Perimeter Protection Solutions

Address: Hungary, 1192 Budapest, Nadasdy str. 2.
Tel/fax: +361-282-9940, +361-280-8395, +361-280-8397

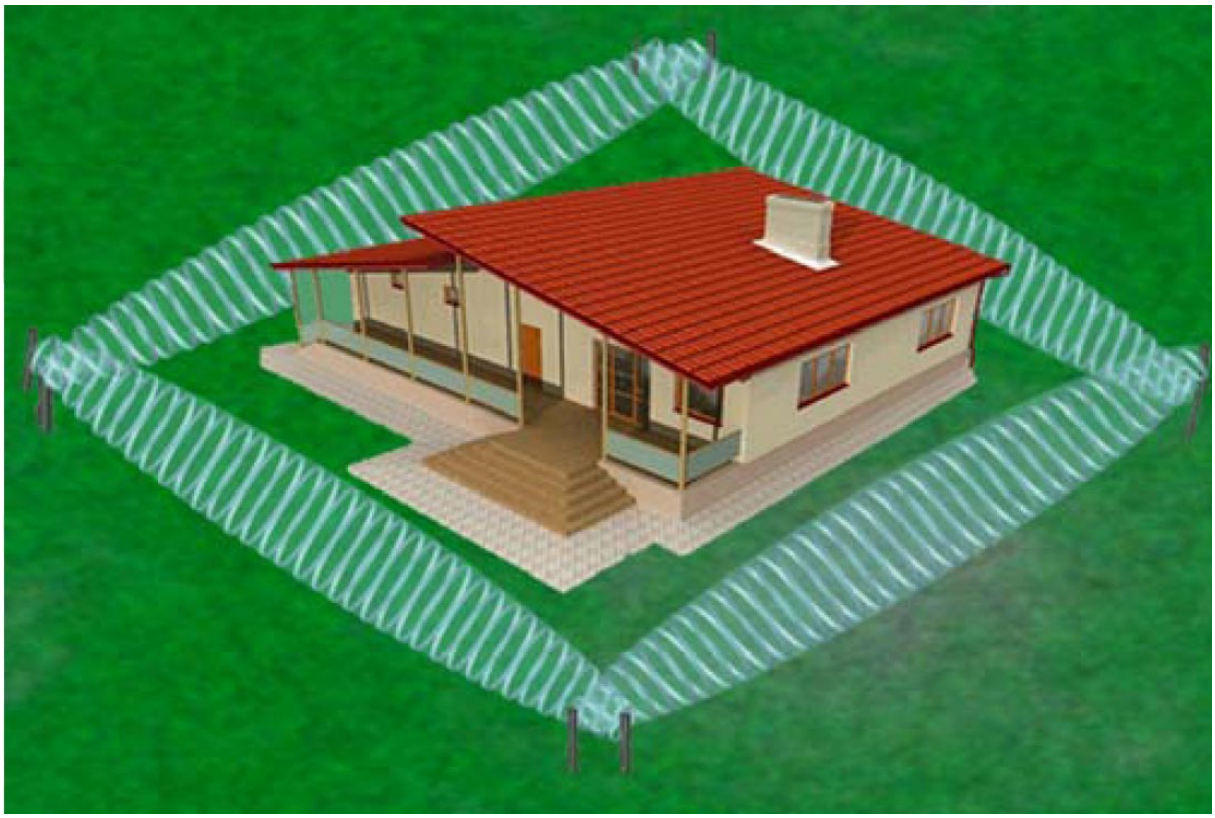
www.umirs.eu

BASIC PRINCIPLES OF PERIMETER SECURITY

v1.0

Basic Principles of Perimeter Security

A
Umirs Europe
Primer



Definition of perimeter security

A perimeter security system is a system of security devices installed around an object (or territory), or sometimes inside the borders of an object. A perimeter security system thus represents the first line of an object's defense.

Importance

The effectiveness of an alarm system depends on how fast it can detect an intruder. If the system is not equipped with perimeter security, an intruder can be detected only once already inside of the defended object. That means the intruder has an opportunity to breach the object's physical barriers (fences, walls, etc.) and have a closer look at the facility, and to further assess any weak points in the system. Even if the actual intrusion finally activates an alarm, a dangerous time lapse has already occurred, which is absolutely intolerable in a modern, effective security system. For decades now, perimeter security systems have been deployed to successfully defend high-security objects (airports, military facilities, power plants, etc.) against intrusion. Nowadays, perimeter security is also gaining recognition in the civil sphere as effective protection for warehouses, industrial facilities, offices and private residences. Without perimeter security, an alarm system issues an alert only after an actual intrusion has already occurred. Perimeter security more preemptively acts to prevent actual intrusions - an intruder is detected in the first line of defense, before having jeopardized the safety of persons and property inside the facility itself.

Basic principles

Efficient operation of a perimeter security system is greatly affected by environmental conditions. Frequent changes of weather, extreme temperature fluctuations, diversity of nearby vegetation and movement of animals may pose serious challenges to perimeter security systems. Comprehensive observation and analysis of the area where the system is to be deployed is essential, and vital to the successful operation of the installed perimeter security system.

• The installer must always assess the place of installation carefully.
How large is the area to be protected? How can the power supply and cabling be routed? Are there trees, bushes or high grass in the immediate vicinity? If so, is it possible to arrange for their periodic maintenance? Are there any other devices located nearby which might disturb the perimeter security system's operation? Are there high-voltage cables or power transformers in the vicinity? Is the area flat or sloping? How frequently do local weather conditions change? Does fog often occur? Does rainwater drain off, or does it collect in the area? Which sectors are most exposed to sunlight, and which less? Etc. …

• It is important to define precisely what must be protected.
The entire area around the object? The approaches to the object? A trap-like defended sector of the area? The spaces around the gates/doors/windows of the object? What must be prevented, simple trespass, or the theft of only certain goods?

• Who are the potential intruders?
Occasional trespassers? Professional intruders with experience in security systems? Intruders on foot? Intruders arriving by vehicle? Etc. …

• The defended area must be limited and observable.
Another important consideration is that the area must have explicit barriers (fences, walls, etc.). These somewhat keep some potential intruders away from the object, though much more importantly, an intruder cannot penetrate the area by accident, but only with intent. The barriers also keep stray animals away from the object, thus reducing the number of false alarms. In certain cases, fences and walls can also serve as mounting surfaces for detectors. In case of an alarm, the area must be effectively observable by cameras and guards. Proper illumination of the area is also important.

• No security system can guarantee 100% success - this also holds true for perimeter security.
Variable conditions occur much more often outdoors than inside buildings. The installer must take into consideration many more potentially disturbing phenomena during the design and installation of an outdoor system. The efficiency of perimeter security systems is highly dependent upon the quality of installation. False alarms generated by perimeter security nearly always have an identifiable cause, though it can sometimes be difficult to pinpoint it. One or two false alarms per month can be reasonably expected of a perimeter security system.

• The higher the level of security, the higher the number of false alarms.
A moving vehicle can be detected relatively easily because of its size. It's much more difficult to detect a person on foot. If the person is crawling, it's even more difficult to detect him, and if it's a small child, might appear no bigger than a large cat. The smaller the object that must be detected, and the more sophisticated the manner of intrusion, the higher the possibility that something (an animal, or a moving tree branch, for example) will cause a false alarm.

• The less careful the installation, the more frequent the false alarms.
Many perimeter security systems are installed improperly. In these cases, the number of false alarms increases drastically. And, what is even more dangerous, improper installation also increases the likelihood that the system won't detect a real intruder.

• There must always be a reaction to an alarm.
The alert of an alarm system is not valuable in itself, if nobody reacts to it. An alert must always be acted upon, and analyzed to determine what caused the alarm. The cause of periodic false alarms must also be found. It must too be kept in mind that an intruder may initially intentionally provoke a number of false alarms to lull security personnel into believing that the actual intrusion itself is probably just another false alarm.

• The minimization of potentially disturbing conditions has paramount importance.
In an outdoor area much more attention must be given to the minimization of potentially disturbing environmental factors than in indoor conditions. Close to power transformers and power lines, wiring and cabling must be adequately protected (with the use of additional insulation, ferrite rings, etc.). In such areas the use of back-up batteries for continued power supply is often recommended. It is also prudent to equip the system with defense against lightning strikes. All the components of a perimeter security system must be suitable for outdoor use. Often, just one non-outdoor use component (for example, a relay) can be the cause of numerous "mysterious" false alarms.

• Importance of testing.
The successful operation of a perimeter security system depends on numerous factors, which sometimes are left without attention even by highly experienced installers. A perimeter security system is not likely to work successfully without comprehensive preliminary testing. After initial installation, a 3-day test period is recommended, during which the causes of all alarms are noted, and test intrusions are attempted. Because of changable outdoor conditions, periodic testing must be performed more frequently than in the case of indoor devices.

• Importance of maintenance.
In an outdoor area the environment changes constantly. For the proper operation of a perimeter security system, it is vital that adjacent natural features (grass, bushes, tree branches, etc.) always be maintained in consistent trim. Maintenance is always necessary after severe weather (storms, strong winds, etc.) - the continued proper fastening, positioning, isolation and operation of all system components should be verified. Neglect of maintenance could jeopardize the continued proper functioning of the system.

• "The good might also be bad".
Even a high-quality perimeter security system can operate improperly, if its installation, positioning, tuning and testing weren't carried out properly, or if its operational area hasn't been properly prepared and adequately maintained. The design, installation and maintenance of a perimeter protection system demand much more attention and labor than do indoor security devices.

CLASSIFICATION OF DETECTORS

Active and passive detectors

Active detectors always radiate some energy (infrared light, microwave radiation) on the defended area. The detection zone of active detectors is commonly much more precise, as they transmit more data to the signal analyzer. Active detectors are more difficult to sabotage than passive ones. With active detectors, the possible mutual effects of two or more devices defending the same area must always be considered. Typical active detectors are infrared and microwave barriers.

Passive detectors do not radiate any energy, but instead detect an intrusion due to change of environmental conditions. A great benefit of passive detectors is that two or more devices have no mutual effects. Additionally, a line or area defended by passive detectors is difficult to identify even by an experienced intruder. A typical passive perimeter protection detector is a passive infrared detector.

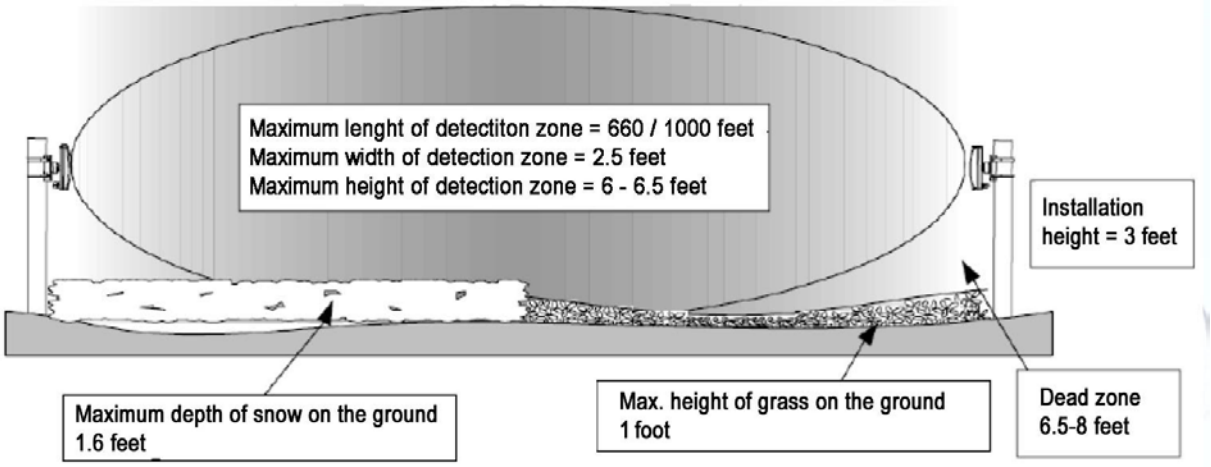
Volumetric and linear detectors

The detection zone of a volumetric detector occupies three dimensions, and is therefore more difficult to penetrate without detection. The weakness of volumetric detectors is that a wider detection zone demands more maintenance. Additionally, the wider zone may result in a higher number of false alarms. Also, with volumetric detectors the border of the detection zone is not always definite, as detection depends much on the size and shape of the intruder, its speed, etc. Volumetric detectors include volumetric microwave and passive infrared detectors.
The detection zone of linear detectors is much narrower, which is therefore easier to "cheat", though they demand much less open space for operation, and the defended area is more easily maintained.

The borders of the detection zone are much more clearly defined, and consequently the number of false alarms is lower. Infrared barriers are typical linear detectors.

CHARACTERISTICS OF MICROWAVE DETECTORS

There are two main types of microwave detectors: one-position microwave detectors, and microwave barriers (two-position detectors). With one-position detectors, the transmitter and receiver are combined in one unit. The device emits microwave radiation, and an alarm is caused by the reflection of the signal from an object inside the detection zone. A microwave barrier consists of two separate units, a transmitter and a receiver, positioned one in front of the other approximately one meter (39 in.) above the ground. The transmitter sends a microwave signal to the receiver. An alarm is caused by the change of received signal strength provoked by an intruder. Microwave radiation is reflected by metal and water-containing objects (for example, a human body). Microwave emissions can pass through thin walls, roofs or other materials. Microwave barriers offer secure protection for relatively long distances, and have superior, all-weather operational capability. It should be noted, however, that microwave barriers also require a much broader operating space than infrared barriers.



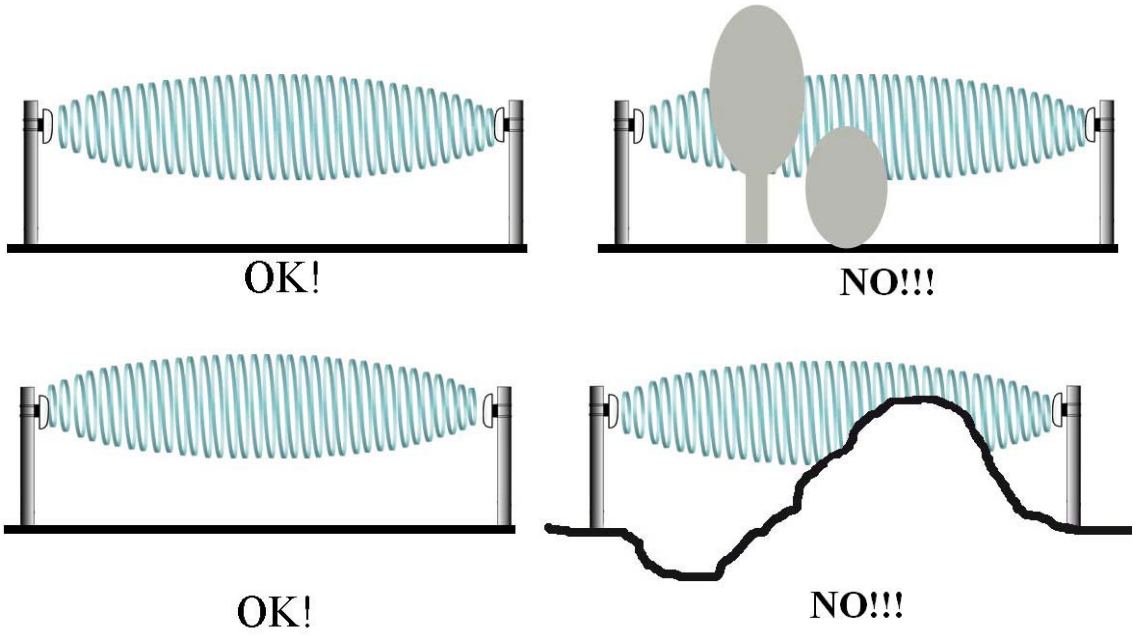
The higher the operating frequency of a detector, the narrower its detection zone. Microwave barriers usually have an operating frequency in the X-range at around 10GHz. It should also be noted that, the longer a detector's operational distance, the more difficult it is to identify an intruder. Thus, rather than protecting a 300-meter (984 ft.), for example, distance with one barrier, often six separate 50-meter (164 ft.) barriers are used instead, to make identification of an intruder easier. Microwave barriers are active perimeter security devices, thus giving a higher level of protection than passive detectors. Often the detection zone of a microwave barrier is more difficult to bypass, as it also has a certain height and width. At the same time, false alarms may occur more often with a wider and higher detection zone, although in the case of a properly installed and maintained microwave barrier this level is also minimal. The detection zone of a one-position microwave detector takes the form of a balloon turned on its side (in the case of long-distance detectors, this shape is a bit elongated). The detection zone of a microwave barrier takes the form of a cucumber. The detection zone of microwave detectors does not have such strict borders as passive and active infrared devices do. The detection zone of microwave detectors must be augmented by a so-called "clear zone". The clear zone is an area which must be kept free of branches, high grass and other objects (especially objects reflecting microwave radiation) for the safe and proper operation of the detector. The clear zone obviously contains the detection zone itself, which occupies approximately half of the clear zone. Required sizes of clear zones for detectors vary, and are usually stated in their manuals. A microwave detector is an active device, and therefore the

radiation emitted from one detector may disturb another. This can be eliminated by correct design of the system, proper installation and the synchronization capabilities of the the devices themselves. With the use of a microwave barrier, there is always a “blind zone” under the transmitter and receiver - the barrier cannot detect motion in this zone. This zone poses a substantial danger if left unaddressed, but may be eliminated by “crossed” installation of the barriers or the installation of supplementary detectors. Of all the devices mentioned above, microwave detectors are the most resistant to changes of environmental conditions. If there is a clear zone of the proper length and width for the operation of the detector, it is considered to be the most effective security solution.

The following points must be considered when installing a microwave detector:

• For proper operation a clear zone, as specified in the manual of the particular device installed, must be established. This area should be free of trees and bushes (including their branches), long grass and other objects which could potentially cause false alarms. It is preferable that the area be as level as possible - hillocks and pits reduce the security level of the detectors, as they may give an intruder (on the receiver-side of a hillock, or in a pit) an opportunity to penetrate the detection zone without being detected. In the case of one-position detectors, objects inside the detection zone would not always present a problem, the main point being that these objects must not move, as motion leads to change of the reflected microwave signal, and causes an alarm. With microwave barriers, objects within the detection/clear zone are not recommended, as their presence reduces the level of microwave signal reaching the receiver, and could disturb the proper operation of the barrier. It should also be noted that some objects (for example, wooden fences) in or around the clear zone may absorb water during and after rain or snow, thereby becoming themselves reflectors of microwave radiation. For implementing the most precise installation possible, the device’s manual should always be consulted.

• The motion of a large metal object (gate, truck, train, etc.), even outside the clear zone, may have the same effect on the barrier as an actual penetration by a human. That’s why, in areas where such potential disturbances may occur, it’s prudent to increase - even to double - the width of the clear zone.

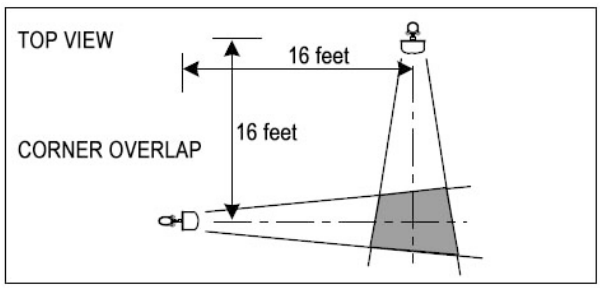


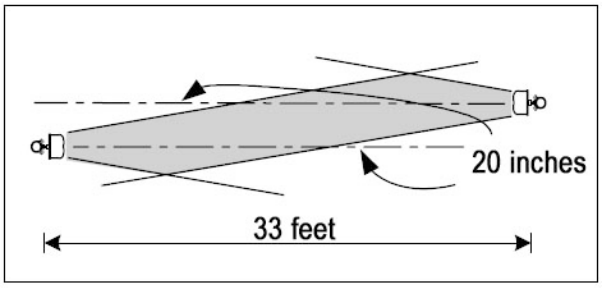
• As mentioned above, when installing two or more microwave detectors in relatively close proximity, attention must be given to the possibility of interference between the detectors. It must be ensured that radiation from one transmitter is not picked up by the receiver of a different barrier-pair either directly, or via reflection. If this is not possible, the detectors must be synchronized. It's prudent to first inspect the area, noting the positions of metal fences and other objects, and to make a rough sketch of everything observed before proceeding with the actual installation. Careful attention should be given to objects which appear innocuous at first glance, but which could conceivably become a source of disturbance later due to water absorption (for example, wooden fences). Prevention of interference is somewhat easier with one-position detectors, although it's also true that such devices are usually installed closer to each other. Microwave barrier transmitters radiate signals further than just the nominal length of the detection zone - a 10GHz microwave barrier transmitter can radiate a direct or reflected signal for a distance 1.3 times longer than the nominal operating distance of the detector at a 30° angle. One of the basic principles of installation is that a crossed configuration place like-devices next to each other (i.e., transmitter-transmitter, receiver-receiver). A reduction of interference may also be achieved by synchronization of the detectors, using different operating frequencies. This solution is viable only with microwave barriers where, depending on the device, two or more operating frequencies are available. Experience of installers shows that most problems with microwave security systems occur because of interference between the devices, so close attention should be given to this possibility.

• To minimize potential unnecessary interference, the installation should be scaled appropriately. Avoid using detectors whose operational distance significantly exceeds the length of the area to be protected. For example, use a 100-meter (328 ft.) barrier-pair, not a 300-meter (984 ft.) barrier-pair, to protect a standalone 100-meter (328 ft.) perimeter segment. Also, avoid chaining together detectors having different operational distances. For example, the more powerful microwave signal emitted by the transmitter of a 300-meter (984 ft.) barrier-pair might interfere with the proper operation of an immediately adjacent 100-meter (328 ft.) barrier-pair.

• The general surroundings of the installation area should be assessed - if there is a microwave device already in operation in the vicinity, it could conceivably cause plenty of "undefinable" anomalies in the operation of the microwave security system. In this event, ask the dealer/distributor for advice/assistance. It is a basic principle that the use of unrelated microwave devices in the same area should be avoided wherever possible, as their synchronization is at best difficult, or simply not possible.

• For elimination of blind zones, a crossed installation is always recommended. This may be either a perpendicular or straight-line crossing, depending on the area. If a crossed installation is not possible, the columns should be augmented by an additional detector. Illustrated below are examples of perpendicular and straight-line crossed installations.





• The cabling and positioning of microwave detectors usually do not cause problems. The most difficult challenge is to design the system in such a way as to eliminate interference. To check for flaws in the design of a system, the system must be tested - after installation, a 3-day test period with test intrusions

and analysis of all alarms is recommended. One good way of testing a microwave barrier is to switch off the transmitter - if the receiver does not issue an alarm signal, there surely must be interference, as the receiver still receives a microwave signal from another transmitter.

• With microwave security systems, as with other perimeter security systems, maintenance (mowing grass, cutting down protruding branches, etc.) of the operational area of the detectors is critical for proper operation. This must be done both periodically, and after severe weather (storms, strong winds, etc.).

The reliable operation of the microwave detectors offered by our company is ensured by the expertise of the manufacturer, and confirmed by numerous successful installations the world over. In addition to one-position microwave detectors and microwave barriers, we also offer sophisticated portable microwave protection systems for the temporary protection of objects.

We encourage you to visit our website (www.umirs.eu) to learn more about us and our outdoor perimeter security solutions.

Further inquiries are welcome and should be directed to:

Mr. Ronnie Walling (Export Manager - Americas, rwalling@umirs.eu).