



Cesit Ingegneria S.P.A.  
[www.cesit.net](http://www.cesit.net)

Special Systems

# Access Control

# The increasing importance of controlling flows of people who have daily access to rooms or areas subject to a high degree of security for various reasons, makes it necessary to adopt identity verification and transit and access control systems. The purpose of access control systems is to manage inbound and outbound flows to and from an area that requires control.

The purpose of access control systems is to manage inbound and outbound flows to and from an area that requires control. They can therefore be sub-units of an overall security system which, in order to en-

sure effective management of emergency procedures, especially in the case of building evacuation, must be coordinated and integrated with the safety procedures

Cesit Ingegneria S.P.A. designs and produces integrated control systems for controlling access points and equipment by means of monitoring devices (closed circuit television cameras, access control terminals, registration number reading systems, etc.). To ensure maximum effectiveness, access control systems must be capable of supervising even the most complex plants, combining advanced functions with ease of use, and fully meeting all the security and reliability requirements of comprehensive, latest-generation systems.

**Our Company designs, installs and maintains access control systems for:**

- **Personal recognition (by means of badges, fingerprints, iris and retina scans, hand geometry, voice, facial geometry, etc.)**
- **Vehicle recognition**
- **Authorisation control (on-line or stand-alone)**
- **Access reporting**

## Biometric Systems

Biometric recognition systems represent the latest state of the art in personal recognition and are based on a number of unique characteristics of the human body:

- **Iris or retina scanning**
- **Fingerprints**
- **Hand geometry**
- **Facial geometry**
- **Voice analysis and recognition**

Thanks to technological consolidation, biometrics has reached a high level of efficiency by focusing attention on the unbeatable aspects of these technologies:

- **biometric data cannot be lost or forgotten**
- **biometric features cannot be stolen**
- **biometric features are not transferable**

## Main functions

Access control systems are divided into three functional macro-blocks:

- **personal recognition**
- **authorisation control**
- **access reporting**

The term “personal recognition” means associating requests for access with the identity of the person requesting such access. Requests can be made using various technologies, which can be divided into two categories: conventional recognition systems (optical, magnetic and proximity badges) and biometric recognition systems (fingerprints, iris or retina scanning, hand geometry, facial geometry).

Authorisation control follows each request for access and consists in checking the level of authorisations associated with the identity of the person requesting access, and granting or denying access accordingly.

**Registration, which fulfils an analytical rather than a direct control function, enables the system to check:**

- **transits, with the possibility of associating each transit with parameters such as the identity of the person who requested transit, the time and the access point**
- **the route taken by any individual within the controlled area**
- **attempted break-ins**