



INTRUSION DETECTION

New EN Guidelines for Intrusion Detectors

European Standards Assure High, Consistent Quality Standards

A new single set of European standards for electronic intrusion detection systems was introduced several years ago aimed at unifying and improving existing national standards. The result of this initiative is a set of regulations that manufacturers, distributors, installers and end users must all follow. Moreover, countries without clear guidelines or with no guidelines at all will be able to benefit from a clear set of European standards outlining specification levels and requirements for security products. The standards will also enable end users to compare similar products, services and systems.

For several years, the market has benefited from a set of European guidelines (EN50131) relating to electronic intrusion detection systems. These guidelines document the standards that devices must fulfill in order to achieve specific security grades numbered from 1 to 4. The grades relate to security requirements that must be met by the different systems in order to combat various risks, as well as to ensure environmental protection. They range from low-risk (Grade 1), through low-to-medium risk (Grade 2), medium-to-high risk (Grade 3), to high risk (Grade 4). There are also four equipment application grades (from

How detection systems are integrated to achieve immunity levels resulting in exceptionally reliable detection.



indoor to outdoor use). Currently, guidelines exist for intrusion systems, power supplies, warning devices, and wireless elements, as well as for general alarm system requirements. All of these are covered by EN50131.

Specifications for Infrared or Dual Detectors

This article focuses on the two sets of guidelines that exist for the most popular detectors on the security market: EN50131-2-2 for passive infrared detectors and EN50131-2-4, which relates to combined passive infrared and microwave detectors. The aim here is to outline the standards that all manufacturers must adhere to when developing these products. The result of this will be that when the end user buys a grade 3 detector, this device fulfils all necessary requirements, guaranteeing high, consistent quality of the installations using these devices.

What do the Standards Say?

The standards themselves raise some important issues that are worth exploring as they help to explain the differences between the requirements for each detector grade.

Requirements During the General Walk Test

The test includes a series of criteria that must be met, taking into account the speed and position of the object. Grades 2 and 3 are highlighted specifically. The table here shows a series of intrusion detection situations where speed and position are taken into account. The Table shows that there is a series of priority requirements for detectors to comply with Grade 3 (Tab. 1).

Immunity Issues

Section 4.4 of the standard is an important section dealing with intrinsic immunity of individual detector technologies to external influences – specifically the technology's resistance to false alarms. Subsequent sections of the same document refer to tests and specific technical characteristics, which include the following:

Immunity to air currents: An air current blowing in front of the detector must not cause the infrared component to generate any form of intrusion signal or message.

Immunity to radiation visible to the infrared sensor from a source near to it: Radiation that is visible to the infrared sensor from a nearby light source such as a car headlamp must not cause the infrared component to generate any form of intrusion signal or message.

Immunity to interference caused by microwave signals from fluorescent lights: Fluorescent light sources near the sensor must not result in the detector's microwave components generating any form of intrusion signal or message.

Tab. 1: Intrusion detection situations involving the speed and position of the detector

Test	Grade 2	Grade 3
Detection when limit is crossed	Required	Required
Speed (m/s)	1.0	1.0
Position	Vertical	Vertical
Detection within the limit	Required	Required
Speed (m/s)	0.3	0.2
Position	Vertical	Vertical
Detection at high speed	Required	Required
Speed (m/s)	2.0	2.5
Position	Vertical	Vertical
Functional characteristics of proximity detection (dist, m)	2.0	0.5
Speed (m/s)	0.4	0.3
Position	Vertical	Crawling
Functional characteristics of detection with intermittent movement *	Not required	Required
Speed (m/s)	–	1.0
Position	–	Vertical
Effect of control adjustments *	Required	Required
Speed (m/s)	0.3	0.2
Position	Vertical	Vertical
Significant reduction in specified scope	Not required	Not required
Speed (m/s)	–	–
Position	–	–

* See standard EN50131-2-4 (Table 2) for more information

Security Against Tampering

The Table shows the tamper-protection specifications for each detector grade.

Besides the standard functional requirements, electrical requirements exist for both grades (Grade 2 and 3). Required are: Constraints on detector current consumption, constraint on supply voltage interval and slow voltage increase, constraints on supply voltage fluctuation, constraints on sudden change in supply voltage and constraints on total loss of power (Tab. 2).

Standardized Test Subject

The standards also specify a test target (simulating a human being in a real intrusion situation). The height for this target must be between 160 cm and 185 cm, and it must weigh 70 kg (± 10 kg). The target must wear tight-fitting clothing that emits heat over more than 80% of its surface area at wavelengths between 8 µm and 14 µm. No metallic objects may be worn or carried. The average temperature difference between the walk test target and the background must be measured. The temperature must be

Tab. 2: Tamper protection

Specification	Grade 2	Grade 3
Protection against access to inside of detector through existing covers and holes and detection if such access has taken place	Required	Required
Protection against removal of assembly from mounting surface *	Required *	Required
Resistance to reorientation	Required	Required
Applied torque (Nm)	2	5
Immunity to magnetic field interference	Required	Required
Immunity (T)	0.12	0.24
Anti-masking feature	Not required	Required

* Required for wireless detectors only

measured on areas of the test target's body on the surface, and the background temperature must be measured close to each simultaneously measured area. The areas are: 1) head, 2) chest, 3) back of hand, 4) knee and 5) feet.

This demonstrates the importance of the standards in ensuring successful intrusion detection.

Anti-Masking

With regard to the anti-masking feature referred to in the table earlier, section 4.5.5 of the standard indicates that it must be possible to identify if the function of the detector is being hindered by the application of masking material and if the detection area and sensor have been covered while the sensor was in inactive (i.e. disarmed) mode – thereby preventing the detection of movement afterwards. This leads to the following requirements:

- When in the disarmed mode, the detector must be able to generate an anti-masking signal within 180 seconds of the introduction of material being used to mask activity in its field of view.
- Signals or messages must be emitted constantly until the situation is resolved
- When the device is inactive, normal human movement of 1 m/s at a distance of more than 1 m should not cause an anti-masking signal or message to be generated.

Anti-Masking Testing

The detector must always meet the required standards and must be in inactive mode for every test. Any changes in signal or message state must be monitored. There are several anti-mask tests, some so called spray tests are intended to cover the detector lens with an invisible spray material, other anti mask tests are focused on solid material that covers the detector, e.g. a cardboard box.

To carry out the spray test, an aerosol dispenser must be used to spray the materials specified in the following table. Spraying must be intermittent and each spray must be no longer than two seconds. For the transparent varnish test, the material must be applied with one brush stroke. Following each application, the detector should be switched into active mode after 180 s and the basic detection test should be car-

ried out. Applications of the material should be repeated until the detector stops responding or until the anti-masking signal is generated.

The sheet material samples specified in the table are applied directly onto the entire front part of the detector. If necessary, they can be cut to fit the detector window. Next, the samples should be applied again across the front of the detector at a distance of 0 and 50 mm. Two tests must be carried out, one that takes one second to cover the detector lens/window and the other 10 seconds. Self adhesive vinyl is applied directly to the front of the detector. As with the spray-on and brush-on materials, after applying each material, 180 seconds should be allowed to elapse to enable the system to settle down before switching to active mode and monitoring for anti-masking indication indication.

Materials used for masking tests:

Test no.	Material
1	Sheet of black paper
2	2 mm thick sheet of aluminum
3	3 mm thick sheet of acrylic
4	White polystyrene foam sheet
5	Self-adhesive transparent vinyl sheet*
6	Polyurethane spray film*
7	Transparent varnish applied with a brush* *only applied on the front

All the material samples must be large enough to hinder detection.

Pass/fail criteria: within 180 seconds of the device being masked, a signal or message must be emitted to indicate an intrusion or fault and must continue to be generated for as long as the material is in place. Alternatively, both the microwave and PIR technologies must continue to operate normally. If an individual test fails, it must be repeated twice more. Two passes out of the three tests constitutes a passed test.

The Importance of Independent Testing

Recognizing the importance of the new EN50131 standards to their sales in Europe, many manufacturers are making rather enthusiastic claims for their intruder-alarm products based on self evaluation. However, for the new EN50131 standards to gain credibility and become widely accepted throughout the industry, it is essential for products to be certified by independent laboratories and not by the manufacturers themselves. A self declaration of compliance to

EN50131-2-4, for example, provides absolutely no guarantee of product quality or product features.

As in other industries, the certification process must be carried out by a completely independent laboratory. This will ensure that the entire security industry, from the manufacturers, distributors, installers through to the end users, can implicitly trust the quality and function of the standards. Independent certification will also give recognition to the work of system manufacturers' R&D departments as well as the combined efforts of national and European associations to promote the correct implementation of the guidelines. And most important, it will mean that the end user can be confident of receiving a product that meets all the new standard's relevant requirements.

For this reason, many national laboratories such as CNPP in France, VdS in Germany and ANPI in Belgium have already initiated product testing based on the available EN standards and technical specifications.

As a member of the Cenelec committee developing the EN50131 standards, Bosch Security Systems has been a strong supporter of the standard as an important quality label on which installers, distributors and end users can rely. It is also one of the first companies to submit its intrusion alarm products for independent certification. The relevant certificates, issued by CMPP, are published on the Bosch website and the company is making test reports available to potential customers on request to provide a guarantee of product quality based not only on a self declaration but also rigorous testing by an independent organization.

▶ THE AUTHOR

Carlos Alonso
Director Intrusion Detection Systems
Bosch Security Systems

▶ CONTACT

Erika Görg
Bosch GmbH, Ottobrunn, Germany
Tel.: +49 89 6290 1647
Fax: +49 89 6290 281647
emea.securitysystems@bosch.com
www.boschsecurity.com