September 2004 System Assessment and Validation for Emergency Responders (SAVER)

Homeland Security

Science and Technology

Summary

Intrusion Detection Sensors

SPAWAR Systems Center, Charleston, prepared the Handbook of Intrusion Detection Sensors *at the request of the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Charleston, SC 2004. It is available by request at* https://www.rkb.us/saver.

Background

The *Handbook of Intrusion Detection Sensors* contains information on perimeter security and intrusion detection sensor technologies. The handbook is intended to be used as a reference for first responders, military, law enforcement, and other security specialists who need general knowledge of the types of tools available. Construction of an integrated security system involves not only design, construction, and testing, but also the long-term issues of monitoring, maintenance, and training. Security consultants may need to be involved in several aspects of a system's life cycle.

Sensor Employment Considerations

Operational Requirements

The type of facility or material to be protected, the surrounding natural and human environment, assumptions about potential threats, the activity level in and around the facility, the physical configuration of the facility, weather variations, permanence, training, maintenance, support, and the client's previous security experience all need to be assessed before a security solution can be developed. The main elements of an intrusion detection system include the sensors, the alarm processor, the monitoring system, and the communications architecture that connects these elements. In most cases, detection sensors are used in conjunction with physical barriers, access control systems for personnel and vehicles, and other sensor technologies. Training, monitoring, and the availability of a professional team to respond to intrusions are also essential for an effective system.

U.S. Department of Homeland Security

SAVER

System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective operational tests on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

To contact the SAVER Program Support Office
Telephone: 877-336-2752
E-mail: saver@dhs.gov
Visit the SAVER Web site:
https://www.rkb.us/saver

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. Neither the United States Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

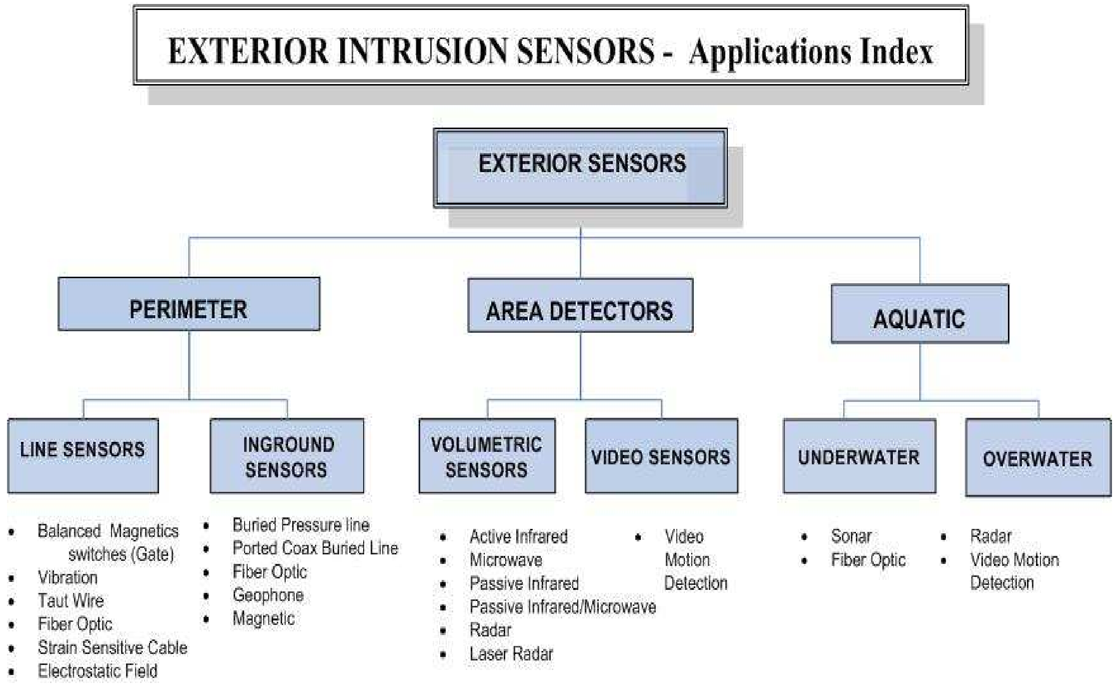

Table 1. List of Exterior Intrusion Sensor Applications

Performance Characteristics

A major goal of a security planner is to design a system that has a low false alarm rate, low nuisance alarm rate, low vulnerability to defeat, and a high probability of detection. Adjusting a sensor's parameters to improve one variable may have an adverse effect on another. Therefore, settings must often be balanced to achieve an acceptable overall level of performance.

The probability of detection is a measure of the sensor's ability to detect an intrusion within the zone of coverage. It is affected by several factors, including the environment, installation, adjustment, and the behavior of the intruder.

A nuisance alarm is a legitimate detection caused by something other than an intruder. Since sensors interact with their environments, all sensor systems are vulnerable to nuisance alarms. The cause of an alarm is not always discernable; therefore, an alarm assessment capability needs to be included in the design of the security system to prevent security personnel from having to respond to every alarm.

When the cause of a nuisance alarm is not immediately discernable, it may be counted as a "false" alarm. The false alarm rate indicates the expected rate of occurrence of alarms that are not due to a legitimate detection. The false alarm rate of any sensor system should be very low.

The vulnerability to defeat is another measure of a sensor's effectiveness. Since no sensor is absolutely reliable, a system's design should incorporate measures using multiple sensors and sensor types to lower the potential for defeat.

Factors Affecting the Probability of Detection

The probability of detection for an integrated sensor system will depend on the selected sensors, the installation, sensitivity settings, local environmental conditions, maintenance, and assumptions about potential intruders. When calculating the probability of detection, it is better to specify parameters that are testable, instead of relying on a specific number. Maintaining a high probability of detection through out the life of a security system is an ongoing process that involves maintenance, training, and many other considerations.

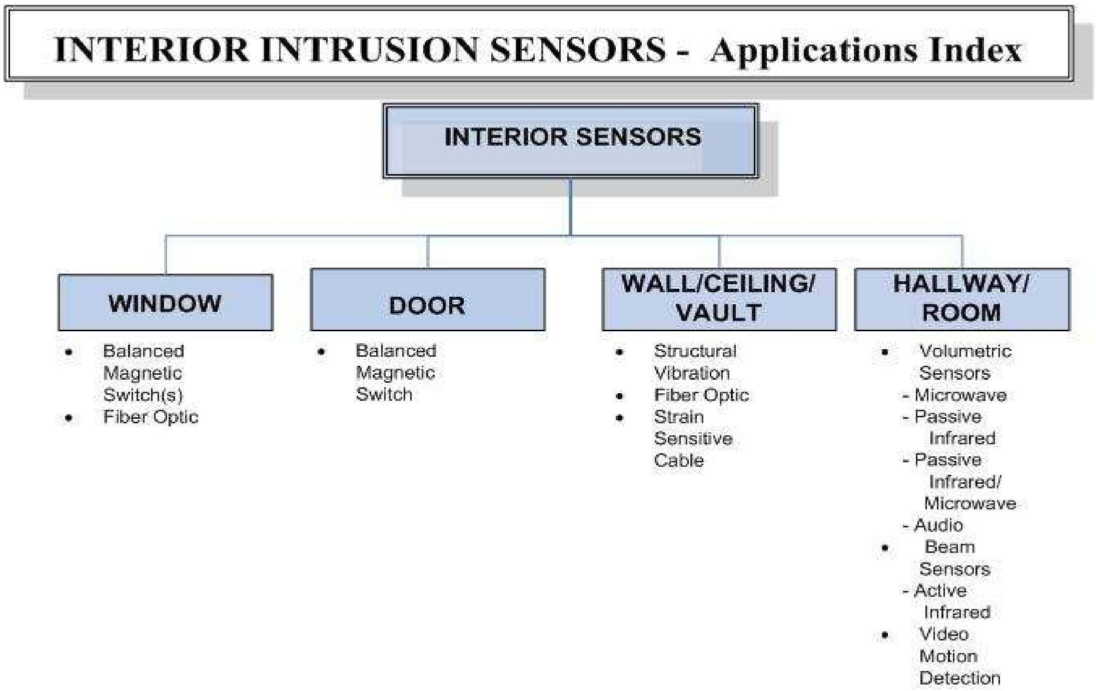

Table 2. List of Interior Intrusion Sensor Applications

Sensor Categories

The most basic categories of intrusion sensors are interior and exterior. There are sensors designed for underwater use and others that are portable or quickly deployable.

Interior sensors perform one of three functions:

1. Detection of an intruder approaching or penetrating a secured boundary, such as a door, wall, roof, floor, vent, or window;
2. Detection of an intruder moving within a secured area, such as a room or hallway;
3. Detection of an intruder moving, lifting, or touching a particular object.

Exterior sensors detect intruders crossing an outdoor boundary or entering a protected zone. While many interior sensors should not be exposed to weather, exterior sensors must be able to withstand outdoor weather conditions. Exterior sensors have a higher nuisance alarm rate than their interior counterparts and a lower probability of detection, primarily because of uncontrollable environmental factors. Underwater sensors detect or deter divers, swimmers, and watercraft, and are of most interest in situations such as ports, harbors, offshore rigs, and individual vessels. Portable devices are interior, exterior, or aquatic and are of most interest to incident response teams, who must quickly isolate an area and control ingress and egress.

Environmental Considerations

The environment must be considered when designing and building any security system. Exterior sensors are likely to be affected by weather, animal activity, and human activity patterns. Air movement, machinery noise, vibrations, changes in temperature, and changes in lighting are some factors that can affect interior sensors.

Alarm Monitoring Systems

There is a variety of alarm monitoring systems on the market. All systems announce alarms and display the intrusion locations. State-of-the-art systems provide visual and audible indications. Most are configured for Pentium-type computers utilizing the Windows or UNIX operating system. Laptops and hand-held computers can be used in situations requiring portability.

Alarm Assessment

Assessment elements are used to determine whether an intrusion has occurred within the secured area. Security operators use closed-circuit television, thermal imagery, and sometimes response force observation to analyze the audible and visual alarm data. Many systems can train cameras toward an alarming zone so that security personnel have a real-time view of the situation to track the progress of an intrusion.

Sensor Integration

Intrusion detection systems may need to incorporate multiple detection technologies to protect against the weaknesses of any one technology, to enhance the probability of detection, and to provide security personnel with a means to assess alarms.

Communications

Communications between the command-and-control unit and the field elements should employ standard communications protocols.

Power Supply

All intrusion detection systems are vulnerable to losses of electrical power and should incorporate backup power sources. The best time to define power requirements is during the design phase.

Costs

The costs of an intrusion detection system are easy to underestimate. Some techniques to minimize costs include being careful when defining the threats, buying multiple types of systems, selecting from among several technologies providing similar categories of protection, and using suitable existing infrastructure.

Technology Reviews

The main section of this handbook is a set of twenty-one intrusion sensor technology reviews that cover operating principles, applications, and integration techniques. For a list of exterior intrusion sensors see table 1. Interior intrusion sensors are listed in table 2.

Vendors

Finally, the handbook includes a list of vendors who responded to the request for information in the Federal Business Opportunities Journal. There is a matrix that cross-references the vendors with the types of sensors they have available.