Advanced Biometric Access Control Training

Course # : 14-4156

Content

A. Objectives – 5 mins
B. History of EAC- 10 mins
C. Electronic Access Control in Todays World – 20 mins
D. Essential Components of Electronic Access Control – 20 mins
E. What are biometrics and how do they enhance security- 20 mins
F. What benefits do they offer that conventional EAC does not-10 mins
G. Break- 20 mins
H. Review biometric devices and relationship to control panels – 20 mins
I. Stand Alone Biometric Readers – 20 mins
J. Address concerns about privacy/encryption in biometric systems – 5 mins
K. Benefits / comparison of IP vs. 485 – 10 mins
L. Comparison client/server application vs. browser based – 10 mins
M. Advanced Biometrics or enhancement to traditional systems.- 10 mins

Objectives

- Give an overview of essential electronic access control (EAC) equipment, concepts and techniques.
- Introduction of Biometric Technologies- Fingerprint , Facial, Voice, Speech, Iris and Retina recognition.
- Use of Biometric technologies in Access Control Solutions
- Integration of IP Cameras with Access Control
- Future of Access Control

History

The practice of installing electronic access control systems began in the 60s to eliminate the problems associated with lost keys. Historically, credentials for authorized access included a plastic access card and/or PIN (personal identification number) code, like an ATM, to gain authorized access to specific areas of a building with specific time zones.

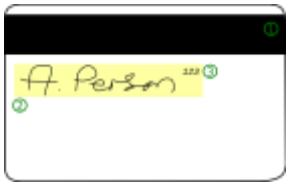
Electronic Access Control (EAC) has been an integral security tool for physical security professionals for over 40 years and provided customers the control to authorize access for:

- Employees
- Contractors
- Suppliers
- Visitors into their facilities

Credentials for authorized access included:

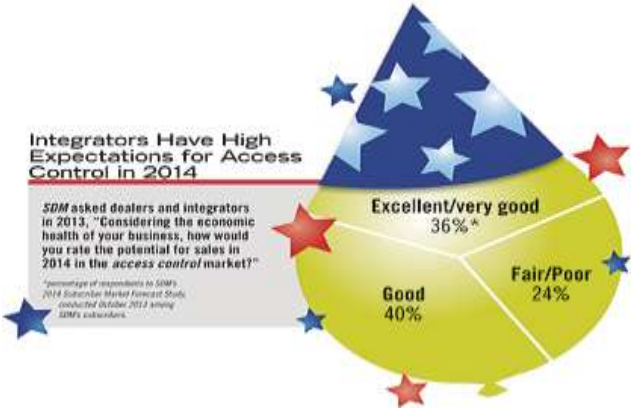
- Keys
- PIN (personal identification number)
- Plastic access card

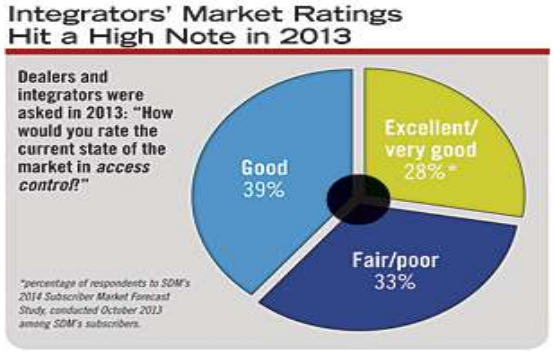
{123555}

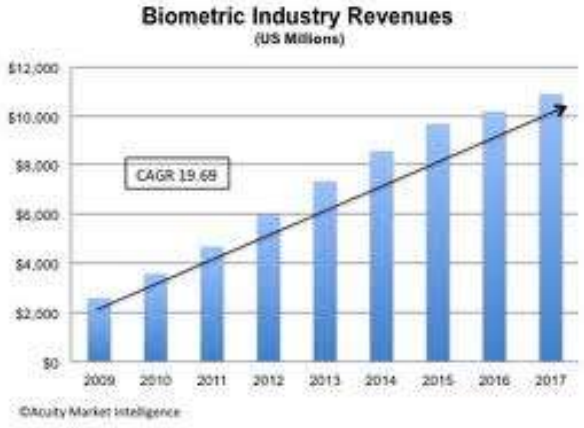


Electronic Access Control in Todays World

In our current economy, no matter what your budget is, companies still have a need to secure and protect their assets. In today's economic climate, businesses are looking for cost effective and reliable methods of securing their facilities and keeping their employees safe by using various locking hardware and accessories.





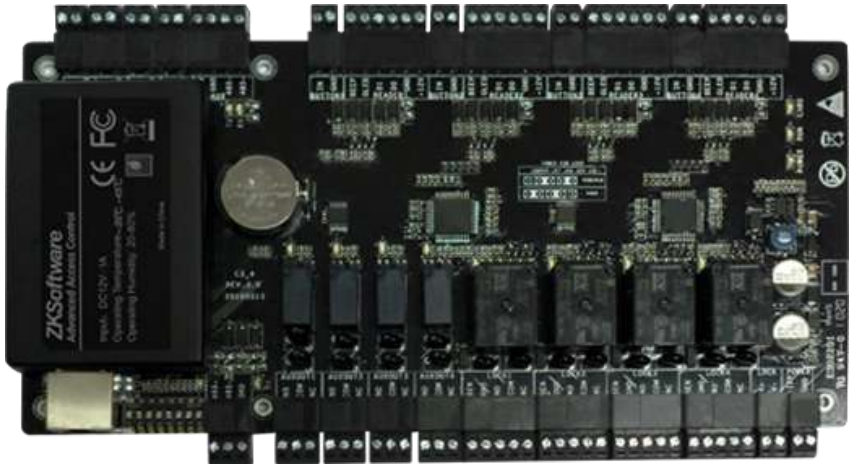


Essential Components of Electronic Access Control

Readers

Locks

Access Control Panel



Request to Exit Devices

Door Contacts

Credentials

Advanced Electronic Access Control of Today

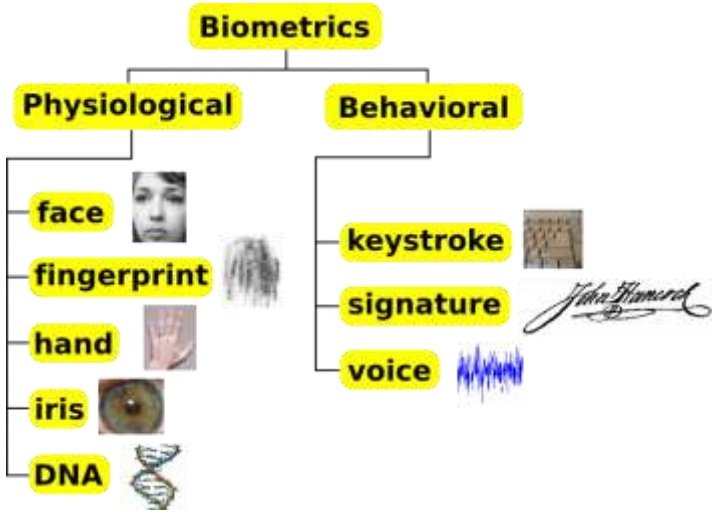
Biometrics combined with IP video technology adds flexibility and enhance traditional Electronic Access Control systems.

What is Biometrics?

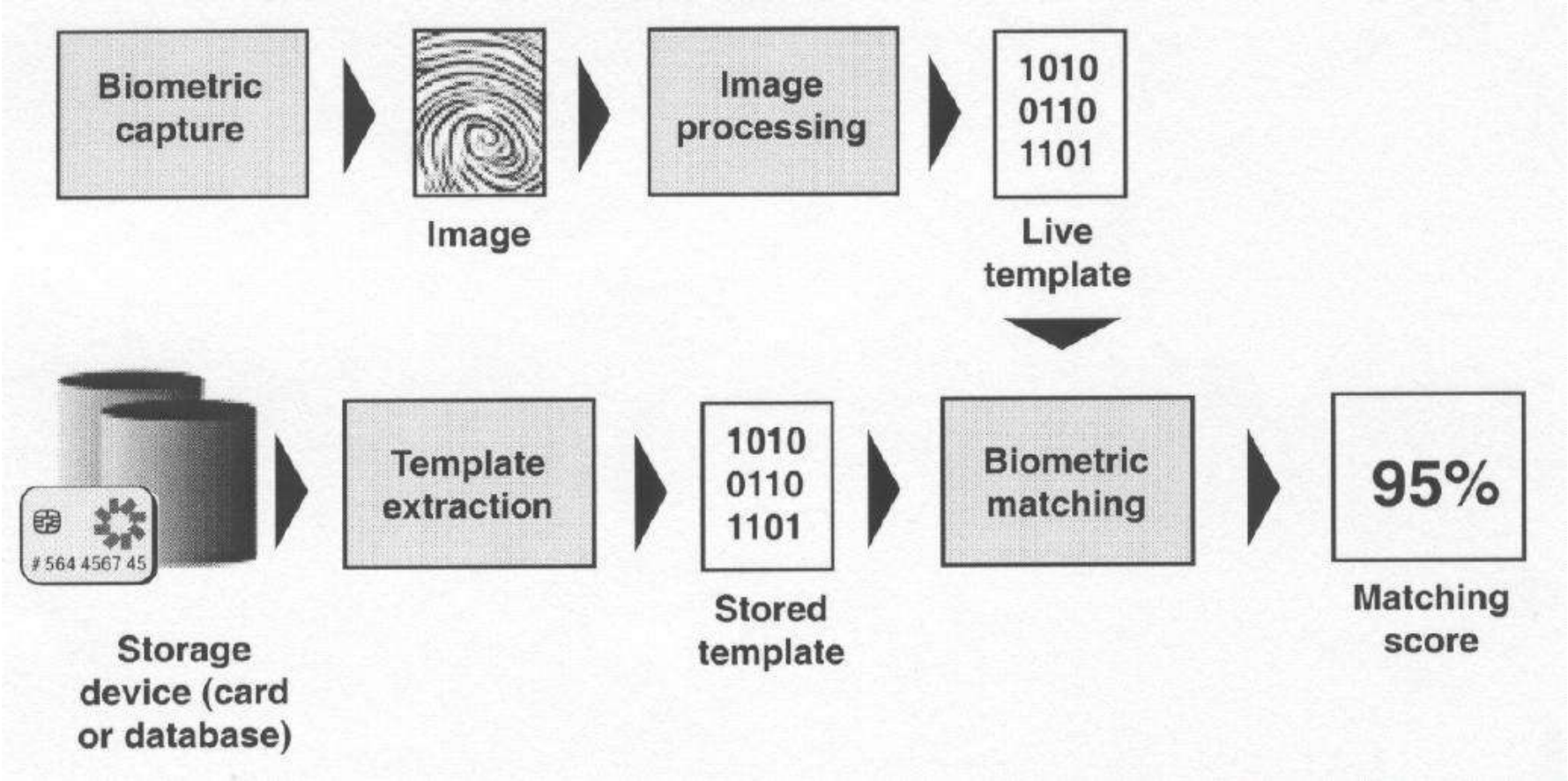
Biometrics refers to technologies that measure and analyze human body characteristics, such as:

- DNA
- Fingerprints
- Eye retinas and irises
- Vein Geometry
- Voice patterns
- Facial patterns

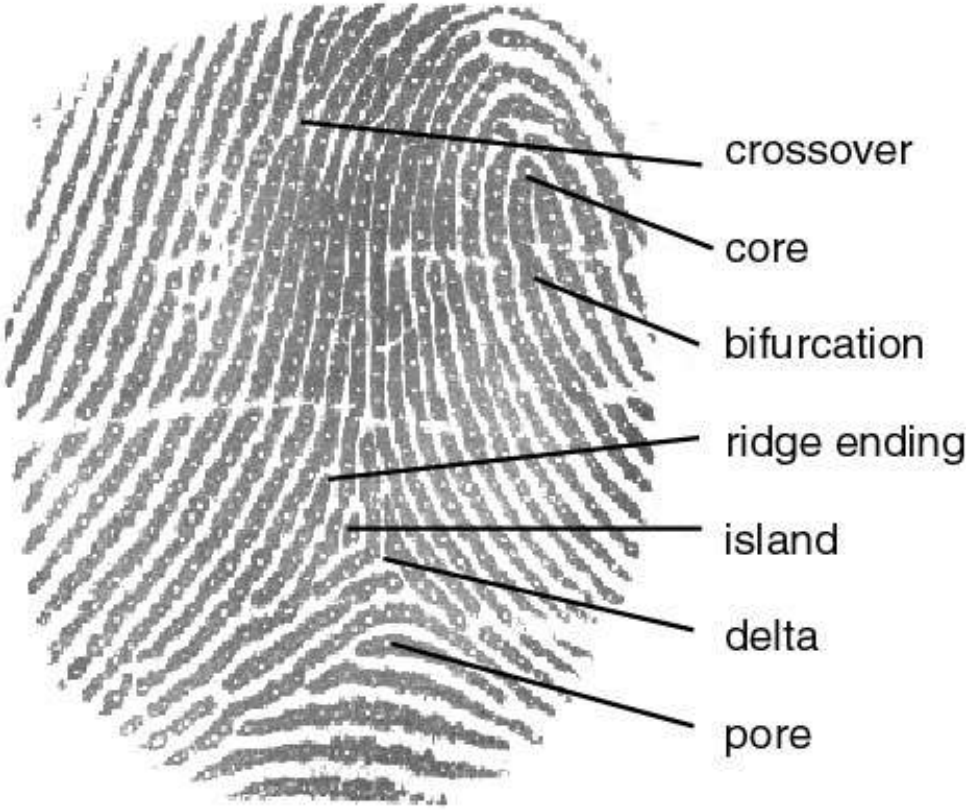
Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods



Enrollment and Recognition Process



Fingerprint



Finger Scanners

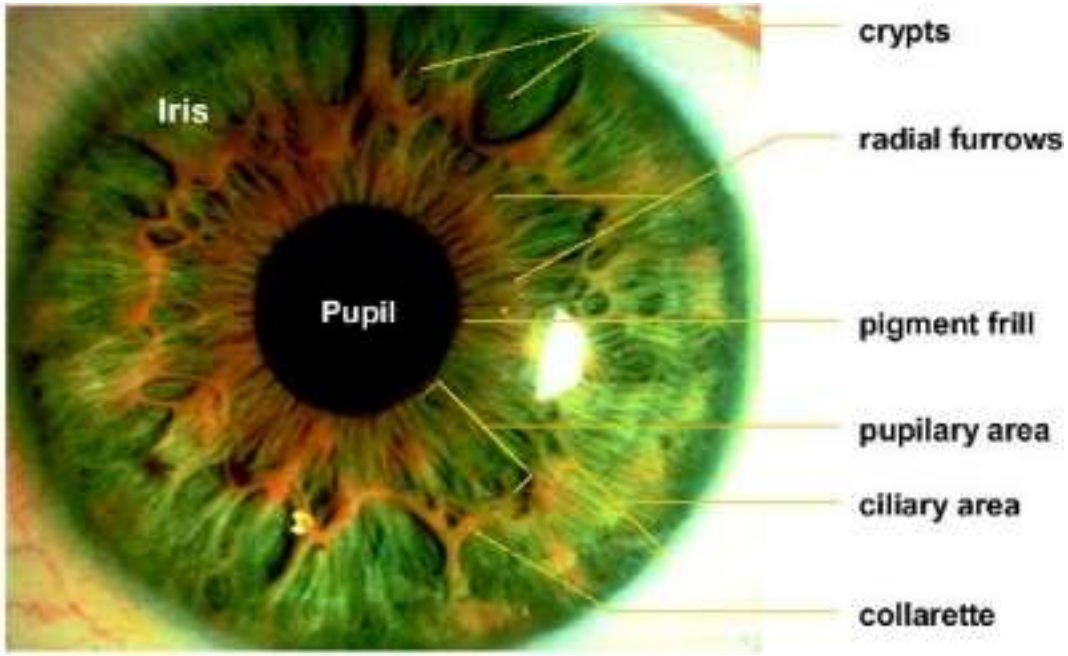
Biometric devices, such as fingerprint scanners, consist of:

A reader or scanning device

Software

Database that stores the biometric data for comparison

Iris and Retina



Iris & Retina Scanners

Biometric devices, such as iris or retina scanners, consist of:

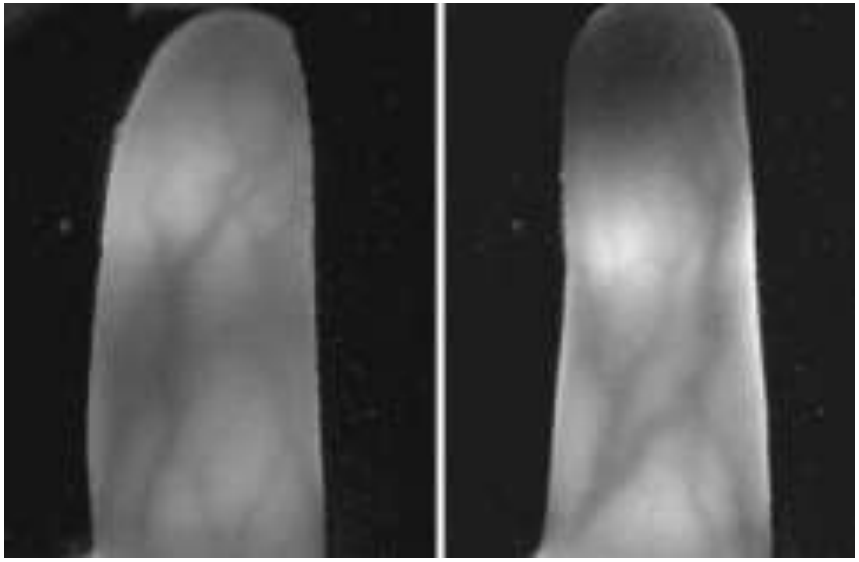
A reader or scanning device

Software

Database that stores the biometric data for comparison

Vein Recognition

Palm Vein



Finger Vein

Palm/Finger Vein Authentication

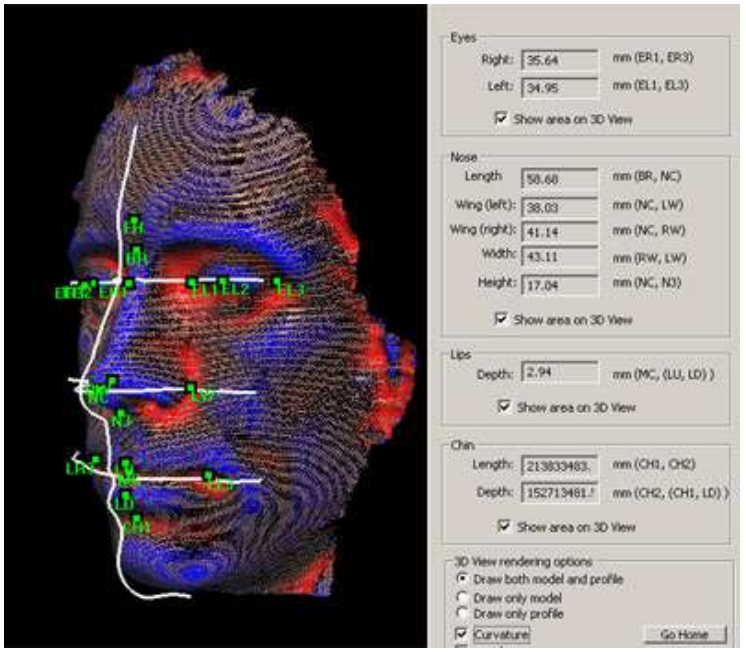
Biometric devices, such as vein scanners, consist of:

A reader or scanning device

Software

Database that stores the biometric data for comparison

Facial Recognition



Facial Recognition Scanners

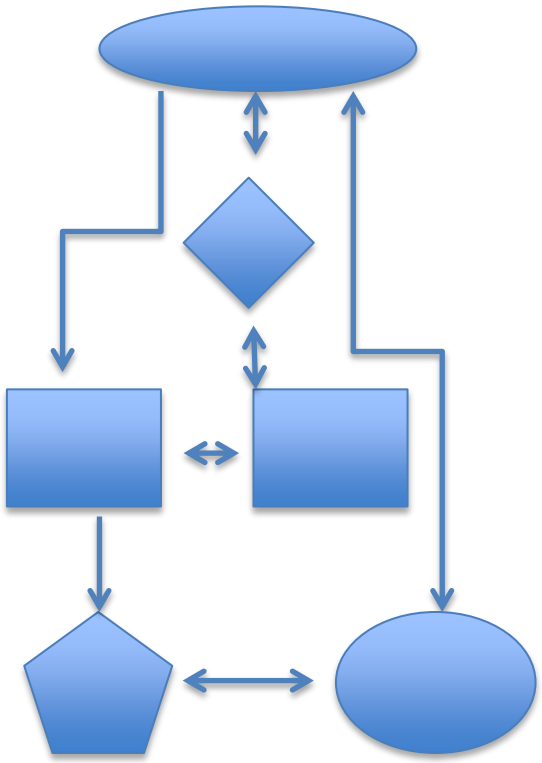
Biometric devices, such as facial recognition scanners, consist of:

A reader or scanning device

Software

Database that stores the biometric data for comparison

Privacy Concerns for Biometric Technology



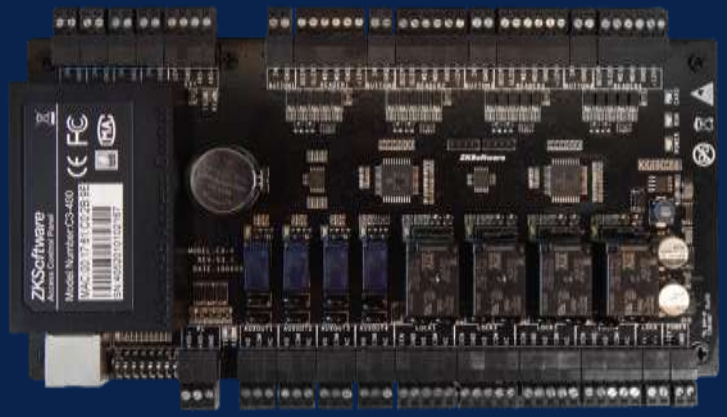
Unlike the technology used by Automated Fingerprint Identification Systems (AFIS) for law enforcement purposes, biometric terminals are designed to not capture and store actual fingerprint images. Instead, it collects only sample data, convert it into binary data using mathematical algorithms and then store only a digital representation of the fingerprint (not an actual fingerprint image), from which it is virtually impossible to recreate the original image.

Biometrics vs Conventional EAC

- ✓ More Secure
- ✓ More Flexible
- ✓ More Cost Effective
- ✓ Easy to Install
- ✓ Easier to Sell
- ✓ High Performance
- ✓ Low TCO for Customer
- ✓ Priced to Win Projects

Biometric Readers and Access Control Panels

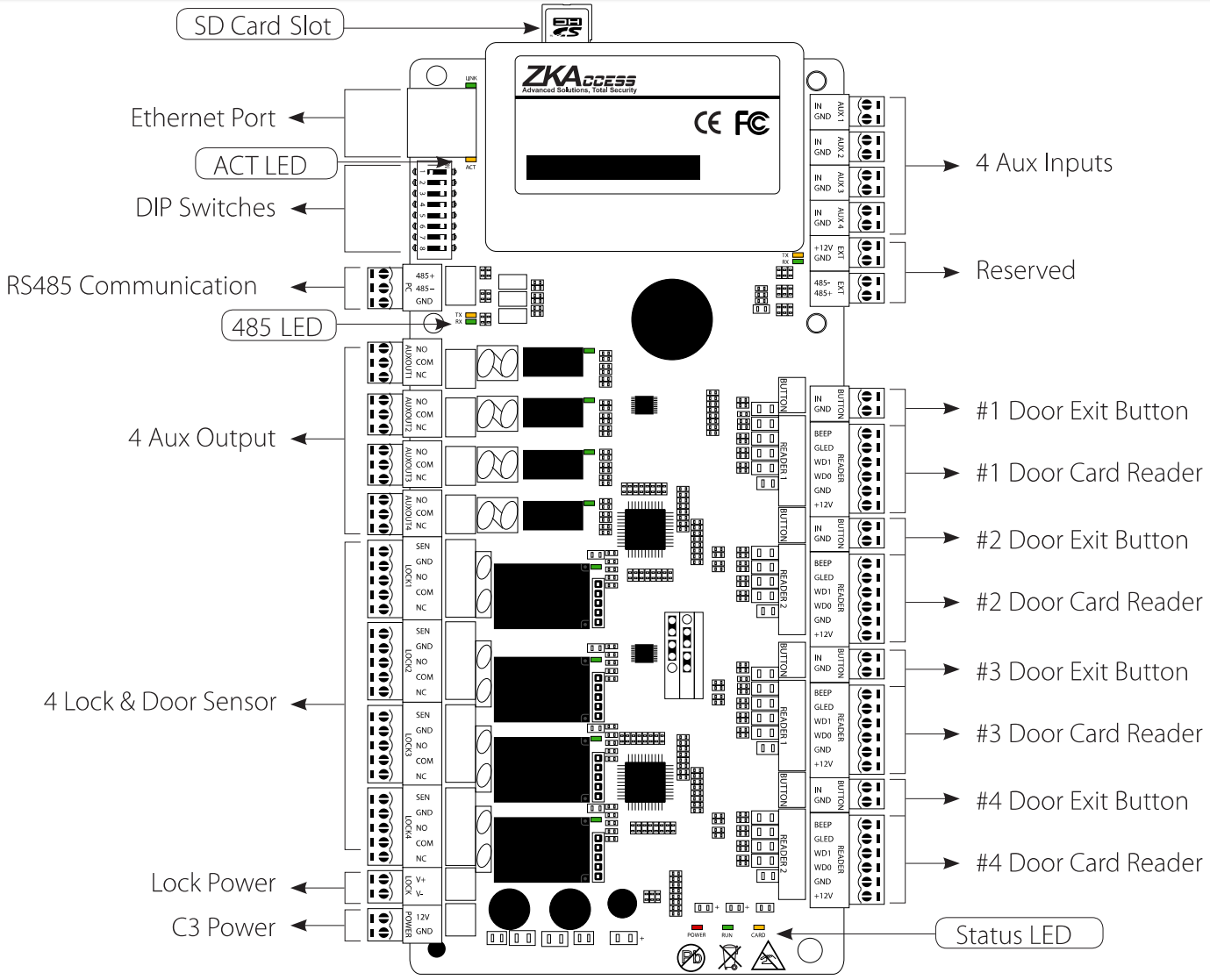
IP Based Access Control Panels



IP Based Access Control Panels

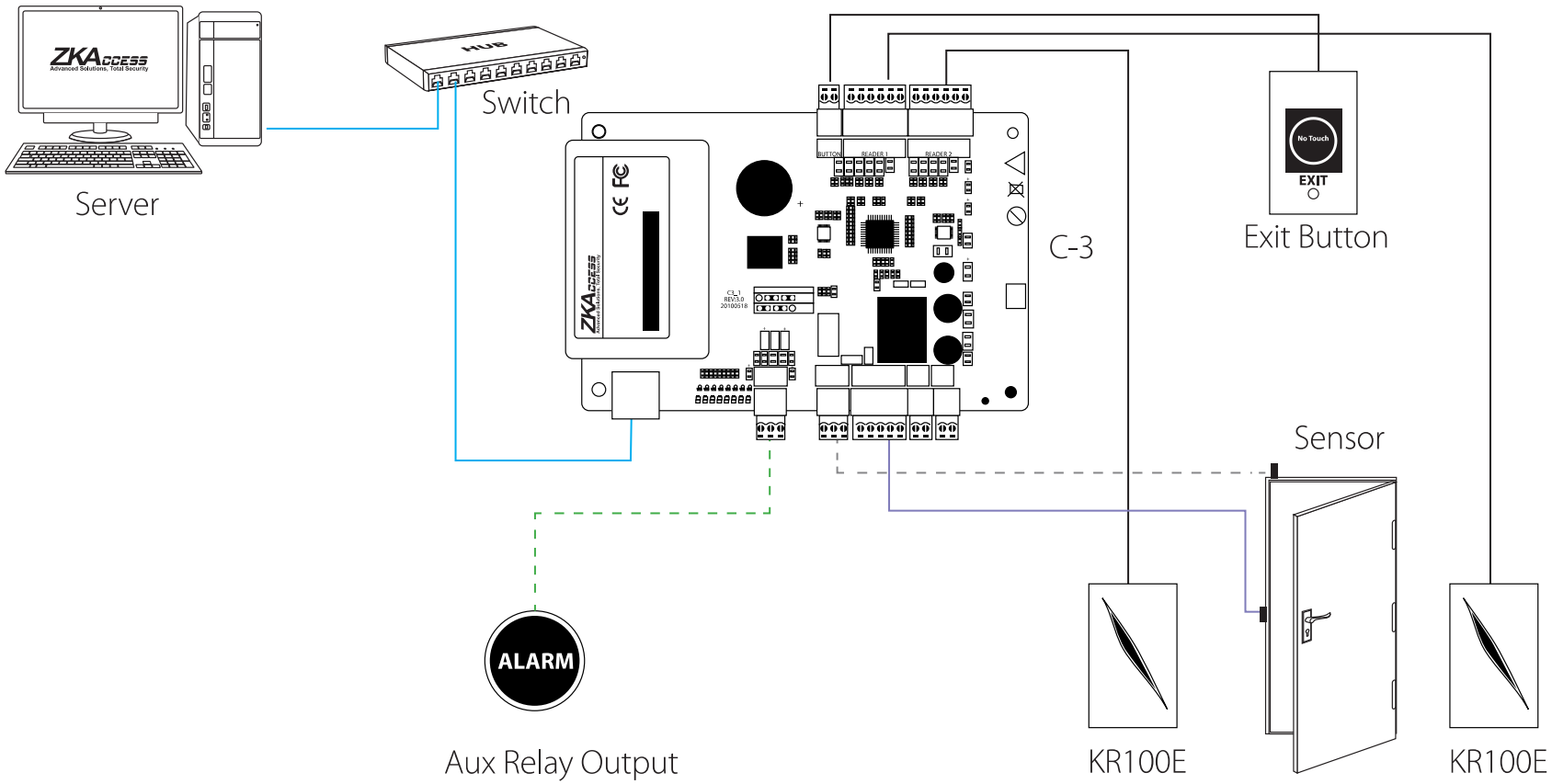
- Easy to install easy to program, saves money
- Flexible design supports many types of readers
- Stores user information and events
- Programmable auxiliary inputs and outputs
- Software to manage the panels and users

IP Based Access Control Panel



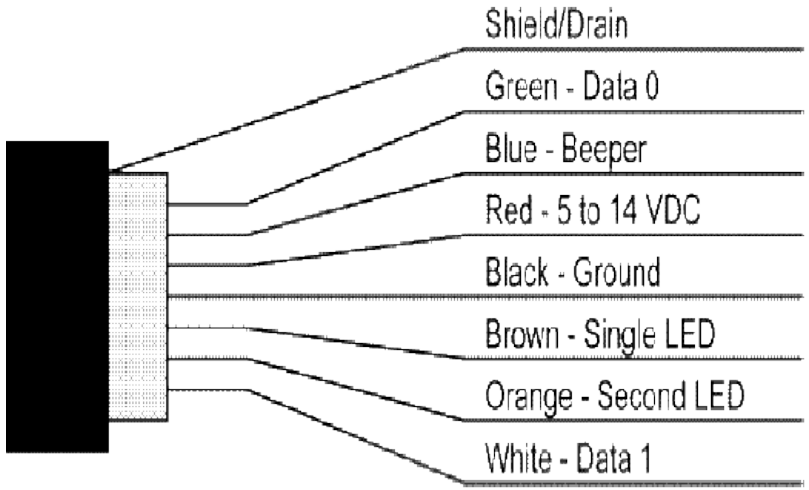
Access Control Panel with RFID card readers

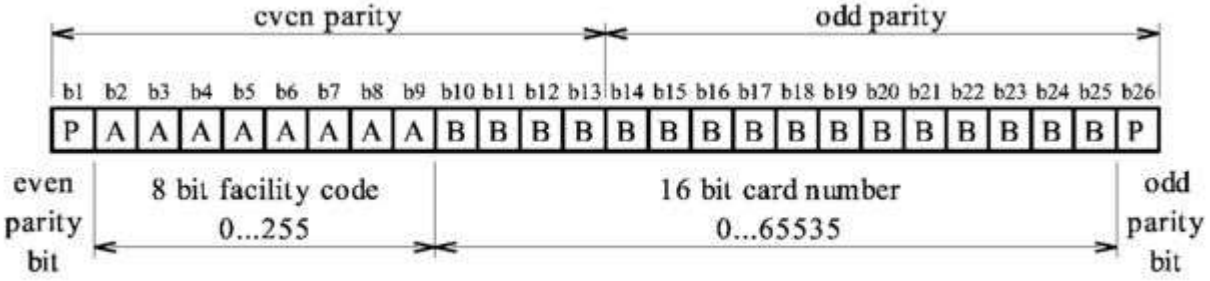
Typical Installation



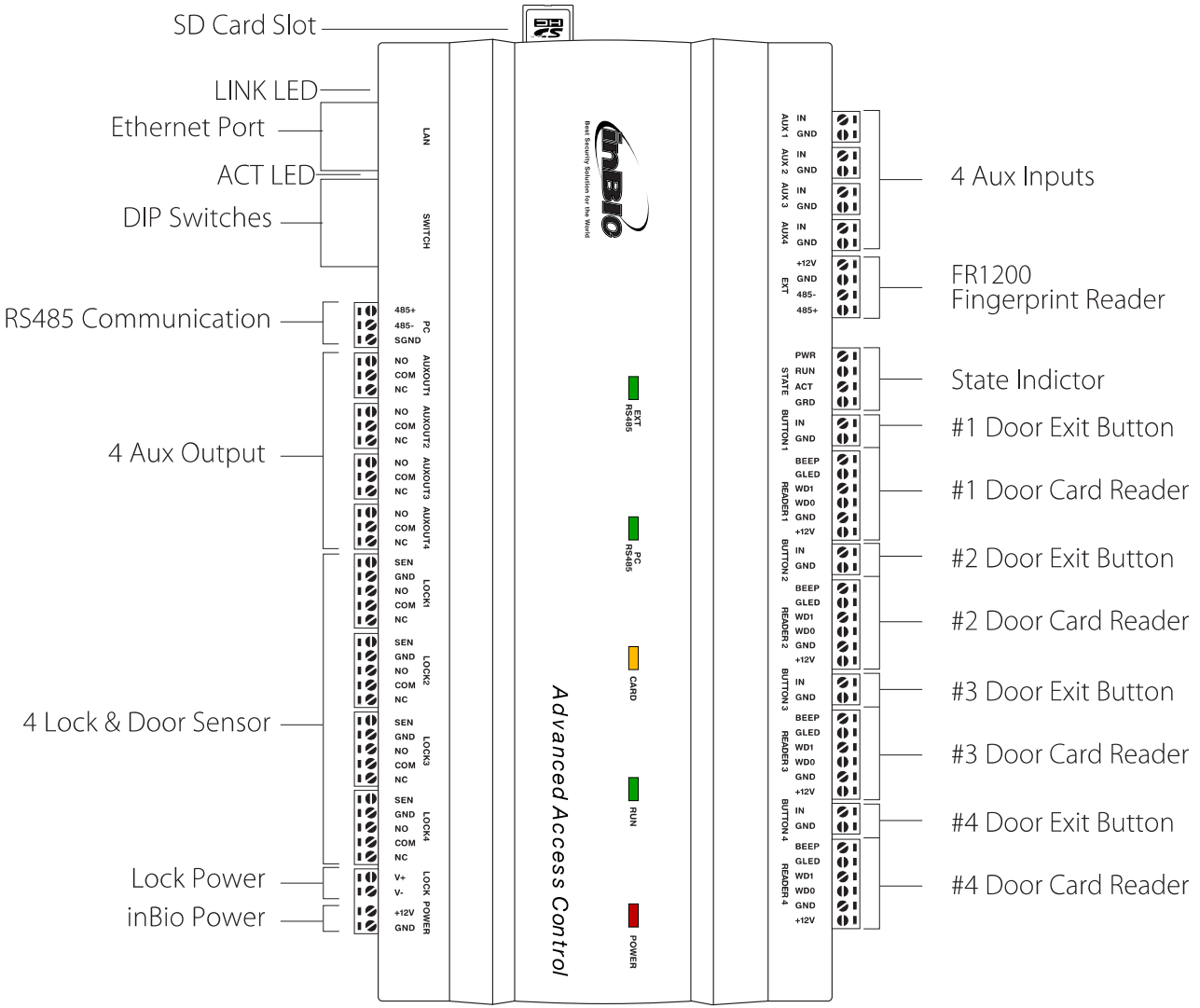
Wiegand Data Format

- Most common data format
- 5 to 8 conductor shielded cable
- Data and power to reader
- 26 bit is industry standard



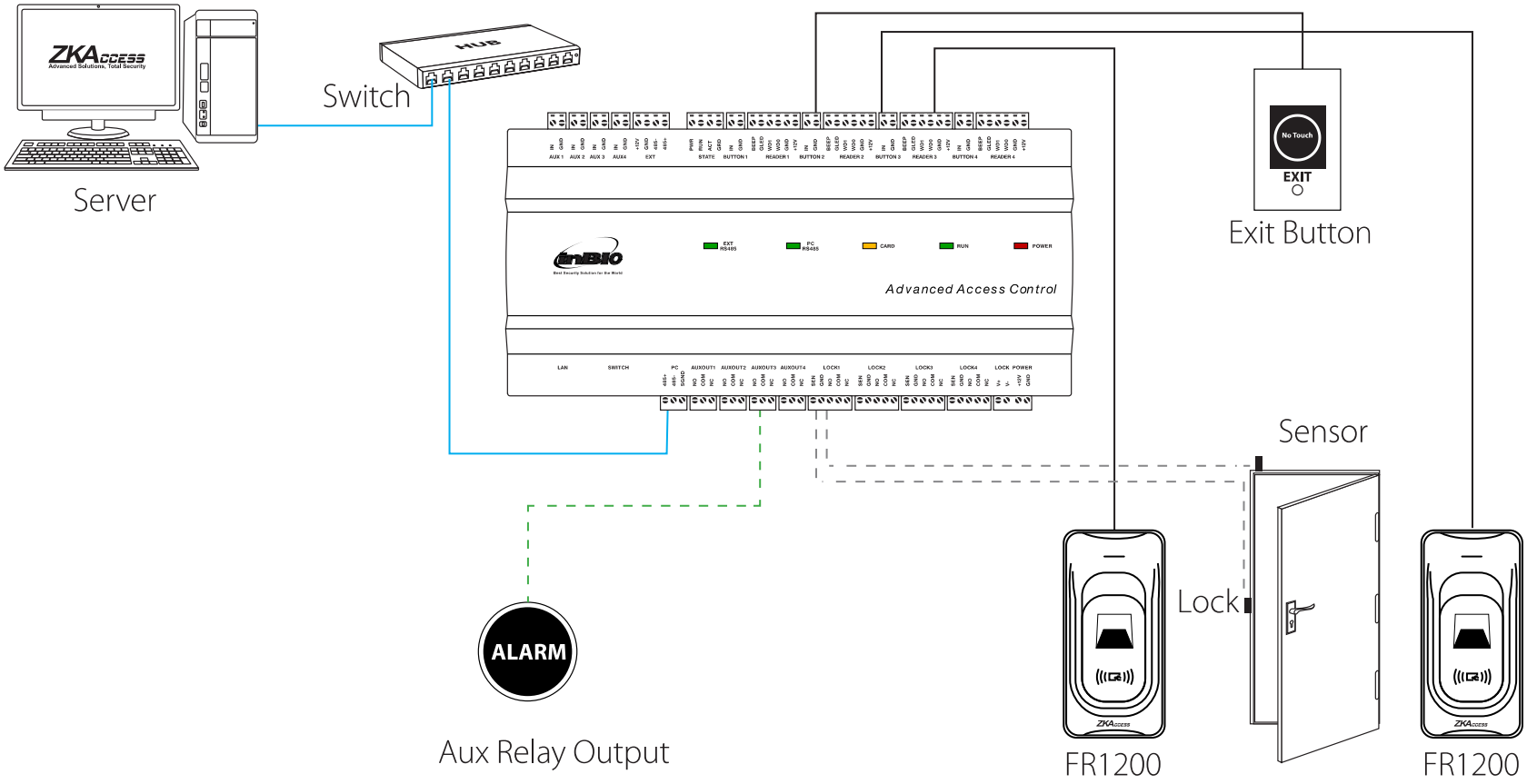


Biometric IP Based Access Control Panel

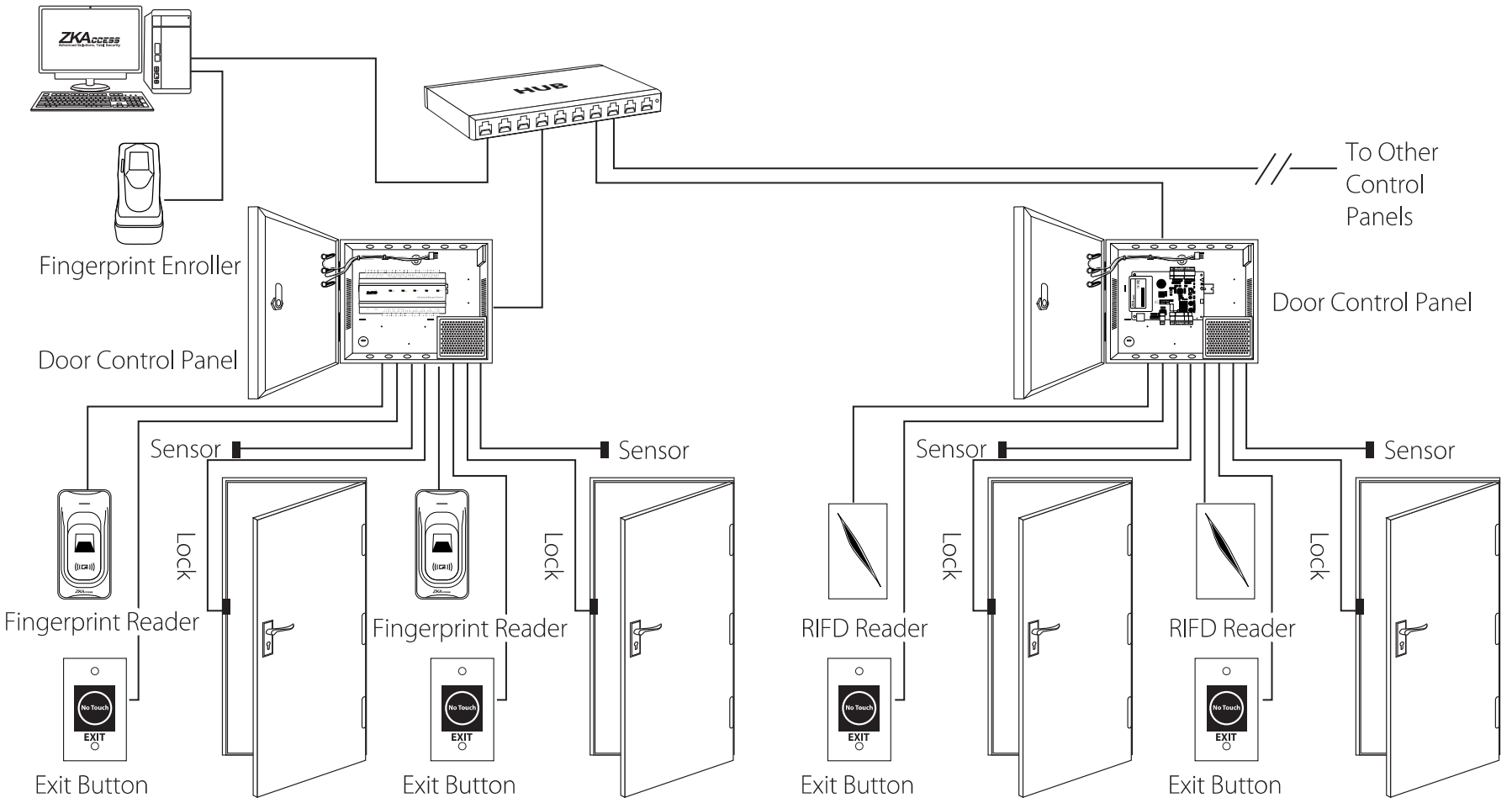


Biometric IP Based Access Control Panel

Typical Installation



Combination of Biometric and RFID Access Control Installation

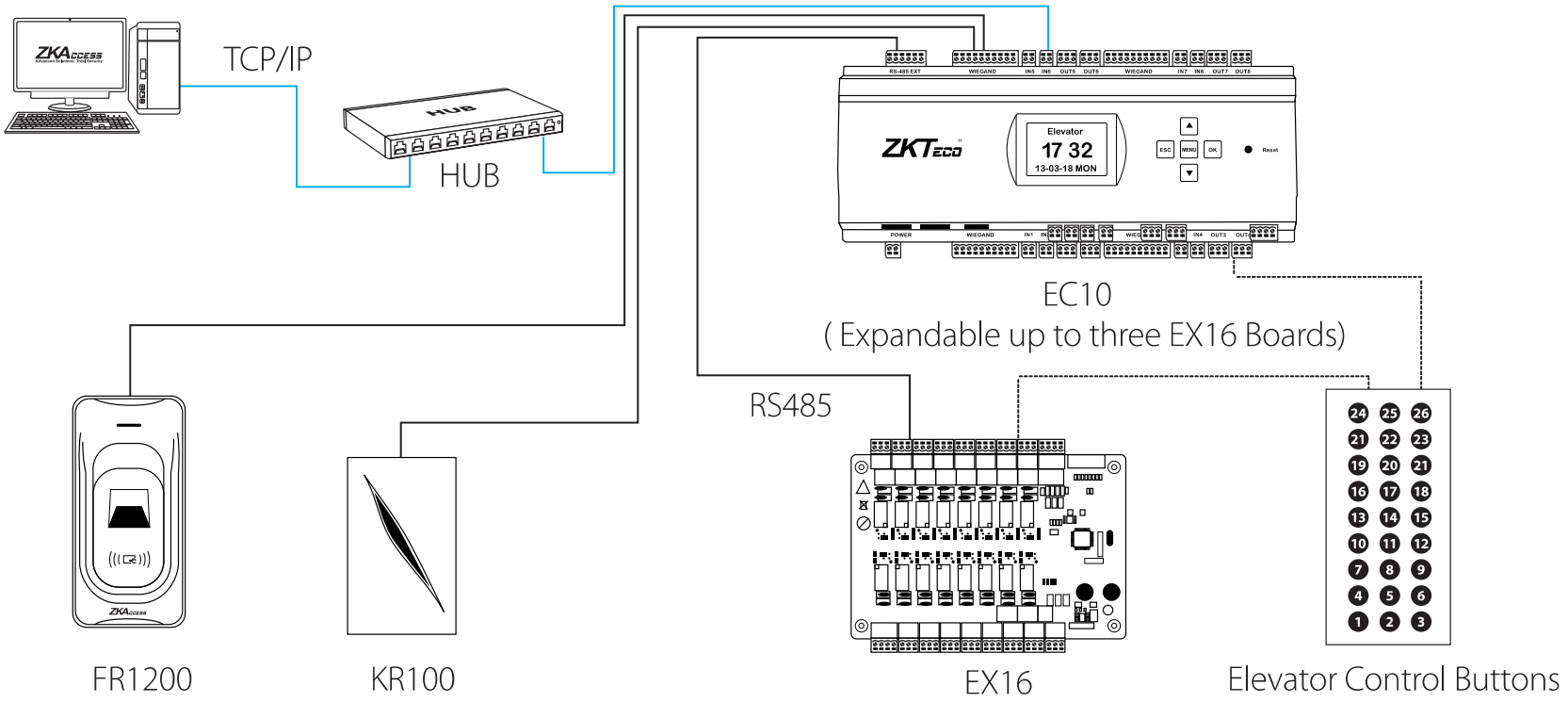


Elevator Control Panel & EX16 Expansion Board

Designed specifically for elevator control, the panel and floor extension boards provide customers the most secure, scalable, versatile and affordable access control solution available today for elevators.

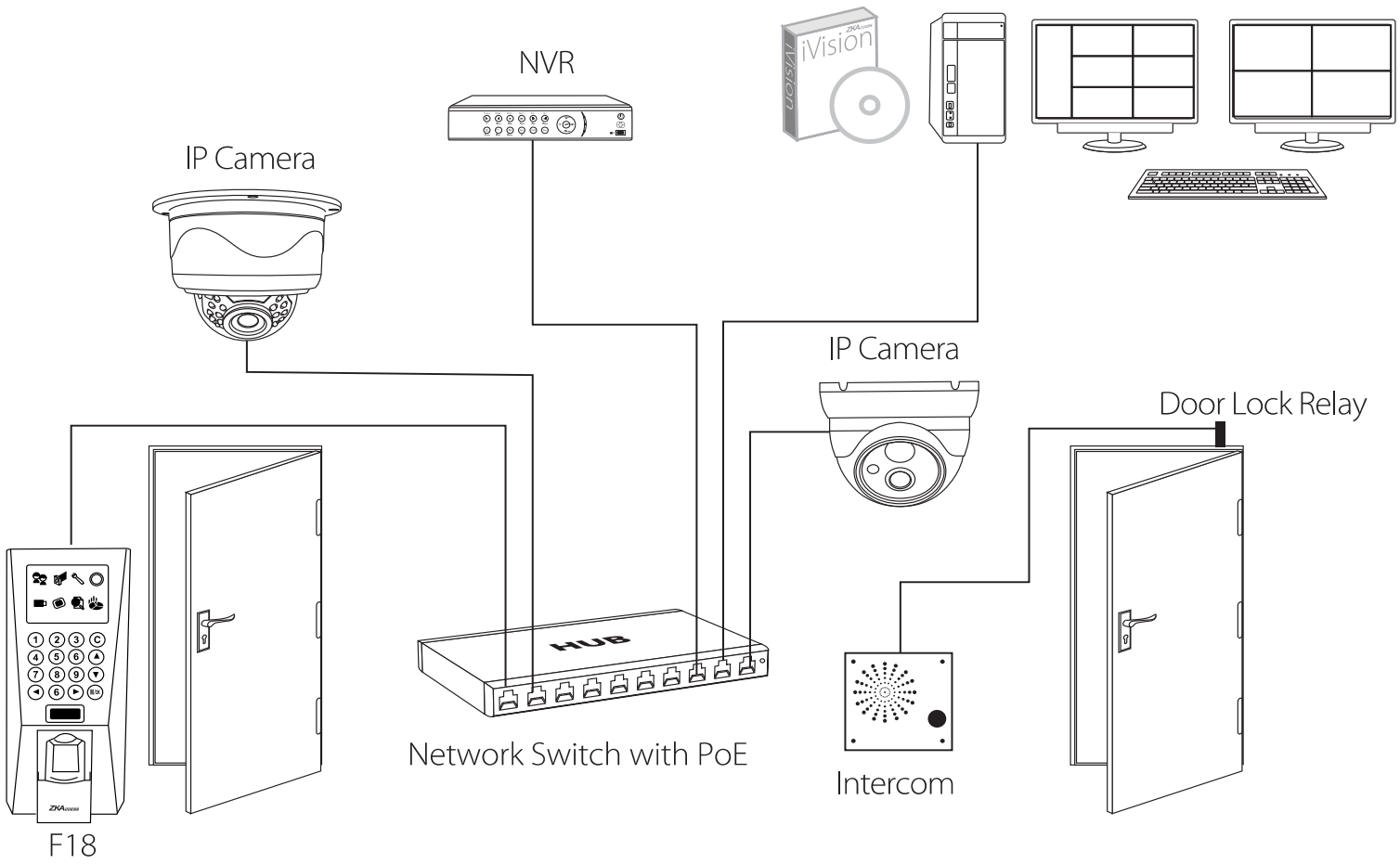
Elevator Control Panel

Typical Installation



IP Cameras integrated with access control

Integrated IP Camera and Access Control



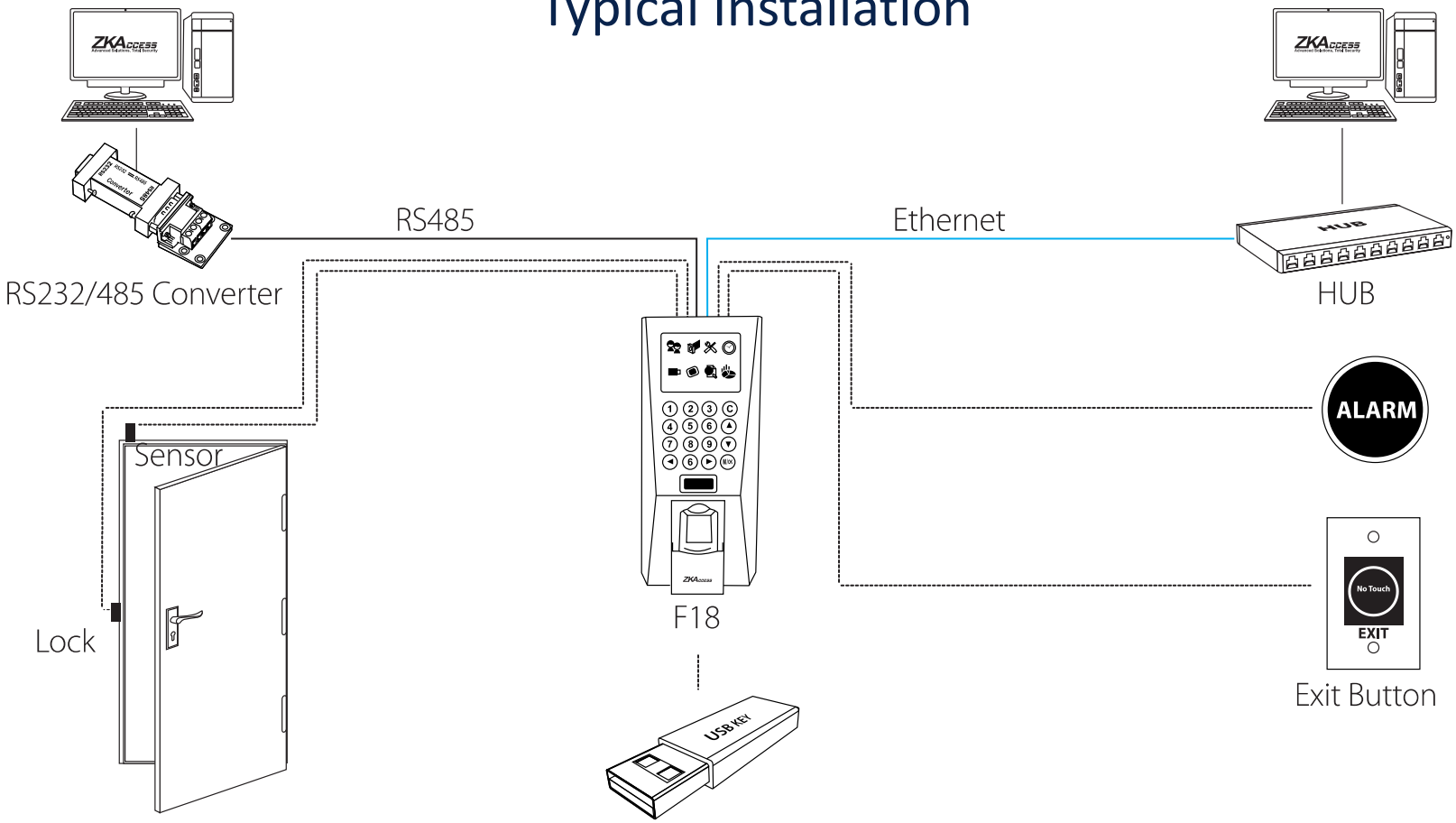
Common design and installation errors

- Ground Loops
- Faulty or incorrect Cabling
- Poor terminations of the cables
- Placement of devices/readers
- Improper enrollment of biometric credentials
- Improper configuration of the software
- Network parameter configuration

Stand Alone Readers with Biometric Authentication

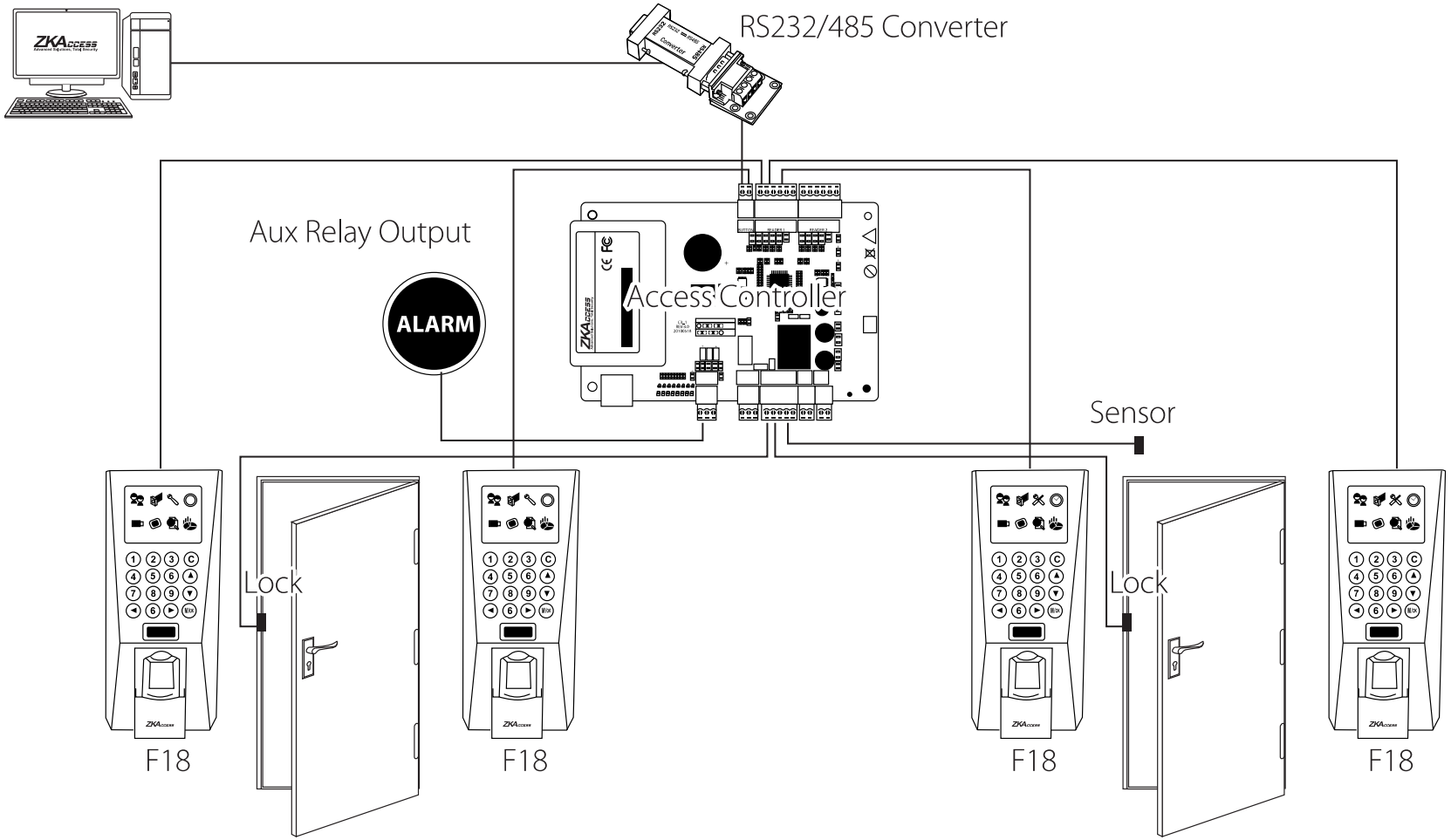
Stand Alone Wiring

Typical Installation



Stand Alone Wiring

Expanded Installation



IP Based vs RS485

IP addressable are more compatible to existing networks and has the ability to have global access over the internet.

The speed of communication is faster with IP addressable devices

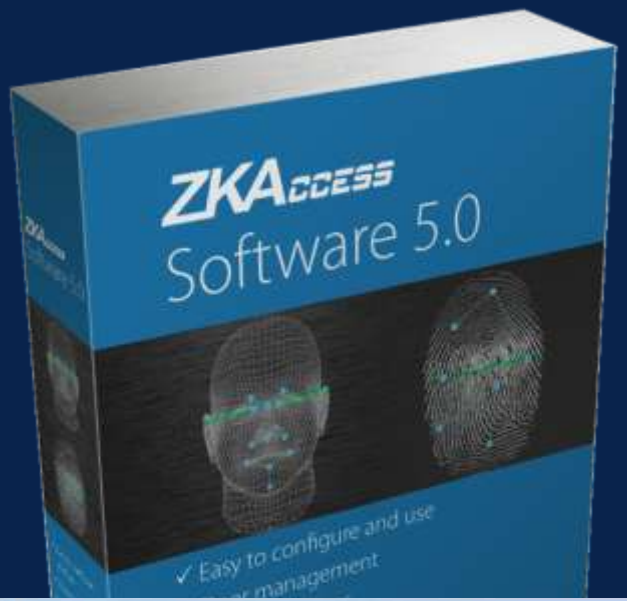
The maximum distance for a single cable run is 330ft.

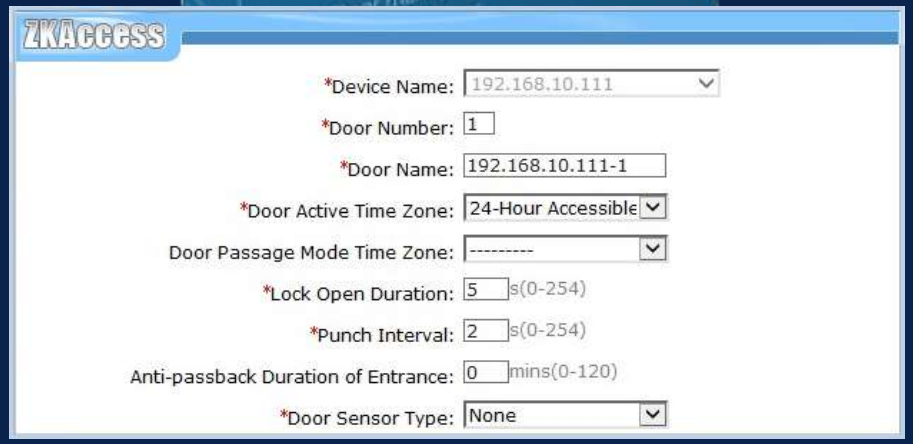
RS 485 can handle higher levels of EMI (Electro magnetic Interference) and communicate over long distance

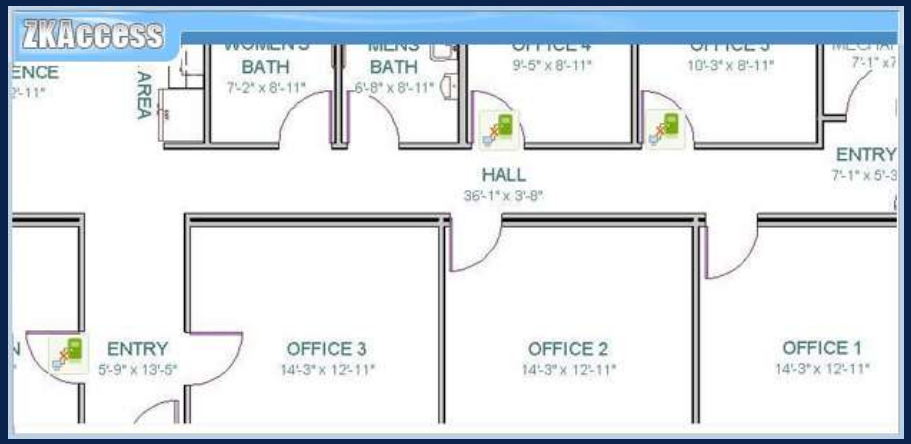
The speed of communication is slow.

Software

The management software helps Security administrators Monitor/Edit/ Update Access for Users







Client Server vs Web-based

Pros

Software is accessible through the local network, creating reasonably quick response and provide advanced level of connectivity with the backend server and database.

Software is accessed from anywhere with a standard browser and an Internet connection

No need to install thin or thick client on different computers

Client Server vs Web-based

Cons

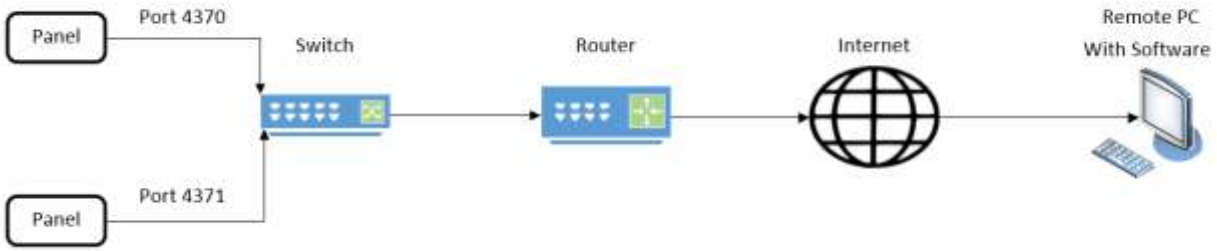
Users must be on the local network to access the software

Access requires an Internet connection.

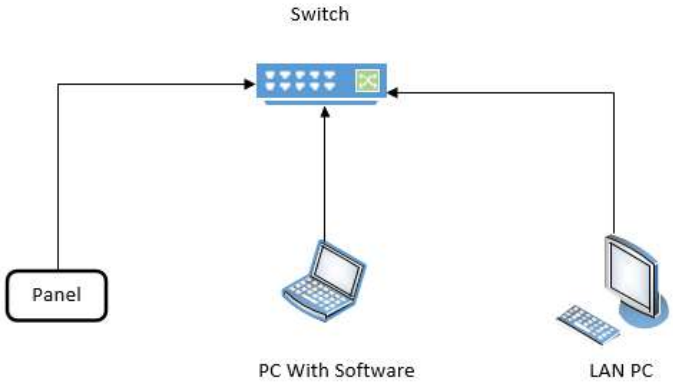
While access to the Internet is growing, it's still not everywhere.

Since software can be accessed from public computers, security is a concern.

Remote Access

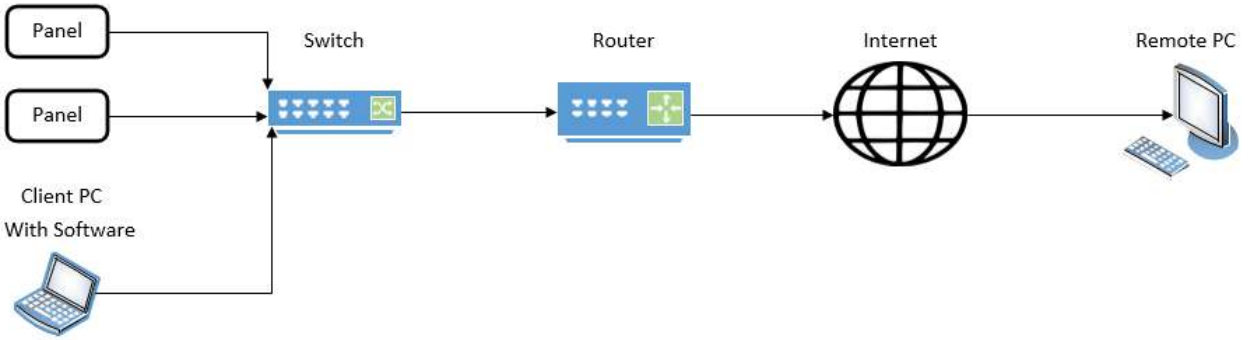


Remote With Software Out of Network



Software in Local Area Network

Remote With Software In Network



Future of Access Control

Beyond biometrics and smart cards, other new reader technologies such as wireless and edge devices, are also generating excitement from integrators for their potential and from end users for their affordability. And virtually everybody is talking about near field communications (NFC), which isn't here yet but holds huge potential to change the access control card and reader market in the future.

Future of Access Control

- Hands free Standalone Biometric Reader Controller using Facial Recognition
- HD IP camera with 1.3MP for Networked Video Surveillance
- Can identify users from a distance of 12.5 feet
- Infrared light source enables face detection and matching in dimly lit environments in less than 1 second