example of using a proximity card reader to positively identify an individual is to include a proximity card reader with a keypad where the individual has to also key-in their personal four or five digit personal PIN number before access is granted.

If using Biometric readers, remember that most biometric readers take longer to operate and that certain types of biometric reader are frowned upon by union membership due to perceived health effects.

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Examples of Good Security Design and Design Criteria:

Identification:

1. Utilizing identity cards is strongly recommended in virtually every situation as it is an excellent way to isolate strangers in a facility that are clearly out of place as they have no identity card.

Good design criteria will consider color coded ID cards that can be seen at a distance such as bright yellow or orange to identify, for example, airport workers that are authorized to be inside the airport perimeter close to active runways.

Using symbols that represent membership of certain clubs or after-school activities can be a good way to help persuade students to wear their ID badges.

Use of good design criteria coupled with a clear understanding of the countermeasures and security system objectives will go a long way to preventing the situation discussed earlier where the firm's Procurement Department attempts to understand what the undefined security objectives and undefined security equipment are to be able to create a meaningful RFP. The result is the generation of an inadequate RFP that the security contractor attempts to understand. Customarily, the security contractor will respond by providing equipment and systems that provides the most profit for them and what they believe will win the bid.

Unfortunately, in such circumstances, particularly when there has been an incident and you are sitting in the "hot" seat in open Court; you are the one that will have to answer difficult questions, such as:

Likely Questions in Court:

- A). **Why Did You Use This Equipment?** As applied to the following:

Types and Locations of Camera(s)

Types and Locations of Motion Detector(s)

The Type and Configuration of the Video Recording System

Types and Locations of Intrusion Detection Equipment
Types of Fences and Other Barriers
HAS YOUR NEW SECURITY SYSTEM INCREASED
YOUR FACILITY'S LIABILITY?

Likely Questions in Court:

Types and Locations of Access Control
Other Equipment

- B). **Explain The Reasons for Installing This Type Of Security System?**
- C). **Why Did Security Only Attempt To Cover The Outer Site Perimeter?**
- D). **Why Were Insider Threats Ignored?**
- E). **Why Were There No Personnel Electronic Access Control System Restrictions?**
- F). **What Was The Design Criteria For Your Security System?**

IF YOU ARE UNABLE TO REASONABLY ANSWER ANY OF THE QUESTIONS POSED ABOVE CONSISTENT WITH SECURITY INDUSTRY GUIDANCE, REQUIREMENTS, AND STANDARDS, IT IS GOING TO BE DIFFICULT TO CONVINCE A JURY THAT YOU AND YOUR FACILITY ACTED IN A REASONABLE MANNER IN IMPLEMENTING AN EFFECTIVE SECURITY SYSTEM.

The Importance of Good Design Criteria:

Taking the time to assess the main protection objectives of a new security system, establish good design criteria for the security system, utilize appropriate systems and equipment that will operate successfully in your facility's specific operational environment, and set goals for the system that are feasible and practical will achieve the following:

- Justify and explain why various decisions were made ~~take~~ in the design of the system based on weighted objectives
- Provide qualified reasoning for all aspects of the security system
- Clarify and further justify why the specified security system(s) meet the Level of Protection against the identified Threat Level and identified Vulnerabilities

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

What Do I Do If My Security System(s) is already installed?

Security upgrades and corrections can be achieved where the security system or systems are already installed and implemented but there is protection validity due to the lack of professional design and adequate design criteria. It is not too late to correct and improve the various security measures to ensure that the system(s) can be substantially and properly defended in the event of an incident.

There are several options available to you as follows:

- 1). Have an experienced security professional Review the Security System(s)**
- 2). Prepare Sound Security System Design Criteria**
- 3). Modify the installed system and equipment to meet the design criteria**
- 4). If necessary, install additions that will then allow your security system to meet design criteria**
- 5). Consider the addition of appropriate equipment and measures that will provide a clear Deterrent to “would-be” adversaries**

Summary

In summary, this paper makes the case that where a facility has followed-up with its respective Vulnerability Assessment recommendations concerning the upgrading and implementation of new security systems; it may have resulted in the facility increasing its liability.

The basis for such increased liability results from the creation of new security measures that were not designed to security industry guidance, requirements, and standards, and that do not include adequate design criteria. The primary elements of any new security system tend to include:

Access Control
CCTV Camera Surveillance
Site Perimeter Fencing and Other Barriers
Site and Site Perimeter Lighting

Site Perimeter and Facility Intrusion Detection

HAS YOUR NEW SECURITY SYSTEM INCREASED YOUR FACILITY'S LIABILITY?

Summary

It was further discussed that the lack of Good Design Criteria can create four major problems, being:

- 1). **Inadequate Counter Measures to Meet Threat Level**
- 2). **Faulty Security System Design**
- 3). **Inability to Support the Installed Security System**
- 4). **Possible Legal Consequences**

This paper put forward various examples with respect to Inadequate Security as well as addressing Faulty Security Design, the likely Inability to Support the Installed Security System, and then discussed Possible Legal Consequences.

This paper also discussed Proper Design Criteria and gave examples of issues that will affect such design criteria. These issues included:

Site Perimeter Detection
CCTV Camera Surveillance
Alarm Systems
Access Control
Identification

In the legal consequences section, this paper also gave examples of likely questions that would be asked in the event of an incident ranging from use of specific equipment to who had particular clearance via the electronic access control system.

The conclusion is that **Proper Design Criteria Consistent With Security Industry Guidance, Requirements, and Standards** will provide solid answers to such questions, and will alleviate or reduce the risk of legal action.

This paper also dealt with the issue of what can be done if the new security system is already installed, but without the benefit of Proper Design Criteria, and offered a number of options that included utilizing security professionals to:

Review the Security System
Prepare Sound Design Criteria

**Modify and Upgrade Equipment
Add to System Configuration**
**HAS YOUR NEW SECURITY SYSTEM INCREASED
YOUR FACILITY'S LIABILITY?**

Summary

Add a Deterrent Factor to the System

Finally the paper concluded that the **Benefits of Proper Design Criteria** would be:

- **Sound Basis of Design to Industry Guidance, Requirements, and Standards**
- **Provides the Foundation for a Proper Security System**
- **Establishes Optimum Protection Level in Keeping with the Identified Threat (DBT) and Vulnerabilities**
- **Provides Clear Reasons for Types of Equipment and Positioning of Such Equipment**
- **Likely to Prevent Possible Legal Action in the Event of an Incident**

Questions and Contact Information:

Questions on any part of this presentation and paper can be addressed to the following:

David S. McCann -

Principal Consultant & Vice President
dmccann@wivenhoegroup.com

Wivenhoe Management Group -
www.wivenhoegroup.com

One Pheasant Run
Clarksburg, NJ 08510-1709
Tel: (609)-208-0112

Fax: (609)-208-1295