Access Control

Access Control along with **Intrusion Detection** and **Video Surveillance** are considered to be the three main elements of an electronic security system.

Buildings often require some type of controlled access so that only authorized personnel are permitted entrance to the facility. There are a wide variety of systems that can be deployed to secure the facility, from simple magnetic card readers and key pads to more sophisticated biometric methods such as iris and fingerprint scanning technologies.

Types of Access Control:

- **Card reader**
- **Chip cards**
- **Key pads**
- **Finger scanner**
- **Biometrics**

Card readers are the most common types of access control systems. An appropriately programmed card is needed to gain access. The card must be physically swiped through or inserted into the card reader. More sophisticated "chip" cards containing RFID technology simply need to be placed in closed proximity to the card reader in order to release the locked door mechanism. Cards can be programmed so that access can be gained at any time or only during certain hours of the day.

Key pads work in similar fashion, requiring a pre-programmed series of several numbers in order to gain access. Different numbers can be assigned to different personnel, so there will be a record of which personnel entered the facility and at what time. Numbers can be changed from time to time or deleted in the event of employee dismissal. More sophisticated keypad systems allow entrance to only certain areas of a facility and can show which areas of the facility remain un-secure, prompting investigation to see if doors or windows may have been inadvertently left open.

Biometrics is increasingly being used to aid in security measures. Biometrics makes use of the quantifiable human characteristics that are unique to each of us – characteristics such as finger prints or the digital image of the iris portion of a human eye. Companies like Nexus use retinal scan technology as a security measure to allow access to certain areas of an airport. The application process for a Nexus card requires that a digital image of your iris be registered with Nexus. At a Nexus security point, the Nexus card holder is required to look into a device that "reads" your iris to determine if the image captured has been duly registered with Nexus, thereby allowing access.

Fingerprint technology works in a similar way. A digital image of your fingerprint is registered with a security authority. In order to gain access to a secure environment, the person must place a finger on a scanning device to detect their digital finger print image. If the finger print image has been duly registered as an authorized fingerprint, then the area is opened to the authorized person. This type of technology is now being used on computing devices such as laptops in place of previously required passwords that can be more easily circumvented.

If you would like additional information on access control systems and how Fancom can help with your electronic security requirements, please give us a call at 905-990-4845 or send us an email to info@fancomni.com indicating "access control" in the subject line.

FANCOM
Communications Engineering