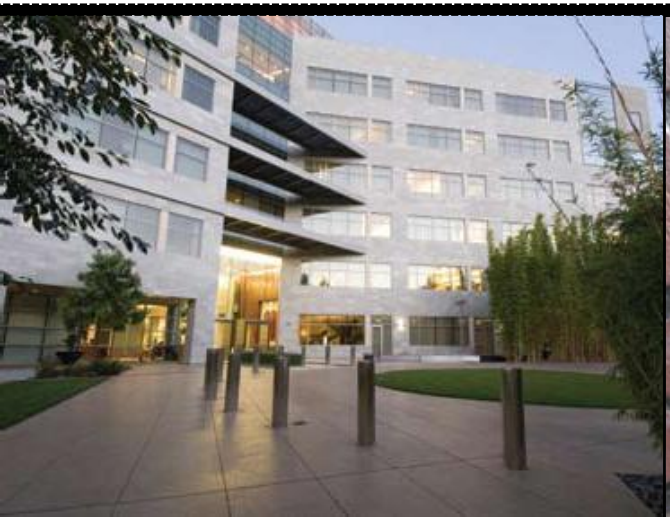
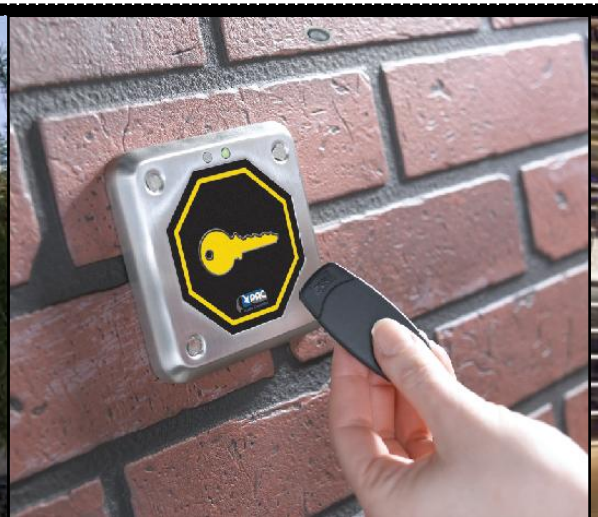
SPECIFYING ELECTRONIC ACCESS CONTROL – integrated solutions utilising wireless connectivity

STANLEY®
Security Solutions





Access Control

- For the last 30 years, PAC has engineered integrated access control solutions for both large and small businesses.
- We offer a complete range of products and systems from single door applications to integrated web based global systems.
- Our systems combine the proven traditional methods with the newest technologies offering a cost effective and complete solution.
- We are proud of the reliability and quality of our products.
- We are dedicated to continually designing and manufacturing access control systems that are innovative and customer led.
- Part of Stanley Security Products, a sales division of global security and communications specialist, Stanley Security Solutions, PAC are able to offer installers the highest level of product quality and technical support.

What is Access Control?

Access Control is the use of devices or methods, at various points within a building, to control the passage of people and / or vehicles into or out of an area or structure.

Electronic Access Control

- Restrict entry or exit of an individual using a reader (using an authorised ID device)
- Allows a User's identity to be validated, granting or denying access based on preprogrammed data

Proximity Access Control

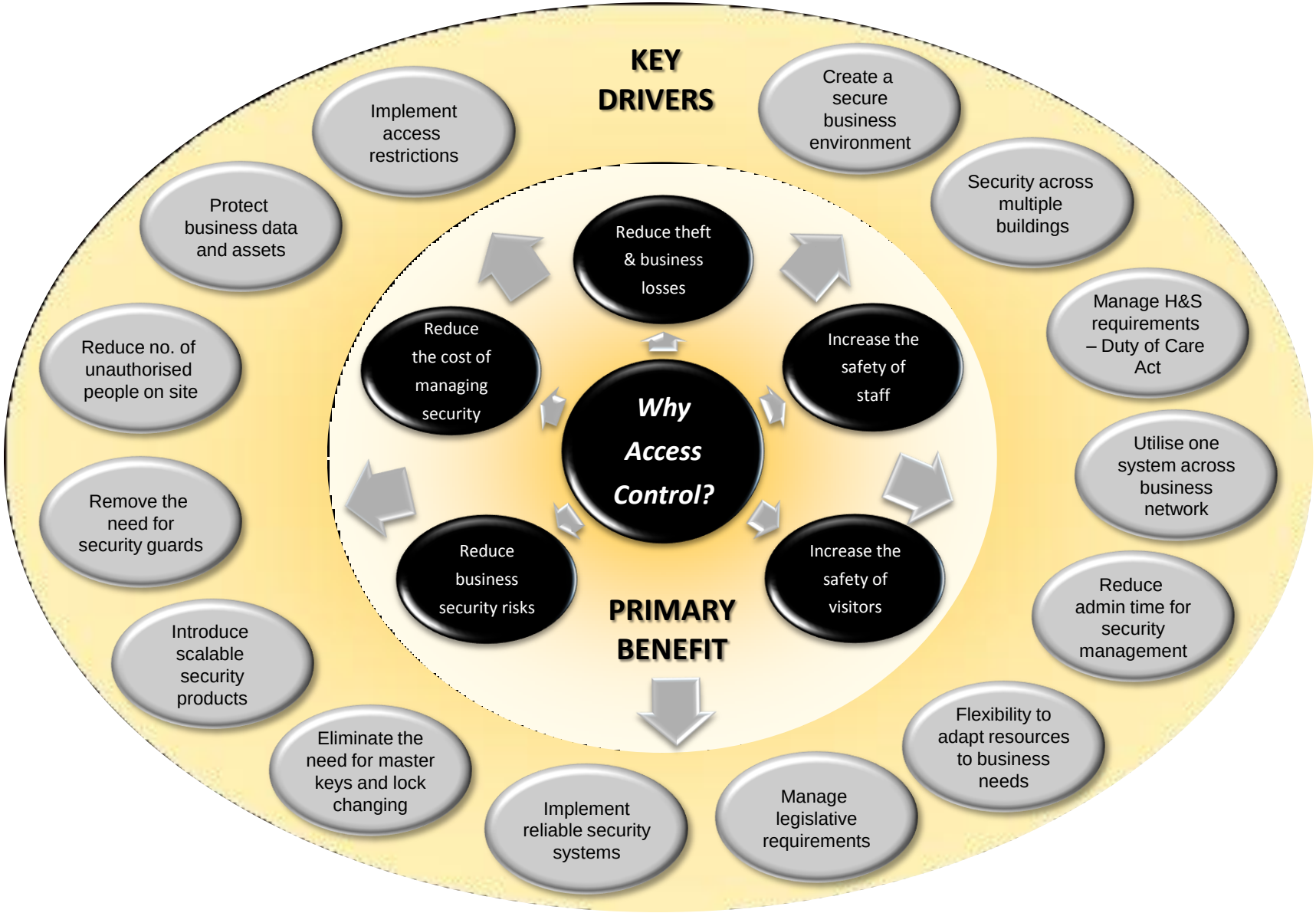
- Controlling access to an area using proximity readers
- Proximity readers lets the user hold the ID device near the reader to unlock the door

Standalone Access Control

- A system incorporating local administration, readers and controllers

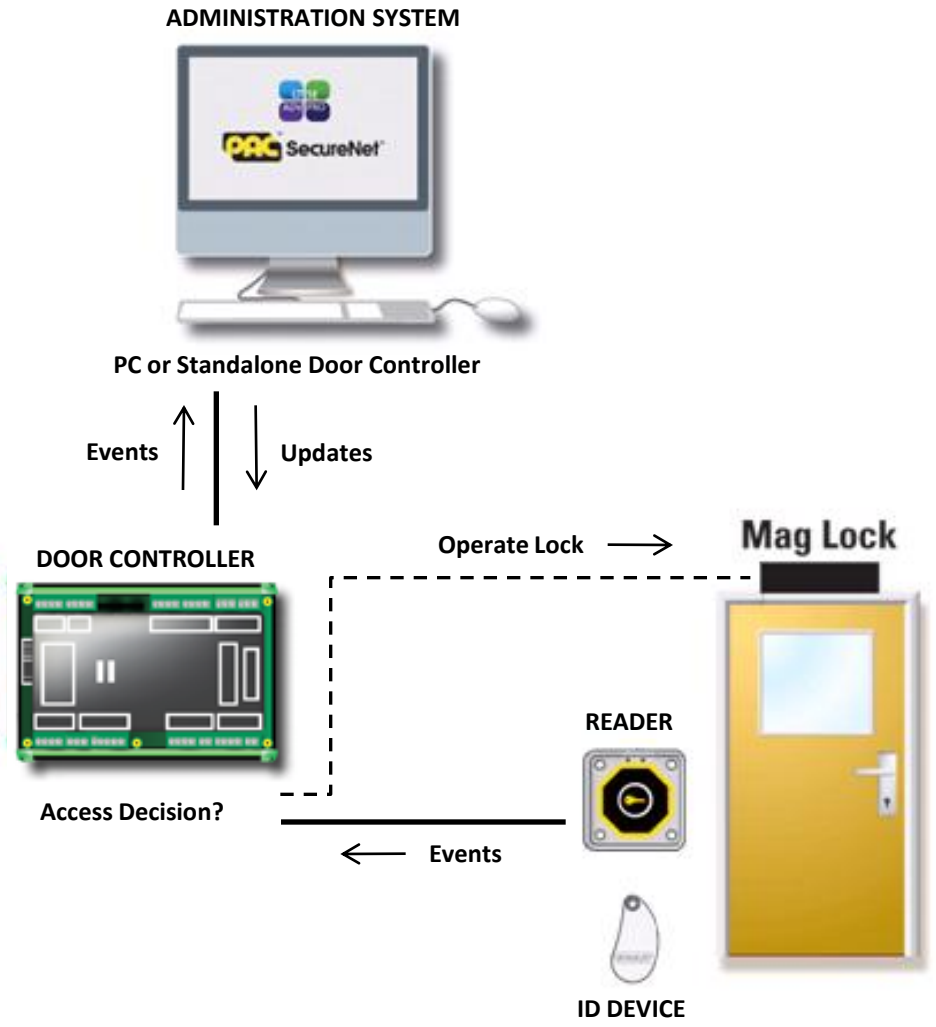
Integrated Acess Control

- A networked system incorporating centralised administration software, readers and controllers
- A system that seamlessly incorporates additional features
- Allows individual systems to "talk" to each other electronically


KEY DRIVERS
Implement access restrictions
Create a secure business environment
Protect business data and assets
Security across multiple buildings
Reduce no. of unauthorised people on site
Manage H&S requirements – Duty of Care Act
Remove the need for security guards
Utilise one system across business network
Introduce scalable security products
Reduce admin time for security management
Eliminate the need for master keys and lock changing
Flexibility to adapt resources to business needs
Implement reliable security systems
Manage legislative requirements
Reduce theft & business losses
Increase the safety of staff
Reduce the cost of managing security
Why Access Control?
Reduce business security risks
Increase the safety of visitors
PRIMARY BENEFIT

Main Considerations when Specifying Access Control

- How many doors need to be secured?
- What type of door hardware / level of physical security is needed?
- What reader technology is required?
- How many people will use the access control system?
- Is administration via a PC required?
- Will the system require alarm reporting?
- Will the system require attendance reporting?



Door Hardware | Electronic Locks

Electro-Magnetic Locks – Always fail safe. Consideration needs to be given to head clearance (min 6ft 6”) and which way the door opens as locks are usually fitted at the top of the door - housings for glass doors are available.

Electro –Magnetic Shearlocks – Always fail safe. Often morticed into the door and frame. Good for swing through doors but it is important that the door closes.

Electric Strikes – Can be flush or surface mounted. Fail safe or fail secure. Specialist carpentry skills required. Glass door options are available.

Electronic Locks – Most secure option. Specialist carpentry skills are required. Fail safe or fail secure. Always morticed into the door frame but they give a good level of physical security.

Electro-Magnetic Shearlock

Electro-Mechanical Lock

Electronic Lock

Reader Technologies

There are a number of reading technologies on the market, ranging from inexpensive, low security keypads to high security proximity cards and biometric systems.

Technology	Description
Proximity	The most popular form of ID device. The User simply presents the card / token in close vicinity of the reader to release the door. It offers high security as card cannot be copied and can incorporate magnetic stripe for cashless vending
Smart (MiFare)	A variant of the proximity card that offers the ability to store data on the card and read / write information such as cashless vending, student library
Biometric	Biometric systems use physical attributes such as fingerprints, retina scans and facial recognition for identification
Keypad PIN & Proximity	This requires the user to present a proximity ID device together with a PIN in order to gain access, offering a higher level of security
Wiegand	Wiegand cards are manufactured with a wiegand ribbon or tape. This tape has short wires embedded which are individually polarised giving a code when passed through a magnetic sensor
Magnetic Stripe	Uses an encoded magnetic stripe laminated onto a PVC card. Magstripe readers are not suitable for harsh environments and the exposed reader head requires regular maintenance. They are not suitable for high security applications
Others	Barcode, Watermark, Infra-red

Smart Card Explained

Smart cards are a single card solution that incorporates access control with applications such as cashless vending and ticketing systems, offering a cost effective and enhanced alternative to the conventional proximity card.

Smart cards help businesses evolve and expand their applications and services and offers many benefits:

Intelligence

- Capable of processing information, not just storing
- The cards can communicate with computing devices through a Smart reader
- Information and applications can be updated without having to issue new cards

Security

- Chip is tamper resistant
- Information stored can be read / write protected
- Each card has its own unique serial number

Convenience

- Wallet sized and easily portable

Applications

Banking & Payment

Supply chain & logistics

Loyalty & Retail

Schools / Universities

Healthcare & Social Services

Smart Tracking

Pay TV

Communication

Biometrics Explained

Biometric systems use physical attributes such as fingerprints, retina scans, palm vein and voice recognition for identification.

Available as standalone systems or as a reader integrated into an existing access control system, Biometric readers offer a solution for high security applications.

The most commonly used form is fingerprint with the use of an industry standard Mifare card that stores the fingerprint template, eliminating the need for a centrally stored database. On presentation of a valid fingerprint to the fingerprint template on the card and in line with the card's authority levels access will be granted / denied.

Biometric technology is growing in popularity with the increase in reliability and decrease in cost.

Applications

Government

Transport

Pharmaceutical

ICT

Finance

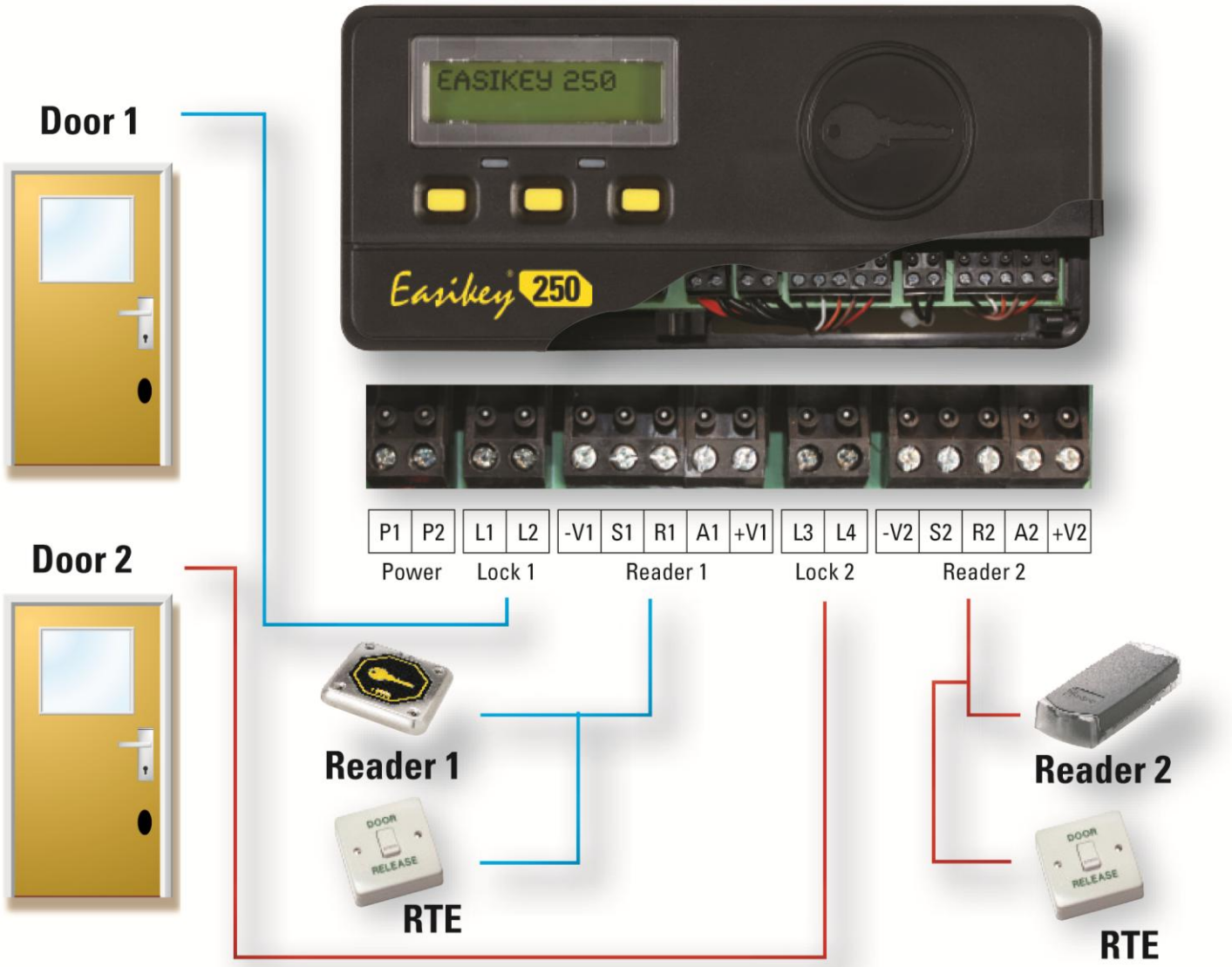
Commercial

Health

Education

Petrochemical

1 - 2 Door System



Integrated Systems

- Comprehensive software packages
- Based on Microsoft Windows®
- Allows remote administration
- Event log – detailed list of events
- Ability to monitor alarms
- Customisable reports
- Alarm reporting
- Evacuation / muster reports
- Graphical map support providing interactive alarm and event icons
- Lift control
- Individual door access (DDA compliant feature)
- Photo ID badge creator
- Advanced systems utilise TCP/IP connections directly onto LAN / WANs, allowing the ability to control numerous sites globally, from a single location

- Additional integrated features:
  - CCTV monitoring
  - Guard tour
  - Alarm event management
  - Attendance reporting
  - BMS integration

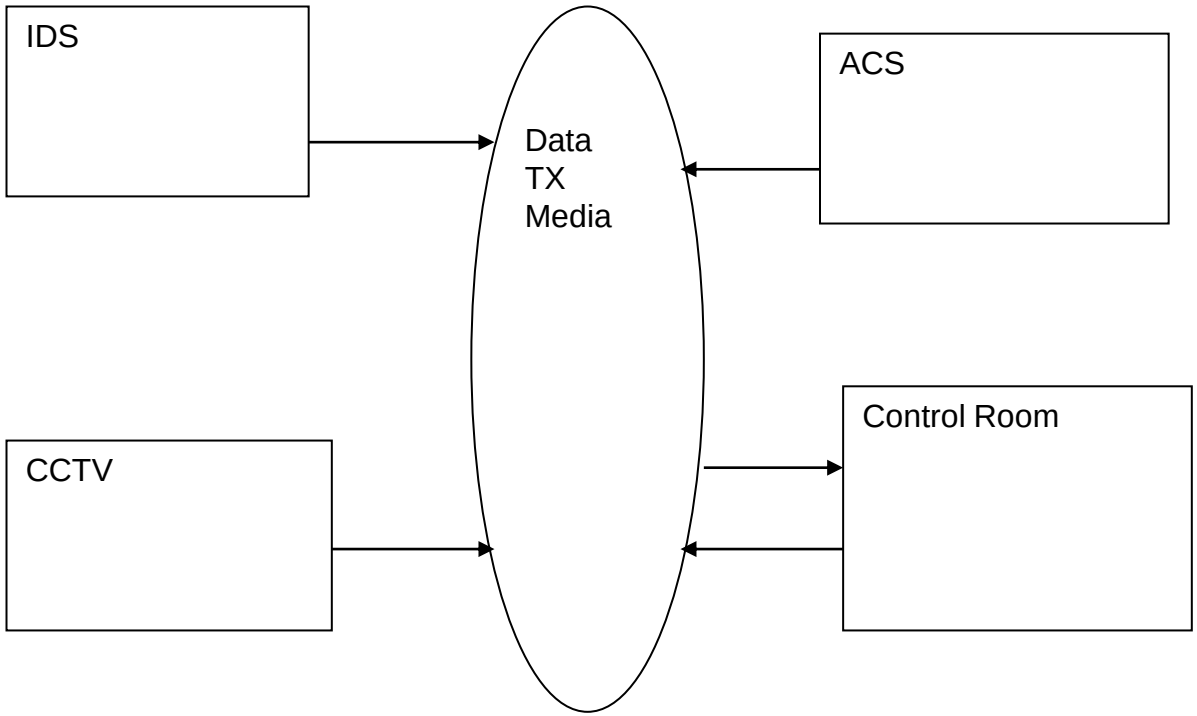
Specifying Integrated Solutions

- Establish the requirements
- Generate interdisciplinary planning team
- Involve all affected functions and departments
- Identify design criteria
- Assess threat, assets to be protected, budgetary constraints, level of protection required
- Evaluate costs V threat
- Prepare detailed specification

Scale and scope of solution

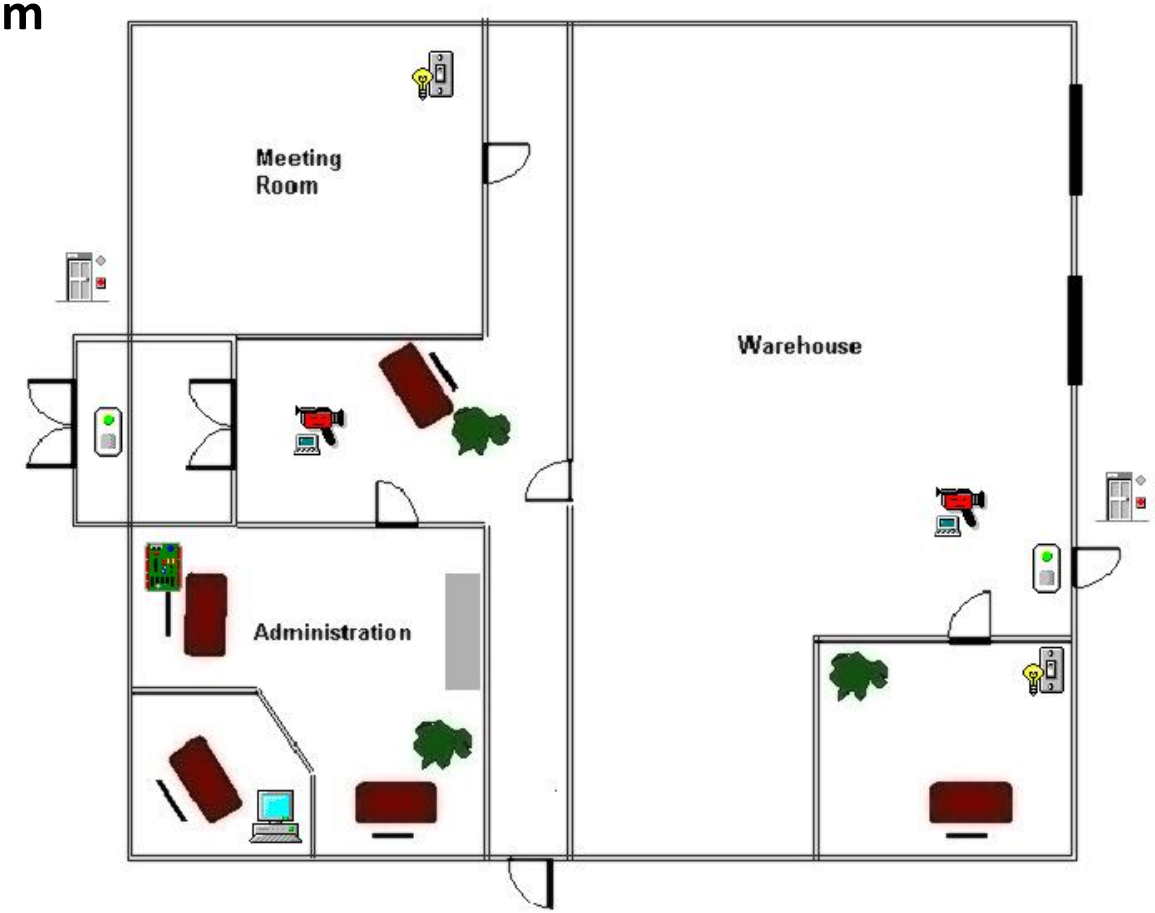
- RS485 or Networked
- No of workstations
- Alarm Monitoring method
- No of sites/buildings
- Access Control
- Intruder Detection System
- CCTV system
- Remote sites interface
- Central or local monitoring

Typical Integrated system



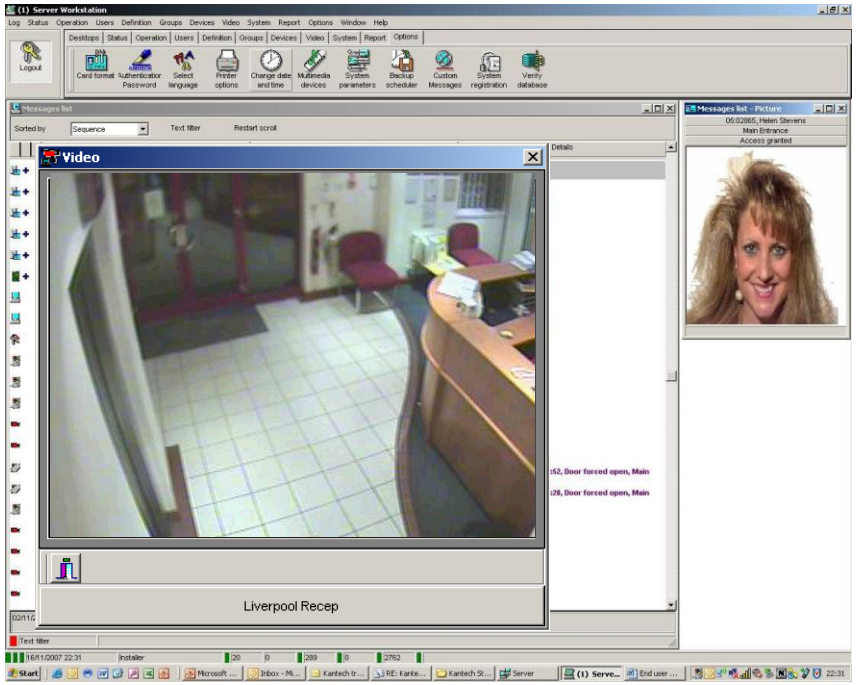
Integration Example

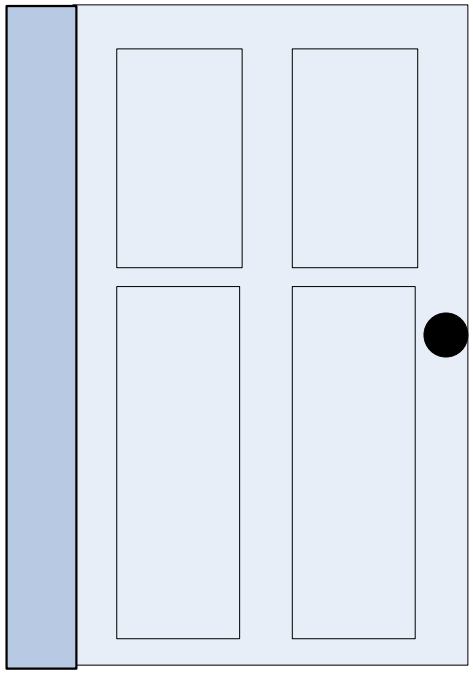
- **Call Camera directly from the Access Control graphical map**



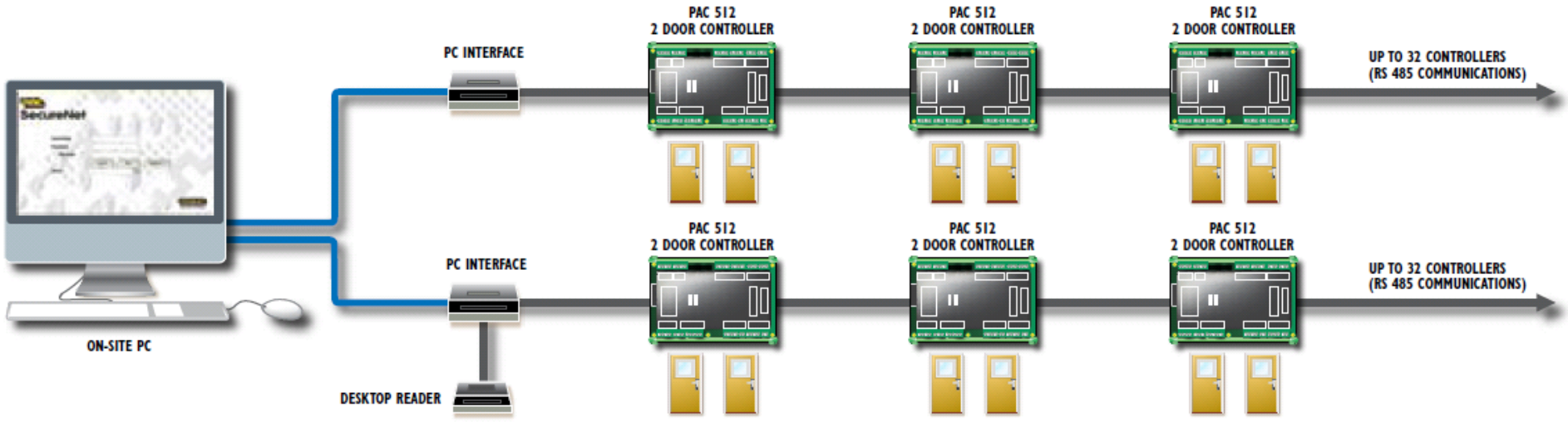
Integration Example

- **Generate Automatic Live Video Display upon an Access or Intruder system event**

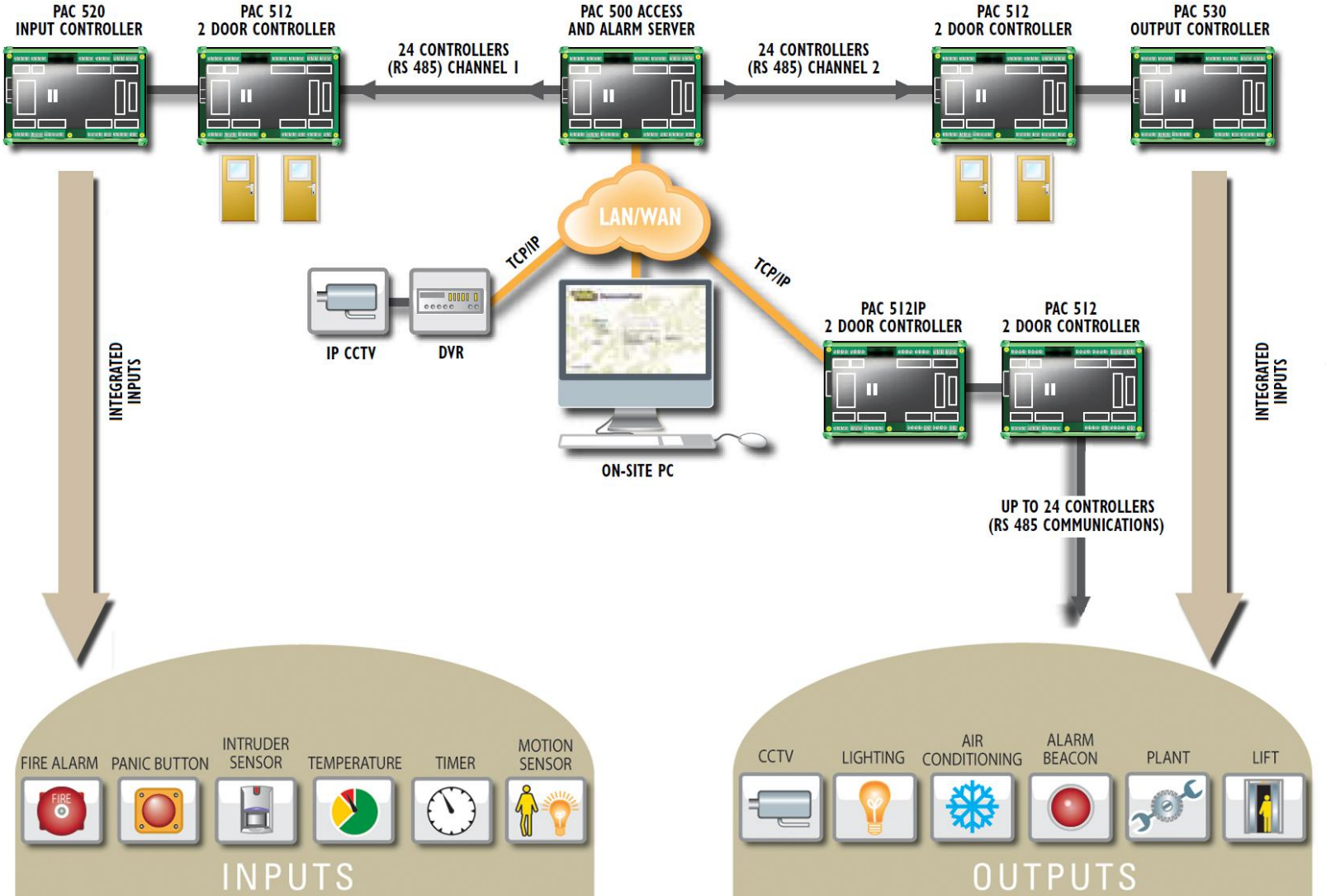




Integrated Systems | Basic System Schematic

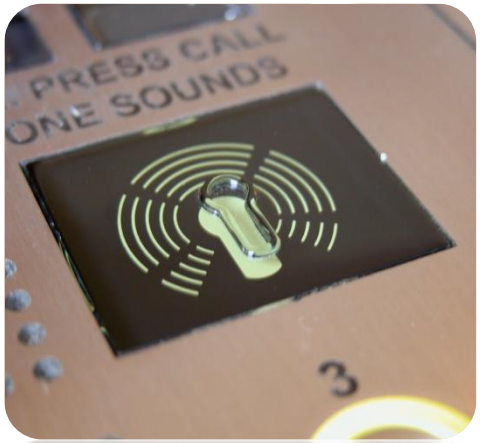


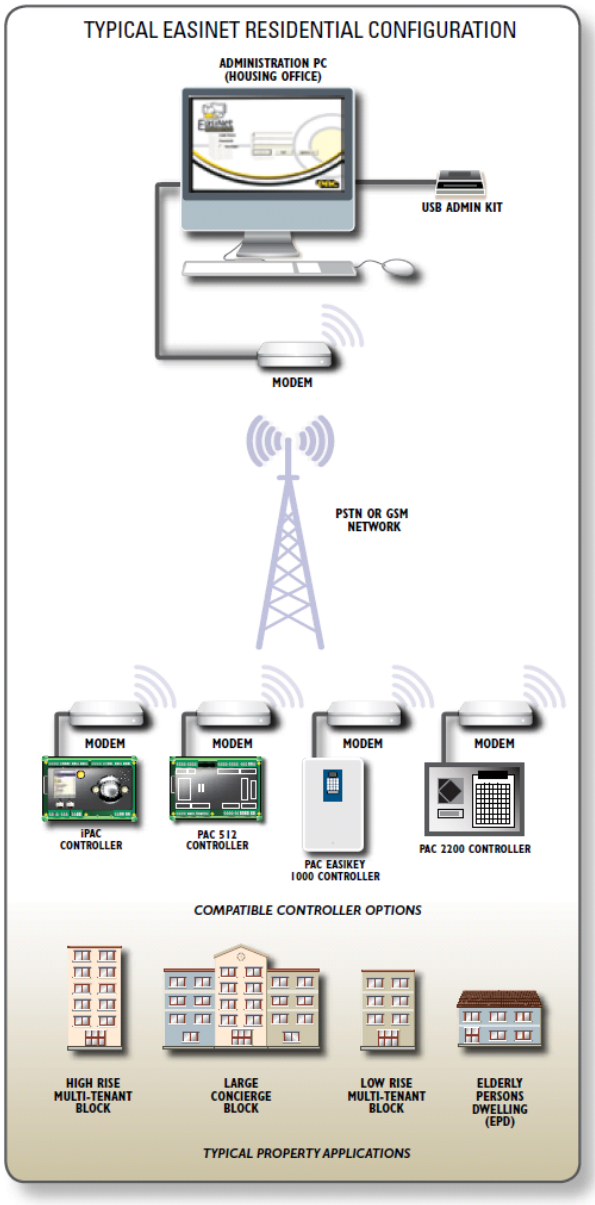
Integrated Systems | Integrated Schematic



Residential Projects

- Integrated systems with comprehensive software packages
- Access control and security solution for multi-tenanted dwellings
- Access control to communal entrances in flats
- Access (using authorised ID devices) for residents and Staff
- Comprehensive reports
- Extra door opening time – DDA compliant feature



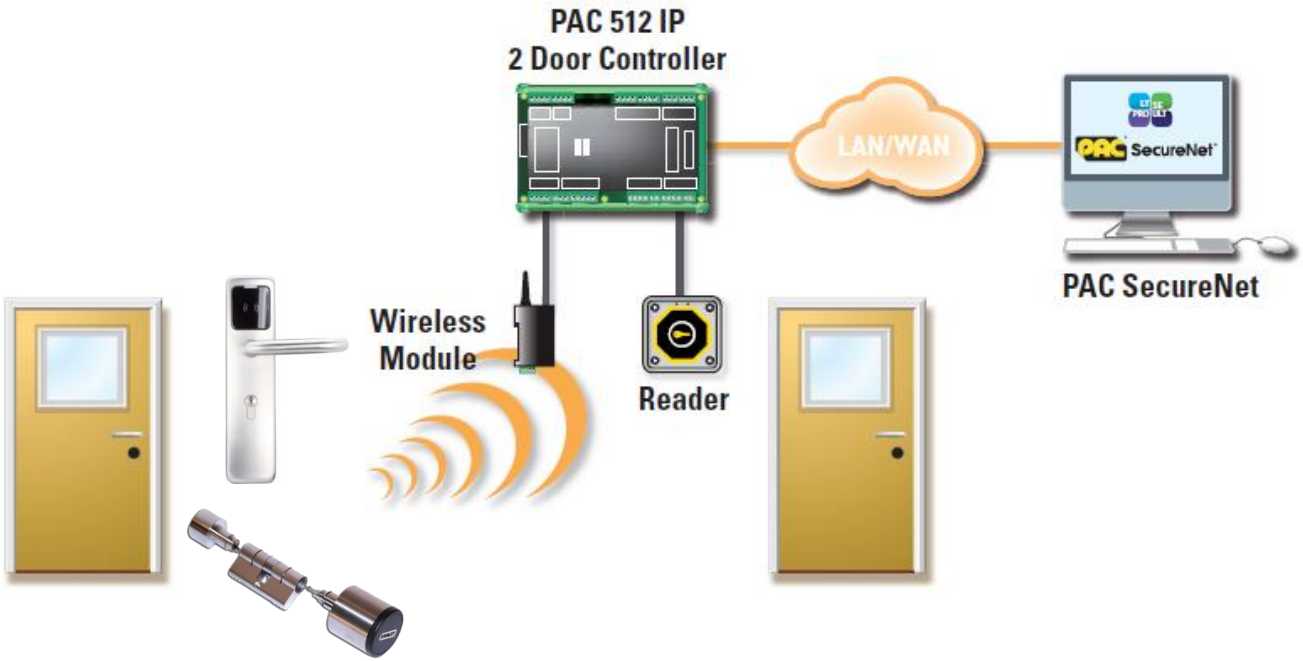


Future Trend| Wireless

There is a growing trend towards the wireless connection of door locks to access controllers using battery operated, electronic cylinders or electronic escutcheons.

Key Benefits:

- Easily replaces existing manual key based locks
- Reduces installation time
- Reduced number of components / wiring required providing a more cost effective solution

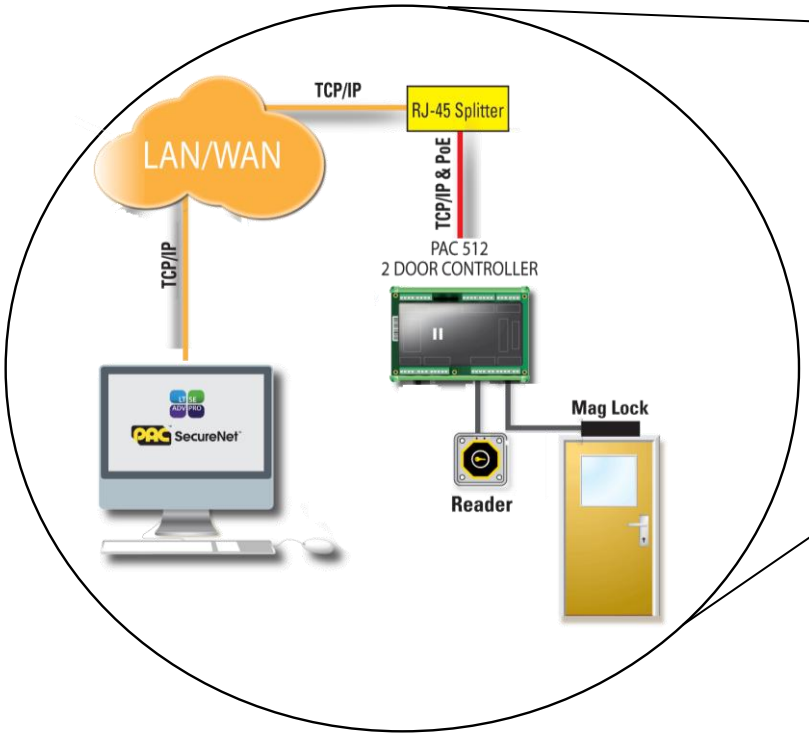


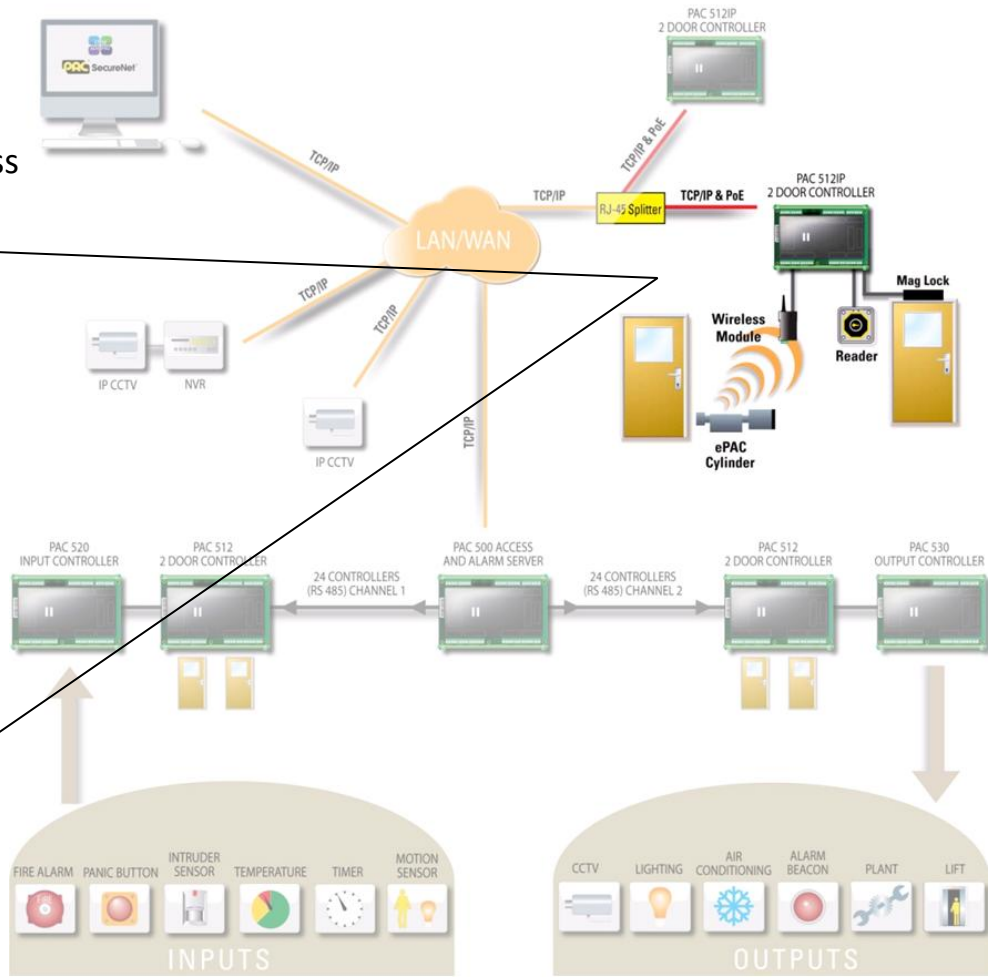
Future Trend| Power over Ethernet

The ability to power and pass data to an access controller via Ethernet cabling with the use of industry standard PoE Splitters in conjunction with powered routers.

Key Benefits:

- Allows an existing network to be used as a platform (supported by a reliable power supply provided by a router)
- Helps provide an economical and quick to deploy access control system





Applications

Finance

Commercial

Health

Education

Utilities

Retail

Government

Transport

Residential

Construction

Industry / Manufacturing

Petrochemical

Pharmaceutical

ICT

Leisure

British Standards

For specifying access control systems including locking hardware

BS EN 50133 - Part 1	**System Requirements**
BS EN 50133 - Part 2-1	**General Requirements for Components**
BS EN 50133 - Part 7	**Application Guidelines**

For Panic Doors

BS EN 1125	**Panic exit devices operated by horizontal bar (must be used in public places)**
BS EN 179	**Panic exit devices operated by a lever handle or push pad (can be used in buildings where personnel have evacuation procedure training)**