Perimeter security: because walls alone are not enough.

Individual security concepts and intelligent systems for your outdoor space.

For our customers, success is defined by how well they manage these challenges. Siemens has the answers.

“We are the preferred partner for energy-efficient, safe, and secure buildings and infrastructure.”

Answers for infrastructure.

Our world is undergoing changes that force us to think in new ways: demographic change, urbanization, global warming, and resource shortages. Maximum efficiency has top priority – and not only where energy is concerned. In addition, we need to increase comfort for the well-being of users. Also, our need for safety and security is constantly growing. For our customers, success is defined by how well they manage these challenges. Siemens has the answers.
Perimeter security is more than just the details.

Fences, walls, intelligent detection technology, and the latest surveillance measures: today the options for comprehensive perimeter security around a property are more diverse and complex than ever before. And that’s a good thing. Whether for VIPs, airports, forensics, penal institutions, industrial properties with high security requirements (such as logistics or chemical companies), solar facilities, outside warehouses, or power plants, appropriate preventive measures help to preclude or minimize damage. They contribute to the early recognition of offenders and support the rapid introduction of countermeasures as soon as danger is imminent.

However, just as it is not enough to stack individual building blocks on top of each other to form a wall, perimeter security requires a suitable “mortar” that binds all the parts together and optimally balances them for perfect stability. We are happy to create this connection for you. With individual security concepts that have one objective above all others: complete security. For the entire premises.
Security is a feeling – and a fact. While in certain senses feeling secure can be a very subjective thing, we first analyze your actual security needs for you and use this as a basis to develop an integrated security concept that factors in all security-relevant questions concerning perimeter security. This provides you with an overview – with optimal transparency and maximum assurance in making decisions.

**At the beginning, there is risk analysis:**
Every property is different and is “predetermined” in its own way to vulnerabilities from different threats and offenders. For this reason, the first thing we do in our analysis is to determine the types of possible threats your building periphery is exposed to as well as the profiles of potential offenders or offender groups. After site inspections and interviews, we prepare the individual security profile in cooperation with you. In the process, it is worth considering that threats to a property can emanate from two scenarios.

- **Your security goals: a matter of definition**
Before we consider how your security concept would appear in its ideal form, we first need to define more precisely the area to be protected. Depending on the local conditions, within the framework of the risk analysis we define if and how the legal boundary line is shown as well as if and how special security measures are used before this line. Furthermore, we clarify the best way to protect you from intrusions, breakouts, and vandalism or from the illicit transfer of products or money.

- **All good things come in threes:** your security measures
After this preliminary work, we can derive the additional security measures – from the technical solution to its coordination and connection. Generally, a property is only well protected if the resistance time of a mechanical security measure is equal to or greater than the reaction time the guards need to arrive on site.

- **Mechanical security measures**
One of the first steps in defining a security concept is devising appropriate – and lasting – mechanical security devices. In addition to indicating the property lines, the purpose of mechanical security measures is to prevent intrusion into the secured area or movement within it. In many cases, naturally occurring features – such as ditches and embankments, thorn bushes, moats, and ponds – already provide good perimeter protection that can be reinforced with fences, bollards, and road blocks. Nevertheless, it should be taken into account that mechanical security still needs to function properly if weather conditions change.

- **Electronic monitoring**
For different applications, such as fence surveillance, detectors that secure the ground area, or different detection devices that monitor smaller or larger spaces, Siemens can offer you the best solutions.

- **Organizational measures**
If anything is detected, notification will be conveyed to the appropriate sites. In this case, only the interventions that have been specifically agreed upon for the property will be initiated. Thus everything is perfectly organized.

**At the end, there is the overall concept**
An overall concept includes securing both the inside and outside of buildings and consists of the synergistic total of individual measures to achieve the desired security objectives. Profit from our experience and focus on an overall solution. For your secure satisfaction.

---

**Step by step to the security concept**

1. **Step 1: Risk analysis**
   Describing possible threat scenarios and perpetrator profiles, determining risk potential and vulnerabilities.

2. **Step 2: Security objectives**
   The most important security objectives are determined depending on the local conditions, for example, indicating the property line or protecting against vandalism.

3. **Step 3: Security measures**
   The mechanical, electronic, and organizational security measures are derived from the security objectives.

**Security concept**
In the end, there is the overall concept that optimally aligns all security measures with each other.
The most important application areas at a glance:

1. Area between fences (“sterile” zones)  
2. Laser scanners  
3. Rooftop areas  
4. Microphone sensor cables  
5. Active IR light barrier  
6. Fiber-optic sensor cables  
7. High-frequency signal cables  
8. IR motion detectors  
9. Ground sensors  
10. Long fences  
11. Individual fence panels  

Using our overview graphic, we have provided you with examples of where each perimeter security solution can be used to best effect.

Adaptability is everything. Therefore, application-specific sensors that have been optimally adjusted to the requirements of their respective fields of application are used to electronically survey critical outdoor spaces and to monitor fences, boundaries, and rooftops as well as to automatically trigger the necessary security measures.

Our building blocks for perimeter security
Four sectors for comprehensive security.

Your property can be threatened from every direction. Therefore, dividing your perimeter into clearly structured sectors helps to determine various security measures that make it possible to prepare rapidly and securely for any scenario.

Monitored perimeter areas are divided into four sectors so you can find the optimal orientation and plan. Both mechanical and electronic measures can be allocated according to your security objective.

- **Sector 0**
  A single, specific strip of ground that lies outside the perimeter area to be protected. In this sector, it is possible to hinder and detect an unauthorized approach.

- **Sector 1**
  A closed boundary line along the perimeter area that may be defined, for example, by a fence, wall, or moat, and that prevents or detects crossing into this sector.

- **Sector 2**
  The entire area within the perimeter without buildings or facilities to be protected. Entry into this sector or movement within it should be hindered or detected.

- **Sector 3**
  A space within sector 2 that encompasses the buildings or facilities requiring protection. A possible surveillance objective may be to detect anyone who is entering, climbing, or damaging such buildings or to prevent these from happening.

Using the color-mapping of the individual sectors, it is possible to see the respective effectiveness in the corresponding areas in the following overview.

Sensitive sensors – reliable detection.

Different security objectives demand different sensors. As a result, the following criteria should be considered when deciding on electronic detection measures.

- Reliability of detection
- Number of unwanted notifications
- Detection possibilities
- Security against tampering
- Security against transmission

Active IR light barriers

Light barriers are suitable for monitoring lines along fences and gates and for curtain monitoring of properties, windows, and walls. This monitors any persons or vehicles entering the property while also monitoring passage and access.

- **Detection principle and specification**
  - Systems consist of transmitter and receivers with one or more light beams
  - Monitor the light beam for interruption and manipulation by extraneous light
  - Any interruption of the light beam by intruders will be reliably recognized

- **Pros and cons**
  Good monitoring of linear stretches. The monitoring height can be flexibly varied by individual configuration of the columns. Limited functionality in the event of poor visibility (monitoring approx. 1.5 m × visibility range).

Microwave detectors

They are used to monitor lines along fences, on rooftops, and over large areas and report anyone who walks into or drives through the surveillance area.

- **Detection principle and specification**
  - The sensor consists of separate transmitting and receiving units and creates a volumetric electromagnetic field between them
  - Changes to the field due to absorption or reflection of objects or people in the detection area are consistently recognized

- **Pros and cons**
  Due to its high sensitivity, this solution enables good detection under almost any weather conditions at a height of up to 15 m. However, it is less suitable when narrow detection zones of less than 2 m are required.

Laser scanner

They serve as curtain sensors for properties or penetration detectors for walls and larger flat, open spaces (for example, zones between two fences) and monitor possible access as well as anyone walking or driving into the area.

- **Detection principle and specification**
  - They scan the surrounding area in two dimensions with laser beams
  - Objects and people are detected using time-of-flight measurement of the reflected light, and their size, distance, and speed with regard to the sensor are determined

- **Pros and cons**
  This first-rate solution proves itself through its significantly low false-alarm rate and can be installed easily in all areas. Additionally, it offers the option of concealed mounting.

Surveillance area/detection

- Range of approx. 100 m, scanning angle of max. 270°
- Exact localization of an object, universally adjustable detection areas and object properties, multiple alarm zones that can be adjusted with different parameters
Video sensors

- Detection principle and specification
  - The video sensors use algorithms to define objects that should be recognized or followed in the video image.
  - In the video image, the algorithms recognize objects and people who move within a camera’s viewing range.

- Pros and cons
  - The easy tracking of objects is also possible through the camera. Algorithms make it possible to recognize alarm situations with certainty.

Microphone sensor cables

- Detection principle and specification
  - The sensor cable is attached to the fence.
  - Vibrations on the fence caused by intruders are immediately recognized and analyzed.
  - In contrast to analog systems, digital systems can precisely localize alarms using time-of-flight measurement.

- Pros and cons
  - The security measure can be installed easily and quickly and offers the advantages of low cost and easy maintenance. It should be kept in mind that the system is also vulnerable to attack.

High-frequency signal cables

- Detection principle and specification
  - Invisible HF field between two concealed sensor cables buried in the ground.
  - Changes to the field caused by intruders are recognized and evaluated.

- Pros and cons
  - Assembly costs are high, but so are the advantages: The surveillance field follows the shape of the landscape and adjusts to it perfectly. Furthermore, the cables are in the ground and can only be installed so that they are invisible.

Ground sensors

- Detection principle and specification
  - Concealed individual sensors are networked with each other.
  - They work dynamically and transform changes in pressure into electrical signals via piezo elements.
  - Changes to the field caused by intruders are recognized and evaluated.

- Pros and cons
  - Detection depends heavily on the installation (assembly depth), and assembly in turn brings higher costs with it. The major advantage: the option of precisely defining detection areas.

Fiber-optic sensor cables

- Detection principle and specification
  - The sensor cable is attached to the fence.
  - Vibrations on the fence caused by intruders affect the optical behavior of the fiber-optic sensor and are recognized.
  - Analog systems measure and evaluate light intensity, while digital systems precisely locate alarms.

- Pros and cons
  - Assembly costs are high, but so are the advantages: The surveillance field follows the shape of the landscape and adjusts to it perfectly. Furthermore, the cables are in the ground and can only be installed so that they are invisible.

IR motion detectors

- Detection principle and specification
  - IR detectors can measure changes in temperature, which enables them to recognize heat-radiating objects.
  - Temperature changes in the surveillance area caused by a moving intruder are reliably recognized.

- Pros and cons
  - The solution is cost-effective and is easy to install and maintain. Sensitivity can also be adjusted for each sensor. However, its dependence on weather conditions is a disadvantage. Detection is severely restricted when visibility is poor.

Radar sensor

- Detection principle and specification
  - The sensor cable is attached to the fence.
  - Vibrations on the fence caused by intruders affect the optical behavior of the fiber-optic sensor and are recognized.
  - Analog systems measure and evaluate light intensity, while digital systems precisely locate alarms.

- Pros and cons
  - Assembly costs are high, but so are the advantages: The surveillance field follows the shape of the landscape and adjusts to it perfectly. Furthermore, the cables are in the ground and can only be installed so that they are invisible.

Fence sensors

- Detection principle and specification
  - Piezoelectric or capacitive sensors installed at various points measure vibrations from intruders (structure-borne sound) and transform them into electric signals.
  - Capacitive sensors can also be used in part to check the installation position.

- Pros and cons
  - They are used primarily to monitor fences or walls and report anyone climbing over or climbing through secured areas.

- Detection principle and specification
  - Pressure-change systems react to any persons or vehicles entering the property and are ideal for area surveillance of open spaces and paths or of uneven ground.

- Pros and cons
  - They report anyone entering large areas on foot or by vehicle or, in the case of curtain monitoring on fences, anyone attempting to climb through.

- Pros and cons
  - This solution is especially well suited to monitoring lines, such as long fences, solar panels, or pipelines, as well as preventing anyone from climbing over or through them or from digging them up.

- Pros and cons
  - This can be implemented over long distances and the cable can simultaneously be used by other applications, such as video, and thus reduce costs. However, cost reductions are only seen when used at distances of 8 km and greater.
In the end, one thing matters more than anything else: perfect integration.

It’s good to know what holds the security world together at its innermost core. Benefit from our knowledge and perfect your perimeter security concept. We offer you diverse integration possibilities in higher-level systems that you can use to centrally administer every component of your security technology.

• Siveillance SiteIQ: wide area surveillance for a complete overview of the situation on site
  With SiteIQ, we offer you a solution that makes it possible for you to stop attempted security breaches before they even occur. The automatic wide-area surveillance solution combines traditional perimeter surveillance using fence and other sensors with intelligent video technology. It displays security-relevant data on a monitor in real time and continuously keeps your security personnel up to date regarding all events in the surrounding area. SiteIQ can be easily adapted to site-specific operational and security conditions and can be integrated into higher-level hazard management systems and control stations. In the process, it is possible to restrict access to selected areas or to the entire site, establish different security levels within a site, and upgrade or downgrade the respective security level.

• Intrusion detection systems at the highest level
  Perimeter monitoring devices are usually connected to standard intrusion detection systems. Here Siemens offers a comprehensive range of products for your customized solution. Whether you work with traditional stand-alone intrusion detection systems – such as our Sintony devices – with the innovative new SPC product family, or with the network-compatible Transliner Ringbus technology for the highest requirements, you are always assured that reports from the perimeter system are correctly prioritized. In the intrusion detection systems, perimeter reports can be interpreted and processed similarly to conventional intrusion, theft, and accident reports. Consequently, the alerting of response forces is assured either directly or via our own security control center.

Professional handling of all reports from the security system makes it possible for us to send you the necessary support quickly. No matter what measures become necessary. Both immediate intervention by security forces and the coordination of support through our service technicians: everything will be reliably attended to and with the greatest care in our emergency call and service center.

Paths to information bundling: react quickly, maintain security.

Particularly when different security mechanisms are combined, this can lead to a security vulnerability in the monitoring of various components. Our systems merge information under a common platform and offer you an additional security factor. Straightforward, low maintenance, scalable.

• Security management systems for comprehensive security
  Only combining all reports from the individual security solutions can give you control over the system and make security assessable. For this, Siemens offers you a range of different security management systems.

  The advantage is that all reports are brought together on a single surface. The management systems differ in the complexity of their options and specific primary uses. Your security requirements must be brought together into a common security concept with consideration of local conditions. Just as the management system must be adapted to the given requirements. The Siveillance Fusion system from Siemens security management offers you a reliable, scalable, and user-friendly solution for centrally administering your access control, video surveillance, and intrusion detection technology. The multisite approach for this solution makes it possible for you to receive reports from various sites and to attend to all systems at once as if they were a single system.

  The GMA manager is a management station that easily attends to and manages notifications from fire detection and security systems such as your intrusion or perimeter security system, including video cameras.

  Siveillance Vantage is used primarily when critical infrastructure needs to be monitored. In addition to the display and processing options of the individual security systems, Vantage also offers you the ability to manage response teams and resources.

Highlights

• A variety of integration options for all components in available systems
• Automatic wide-area surveillance with Siveillance SiteIQ
• Reliable intervention through intrusion detection systems
• Security at a glance with comprehensive management solutions