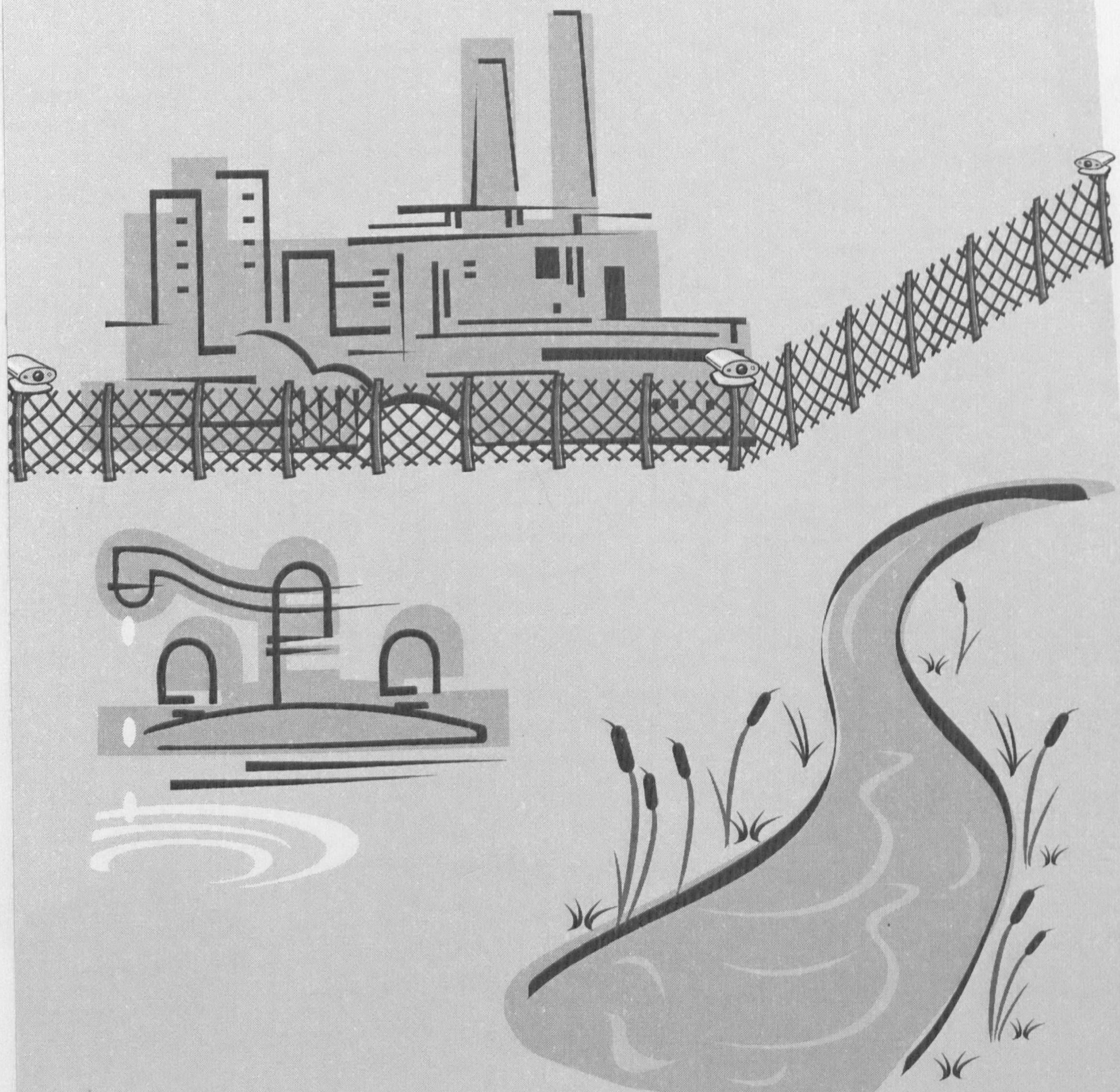
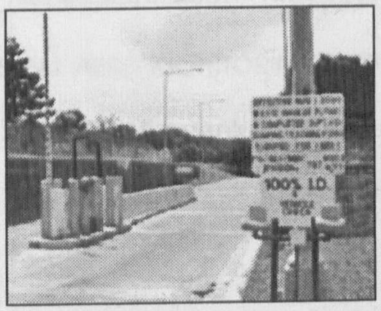
UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

SECURITY PRODUCT GUIDE

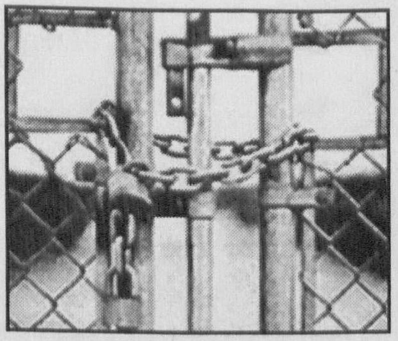


EPA

SECURITY PRODUCT GUIDE



Recent events have created a heightened awareness of security at the nation's critical infrastructure, including its drinking water and wastewater systems. These systems are potentially vulnerable to different kinds of natural disasters and terrorist threats. EPA has developed a series of Security Product Guides to assist treatment plant operators and utility managers in reducing risks from, and providing protection against, possible natural disasters and intentional terrorist attacks.



The guides provide information on a variety of products available to enhance physical security (such as walls, gates, and manhole locks to delay unauthorized entry into buildings or pipe systems) and electronic or cyber security (such as computer firewalls and remote monitoring systems that can report on outlying processes). Other guides present information on monitoring tools that can be used to identify anomalies in process streams or finished water that may represent potential threats. Individual products evaluated in these guides will be applicable to distribution systems, wastewater collection systems, pumping stations, treatment processes, main plant and remote sites, personnel entry, chemical delivery and storage, SCADA, and control systems for water and wastewater treatment systems.

DISCLAIMER

The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

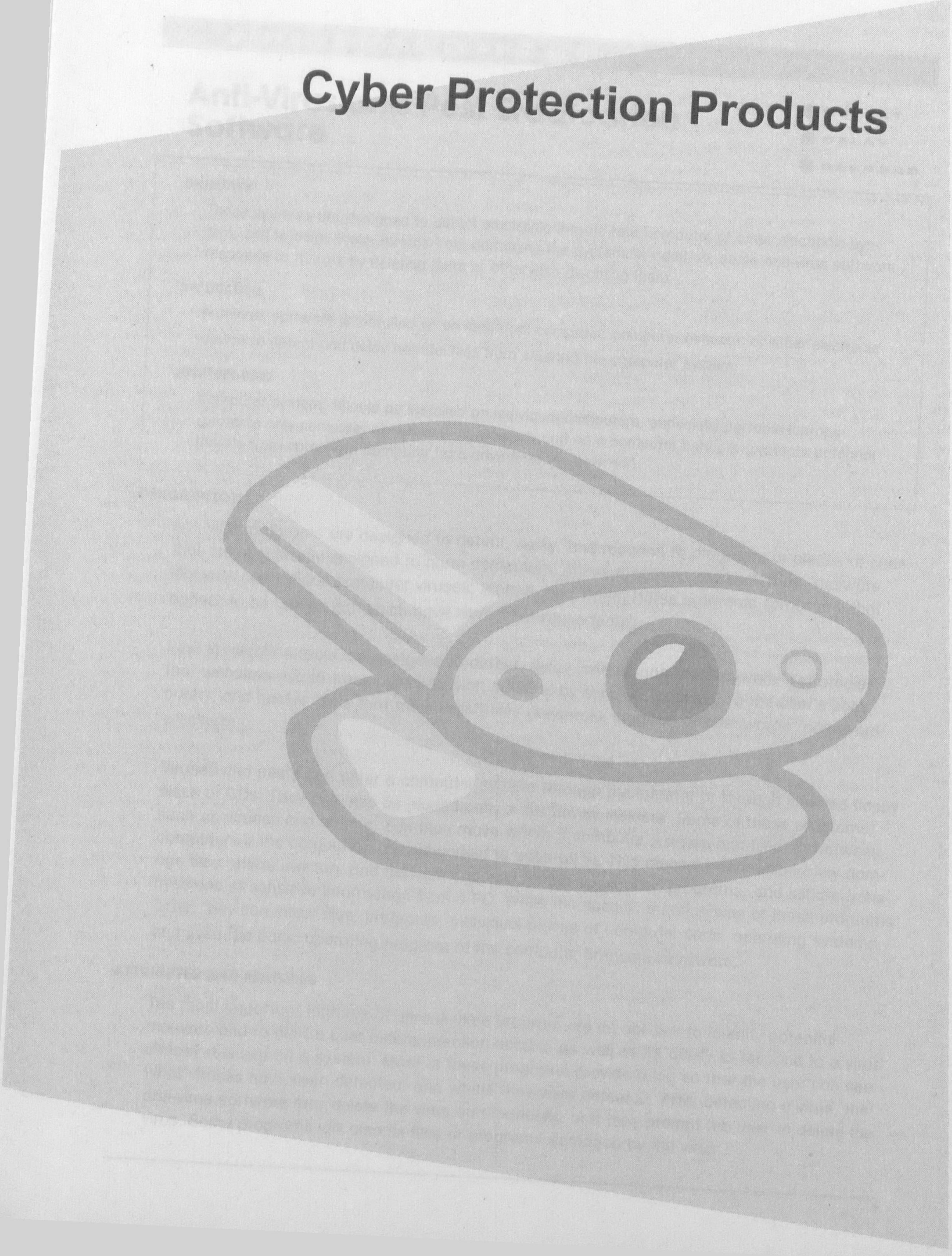
CONTENTS

CYBER PROTECTION PRODUCTS

PHYSICAL ASSET MONITORING AND CONTROL PRODUCTS

WATER MONITORING PRODUCTS

Cyber Protection Products



Anti-Virus and Pest Eradication Software

● DETECT
● DELAY
● RESPOND

OBJECTIVE

These systems are designed to detect electronic threats to a computer or other electronic system, and to delay these threats from damaging the system. In addition, some anti-virus software responds to threats by deleting them or otherwise disabling them.

APPLICATION

Anti-virus software is installed on an individual computer, computer network, or other electronic device to detect and delay harmful files from entering the computer system.

LOCATION USED

Computer system. Should be installed on individual computers, especially portable laptops (protects only computer on which it is installed) and on a computer network (protects potential threats from entering a computer hard drive from the network).

DESCRIPTION

Anti-virus programs are designed to detect, delay, and respond to programs or pieces of code that are specifically designed to harm computers. These programs are known as "malware." Malware can include computer viruses, worms, and Trojan Horse programs (programs that appear to be benign but which have hidden harmful effects).

Pest eradication tools are designed to detect, delay, and respond to "spyware" (strategies that websites use to track user behavior, such as by sending "cookies" to the user's computer), and hacker tools that track keystrokes (keystroke loggers) or passwords (password crackers).

Viruses and pests can enter a computer system through the internet or through infected floppy discs or CDs. They can also be placed onto a system by insiders. Some of these programs, such as viruses and worms, can then move within a computer's drives and files, or between computers if the computers are networked to each other. This malware can deliberately damage files, utilize memory and network capacity, crash application programs, and initiate transmissions of sensitive information from a PC. While the specific mechanisms of these programs differ, they can infect files, programs, individual pieces of computer code, operating systems, and even the basic operating program of the computer firmware/hardware.

ATTRIBUTES AND FEATURES

The most important features of qn anti-virus program are its abilities to identify potential malware and to alert a user before infection occurs, as well as its ability to respond to a virus already resident on a system. Most of these programs provide a log so that the user can see what viruses have been detected, and where they were detected. After detecting a virus, the anti-virus software may delete the virus automatically, or it may prompt the user to delete the virus. Some programs will also fix files or programs damaged by the virus.

Various sources of information are available to inform the general public and computer system operators about new viruses being detected. Since anti-virus programs use signatures (or snippets of code or data) to detect the presence of a virus, periodic updates are required to identify new threats. Many anti-virus software providers offer free upgrades that are able to detect and respond to the latest viruses.

COST

The cost of anti-virus software packages varies depending on the complexity and level of protection provided (i.e., some anti-virus software may be able to respond to new viruses because they respond to certain patterns in the computer code). Shareware (software that can be downloaded for free from the internet) anti-virus programs can be obtained via the internet free-of-charge. These free programs provide a basic level of protection. Individual PC anti-virus programs, which provide additional virus protection, range from $25 to $60. Network versions for a typical system of 10-25 computers range from $250 to $1000 or more. Installation and maintenance costs will vary depending on the ease-of-use, setup and configuration. Installation time ranges from a few hours for an individual PC to 8-40 hours or more of man-hours for a small to medium size network of workstations. Installation time varies depending on the level of computer software and hardware skills of the installer. Ongoing maintenance of anti-virus systems typically requires computer support time of several hours or more per month.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

McAfee Corporation/Network Associates
3965 Freedom Circle
Santa Clara, California 95054
(972) 963-8000
www.mcafee.com

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, California 95014
(408) 517-8000
www.symantec.com

PestPatrol, Inc.
453 Lincoln Street
Carlisle, Pennsylvania 17013
(717) 243-6588
www.safersite.com

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, California 95014
(800) 228-5651
www.antivirus.com

Firewalls

● DETECT
● DELAY
○ RESPOND

OBJECTIVE

Firewalls are used to detect unauthorized connections or access to a computer system or to specific computer files, and to deny that access. This can delay unauthorized access to the system.

APPLICATION

These systems are installed on a facility's computer system to detect electronic threats to a computer or other electronic system, and to delay these threats from damaging the system. In addition, some anti-virus software responds to threats by deleting them or otherwise disabling them.

LOCATION USED

Computer system. Can be installed on individual computers (protects only computer on which it is installed) or on a computer network (protects all computers on network).

DESCRIPTION

A firewall is an electronic barrier designed to keep computer hackers, intruders, or insiders from accessing specific data files and information on a utility's computer network or other electronic/computer systems. Firewalls operate by evaluating and then filtering information coming through a public network (such as the internet) into the utility's computer or other electronic system. This evaluation can include identifying the source or destination addresses and ports, and allowing or denying access based on this identification.

There are two methods used by firewalls to limit access to the utility's computers or other electronic systems from the public network:

- The firewall may deny all traffic unless it meets certain criteria; or
- The firewall may allow all traffic through unless it meets certain criteria.

A simple example of the first method is to screen requests to ensure that they come from an acceptable (i.e., previously identified) domain name and Internet Protocol address. Firewalls may also use more complex rules that analyze the application data to determine if the traffic should be allowed through. For example, the firewall may require user authentication (i.e., use of a password) to access the system. How a firewall determines what traffic to let through depends on which network layer it operates at and how it is configured. Some of the pros and cons of various methods to control traffic flowing in and out of the network are provided in Table 1.

Table 1: Pros and Cons of Various Firewall Methods for Controlling Network Access

Method	Description	Pros	Cons
Packet Filtering	Incoming and outgoing packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded. There are two type of packet filtering: static (the most common) and dynamic.	Static filtering is relatively inexpensive, and relatively little maintenance is required. It is well-suited for closed environments where access to or from multiple addresses is not allowed.	Leaves permanent open holes in the network; allows direct connection to internal hosts by external sources; offers no user authentication; method can be unmanageable in large networks
Proxy Service	Information from the internet is retrieved by the firewall and then sent to the requesting system and vice versa. In this way, the firewall can limit the information made known to the requesting system, making vulnerabilities less apparent.	Only allows temporary open holes in the network perimeter. Can be used for all types of internal protocol services.	Allows direct connections to internal hosts by external clients; offers no user authentication
Stateful Pattern Recognition	This method examines and compares the contents of certain key parts of an information packet against a database of acceptable information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. If not, the information is discarded.	Provides a limited time window to allow packets of information to be sent; does not allow any direct connections between internal and external hosts; supports user-level authentication	Slower than packet filtering; does not support all types of connections

ATTRIBUTES AND FEATURES

A variety of different portable and on-line chlorine monitors are commercially available. These range Firewalls may be a piece of hardware, a software program, or an appliance card that contains both.

Advanced features that can be incorporated into firewalls allow for the tracking of attempts to log-on to the local area network system. For example, a report of successful and unsuccessful log-in attempts may be generated for the computer specialist to analyze. For systems with mobile users, firewalls allow remote access in to the private network by the use of secure log-on procedures and authentication certificates. Most firewalls have a graphical user interface for managing the firewall.

In addition, new Ethernet firewall cards that fit in the slot of an individual computer bundle additional layers of defense (like encryption and permit/deny) for individual computer transmissions to the network interface function. These new cards have only a slightly higher cost than traditional network interface cards.

COST

The cost of firewall systems varies depending on the complexity and level of protection provided. Basic firewalls begin at around $50 and can be installed on a single machine in a few hours by a knowledgeable computer user. A typical small network system of hardware and software designed for a system of 10-50 computers would cost approximately $1,000-$1,500 and would require an initial installation and configuration time of between 8-40 man-hours by an information technology specialist. Larger systems will have additional costs for more software license fees, hardware equipment capable of handing more traffic, and increased installation and testing time for additional workstations.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Zone Labs
1060 Howard Street
San Francisco, California 94103
(415) 341-8200
www.zonelabs.com

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, California 95014
(408) 517-8000
www.symantec.com

Sygate Technologies
6595 Dumbarton Circle
Fremont, CA 94555
(510) 742-2600
www.sygate.com

SonicWALL
1143 Borregas Avenue
Sunnyvale, California 94089
(408) 745-9600
www.sonicwall.com

Check Point Software Technologies
Three Lagoon Drive, Suite 400
Redwood City, California 94065
(650) 628-2000
www.checkpoint.com

SMC Networks
38 Tesla
Irvine, California 92618
(800) 762-4968
www.smc.com

DASCORE, Inc.
(866) 321-3804
www.dascore.com

CHEMetrics, Inc.
4295 Catlett Rd.,
Calverton, Virginia 20138
(800) 356-3072
www.chemetrics.com

Lucent Technologies
600 Mountain Avenue
Murray Hill, New Jersey 07974
(888) 426-2252
www.lucent.com

Net Screen Corporation
805 11th Ave., Building 3
Sunnyvale, California 94089
(408) 543-2100
www.netscreen.com

Sun Microsystems
4150 Network Circle
Santa Clara, California 95054
(800) 786-0404
www.sun.com

3Com Corporation
5500 Great America Parkway
Santa Clara, California 95052
(800) 638-3266
www.3com.com

Network Intrusion Hardware / Software

● DETECT
● DELAY
○ RESPOND

OBJECTIVE

Designed to detect and delay an unauthorized attack on a computer network system.

APPLICATION

These systems are installed on individual computers, computer networks, or other electronic assets.

LOCATION USED

Computer system. Can be installed on individual computers (protects only computer on which it is installed) or on a computer network (protects all computers on network).

DESCRIPTION

Network intrusion detection and prevention systems are software- and hardware-based programs designed to detect unauthorized attacks on a computer network system.

While other applications, such as firewalls and anti-virus software, share similar objectives with network intrusion systems, network intrusion systems provide a deeper layer of protection beyond the capabilities of these other systems because they evaluate patterns of computer activity rather than specific files.

It is worth noting that attacks may come from either outside or within the system (i.e., from an insider), and that network intrusion detection systems may be more applicable for detecting patterns of suspicious activity from inside a facility (i.e., accessing sensitive data, etc.) than are other information technology solutions.

ATTRIBUTES AND FEATURES

- Network intrusion detection systems employ a variety of mechanisms to evaluate potential threats. The type of search and detection mechanisms are dependent upon the level of sophistication of the system. Some of the available detection methods include:

- Protocol analysis - Protocol analysis is the process of capturing, decoding, and interpreting electronic traffic. The protocol analysis method of network intrusion detection involves the analysis of data captured during transactions between two or more systems or devices, and the evaluation of these data to identify unusual activity and potential problems. Once a problem is isolated and recorded, problems or potential threats can be linked to pieces of hardware or software. Sophisticated protocol analysis will also provide statistics and trend information on the captured traffic.

- Traffic anomaly detection -Traffic anomaly detection identifies potential threatening activity by comparing incoming traffic to "normal" traffic patterns, and identifying deviations. It does this by comparing user characteristics against thresholds and triggers defined by the network administrator. This method is designed to detect attacks that span a number of connections, rather than a single session.

- Network honeypot - This method establishes non-existent services in order to identify potential hackers. A network honeypot impersonates services that don't exist by sending fake information to people scanning the network. It identifies the attacker when they attempt to connect to the service. There is no reason for legitimate traffic to access these resources because they don't exist, therefore any attempt to access them constitutes an attack.

Anti-intrusion detection system evasion techniques - These methods are designed to identify attackers who may be trying to evade intrusion detection system scanning. They include methods called IP defragmentation, TCP streams reassembly, and deobfuscation.

While these detection systems are automated, they can only indicate patterns of activity, and a computer administer or other experienced individual must interpret activities to determine whether or not they are potentially harmful. Monitoring the logs generated by these systems can be time consuming, and there may be a learning curve to determine a baseline of "normal" traffic patterns from which to distinguish potential suspicious activity.

COST

The cost of network instruction detection systems varies depending on the level of sophistication of the system and the corresponding protection provided. Basic intrusion detection systems begin at around $100 and can be installed on a single machine in a few hours by a person who is knowledgeable in computers. A typical small network system of hardware and software designed for a system of 10-50 computers would cost approximately $1,000-$5,000 and would require an initial installation time of between 20-60 hours of man-hour time by an information technology specialist. Larger systems will have additional costs for more software license fees, hardware equipment capable of handing more traffic, and increased installation and testing time for additional workstations. Routine maintenance of the software or hardware system is required to analyze the information collected and update the system with information on new threats.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Zone Labs
1060 Howard Street
San Francisco, California 94103
(415) 341-8200
www.zonelabs.com

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, California 95014
(408) 517-8000
www.symantec.com

Syygate Technologies
6595 Dumbarton Circle
Fremont, California 94555
(510) 742-2600
www.sygate.com

Check Point Software Technologies
Three Lagoon Drive, Suite 400
Redwood City, California 94065
(650) 628-2000
www.checkpoint.com

Internet Security Systems (ISS)
6303 Barfield Road
Atlanta, Georgia 30328
(888) 901-7477
www.iss.net

Cisco Systems
170 West Tasman Dr.
San Jose, California 95134
(800) 553-6387
www.cisco.com

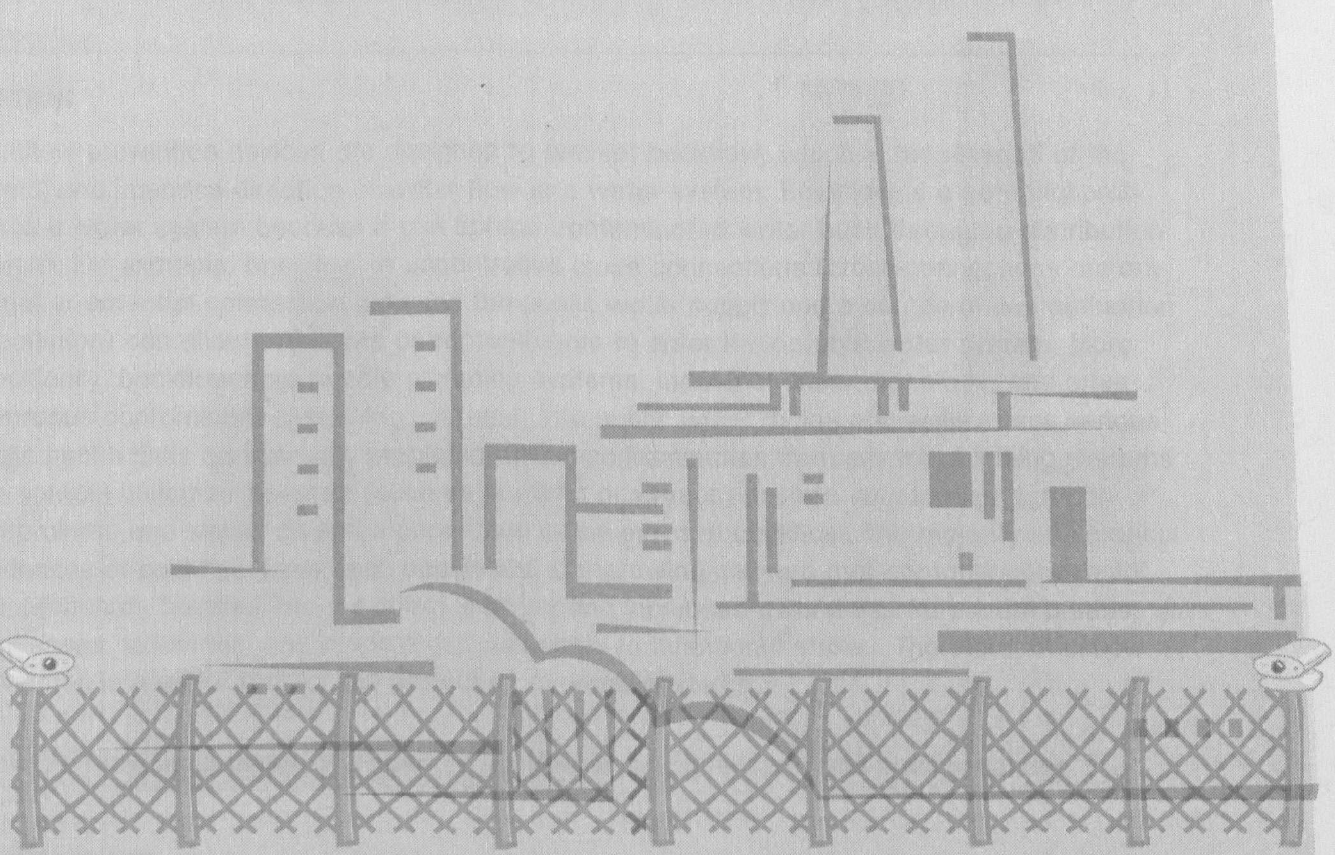
Lucent Technologies
600 Mountain Avenue
Murray Hill, New Jersey 07974
(888) 426-2252
www.lucent.com

Net Screen Corporation
805 11th Ave., Building 3
Sunnyvale, California 94089
(408) 543-2100
www.netscreen.com

SonicWALL
1143 Borregas Avenue
Sunnyvale, California 94089-1209
(408) 745-9600
www.sonicwall.com

TippingPoint Technologies, Inc.
7501B North Capital of Texas Highway
Austin, Texas 78731
(888) 648-9663
www.tippingpoint.com

Physical Asset Monitoring and Control Products



Backflow Prevention Devices

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Visually monitor an asset to detect potential intruders, unauthorized or suspicious materials or objects, or other threats.

APPLICATION

Used to detect physical threats to an asset (i.e., persons or materials) through surveillance of asset. Can be used to monitor any water or wastewater assets (perimeter of facility, remote pumphouses, potential access points to distribution or collection systems, etc.). Primarily used to monitor exterior areas, but can be used in interior of buildings or facilities.

LOCATION USED

Usually mounted at a strategic location at the asset to be monitored to monitor as large an area as possible. Can be mounted near doors or windows, on or along fences, or within buildings.

DESCRIPTION

Backflow prevention devices are designed to prevent backflow, which is the reversal of the normal and intended direction of water flow in a water system. Backflow is a potential problem in a water system because it can spread contaminated water back through a distribution system. For example, backflow at uncontrolled cross connections (cross-connections are any actual or potential connection between the public water supply and a source of contamination or pollution) can allow pollutants or contaminants to enter the potable water system. More specifically, backflow from private plumbing systems, industrial areas, hospitals, and other hazardous contaminant-containing systems, into public water mains and wells poses serious public health risks and security problems. Cross-contamination from private plumbing systems can contain biological hazards (such as bacteria or viruses) or toxic substances that can contaminate and sicken an entire population in the event of backflow. The majority of historical incidences of backflow have been accidental, but growing concern that contaminants could be intentionally backfed into a system is prompting increased awareness for private homes, businesses, industries, and areas most vulnerable to intentional strikes. Therefore, backflow prevention is a major tool for the protection of water systems.

Backflow may occur under two types of conditions: backpressure, and backsiphonage.

Backpressure

Backpressure is the reverse from normal flow direction within a piping system that is the result of the downstream pressure being higher than the supply pressure. These reductions in supply pressure occur whenever the amount of water being used exceeds the amount of water being supplied, such as during water line flushing, fire fighting, or breaks in water mains.

Backsiphonage

Backsiphonage is the reverse from normal flow direction within a piping system that is caused by negative pressure in the supply piping (i.e., the reversal of normal flow in a system caused by a vacuum or partial vacuum within the water supply piping). Backsiphonage can occur when there is a high velocity in a pipe line; when there is a line repair or break that is lower than a service point; or when there is lowered main pressure due to high water withdrawal rate, such as during fire fighting or water main flushing.

Aging water systems, leaking sewer connections, contaminated groundwater, cross-over connections, and growing numbers of users all contribute to the potential for backflow in a system because they can lead to unintended connections between different parts of the system or leaks that can contribute contaminants to the system. Therefore, backflow preventers are typically installed at critical points in a distribution system to prevent contamination. Currently, backflow preventers are mandated in many jurisdictions at the point where the backflow may occur, such as at a hose bib or at a feed point to a fire sprinkler system. However, security concerns dictate that wider use of backflow preventers be considered.

It should be noted that water systems are typically designed with numerous interconnections so that water can routinely flow in either direction in many areas of the water system. This improves the system hydraulics while minimizing the required sizes of water mains. It is desirable that each point in the system be fed from at least two points so that a maintenance problem can be isolated within the smallest possible area. Therefore, the use of backflow preventers within the water service network may have limited applicability. However, they may be applicable in other places in the network, such as at user connections.

The appropriate type of backflow preventer for any given application will depend on the category of hazard which may flow into the potable water supply if backflow occurs. Municipalities define their own hazard classifications, which usually include two or three general classifications, depending on the municipality. These categories include:

- Pollutants/non-health hazards - A pollutant/non health hazard is any substance which would affect the color or odor of the water, but would not pose a health hazard.
- Contaminants/health hazards - A contaminant/health hazard is any substance that causes illness or death if ingested.
- Lethal hazards - Some communities establish a separate classification for hazards that are typically lethal. These municipalities define a lethal hazard is any substance that could/would be lethal to water users. For example, lethal hazards could include high concentrations of sewage, toxic chemicals, and radioactive materials.

As noted above, the appropriate type of backflow preventer for any given application will depend on the category of hazard which may flow into the potable water supply if backflow occurs. The primary types of backflow preventers that are appropriate for use at municipalities and utilities are:

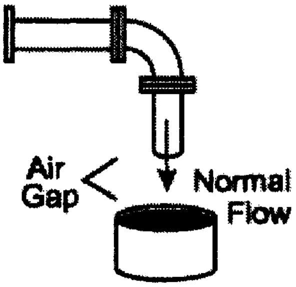
- Air Gap Drains;
- Double Check Valves;

- Reduced Pressure Principle Assemblies; and

- Pressure Vacuum Breakers.

Each of these types of backflow preventers is manufactured to achieve certain standards. For example, the American Water Works Association (AWWA), the American Society of Sanitary Engineers (ASSE), the American Society of Mechanical Engineers (ASME), and the International Association of Plumbing and Mechanical Officials (IAPMO) have standards for the construction materials, design, workmanship, testing, and delivery of several types of backflow prevention devices. Interested parties can consult these standards and verify with vendors that their products meet these requirements. Each backflow preventer type is described in detail below.

AIR GAP DRAIN



An air gap is a non-mechanical backflow prevention method that is effective against backsiphonage or backpressure conditions. An air gap system is implemented by physically separating the supply pipe from the receiving vessel (see accompanying figure). This breaks the pressure between the inlet and the outlet, and thereby prevents backflow. According to standard engineering design practice, the distance between the supply pipe and the receiving vessel should be at least twice the diameter of the water supply outlet and never less than one inch. An air gap is acceptable for use in applications to protect against contaminant or pollutant hazards. In addition, an air gap may be the best means of protecting against accidental contamination from lethal hazards.

An air gap system may be constructed using commercially available plumbing components, or it may be purchased as separate components, which are then integrated into existing plumbing and piping configurations. Because an air gap breaks the pressure between the inlet and the outlet, a booster pump is usually needed downstream to ensure downstream pressure, unless the flow of the water by gravity is sufficient for the downstream water use. The air gap drain is a very effective way to prevent accidental contamination of the water system; however, it is important to note that an air gap is not always practical and can easily be bypassed. If the distance between the supply pipe and receiving vessel is compromised either purposely or inadvertently to prevent excessive splash, the air gap is defeated. Also, with an air gap, water is exposed to the surrounding air; therefore, the aspiration effect could potentially drag down airborne pollutants or contaminants into the receiving vessel.

AMSE standards A112.1.1 and A112.1.2 and IAPMO PS 65 provide standards for air gap drains. Some of these standards are for specific applications (for instance, IAPMO PS 65 is for water conditioning equipment).

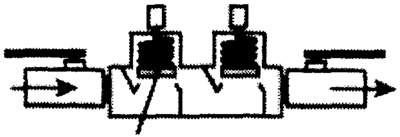
When it is not possible to design an air gap into a system, designers may opt to install mechanical backflow prevention devices, which provide physical barriers to backflow. Physical backflow prevention devices are described on the following pages.

Double Check Valve

A double check valve is a mechanical device that consists of two single check valves coupled within one body, and two tightly closing gate valves, one located at each end of the unit. Each check valve consists of a physical plate connected to the top of the pipe by a hinge. The hinge is oriented such that flow in the intended flow direction keeps pressure on the plate and keeps it open, permitting the passage of fluid in the intended flow direction. Thus, under normal conditions, the check valves remain open. In the absence of water flow, the plate is not being held open by flow in the correct direction, and the valves close until the normal water flow resumes. In the event of backflow, the flow is against the direction of the hinge, so the plate remains closed. A double check valve may be used under continuous pressure. It can be effective against either backpressure or backsiphonage, and may be used to protect against pollutant hazards. It should be noted that double check valves are susceptible to interference from materials within the piping system. For example, grit or fibers can catch under the valves, causing them to remain open and potentially allowing leakage back into the system.

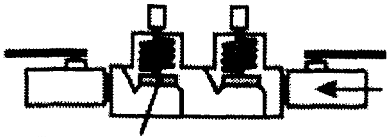
AWWA standard C510-97 and ASSE standard 1015 cover double check valve backflow prevention assemblies.

Normal Flow



Spring Loaded Check Valve
Open During Normal Flow

Reverse Flow

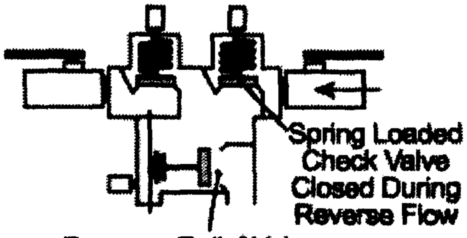


Spring Loaded Check Valve
Closed During Reverse Flow

Reduced Pressure (RP) Principle Assembly

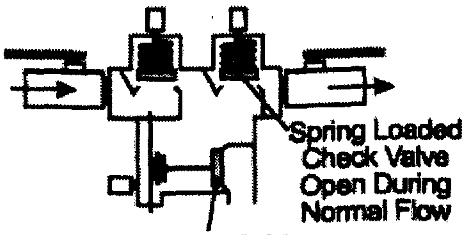
The principle behind a reduced pressure principle backflow prevention device is to reduce a negative pressure differential between the upstream and downstream ends of a line, thereby preventing backflow. A reduced pressure principle assembly is a mechanical backflow preventer that is essentially two check valves with an automatically operating pressure relief valve placed between the two checks. This system is designed such that this "zone" between the two checks is always kept at a lower pressure than the supply pressure. Under normal flow conditions, the check valves remain open and the relief valve is closed. In the event of backsiphonage, the relief valve will open to allow the induction of air to break the vacuum. In the event of backpressure, the opened relief valve routes the contaminated water out of the system (drainage can be provided for such spillage). The reduced pressure principle assembly also contains two shut-off valves upstream and downstream of the check valves and a series of test cocks for periodic testing of the valves.

Reverse Flow



Pressure Relief Valve
Open During Reverse Flow

Normal Flow



Pressure Relief Valve
Closed During Normal Flow

A reduced pressure principle assembly is effective against either backpressure or backsiphonage, and may be used to protect against pollutant or contaminant hazards. Reduced pressure principle assemblies may be used under constant pressure, and are commonly installed on high hazard installations.

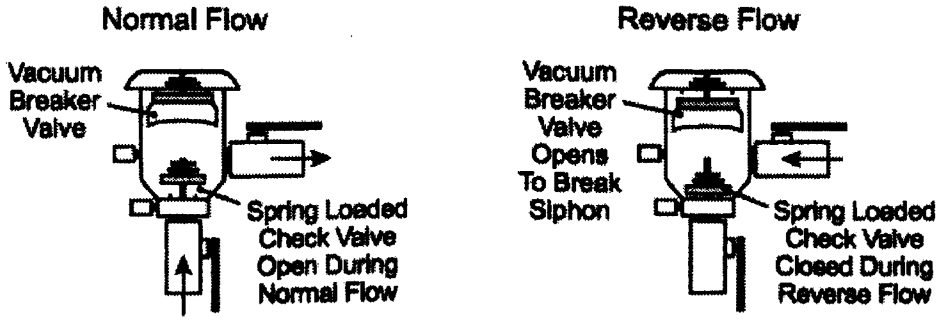
AWWA standard C511-97 and ASSE standard 1013 cover reduced pressure principle backflow prevention assemblies.

Pressure Vacuum Breaker

The principle behind a pressure vacuum breaker (PVB) backflow prevention device is to break the vacuum created during a backsiphonage event, thereby preventing backflow. A PVB consists of a spring-loaded check valve which closes tightly when the pressure in the assembly drops or when zero flow occurs, plus an air relief valve (located on the discharge side of the check valve) that opens to break a siphon when the pressure in the assembly drops. The assembly also includes two shut off valves and two test cocks for periodic testing of the assembly. The air relief valve ensures that no non-potable liquid is siphoned back into the potable water system.

PVBs prevent the backflow of contaminated water into a potable drinking main line, but they are not designed for backpressure conditions. PVBs may be used under continuous pressure, but the air inlet valve may become stuck in the closed position after long periods of continuous pressure. A PVB may only be used against backsiphonage and may be used to protect against pollutant or contaminant hazards.

ASSE standard 1020 covers PVB backflow prevention assemblies.


Normal Flow

Reverse Flow

Vacuum Breaker Valve
Spring Loaded Check Valve Open During Normal Flow
Vacuum Breaker Valve Opens To Break Siphon
Spring Loaded Check Valve Closed During Reverse Flow

A summary of the typical applications for the backflow prevention devices discussed above is provide in the following table.

Table 1: Backflow Prevention Devices and Typical Uses

Product	Typical Applications
Air Gap Drain	Faucets and sinks, process waters
Double Check Valve	In-house pumps, elevated tanks, non-toxic boilers
Reduced Pressure Principle Assembly	Industrial plants, hospitals, morgues, chemical plants, irrigation systems, pumps, elevated tanks, boilers, fire sprinkler systems
Pressure Vacuum Breakers	Industrial plants, cooling towers, laboratories, laundries, swimming pools, lawn sprinkler systems, fire sprinkler systems

Implementation of Backflow Prevention Devices and Backflow Prevention Programs

The implementation of backflow prevention devices within a water or wastewater system can be complex. Because backflow and cross connections can occur at so many different places within a typical system, and because many systems have large numbers of connections, it is not practical for a municipality to implement backflow preventers completely on their own to protect their system. Therefore, most municipalities have adopted ordinances requiring end users to install and maintain appropriate backflow preventers.

Determining where the implementation of backflow prevention devices is appropriate or feasible is an important consideration in any backflow prevention program. For example, as discussed above, the reversal of the direction of flow is a normal condition within an average municipal water system. As a result, backflow preventers are not practical for use in many areas of a water system. However, backflow preventers can be used at a point where water is fed to individual users to prevent flows back into the water system.

In order to be effective in reducing the potential for tampering, backflow preventers can be installed within secured locations, such as within locked underground vaults or within secured rooms within a building. However, the need to secure the backflow prevention devices must be balanced with the need to access the devices for testing.

As mentioned above, many municipalities, and many end-users, have implemented backflow prevention programs. These backflow prevention programs typically require periodic testing of each backflow prevention device (typically on an annual basis) to ensure that it is functioning properly. These programs typically require that testing be conducted by a trained and certified technician.

COST

Capital Costs

The primary factor affecting cost of a given type of backflow prevention device is the size of the pipe for which it is designed. The following will also contribute to the total cost for installing a backflow preventer: system design (including consultation as to which products are appropriate); on-site delivery; installation and retrofit; maintenance; and inspection, testing, and surveying. Costs for individual backflow preventers or backflow preventer systems will vary depending on the product brand and vendor. However, some general prices are provided below. These prices are capital costs for the backflow preventer and do not include installation or service costs.

- Costs for double check assemblies range from $100 for a -inch diameter unit to $2,000 for 8-inch diameter units. Larger sizes could be $10,000 or more.
- Costs for reduced pressure principle assemblies range from $180 for a -inch diameter unit to $3,000 for 8-inch diameter units. Larger sizes can be $12,000 or more.
- Costs for vacuum breakers range from $10 for a hose bib to $400 dollars for a 2-inch pressure vacuum breaker.
- Costs for air gap drains will be site-specific, and will depend on the size of the pipe and the area in which it is located. If re-pumping is required, the capital and operating costs will most likely be higher than for all other devices.

Operation and Maintenance Costs

As discussed above, backflow prevention devices must be tested on a periodic basis. Testing must be conducted by a trained and certified technician. Testing time for an individual backflow prevention device will vary with the size of the device and its accessibility. Typically, testing time can range from half an hour for a small, easily accessible device to several hours for larger units located in areas that are not easily accessible. When these requirements are extrapolated to include testing for each backflow prevention device within a system, costs for a backflow prevention testing program can be considerable.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Watts Regulator Company
815 Chestnut Street
North Andover, Massachusetts 01845
(978) 688-1811
www.wattsreg.com

Zurn-Wilkins
1747 Commerce Way
Paso Robles, California 93446
(805) 238-7100
www.zurn.com

Cla-Val
P.O. Box 1325
Newport Beach, California 92659-0325
(800) 942-6326
www.cla-val.com

Conbraco
PO Box 247
Matthews, North Carolina 28106
(704) 841-6000
www.conbraco.com

Ames Fire and Waterworks
875 National Drive Suite 107
Sacramento, California 95834
(916) 928-0123
www.amesfirewater.com

FEBCO Backflow Prevention
SPX Valves & Controls
PO Box 8070
Fresno, California 93747
(559) 441-5300
www.cmb-ind.com/febco.asp

Danfoss Flowmatic Valves Flomatic Corporation
15 Pruyn's Island Drive
Glens Falls, New York 12801
(800) 833-2040
www.flomatic.com

Exterior Intrusion - Buried Sensors

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor asset perimeters to detect intruders.

APPLICATION

Designed to detect attempted physical access to a water/wastewater asset. Can be connected to an alarm, lights, or video surveillance cameras to alert facility personnel of attempted access.

LOCATION USED

Buried in ground around perimeter of asset. Monitor water samples to detect chemical, biological, or radiological parameters that may represent threats to the system.

DESCRIPTION

Buried sensors are electronic devices that are designed to detect potential intruders. The sensors are buried along the perimeters of sensitive assets and are able to detect intruder activity both above- and below-ground. Some of these systems are composed of individual, stand-alone sensor units, while other sensors consist of buried cables.

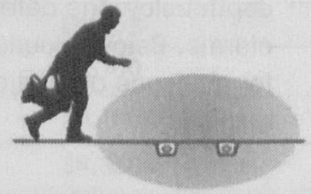
There are four types of buried sensors that rely on different types of triggers. These are: pressure or seismic; magnetic field; ported coaxial cable; and fiber-optic cables. These four sensors are all covert and terrain-following, meaning they are hidden from view and follow the contour of the terrain. The four types of sensors are described in more detail below.

Pressure/Seismic

Pressure or seismic sensors are passive detectors that respond to a change or a disturbance in the soil caused by an intruder. Pressure sensors consist of a container filled with liquid, which is connected to a transducer. A seismic sensor consists of geophones that are made up of conducting coils. Pressure sensors are more sensitive to lower frequency pressure waves than are seismic sensors. Pressure or seismic types of sensors would be most useful for detecting intruders by foot.

Magnetic Field

Magnetic field sensors are also passive detectors that respond to a change in the local magnetic field. This change may be caused by the movement of metallic material nearby, such as movement of an intruder with a metallic weapon. Magnetic field sensors consist of series of wire loops or coils buried in the ground. These sensors can be susceptible to false alarms due to electromagnetic disturbances, such as lightning.



Buried Sensor Detection Field

Ported Coaxial Cables

Ported coaxial cable sensors are active sensors that respond to nearby material with a high dielectric constant or high conductivity. Two cables-one acting as a transmitter, the other as a receiver-are run parallel to one another and are spaced approximately two meters apart. The signal leaking from one to the other creates a field between the two cables, and active disturbance of the field triggers the sensor. Materials that trigger these types of sensors can be found in people and metal vehicles.

Fiber-Optic Cables

Optical fibers are long, hair-like stands of transparent glass or plastic that use optical technology to guide light from one end of the fiber to the other. Pressure on the fiber causes a distortion in the light signal, which is detected and analyzed at the far end of the fiber. These sensors are typically woven into a mesh grid to ensure complete coverage of an area to be protected. The fibers require a burial depth of only a few centimeters to be effective. These sensors are ideal for wet environments since the non-metallic, fiber-optic cable is designed as a direct burial cable with a 20-year life expectancy.

ATTRIBUTES AND FEATURES

Buried sensors are designed to follow the existing terrain and are feasible options if a site is hilly. The sensors are buried at a relatively shallow depth (ranging from a few inches to one foot, depending on the type). These types of sensors are also covert, because they are buried and potential intruders cannot see them.

These systems may be continuous or discrete. A continuous system consists of a continuous cable, such as a fiber optic or ported coaxial cable. These types of systems monitor along a continuos line corresponding to the location of the cable. Discrete sensors consist of individual sensor units that can be buried in non-linear patterns to increase the area monitored. For example, Qual-Tron sensors are designed to monitor all activity within a 30-foot radius in any direction.

A drawback to these type of systems is that they may have different sensitivities when they are buried below different media. For example, if continuous systems are buried below different types of media (such as under a lawn, then under an intersecting concrete driveway, and then back to lawn again), the sensitivities required for different types of media may be different. For example, a good sensitivity adjustment for concrete may be too sensitive for grass. Therefore, it may be best to individually zone those areas.

Another factor that must be considered when using a buried sensor is underground utilities. Underground utilities, such as gas, water, and sewer lines, must be located at a sufficient depth below the detection zone (typically three feet), so as to not cause false and nuisance alarms. Below-ground electrical wires must also be compensated for; however, the potential for nuisance alarms caused by underground power lines is not as great as with other types of utilities.

Several other factors must be considered when using a buried sensor. Rodents have been known to cause maintenance problems by gnawing on the sensor cables; this problem is limited primarily to the Western states. Installations also should not be in areas where running water will either wash away the soil that buries the sensor or cause nuisance alarms during a heavy rain. Table 1 presents the distinctions between the four types of buried sensors.

Table 1: Types of Buried Sensors

Type	Discussion
Pressure or Seismic	Responds to disturbances in the soil. Effective in detecting an intruder walking, running, jumping, or crawling on the ground.
Magnetic Field	Responds to a change in the local magnetic field caused by the movement of nearby metallic material. Effective for detecting intruders carrying weapons as small as a pocketknife.
Ported Coaxial Cables	Responds to motion of a material with a high dielectric constant or high conductivity near the cables. Effective in detecting materials found in the human body and metallic vehicles.
Fiber-Optic Cables	Responds to a change in the shape of the fiber that can be sensed using sophisticated sensors and computer signal processing. Effective in detecting intruders by foot.

In order to be effective security measures, sensors must be tied into some type of alarm system or other system that alerts facility personnel when the sensors have been tripped. Many sensor systems include these features; in other cases, these features can be added on and the alert system can be networked to go off when the sensors are tripped.

COST

Stand-alone sensors, such as pressure/seismic and magnetic field sensors, are often sold as individual components, and the cost will depend on the number of sensors required and the sophistication of the transmitting, receiving, and recording equipment. For example, a typical system will require sensor/transmitters and a receiver. In some cases, the system may need a relay if the transmitter and receiver are located at a sufficient distance from one another.

Qual-Tron Inc. provides two types of pressure/seismic or magnetic sensor systems. The first, Mini-Intrusion Detection System (MIDS) includes sensors that transmit on a single channel at a fixed frequency. This system can handle up to 32 sensors. The EMIDS system can transmit on multiple channels and frequencies, and can handle up to 999 individual sensors. Costs for these systems are provided in Table 2 below.

Table 2: Example Cost for Individual Sensor-Based Systems

Component	MIDS	EMIDS
Sensor/Transmitter	$850	$1,100
Hand-held Receiver	$720	$1,150
Relay	$1,400	$4,350

Both of these systems can be installed and maintained by the customer. Qual-Tron indicates that training on installation and maintenance can be accomplished in a day or less. Costs for ported coaxial cable and fiber optic cable systems are provided in Table 3 below.

Table 3: Example Costs for Buried Line Sensors

Type	Cost/Ft	Notes
Ported Coaxial Cable - Stand alone	$24 - $46	Stand alone
Networked	$24 - $34	Cost for hardware only. Typical installation is 300-500 ft/day.
Fiber-Optic Cables	$10 - $15 .	Cost for hardware only. Costs for both 2-core (basic) and 4-core (advanced)

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Qual-Tron, Inc.
9409 East 55th Place South
Tulsa, Oklahoma 74145-8157
(918) 622-7052
www.qual-tron.com

Fiber SenSys, Inc.
9640 SW Sunshine Court, Suite 400
Beaverton, Oregon 97005
(503) 641-8150
www.fibersensys.com

Auratek Security, Inc.
Richelieu Industrial Park
15 Buteau Street
Gatineau, Quebec J8Z 1V4
Canada
(888) 778-8440
www.auratek.net

Sparton Electronics
Division Headquarters
Johnson Lake Road
DeLeon Springs, Florida 32130

Senstar-Stellar, Inc.
43184 Osgood Road
Fremont, California 94539
(510) 440 1000
www.senstarstellar.com

Whitaker Security, Inc.
4501 Lantern Place, Suite 100
Alexandria, Virginia 22306
(703) 768-5025
www.whitakersecurity.com

DAQ Electronics
Piscataway Corporate Center
262B Old New Brunswick Road
Piscataway, New Jersey 08854-0050

(732) 981-0050
www.daq.net/security/sabre_solutions.html

Hach Company
PO Box 389
Loveland, Colorado 80539
800-227-4224
www.hach.com

Fences

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Physically deter potential intruders from gaining access to an asset.

APPLICATION

Installed around the perimeter of any water or wastewater asset to deter unauthorized access to that asset. Fences are often placed around the perimeter or boundary of a facility, or around the perimeter of a sensitive structure within a facility. Access to the asset is controlled by directing all traffic through specific access points (e.g., gates or doors).

LOCATION USED

Perimeter of any asset to be protected.

DESCRIPTION

A fence is a physical barrier that can be set up around the perimeter of an asset. Fences often consist of individual pieces (such as individual pickets in a wooden fence, or individual sections of a wrought iron fence) that are fastened together. Individual sections of the fence are fastened together using posts, which are sunk into the ground to provide stability and strength for the sections of the fence hung between them. Gates are installed between individual sections of the fence to allow access inside the fenced area.

Many fences are used as decorative architectural features to separate physical spaces from each other. They may also be used to physically mark the location of a boundary (such as a fence installed along a property line). However, a fence can also serve as an effective means for physically delaying intruders from gaining access to a water or wastewater asset. For example, many utilities install fences around their primary facilities, around remote pump stations, or around hazardous materials storage areas or sensitive areas within a facility. Access to the area can be controlled through security at gates or doors through the fence (for example, by posting a guard at the gate or by locking it). In order to gain access to the asset, unauthorized persons would either have to go around or through the fence.

Fences are often compared with walls when determining the appropriate system for perimeter security. While both fences and walls can provide adequate perimeter security, fences are often easier and less expensive to install than walls. However, they do not usually provide the same physical strength that walls do. In addition, many types of fences have gaps between the individual pieces that make up the fence (i.e., the spaces between chain links in a chain link fence or the space between pickets in a picket fence). Thus, many types of fences allow the interior of the fenced area to be seen. This may allow intruders to gather important information about the locations or defenses of vulnerable areas within the facility.

ATTRIBUTES AND FEATURES

There are numerous types of materials used to construct fences, including chain link, iron, aluminum, wood, or wire. Some types of fences, such as split rails or pickets, may not be appropriate for security purposes because they are traditionally low fences, and they are not physically strong. Potential intruders may be able to easily defeat these fences either by jumping or climbing over them or by breaking through them. For example, the rails in a split rail fence may be removed, and the pickets in a picket fence may be able to be broken easily.

Important security attributes of a fence include the height to which it can be constructed, the strength of the material comprising the fence, the method and strength of attaching the individual sections of the fence together at the posts, and the fence's ability to restrict the view of the assets inside the fence. Additional considerations should include the ease of installing the fence and the ease of removing and reusing sections of the fence. Table 1 provides a comparison of the important security and usability features of several different types of fences.

Table 1 Comparison of Different Fence Types

Specifications	Iron	Aluminum	Chain Link
Height Limitations	12″	10″	12″
Strength	High	Medium	Medium
Installation Requirements	High	High	Low
Ability to Remove/Reuse	High	High	Low
Ability to Replace/Repair	High	High	Medium

Some fences can include additional measures to delay, or even detect, potential intruders. Such measures may include the addition of barbed wire, razor wire, or other deterrents at the top of the fence. Barbed wire is sometimes employed at the base of fences as well. This can impede a would-be intruder's progress in even reaching the fence. Fences may also be fitted with security cameras to provide visual surveillance of the perimeter. Finally, some facilities have installed motion sensors along their fences to detect movement on the fence. Several manufacturers have combined these multiple perimeter security features into one product and offer high security fences that incorporate stronger materials, sensors, alarms, and other security features. These specialized fences will be covered in other product guides.

COST

Costs for fences will vary depending on the type of material chosen, the height of the fence, and the length of fence to be installed. Table 2 provides cost information for several different kinds of fences, including capital costs plus estimates of the number of manhours required to install the fence.

Table 2 Fencing Costs

Fence Type	Material Cost (per linear ft)	Labor Cost (man-hours/100 linear ft)*
Chain link, 2" mesh, 9 gauge	$3.55	124
6' high	$4.90	28
8' high	$6.20	32
10' high		
Aluminum, 6' section	$148	18
6' high	$210	23
8' high		
Steel, 6' section	$157	31
6' high	$198	36
8' high	$237	43
10' high		

Some security fencing systems include enhanced security features, such as razor wire at the top of the fence. However, additional security features can be installed along with the fence at additional cost. Two examples are listed below:

- 18" Razor Wire with a high tensile wire core - $63 for a 50 foot roll, not including installation.
- Vibration/Motion sensors - These units are sold as complete detection systems only. One unit includes a battery-operated burglar alarm, with a motion detector. With one electrician installing the system, the cost is $325 per unit.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

AMESCO, Inc., Metalco Products
7800 S. Quincy Street
Willowbrook, Illinois 60527
(800) 708-2526
www.metalco.tv/default.htm

FenceCenter.com
(888) 336-2358
www.fencecenter.com

Alabama Metal Industries Corporation
3245 Fayette Avenue
Birmingham, Alabama 35208
(800) 366-2642
www.amico-securityproducts.com/fence.htm

Fiber Sensys, Inc.
9640 SW Sunshine Court
Beaverton, Oregon 97005
(503) 641-8150
www.fibersensys.com

Hoover Fence Co.
P.O. Box 563
5531 McClintocksburg Rd.
Newton Falls, Ohio 44444
(800) 355-2335
www.hooverfence.com

Ameristar Fence
PO Box 581000
Tulsa, Oklahoma 74158
(866) 467-2773
www.impassefence.com/

Alamo Fence Company
9618 Honeywell
Houston, Texas 77074
(713) 981-1113
www.alamofence.com/contents.htm

Fence City
619 Bethlehem Pike
P.O. Box 779
Montgomeryville, Pennsylvania 18936
(800) 336-2310
www.fencecity.com

Films for Glass Shatter Protection

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Protect windows, glass doors, and other glass from shattering.

APPLICATION

Can be used on any glass surface to prevent the glass from shattering. Preventing the glass from shattering may prevent access to a building or a room through the broken glass, and may also help to reduce injuries to personnel located behind the glass.

LOCATION USED

Windows, glass doors, and any other piece of glass at a water/wastewater utility.

DESCRIPTION

Most water and wastewater utilities have numerous windows on the outside of buildings, in doors, and in interior offices. In addition, many facilities have glass doors or other glass structures, such as glass walls or display cases. These glass objects are potentially vulnerable to shattering when heavy objects are thrown or launched at them, when explosions occur near them, or when there are high winds (for exterior glass). If the glass is shattered, intruders may potentially enter an area. In addition, shattered glass projected into a room from an explosion or from an object being thrown through a door or window can injure and potentially incapacitate personnel in the room. Materials that prevent glass from shattering can help to maintain the integrity of the door, window, or other glass object, and can delay an intruder from gaining access. These materials can also prevent flying glass and thus reduce potential injuries.

Materials designed to prevent glass from shattering include specialized films and coatings. These materials can be applied to existing glass objects to improve their strength and their ability to resist shattering. The films have been tested against many scenarios that could result in glass breakage, including penetration by blunt objects, bullets, high winds, and simulated explosions. Thus, the films are tested against both simulated weather scenarios (which could include both the high winds themselves and the force of objects blown into the glass), as well as more criminal/terrorist scenarios where the glass is hit directly with an object with the intent of penetrating the glass, or is subject to explosives or bullets. Many vendors provide information on the results of these types of tests, and thus potential users can compare different product lines to determine which products best suit their needs.

This product guide focuses on specialized films that can be applied to glass. Most of these films are constructed of specialized polyesters to which adherents are added to ensure a secure bond to the glass surface. The films are available in a number of different thicknesses depending on the level of protection needed for certain objects. These films are easy to add existing glass surfaces, making them excellent security features to retrofit at a water or wastewater utility. The films are also multi-functional, and many product lines absorb UV rays, shading the interior and reducing energy requirements for heating and cooling.

Additional product guides that focus on coatings for glass shatter protection and other types of safety glass are available from EPA.

ATTRIBUTES AND FEATURES

The primary attributes of films for shatter protection are:

- The materials from which the film is made;
- The adhesive that bonds the film to the glass surface; and
- The thickness of the film.

Standard glass safety films are designed from high strength polyester. Polyester provides both strength and elasticity, which is important in absorbing the impact of an object, spreading the force of the impact over the entire film, and resisting tearing. The polyester is also designed to be resistant to scratching, which can result when films are cleaned with abrasives or other industrial cleaners.

The bonding adhesive is important in ensuring that the film does not tear away from the glass surface. This can be especially important when the glass is broken, so that the film does not peal off the glass and allow it to shatter. In addition, films applied to exterior windows can be subject to high concentrations of UV light, which can break down bonding materials.

Film thickness is measured in gauge or mils. According to test results reported by several manufacturers, film thickness appears to affect resistance to penetration/tearing, with thicker films being more resistant to penetration and tearing. However, the application of a thicker film did not decrease glass fragmentation.

Many manufacturers offer films in different thicknesses. The "standard" film is usually one 4 mil layer; thicker films are typically composed of several layers of the standard 4 mil sheet. However, newer technologies have allowed the polyester to be "microlayered" to produce a stronger film without significantly increasing its thickness. In this microlayering process, each laminate film is composed of multiple micro-thin layers of polyester woven together at alternating angles. This provides increased strength for the film, while maintaining the flexibility and thin profile of one film layer.

As described above, many vendors test their products in various scenarios that would lead to glass shattering, including simulated bomb blasts and simulation of the glass being struck by wind-blown debris. Some manufacturers refer to the Government Services Administration standard for bomb blasts, which require resistance to tearing for a 4 PSI blast. Other manufacturers use other measures and tests for resistance to tearing. Many of these tests are not "standard," in that no standard testing or reporting methods have been adopted by any of the accepted standards-setting institutions. However, many of the vendors publish the procedure and the results of these tests on their websites, and this may allow users to evaluate the protectiveness of these films. For example, several vendors evaluate the "protectiveness" of their films and the "hazard" resulting from blasts near windows with and without protective films. Protectiveness is usually evaluated based on the percentage of glass ejected from the window, and the height at which that ejected glass travels during the blast (for example, if the blasted glass tends to project upward into a room - potentially towards people's faces - it is a higher hazard than if it is blown downward into the room towards people's feet). There are some standard measures of glass breakage. For example, several vendors indicate that their products exceed the American Society for Testing and Materials (ASTM) standards 1' 1 64Z-95 "Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings." Vendors often compare the results of some sort of penetration or force test, ballistic tests, or simulated explosions with unprotected glass vs. glass onto which their films have been applied. Results generally show that applying films to the glass surfaces reduces breakage/ penetration of the glass and can reduce the amount and direction of glass ejected from the frame. This in turn reduces the hazard from flying glass.

In addition to these types of tests, many vendors conduct standard physical tests on their products, such as tests for tensile strength and peel strength. Tensile strength indicates the strength per area of material, while the peel strength indicates the force it would take to peel the product from the glass surface. Several vendors indicate that their products exceed American National Standards Institute (ANSI) standard Z97.1 for tensile strength and adhesion.

Vendors typically have a warranty against peeling or other forms of deterioration of their products. However, the warranty requires that the films be installed by manufacturer-certified technicians to ensure that they are applied correctly, and therefore that the warranty is in effect. Warranties from different manufacturers may vary. Some may cover the cost of replacing the material only, while others include material plus installation. Because installation costs are significantly greater than material costs (see discussion below), different warranties may represent large differences in potential costs.

COST

As discussed above, all of these products must be installed by manufacturer-certified technicians. For any individual product line, costs are dependent upon the area of glass to be covered and the configuration of the area. In general, labor costs are higher than material costs for installation of these films, and the primary factor affecting labor costs is the amount of cutting and fitting that must be done with the film. The more individual panes or surfaces to be covered, the higher the cost. For example, a 9' x 9' window composed of a single pane of glass would be less expensive to treat than would a 9' x 9' window composed of nine 3' x 3' panes. In addition, costs of the films generally increase as the thickness or gauge of the film increases. However, costs generally range from $3-$7 per ft2, installed.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Plastic-View International, Inc.
4585 Runway, Suite B
Simi Valley, California 93063
(805) 520-9390
www.pvifilm.com

FShatterguard.com
(888) 306-7998
www.shatterguard.com

Bekaert Specialty Films, LLC
13770 Automobile Blvd.
Clearwater, Florida 33762
(800) 282-9031
www.bekaertspecialtyfilms.com

HCPFilms, Inc.
Llumar Technical Services
P.O. Box 5068
Martinsville, Virginia 24115
(800) 255-8627
www.llumar.com

A3M
3M Center
St. Paul, Minnesota 55144
(888) 364-3577
www.3m.com

Perma-Gard Window Protection, Inc.
100 South Federal Highway
Pompano Beach, Florida 33062
(888) 946-6300
www.perma-gard.com

○ DETECT
● DELAY
○ RESPOND

Fire Hydrant Locks

OBJECTIVE

Hydrant locks can be used to prevent unauthorized physical access to a water asset via a fire hydrant.

APPLICATION

Installing hydrant locks on all hydrants in a system may help to prevent introduction of unauthorized substances into the system.

LOCATION USED

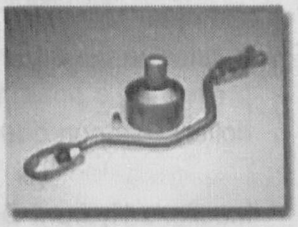
On any fire hydrant valve.

DESCRIPTION

Fire hydrants are installed at strategic locations throughout a community's water distribution system to supply water for fire fighting. However, because there are many hydrants in a system and they are often located in residential neighborhoods, industrial districts, and other areas where they cannot be easily observed and/or guarded, they are potentially vulnerable to unauthorized access. Many municipalities, states, and EPA Regions have recognized this potential vulnerability and have instituted programs to lock hydrants. For example, EPA Region 1 has included locking hydrants as number 7 on its "Drinking Water Security and Emergency Preparedness" Top Ten List for small ground water suppliers.

A "hydrant lock" is a physical security device designed to prevent unauthorized access to the water supply through a hydrant. They can also ensure water and water pressure availability to fire fighters and prevent water theft and associated lost water revenue. These locks have been successfully used in numerous municipalities and in various climates and weather conditions.

Fire hydrant locks are basically steel covers or caps that are locked in place over the operating nut of a fire hydrant. The lock prevents unauthorized persons from accessing the operating nut and opening the fire hydrant valve. The lock also makes it more difficult to remove the bolts from the hydrant and access the system that way. Finally, hydrant locks shield the valve from being broken off. Should a vandal attempt to breach the hydrant lock by force and succeed in breaking the hydrant lock, the vandal will only succeed in bending the operating valve. If the hydrant's operating valve is bent, the hydrant will not be operational, but the water asset remains protected and inaccessible to vandals. However, the entire hydrant will need to be replaced.



McGard Hydrant Lock and Wrench

Hydrant locks are designed so that the hydrants can be operated by special "key wrenches" without removing the lock. These specialized wrenches are generally distributed to the fire department, public works department, and other authorized persons so that they can access the hydrants as needed. An inventory of wrenches and their serial numbers is generally kept by a municipality so that the location of all wrenches is known. These operating key wrenches may only be purchased by registered lock owners.

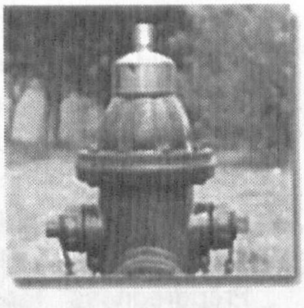
ATTRIBUTES AND FEATURES

The most important features of hydrant locks are their strength and the security of their locking systems. The locks must be strong so that they cannot be broken off. Hydrant locks are constructed from stainless or alloyed steel. Stainless steel locks are stronger and are ideal for all climates; however, they are more expensive than alloy locks. The locking mechanisms for each fire hydrant locking system ensure that the hydrant can only be operated by authorized personnel who have the specialized key to work the hydrant.

There are three major vendors for fire hydrant locks: Mueller Company, McGard, and Hydra-Shield. Specifics of hydrant locking systems are discussed below.

At a minimum, a fire hydrant lock system consists of a steel locking system and a special key wrench that operates the hydrant without unlocking it. In addition, the McGard locks require a universal security plug key for installing and removing the hydrant locks.

The principle behind the McGard and Hydra-Shield hydrant locks is the same. First, a "mating collar" is fitted over the operating nut. The mating collar surrounds the operating nut, preventing a wrench from gripping the nut and allowing access to the nut only from the top. Next, a "drive plug" is installed on the top part of the operating nut. The drive plug secures the hydrant's operating nut and prevents it from being from turned. Last, an outer collar is installed over the drive plug, effectively "locking" the hydrant by denying access to the operating nut.

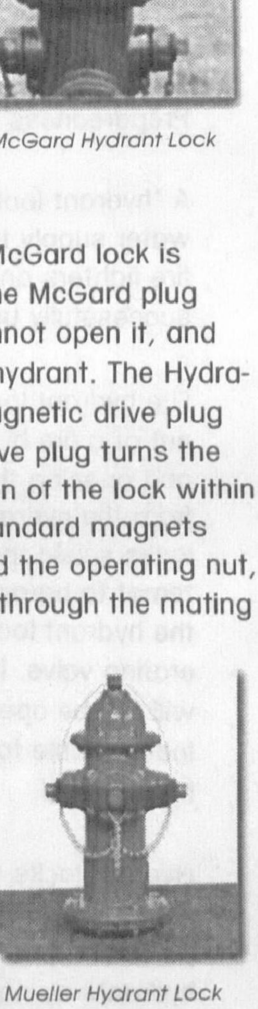


McGard Hydrant Lock

McGard Hydrant Lock

The McGard and Hydra-Shield locking mechanisms operate differently. The McGard lock is mechanical, and is installed and uninstalled using a specialized plug key. The McGard plug cap is rounded and has no edges to grip; therefore, standard wrenches cannot open it, and only McGard's specialized operating wrenches can be used to operate the hydrant. The Hydra-Shield lock is magnetic. The specialized key wrench works by pulling the magnetic drive plug up and "unlocking" the hydrant. Turning the wrench after "unlocking" the drive plug turns the hydrant's operating nut to the open position. The combination of the location of the lock within the outer body and the specialized properties of the magnet ensure that standard magnets cannot be used to remove the lock. The outer collar also spins freely around the operating nut, preventing a potential vandal from gripping the operating nut and turning it through the mating collar. This can add an additional layer of protection for the hydrant.

Mueller's Hydrant Defender™ systems consist of covers that fit over the operating nut and the hydrant valves, and 14 gauge stainless steel straps that connect the caps and keep them from being removed. The straps are locked in place by a uniquely coded mechanical lock. The manufacturer recommends a specific lock, although users may substitute other types of locks if they wish.



Mueller Hydrant Lock

The Mueller and McGard locks are manufactured to fit standard hydrant sizes. Hydra-Shield customizes its locks for any hydrant.

Mueller Hydrant Lock

Installation of a hydrant lock is straightforward, although the process may differ depending on the lock vendor. Locks are either installed on the existing hydrant operating nut, or on a new nut that is supplied with the hydrant lock. In the latter case, the standard hydrant operating is removed and replaced with a special nut that will operate with the hydrant lock.

COST

Individual components of fire hydrant locks are sold separately. Standard Hydra-Shield locks sell for between $185 and $240 apiece. Wrenches range from $105-$135 each. Heavy duty locks can be more expensive. McGard locks range from $142.50 per lock for large orders (typically >1000) to $203 per lock for small orders (<50). As with the locks, the costs for operating wrenches depend on the quantity ordered, but typical costs are $47-$62 per wrench. Plug keys are approximately $16.50 per key and can be ordered in any amount.

The Mueller Hydrant Defender™ systems are sold through local distributors and sell for approximately $70-85 apiece. The locks and keys are sold separately. Locks are under $10 apiece, while the specialized keys will cost approximately $40 apiece.

Fire hydrant locks do not required specialized knowledge to install, and thus they can typically be installed by the owner's maintenance crews. Installation is quick - a typical lock that does not require the operating nut to be replaced can be installed in approximately five minutes. The locks do not typically require maintenance, and thus overall installation and maintenance costs are low.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

McGard Special Products Division
3875 California Road
Orchard Park, New York 14127
(716) 662-8980
www.mcgard.com

Mueller Company
500 West Eldorado Street
P.O. Box 671
Decatur, Illinois 62525
(217) 423-4471
www.muellercompany.com

Hydra-Shield Manufacturing, Inc.
3249 West Story Road
Irving, Texas 75038
(800) 676-0911
www.hydra-shield.com

Ladder Access Control

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

To delay access to assets such as roofs, raised water tanks, pipes, or other assets by controlling access to the ladders leading to the asset.

APPLICATION

Used to protect any indoor or outdoor ladder.

LOCATION USED

On any indoor or outdoor ladder, such as ladders leading to roofs, water tanks, raised pipes, or other raised assets.

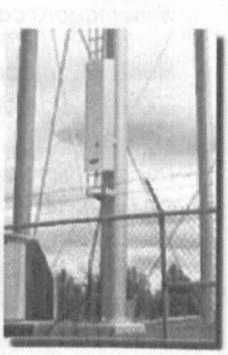
DESCRIPTION

Water and wastewater utilities have a number of assets that are raised above ground level, including raised water tanks, raised chemical tanks, raised piping systems, and roof access points into buildings. In addition, communications equipment, antennae, or other electronic devices may be located on the top of these raised assets. Typically, these assets are reached by ladders that are permanently anchored to the asset. For example, raised water tanks typically are accessed by ladders that are bolted to one of the legs of the tank. Controlling access to these raised assets by controlling access to the ladder can increase security at a water or wastewater utility.

A typical ladder access control system consists of some type of cover that is locked or secured over the ladder. The cover can be a casing that surrounds most of the ladder, or a door or shield that covers only part of the ladder. In either case, several rungs of the ladder (the number of rungs depends on the size of the cover) are made inaccessible by the cover, and these rungs can only be accessed by opening or removing the cover. The cover is locked so that only authorized personnel can open or remove it and use the ladder. Ladder access controls are usually installed at several feet above ground level, and they usually extend several feet up the ladder so that they cannot be circumvented by someone accessing the ladder above the control system.

Permanent Covers with Locking Doors

Permanent ladder covers usually consist of some type of door that is bolted over the ladder. The door hides the rungs and prevents them from being accessed when the door is closed and locked. To access the ladder, the door is unlocked and then opened, enabling the ladder behind it to be used. Several types of permanent covers are discussed below:

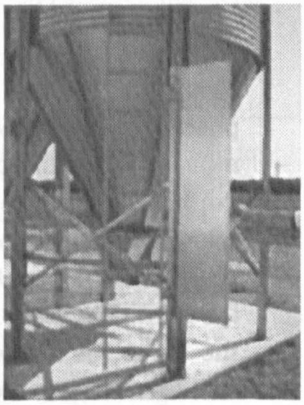

RB Industries, Ladder Gate

RB Industries manufactures the Ladder Gate, which consists of an 8 foot high by 36 inches wide by 1/8 inch thick aluminum cover that is installed over a ladder leading to a water tank, a raised pipe, or another raised asset. The Ladder Gate has a front and two sides. The front of the Ladder Gate fits over the front of the ladder and covers the rungs, preventing anyone from accessing the ladder from the front. The two sides extend behind the ladder and back to the base of the structure to which the ladder is attached. This prevents anyone from reaching around or behind the Ladder Gate to grasp the ladder. Therefor, although the Ladder Gate does not enclose the entire ladder, it does cover the front and both sides of the ladder for an 8 foot length.

The Ladder Gate's height ensures that intruders cannot reach above it to grasp the ladder. These systems are usually installed above ground level to provide additional height before an intruder could reach an unprotected part of the ladder. For example, by installing a Ladder Gate at 10 feet above ground level, an intruder would have to be 18 feet above ground level (10 feet plus the 8-foot height of the Ladder Gate) to reach the unprotected part of the ladder above the Ladder Gate.

The Ladder Gate is anchored to the ladder frame using 3 brackets that are bolted using galvanized steel bolts. Because the gate's hinge is at the angle between the side and the front of the unit, the hinge is not bolted directly to the ladder frame, which makes the system more secure. Another plate containing an eye bolt is mounted on the other side of the ladder. The side panel opposite the hinge has a slot through which the eye bolt fits when the Ladder Gate is closed. A padlock can then be placed on the eye bolt to lock the Ladder Gate. Depending on how the Ladder Gate is installed, it can be oriented so that it opens to the left or to the right. The system accommodates ladders up to 20 inches wide.

Two manufacturers (Brock Manufacturing and Carbis, Inc.) have designed ladder access controls that consist of a door that is fastened to one side of the ladder frame. When the door is open, the rungs are accessible, and the ladder can be climbed. When the door is closed and locked, the ladder rungs are blocked, and the ladder cannot be climbed. The door is secured by a padlock that locks the handle on the door to a hasp bolted to the ladder frame. Only authorized personnel can unlock the padlock, open the door, and access the part of the ladder behind the door. The Brock product is a 17 gauge galvanized steel door that is 6 feet high and weighs 30 lbs. The door is secured to the ladder frame by upper and lower hinges fastened with 5/16-inch bolts. The bolts are located on the inside of the door so they cannot be removed from the outside. The Carbis doors are also 6 feet high and are available in several materials, including aluminum and mill, primed, galvanized, or stainless steel. Carbis doors weigh from 22 to 56 lbs.

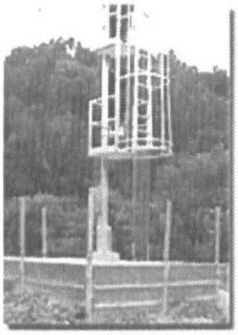


Brock Manufacturing, Locking Door Ladder Cover

While the Brock and Carbis doors protect access to the front side/outside of the ladder, they do not protect access from the back side of a free-standing ladder. Therefore, these products may be most appropriate for a ladder that is bolted to a wall because the wall prevents access to the other side of the ladder. However, even in the case of a freestanding ladder, access up the back side of the ladder may be blocked from above by the structure to which the ladder provides access.

Removable Covers

Serrmi Products, Inc. provides removable protective covers for ladders that it installs on structures designed for the railroad industry. The Serrmi ladder protection device is a 6 foot high aluminum sheet which weighs about 10 lbs and is hung from the upper rung of a ladder. The bottom of the sheet is locked in place using a bar that is placed behind the ladder and is padlocked to the aluminum cover. This prevents the cover from being moved vertically, which prevents it from being slid up and off the top rung from which it is hung. This product is currently manufactured for standard 16 inch-wide railroad industry ladders.

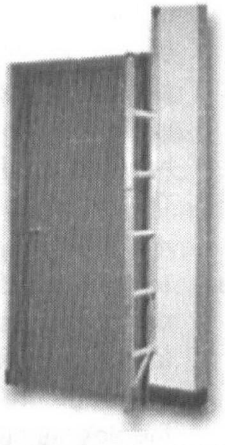


Serrmi Products, Inc. Removable Ladder Cover

The ladder covers described above can also be used on ladders with safety cages. However, they must be installed above or below the safety cages.

Folding Ladders

While the products discussed above are installed on existing ladders, Carbis, Inc. has designed a folding ladder that may also be appropriate for purchase and installation for security applications. Although it has primarily been marketed for other purposes (such as fire escape), the Carbis Security Access Ladder can easily be applied to provide protected access to rooftops or other raised assets. The ladder consists of a 12 inch-wide, marine-grade aluminum ladder that is hinged at the rungs so that it can close in on itself from side to side. One side of the ladder is bolted to a wall, and the other side of the ladder frame is folded up against it. To open the ladder, the free (unbolted) side of the ladder is pulled out and down away from the wall, which extends the rungs and moves them from a vertical to a horizontal position. To close the ladder, the free side of the ladder is pushed up and towards the wall, which folds the rungs up against the wall. The entire unit is only 2 inches wide when closed. The units can be secured using a normal padlock, which must be purchased separately. Depending on the ladder's design, the padlock can be installed at the top or the bottom of the ladder. When the ladder is closed and locked, the entire ladder is hidden from view and cannot be accessed. In addition, the closed unit is not easily recognized as a ladder. The unit is available in heights ranging from 9 to 26 feet. Because this unit must be bolted to an existing wall, it may be most appropriate to protect access to a building roof rather than an asset that does not have walls, such as a raised water tank or raised pipes.



Carbis, Inc. Security Access Ladder

ATTRIBUTES AND FEATURES

The important features of ladder access control are the size and strength of the cover and its ability to lock or otherwise be secured from unauthorized access.

The covers are constructed from aluminum or some type of steel. This should provide adequate protection from being pierced or cut through. The metals are corrosion resistant so that they will not corrode or become fragile from extreme weather conditions in outdoor applications. The bolts used to install each of these systems are galvanized steel. In addition, the bolts for each cover are installed on the inside of the unit so they cannot be removed from the outside. A discussion of these attributes is provided in Table 1.

Table 1 Ladder Access Control Systems

Manufacturer/ Product	Description	Discussion
HRB Industries Ladder Gate	Consists of an 8 foot high, 1/8 inch thick aluminum cover that covers the front and both sides of the ladder. It does not enclose the entire ladder.	This product is installed over an existing ladder, and can be installed on both freestanding and wall-mounted ladders. It weighs 65 lbs, and the manufacturer recommends that it be installed at least 10 feet above ground level
Brock Manufacturing Ladder Security Door	17 gauge galvanized steel door bolted to one side of an access ladder. Door secured by a padlock.	Protects only one side of the ladder (front side). Back side of ladder is accessible, but total access may be blocked by the structure that ladder leads to. May work best when ladder is against a wall so back side cannot be accessed.
Carbis, Inc. Security Cover	Available in aluminum or several types of steel. Door is bolted to one side of the ladder and is secured by a padlock.	Protects only one side of the ladder (front side). Back side of ladder is accessible, but total access may be blocked by the structure that ladder leads to. May work best when ladder is against a wall so back side cannot be accessed.
ACarbis, Inc. Security Access Ladder	Consists of a ladder that can fold up against a wall. The ladder is bolted to a wall and locked. The ladder must be unlocked and folded out to be used.	The ladder is closed up against a wall and locked, potentially providing two levels of security. First, the ladder is hidden from view and the structure may not be recognized as a potential access point to the raised asset that is being protected; and second, the ladder is locked, preventing access unless it is unlocked. The unit is very lightweight (between 12 and 26 lbs, depending on the size).
Serrmi Products, Inc. Ladder Locking Product	Aluminum plate is hung from an upper rung of a ladder and locked in place at a lower rung. The plate then covers several rungs of the ladder.	This is a very simple system for providing security to a ladder. It is removable and portable, which may give this product some advantages over other protection devices. Manufacturer supplies products to the railroad industry, but product could have applications to all types of ladders.

COST

RB Industries' Ladder Gate is sold by distributors, and costs approximately $750. A padlock to secure the door must be purchased separately. The Ladder Gate can be installed by the purchaser in approximately 1-2 hours. The manufacturer indicates that a team of 2 is typically needed for installation.

Carbis, Inc.'s Security Access Ladder ranges from $340 for the smallest model (shortest ladder) to $732 for the largest model. The Security Access Ladder can be installed by one person in less than an hour. It requires that holes be drilled into the wall on which the ladder will be installed so that the bolts can be anchored. A padlock to secure the compartment must be purchased separately.

The Carbis Security Covers range from $90 to $120 depending on the material. Padlocks are sold separately. The Security Covers can be installed easily by the purchaser.

The Brock Manufacturing Ladder Security Door costs $86. A padlock to secure the door must be purchased separately. Installation of the door is quick (less than one hour), and it can be installed by the purchaser.

The Serrmi ladder lock is currently not sold as a stand-alone product. However, interested parties should contact the manufacturer to discuss options for obtaining the product. The manufacturer indicates that this product is very simple to install and that installation can be done by a single staff person.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

R B Industries
P.O. Box 4734
Greensboro, North Carolina 27404
(336) 852-6276
www.laddergate.com

Serrmi Products, Inc.
PO Box 43346
5290 Tulane Rd.
Atlanta, Georgia 30336
(404) 691-8033
www.serrmi.com

Brock Manufacturing
611 N. Higbee St.
PO Box 2000
Milford, Indiana 46542
(574) 658-4191
www.ctbinc.com

Carbis, Inc.
1430 West Darlington St.
Florence, South Carolina 29501
(800) 948-7750
www.carbis.net

Locks

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Locks are used to prevent physical access to an asset.

APPLICATION

Locks are applied on any physical asset to be protected. Most applications require some type of strong physical structure to which the lock can be attached so that access to the asset is impeded or blocked. The use of locks also requires management of authorized access to the lock, which could include distribution and control of keys to the locks, distribution and control of combinations to the lock, management of data allowing the lock to be opened, etc.

LOCATION USED

Used on any physical asset that needs to be secured, including doors, windows, vehicles, cabinets, drawers, equipment, etc.

DESCRIPTION

A lock is a type of physical security device that can be used to delay or prevent a door, a window, a manhole, a filing cabinet drawer, or some other physical feature from being opened, moved, or operated. Locks typically operate by connecting two pieces together - such as by connecting a door to a door jamb or a manhole to its casement. Every lock has two modes - engaged (or "locked"), and disengaged (or "opened"). When a lock is disengaged, the asset on which the lock is installed can be accessed by anyone; but when the lock is engaged, only persons that can disengage the lock (through the use of a key, a combination, etc.) can gain access to the locked asset.

Locks are excellent security features because they have been designed to function in many ways and to work on many different types of assets. Locks can also provide different levels of security depending on how they are designed and implemented. The security provided by a lock is dependent on several factors, including its ability to withstand physical damage (i.e., can it be cut off, broken, or otherwise physically disabled) as well as its requirements for supervision or operation (i.e., combinations may need to be changed frequently so that they are not compromised and the locks remain secure). While there is no single definition of the "security" of a lock, locks are often described as minimum, medium, or maximum security. Minimum security locks are those that can be easily disengaged (or "picked") without the correct key or code, or those that can be disabled easily (such as small padlocks that can be cut with bolt cutters). Higher security locks are more complex and thus are more difficult to pick, or are sturdier and more resistant to physical damage.

Many locks, such as many door locks, only need to be unlocked from one side. For example, most door locks need a key to be unlocked only from the outside. A person opens such devices, called single-cylinder locks, from the inside by pushing a button or by turning a knob or handle. Double-cylinder locks require a key to be locked or unlocked from both sides.

Parts of a Lock

There are many different types of locks that function in many different ways. However, the basics of a lock are relatively standard. Every lock must have a fastening mechanism (i.e., a way to hold together the parts to be "locked"), and a method for engaging and disengaging the fastening mechanism. The fastening mechanism may be physical (such as a deadbolt lock that connects a door to a door jamb) or non-physical (for example, a strong magnetic current in an electromagnetic lock). Similarly, the method for engaging and disengaging the lock can also be physical (such as inserting a key or dialing a combination on a combination lock), magnetic (such as a door that is held in place by the force of two magnets), or electric (such as an electric signal that is generated when the correct keys are pressed on a keypad). Several major parts of typical types of fastening mechanisms are defined below. Different methods for engaging locks are described in more detail in the following sections.

Bolt/Latch and Strike-Type Locks

The bolt or latch is the part of a lock that extends into the strike to physically connect two objects. Bolts and latches are typically mounted within a door or on a window and are usually set on a spring so that they can be extended or retracted. When a bolt or latch is engaged, it slides across the open space between the two parts to be fastened, connecting them. The strike is the part of the lock into which the bolt or latch fits. For example, the strike could be a metal plate with a hollowed out area for the bolt inserted within a door frame.

Hasp and Shackle-Type Locks

A hasp is a fastener that consists of at least two parts that fit together or next to each other. An example is the hasp on a metal locker. This hasp consists of a fixed metal ring on the locker frame (usually oriented on the perpendicular) and a moveable metal ring mounted on the door. When the locker door is closed, the ring on the door can be moved over and behind the ring on the locker frame. A combination lock can then be put on the top ring. This lock prevents the bottom ring from moving across the top ring, and thus prevents the locker door from being opened.

A shackle is a physical device by which the parts of a hasp are connected, such as the curved metal piece in a padlock which fits through the rings of the hasp and then inserts into the base of the padlock.

Lock Types

There are many ways to name or describe a lock, including names that describe a lock's mechanical features and names describing the way the lock is used. Locksmiths often refer to locks based on their installation method. For example, a rim lock is a lock that mounts on the surface, or rim, of a door or object. A mortise lock is installed in a hollowed out, or mortised, cavity. In other cases, a generic term can be used to group together different types of locks that have similar features. For example, a "padlock" is a generic term used to describe removable, portable hasp and shackle type locks that consist of a piece of curved metal, both ends of which connect to a base. One of these ends is permanently attached to the base, but the other is attached to the base only when the lock is engaged. When the lock is disengaged, the piece of curved metal can be looped through a hasp to secure an asset, such as a door on a locker or a file cabinet drawer.

Locks can also be defined or described by their functional, or "locking," mechanism. Different types of locking mechanisms include keys, combinations, and electronic or magnetic signals. Keyed locks, which are among the most familiar types of locks, open after a person inserts and turns the correct key. Other locks, such as combination locks, are opened by pressing a series of buttons on a keypad or by turning a dial to the correct sequence of numbers or letters. Some electronic locks are opened by inserting a specially coded "key card." Sophisticated electronic locks open after a computer has identified a feature, such as a fingerprint, of the person desiring access.

Mechanical Locks

Mechanical locks have moving parts that operate without electric current. There are two types of mechanical locks: warded and tumbler.

Warded locks operate through the physical insertion of a key into the lock. These locks have several fixed ridges or obstacles called wards that fit the correct key and block other keys from operating the lock. When a person inserts the correct key, the key fits past the wards and moves a spring inside the lock. The bolt (or shackle) slides into a locked or unlocked position when the spring moves.

Warded locks are easy to pick with a stiff piece of wire or thin strip of metal. Therefore, warded locks are usually used in areas that do not require a high level of security.

Tumbler locks are similar to warded locks except that they have movable metal parts called tumblers that prevent the wrong key from opening the lock. Because tumblers provide more security than wards, most door locks use some type of tumbler arrangement.

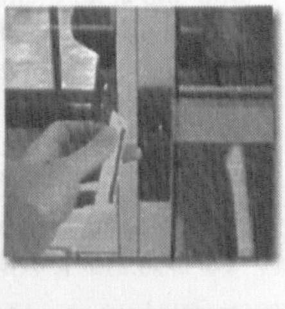
There are three types of tumbler locks. These are outlined in the table below.

Type of Tumbler Lock	Locations Commonly Used
Pin-tumbler locks (most common)	Automobiles
Disk-tumbler locks	Desks and file cabinets
Lever-tumbler locks	Briefcases and lockers

A combination padlock is a special disk-tumbler lock combined with a padlock. A combination padlock has a movable dial with a series of numbers around it. To open the lock, a person must turn the dial left and right in the correct sequence of numbers.

Electric Locks

Card Access Lock



Electric locks require electric current to operate. Many electric locks include electronic devices with scanners that identify users and computers that process codes. If the correct code or data is received by the scanner, computer, or other input device, an electric current engages or disengages the lock. The specific fastening devices used in electronic locks may be a bolt or an electromagnetic field. Types of electric locks include:

- card access systems
- electronic combination locks
- electromagnetic locks
- biometric entry systems

Card access systems, such as those used in many hotels and office buildings, are the most common electronic lock systems. A person desiring access needs a card or a special "key" to engage/disengage the lock. A device reads the code on the card and sends the information to a computer. If the code matches the one in the computer's memory, the locking mechanism releases and the door opens. Several different card access systems have been developed. One system uses a paperboard or plastic card, on which the code appears as a series of holes or bumps. Another system uses cards or keys that have their code on a microchip or a magnetic strip.

Card Access Lock

Electronic Combination Lock. Electronic combination locks are used in many stores and other businesses. To open a typical electronic combination lock, a combination or sequence of numbers must be entered on a numbered keypad. Once the combination is entered, the internal computer compares it with the combination stored in its memory and the door opens if the codes match.

Electronic
Combination Lock

Electromagnetic locks use magnetism rather than bolts to hold a door shut. In these locks, a strike is mounted on the top of the door. A strong electromagnet (a device that acts as a magnet when electric current flows through it) is fastened to the door frame in alignment with the strike. An electric current is put through the system, causing the electromagnet in the door to be attracted to the strike. To disengage the lock, a key is used to stop the flow of current. Doors with electromagnetic locks are often used as emergency exits from buildings. In some electromagnetic systems, the doors automatically unlock when a fire alarm is activated.

Other kinds of electric locks include some types of time locks and delayed-access timers. Time locks are designed to open only at certain times on certain days. They are commonly used on vaults or safes, and the release of the lock can be coordinated with shift changes or working hours. Once the correct combination has been entered, a safe protected by such a timer can only be opened at a pre-set time.

Biometric entry systems are unique forms of electric locks that identify a person by using a computer to compare the unique features of a fingerprint, palm, voice, eye, or signature with the one in its memory. In a fingerprint system, for example, a person who wants to open the lock places his or her finger on a plate. A scanner analyzes the print. If it matches the information in the computer's memory, the lock will disengage. Biometric entry systems are most often used in high-security areas.

Electric locks may be combined with mechanical locks to provide a higher amount of security than electric or mechanical locks alone. For example, electric bolt locks are a type of mechanical lock that provides higher security than magnetic locks. They are available in surface mount or concealed mortise mount and are often used for security applications where electromagnetic locks are not required.

Specifics on different types of locks, including individual information on costs and vendors, are provided in product guides on specific types of locks.

Manhole Locks

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Manhole locks can be used to prevent unauthorized physical access to sewer lines, water valves, or other water or wastewater assets via a manhole.

APPLICATION

Installing manhole locks on all manholes in a system may help to prevent unauthorized personnel from accessing or entering the system. Locking manholes may also prevent the introduction of hazardous substances into the storm water or wastewater system.

LOCATION USED

On any type of manhole.

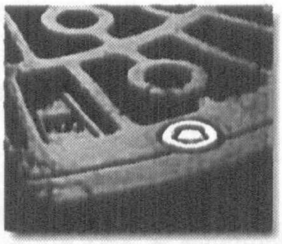
DESCRIPTION

Manholes are located at strategic locations throughout most municipal water, wastewater, and other underground utility systems. Manholes are designed to provide access to the underground utilities, and therefore they are potential entry points to a system. For example, manholes in water or wastewater systems may provide access to sewer lines or vaults containing on/off or pressure-reducing water valves. Because many utilities run underneath other infrastructure (roads, buildings), manholes also provide potential access points to other critical infrastructure as well as water and wastewater assets. In addition, because the portion of the system to which manholes provide entry is primarily located underground, access to a system through a manhole increases the chance that an intruder will not be seen. Therefore, protecting manholes can be a critical component of guarding an entire community.

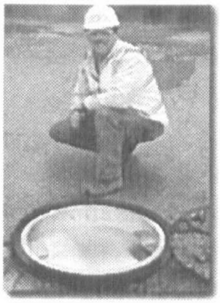
A "manhole lock" is a physical security device designed to delay unauthorized access to the utility through a manhole. Locking a manhole that provides access to a water or wastewater system can mitigate two distinct types of threats. First, locking a manhole may delay access of unauthorized personnel to water or wastewater systems or assets through the manhole. Second, locking manholes may also prevent the introduction of hazardous substances into the wastewater or storm water system. There are two design types for manhole locks: a bolt-type manhole lock and a pan-type manhole lock. These two design types are discussed below.

Bolt-Type Manhole Lock

McGard, Inc., has developed a bolt-type manhole lock called the Intimidator Man-Lock™. This product is a specialized bolt that is installed at two separate locations in the top of the manhole cover, anchoring the cover to the frame beneath the cover. The top of the bolt has a uniquely designed groove that can only be turned with a matching "key wrench." The bolt therefore serves as a locking mechanism and helps prevent unauthorized persons from opening the manhole cover.



The Intimidator™ Manhole Lock



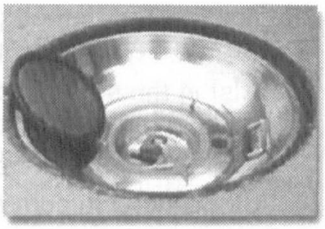
The No Access™ Manhole Lock

Pan-Type Manhole Lock

The pan-type manhole lock design consists of a steel pan that is inserted within the manhole and locked into place. This design does not lock the manhole cover on the manhole, but it physically obstructs the manhole entrance. The pan is typically 10 to 12 gauge stainless steel and has a flared edge that rests on the same base or frame ledge as the manhole cover. The body of the pan is more narrow than the manhole opening and is slightly recessed into the manhole. The locking mechanism is located in this recessed portion of the pan.

Two manufacturers currently market pan-type manhole locks. The No Access™ (patent pending) manhole security device by Henkels & McCoy consist of a pan which has two cutouts in its sidewalls, opposite from one another. Stainless steel pins are inserted horizontally from inside the pan through each cutout so that they extend outside the pan and under the manhole casement. An eyelet on each pin is matched to an eyelet welded to the interior wall of the pan next to each cutout. A padlock is then inserted through each eyelet pair to secure the pin in place. The manhole cover is then replaced over the pan and the manhole.

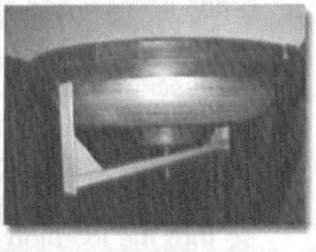
The LockDown-LockDry™ pan locking system, manufactured by Barton Southern Company, has been used since 1996. This pan locking system, secures the pan in the manhole with a "bolt and bar" system. After the manhole cover is removed, the steel "bar" portion of the system is tilted and lowered into the manhole. A threaded rod with a cable attached at the top is then screwed into the center of bar, forming a "t." The pan is then seated on the same ledge where the manhole cover normally sits. The pan has a hole through the center, and the cable attached to the threaded rod is pulled up through the center of the pan. As the cable is raised, the threaded rod is also pulled up through the center of the pan. A lock nut on the cable above the threaded rod is tightened down onto the threaded rod.



The LockDown-LockDry™ Manhole Lock

The Lockdown-Lockdry™ Manhole Lock

This pulls the steel bar upward towards the manhole frame, while compressing the pan down on the frame edge. This forms a seal between the manhole frame and pan and secures the pan in place. The threaded rod also has a hole bored through it. As the locknut is tightened, the threaded rod is pulled further upward, eventually exposing the hole. Once the hole is raised above the locknut, a padlock can be inserted through the hole. This prevents the loosening of the locknut and the lowering of the horizontal bar. The padlock is protected with a standard lock guard to deter unauthorized personnel from tampering. In addition, the entire lock, lock guard, and lock nut sit in a recessed portion of the pan, which is then concealed underneath a hinged cover plate to protect it from water and other contaminants. The manhole cover is then replaced over the pan and the manhole.



Section of the Lockdown-Lockdry™ Manhole Lock

As stated above, a standard padlock can be used to secure the locknut and pan locking assembly in place. For added security, more sophisticated locks are available that can sound an alarm or send out an electronic signal if they are disturbed. This can notify the owner of attempted unauthorized access to the manhole. These types of locks are available separately and are not part of the standard pan locking system supplied by the vendors.

An important security feature of each of the pan-type manhole locks is their seal against the manhole casement. A tight seal prevents groundwater inflow into the manhole. In addition, the seal can also be an effective barrier against the introduction of hazardous substances into the water or wastewater system. The LockDown-LockDry™ pan style locking system is designed to form a watertight seal with the manhole frame. The No Access™ pan locking system can be custom manufactured to form a watertight seal with the manhole frame.

Some utilities have constructed makeshift locks that consist of a steel bar bolted over a manhole. The bars are secured by padlocks, and the padlocks must be unlocked before the steel bar can be removed and the manhole can be accessed. These makeshift locks are usually located in off-street areas so that they do not impede vehicle traffic over the manhole.

ATTRIBUTES AND FEATURES

Bolt-Type Manhole Lock

The Intimidator Man-Lock™ bolt locking system uses a specialized bolt that is installed at two locations in the top of the manhole cover, anchoring it to the frame beneath the cover. The product is designed with several security features. First, the top of the bolt has a uniquely designed, patterned groove that can only be turned with a specially designed matching "key wrench." These specialized patterns are regionally distributed so that no two like patterns co-exist in the same geographical region. Each bolt type lock is also fitted with a threaded plastic cap to prevent debris from obstructing the keyed groove. To provide additional security, the bolt is either countersunk in the cover or has a special angled head to further protect against tampering with common gripping devices. Finally, Intimidator Man-Lock™ manhole cover locks are constructed from alloy or stainless steel, which can deter attacks from common tools and also withstand various environmental conditions. Custom plating is applied to suit a variety of different environments and applications. The vendor can be consulted to determine which grade of steel and plating is appropriate for a particular situation.

As described above, the Intimidator Man-Lock™ manhole cover locks can only be opened with specialized key wrenches. These specialized wrenches are tightly controlled and available only to authorized persons registered by the end-user so that they can access the manholes as needed. An inventory of wrenches and their serial numbers are generally kept by a municipality so that the location of all wrenches is known. Controlling access using these patented keys minimizes the potential for unauthorized access to the manholes.

Intimidator Man-Lock™ manhole cover locks do not require specialized knowledge to install, and they can typically be installed by the owner's maintenance crews with a special heavy duty electromagnetic drill and carbide-tipped drill bits. Installation instructions are provided by the vendor. The vendor can also be consulted to determine the appropriate bolt size for a given application, or to determine where to drill holes in different types of manhole covers. This type of manhole lock is suitable for retrofitting in place for concrete, steel and cast iron access covers of any size and shape. In addition, this lock can be retrofitted into manhole covers that are already fitted with non-locking bolts that secure the cover to the frame. Many of the current installations are in manholes which have been custom-ordered with pre-drilled holes in the manhole. These locks do not typically require maintenance, except for periodic greasing, and thus overall installation and maintenance costs are low.

The Intimidator Man-Lock™ can also be used to secure other infrastructure assets. For instance, this product can also be installed on most storm water and sewer grates, which could delay intruders from entering the storm water system.

Pan-Type Manhole Lock

Pan-type manhole locks are constructed from strong, durable, corrosion-resistant stainless steel. They require no special tools for installation, and installation requires no modifications to the manhole cover or frame. A typical installation can be accomplished by one person in a few minutes. The most important factor in choosing a pan-type manhole lock is choosing the right size for the manhole; therefore, taking proper measurements of the manhole diameter prior to ordering the pan-type manhole lock is essential. Vendors can help with any questions and will generally be willing to send a representative to take the required measurements if necessary. Standard padlocks can generally be used to secure the assembly, although vendors may recommend a specific type suitable to the owners' unique requirements.

COST

Bolt-Type Manhole Lock

The Intimidator Man-Lock™ bolt-type manhole locks range from about $10.00 per lock for orders over 1000 to around $20.00 per lock for orders less than 50. The manufacturer recommended that each manhole be fitted with two separate manhole locks to ensure security. The large t-shaped key wrench sells for around $40.00. They also make a smaller key adaptable to a regular socket wrench that costs about $16.50. Keys are available only to registered users.

Pan-Type Manhole Lock

Prices for the No Access™ manhole locking system by Henkels & McCoy, Inc. range from about $495 to $600 apiece depending on the manhole size and quantity ordered. Each No Access™ locking system is custom manufactured to the precise manhole dimensions required with each order.

Pricing for the LockDown-LockDry™ pan locking system from the Barton Southern Company ranges from about $390 to $525 apiece depending on the manhole size and quantity ordered. They can be ordered from standard sizes or they can be custom designed for specific needs.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

McGard, Inc.
3875 California Road
Orchard Park, New York 14127-4198
(716) 662-8980
www.mcgard.com

Henkels & McCoy, Inc.
985 Jolly Road,
Blue Bell, Pennsylvania 19422
(888) 436-5357
www.henkels.com

LockDown-LockDry Division,
Barton Southern Company
2387 Kinmor Industrial Parkway
Conyers, Georgia 30012
(800) 572-3119
www.lockdown-lockdry.com

Security for Doorways-Side Hinged Doors

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Protect a door from being forcefully entered. Security of the doorway can be enhanced by modifying the door, the door frame, the hinges, or the lock. Different doorway security measures may protect against various potential threats, including breaking, blasting, or fire.

APPLICATION

Can be applied to any doorway. An individual application may consist of modifying one or more features of the doorway, depending on the potential threats.

LOCATION USED

Used in any doorway that may be a target for intruders.

DESCRIPTION

Doorways are the main access points to a facility or to rooms within a building. They are used on the exterior or in the interior of buildings to provide privacy and security for the areas behind them. Different types of doorway security systems may be installed in different doorways depending on the needs or requirements of the buildings or rooms. For example, exterior doorways tend to have heavier doors to withstand the elements and to provide some security to the entrance of the building. Interior doorways in office areas may have lighter doors that may be primarily designed to provide privacy rather than security. Therefore, these doors may be made of glass or lightweight wood. Doorways in industrial areas may have sturdier doors than do other interior doorways and may be designed to provide protection or security for areas behind the doorway. For example, fireproof doors may be installed in chemical storage areas or in other areas where there is a danger of fire.

Because they are the main entries into a facility or a room, doorways are often prime targets for unauthorized entry into a facility or an asset. Therefore, securing doorways may be a major step in providing security at a facility. This Product Guide provides information on several areas that can help upgrade security for a doorway.

A doorway includes four main components:

- The door, which blocks the entrance. The primary threat to the actual door is breaking or piercing through the door. Therefore, the primary security features of doors are their strength and resistance to various physical threats, such as fire or explosions.

- The door frame, which connects the door to the wall. The primary threat to a door frame is that the door can be pried away from the frame. Therefore, the primary security feature of a door frame is its resistance to prying.

- The hinges, which connect the door to the door frame. The primary threat to door hinges is that they can be removed or broken, which will allow intruders to remove the entire door.

Therefore, security hinges are designed to be resistant to breaking. They may also be designed to minimize the threat of removal from the door.

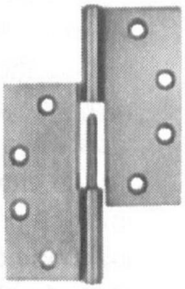
- The lock, which connects the door to the door frame. Use of the lock is controlled through various security features, such as keys, combinations, etc., such that only authorized personnel can open the lock and go through the door. Locks may also incorporate others security features, such as software or other systems to track overall use of the door or to track individuals using the door, etc.

Each of these components is integral in providing security for a doorway, and upgrading the security of only one of these components while leaving the other components unprotected may not increase the overall security of the doorway. For example, many facilities upgrade door locks as a basic step in increasing the security of a facility. However, if the facilities do not also focus on increasing security for the door hinges or the door frame, the door may remain vulnerable to being removed from its frame, thereby defeating the increased security of the door lock.

Security for doors, door frames, and hinges are discussed below. Locks are discussed in the Locks Product Guide.

Doors

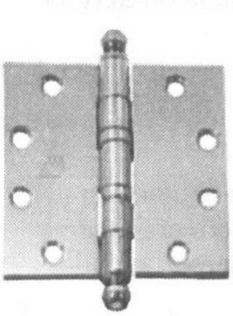
The door provides physical protection for the asset located behind it, and its main security aspects are its strength and resistance to physical damage from various forces, including physical instruments, fire, or explosion. "Security doors" is a generic term that usually refers to a door that is reinforced in some way to prevent damage to the door. Many security doors are manufactured from some type of metal (mainly steel) or wood with a steel frame or core. Security doors may be specialized to withstand fire, explosions, bullets, other projectiles, fragmentation, etc.



McKinney Two Knuckle Door Hinge

Doors may also have windows in them to allow people to see to the other side of the door. These windows are referred to as "glazing." Glazing on security doors may also have its own security features, such as bullet-, blast-, fire-, or shatter-resistance.

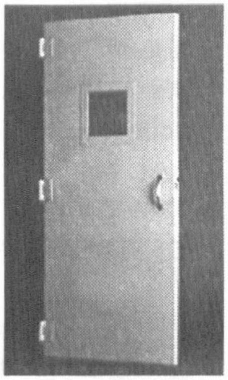
Door Frames



McKinney Five Knuckle Door Hinge

The door frame is the structure which integrates all of the other pieces of the doorway together. The door is hung from the door frame using hinges. The door frame anchors the doorway to the wall, and also provides a physical structure for the lock to connect the door to the wall. Door frames are typically anchored to a wall by screwing them into the wall; by casting them into the masonry as it is being erected or poured; by building them into stud partitions; or by welding them to a wall (if the wall is metal or if masonry is end-capped with steel channels or similar structures). Frames screwed into a wall are potentially the least secure of these frame types because the screws may be able to be removed, allowing removal of the frame.

Door hinges are used to secure any door to its door frame. A typical hinge includes two steel plates held together by a hinge pin. One plate is mounted to the door, and the other is mounted to the door frame. Steel screws are typically used to mount the plate to the door and the door frame. In general, the longer the screws, the more difficult it will be to remove the hinges, and therefore the door will be more secure. Hinges can be attached using wood screws, although machine screws are considered more secure.



Maximum Security Products Corporation Steel Door

ATTRIBUTES AND FEATURES

Doors and Frames

As described above, the primary attribute for the security of a door Is its strength. Many security doors are 14-20 gauge hollow metal doors consisting of steel plates over a hollow cavity reinforced with steel stiffeners to give the door extra stiffness and rigidity. This increases resistance to blunt force used to try to penetrate through the door. The space between the stiffeners may be filled with specialized materials to provide fire-, blast-, or bullet resistance to the door.

The Windows and Doors Manufacturers Association has developed a series of performance attributes for doors.

- Structural Resistance;
- Forced Entry Resistance;
- Hinge Style Screw Resistance;
- Split Resistance;
- Hinge Loading;
- Security Rating;
- Fire Resistance;
- Bullet Resistance; and
- Blast Resistance.

The first five bullets provide information on a door's resistance to standard physical breaking and prying attacks. These tests are used to evaluate the strength of the door and the resistance of the hinges and the frame in a standardized way. For example, the Rack Load Test simulates a prying attack on a corner of the door. A test panel is restrained at one end, and a third corner is supported. Loads are applied and measured at the fourth corner. The Door Impact Test simulates a battering attack on a door and frame using impacts of 200 foot pounds by a steel pendulum. The door must remain fully operable after the test. It should be noted that door glazing is also rated for resistance to shattering, etc. Manufacturers will be able to provide security ratings for these features of a door as well.

Door frames are an integral part of doorway security because they anchor the door to the wall. Door frames are typically constructed from wood or steel, and they are installed such that they extend for several inches over the doorway that has been cut into the wall. For added security, frames can be designed to have varying degrees of overlap with, or wrapping over, the underlying wall. This can make prying the frame from the wall more difficult. A frame formed from a continuous piece of metal (as opposed to a frame constructed from individual metal pieces) will prevent prying between pieces of the frame.

Many security doors can be retrofit into existing frames; however, many security door installations including replacing the door frame as well as the door itself. For example, bullet-resistance per Underwriter's Laboratory (UL) 752 requires resistance of the door and frame assembly, and thus replacing the door only would not meet UL 752 requirements.

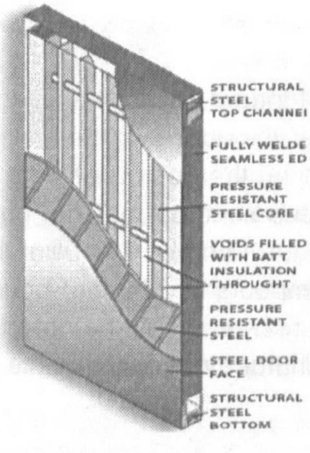
Specialty Security Doors

Some doors/door systems are also designed for resistance to other types of physical attacks, such as fire, explosion, or bullets. Doors designed to resist these types of incidents are discussed in more detail below.

Fire Resistance

Fire resistant and fire proof doors are specially manufactured to resistant burning and/or to reduce the temperature increase on the side of the door away from the fire. Resistance to burning is usually given as the number of minutes that it would take a door to burn under standard conditions (for example, a 20-minute fire door would take 20 minutes to burn, while a 90-minute fire door would take 90 minutes to burn). These ratings include evaluation of the fire resistance of the door, the door frame, and the hardware. Evaluations of temperature increases on the side of the door away from the fire are indicated as "temperature rise" ratings. The temperature rise rating indicates a maximum temperature rise, above ambient, developed on the unexposed face of the door at the 30 minute point of a Standard Fire Test. Thus, a door rated for a 250 degree temperature rise would only allow the temperature to rise 250 degrees on the other side of the door after 30 minutes, whereas a 450 degree temperature rise door would allow the temperature to rise 450 degrees.

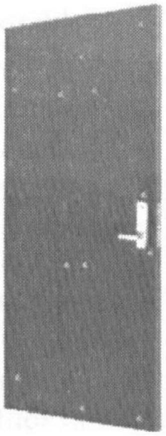
Ambico Blast Door Cutaway


STRUCTURAL STEEL TOP CHANNEI
FULLY WELDE SEAMLESS ED
PRESSURE RESISTANT STEEL CORE
VOIDS FILLED WITH BATT INSULATION THROUGHT
PRESSURE RESISTANT STEEL
STEEL DOOR FACE
STRUCTURAL STEEL BOTTOM

Door Cutaway

There are a number of different associations and organizations that provide fire ratings, including the American Society for Testing and Materials (ASTM), the National Fire Protection Association (NFPA), the Underwriters Laboratory (UL), and Intertek Testing Services - Warnock Hersey. The current standards for fire rating require testing under positive pressure; previous fire door ratings may be quoted under positive and/or negative pressure. Individual tests that may be performed or cited by manufacturers include ASTM E152 (Methods of Fire Tests of Door Assemblies), ASTM E-2074 (Standard Methods of Fire Tests of Door Assemblies, Including Positive Pressure Testing of Side-Hinged and Pivoted Swinging Door Assemblies), NFPA-80 (Fire Doors and Windows), NFPA 252 (Standard Methods of Fire Tests of Door Assemblies), and UL 10B (Fire Tests of Door Assemblies), Intertek Testing Services - Warnock Hersey (Fire Tests of Door Assemblies). It should be noted that most of these standards (for example, ASTM E-2074) do not provide information regarding the reduction of smoke or toxic gases provided by these doors. However, other standards (for example, ASTM Test Method E 84, which examines flame spread and smoke development) may provide information about these other factors.

Blast Resistance



Ceco Bullet Resistant Door

Blast-resistant doors are typically constructed of two metal plates enclosing a hollow cavity. The cavity typically contains an interior structure, such as reinforced steel ribbing or a steel frame. The void space may be filled with fire-resistant material or insulation to provide fire protection as well as blast protection. Typically, these doors are installed as an entire doorway and include a reinforced steel frame, blast resistant hinges, and blast resistant latching hardware.

In general, the doors are rated depending on the strength of the blast they are designed to withstand, as expressed in pounds per square inch (psi) and/or pounds per square foot (psf). As a general rule, the thicker and heavier the door, the higher the blast rating. However, as described above for fire-proofing, newer construction materials are reducing the need to merely make the door thicker to meet the blast-proofing requirements. Standard tests conducted by manufacturers to evaluate blast resistance of their products include meeting the requirements of Uniform Building Codes (UBCs), Institute of Building Control Officers (IBCO) standards, and ASTM E330-97e1 (Standard Test Method for Structural Performance of Doors by Uniform Static Air Pressure Difference). Testing for the blast doors also includes ensuring that the frame and the door hardware survive the blast.

Many manufacturers offer blast doors that can be retrofit into existing frames (including existing wooden frames). However, in many cases, the entire door system (door, frame, and hardware) must be purchased in order for the blast rating and the warranty to be valid.

Bullet Resistance

In contrast to blast proof doors, which are designed to withstand positive pressure over the entire door and at the hinges, bullet resistant doors are designed to absorb the impact of a bullet, which directs its impact force over a small area of the door. These doors are similar to blast-proof doors in that they contain a hollow inner cavity under an outer shell that can be constructed of heavy duty steel plates, or a solid wooden frame. In many of these doors, the hollow cavity contains a impact-disseminating material, such as fiberglass, polyurethane fiber, or mylar, which helps maintain the integrity of the door when it is struck by a bullet. Other doors have strengthening steel framework similar to the blast resistant doors. Standard tests conducted by manufacturers to evaluate bullet resistance of their products include meeting the requirements of UL 752 weapons criteria. UL 752 rates doors according to their ability to withstand bullets from different weapons - from handguns to rifles and high-powered weapons. Lower ratings offer resistance to lower-powered bullets. Ratings 1 to 3 cover traditional handguns (for example, a rating of 1 is resistant to a bullet from a .38 caliber handgun while a rating of 3 offers resistance to a bullet from a .44 Magnum revolver). Ratings of 4 and above cover high-powered weapons.

Ceco Bullet Resistant Door

As with blast-proof doors, many manufacturers offer bullet resistant doors that can be retrofit into existing frames (including existing wooden frames). However, in many cases, the entire door system (door, frame, and hardware) must be purchased in order for the bullet rating and the warranty to be valid.

Door Hinges

Two major features to consider for adequately secured hinges are their size and their construction material. Larger hinges provide more mass that must be bent or removed before an intruder can force off a hinge. In addition, depending on the construction material, larger hinges may be stronger than smaller hinges and thus will provide more resistance to tampering. A hinge's construction material is also important for strength. The three most commonly used materials for hinges are brass, chrome, and steel. Steel is the strongest of these three materials, and thus it may be most appropriate for security applications.

Plugs concealing the hinge pin. Adding a plug to the top of the hinge pin can provide added security for the hinge by preventing the hinge pin from being removed.

There are a number of specialized hinges types and hinge modifications that offer added security to the hinge, including non-removable pins, safety studs, and fast riveted pins. A non-removable pin has a "set screw" which is screwed through the hinge pin, preventing the pin from being pulled up vertically from the hinge. The set screw is accessible and can be removed when the door is open, but when the door is closed, it is inaccessible. A safety stud is a projection or stud that is molded onto one face of the hinge. When the door is closed, the stud fits into a cavity in the other hinge face. The connection of the studs when the door is closed will hold the door in place even if the hinges are removed. Finally, fast riveted, or crimped, pins, are made longer than the hinge, and then "spun" at the ends to flatten them such that they are wider than the pin hole and they cannot be removed unless the pin is cut.

COST

Doors and Frames

The cost of a security door is dependent on a number of factors, including the type of door, the size of the door, and its design specifications, among other things. This section provides some general costs for different types of security doors. It should be noted that costs for any actual application could be substantially different from the general cost information presented in this document depending on numerous site-specific variables, including the actual vendor chosen to supply the doors and hardware, local building requirements, the threat scenarios for which the door is designed, the hardware (hinges and locks) required to meet the design threat, and any site preparations necessary to install the door system.

Standard "security doors" are designed for strength and resistance vs. structural damage, such as from battering or prying. For example, Maximum Security Products Corporation's Maximum Protection Hollow Steel Door (including the frame), which is constructed from 10 gauge steel face plates with 3/16-inch internal stiffeners and is UL fire-rated, sells for approximately $1,600. A 14 gauge, 2-inch thick hollow metal door from Warren Doors is priced at approximately $1,400 for the door, but adding the door frame and appropriate hardware brings the cost closer to $2,000. The Ceco Door Products RestrictDor® Security Door, a 14 gauge, 2-inch thick hollow metal door, is similarly priced at $1,350-$1,500 for the door and frame.

Standard hollow metal doors can be easily designed with fire resistant cores instead of standard cores, and thus the price of fire-rated hollow metal doors may not be significantly higher than the cost of non fire-rated hollow metal doors. For example, purchasing a fire-rated hollow metal door from Warren Doors may only increase the cost by approximately $40 relative to a non fire-rated door.

In contrast to the relatively minor increase in cost in purchasing a fire-rated hollow metal door, blast-or bulletproof doors may be significantly more expensive. First, the cores of blast and bulletproof hollow metal doors are specially designed to withstand these types of stresses. Second, the door frame, hardware, hinges, and lock must all be rated for withstanding the stress as well, and upgrading these components will increase costs.

While the specific costs will depend on the specific stresses that the door is designed to withstand, purchasers can expect to spend between $1,500 and $10,000 per door for bullet and blast-resistant doors. For example, the Ceco Door Products ArmorShield Level 3 Door and Frame System (rated for UL 752 Level 3, designed to withstand a bullet from a .44 Magnum revolver), which is comprised of a 1 -inch thick 16 gauge steel door with a stiffened steel core and a 14 gauge frame, costs approximately $1,500. This does not include hinges or other hardware, which will be additional costs (for example, the required hinges will cost approximately $200). Similar Level 3 rated doors from Ambico Limited and Krieger Products would cost approximately $1,800. Doors that provide Level 4 resistance and higher (resistance to rifles and higher-powered weapons) cost significantly more than doors rated at Levels 1 to 3.

A door rated for a small explosion (for example, a force of 100 psf) would be in the $2,000 or more, while a door rated for a blast of 5 psi would be closer to $4-$5,000. For example, Krieger Specialty Products, Inc., markets a 1 3/4-inch thick door able to withstand a blast of 100 psf for approximately $2,000. Specialty Doors, Inc.'s BR-07 door is a 1 3/4-inch hollow metal blast door designed to withstand a blast pressure of 150 psf. This door costs approximately $5,000. The BR-20 model, which is 2 3/4 inches thick and is designed to withstand a blast of 6 psi, is approximately $8,000. A Krieger door designed to withstand a 5 psi blast would be in the $4-$5,000 range. Doors rated for larger blasts would be in the $6,000 or higher range.

The costs for installing security doors can be substantial, particularly for doors where the entire doorway (frame, door, hinges, and other hardware) must be replaced. However, these doors can typically be installed by a facility's maintenance crew, if they are familiar with installing frames and doors.

Door Hinges

Costs for door hinge protection systems can vary greatly depending on the level of complexity. Hinge costs depend on the type of hinge purchased, the material, and the finish. The major differential in cost is the style. For instance, hinges with an exposed pin and no extra features cost approximately $9 to $15. A hinge with a concealed ball bearing will cost from $20 to $25. A hinge with a concealed ball bearing and concealed hinge pin will cost approximately $140-$150.

Security hinges can be installed by any facility maintenance crew. Manufacturer installation is not necessary.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

General Security Doors

Commercial Doors and Accessories Inc.
P.O. Box 1503
Macon, Georgia 31202
(800) 689-3667

Maximum Security Products Corporation
3 Schoolhouse Lane
Waterford, New York 12188
(518) 233-1800
www.maximumsecuritycorp.com

Ceco Door Products
9159 Telecom Drive
Milan, Tennessee 38358
(888) 232-6366
www.cecodoor.com

Warren Door
332 Plant Street - PO Box 70
Niles, Ohio 44446
(800) 255-3667
www.warrendoor.com

Norshield Security Products
3224 Mobile Highway
Montgomery, Alabama 36108
(800) 633-1968
www.norshieldsecurity.com

Amweld Building Products, Inc.
PO Box 267
1500 Amweld Drive
Garrettsville, Ohio 44231
(330) 527-4385
www.amweld.com

Fire Resistant Doors

Advance Fiberglass, Inc.
PO Box 13268
Maumelle, Arkansas 72113
(800) 342-7367
www.fibrdor.com

Karona Doors, Inc.
4100 Karona Court
Caledonia, Michigan 49316
(800) 829-9233
www.karonadoor.com

Blast Doors

Overly Door Company
574 West Otterman Street
Greensburg, Pennsylvania 15601
(800) 979-7300
www.overly.com

Krieger Specialty Products
4880 Gregg Road
Pico Rivera, California 90660
(866) 203-5060
www.kriegersteel.com

Ambico Limited
1120 Cummings Avenue
Ottawa, Ontario K1J 7R8
(613) 746-4663
www.doors-ambico.com

Specialty Doors, Inc.
269 West 154th Street
South Holland, Illinois 60473
(708) 339-4331

Bullet Resistant Doors

Gaffco
6 North Street
Mount Vernon, New York 10550
(914) 663-9266
www.gaffco.com

Krieger Specialty Products
4880 Gregg Road
Pico Rivera, California 90660
(866) 203-5060
www.kriegersteel.com

Safeguard Security Services, Ltd.
4728 Goldfield, Building 8
San Antonio, Texas 78218
(800) 880-8306
www.armortex.com

Specialty Hinges

Habersham Metal Products Company
264 Stapleton Road
Cornelia, Georgia 30531
www.habershammetal.com

McKinney Products Company
820 Davis Street
Scranton, Pennsylvania 18505
(800) 346-7707
www.mckinneyhinge.com

Daro Industries, Inc.
3905 California Street, NE
Columbia Heights, Minnesota
(877) 865-4154
www.daro-ind.com

Locks4Less
3225 S. 116th Street
Suite 169
Seattle, Washington 98168
(866) 562-7453
www.locks4less.com

Valve Lockout Devices

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

To prevent or delay unauthorized access to a valve.

APPLICATION

Used to ensure a valve remains in the desired position and is not tampered with by an unauthorized individual. Valve lockout devices are placed on, over, or through valve handles to prevent rotation.

LOCATION USED

On valves located in water or wastewater treatment plants, remote facilities (pumping stations, etc.), water distribution systems, backflow prevention devices, and other piping systems.

DESCRIPTION

Valves are utilized as control elements in water and wastewater process piping networks. They regulate the flow of both liquids and gases by opening, closing, or obstructing a flow passageway. Valves are typically located where flow control is necessary. They can be located in-line or at pipeline and tank entrance and exit points. They can serve multiple purposes in a process pipe network, including:

- Redirecting and throttling flow;
- Preventing backflow;
- Shutting off flow to a pipeline or tank (for isolation purposes);
- Releasing pressure;
- Draining extraneous liquid from pipelines or tanks;
- Introducing chemicals into the process network; or
- As access points for sampling process water.

Valves are located at critical junctures throughout water and wastewater systems, both on-site at treatment facilities, and off-site within water distribution and wastewater collection systems. They may be located either aboveground or below ground. Because many valves are located within the community, it is critical to provide protection against valve tampering. For example, tampering with a pressure relief valve could result in a pressure buildup and potential explosion in the piping network. On a larger scale, addition of a pathogen or chemical to the water distribution system through an unprotected valve could result in the release of that contaminant to the general population.

Different security products are available to protect aboveground vs. below ground valves. For example, valve lockout devices can be purchased to protect valves and valve controls located aboveground. Vaults containing underground valves can be locked to prevent access to these valves. This Product Guide will focus on security for aboveground valves. A separate Product Guide covers security for underground valves.

As described above, a lockout device can be used as a security measure to prevent unauthorized access to aboveground valves located within water and wastewater systems. Valve lockout devices are locks that are specially designed to fit over valves and valve handles to control their ability to be turned or operated. These devices can be used to lock the valve into the desired position. Once the valve is locked, it cannot be turned unless the locking device is unlocked or removed by an authorized individual.

Various valve lockout options are available for municipal and industrial use, including:

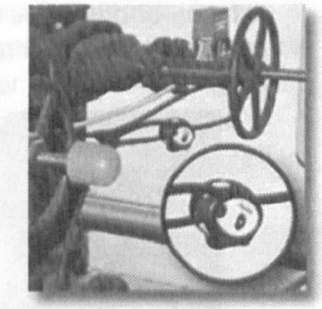
- Cable lockouts;
- Padlocked chains/cables;
- Valve-specific lockouts; and
- Valve box-locks.

Many of these lockout devices are not specifically designed for use in the water/wastewater industry (i.e., chains, padlocks), and are available from a local hardware store or manufacturer specializing in safety equipment. Other lockout devices (for example, valve-specific lockouts or valve box-locks) are more specialized and must be purchased from safety or valve-related equipment vendors.

ATTRIBUTES AND FEATURES

Cable Lockouts

A cable lockout is a section of cable with an attached locking device. Depending on the valve configuration, the cable lockout is looped around or through the spokes of the valve handle, then through another part of the piping system or to an anchoring device in the floor, and finally back through the attached lock. The cable can be pulled tight so that the tension on the cable prevents the handle from being turned. For maximum security protection, cable lockouts can be manufactured from coated, braided steel, which is highly resistant to cutting.



Cable Lockout

Padlocked Chains/Cables

Padlocked chain/cable valve lockouts work in very much the same fashion as cable lockouts, except that they do not have an integrated locking device. Instead, they must be secured with a separate padlock. The chain/cable is looped around or through the spokes of the valve handle, and is then secured to another part of the piping system or to an anchoring device in the floor. The chain/cable can be pulled tight and secured with the padlock so that the tension on the chain/cable prevents the handle from being turned. Chains and cables are available in a wide variety of shapes and strengths, and are most easily purchased through a local hardware store. Hardened steel cables and chains are manufactured for security applications. They are designed to be wear and cut resistant, and to provide a long service life.

Valve-Specific Lockouts

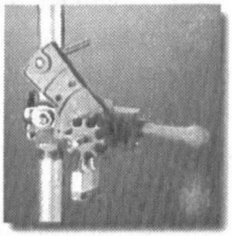
Valve-specific lockout devices are self-contained lockouts that are typically used to cover the valve handle to prevent its rotation, which, in turn, prevents the opening or closing of the valve. They are placed over the valve handle and secured in place with a separate padlock.

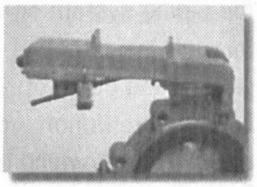
Valve-specific lockout devices are typically similar in design, although they may have minor variations according to the type of valve being locked. They are typically manufactured from polypropylene, so they are nonconductive. Other design specifications include corrosion-resistance (to protect them from potential chemical or solvent spills), temperature-resistance (typically to temperatures of up to 360°F), and weather-resistance.

The three most common types of valves for which lockout devices are available are gate, ball, and butterfly valves. Each is described in more detail below.

- **Gate Valve Lockouts** - Gate valve lockouts are designed to fit over the operating hand wheel of the gate valve to prevent it from being turned. The lockout is secured in place with a padlock. Two types of gate valve lockouts are available: diameter-specific and adjustable. Diameter-specific lockouts are available for handles ranging from 1 inch to 13 inches in diameter. Adjustable gate valve lockouts can be adjusted to fit any handle ranging from 1 inch to 6 inches in diameter.
- **Ball Valve Lockouts** - There are several different configurations available to lock out ball valves, all of which are designed to prevent rotation of the valve handle. The three major configurations available are a wedge shape for 1 inch to 3 inch valves, a lockout that completely covers 3/8 inch to 8 inch ball valve handles, and a universal lockout that can be applied to quarter-turn valves of varying sizes and geometric handle dimensions. All three types of ball valve lockouts can be installed by sliding the lockout device over the ball valve handle and securing it with a padlock.

Gate Valve Lockout


Ball Valve Lockout


Butterfly Valve Lockout

- **Butterfly Valve Lockouts** - The butterfly valve lockout functions in a similar manner to the ball valve lockout. The polypropylene lockout device is placed over the valve handle and secured with a padlock. This type of lockout has been commonly used in the bottling industry.

A major difference between valve-specific lockout devices and the padlocked chain or cable lockouts discussed above is that they do not need to be secured to an anchoring device in the floor or the piping system. In addition, valve-specific lockouts eliminate potential tripping or access hazards that may be caused by chains or cable lockouts applied to valves located near walkways or frequently maintained equipment.

Valve-specific lockout devices are available in a variety of colors, which can be useful in distinguishing different valves. For example, different colored lockouts can be used to distinguish the type of liquid passing through the valve (i.e. treated, untreated, potable, chemical), or to identify the party responsible for maintaining the lockout. Implementing a system of different-colored locks on operating valves can increase system security by reducing the likelihood of an operator inadvertently opening the wrong valve and causing a problem in the system.

PADLOCKS

As described above, padlocks are required for securing several different types of valve lockout devices. Padlocks are available in a variety of sizes and strengths, and with a number of different locking mechanisms (for example, keyed or numerical combination padlocks). Maximum-security padlocks are manufactured with a hardened boron alloy shackle and laminated steel body for strength and cut resistance. More specific information on padlocks is available from the Locks Product Guide.

Controlling the padlocks and implementing an effective key control process is essential in ensuring that the system is adequately protected. Key control includes tracking which keys can open which locks and ensuring that authorized personnel receive the correct keys for the locks for which they are responsible. There are three general types of keying strategies when multiple valves are locked in a system. These are:

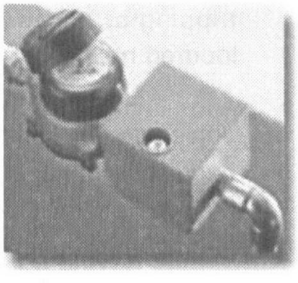
- Keyed-alike systems;
- Master-keyed systems; or
- Individually-keyed padlocks.

In keyed-alike systems, all the locks can be opened with the same key. In a master-keyed system, groups of locks can be opened with the same key. For example, locks could be individually keyed so that each individual would be responsible for his/her own padlock; groups of padlocks could be keyed alike so that only employees in a single group (for example, maintenance personnel) could access a specific group of padlocks; or all of the padlocks in a facility, whether individually- or group-keyed, could be opened by a single master key. In an individually-keyed padlock system, there is no master key, and all of the locks must be opened with their own key.

As with valve-specific lockouts, padlocks are available in different colors. Utilities can use different-colored valve locks to identify specific valves, which can enhance security as described in the Valve-Specific Lockout discussion above.

Valve Box-Locks

Unlike the other types of lockout devices described above, which are designed to prevent a valve handle from being turned, valve box-locks are used to fully enclose the valve and prevent unauthorized access to the valve and its connection points. For example, McGard's Intimidator Valve Box-Lock™ is designed to enclose both the shutoff valve and the coupling nut, thereby preventing tampering with the shutoff valve. The Box-Lock™ consists of two 16-gauge steel pieces that are fastened around an existing straight through- or right angle valve using a specialized locking screw. The screw can only be removed using a specially coded T-key, which is provided by the manufacturer. Installing the box is relatively easy and no modifications are required to the existing valve.



McGard's Intimidator Valve Box-Lock™

COST

Valve lockout devices are generally low cost, and thus locking out the valves in a system can be a relatively inexpensive means of protecting water and wastewater process and distribution/collection systems. Table 1 summarizes costs for several lockout devices.

Table 1: Valve Lockout Costs

Lockout Device	Cost
APadlocks: Keyed Combination	\$6 - \$12 \$20
Cable lockout	\$15 - \$35
Cables and Chains	2 - \$20 per foot
Ball valve lockout	\$25 - \$75
Butterfly valve lockout	\$85
Gate valve lockout	\$30 - \$100
Valve box-lock Coded T-key	\$25 - \$35 \$12

Cost information provided by emedco and McGard Inc.

In addition to their low costs, valve lockouts are easy to acquire and implement. Some types of lockouts, such as chains and padlocks, can be easily purchased at local stores. Other lockouts can be obtained through the internet. The lockouts can be installed easily with minimal labor hours because they do not typically require any modification to the existing valve.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

McGard, Inc.
3875 California Road
Orchard Park, New York 14127-4198
(716) 662-8980
www.mcgard.com

ANorth Safety Products
2000 Plainfield Pike
Cranston, Rhode Island 02921
(800) 430-4110
www.northsafety.com

Prinzing Enterprises, Inc.
30W 196 Calumet Avenue
Warrenville, Illinois 60555
(800) 292-2914
www.prinzing.com

Smith Flow Control (USA)
21 Kenton Lands Road
Erlanger, Kentucky 41018
(859) 578-2395
www.smithflowcontrol.com

Swagelok Company
29500 Solon Road
Solon, Ohio 44139
(440) 248-4600
www.swagelok.com

emedco
P.O. Box 369
Buffalo, New York 14240
(800) 442-3633
www.emedco.com

A BlueBook
PO Box 9004
Gurnee, Illinois 60031-9004
(800) 548-1234
www.usabluebook.com

Sharpe Safety Supply, Inc.
PO Box 3477
Chester, Virginia 23831
(804) 796-4777
www.sharpesafety.com

Regulatory Consultants, Inc. (RCI)
140 West 8th Street
Horton, Kansas 66439
(800) 888-9596
www.rci-safety.com

ANI Safety & Supply, Inc.
PO Box 228
Skokie, Illinois 60076-0228
(800) 676-5581
www.anisafety.com

Visual Surveillance Monitoring

○ DETECT
● DELAY
○ RESPOND

OBJECTIVE

Visually monitor an asset to detect potential intruders, unauthorized or suspicious materials or objects, or other threats.

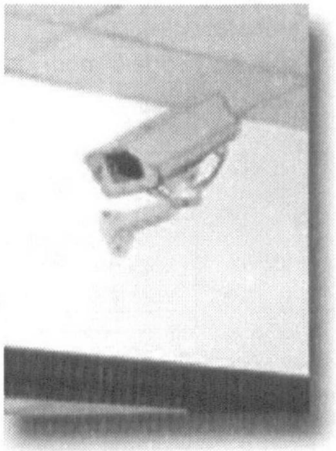
APPLICATION

Used to detect physical threats to an asset (i.e., persons or materials) through surveillance of asset. Can be used to monitor any water or wastewater assets (perimeter of facility, remote pumphouses, potential access points to distribution or collection systems, etc.). Primarily used to monitor exterior areas, but can be used in interior of buildings or facilities.

LOCATION USED

Usually mounted at a strategic location at the asset to be monitored to monitor as large an area as possible. Can be mounted near doors or windows, on or along fences, or within buildings.

DESCRIPTION



Visual surveillance is used to detect threats through continuous observation of important or vulnerable areas of an asset. The observations can also be recorded for later review or use (for example, in court proceedings). Visual surveillance systems can be used to monitor various parts of collection, distribution, or treatment systems, including the perimeter of a facility, outlying pumping stations, or entry or access points into specific buildings. These systems are also useful in recording individuals who enter or leave a facility, thereby helping to identify unauthorized access. Images can be transmitted live to a monitoring station, where they can be monitored in real time, or they can be recorded and reviewed later. Many facilities have found that a combination of electronic surveillance and security guards provides an effective means of facility security.

Visual surveillance is provided through a closed circuit television (CCTV) system, in which the capture, transmission, and reception of an image is localized within a closed "circuit." This is different than other broadcast images, such as over-the-air television, which is broadcast over the air to any receiver within range.

ATTRIBUTES AND FEATURES

At a minimum, a CCTV system consists of:

- One or more cameras;
- A monitor for viewing the images; and
- A system for transmitting the images from the camera to the monitor.

Specific attributes and features of these components are presented in the tables that follow.

Camera Systems

Cameras capture the image for transmission to the monitor. They consist of a lens, which focuses light into the camera, and a system to convert that captured light into an electronic signal which can be transmitted to the monitor. The characteristics of the lens and the camera affect their ability

Table 1: Attributes of Camera Systems

Attribute	Discussion
Camera Types	Major factors in choosing the correct camera are the resolution of the image required and lighting of the area to be viewed (see discussions of these topics below). • **Solid State** (including charge coupled devices, charge priming device, charge injection device, and metal oxide substrate) - these cameras are becoming predominant in the marketplace because of their high resolution and their elimination of problems inherent in tube cameras. • **Thermal** - these cameras are designed for night vision. They require no light and use differences in temperature between objects in the field of view to produce a video image. Resolution is low compared to other cameras, and the technology is currently expensive relative to other technologies. • **Tube** - these cameras can provide high resolution but the tubes burn out and must be replaced after 1-2 years. In addition, tube performance can degrade over time. Finally, tube cameras are prone to burn images on the tube. This requires tube replacement.
Resolution (the ability to see fine details)	User must determine the amount of resolution required depending on the level of detail required for threat determination. A high definition focus with a wide field of vision will give an optimal viewing area.
Field of vision width	Cameras are designed to cover a defined field of vision, which is usually defined in degrees. The wider the field of vision, the more area a camera will be able to monitor.
Type of image produced (color, black and white, thermal)	Color images may allow the identification of distinctive markings, while black and white images may provide sharper contrast. Thermal imaging allows the identification of heat sources (such as human beings or other living creatures) from low light environments; however, thermal images are not effective in identifying specific individuals (i.e., for subsequent legal processes).
Pan/Tilt/Zoom (PTZ)	Panning (moving the camera in a horizontal plane), tilting (moving the camera in a vertical plane), and zooming (moving the lens to focus on objects that are at different distances from the camera) allow the camera to follow a moving object. Different systems allow these functions to be controlled manually or automatically. Factors to be considered in PTZ cameras are the degree of coverage for pan and tilt functions and the power of the zoom lens.

Table 2: Attributes of Lenses

Attribute	Discussion
Format	Lens format determines the maximum image size to be transmitted.
Focal Length	This is the distance from the lens to the center of the focus. The greater the focal length, the higher the magnification, but the narrower the field of vision.
F Number	F number is the ability to gather light. Smaller F numbers may be required for outdoor applications where light cannot be controlled as easily.
Distance and width approximation	The distance and width approximations are used to determine the geometry of the space that can be monitored at the best resolution.

Table 3: Attributes of Lighting Systems

Attribute	Discussion
Intensity	Light intensity must be great enough for the camera type to produce sharp images. Light can be generated from natural or artificial sources. Artificial sources can be controlled to produce the amount and distribution of light required for a given camera and lens.
Evenness	Light must be distributed evenly over the field of view so that there are no darker or shadowy areas. If there are lighter vs. darker areas, brighter areas may appear washed out (i.e., details cannot be distinguished) while no specific objects can be viewed from darker areas.
Location	Light sources must be located above the camera so that light does not shine directly into the camera.

to capture sharp images from a specific field of view under variable light conditions. Cameras and lenses can be purchased separately, which allows users to design a system that is tailored to their needs. Important attributes of camera systems, lenses, and lighting systems are provided in Tables 1-3 below.

Another important consideration when choosing cameras is whether they will be used indoors or outdoors. Camera location will determine the types of lighting available, as well as the types of cameras and lenses that are applicable. Cameras mounted outdoors may require climate-specific weatherproof housing, heaters for snow/ice blockage or reduction, blowers to reduce fogging, etc. These additional features will add to the cost and flexibility of the system.

TRANSMISSION SYSTEMS

Systems may be hardwired (physically connected by cables) or wireless. While hardwiring (such as through coaxial or fiber optic cables) is the traditional method for transmitting video signals in a CCTV system, new wireless applications, such as microwave links, optical systems, and radio frequencies, are becoming more prevalent.

Hardwired systems require a direct physical connection between the transmitter and the receiver. Because the signal is transmitted directly to the receiver and not over the air, hardwired systems may be more secure than wireless systems. However, it may be difficult to hardwire remote locations. Specific factors affecting hardwired cable connections include:

- **Bandwidth:** related to the amount of information that can be transmitted along the system. Affects resolution of recorded vs. received signal.

- **Line loss:** some cables may lose some of the signal depending on their design, and therefore may require signal conditioning to compensate.

- **Signal conditioning:** May be required to compensate for distorted signal based on the types of transmission equipment used.

Wireless transmission systems do not require that the transmitter and the receiver be physically connected to each other. This may make wireless more attractive for remote locations. However, wireless systems require a direct line of sight between transmitter and receivers and may require re-transmitters (also known as repeaters and amplifiers) for remote operations. In addition, wireless systems may be susceptible to interception or interference.

MONITORS

Monitors are used to view images transmitted by cameras. Factors to be considered when choosing the appropriate monitor for a specific application include:

- **Bandwidth:** The monitor's bandwidth should be equivalent to camera/lens bandwidth. This will allow the best resolution of the image transmitted from the camera to be viewed on the screen.

- **Color vs. black and white:** The use of a color vs. black and white monitor depends on user's preference. In some cases, black and white may offer more contrast, but color may offer easier identification of specific or tell-tale marks (distinctive clothing, hair color, skin color).

- **Screen size.** A larger screen and color image make live feed identification more accurate to the employee using the system.

IMAGE STORAGE

In many cases, images generated by camera systems may be stored for later viewing. While the detection of certain images may require real-time, immediate action (such as when intruders are detected), the ability to store and view images at a later time may be important for forensic purposes (i.e., to determine what or how an event occurred at a site) or for legal actions to be taken at a later date. Options for image storage include:

- Digital video recording (DVR) - stores digital images on a PC or on a network/server system;

- Video recording (VCR) - stores images on videocassettes; and

- Solid state recording - stores individual images or frames on a solid state disk.

DVR is rapidly replacing video cassette recording VCR as the medium of choice for recording and storing images. DVR devices record and store images digitally on a computer hard drive (i.e., a PC, handheld computer, or dedicated DVR system) vs. devices such as VCRs, which store images on videotapes using analog technology. Costs for DVR systems have declined in recent years while technology has improved. Other advantages vs. VCRs include:

- Longer recording period
- Clearer images
- Clearer resolution of still ("paused") images
- Search functions enable users to immediately locate images by camera, date, or other methods
- Image files do not degrade over time
- *Requires less storage space than VCR tapes*

However, some digital storage systems using PC hard drives require that the entire PC be dedicated to this system. This may not be practical for some utilities.

One of the important features when setting up a DVR system is determining how many frames per second (fps) will be recorded. The more fps that are recorded, the clearer the image will be, and it will be easier to view still pictures from the camera. However, the more fps that are stored, the more storage space will be required on the hard drive. Many DVRs also have a motion sensor mode that can be set to trigger an action (such as recording or an alarm) when the camera detects motion in its field of vision.

Table 4: Enhanced System Features

Feature	Factors to Consider	Benefits to the System
Video Switcher	Control can be active (controlled by user) or passive (viewed or recorded area switches automatically).	Switches cameras being viewed on monitor or recorded. Can be used to switch monitor or recorder to image tripping an alarm.
Video Controller	Interface between the visual surveillance system and other electronic processes, such as alarm or alert systems.	Can be used to automatically sound alarms based on interpreted data.

Table 4 provides a discussion of several optional features which enhance the management of a CCTV system.

COST

Components for a CCTV/visual surveillance system can be sold separately, or packaged systems may be purchased. For example, a typical lower-end package consisting of a 4 camera CCTV system consisting of cameras/lenses, cables, power supplies, and a monitor can cost as little as $550. This is a capital cost only and does not include maintenance or installation costs, which are facility dependent.

Costs for individual components depend on their specifications. Several example costs and *factors affecting costs are provided in Table 5 on the next page.*

Table 5: Costs for Visual Surveillance Components

Component	Cost	Factors Affecting Cost
Cameras	Black and White: $80 Color: $130 PTZ: $350-$3,000	Resolution desired and the amount of light required for the camera to function properly
Lenses	Manual iris 8 mm lens (for steady-light applications): $50 Auto iris 3.7 mm lenses (for use in applications where light conditions are variable): >$200	Zoom lenses are more expensive.
Monitors	Black and white monitor with 1 camera input: $330 Color monitor with 4 camera inputs: $1,000	The cost of monitors depends on the resolution, the image (black and white or color) and the number of inputs (for example, inputs for one camera vs. inputs for four cameras).
— Storage Systems —		
VCR	VCR unit: <$60 Individual videotapes are several dollars apiece	Higher end features can increase resolution of paused images.
DVR	Low end unit: $770. Higher end units (a 16 camera system capable of recording at 240 frames per second, with a 240GB hard drive): >$5,500	DVR costs depend on the number of camera inputs and the hard drive storage space.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Control Electronic Security
8245 NW 36th Street, Suite #6
Miami, Florida 33166
(305) 499-9396
www.controlelectronic.com

Sperry West Inc.
5575 Magnatron Blvd
San Diego, California 92111
(858) 551-2000
www.sperrywest.com

Extreme Surveillance
Fiesta Tech Business Centre
2150 South Country Club Drive, Suite 16
Mesa, Arizona 85210
(800) 788-7101
www.extremesurveillance.com

Axis Communications, Inc.
100 Apollo Drive
Chelmsford, Massachusetts 01824
(800) 244-2947
www.axis.com

Industrial Video & Control Co.
300 Pleasant St.
Watertown, Massachusetts 02472
(617) 926-7802
www.ivcco.com

Pelco
3500 Pelco Way
Clovis, California 93612
(800) 289-9100
www.pelco.com

Q-Star Technology
9960 Canoga Avenue, Suite D4
Chatsworth, California 91311
(866) 201-4197
www.qstartech.com

Water Monitoring Products

Biological Sensors for Toxicity

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect toxicity.

APPLICATION

Current uses are primarily for wastewater discharge permit compliance or monitoring water samples. Can also monitor for toxicity in other water assets (finished drinking water distribution systems, influent wastewater, raw water, process streams).

LOCATION USED

Potential for use at critical points in water distribution systems (for example, at potentially vulnerable points downstream of distribution pump stations) to detect contamination added to water after treatment. Portable sensors can be used to monitor grab samples at critical areas of a system; off-line systems are used to test samples in the laboratory. It may be difficult to effectively monitor large systems because of their diffuse nature.

DESCRIPTION

Toxicity tests measure water toxicity by monitoring adverse biological effects on test organisms. Toxicity tests have traditionally been used to monitor wastewater effluent streams for National Pollutant Discharge Elimination System(NPDES) permit compliance or to test water samples for toxicity. However, this technology can also be used to monitor drinking water distribution systems or other water/wastewater streams for toxicity. Currently, several types of bio-sensors and toxicity tests are being adapted for use in the water/wastewater security field. The keys to using bio-monitoring or bio-sensors for drinking water or other water/wastewater asset security are rapid response and the ability to use the monitor at critical locations in the system, such as in water distribution systems downstream of pump stations, or prior to the biological process in a wastewater treatment plant. While there are several different organisms that can be used to monitor for toxicity (including bacteria, invertebrates, and fish), bacteria-based bio-sensors are ideal for use as early warning screening tools for drinking water security because bacteria usually respond to toxics in a matter of minutes. In contrast to methods using bacteria, toxicity screening methods that use higher-level organisms such as fish may take several days to produce a measurable result. Bacteria-based bio-sensors have recently been incorporated into portable instruments, making rapid response and field-testing practical. These portable meters detect decreases in biological activity (e.g. decreases in bacterial luminescence), which are highly correlated with increased levels of toxicity.

At the present time, few utilities are using biologically-based toxicity monitors to monitor water/wastewater assets for toxicity, and very few products are now commercially available. Several new approaches to the rapid monitoring of microorganisms for security purposes (e.g. microbial source tracking) have been identified. However, most of these methods are still in the research and development phase.

ATTRIBUTES AND FEATURES

In general, the commercial application of biological toxicity monitoring is quite new. Many biological toxicity monitoring systems have been developed for site-specific applications, and there is little opportunity to compare commercially available products. Therefore, it is difficult to directly define sensitivities and detection limits of biological toxicity meters at the current time. However, sensitivities of some products may be compared relative to each other. For example, temperature control is important in increasing the accuracy of the toxicity measurement, and systems that have temperature **Table** controls are considered to be more accurate in measuring and reproducing results than those without temperature controls.

Biological toxicity monitors provide a kind of relative, nonspecific indication of water quality rather than precise, reportable measurements of specific parameters. The non-specificity is partly by design, because some biological toxicity monitors are typically used to provide a first-order screening test. Broad sensitivity to a wide range of contaminants is considered strength of a good bio-monitor.

Table 1: Comparison of Biological Toxicity Monitoring Systems

Product Sensitivity	Detection Limit	Reliability/ Ruggedness	Response Time	Ease of Installation/ Use
— Portable System —				
DeltaTox Analyzer (SDI (formerly AZUR))	Accurate (use of a luminescent bacteria, Vibrio fischeri)	Medium	15 minutes	Easy to install and use
— Laboratory-Based System —				
Microtox Toxicity Model 500 Analyzer (SDI)	Highly accurate (use of a luminescent bacteria, Vibrio fischeri)	Medium	15 minutes	Easy to install and use

COST

The Microtox toxicity analyzer costs approximately $18,000, while the AZUR DeltaTox analyzer costs approximately $5,900. The difference between these two products is that the portable DeltaTox analyzer does not have temperature controls.

Capital costs for traditional laboratory-based bio-monitoring systems vary widely because of the unique setup for each type of system. Most laboratory-based systems include designated space and equipment (for example, fish tanks or bowls for invertebrate tests) to set up and run the tests. This space may require specialized features (for example, climate control) depending on the types of toxicity tests to be run. Periodic costs include the purchase/use of test organisms for each toxicity test, as well as costs to set up and maintain each test. These facilities may also require regular inspection and cleaning. Some toxicity tests require expensive laboratory equipment.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Strategic Diagnostics Inc. (SDI) / AZUR Environmental
111 Pencader Drive
Newark, Delaware 19702
(800) 544-8881

Chemical Sensor - Arsenic Measurement System

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor arsenic in water samples.

APPLICATION

Primarily water distribution systems and finished drinking water.

LOCATION USED

Portable arsenic detection systems are designed to be used in the field, and can be used to quickly evaluate samples taken at critical areas of system.

DESCRIPTION

Arsenic is an inorganic toxin that occurs naturally in soils. It can enter water supplies from many sources, including: erosion of natural deposits; runoff from orchards; runoff from glass and electronics production wastes; or leaching from products treated with arsenic, such as wood. Synthetic organic arsenic is also used in fertilizer.

Arsenic toxicity is primarily associated with inorganic arsenic. Arsenic ingestion has been linked to cancerous health effects, including cancer of the bladder, lungs, skin, kidney, nasal passages, liver, and prostate. Arsenic ingestion has also been linked to noncancerous cardiovascular, pulmonary, immunological, and neurological, endocrine problems. According to EPA's Safe Drinking Water Act (SDWA) Arsenic Rule, inorganic arsenic can exert toxic effects after acute (short-term) or chronic (long-term) exposure. Toxicological data for acute exposure, which is typically given as a LD50 value (the dose that would be lethal to 50 percent of the test subjects in a given test), suggests that the LD50 of arsenic ranges from 1- 4 milligrams arsenic per kilogram (mg/kg) of body weight. This dose would correspond to a lethal dose range of 70 to 280 mg for 50 percent of adults weighing 70 kg. At nonlethal, but high, acute doses, inorganic arsenic can cause gastroenterological effects, shock, neuritis (continuous pain) and vascular effects in humans. EPA has set a maximum contaminant level goal of 0 for arsenic in drinking water; the current enforceable maximum contaminant level (MCL) is 0.050 mg/L. As of January 23, 2006, the enforceable MCL for arsenic will be 0.010 mg/L.

The SDWA requires arsenic monitoring for public water systems. The Arsenic Rule indicates that surface water systems must collect one sample annually; groundwater systems must collect one sample in each compliance period (once every three years). Samples are collected at entry points to the distribution system, and analysis is done in the laboratory using one of several EPA-approved methods, including Inductively Coupled Plasma Mass Spectroscopy (ICP-MS, EPA 200.8) and several atomic absorption (AA) methods. However, several different technologies, including colorimetric test kits and portable chemical sensors, are currently available for monitoring inorganic arsenic concentrations in the field. These technologies can provide a quick estimate of arsenic concentrations in a water sample. Thus, these technologies may be useful for spot-checking different parts of a drinking water system (for example, reservoirs, isolated areas of distribution systems) to ensure that the water is not contaminated with arsenic.

The two primary technologies for evaluating arsenic concentrations in the field are colorimetric test kits and portable chemical sensors. These two technologies are described in further detail below:

Test Kits

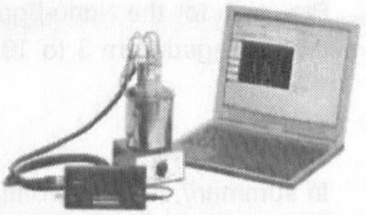
The field test kits detected by mixing the water sample with powdered reagents, which converts the arsenic to arsine gas. A colorimetric test strip is then immersed in the sample, removed, and compared to a reference table to determine the arsenic concentration in the sample. Several vendors (including Industrial Test Systems, Inc., and Peters Engineering) also offer a battery-operated tester, which measures the color change electronically and displays the results on the unit.

Arsenic Test Kit from the Hach Company

Sensors

There are two portable sensor technologies currently on the market (Monitoring Technologies International's PDV 6000 and TraceDetect's Nano-Band™ Explorer). These analyze arsenic using anodic stripping voltammetry (ASV) technology and transmit results to a laptop (not included with the sensor product) loaded with specialized software to interpret, display, and store the results. The ASV technology works through a standard oxidation/reduction (redox) chemical reaction in the test solution. First, a "reducing potential" is applied at the working electrode. When the "reducing potential" exceeds the "ionization potential" of the arsenic ion in solution, the arsenic is "reduced" and collected on the electrode. After a pre-specified time, "oxidizing potential" is applied to the working electrode. This strips off the arsenic and creates an electric current, which is measured and compared to a reference standard to determine the sample concentration. The results are then displayed on the laptop.

The Nano-Band™ Explorer uses a unique electrode configuration to increase its response time. Its electrode is composed of 100 sub-electrodes, and the increase in mass that can be transported across these multiple electrodes allows measurement of the arsenic concentration in a much shorter time relative to conventional electrode technologies (usually within a few seconds).


The Nano-Band™ Explorer

ATTRIBUTES AND FEATURES

The U.S. EPA Environmental Technology Verification (ETV) program has evaluated multiple products for measuring arsenic in water samples, including seven different test kits and two portable sensors. For each product, EPA evaluated accuracy, precision, linearity, method detection limit, matrix interference effects, inter-unit reproducibility, rate of false positives/false negatives, and other factors. In general, EPA evaluated solutions ranging from 0.001 to 0.1 mg/L arsenic. This translates to 10 percent to 1,000 percent of the new 0.010 mg/L standard for arsenic in drinking water. A summary of results of these evaluations are presented below.

For a full discussion of the tests and results, see http://www.epa.gov/etv/verifications/vcenter1-21.html.

Accuracy

Accuracy is a measure of how close a measurement is to the true value. The measured difference between sample reading and the true value is referred to as "bias." Bias is reported as a percentage of the measure value relative to the true value, and can be positive (sample reading is above the true value) or negative (sample reading is below the true value). Bias can vary in magnitude between different analytical techniques or procedures. It should also be noted that small errors can result in a large bias when the actual concentration in the sample is low. For example, an error of 1 ppb in measuring concentrations of 10 ppb arsenic vs. 100 ppb arsenic would result in a positive bias of 10 percent for the first measurement, but only 1 percent for the second measurement.

EPA found that many of the arsenic test kits could have a large bias (up to almost 10,000 percent in some cases) in measuring a known arsenic concentration. Most of the biases were positive (i.e., the results were reported as higher than the actual concentration), although at least one kit (Industrial Test Systems (ITS) Quick™ Ultra Low II) produced results that had negative biases.

Results from the portable sensors also showed biases. While the Nano-Band™ Explorer showed only high bias in the EPA trials, the PDV 6000 showed both positive and negative bias.

Precision

Precision measures the repeatability of a measurement (e.g., the bias in measuring the same sample a number of times). EPA's ETV program expresses precision as the Relative Standard Deviation (RSD) of replicate analyses.

Precision for the test kits ranged from 0 to 139 percent of the original measurement.

Precision for the Nano-Band™ Explorer ranged from 3 to 91 percent. Precision for the PDV 6000 ranged from 3 to 16 percent.

Summary

In summary, it can be difficult to generalize or draw conclusions regarding the overall accuracy and precision of arsenic test kits or portable sensors because there is a wide variation between the different products. Therefore, the use of arsenic test kits or sensors must be tempered with the knowledge of their limitations. While they do provide a quick, inexpensive method to evaluate general concentrations of arsenic in water, they may not be reliable for providing a consistent, accurate result. However, since the use of arsenic testing for security purposes should not require a highly accurate result (i.e., decisions regarding the immediate safety of water would most likely be based on much higher arsenic concentrations than those used for regulatory monitoring, and thus more accurate testing may be done to confirm exact concentrations at a later time), these kits and sensors may be useful for water security applications.

A summary of several available products, ranges, and total test times is provided in below:

Table 1 Arsenic Test Kits and Sensors

Product Range of Arsenic	Concentrations Detected (ppb)	Accuracy (ETV Tests)	Precision (ETV Tests)	Total Test Time (Min)
ITS 481300 Quick™ Ultra Low II	0.2-30	Color Chart method: Bias ranged from -87% to 45% Quick™ Arsenic Scan method: Bias ranged from -95% to 22% Compu Scan method: Bias ranged from -92% to 161%	Color Chart method: RSD ranged from 0% to 84% Quick™ Arsenic Scan method: RSD ranged from 2% to 78% Compu Scan method: RSD ranged from 6% to 139%	12
S 481297 Quick™ Low-Range	2-80	Color Chart method: Bias ranged from -81% to 579% Quick™ Arsenic Scan method: Bias ranged from -93% to 99%	Color Chart method: RSD ranged from 0% to 23% Quick™ Arsenic Scan method: RSD ranged from 0% to 42%	12
Peters Engineering AS75 Arsenic Test Kit	2.5-60 (blue filter holder) 10-100 (grey filter holder)	PeCo test method: Bias ranged from 1% to 113% AS 75 Tester method: Bias ranged from 1% to 310%	PeCo test method: RSD ranged from 0% to 41% AS 75 Tester method: RSD ranged from 10% to 89%	No Data
As-Top Water Test kit	10-300	Bias ranged from 2% to >9,900%	RSD ranged from 0% to 111%	30
Monitoring Technologies International PDV 6000	5-1000	Bias ranged from -74% to 31%	RSD ranged from 3% to 16%	Instrument calibration: 30 min. Analysis: 5 min.
raceDetect Nano-Band™ Explorer	1	Bias ranged from 1% to 499%	Bias ranged from 1% to 499%	< 1 min.

Matrix Interference Effects

Sodium chloride, iron, sulfate, and acidity can potentially interfere with arsenic measurements in water. However, in general, EPA found that the test kits and portable chemical sensors were not affected by the presence of sodium chloride, iron, sulfate, or acidity, and that measurements of arsenic were similar in samples that contained these potential interfering chemicals vs. samples that did not. EPA did find that high iron and/or hydrogen sulfide concentrations biased arsenic measurements by the PDV 6000 analyzer. Arsenic results in samples with high concentrations of iron and/or hydrogen sulfide were biased high.

COST

Costs for arsenic detection systems can vary greatly depending on the level of system sophistication. Costs for test kits depend on the number of tests in the kit, and the range of the test. For example, Industrial Test System, Inc. kits can range from $16 for a two-test kit to $250 for an ultra low-range 25-test kit. The Peters Engineering test kit capable of analyzing 100 samples is $220; refill packs for 100 additional tests can be purchased for $60. The AS 75 tester is $330.

The Nano-Band™ Explorer Portable Water Analyzer costs $8,000. This includes the battery-powered, rechargeable instrument, software, one Nano-Band™ Explorer electrode, an auxiliary electrode, a reference electrode, a cleaning and reconditioning kit for the electrode, and a temperature sensor. The PDV 6000 portable analyzer for the detection of heavy metal ions has a list price of $7,900. This price includes the analyzer unit, software, batteries, charger, and carrying case. Neither system includes a laptop computer, which is necessary to run either technology in the field.

Several arsenic test kits and sensors have been evaluated by the EPA Environmental Technology Verification program. Information on these technologies can be found at http://www.epa.gov/etv/verifications/vcenter1-21.html.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

LaMotte
802 Washington Avenue
P.O. Box 329
Chestertown, Maryland 21620
(800) 344-3100
www.lamotte.com

TraceDetect
180 North Canal Street
Seattle, Washington 98103
(206) 523-2009
www.tracedetect.com/index.htm

Monitoring Technologies International, Pty. Ltd.
10 Main Street, Osborne Park
Perth, Western Australia 6017
618-9444-3377
www.monitoring-technologies.com

Envitop, Ltd.
Riihitie 5
FIN-90240
Oulu, Finland
358-8-372 586
www.envitop.com

Industrial Test Systems, Inc.
1875 Langston Street
Rock Hill, South Carolina 29730
(800) 861-9712
www.sensafe.com

Apyron Technologies, Inc.
4030 Pleasantdale Road
Suite F
Atlanta, Georgia 30340
(770) 263-1012
www.apyron.com

Peters Engineering
Styregasse 78010 Graz
Austria
43(0)316-840792

Hach Company
PO Box 389
Loveland, Colorado 80539
800-227-4224
www.hach.com

Chemical Sensor - Chlorine Measurement System

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect chlorine levels, which can serve as indicators of potential threats.

APPLICATION

Primarily water distribution systems and finished drinking water.

LOCATION USED

Portable sensors used at critical areas of system; on-line tests/monitoring equipment for continuous monitoring.

DESCRIPTION

Residual chlorine is one of the most sensitive and useful indicator parameters in water distribution system monitoring. All water distribution systems monitor for residual chlorine concentrations as part of their Safe Drinking Water Act(SDWA) requirements, and procedures for monitoring chlorine concentrations are well established and accurate. Chlorine monitoring assures proper residual at all points in the system, helps pace re-chlorination when needed, and quickly and reliably signals any unexpected increase in disinfectant demand. Monitoring chlorine levels in the system also can serve as a "surrogate" for detecting potentially threatening contamination, because many chemical and biological contaminants are known to combine with chlorine. Therefore, a significant decline or loss of residual chlorine could be an indication of potential threats to the system.

Several key points regarding residual chlorine monitoring for security purposes are provided below:

- Chlorine residuals can be measured using continuous on-line monitors at fixed points in the system, or by taking grab samples at any point in the system and using chlorine test kits or portable sensors to determine chlorine concentrations.

- Correct placement of residual chlorine monitoring points within a system is crucial to early detection of potential threats. For example, while dead ends and low-pressure zones are common trouble spots that can show low residual chlorine concentrations, these zones are generally not of great concern for water security purposes because system hydraulics will limit the circulation of any contaminants present in these areas of the system.

- Monitoring points and monitoring procedures for SDWA compliance vs. system security purposes may be different, and utilities must determine the best use of on-line, fixed monitoring systems vs. portable sensors/test kits to balance their SDWA compliance and security needs.

It should be noted that not all potential contaminants react with chlorine. One of the key areas of concern with reliance on chlorine residual is microbial adaptation under potable water treatment conditions or within conveyance systems. Microorganisms that develop resistance to potable water disinfectants may be much more problematic as emerging waterborne pathogens than those that are not resistant to chlorine. Several of these organisms are listed in Table 1.

Table 1: Contaminants Known to be Resistant to Chlorine Disinfection

Pollutant or Chemical Agent	**Type**
Anthrax Bacteria	Bacteria
Cholera Bacteria	Bacteria
Plague (Yersinia pestis) Bacteria	Bacteria
Salmonella Bacteria	Bacteria
T-2 Mycotoxin Biotoxin	Biotoxin
Microcystins Biotoxin	Biotoxin
Ricin Biotoxin	Biotoxin
Botulinum Toxin Biotoxin	Biotoxin
Cryptosporidiosis Protozoan	Protozoan

ATTRIBUTES AND FEATURES

A variety of different portable and on-line chlorine monitors are commercially available. These range from sophisticated on-line chlorine monitoring systems to portable electrode sensors to colorimetric test kits. On-line systems can be equipped with control, signal, and alarm systems that notify the operator of low chlorine concentrations, and some may be tied into feedback loops that automatically adjust chlorine concentrations in the system. In contrast, use of portable sensors or colorimetric test kits requires technicians to take a sample and read the results. The technician then initiates required actions based on the results of the test.

Sensitivity and Detection Limit

Because residual chlorine concentrations are surrogates that can indicate potential problems in a system, gross changes in these concentrations are the best indicators of potential threats. Therefore, high-sensitivity probes are not required for security purposes. Chlorine concentrations ranging from 0.5 to 2.0 mg/L are typically required for drinking water monitoring applications, and deviations from this range should be sufficient to identify security threats. Both colorimetric and electrode technologies can detect free or total chlorine to hundredths of a milligram per liter. Linearity of response in the range of 0.5 percent with repeatability of 0.05 mg/L can be expected.

Measurement Method and Maintenance

To operate reliably, the on-line monitoring instruments require regular inspection and frequent maintenance. In many cases, consumables such as compressed gases, reagents, solutions, and calibration standards must be refreshed on a regular basis. Colorimetric monitoring generally requires periodic replenishment of consumable test strips or reagents. Electrode monitors require maintenance, which may include membrane and electrolyte replacement as the cell performance degrades. Power requirements typically are line power with signal output as either milli-volts or milli-amps.

Table 2 provides a list of portable chlorine analyzers. The sensor technology used in these commercial products is readily available for setting up online chlorine measurement in water distribution systems.

Table 2: Comparison of Chlorine Measurement Systems

Product	Sensitivity/ Detection Limit	Reliability/ Ruggedness	Response Time	Ease of Installation/ Use
— On-Line Monitoring Systems —				
CL17 On-line Chlorine Analyzer (HACH)	0.035 mg/L	High -Strong and corrosion-resistant	2.5 min/ cycle	Easy
AccuChlor2 Residual Chlorine Measurement System (HACH (formerly GLI))	0.01 mg/L	High - Amperometric technique, stable and repeatable measurements	2 min/ cycle	Intermediate
— Portable Monitoring Devices —				
Six-CENSE (DASCORE)	0.01 mg/L	High - Sits on a robust ceramic chip, designed for durability	No Data	Easy
B20 Recording Chlorine Analyzer (ATI)	0.01 mg/L	High	1 minute	Easy
VR Water Analysis System (CHEMetrics)	Better than 1%	High	4 seconds	Intermediate
— Field Test Kits —				
AquaCheck Test Strips (HACH)	Low	Low (semi-quantitative)	Very fast	Easy
Color Disc (HACH)	0.01 mg/L	Low	Fast	Easy

COST

Costs for chlorine monitoring systems can vary greatly depending on the level of system sophistication. On-line chlorine analyzers/sensors typically range from $2,700 to $3,100. Chlorine measurement systems that include automatic controls will be more expensive. Portable chlorine measurement systems typically cost around $600. However, multiple-parameter portable chlorine analyzer such as DASCORE's Six-CENSE, which is designed to measure six different parameters, costs $8,000 to $10,000 per unit. In comparison, disposable test kits for chlorine analysis costs about $115 for a pack of 250. The color disc for chlorine cost about $40 for a pack of 50.

Vendors

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Hach Company / GLI International / Hydrolab
P.O. Box 389
Loveland, Colorado 80539-0389
(800) 227-4224
www.hach.com

Analytical Technology Inc. (ATI)
6 Iron Bridge Drive
Collegeville, Pennsylvania 19426
(800) 959-0299 or (610) 917-0991
www.analyticaltechnology.com

DASCORE, Inc.
(866) 321-3804
www.dascore.com

CHEMetrics, Inc.
4295 Catlett Rd.,
Calverton, Virginia 20138
(800) 356-3072
www.chemetrics.com

Chemical Sensor for Toxicity (Adapted BOD Analyzer)

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect toxicity using biochemical oxygen demand (BOD) as a surrogate.

APPLICATION

Current uses are primarily for wastewater discharge permit compliance or monitoring water samples. Can also monitor for toxicity in other water assets (finished drinking water distribution systems, influent wastewater, raw water, process streams).

LOCATION USED

Potential for use at critical points in water distribution systems (for example, at potentially vulnerable points downstream of distribution pump stations) to detect contamination added to water after treatment. Monitor is on-line, and thus location of monitor must be permanent and secure. This also makes placement of monitor important to maximize coverage of distribution system.

DESCRIPTION

One manufacturer has adapted a BOD analyzer to measure oxygen consumption as a surrogate for general toxicity. The critical element in the analyzer is the bioreactor, which is used to continuously measure the respiration of the biomass under stable conditions. As the toxicity of the sample increases, the oxygen consumption in the sample decreases. An alarm can be programmed to sound if oxygen reaches a minimum concentration (i.e., if the sample is strongly toxic). The operator must then interpret the results into a measure of toxicity.

ATTRIBUTES AND FEATURES

At the current time, it is difficult to directly define the sensitivity and/or the detection limit of toxicity measurement devices because limited data is available regarding specific correlations of decreased oxygen consumption and increased toxicity of the sample.

A summary of several available products, their ranges, and the total test times is provided in Table 1 below:

Table 1: Attributes and Features of the adapted BOD Analyzer

Product	CSensitivity/ Detection Limit	Accuracy (ETV Tests)	Response Time	Ease of Installation/Use
ISCO / STIPTOX Adapt W Toximeter	Accurate (may need minor adaptation for general toxicity)	Successfully used in Europe since 1984	3-15 mins. (Quick response to large number of toxins)	Easy to install and use

COST

The cost of the toxicity measurement device will be similar to the costs of a real time BOD analyzer. The ISCO real-time BOD Analyzer generally ranges between $20,000 and $30,000, depending on the user's specific requirements, as well as on the inclusion of any optional features.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

ISCO, Inc.
4700 Superior St.
PO Box 82531
Lincoln, Nebraska 68504
(800) 228-4373
www.ISCO.com

Chemical Sensor - Total Organic Carbon Analyzer

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect total organic carbon concentrations.

APPLICATION

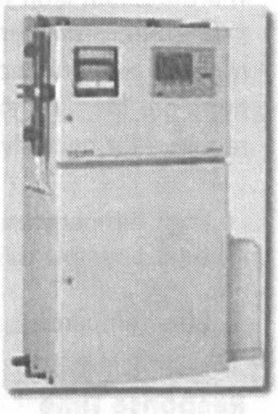
Monitor critical areas of a drinking water distribution system or wastewater influent to detect higher-than-normal total organic carbon concentrations, which can serve as indicators of potential chemical threats to human health or to wastewater treatment processes.

LOCATION USED

On-line monitoring equipment can be placed at critical areas of a drinking water distribution system or at a wastewater influent wet well to detect potential chemical threats.

DESCRIPTION

Total Organic Carbon (TOC) analysis is a well-defined and commonly used methodology that measures the carbon content of dissolved and particulate organic matter present in water. Many water utilities monitor TOC to determine raw water quality or to evaluate the effectiveness of processes designed to remove organic carbon. Some wastewater utilities also employ TOC analysis to monitor the efficiency of the treatment process. In addition to these uses for TOC monitoring, measuring changes in TOC concentrations can be an´effective "surrogate" for detecting contamination from organic compounds (e.g. petrochemicals, solvents, pesticides). Thus, while TOC analysis does not give specific information about the nature of the threat, identifying changes in TOC can be a good indicator of potential threats to a system.



Shimadzu On-Line TOC Analyzer

ATTRIBUTES AND FEATURES

TOC analysis consists of inorganic carbon removal, oxidation of the organic carbon into CO2, and quantification of the CO2. The primary differences between different on-line TOC analyzers are in the methods used for oxidation and CO2 quantification.

The oxidation step can be high or low temperature. The determination of the appropriate analytical method (and thus the appropriate analyzer) is based on the expected characteristics of the wastewater sample (TOC concentrations and the individual components making up the TOC fraction). In general, high temperature (combustion) analyzers achieve more complete oxidation of the carbon fraction than do low temperature (wet chemistry/UV) analyzers. This can be important both in distinguishing different fractions of the organics in a sample and in achieving a precise measurement of the organic content of the sample.

Three different methods are also available for detection and quantification of carbon dioxide produced in the oxidation step of a TOC analyzer. These are:

- Nondispersive infrared (NDIR) detector
- Colorimetric methods
- Aqueous conductivity methods

The most common detector that on-line TOC analyzers use for source water and drinking water analysis is the nondispersive infrared detector.

While the differences in analytical methods employed by different TOC analyzers may be important in compliance or process monitoring, high levels of precision and the ability to distinguish specific organic fractions from a sample may not be required for detection of a potential chemical threat. Instead, gross deviations from normal TOC concentrations may be the best indication of a chemical threat to the system (see below).

Sensitivity and Detection Limit

The detection limit for organic carbon depends on the measurement technique used (high or low temperature) and the type of the analyzer. Because TOC concentrations are simply surrogates that can indicate potential problems in a system, gross changes in these concentrations are the best indicators of potential threats. Therefore, high-sensitivity probes may not be required for security purposes. However, the following detection limits can be expected:

- High temperature method (between 680°C and 950°C or higher in a few special cases, best possible oxidation): = 1 mg/L carbon
- Low temperature method (below 100°C, limited oxidation potential): = 0.2 mg/L carbon

Response Time

The response time of a TOC analyzer may vary depending on the manufacturer's specifications, but it usually takes from 5 to 15 minutes to get a stable, accurate reading.

Maintenance

On-line TOC analyzers are designed to operate in remote locations without continuous surveillance by an operator. However, to operate reliably, the instruments require regular calibration, inspection, and maintenance by technically skilled personnel. Previous research recommends that, at a minimum, a weekly check should be done if the analyzer is in a remote location. Table 1 provides a list of available TOC analyzers and summarizes their important attributes.

Table 1 Comparison of Chlorine Measurement Systems

Product	Sensitivity/ Detection Limit	High	Response Time
HACH / 1950plus On-Line TOC Analyzer	0.015 mg/L for range of 0-5mg/L	High	8 min
ISCO / STIP-toc High-Temperature TOC Analyzer	2 mg/L	High	3-15 min
CO / EZ TOC Low-Temperature TOC Analyzer	21.5% for 0-75% full scale; 2.5% for 75-100% full scale	High	8 min
Shimadzu TOCN 4000	Variable. Settings from 0-5 ppm to 0-1000 PPM	High	4 min
kmar Dohrmann Phoenix 8000 UV-Persulfate TOC Analyzer	2 ppb - 1000 PPM	High	No Data
Tekmar Dohrmann Apollo 9000/9000 HS Combustion TOC Analyzer	100 ppb- 25,000 PPM	High	1-3 min

Sensors for Monitoring Chemical, Biological, and Radiological Contamination

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect chemical, biological, or radiological parameters that may represent threats to the system.

APPLICATION

Can be used to monitor finished water assets (i.e., water distribution system) to detect potential threats to downstream users introduced to the system after treatment. Can also be use to monitor water or wastewater influent to detect potential for upset of treatment processes or for potential pass-through of harmful contaminants.

LOCATION USED

Downstream of potential access to the water distribution system (i.e., downstream of pumping stations). Also, raw water assets (reservoirs, etc.), influent wet wells (wastewater treatment plants) or wastewater treatment plant effluent. Monitoring can be at fixed or random locations depending on the perceived threat..

DESCRIPTION

Water quality monitoring sensor equipment may be used to monitor key elements of water or wastewater treatment processes (such as influent water quality, treatment processes, or effluent water quality) to identify anomalies that may indicate threats to the system. Some sensors, such as sensors for biological organisms or radiological contaminants, measure potential contamination directly, while others, particularly some chemical monitoring systems, measure "surrogate" parameters that may indicate problems in the system but do not identify sources of contamination directly. In addition, sensors can provide more accurate control of critical components in water and wastewater systems and may provide a means of early warning so that the potential effects of certain types of attacks can be mitigated. One advantage of using chemical and biological sensors to monitor for potential threats to water and wastewater systems is that many utilities already employ sensors to monitor potable water (raw or finished) or influent/effluent for Safe Drinking Water Act (SDWA) or Clean Water Act (CWA) water quality compliance or process control.

Chemical sensors that can be used to identify potential threats to water and wastewater systems include inorganic monitors (e.g. chlorine analyzer), organic monitors (e.g. total organic carbon analyzer) and toxicity meters. Radiological meters can be used to measure concentrations of several different radioactive species. Monitors that use biological species can be used as sentinels for the presence of contaminants of concern, such as toxics. At the present time, biological monitors are not in widespread use and very few bio-monitors are used by drinking water utilities in the U.S.

Continuous Online Monitoring vs. Grab Sample Analysis

Monitoring can be conducted using either portable or fixed-location sensors. Fixed-location sensors are usually used as part of a continuous, on-line monitoring system. Continuous monitoring has the advantage of enabling immediate notification when there is an upset. However, the sampling points are fixed and only certain points in the system can be monitored. In addition, the number of monitoring locations needed to capture the physical, chemical, and biological complexity of a system can be prohibitive. The use of portable sensors can overcome this problem of monitoring many points in the system. Portable sensors can be used to analyze grab samples at any point in the system, but have the disadvantage that they provide measurements only at one point in time.

Sensor Technology in Water vs. Wastewater Applications

Because of the direct threats to drinking water systems, the chemical, biological, and radiological sensors described in the subsequent Product Guides have primarily been used for source water and water distribution applications. However, the same technology can also be used in wastewater security, primarily for detecting disruptions in the treatment process. This guide on chemical and biological sensors covers the following individual products:

Chemical Sensor - Arsenic Measurement System

Chemical Sensor - Chlorine Measurement System

Chemical Sensor - Total Organic Carbon Analyzer

Radiation Detection Equipment

Radiation Detection Equipment for Monitoring Personnel and Packages

Radiation Detection Equipment for Monitoring Water Assets

Toxicity Monitoring/Toxicity Meters

Chemical Sensor for Toxicity (Adapted BOD Analyzer)

Biological Sensors for Toxicity

Toxicity Monitoring/Toxicity Meters

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect toxicity.

APPLICATION

Designed to detect chemical/biological threats to water assets. Current uses are primarily for wastewater effluent. Can also monitor for toxicity in other water assets (finished drinking water, influent wastewater, raw water, process streams).

LOCATION USED

Portable sensors used at critical areas of system; off-line tests/monitoring conducted in laboratory

OVERVIEW

Toxicity measurement devices measure general toxicity to biological organisms, and detection of toxicity in any water/wastewater asset can indicate a potential threat, either to the treatment process (in the case of influent toxicity), to human health (in the case of finished drinking water toxicity) or to the environment (in the case of effluent toxicity). Currently, whole effluent toxicity tests (WET tests), in which effluent samples are tested against test organisms, are required of many National Pollutant Discharge Elimination System (NPDES) discharge permits. The WET tests are used as a complement to the effluent limits on physical and chemical parameters to assess the overall effects of the discharge on living organisms or aquatic biota. Toxicity tests may also be used to monitor wastewater influent streams for potential hazardous contamination, such as organic heavy metals (arsenic, mercury, lead, chromium and copper) that might upset the treatment process.

- Meters measuring direct biological activity (e.g. luminescent bacteria) and correlating decreases in this direct biological activity with increased toxicity; and

- Meters measuring oxygen consumption and correlating decreases in oxygen consumption with increased toxicity.

● DETECT
○ DELAY
○ RESPOND

Radiation Detection Equipment

OBJECTIVE

Detect radioactive contamination.

APPLICATION

Some types of radiation monitoring equipment can be used to monitor for radioactive contamination of water assets (e.g., finished water, etc.). Other types of equipment can be used to monitor personnel or packages for radioactive contamination.

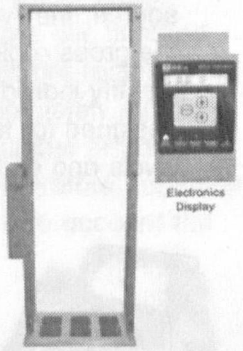
LOCATION USED

On-line equipment to monitor water assets would be located at critical points in the system; portable equipment would be used in specific locations as necessary. Equipment used to monitor personnel or packages for radioactive contamination would be located at building entrances or screening areas.

DESCRIPTION

Radioactive substances (radionuclides) are known health hazards that emit energetic waves and/or particles that can cause both carcinogenic and non-carcinogenic health effects. Radionuclides pose unique threats to source water supplies and water treatment, storage, or distribution systems because radiation emitted from radionuclides in water systems can affect individuals through several pathways - by direct contact with, ingestion or inhalation of, or external exposure to, the contaminated water. While radiation can occur naturally in some cases due to the decay of some minerals, intentional and non-intentional releases of man-made radionuclides into water systems is also a realistic threat.

Threats to water and wastewater facilities from radioactive contamination could involve two major scenarios. First, the facility or its assets could be contaminated, preventing workers from accessing and operating the facility/assets. Second, at drinking water facilities, the water supply could be contaminated, and tainted water could be distributed to users downstream. These two scenarios require different threat reduction strategies. The first scenario requires that facilities monitor for radioactive substances being brought on-site; the second requires that water assets be monitored for radioactive contamination. While the effects of radioactive contamination are basically the same under both threat types, each of these threats requires different types of radiation monitoring and different types of equipment. This document provides a general discussion of radiation and radiation monitoring. Specific information on radiation monitoring equipment designed for these two different threat scenarios is provided in the two documents below:



Ludlum Measurements, Inc.
Portable Scintillation Portal

- Radiation Detection Equipment for Monitoring Personnel and Packages
- Radiation Detection Equipment for Monitoring Water Assets

Radioactivity and Radiation Measurements

The most common types of radiation are alpha, beta and gamma radiation.

Alpha emitters emit heavy, positively-charged alpha particles. Many alpha emitters are naturally occurring, but some are man-made. Examples include plutonium, radon, radium, uranium, and thorium. Alpha radiation is short range (i.e., it can only travel a few centimeters from the source through air) and it cannot penetrate human skin. Alpha emitters can be a serious health hazard if they are ingested, such as if they are consumed from radiation-contaminated water.

Beta emitters emit lightweight, negatively-charged particles (electrons). Beta emitters are primarily man-made and include strontium-90, carbon-14, tritium (H-3), and sulfur-35. Beta radiation has a medium range (i.e., it can travel several feet from its source through air) and it has moderate capabilities to penetrate through objects.

Gamma emitters emit very long range electromagnetic radiation, and can be both man-made and naturally-occurring. Examples of man-made gamma emitters generated by the nuclear industry include iodine-131, cesium-137, and cobalt-60. Gamma radiation is highly penetrating, and it can travel through many types of objects, including human skin and clothing. It is effectively shielded or absorbed by materials such as concrete, steel, or lead.

Radiation Monitoring and Radiation Monitoring Equipment

Different types of radiation monitoring instruments have been designed for different purposes. In general, this equipment is designed to measure either:

- The total amount of radiation emitted from a source (the "gross" radiation); or
- The specific type and energy level of radiation emitted from a source.

For example, if a utility wished to determine whether there was elevated radiation from some source, they would most likely use some type of "screening"-type equipment to measure the gross radiation from the source. If a high level of radiation was detected, the utility may identify individual species of radionuclides and their energy levels using equipment specifically designed for this purpose. This would allow the calculation of radiation doses and exposure levels and an evaluation of the potential health effects of the radiation exposure.

Ludlum Measurements, Inc.
Geiger Mueller Meter

While the goals of the radiation monitoring influence the type of analysis to be done, other factors also affect the specific type of equipment to be used to conduct the monitoring. Different types of radiation have unique properties (i.e., particle vs. wave radiation, ability of different types of radiation to penetrate different materials, distance that different forms of radiation travel from their source, interaction of radiation with matter, and the unique energy signatures of different types of radiation), and therefore radiation detection instrumentation is somewhat specific to the radiation to be detected. For example, survey meters such as Geiger-Mueller (GM) counters allow the rapid evaluation of different types of radiation from solid surfaces. Therefore, these GM meters are appropriate for evaluation of radioactive spills. However, due to the fact that water is not a smooth surface, and because alpha and beta emissions are relatively short range and can be attenuated within the water, these types of instruments are not suitable for measuring alpha or beta radiation in water samples. A more appropriate method for measuring alpha and beta radiation in water is in a laboratory setting with a liquid scintillation counter. While field measurements of gamma radiation in water may be easier to accomplish than field measurements of alpha or beta radiation in water, they still may not be highly accurate. For example, gamma emissions may be attenuated by the sample container and/or the water itself, reducing the efficiency of the detection device.

With all of these factors affecting the appropriate choice of radiation monitoring equipment, choosing the appropriate instrument to achieve an individual's monitoring goals can be a daunting task. Therefore, it may be appropriate to consult an expert in radiation monitoring to ensure that the goals of any radiation monitoring program are met (i.e., to ensure that the appropriate type of radiation is measured and that the appropriate type of instrumentation is used).

Radiation Monitoring - Evaluating Overall Radioactivity

As discussed above, different equipment has been developed to evaluate gross radiation vs. specific radionuclides. For security monitoring purposes, it may be most appropriate to initially evaluate the overall radiation from a source, whether it be a package coming into the plant or a water sample from a drinking water reservoir. Should elevated levels of radiation be detected, additional measurements can be made to identify the specific radionuclides present. Therefore, this document will focus on detection devices that are used to perform screening-type measurements for gross levels of radiation.

Radiation Measurements

Radioactivity is expressed in the number of disintegrations per unit time. For example, 1 becquerel (Bq) is 1 disintegration per second, and 1 curie (Ci) is 3.7 x 1010 disintegrations per second. However, due to various physical and statistical factors related to detection efficiency, determining the actual number of disintegrations per unit time is almost impossible. For example, measuring the actual radiation from a source would require one hundred percent efficiency in measuring all alpha, beta, and gamma emissions, which are radiating in every direction from the source. This would require a detector that would completely surround the sample and could capture a large range of energies from an unlimited number of sample shapes and physical properties within a defined distance from the sample. Therefore, radiation emissions are typically measured as counts per minute (cpm), which takes into account the detection efficiency of the instrument.

Operational Parameters

As discussed above, the most important factor in purchasing any radiation monitoring equipment is ensuring that the equipment is appropriate for the type of survey being conducted. There are many different detection methods available for different types of radiation, and thus individual users must determine the appropriate equipment for their needs. Other factors in choosing the appropriate equipment are the local conditions at the site (i.e., temperature, humidity), and the specific properties of the radionuclides at the site.

Department of Energy (DOE)/Department of Justice (DOJ) Equipment Program

The U.S. DOE is working with the U.S. DOJ to make older-generation equipment available to emergency preparedness organizations in major U.S. cities. Types of radiological instrumentation redeployed through this program include portable instrument probes (e.g., GM counters *and alpha and gamma scintillators) and self-reading pocket dosimeters (dosimeters are used* to track an individual's exposure levels, and they are not discussed in this document). Starting in April 2003, DOE formally transferred excess radiological detection instrumentation to cities across the country through the Homeland Defense Equipment Reuse (HDER) Program.

Radiation Detection Equipment for Monitoring Personnel and Packages

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor facility entrances to detect radioactive substances.

APPLICATION

Radiation detection equipment can be implemented at entrances to buildings and facilities to detect radioactive substances that are being brought into the facility

LOCATION USED

Equipment to monitor personnel for radioactive substances would be located at entrance points to the facility, or at entrance points to sensitive locations within the facility.

DESCRIPTION

One of the major potential threats facing water and wastewater facilities is contamination by radioactive substances. Radioactive substances brought on-site at a facility could be used to contaminate the facility, thereby preventing workers from safely entering the facility to perform necessary water treatment tasks. In addition, radioactive substances brought on-site at a water treatment plant could be discharged into the water source or the distribution system, contaminating the downstream water supply. Therefore, detection of radioactive substances being brought on-site can be an important security enhancement.

The basic principles of radiation and radiation detection are described in the Radiation Detection Equipment Product Guide. As described in that document, different radionuclides have unique properties, and different equipment is required to detect different types of radiation. However, as is also discussed in that document, it is impractical and potentially unnecessary to monitor for specific radionuclides being brought on-site Instead, for security purposes, it may be more useful to monitor for gross radiation as an indicator of unsafe substances. An expanded discussion of the pluses and minuses of monitoring for gross radiation vs. specific radionuclides can be found in the document cited above.

In order to protect against these radioactive materials being brought on-site, a facility may set up monitoring sites outfitted with radiation detection instrumentation at entrances to the facility. Depending on the specific types of equipment chosen, this equipment would detect radiation emitted from people, packages, or other objects being brought through an entrance. Specific discussions regarding the differences in implementation/detection and effectiveness of the different types of monitoring equipment are provided under the Attributes and Features section below.

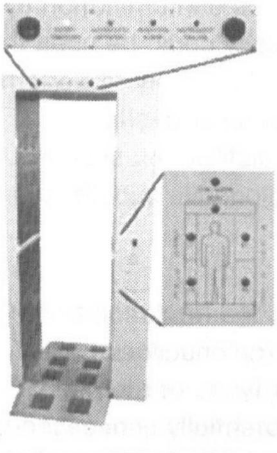
ATTRIBUTES AND FEATURES

One of the primary differences between the different types of detection equipment is the means by which the equipment reads the radiation. Radiation may either be detected by direct measurement or through sampling.

Direct radiation measurement involves measuring radiation through an external probe on the detection instrumentation. Some direct measurement equipment detects radiation emitted into the air around the monitored object. Because this equipment detects radiation in the air, it does not require that the monitoring equipment make physical contact with the monitored object. Direct means for detecting radiation include using a walk-through portal-type monitor that would detect elevated radiation levels on a person or in a package, or by using a hand-held detector, which would be moved or swept over individual objects to locate a radioactive source.

As described above, some types of radiation, such as alpha or low energy beta radiation, have a short range and are easily shielded by various materials. These types of radiation cannot be measured through direct measurement. Instead, they must be measured through sampling. Sampling involves wiping the surface to be tested with a special filter cloth, and then reading the cloth in a special counter. For example, specialized smear counters measure alpha and low energy beta radiation.

Examples of both direct measurement and sampling equipment are described in more detail below.



Ludlum M-53 Portal Monitor

Portal Monitors

Portal monitors can be used at facility entrances, or at entrances to locations within facilities that require extra security (for example, pump houses, etc.). Portal monitors are designed to monitor for gamma radiation only or for high-energy beta and gamma radiation. Because of their limited range in air and other materials, low-energy beta and alpha radiation are typically not detected by these monitors.

Portal monitors may be stationary or portable. Stationary portal monitors (See Figure) are heavy and more expensive than are portable portal monitors, but their increased shielding relative to portable portals lowers the amount of background radiation detected by the portal, and therefore increases the instrument's sensitivity. Portable portal monitors are generally less expensive than the stationary models, which allows for greater flexibility in their use, but they are less sensitive than stationary models.

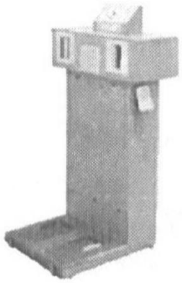
Hand-Held Instruments

Ludlum Handheld M-44-9 Pancake GM Detector

An additional option for scanning personnel or packages entering a facility is to monitor them using hand-held monitors. For example, survey instruments such as a Geiger-Mueller (GM) detector (See Figure) can be used to frisk personnel or equipment entering a facility for alpha, beta, and/or gamma radiation. GM detectors and meters and similar survey instruments are manufactured by several companies, are generally easy to use, and are relativity inexpensive. Using this type of smaller, hand-held equipment may allow for more flexibility in frisking personnel coming through an entrance and in pinpointing the location of a radioactive source than does a portal monitor. However, the smaller probe size of a handheld monitor vs. a portal would also result in an increased monitoring time.

Hand and Shoe Monitors

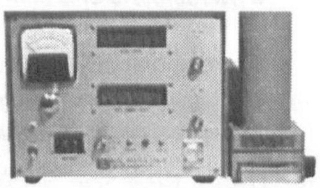
Specially designed hand and shoe monitors are available to detect alpha, beta, and/or gamma radiation on a person's hands or feet. To use this equipment, personnel to be scanned are required to stand on a platform and simultaneously place their hands in another part of the detector. While this type of detector may give highly accurate readings, it can also be time-consuming to screen all personnel coming into a facility. The adjacent figure shows a typical hand/foot monitor.



Ludlum M-49-12-1 Hand and Shoe Monitor

Smear Counters

As described in the Radiation Detection Equipment Product Guide, alpha and low energy beta radiation does not travel very far in air, and can be shielded or blocked by many types of materials. Therefore, equipment that is more sensitive to alpha and low energy beta radiation, such as a smear counter (See Figure), may be required to detect these types of radiation. Smear counters require that a sample (or a "smear") be taken from the object or person being monitored. The smear sample is taken by wiping a small cloth filter over a certain area on a surface. The smear filter is then placed in a specially designed smear sample counter, and is read over a specific period of time (typically 1-30 minutes, depending on the required sensitivity). Alpha/beta smear sample counters are typically portable, so the analysis does not necessarily need to take place at the location where the sample was taken



Ludlum M-2929 Alpha/Beta Scaler

Appropriate devices for detecting various types of radiation is summarized in Table 1 below.

Table 1: Instruments for Measuring Different Types of Radiation at Facility Entrances

Instrument	Cost
GM Probe and Meter (alpha, beta, and gamma radiation)	$500 - $700
Portal Monitor (beta and gamma radiation)	$9,000 - $25,000
Hand/Shoe Monitor (alpha and beta radiation)	$9,000 - $25,000
Smear Counter (alpha and beta radiation)	$800 - $5,000
Smear Filters (box of 250)	$25 - $50

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Technical Associates
7051 Eton Avenue
Canoga Park, California 91303
(818) 883-7043
www.tech-associates.com

LAURUS Systems, Inc
8779 Autumn Hill Drive
Ellicott City, Maryland 21043
(410) 465-5558
www.laurussystems.com

Environmental Restoration Group, Inc.
8809 Washington St. NE - Suite 150
Albuquerque, New Mexico 87113
(505) 298-4224
www.ergoffice.com

Canberra, Inc.
Radiation Monitoring Systems
800 Research Parkway
Meriden, Connecticut 06450
(423) 282-4621
www.canberra.com/homeland.htm

Saint-Gobain Crystals & Detectors
1655 Townhurst Drive
Houston, Texas 77043
(281) 355-1033
www.detectors.saint-gobain.com

Ludlum Measurements, Inc.
P.O. Box 810
501 Oak Street
Sweetwater, Texas 79556
(800) 622-0828
www.ludlums.com

Radiation Detection Equipment for Monitoring Water Assets

● DETECT
○ DELAY
○ RESPOND

OBJECTIVE

Monitor water samples to detect radioactive contamination.

APPLICATION

Primarily finished water assets. Can also monitor for contamination of other water assets (influent/effluent wastewater, raw water, process streams).

LOCATION USED

On-line equipment to monitor water assets would be located at critical points in the system; portable equipment would be used in specific locations as necessary.

DESCRIPTION

Most water systems are required to monitor for radioactivity and certain radionuclides, and to meet Maximum Contaminant Levels (MCLs) for these contaminants, to comply with the Safe Drinking Water Act (SDWA). Currently, EPA requires drinking water to meet MCLs for beta/photon emitters (includes gamma radiation), alpha particles, combined radium 226/228, and uranium. However, this monitoring is required only at entry points into the system. In addition, after the initial sampling requirements, only one sample is required every 3 to 9 years, depending on the contaminant type and the initial concentrations.

While this is adequate to monitor for long-term protection from overall radioactivity and specific radionuclides in drinking water, it may not be adequate to identify short-term spikes in radioactivity, such as from spills, accidents, or intentional releases. In addition, compliance with the SDWA requires analyzing water samples in a laboratory, which results in a delay in receiving results. In contrast, security monitoring is more effective when results can be obtained quickly in the field. In addition, monitoring for security purposes does not necessarily require that the specific radionuclides causing the contamination be identified. Thus, for security purposes, it may be more appropriate to monitor for non radionuclide-specific radiation using either portable field meters, which can be used as necessary to evaluate grab samples, or online systems, which can provide continuous monitoring of a system. This document will focus on field meters and on-line systems that can be used in the field to provide quick, nonspecific measurements of radiation.

Radiation Detection Equipment

Ideally, measuring radioactivity in water assets in the field would involve minimal sampling and sample preparation. However, the physical properties of specific types of radiation combined with the physical properties of water make evaluating radioactivity in water assets in the field somewhat difficult. For example, alpha particles can only travel short distances and they cannot penetrate through most physical objects. Therefore, instruments designed to evaluate alpha emissions must be specially designed to capture emissions at a short distance from the

Gamma radiation does not have the same types of physical properties, and thus it can be measured using different detectors.

Measuring different types of radiation is further complicated by the relationship between the radiation's intrinsic properties and the medium in which the radiation is being measured. For example, gas-flow proportional counters are typically used to evaluate gross alpha and beta radiation from smooth, solid surfaces, but due to the fact that water is not a smooth surface, and because alpha and beta emissions are relatively short range and can be attenuated within the water, these types of counters are not appropriate for measuring alpha and beta activity in water. An appropriate method for measuring alpha and beta radiation in water is by using a liquid scintillation counter. However, this requires mixing an aliquot of water with a liquid scintillation "cocktail." The liquid scintillation counter is a large, sensitive piece of equipment, so it is not appropriate for field use. Therefore, measurements for alpha and beta radiation from water assets are not typically made in the field.

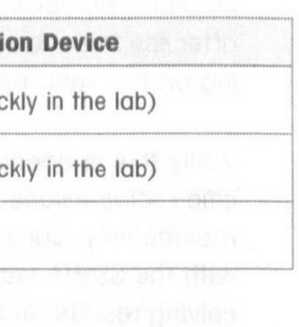
Unlike the problems associated with measuring alpha and beta activity in water in the field, the properties of gamma radiation allow it to be measured relatively well in water samples in the field. The standard instrumentation used to measure gamma radiation from water samples in the field is a sodium iodide (NaI) scintillator. This information is summarized in Table 1 below.

Table 1: Instruments for Measuring Different Types of Radiation in Water Assets in the Field

Raditation Type	Appropriate Field Detection Device
Alpha	N/A (liquid scintillation may be done quickly in the lab)
Beta	N/A (liquid scintillation may be done quickly in the lab)
Gamma	Sodium iodide scintillation survey meter

Although the devices outlined above are the most commonly used for evaluating total alpha, beta, and gamma radiation, other methods and other devices can be used. In addition, local conditions (i.e., temperature, humidity) or the properties of the specific radionuclides emitting the radiation may make other types of devices or other methods more optimal to achieve the goals of the survey than the devices noted above. Therefore, experts or individual vendors should be consulted to determine the appropriate measurement device for any specific application.

Continuous Online Monitoring vs. Grab Sample Analysis


Technical Associates MEDA-5T

The section above described the different detection methods and equipment available to monitor radiation. An additional factor to consider when developing a program to monitor for radioactive contamination in water assets is whether to take regular grab samples or sample continuously. For example, portable sensors can be used to analyze grab samples at any point in the system, but have the disadvantage that they provide measurements only at one point in time. On the other hand, fixed-location sensors are usually used as part of a continuous, on-line monitoring system. These systems continuously monitor a water asset, and could be outfitted with some type of alarm system that would alert operators if radiation increased above a certain threshold. However, the sampling points are fixed and only certain points in the system can be monitored. In addition, the number of monitoring locations needed to capture the physical and radioactive complexity of a system can be prohibitive.

On-line instruments for monitoring alpha, beta, and gamma radiation in water assets have been developed, although there are a limited number of these currently available. Technical Associates offers the SSS-33-5FT, which is a continuous flow-through scintillation detection system for alpha, beta, and gamma radiation; and the MEDA-5T, which is designed for continuous gamma radiation monitoring. Both are outfitted with alarms that will be triggered if the radiation exceeds a certain threshold. Canberra has developed several on-line radiation monitoring systems, including the OLM-100 On-Line Liquid Monitoring System, which is an on-line monitor attached to a pipe that is designed to continuously measure the quantity of radioactive gamma isotopes in the liquid stream; and the ILM-100, which is a similar system that is installed within the pipe system. Canberra's 4Pi series offers on-line gamma or beta and gamma analysis using a specialized 3- or 4-Pi geometry monitor to enhance the effectiveness of the evaluation, while the LEMS-600 series offers continuous off-line evaluation of beta and gamma radiation. In addition, the Department of Energy (DOE) has tested a prototype on-line real-time alpha radiation detection instrument. Development of this technology was moved to the Los Alamos National Laboratory in 2001. Other applications of small-scale flow-through scintillation technology are being developed for field measurements of alpha, beta, and gamma radiation. In most cases, utilities interested in on-line monitors for radionuclides/radioactivity will need to work with a manufacturer to configure a custom monitor adapted from monitors intended for small-scale applications.

Because of the limited number and high costs of on-line analyzers, they may be of limited use for most facilities. Therefore, the regular analysis of grab samples for alpha, beta, and gamma activity may be more appropriate for many facilities.

ATTRIBUTES AND FACILITIES

In addition to choosing the most appropriate type of equipment for the evaluation to be performed, there are other important factors in choosing the specific type of detector. Among these other important features of individual radiation detectors are their specificity and their sensitivity. These attributes are discussed in more detail below.

Specificity

Specificity is the ability of an instrument to quantify or evaluate the specific type of radiation or radionuclide for which it is designed without interference from other radiation or radionuclides. Such interference could lead to false conclusions about the nature and extent of potential radioactive contamination.

A general discussion of the sensitivities of the instruments summarized in Table 1 above is provided in Table 2 below. This information is summarized from the MARSSIM.

Table 2: Summary of Specificity of Survey Equipment

Scanning Device	Evaluation of Specificity
Liquid scintillation counter (alpha, beta radiation)	This method is extremely flexible and accurate when used with proper calibration and compensation for quenching effects (compensating for the fact that the full energy pulse may not reach the photo-multiplier detector). Quantitative determination of complex multi-energy beta spectra is possible because energy spectra are 10 to 100 times broader than gamma spectra.
Sodium iodide scintillation survey meter (gamma radiation)	Some meters have the ability to analyze at selected ranges of gamma energies, which can allow for the preliminary identification of specific isotopes

Sensitivity

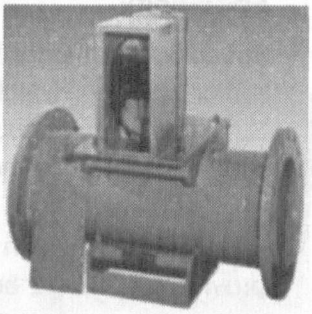
The Multi-Agency Radiation Survey and Site Investigation Manual (MARSSIM, EPA 402-R-97-016, August, 2000), which was developed as a multi-agency document by the Environmental Protection Agency (EPA), the DOE, the Department of Defense, and the Nuclear Regulatory Commission, defines the detection sensitivity of a given radiation measurement system as the radiation level or quantity of radioactive material that can be measured or detected with some estimated level of confidence. MARSSIM continues on to note that an instrument's sensitivity is a factor of both the instrumentation and the technique or procedure being used to measure the radiation. As described above, different types of radiation detection devices are designed for different purposes, and thus their sensitivities and detection limits will be very different and will reflect the purposes for which they were designed. However, a general discussion of the sensitivities of the instruments summarized in Table 1 above is provided in Table 3 below. This information is summarized from MARSSIM.

Table 3: Summary of Sensitivity of Survey Equipment

Scanning Device	Evaluation of Specificity
Liquid scintillation counter (alpha, beta radiation)	Ideal for moderate to high energy beta emitters, as well as alpha emitters, because pulse shape discrimination allows different radiation types to be distinguished easily.
Sodium iodide scintillation survey meter (gamma radiation)	Minimum sensitivity is 200-1,000 cpm, lower in digital integrate mode.

On-line Systems

The sensitivity/detection limit of Canberra's OLM-100 On-line Liquid Monitoring System (which detects gamma radiation) depends on a preset Lower Limit of Detection (LLD) and normal background.



Canberra, Inc. OLM-100 System, Clamp-On Configuration

Installation and Maintenance

While certain radiation detectors are "maintenance free" in design, specialized expertise is usually needed for installation, setup, and routine calibration of radiation monitoring equipment, whether it is field survey detectors or on-line monitoring equipment.

COST

TMARSSIM also provides rough equipment costs for radiation detection equipment summarized in Tables 1-3.

Table 4: Summary of Instrumentation Costs

Instrument	Cost
Liquid scintillation counter (alpha, beta radiation)	$20,000-$70,000
Sodium iodide scintillation survey meter (gamma radiation)	$2,000

Depending on the size of pipe for a specific application, the price of Canberra's ILM and OLM-100 On-line Liquid Monitoring Systems range from $35,000 to $75,000, with the OLM system in the lower part of the range because it can be clamped onto an existing pipe, and the ILM system closer to the higher end of the range because it must be fitted into the pipe. A major factor in determining the cost is the pipe size. The larger the pipe size, the higher the cost because of the added expense of ensuring that the detector is properly fitted into the pipe. However, the manufacturer notes that both systems can be fitted into inch to 16 inch pipes. Canberra's 4Pi series ranges from $60,000-$130,000, while the LEMS system is in the $100,000-$150,000 range. Technical Associate's MEDA-5T for continuous gamma radiation monitoring costs approximately $20,000, while the SSS-33-5FT continuous flow-through scintillation detection system for alpha, beta, and gamma radiation costs approximately $58,000.

VENDORS

Disclaimer: The information provided in this guide does not constitute an endorsement by the Environmental Protection Agency of any non-Federal entity, its products or its services. In addition, EPA does not endorse the vendors and products listed on this site. EPA is publishing lists of vendors on this site in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of the different types of security equipment. The Agency has selected the listed vendors on that basis. The list of vendors is not a complete list, and EPA does not endorse the products or services of these vendors.

Technical Associates
7051 Eton Avenue
Canoga Park, California 91303
(818) 883-7043
www.tech-associates.com

Canberra, Inc.
Radiation Monitoring Systems
800 Research Parkway
Meriden, Connecticut 06450
(423) 282-4621
www.canberra.com/homeland.htm

Mineralab, Inc.
2860 W. Live Oak Drive
Prescott, Arizona 86305
(800) 818-3811
www.geigercounters.com

Ludlum Measurements, Inc.
P.O. Box 810
501 Oak Street
Sweetwater, Texas 79556
(800) 622-0828
www.ludlums.com

IN/US Systems, Inc.
5809 North 50th Street
Tampa, Florida 33610
(813) 626-6848
www.inus.com

Saint-Gobain Crystals & Detectors
1655 Townhurst Drive
Houston, Texas 77043
(281) 355-1033
www.detectors.saint-gobain.com