



**SIEMENS**

*Ingenuity for life*

## Einbruchmeldeanlagen

Safety • Security • Comfort • Solutions

[www.siemens.at/gebaeudetechnik](http://www.siemens.at/gebaeudetechnik)

## Einführung

Das vorliegende Kapitel enthält eine Zusammenfassung der wesentlichsten Aspekte der Intrusionsmeldetechnik. Diese Grundlagen sollen dem Anwender ein fundiertes Basiswissen in diesem Fachgebiet vermitteln.

### Definition Intrusion

Unter dem Sammelbegriff «Intrusion» wird, in Anlehnung an den englischen Sprachgebrauch, das gewaltsame oder durch List erreichte Eindringen Unberechtigter in einen umgrenzten Bereich bezeichnet. Der Einbruch geschieht mit der Absicht des Diebstahls, der Beschädigung oder des Missbrauchs, verbunden mit all den Begleiterscheinungen

wie Bedrohung oder Erpressung. Im weitesten Sinn fallen alle Arten krimineller Handlungen darunter.

Als Schutzsystem gegen Intrusion in diesem Sinne ist ein umfassendes Paket von Geräten, Steuerungen und organisatorischen Maßnahmen zur automatischen Entdeckung eines unerlaubten Eindringens (Intrusion) zu schnüren. Es ist wichtig, dass bei Entdeckung des Eindringlings innert nützlicher Frist geeignete stille oder deutlich wahrnehmbare Maßnahmen (Intervention) zur Verhütung von Schäden einzuleiten.

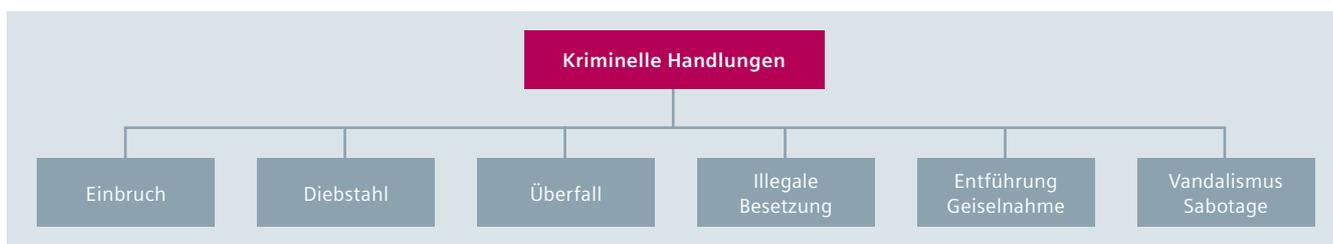


Abb. 1: Kriminelle Handlungen

### Zweck des Intrusionsschutzes

Das Schadenrisiko für Menschen und Sachwerte möglichst minimal halten durch:

- Prophylaktische Wirkung
- Abschreckung, Verunsicherung des Täters
- Frühzeitige Alarmierung der Interventionsstelle
- Verhinderung von Diebstahl

## Intrusionsmeldeanlage

### Das Grundprinzip des Intrusionsschutzes

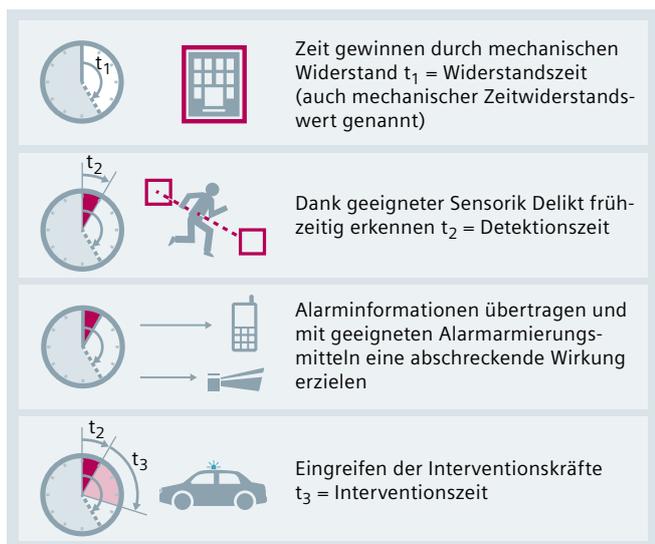


Abb. 2: Anforderung an ein Intrusionsschutz-System

### Das Schutzkonzept

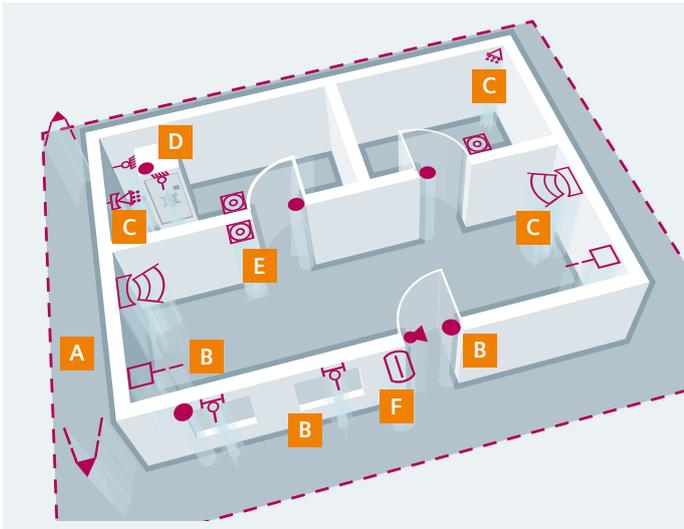
Jede Intrusionsmeldeanlage muss auf einem Schutzkonzept basieren. Darin sind alle zur Erreichung der angestrebten Schutzziele notwendigen Einzelmaßnahmen enthalten. Anzustreben ist eine sinnvolle Kombination von mechanischem

Schutz und elektronischer Überwachung. Sind die Bedrohungsarten nicht bekannt, müssen diese im Rahmen einer angemessenen Risikoanalyse festgestellt werden. Jeder erkennbaren Bedrohungsart ist im Sinne der Gefahrenabwehr ein Schutzziel entgegenzustellen mit der Absicht, gezielt das zweckmäßige Überwachungskonzept zu bestimmen.

Eine Typisierung von Schutzkonzepten nach Branchen (z. B. Gewerberäume, Bürogebäude, Bijouterien, Banken, Museen) sowie von Teilkonzepten nach Anwendungsfällen (z. B. Wertbehältnisse, Tresore, Personalschleusen) sichert die Nutzung von Erfahrungsgut und erleichtert zudem die Planungsarbeiten erheblich.

In ein Schutzkonzept einzubeziehen sind in jedem Fall auch die zur Erreichung der Schutzziele notwendigen baulichen (z. B. Mauerstärken, Türkonstruktionen) und die organisatorischen Maßnahmen (z. B. Sicherheitsdispositiv, Vertraulichkeit Schließpläne).

Zur fachgerechten Planung und Projektierung jeder Intrusionsmeldeanlage zählen auch Maßnahmen zur Vermeidung von Falschalarmen (z. B. Instruktion, angepasstes Bedienungskonzept, etc.).



- A Perimeter-Überwachung**  
Schutzziel: Unbefugtes Eindringen in oder Betreten von Gelände melden.
- B Peripherie-Überwachung**  
Schutzziel: Angriff auf die Peripherie eines Gebäudes oder Gebäudeteiles melden.
- C Raum-Überwachung**  
Schutzziel: Bewegungen in oder Betreten von bestimmten Räumen oder Bereichen von Räumen melden.
- D Objekt-Überwachung**  
Schutzziel: Angriff auf bestimmte einzelne Objekte im Gebäude melden.
- E Überfallmeldung**  
Schutzziel: Bei Bedrohung Alarm auslösen (still oder laut) können oder/und Bedrohungsablauf im Bild festhalten.
- F Zutrittskontrolle**  
Schutzziel: Bestimmten Personen den Zutritt zu bestimmten Gebäudeteilen zu bestimmten Zeiten gestatten.

Abb. 3: Überwachungskonzepte

**Der Aufbau der Intrusionsmeldeanlage**

Eine automatische Intrusionsmeldeanlage erkennt einen Eindringungsversuch durch Detektieren der Begleiterscheinungen wie Form-, Lage- oder Druckveränderung, Bewegung, Körper- oder Raumschall, Temperaturveränderung usw. Aufgrund vorgegebener Parameter wird automatisch die Gefährdungsstufe ermittelt und angemessene Maßnahmen in Form von Alarm- und Steuerfunktionen ausgelöst.

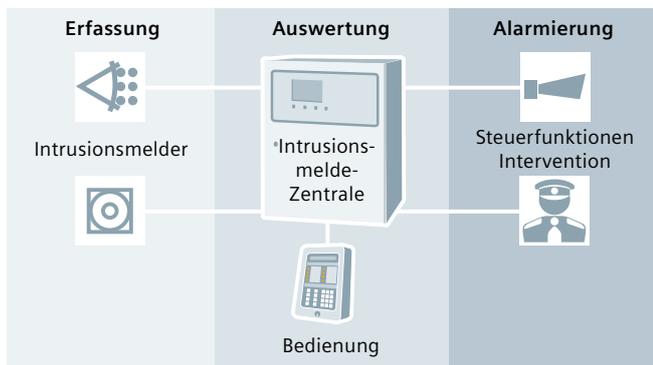


Abb. 4: Aufbau von Intrusionsmeldeanlagen

**Erfassung**

Automatische Melder setzen physikalische Kenngrößen in elektrische Signale um. Sie überwachen so umgrenzende Bereiche, Räume, Durchgangswegen und Objekte. Manuelle Melder dienen anwesenden Personen zur unverzüglichen Alarm- und Interventionsauslösung. Die Melder sind mit der Intrusionsmeldezentrale verbunden.

**Auswertung**

Die Intrusionsmeldezentrale ist das Gehirn der Anlage. Moderne Zentralen verfügen über eine Vielzahl von Parametrier- und Programmiermöglichkeiten um Benutzer, Bereiche, Zeitprofile Eingangsbeschaltungen sowie das Verhalten von Ein- und Ausgängen zu programmieren. Intrusionsmeldezentralen enthalten meistens auch integrierte Fernübermittlungssysteme und kommunizieren gleichzeitig mit Benutzern via Bedienteile, PC oder APPs sowie mit übergeordneten Managementsystemen, Remote-Service-Zentren und Alarmempfangszentralen.

Die Festlegung all dieser Parameter ist zentraler Bestandteil des Anlagenengineering.

**Alarmierung/Steuerfunktionen**

Die Alarmierung wird (intern, extern, örtlich, fern) durch die Intrusionsmeldezentrale gesteuert. Bei Bedarf erfolgt ein Anschluss an eine übergeordnete Managementebene (Leitsystem) oder der lokale Verbund mit anderen Subsystemen wie Zutrittskontrollsystemen oder Videoüberwachungsanlagen, die untereinander interoperabel sind.

**Die Meldelinie**

Die Meldelinie verbindet die Melder mit der Zentrale. Es können zwei Arten von Meldelinien unterschieden werden, nämlich «kollektive» Meldelinien und «adressierbare» Meldelinien.

**Kollektive Meldelinie**

An einer kollektiven Meldelinie (physikalische Verbindung) sind in der Regel mehrere Melder angeschlossen. Es ist nur eine Standortanzeige pro Meldelinie möglich. Das Erkennen der einzelnen Meldestandorte respektive eines einzelnen Melders ist nicht möglich, es sei denn, die Meldelinie enthält nur einen einzigen Melder.

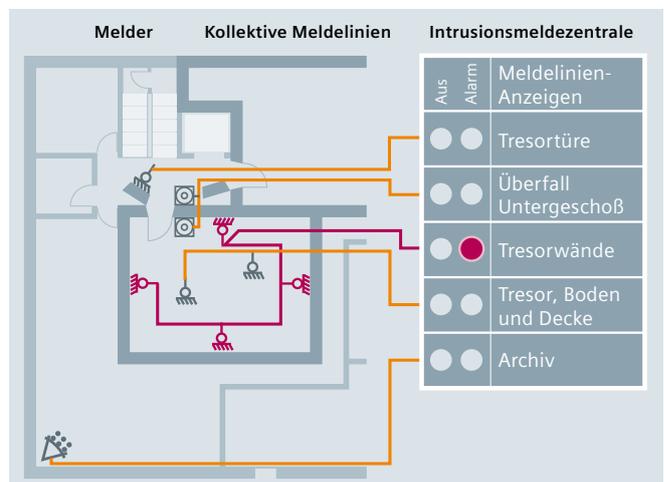


Abb. 5: Prinzip der kollektiven Meldelinie

## Adressierbare Meldelinie

Die adressierbare Meldelinie erlaubt für die angeschlossenen Melder die Anzeige der einzelnen Melder-Standorte. Die einzelnen Melder werden über Busmodule oder auch Adressierelemente an die Melderlinie angeschlossen. Bei diversen Meldern sind die Busmodule bereits integriert.

Die Meldelinie ist in der Regel als Vierdraht-Leitung ausgeführt, wobei zwei Drähte der Übermittlung der Daten zur Zentrale dienen und die restlichen zwei Drähte für die Stromversorgung elektronischer Melder benötigt werden. Dies ist notwendig, da insbesondere Intrusionsmeldesysteme einen höheren Stromverbrauch aufweisen als z. B. die Meldelinie einer Brandmeldeanlage.

Adressiersysteme erlauben den Datenverkehr in zwei Richtungen, d. h. es können sowohl (mehrere) Zustände vom Melder zur Zentrale, als auch Steuerbefehle von der Zentrale zum Melder übermittelt werden. Wird pro Adresse nur ein Melder angeschlossen, spricht man von Einzeladressierung. Werden pro Adresse mehrere Melder angeschlossen, so haben diese eine gemeinsame Standortbezeichnung.

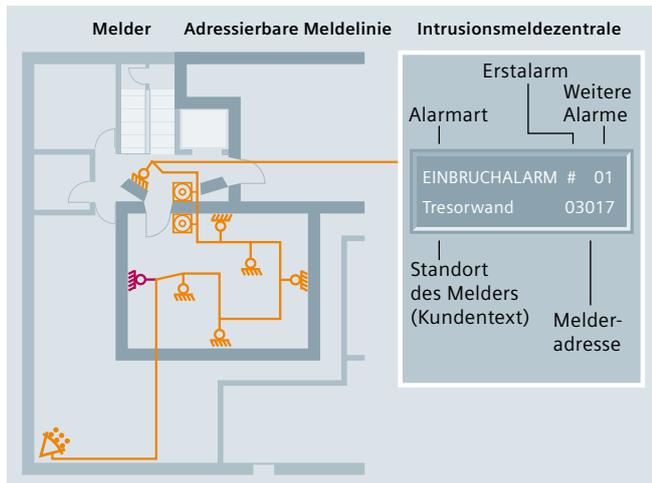


Abb. 6: Prinzip der adressierbaren Meldelinie

## Sabotagesicherheit

Die Sabotagesicherheit ist eine unabdingbare Grundforderung an jede Intrusionsmeldeanlage. Die dazu erforderlichen Maßnahmen umfassen die fachgerechte Anordnung von Geräten und Leitungen, sowie eine lückenlose Sabotageüberwachung der Melder, Leitungen, Zentrale, Bedienungs-, Alarmierungs- und Übermittlungsgeräte.

Geräte und Leitungen einer Intrusionsmeldeanlage sind nach Möglichkeit (Zentralen, Anschluss- und Verteildosen) im geschützten Bereich anzuordnen. Leitungen außerhalb des geschützten Bereiches sind durch besondere Maßnahmen (Verlegung im Unterputz oder im Panzerrohr) gegen unbefugten Zugriff zu schützen. Zusätzlich müssen durch eine dauernde Sabotageüberwachung aller Geräte und Leitungen sämtliche unerlaubten Eingriffs- und Manipulationsversuche erkannt und gemeldet werden.

## Vertraulichkeit

Mit dem Erwerb einer Intrusionsmeldeanlage erwartet der Kunde angemessene Sicherheit. Die Gewährleistung dieser Sicherheit macht es notwendig, Unberechtigten jeden Zugriff zu vertraulichen Informationen zu verwehren. In diesem Sinne erfordert Intrusionsschutz im gesamten Tätigkeitsbereich (Planung, Projektierung, Realisierung) ein ausgeprägtes Sicherheitsdenken. Die dafür notwendige Verhaltensweise ist durch laufende Schulung im Bewusstsein der Beteiligten zu verankern.

Die Wahrung der Vertraulichkeit im Umgang mit Akten und Dokumenten, wie auch im mündlichen Verkehr mit Drittpersonen, muss eine Selbstverständlichkeit sein.

## Vertraulichkeiten von Akten und Dokumenten

Als vertraulich sind alle Akten und Dokumente zu behandeln, die Rückschlüsse auf betroffene Gebäude, Schutzmaßnahmen (Geräte, Funktionen, Installationen) sowie Organisationen (Personen, Abläufe) ermöglichen. Es sind dies z. B.:

- Pflichtenhefte, Submissionen, Angebote, Rechnungen
- Pläne, Schemata, Skizzen, Programmierunterlagen
- Apparatelisten, Gerätebeschreibungen, Anleitungen
- Sicherheitsdispositive (Alarmierung/Intervention)
- Notizen

Solche Akten und Dokumente sind grundsätzlich unter Verschluss zu halten. Sie sollen nie ohne Aufsicht offen liegen. Sie dürfen nur an dafür bestimmte Personen weitergegeben und nur in kontrollierbaren Mengen vervielfältigt werden.

Unbefugte suchen den Zugriff zu Informationen oft über «Schwachstellen», die unbewusst in täglichen Abläufen entstehen können, wie:

- Offene Büros
- Papierkörbe
- Baustellen
- Dienstfahrzeuge
- Versandwege (elektronisch oder physikalisch)
- Kopien
- Gesprächsaufzeichnungen
- Dateien
- Internetdatenverkehr

## Vertraulichkeit im mündlichen Verkehr

Vom Sicherheitsdenken geleitete Diskretion muss eine Selbstverständlichkeit sein. Dies bedeutet im Einzelnen:

- Auskünfte (auch telefonische) nur an identifizierte und zuständige Personen erteilen
- Auskünfte auf das Notwendigste beschränken
- Auskünfte über Anlagen nur im Einverständnis des betreffenden Kunden erteilen
- Nicht in der Öffentlichkeit über Anlagen diskutieren

## Normen und Anforderungen

### Normen für Intrusionsmeldeanlagen

#### Grundlagen Österreich

Für Österreich gelten Grundsätzlich die EN Richtlinien für Alarm-, Einbruch- und Überfallmeldeanlagen. In verschiedenen Anforderungspunkten können die Europäischen Normen EN 50131 die in Österreich bis anhin geltenden Anforderungen an z. B. an Bedienung, Sabotageüberwachung, Alarmierung nur teilweise oder gar nicht erfüllen. Damit das bisher in Österreich geltende Sicherheitsniveau gewährleistet werden kann, wurde vom VSÖ Verband der Sicherheitsunternehmen Österreichs die „TRVE 31-7 und ÖVE Richtlinie R2 Technische Richtlinie Einbruch- und Überfallmeldeanlagen“ erlassen, die zum einen Lücken schließt und zum anderen die Qualitätssicherung gewährleistet. Die österreichischen Richtlinien beinhalten die österreichischen Anforderungen an die technische Ausführung von Einbruch- und Überfallmeldeanlagen. Diese basieren grundsätzlich auf der Europäischen Normenreihe EN 50131:

#### ■ Alarmanlagen- Einbruch- und Überfallmeldeanlagen

- EN 50131-1: Systemanforderung
- EN 50131-2: Einbruchmelder
- EN 50131-3: Melderzentrale
- EN 50131-4: Signalgeber
- EN 50131-5: Verbindungseinrichtungen
- EN 50131-6: Energieversorgungen
- EN 50131-7: Anwendungsregeln
- EN 50131-8: Sicherheitsnebelgeräte
- EN 50136: Fernalarmierung
- EN 54-4: Energieversorgung für Brandmeldeanlagen\*

\*Bei Anlagen mit mehreren Systemen (wie Brand- und Einbruchmeldeanlagen) und mit gemeinsamem Fernübermittlungsgerät, das wegen Sabotageschutzgründen in der Intrusionanlage installiert wird, muss das Netzteil der Intrusionsmeldeanlage auch die EN-Norm 54-4 erfüllen.

### Anforderungen an Intrusionsmeldeanlagen

Zur Wahrung weiterer anwendungsorientierter Interessen und zur Sicherung der Funktionstüchtigkeit im Allgemeinen werden Vorschriften auch von verschiedenen Stellen erlassen, wie z. B.:

- Versicherungen
- Polizei
- Kunden (Banken, Industrie etc.)
- Verbänden

### Prüf- und Zulassungsstellen für Intrusionsmeldeanlagen

Es sind dies auf nationaler Ebene tätige Organisationen. Sie erlassen eigene Richtlinien für Intrusionsmeldeprodukte und -anlagen. Zudem überwachen sie in speziellen Prüfverfahren die Einhaltung ihrer Richtlinien und der in Betracht fallenden Normen und erteilen bei erfüllter Qualifikation Anerkennung und Zulassung für ihren Geltungsbereich.

## Das Projekt

### Projektierungsrichtlinien

#### Produktespezifische Projektierungsrichtlinien

Herausgeber sind vorwiegend die Produkthersteller. Diese Richtlinien sollen sicherstellen, dass ein Produkt seinen Leistungsmerkmalen entsprechend eingesetzt wird.

#### Allgemeingültige Projektierungsrichtlinien

Herausgeber sind Genehmigungsbehörden bzw. Versicherungsorganisationen sowie staatliche Institutionen. Diese Richtlinien enthalten zumeist generelle Regeln für den Einsatz von Intrusionsmeldeprodukten.

#### Anwendungsorientierte Projektierungsrichtlinien

Herausgeber sind Anlagenbaufirmen, Kunden (z. B. Banken, Industrie), Produkthersteller, staatliche Institutionen (z. B. Polizei etc.) und Versicherungen.

Diese Richtlinien behandeln anwendungsspezifische Anliegen und stehen zumeist in Verbindung zu Branchen (z. B. Banken, Museen), besonderen Risiken (z. B. IT-Anlagen), Umfeldbedingungen (z. B. Kraftwerke, Sendeanlagen) und öffentlichen Interessen (Bevölkerung).

#### Projekttablauf

Ein Intrusionsschutz-Projekt enthält mehrere Teilaufgaben, die fachgerecht zu lösen sind. Ein methodisches Vorgehen sichert einen effizienten Projekttablauf:



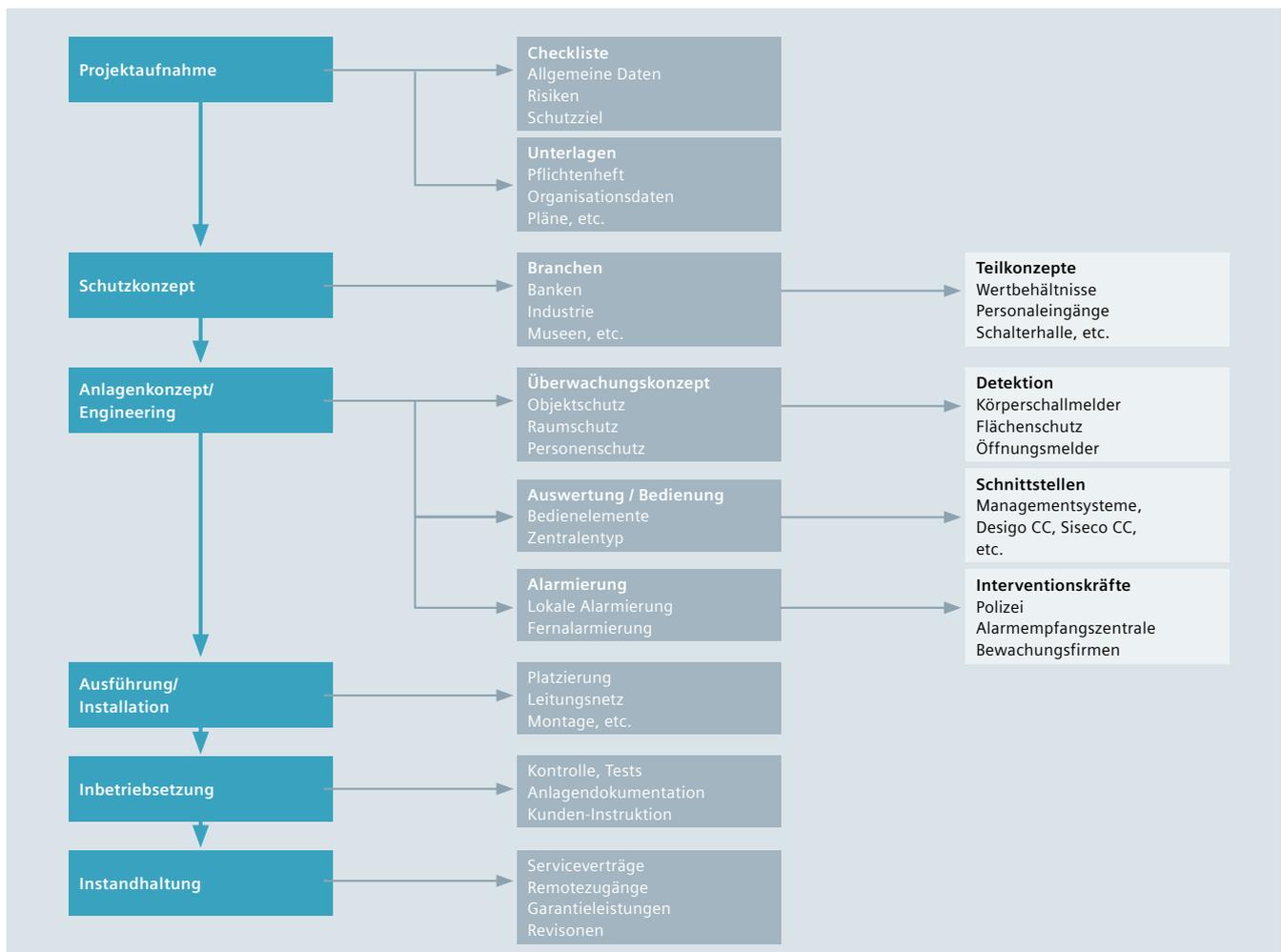


Abb. 7: Projektablauf

## Detektionsprinzipien

Intrusionmelder können – abgesehen von den physikalischen Unterschieden der Detektionsprinzipien – auf zwei grundsätzlich verschiedene Arten arbeiten, nämlich «passiv» oder «aktiv».

### Passive Meldersysteme

Diese arbeiten als reine «Empfänger». Ein passiver Melder kann mithilfe eines geeigneten Sensors das Auftreten oder Verändern bestimmter physikalischer Werte wahrnehmen und als «Alarmsituation» erkennen. Die normalerweise (keine Bedrohung) im Wahrnehmungsbereich des Sensors vorherrschenden physikalischen Grundwerte bilden den Bezugspunkt für die Alarmerkennung. Je stabiler diese Grundwerte sind, desto geringer ist die Gefahr von Täuschungsalarmen. Wegen den zumeist schwachen Nutzsignalen werden in der Regel hohe Ansprüche an die Auswertung gestellt. Umgebungsbedingte Veränderungen werden durch Filterung und zum Teil auch durch Nachführen der Ansprechempfindlichkeit berücksichtigt.

Beispiele passiver Meldersysteme:

- Passiv-Infrarot-Bewegungsmelder
- Körperschallmelder
- Vibrationsmelder
- Bilderüberwachung
- Glasbruchmelder

- Akustikmelder
- Kontaktmelder

### Aktive Meldersysteme

Diese arbeiten mit «Sender» und «Empfänger». Ein aktives Meldersystem besteht aus einem Sendeteil, der in einer elektronischen Schaltung ein definiertes Signal generiert und aussendet, und einem Empfangsteil, der das ausgesendete Signal empfängt, überwacht und Veränderungen als «Alarmsituation» erkennt. Aktive Meldersysteme haben aufgrund der zusätzlichen Parameter aus dem Vergleich des gesendeten mit dem empfangenen Signal gute Alarmerkennungseigenschaften und bieten zusätzliche Möglichkeiten zur Vermeidung von Täuschungsalarmen. Umgebungsbedingte Störeinflüsse werden durch Filter eliminiert. Sender und Empfänger können im gleichen oder je in einem separaten Gerät sein.

Beispiele aktiver Meldersysteme:

- Ultraschallmelder
- Lichtschranken
- Mikrowellenmelder
- Feldänderungsmelder
- Kapazitive Melder

Körperschallmelder

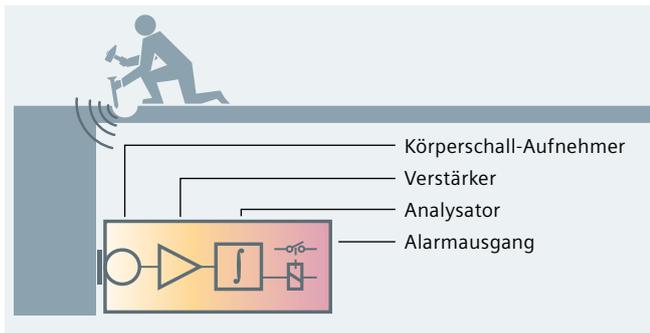


Abb. 8: Prinzip eines Körperschallmelders

Durch die Einwirkung von Einbruchwerkzeugen auf feste Werkstoffe entstehen mechanische Schwingungen, die sich als «Körperschall» im Werkstoff ausbreiten. Der Körperschall wird durch einen eng mit dem Werkstoff verbundenen, zumeist piezoelektrischen Sensor aufgenommen und in einer elektronischen Schaltung analysiert und zur Alarmauslösung ausgewertet. Körperschallmelder arbeiten als passive Systeme. Sie erkennen eine Alarmsituation aufgrund der Kriterien «Amplitude», «Frequenz» und «Zeitdauer» des detektierten Signals.

Körperschall kann nur auf kompakten Baustoffen wie Stahl, Beton usw. erfolgreich detektiert werden. Gedämpft wird der Körperschall, insbesondere seine hohen Frequenzen, in jedem Material. Richtig eingesetzt, detektieren gute Körperschallmelder alle Werkstoff zerstörenden Angriffsmethoden auf Wände, Decken, Böden und Türen von Tresoren, Panzerschränken und Ähnlichem.

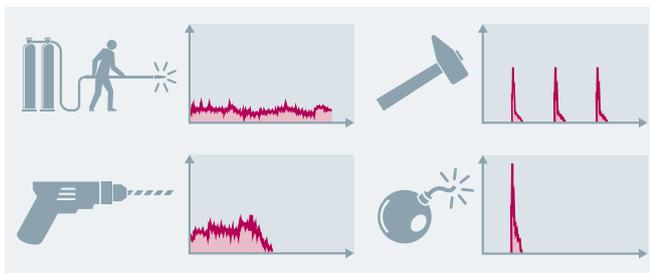


Abb. 9: Körperschallschwingungen typischer Einbruchwerkzeuge

Glasbruchmelder

Beim Einschlagen von Glasscheiben entstehen Vibrationen, die sich als mechanische Schwingungen im Glas fortpflanzen. Der Sensor des Melders empfängt diese Schwingungen und wandelt sie in elektrische Signale um. Die Melderelektronik verstärkt die für brechendes Glas typischen Frequenzen und wertet die so aufbereiteten Signale zur Alarmauslösung aus.

Man unterscheidet bei der Überwachung von Glasflächen verschiedene Detektionsprinzipien:

- Passive Glasbruchmelder
- Akustische Glasbruchmelder
- Aktive Glasbruchmelder

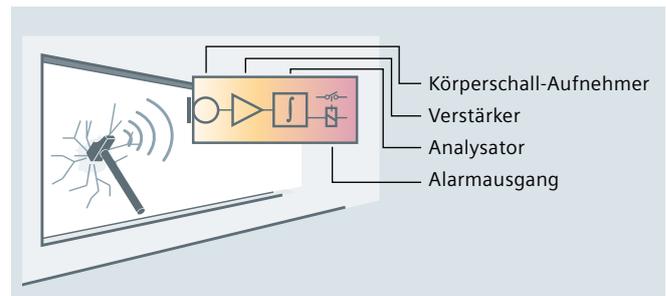


Abb. 10: Prinzip eines passiven Glasbruchmelders

Passive und akustische Glasbruchmelder erkennen eine Alarmsituation (Glasbruch) aufgrund der Kriterien «Amplitude», «Frequenz» und «Zeitdauer» des detektierten Signals. Die für Glasbruch typischen Frequenzen liegen im Bereich von 0,1 bis 1 Megahertz (MHz). Glasbruchmelder eignen sich für die Überwachung aller gebräuchlichen Glasarten wie:

- Kristallglas
- Isolierglas
- Securitglas
- Opalglas (Milchglas, Opal-Übergangsglas)

Bei Glas mit größeren Dämpfungswerten wie z. B.

- Mehrschichtglas (Verbund- und Panzerglas),
- Mit Splitter- oder Sonnenschutzfolie oder Plakaten beklebtes Glas

eignen sich Alarmgläser oder eingebaute Alarmschlaufen mit Vorspannung im Glas.

Glasbruchmelder eignen sich nicht zur Überwachung von Kunststoffscheiben. Bei Kunststoffglas oder Glas mit Drahteinlagen mit unebener Oberfläche werden vorzugsweise Vibrationsmelder eingesetzt, die niederfrequente Angriffsgereusche detektieren.

Alarmglas

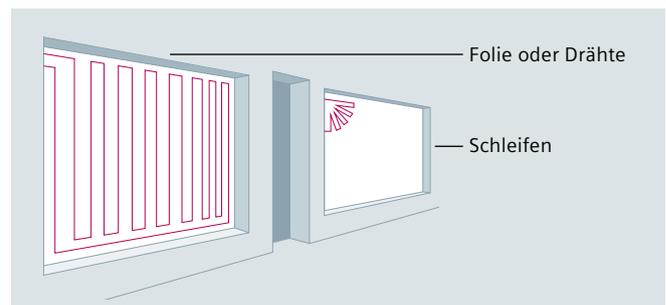


Abb. 11: Prinzip Alarmglas

Alarmgläser sind Glasscheiben, die mithilfe feinsten, elektrischer Leiter auf Durchbruch überwacht werden. Die Leiter bilden einen Ruhestromkreis, der bei Glasbruch unterbrochen wird. Die elektrischen Leiter können als Drähte in der Scheibe eingelegt, als Folie auf der Scheibe aufgeklebt oder als kleine Schleife in einer Ecke der Scheibe eingebrannt sein.

## Bilderüberwachung

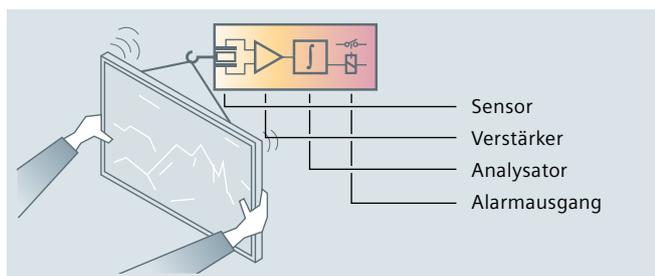


Abb. 12: Prinzip der Bilderüberwachung

Zur Überwachung von Bildern, Gemälden und anderen Kulturgütern kommen verschiedene Detektionsarten zum Einsatz. Es sind dies:

- Piezoelektronische Bildermelder (obiges Beispiel)
- Kapazitive Annäherungssensoren
- Lasermesssysteme
- Optische Distanzmelder
- Kontaktmelder

Obige Grafik beschreibt einen piezoelektronischen Melder, der gleichzeitig als Bildaufhängemechanik genutzt werden kann. Dieses System ist besonders geeignet bei wechselnden Bildausstellungen.

Angriffsversuche auf Bilder (Diebstahl, Beschädigung) bewirken an deren Aufhängevorrichtungen Zug- und Druckveränderungen. Diese werden durch einen mit der Aufhängevorrichtung (Haken) verbundenen Sensor (piezoelektrischer Wandler) aufgenommen und in einer elektronischen Schaltung analysiert und zur Alarmauslösung ausgewertet. Die Bilderüberwachung arbeitet als passives System. Das System erkennt eine Alarmsituation aufgrund der Kriterien «Amplitude» und «Frequenz» des vom Sensor detektierten Signals. Bilderüberwachungssysteme eignen sich für die Überwachung aller an Wänden aufgehängten Gegenstände wie Gemälde, Waffen, Teppiche, Masken usw.

### Passiv-Infrarotmelder

Jeder Gegenstand (Umgebung, z. B. Wände, Möbel) und jeder Körper (Mensch, Tier) strahlt eine von seiner Oberflächentemperatur abhängige Infrarotenergie ab. Im Gegensatz zur ruhenden Umgebung stellen Mensch und Tier sich bewegende Infrarotquellen dar. Alternativ dazu existieren völlig unsichtbare Systeme die bereits beim Annähern an Bilder oder Objekte einen Alarm oder Voralarm auslösen.

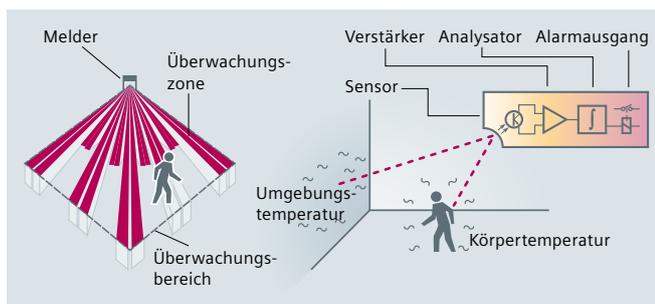


Abb. 13: Prinzip der zonenweisen Überwachung und der Infrarotdetektion

Über eine geeignete Optik wird die im überwachten Bereich vorhandene Infrarotenergie zonenweise einem pyroelektrischen Sensor konzentrisch zugeführt. Dieser misst stetig die eintreffende Infrarotenergie. Durchquert nun ein Körper (z. B. Mensch) eine dieser Zonen, so misst der Sensor die damit verbundene Temperaturänderung.

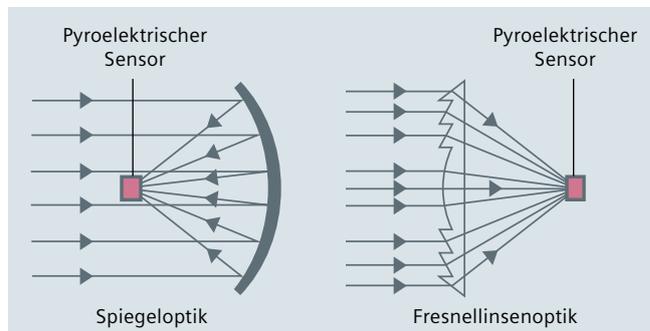


Abb. 14: Prinzip der Spiegeloptik und der Fresnellinsenoptik

Das Änderungssignal wird in einer elektronischen Schaltung analysiert und zur Alarmauslösung ausgewertet. Passiv-Infrarotmelder arbeiten, wie schon der Name sagt, als passive Systeme. Sie erkennen eine Alarmsituation aufgrund der vom Sensor detektierten Temperaturdifferenz und Temperaturänderungsgeschwindigkeit. Für Passiv-Infrarotmelder werden zwei Arten von Optiken eingesetzt, die «Spiegeloptik» und die «Fresnellinsenoptik».

### Spiegeloptische Melder

Bei der Spiegeloptik wird die Infrarotstrahlung über einen Hohlspiegel gesammelt und konzentrisch dem pyroelektrischen Sensor zugeführt. Zur Bildung von Wirkzonen werden mehrere Spiegelsegmente eingesetzt. Bei hochwertigen Meldern sind diese Spiegel exakt gefräst. Dies ergibt exakte optische Detektionszonen, die bereits durch die mechanische Eigenschaft des Spiegels selbst einen schnellen Anstieg des messbaren Signals ergeben. Zudem sind die gefrästen Zonen in den Spiegeln so angepasst und gebogen, dass sich – ähnlich wie bei einem hochwertigen Objektiv für die Fotografie – abgestimmte Nah- und Fernzonen ergeben. Diese erlauben es, den Menschen über den gesamten Detektionsbereich in der optimalen Größe abzubilden.

### Fresneloptik-Melder

Das Fresnell-Prinzip basiert auf der Unterteilung einer Linsenoptik in kleine Teiloptiken, welche die Infrarotstrahlung konzentrisch dem pyroelektrischen Sensor zuführen. Die Bildung von Wirkungsbereichen erfolgt durch spezielle Formung der Teiloptiken und Wölbung der ganzen Linsenoptik. Solche Melder sind einfacher in der Herstellung und deshalb meist auch etwas günstiger in der Anschaffung.

Passiv-Infrarotmelder eignen sich als Bewegungsmelder für einen Teil- und Vollraumschutz und je nach Ausführung auch für die Überwachung im Außenbereich.

### Infrarotschranken

Infrarotschranken bestehen aus Sendern, die unsichtbare Infrarotstrahlen aussenden, und Empfängern, welche die eintreffende Infrarotenergie sammeln und auswerten.

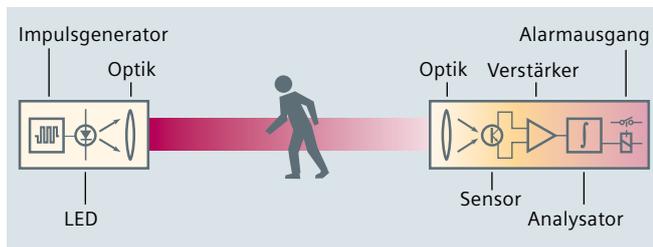


Abb. 15: Prinzip der Infrarotschranke

Im Sender wird die Infrarotenergie von einer lichtemittierenden Diode (LED) ausgestrahlt und über eine Optik gebündelt. Zum Schutz gegen Fremdlicht (Sabotage, Sonne usw.) wird der Infrarotstrahl in der Regel moduliert. Vom Empfänger wird die eintreffende Infrarotenergie über eine Optik dem Sensor, einem Fotohalbleiter, zugeführt. Das vom Sensor detektierte Signal wird in einer elektronischen Schaltung analysiert und zur Alarmauslösung ausgewertet. Infrarotschranken arbeiten als aktive Systeme. Sie erkennen eine Alarmsituation aufgrund der Intensität der empfangenen Infrarotenergie und, bei moduliertem Infrarotstrahl, zusätzlich aufgrund der Impulslänge, Flankensteilheit und Frequenz. Für erhöhte Sicherheit kann zusätzlich die Phasenlage des Signals geprüft werden.

Infrarotschranken eignen sich zur Überwachung von Korridoren, Zwischengängen, Wänden, Fenstern und Türen sowie von anderen engbegrenzten Bereichen.

Besondere Konstruktionen erlauben auch den Einsatz im Freien (Perimeter-Überwachung). Dabei wird die praktisch erzielbare Reichweite durch die am Einsatzort zu erwartende Nebeldichte begrenzt. Es existieren auch Geräte mit «Nebelschaltungen», die bei Nebel die Alarmfunktion unterdrücken und dafür ein separates Signal abgeben.

### Ultraschall-Bewegungsmelder

Der Ultraschall-Bewegungsmelder besteht aus einem Sender, der über einen elektroakustischen Wandler kontinuierlich Schallwellen im unhörbaren Frequenzbereich abstrahlt, und einem Empfänger, der über ein Mikrofon die von der Umgebung reflektierte Schallenergie aufnimmt, auf Frequenzänderung analysiert und zur Alarmauslösung auswertet.

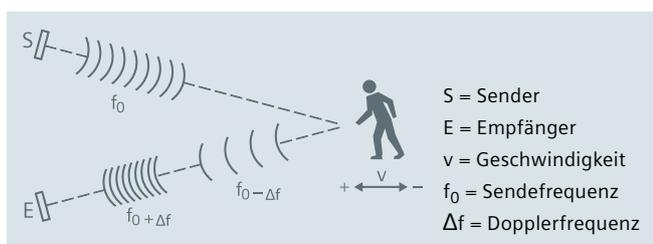


Abb. 16: Prinzip Ultraschall-Bewegungsmelder

Frequenzänderungen werden verursacht durch Körper, die sich im Schallfeld bewegen (Mensch, Tier, Gegenstand). Diese Frequenzänderung wird «Dopplerfrequenz» genannt und ist proportional zur Bewegungsgeschwindigkeit, die in radialer Richtung zum Melder gemessen wird. Die wirksame Geschwindigkeitskomponente und damit die Frequenzänderung ist somit am größten bei Bewegung auf den Melder zu oder davon weg, und wird umso kleiner, je mehr sich die Bewegungsrichtung einem Kreisbogen um den Melder annähert.

Ultraschall-Bewegungsmelder arbeiten als aktive Systeme. Sie eignen sich für den Vollraumschutz beliebig großer Innenräume sowie auch für dessen Teilraumschutz.

### Dual-Bewegungsmelder (IR/US)

Dual-Bewegungsmelder kombinieren die Eigenschaften von zwei physikalischen Meldern. Solche Melder sind besonders robust und falschalamsicher. Im Beispiel mit einem Ultraschall- und einem Passiv-Infrarot-Teil wird dank raffinierter, digitaler Signalverarbeitung und Systemverknüpfung eine sichere Erkennung von Eindringlingen gewährleistet. Dabei werden beide Teilsysteme einer komplexen Mehrkriterien-Analyse unterworfen und Störungseinflüsse in den einzelnen Teilsystemen erkannt und unterdrückt.

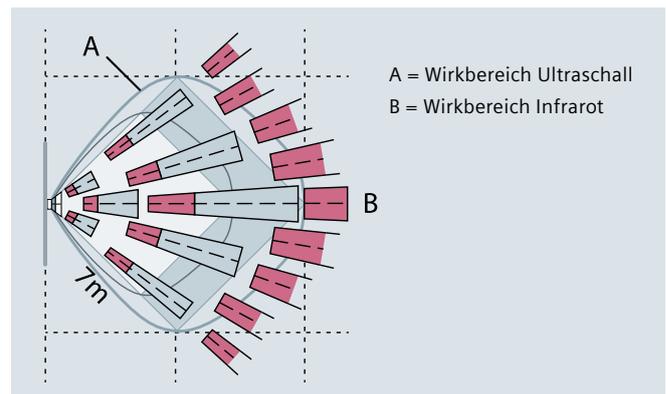


Abb. 17: Zonen eines Dual-Bewegungsmelders mit Infrarot- und Ultraschallsystem

### Dual-Bewegungsmelder (IR/MW)

Der Mikrowellenmelder-Teil in diesen Meldern funktioniert wie der vorher beschriebene Ultraschall-Bewegungsmelder nach dem Prinzip des Dopplereffektes. Der Mikrowellen-Bewegungsmelder arbeitet jedoch mit Hochfrequenzwellen im Bereich von 9 bis 11 Gigahertz (GHz).

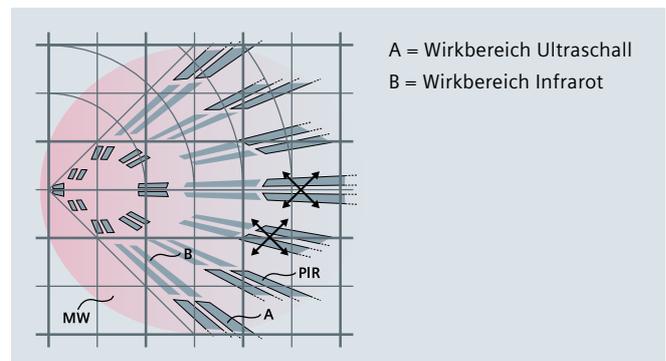


Abb. 18: Zonen eines Dual-Bewegungsmelders mit Infrarot- und Mikrowellenmelder

## Intrusion / Einbruchschutz

Die Pfeilrichtung in Abb. 18 markiert die für den InfrarotTeil optimale Bewegungsrichtung. Beim Einsatz von Mikrowellen-Bewegungsmeldern ist zu beachten, dass die Hochfrequenzwellen gewisse Baustoffe (z. B. dünne Wände, Glas oder Holz) durchdringen (Falschalarm-Risiko).

Beim Einsatz solcher Melder, die in der Anschaffung etwas teurer sind, rechtfertigt der Zweck die Mittel. Hierbei müssen nicht immer Anwendungen mit hohen Risiken im Vordergrund stehen, sondern ebenso z. B. Anwendungen im Retailbereich. In Ladengeschäften stellen teils Störeinflüsse wie Deckenhänger oder auch offene, arbeitende Kühltruhen, die thermische Störungen verursachen können, höhere Anforderungen an die Melder.

Kombiniert mit beispielsweise langen Anfahrtswegen für die Intervention oder dem Wartungspersonal ist ein Einsatz solcher Melder auch in einer solchen Anwendung durchaus sinnvoll und angebracht.

### Mikrowellen-Schranke

Die Mikrowellen-Schranke besteht aus einer getrennten Sendeeinheit und Empfangseinheit, zwischen denen ein elektromagnetisches Feld im 10-GHz-Bereich aufgebaut wird. Körper, die sich in diesem Feld bewegen, bewirken eine Feldänderung, die im Empfänger analysiert und zur Alarmauslösung ausgewertet wird. Die Detektionssicherheit der Mikrowellen-Schranke wird durch Umwelteinflüsse wie Nebel, Regen oder Schnee kaum beeinträchtigt. Sie eignet sich deshalb für Perimeter-Überwachung. Mikrowellen-Schranken arbeiten als aktive Systeme.

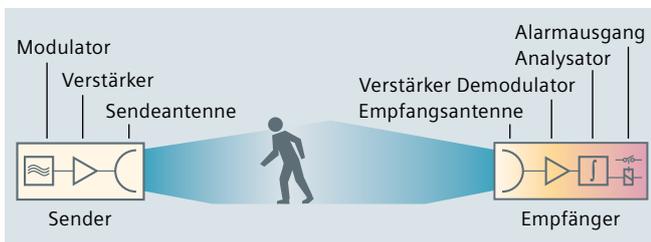


Abb. 19: Prinzip der Mikrowellen-Schranke

### Leckkabel-System

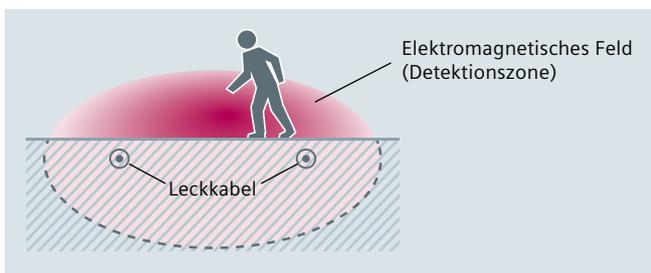


Abb. 20: Prinzip der Detektion mittels Leckkabel

Dieses besteht aus zwei im Boden verlegten speziellen Koaxialkabeln, die in ihren Abschirmungen definierte Öffnungen, sogenannte «Leckstellen» aufweisen. Das eine der beiden Kabel arbeitet als Sende-, das andere als Empfangskabel. Das Sendekabel wird mit einem 40-MHz-Signal gespeist. Über die «Leckstellen» baut sich entlang des Kabels in dessen Nahbereich ein elektromagnetisches Feld auf. Gelangt ein Körper in dieses Feld, z. B. eine Person, ändert sich dieses Feld bzw. die Kopplung zum Empfangskabel. Dadurch ändert sich das beim Empfänger anliegende Signal, was zu einer Alarmauslösung führt. Leckkabel arbeiten als aktive Systeme. Sie werden zur Freilandsicherung eingesetzt.

### Vibrationsmelder

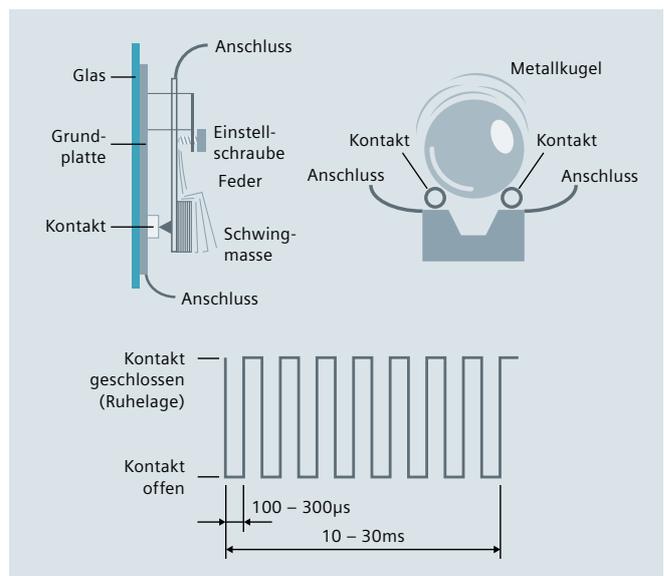


Abb. 21: Prinzip des mechanischen Vibrationsmelders

### Mechanische Vibrationsmelder

Der Vibrationsmelder detektiert Gewalteinwirkungen bei Einbruchversuchen anhand der dabei auftretenden Erschütterungen. Die Erschütterungen versetzen eine Schwingmasse im Melder in Bewegung, sodass ein elektrischer Kontakt im Rhythmus der Schwingungen öffnet und schließt und dadurch Alarm auslöst. Die von den Erschütterungen typischerweise erzeugten Kontaktbewegungen haben extrem kurze Signale zur Folge. Vibrationsmelder können deshalb nicht direkt, sondern nur über eine elektronische Auswerteeinheit an die Alarমেingänge von Zentralen oder Adressierelementen angeschlossen werden.

### Elektronische Vibrationsmelder

Heute sind mehrheitlich elektronische Vibrationsmelder im Einsatz. Diese nehmen den Körperschall mit einem mit dem Werkstoff verbundenen, zumeist piezoelektrischen Sensor auf. Die Signale werden in einer elektronischen Schaltung analysiert und so zur Alarmauslösung ausgewertet. Die Melder eignen sich zur Objekt- und Peripherie-Überwachung von Glasscheiben (min. 6 mm dick), Glasbausteinen, beklebten oder bestrichenen Glasflächen, Mehrschichtglas, etc. oder je nach vorgängigem Test auch für andere Werkstoffe.

## Magnetkontakte

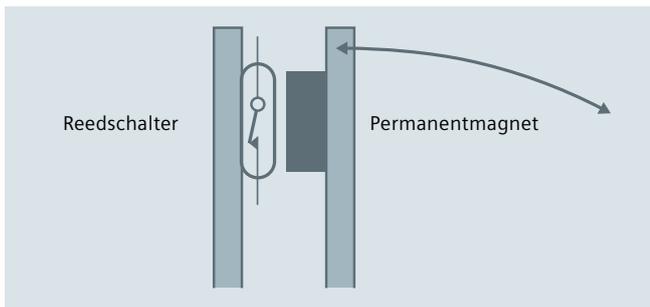


Abb. 22: Prinzip des Magnetkontaktes

Der Magnetkontakt besteht aus den beiden Einheiten «Reedschalter» und «Magnet». Diese werden so an der zu überwachenden Einrichtung angebracht, dass sie in Ruheposition (kein Alarm) dicht beieinander liegen. In dieser Position ist der Reedschalter durch die Wirkung des Magnetfeldes geschlossen. Bewegt sich der Magnet vom Reedschalter weg, so verringert sich der Einfluss des Magnetfeldes rasch, bis schließlich der Reedschalter öffnet und dadurch Alarm auslöst. Magnetkontakte arbeiten als passive Systeme und melden das Öffnen von Türen, Fenstern, Drehtüren, Rolltoren, Apparategehäusen, Schubladen, etc.

## Überwachungskontakte

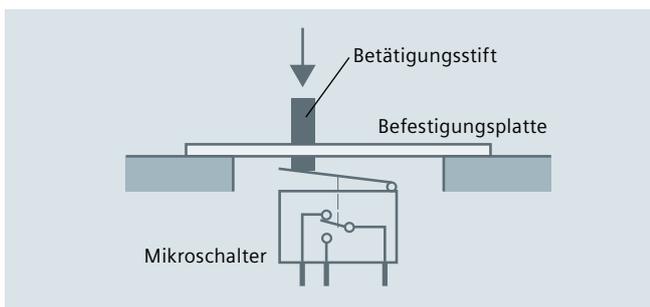


Abb. 23: Prinzip des Überwachungskontaktes

Der Überwachungskontakt besteht zur Hauptsache aus einem Mikroschalter, der mit konstruktiven Ergänzungen für den Einsatz in Intrusionsmeldeanlagen optimiert ist. Der Überwachungskontakt wird so an der zu überwachenden Einrichtung angebracht, dass in der Position «kein Alarm» der Betätigungsstift gedrückt ist. Überwachungskontakte sind passive Melder, die das Öffnen von Türen, Fenstern, Schränken, Apparategehäusen und Ähnlichem melden. Sie eignen sich insbesondere auch zur Überwachung der Riegelstellung in Schließkontrollanlagen.

## Flächenschutz

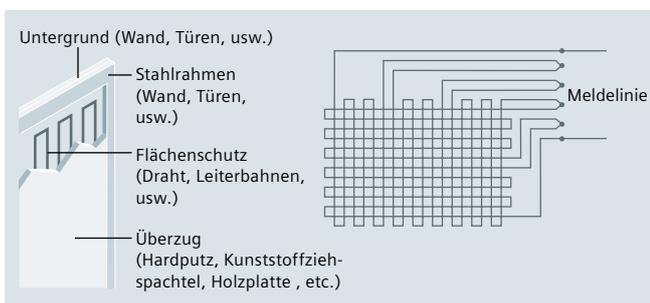


Abb. 24: Prinzip des Flächenschutzes

Der Flächenschutz besteht im Wesentlichen aus elektrischen Leitungen, die als Schleifen oder Netz die zu überwachende Fläche bedecken. Die Leitungen bilden einen Ruhestromkreis, der beim Durchbrechen der überwachten Fläche unterbrochen wird und dadurch Alarm auslöst. Der Flächenschutz eignet sich zur Überwachung von Wänden, Türen, Apparategehäusen, usw. und wird auf Beton, Stahl, Ziegelmauerwerk, Holz, etc. angewendet.

## Manuelle Melder/Alarmtaster



Abb. 25: Prinzip des Alarmtasters

Alarmtaster dienen der manuellen Alarmauslösung. Durch Drücken des Tasters wird ein elektrischer Kontakt betätigt und damit ein Alarm ausgelöst. Alarmtaster werden eingesetzt, um bei Bedrohung durch Überfall Alarm und/oder Kameras auszulösen.

## Fußkontaktschienen

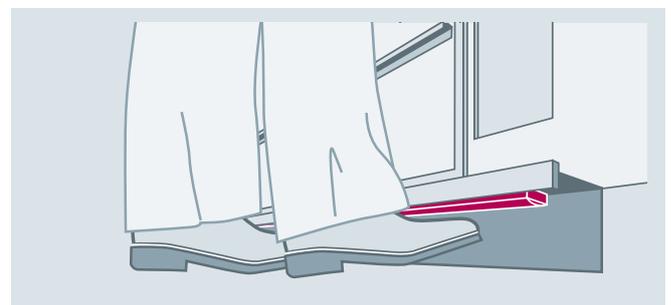


Abb. 26: Prinzip der Fußkontaktschiene

Fußkontaktschienen ermöglichen die fußbetätigte Alarmauslösung. Die Fußkontaktschiene besteht aus einem etwa 60 cm langen Betätigungselement (Pedal), das in einem ebenso langen Gehäuse beweglich gelagert ist. Der eingebaute elektrische Kontakt löst Alarm aus, wenn das Pedal an einer beliebigen Stelle gedrückt wird. Fußkontaktschienen werden an Schalterkorpussen, Ladentischen, Büropulten und ähnlichen Einrichtungen angebracht. Sie eignen sich zur unauffälligen Alarmauslösung bei akuter Bedrohung durch Überfall und auch zur Auslösung von Kameras.

## Drahtlose manuelle Meldesysteme

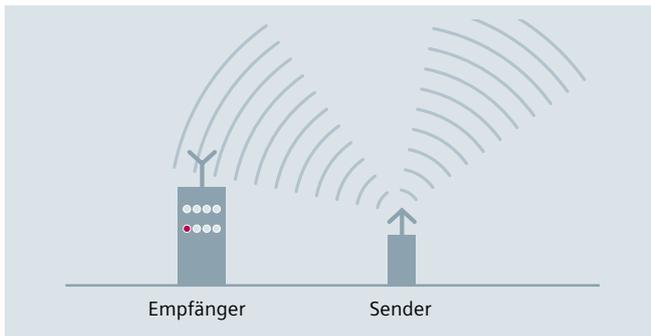


Abb. 27: Prinzip des drahtlosen Meldesystems

Drahtlose Meldesysteme erlauben die Alarmauslösung über eine Funkverbindung. Das Funksignal wird an einem persönlich mitgeführten Sender ausgelöst und von diesem ausgestrahlt. Ein zentral angeordneter Empfänger wertet die Funksignale zur Alarmauslösung aus. Drahtlose Meldesysteme werden zum Schutz des Wachpersonals, Werkschutzdienste, und Ähnlichem eingesetzt. Es können mehrere Sender an einem Empfänger betrieben werden. Die Sender werden manuell oder durch Lageveränderung (Totmann) ausgelöst.

## Betrieb und Instandhaltung

Damit die Intrusionsmeldeanlage ihren Schutzwert dauernd behält, ist sie durch regelmäßige Kontrollen und Unterhaltsarbeiten funktionsfähig zu halten.

Dies erleichtern spezielle Prüf- und Messgeräte, wie:

- Prüfsoftware zur Überwachung von Betriebsabläufen
- Testmodi und automatische Tests in der Einbruchmeldezentrale
- Multimeter für Pegel-Überwachungen
- Logik-Tester
- Linien- und Punktschreiber
- Anlagen-Testgeräte z. B. in Form von Smartphones zur Überprüfung der einzelnen Melder und deren korrekte Funktion
- Wartungsgeräte, passend zu den verschiedenen Meldersystemen

Ein Betriebsbuch vermittelt Informationen über die Betriebsbereitschaft der Intrusionsmeldeanlage. In dieses sind durch den Anlagen-Betreiber einzutragen:

- Einbruchmeldungen
- Überfallmeldungen
- Störungsmeldungen
- Abschaltungen
- Sonstige Betriebsereignisse

Durch die Mitarbeitenden des Anlagen-Erstellers sind einzutragen:

- Instandhaltungsereignisse wie Inspektionen, Wartungen, Instandsetzungen

Es ist zweckmäßig, zwischen Anlagenbetreiber und Ersteller bzw. Hersteller der Intrusionsmeldeanlage ein Instandhaltungsvertrag (Wartungsvertrag) abzuschließen:

- Damit wird die dauernde Funktionsbereitschaft der Intrusionsmeldeanlage sichergestellt.
- Revisions- und Kontrollintervalle sind definiert.
- Bedingungen über Störungsbehebungen außerhalb und während der Arbeitszeit (Pikett-Dienst) sind definiert.
- Die statistische Erfassung und Auswertung aller Ereignisse ermöglichen dem Hersteller und Ersteller der Intrusionsmeldeanlagen, die Apparate und deren Anwendung weiter zu optimieren.



Abb. 28: Betriebsbuch und Instandhaltungsvertrag

Smart Infrastructure verbindet auf intelligente Weise Energiesysteme, Gebäude und Industrien, um die Art, wie wir leben und arbeiten, weiterzuentwickeln und zu verbessern.

Gemeinsam mit unseren Kunden und Partnern schaffen wir ein Ökosystem, das intuitiv auf die Bedürfnisse der Menschen reagiert und Kunden dabei unterstützt, Ressourcen optimal zu nutzen.

Ein Ökosystem, das unseren Kunden hilft zu wachsen, das den Fortschritt von Gemeinschaften fördert und eine nachhaltige Entwicklung begünstigt.

**Creating environments that care.**  
[siemens.at/smart-infrastructure](https://www.siemens.at/smart-infrastructure)

**Siemens AG Österreich**

Smart Infrastructure  
Gebäudelösungen & Services  
Siemensstraße 90  
1210 Wien  
Österreich  
Tel +43 (0) 5 1707-32300

[gebäude.at@siemens.com](mailto:gebäude.at@siemens.com)

**AREA Vienna**

Siemensstraße 90  
1210 Wien  
Tel +43 (0) 5 1707-32383

Werner-von-Siemens-Straße 1  
3100 St.Pölten  
Tel +43 (0) 5 1707-32541

Marktstraße 3  
7000 Eisenstadt  
Tel +43 (0) 5 1707-32383

**AREA Linz**

Wolfgang-Pauli-Straße 2  
4020 Linz  
Tel +43 (0) 5 1707-65571

Werner-von-Siemens-Platz 1  
5021 Salzburg  
Tel +43 (0) 5 1707-66800

**AREA Graz**

Strassganger Straße 315  
8054 Graz  
Tel +43 (0) 5 1707-63322

Werner-von-Siemens-Park 1  
9020 Klagenfurt  
Tel +43 (0) 5 1707-64353

**AREA Bregenz**

Josef-Huter-Straße 6  
6901 Bregenz  
Tel +43 (0) 5 1707-68254

Werner-von-Siemens-Straße 9  
6020 Innsbruck  
Tel +43 (0) 5 1707-67316

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

© Siemens 2019