



APICE s.r.l.

**SISTEMA DI CONTROLLO ACCESSI
FUNZIONANTE SU RETE LonWorks
(ANSI/EIA 709, EN 14908) E
CONFORME ALLE DIRETTIVE LonMark
DI INTEROPERABILITA'.**

*Descrizione del sistema
Luglio 2006*



SISTEMA DI CONTROLLO ACCESSI SU PIATTAFORMA ANSI/EIA 709 – EN 14908 (LonWorks)

Realizzare un investimento intelligente, utilizzando una tecnologia aperta ed interoperabile e che non sia vincolata ad un unico costruttore 'apparecchiature.

INTRODUZIONE

APICE s.r.l. è una società Italiana, con sede ad Empoli, specializzata dal 1990 nella costruzione d'apparecchiature elettroniche rivolte a realizzare soluzioni di **controllo accessi professionali** e d'automazione degli edifici (building automation).

APICE è attenta a proporre apparecchiature che funzionino su una piattaforma **standard ed aperta** in modo che l'investimento fatto per realizzare il sistema non si vanifichi per una precoce obsolescenza oppure per scarse o difficili possibilità di espansioni future.

Scopi principali del sistema di controllo accessi

- Garantire un'elevata sicurezza per gli accessi nell'edificio.
- Mantenere la massima agilità dei movimenti delle persone all'interno dell'edificio, evitando ad esempio identificazioni complesse che risultano inutili su certi varchi durante particolari momenti della giornata.
- Aumentare la flessibilità degli orari lavorativi senza aggravare i costi della vigilanza. Diminuire i costi della vigilanza.
- Introdurre un deterrente contro azioni illecite e furti interni di materiali o di informazioni.
- Ottenere un risparmio nelle spese di conduzione dello stabile, utilizzando le informazioni del controllo accessi per limitare gli sprechi energetici.
- Monitorare in tempo reale lo stato delle porte.

Avere in tempo reale la situazione dei presenti all'interno di una o più aree, in modo da assicurarsi della completa evacuazione delle persone in caso di pericolo.



Funzionamento del sistema

Il sistema di controllo accessi APICE rappresenta un'ottima soluzione per la gestione del flusso delle persone all'interno di un edificio intelligente, garantisce un'elevata sicurezza congiuntamente ad un'elevata mobilità, perché riesce a adattarsi facilmente alle differenti situazioni che si verificano durante una giornata lavorativa all'interno degli spazi operativi.

Questo sistema è costruito in maniera da essere interoperabile con altri apparecchi conformi LONMARK^{®1}, anche di diverse marche e che compiono differenti funzioni all'interno di un edificio intelligente. Esso, utilizzando lo stesso cavo di rete, può prelevare e fornire informazioni utili agli altri sistemi.

Il controllo accessi APICE nasce per essere il primo impianto tecnologico con cui una persona interagisce al momento dell'entrata in un edificio e anche l'ultimo al momento dell'uscita. Ecco che diventa un'importante fonte d'informazione riguardante lo stato d'occupazione dell'edificio, per essere sfruttata ad esempio per regolare in maniera ottima i consumi d'energia o attivare automaticamente l'impianto di sicurezza.

Ciascun varco con accesso controllato è in grado di operare con tre differenti livelli di sicurezza:

Bassa sicurezza:

- Quando l'ambiente è presidiato.
- Nessun tipo di identificazione richiesto.
- Aperture automatiche delle porte abilitate.
- Allarmi forzature del varco disabilitati.
- Conteggio delle persone presenti disabilitato.

Media sicurezza:

- Quando l'ambiente è scarsamente presidiato.
- Necessità di identificazione.
- Aperture automatiche disabilitate.
- Allarmi forzature del varco abilitati.
- Conteggio delle persone presenti abilitato.

¹ LonMark[®]: Organizzazione mondiale che stabilisce le regole di interoperabilità per i dispositivi funzionanti sulla rete EN14908 (LonWorks[®]). Vedi www.lonmark.org

Alta sicurezza

- Quando l'ambiente non è presidiato. Antintrusione inserito.
- Necessità di identificazione eventualmente a livello superiore (carta + PIN...).
- Lista degli utenti abilitati ristretta.
- Aperture automatiche disabilitate.
- Allarmi forzature del varco abilitati.
- Conteggio delle persone presenti abilitato.

La mobilità all'interno dell'edificio è massima nel livello di bassa sicurezza e minima in quello di alta sicurezza. Non è detto che tutto il sistema di controllo accessi debba avere il medesimo stato, l'impianto può essere suddiviso in zone e ciascuna zona può avere un proprio livello di sicurezza. Il funzionamento di default del sistema è la media sicurezza, il passaggio da un livello ad un altro può essere determinato da stati provenienti da altri dispositivi.

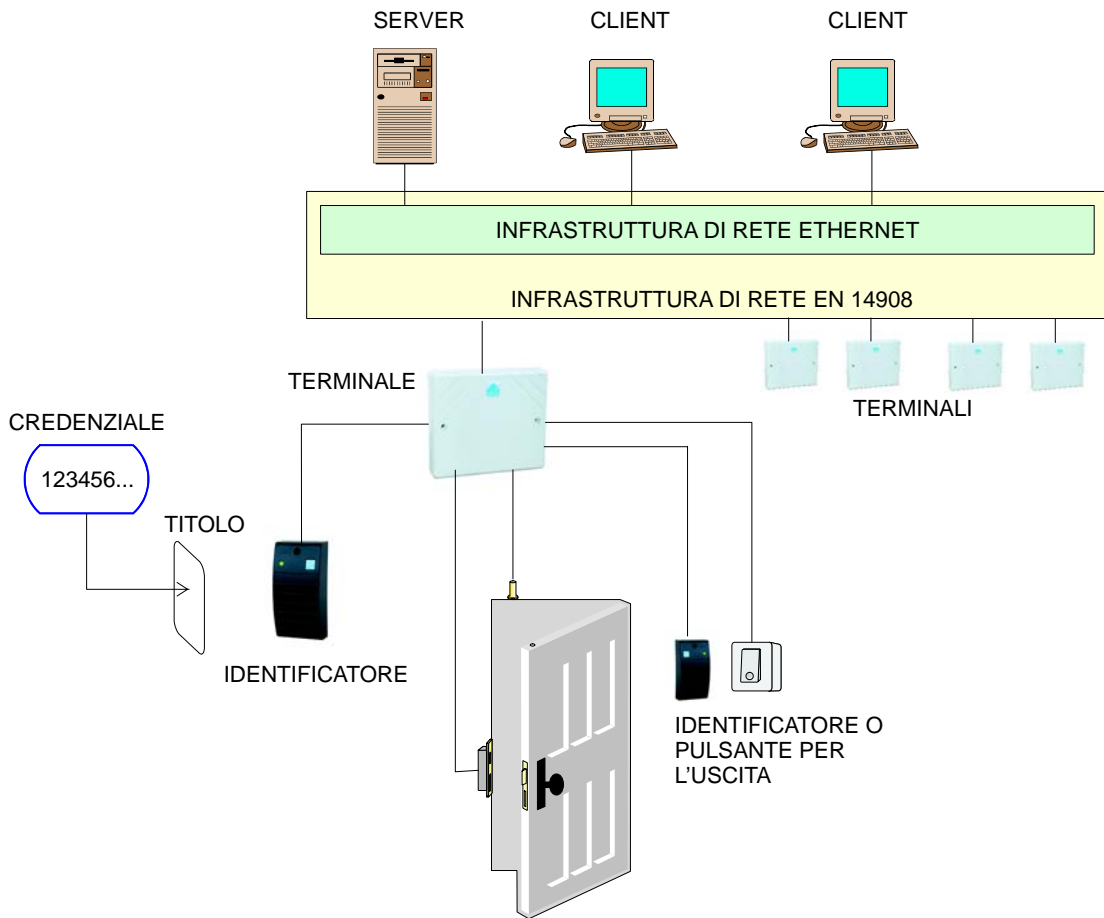
Il funzionamento del sistema è indipendente dal software di gestione che gira su un PC o su un server. L'impianto garantisce il 100% delle funzionalità anche in modalità off-line.

Il controllo accessi APICE si basa su una logica di intelligenza distribuita, completamente modulare ed espandibile in maniera orizzontale sulla rete di comunicazione EN 14908; come conseguenza si ottiene che non esistono centrali che in caso di guasto possono compromettere il funzionamento dell'intero sistema.

L'amministratore di sistema, grazie al software di gestione, stabilisce una serie di regole per permettere o negare l'accesso degli utenti ai singoli varchi. Le regole, per ciascun varco, comprendono la data di scadenza, la fascia oraria settimanale, i percorsi obbligatori/antipassback², nonché la possibilità di accesso in alta sicurezza.

² Antipassback: Funzionalità che impedisce l'accesso in un area quando la persona risulta essere all'interno e ne impedisce l'uscita se invece risulta essere all'esterno. E' utilizzata per evitare l'utilizzo di una tessera per fare due accessi consecutivi alla stessa area ad esempio perché si passa la tessera ad un collega.

Componenti di un sistema di controllo accessi



Credenziali: Sono i codici d'accesso ad un sistema e possono essere memorizzati su un supporto fisico, tenuti in memoria dall'utente (come ad esempio il codice PIN), oppure costituite da parti fisiche dell'utente (come nel caso di identificazioni biometriche).

Titoli: Sono i supporti che conservano le credenziali di accesso. Possono essere tessere con banda magnetica, tessere o oggetti dotati di trasponder di prossimità ecc.. APICE offre una vasta gamma di tecnologie di titoli per venire in contro a qualsiasi esigenza di identificazione. E' bene non trascurare che la sicurezza di un sistema dipende anche da quanto può essere difficile clonare le credenziali di accesso contenute in un titolo.

Identificatori: Sono dispositivi come tastiere per digitare i codici PIN o lettori di tessere che convertono le credenziali di accesso in segnali digitali che sono inviate ai terminali di controllo accessi.



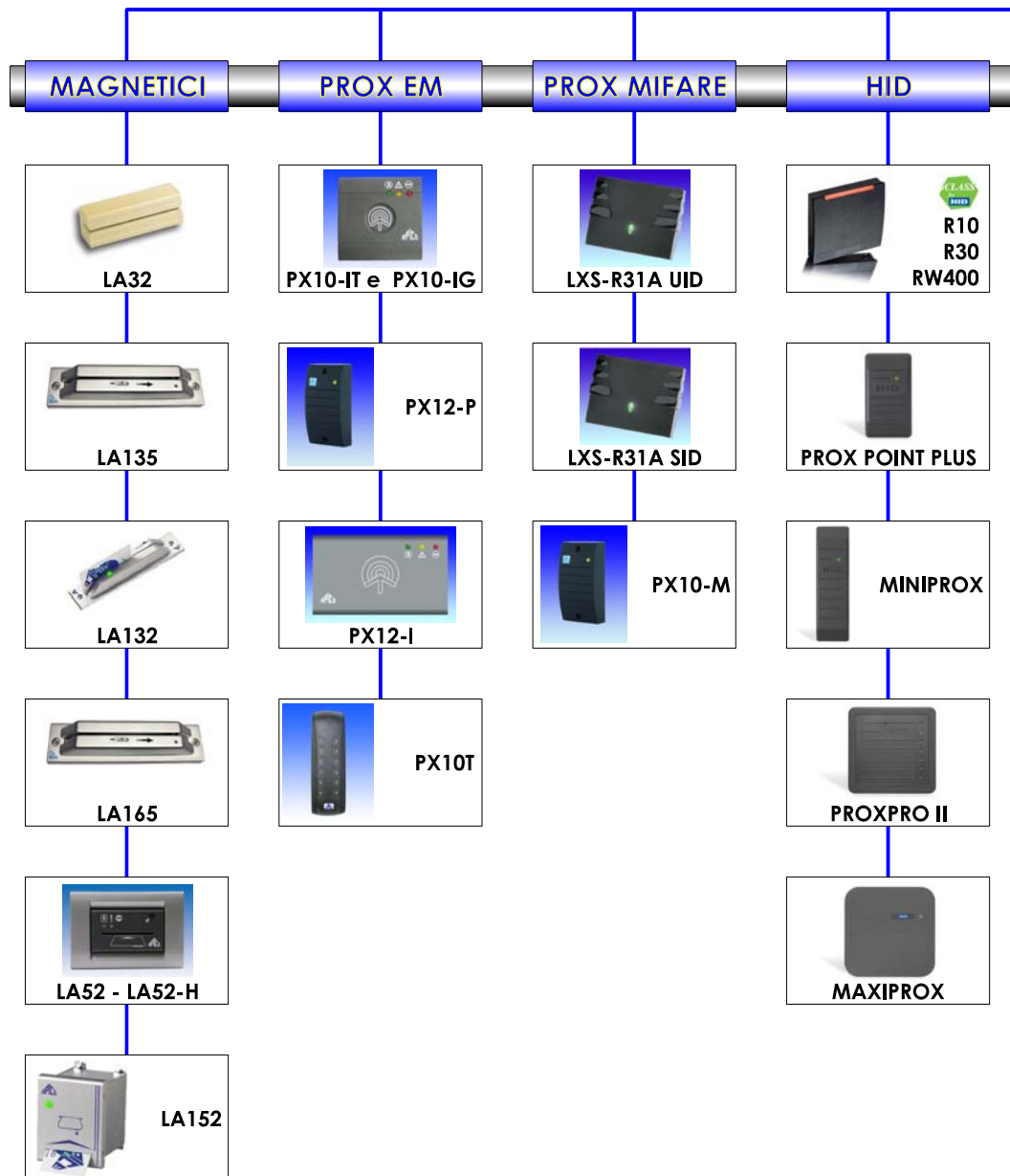
- Terminale:** Dispositivo che riceve un segnale digitale da un identificatore e che è in grado di concedere o negare l'accesso in base a tutta una serie di criteri impostati dall'amministratore del sistema mediante un software di gestione. Il terminale è in grado anche di gestire i segnali elettrici per aprire il varco (ad esempio pilotare una elettroserratura o un automatismo) e per ricevere lo stato del varco (ad esempio da un interruttore magnetico che controlla se la porta è aperta o chiusa).
- Software:** Software di gestione del sistema di controllo accessi che consente di definire le regole di accesso da assegnare agli utenti nei vari varchi, assegnare le credenziali di accesso agli utenti, controllare lo storico dei movimenti, controllare in tempo reale lo stato dei varchi e l'occupazione delle aree, esportare i dati degli utenti e dello storico in formati di database noti come ad esempio i fogli di calcolo excell. Il software gira su un PC o su un server, in funzione delle esigenze del cliente. Quando il software gira su un server ci sono solitamente una serie di applicazioni client che funzionano su altri PC della rete.
- Infrastruttura:** Componenti necessari al collegamento in rete di tutti i terminali del sistema con il server o PC che contiene il software di supervisione. Il sistema di controllo accessi APICE utilizza una infrastruttura di rete standard EN14908 e può essere naturalmente utilizzata anche per dispositivi di altre marche.

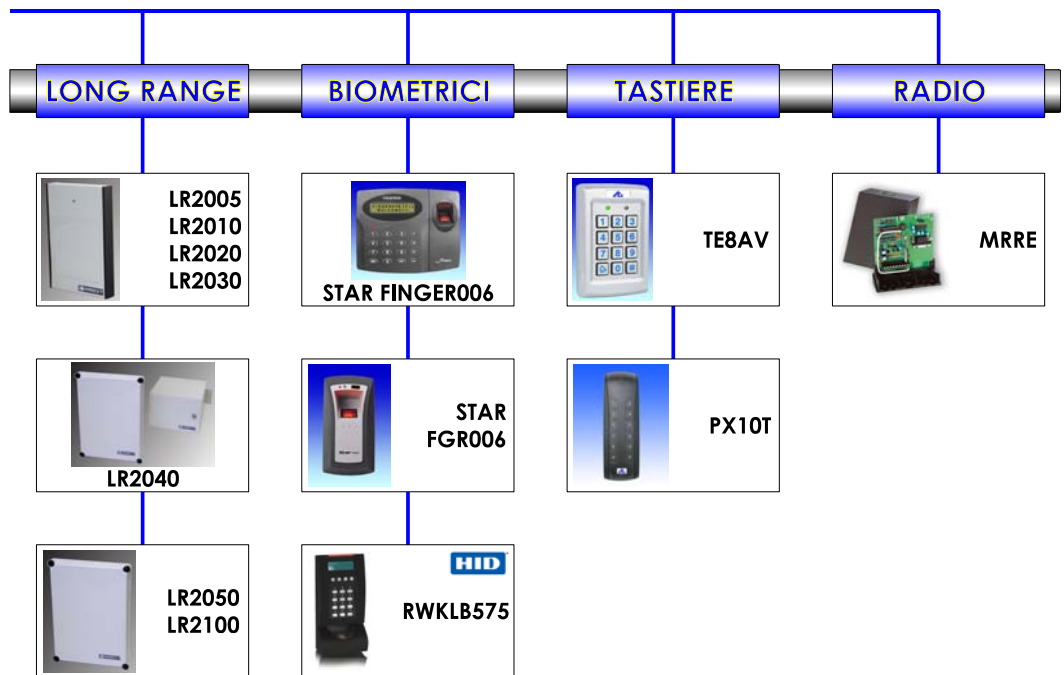
Si noti come il sistema si estende in maniera orizzontale lungo la rete EN 14908, senza che sia interposta tra il server (o PC) di gestione e i terminali, alcuna centrale o convertitore di protocollo.

La rete ethernet esistente è utilizzata anche come infrastruttura di rete EN14908.

Tecnologia dei titoli e degli identificatori

Il catalogo controllo accessi APICE offre un'ampia gamma di possibilità di tecnologia per titoli ed identificatori in modo da venire in contro a qualsiasi esigenza. Qui di seguito riassumiamo le caratteristiche principali di ciascuna tecnologia, per maggiori dettagli si rimanda al catalogo APICE.





Banda magnetica: Ha la necessità di un contatto col lettore, quindi c'è un'usura meccanica di quest'ultimo. Il titolo ha un costo molto basso. Il titolo è clonabile con una modesta attrezzatura.

Trasponder di prossimità EM: Come tutte le tecnologie di prossimità, ha il vantaggio di non richiedere il contatto col lettore. Funziona alla frequenza di 125 KHz i titoli si possono reperire nelle varie forme (carta, portachiavi, stick adesivo, orologio...). E' una tecnologia molto utilizzata, il titolo ha un costo relativamente basso, è clonabile con l'attrezzatura di duplicazione delle chiavi delle automobili o con apparecchiature tipo il nostro TAG-CODER.

Trasponder di prossimità HID PROX: E' un trasponder che funziona a 125 KHz, difficilmente clonabile perché richiede una apparecchiatura particolare che normalmente viene venduta solo ai partner di HID. Costa più del tipo EM, si trova sotto forma di carta, stick adesivo o portachiavi. Ha il vantaggio di offrire una buona gamma di lettori con distanza di riconoscimento anche di 50 centimetri.



Trasponder di prossimità MIFARE: Funziona con lo standard ISO 14443A e lavora alla frequenza di circa 13 MHz che consente di scambiare una mole di dati maggiore delle tecnologie a 125 KHz. E' un trasponder che ha il vantaggio di avere un'area di memoria protetta che ne impedisce la clonazione. Per sfortuna non esiste uno standard specifico per il controllo accessi e, di conseguenza, abbiamo notato che l'80% di queste applicazioni si limitano ad utilizzare come credenziale il serial number del trasponder, anziché un dato scritto nella memoria protetta. Rispetto alle tecnologie precedenti ha il vantaggio di essere una tessera multi-servizi (può essere utilizzata per applicazioni diverse, come borsellino elettronico ecc..) e come controllo accessi, con il limite nella sicurezza spiegato sopra. Consigliamo di utilizzare questa tecnologia per il controllo accessi solo quando le carte MIFARE sono già in dotazione degli utenti per altri servizi, ma non usarle per una nuova proposta.

Trasponder di prossimità i.class: E' un'evoluzione della precedente tecnologia, funziona secondo lo standard ISO 14443B ed è una carta multiservizi che funziona alla frequenza di circa 13 MHz. Le credenziali di accesso risiedono in una locazione specifica nella memoria protetta e diventano praticamente non clonabili. Per elevare il grado di sicurezza i dati tra il lettore e il trasponder vengono scambiati in maniera criptata e solo dopo una mutua³ autenticazione dei dispositivi (lettore e titolo). I titoli sono disponibili con vari tagli di memoria (2K, 16K, 32K) e in diversi formati (Carta, portachiavi). Le sue caratteristiche la rendono la carta multiservizi e di controllo accessi del futuro. Da preferire quindi alla MIFARE per nuove proposte.

Trasponder a lunga distanza: Sono trasponder che riescono ad essere identificati fino ad una distanza di 10 metri, adatti soprattutto per controlli accessi veicolari oppure a mani libere.

Lettori biometrici: Normalmente sono lettori di impronta digitale che consentono di elevare il grado di sicurezza della identificazione. In genere si utilizzano in abbinamento ad un'altra credenziale di accesso, come un titolo o un codice PIN. L'identificazione solo biometrica è sconsigliabile, non ha dato fino ad adesso risultati soddisfacenti in termini di sicurezza, soprattutto quando gli utenti autorizzati all'accesso superano le 50 unità.

Tastiere: Si utilizzano per digitare un codice PIN. Tenere presente che l'identificazione con solo codice è la più bassa in termini di sicurezza e deve essere utilizzato un rapporto tra i codici totali e quelli abilitati di almeno 100:1

³ Mutua: Reciproca. Il lettore si assicura della autenticità della carta e la carta fa lo stesso del lettore.



Radiocomandi: Sono radiocomandi codificati, ciascun trasmettitore ha un proprio codice identificativo e la trasmissione dei dati è protetta dalla clonazione da un meccanismo di tipo rolling-code. Si utilizzano normalmente per accessi veicolari ed hanno una portata di 30...50 metri, tipica dei normali trasmettitori per telecomandi. Non sono direzionali.

Terminali

I terminali hanno in comune il fatto che sono collegati alla rete di comunicazione EN14908 e possiedono intelligenza locale per svolgere delle funzionalità. Essi si dividono in cinque categorie:

- Terminali per controllo varco (IOL222 e IOL332)
- Terminale per gestione database (LonServer)
- Terminale per gestione antipassback. (APB Manager)
- Terminale identificatore, con lettore, tastiera e display. (JLon)
- Terminale per gestione differenziata livelli di sicurezza.

Solo i primi due tipi di terminali sono indispensabili alla realizzazione di un sistema di controllo accessi, gli altri sono utilizzati per espandere le funzionalità del sistema in maniera modulare e orizzontale⁴.

⁴ Espansione orizzontale: Il cablaggio della rete è unico, non ci sono terminali che, una volta connessi alla rete principali fanno dipartire a sua volta una sottorete dove connettere altri terminali. Tutti i terminali sono connessi sulla medesima rete ed allo stesso livello, essa quindi è unica ed ha una struttura 'piatta'.

Terminali per controllo varco IOL222 e IOL332

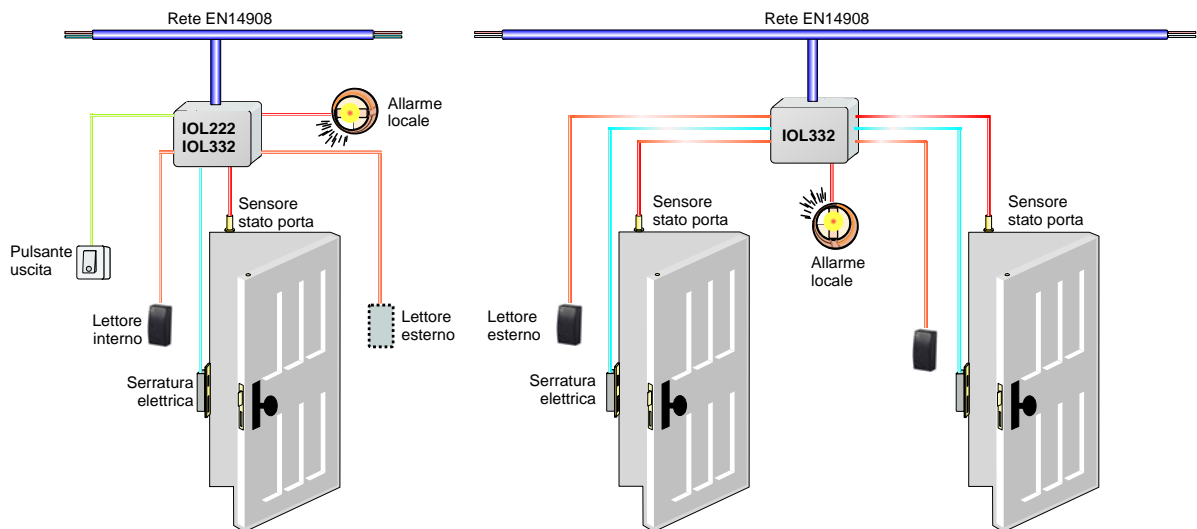


APICE propone due tipi di terminali: IOL222 e IOL332. Il primo può gestire una sola porta e gli identificatori con uscita ISO clock/dati, mentre il secondo può gestire anche due porte e gli identificatori sia con uscita ISO clock/dati, sia con uscita wiegand, ovvero tutta la gamma offerta da APICE.

Ciascun varco del sistema richiede che sia installato un terminale di questo tipo (oppure un terminale per ogni due porte se l'identificatore è solo dal lato di entrata).

Il terminale possiede gli ingressi e le uscite per interfacciare le apparecchiature del varco (esempio l'uscita per la serratura e l'ingresso per segnalare lo stato della porta). Va installato dal lato a maggior sicurezza in modo da evitare sabotaggi.

Il terminale di controllo varco gestisce in maniera autonoma tutte le logiche di controllo del varco, come ad esempio il tempo di eccitazione dell'elettroserratura e gli allarmi.

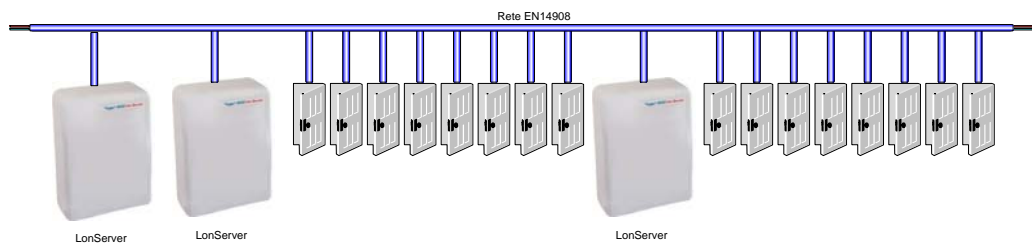


Terminale per gestione database LonServer

E' un terminale che si connette sulla rete di comunicazione e gestisce il database degli utenti abilitati su 8 porte. Di conseguenza ogni 8 porte controllate dal sistema, è necessario installare un terminale di questo tipo.

Da un punto di vista fisico si installa in qualsiasi punto della rete EN14908, tipicamente in maniera distribuita e in un'area prossima alle 8 porte da controllare. Talvolta i LonServer sono anche concentrati in un unico quadro e questo dipende dalle dimensioni dell'impianto e dalle esigenze dell'installazione.

Ciascun LonServer gestisce un database di 26.000 utenti e di 4.000 eventi, nonché fasce orarie, date di scadenza, giorni festivi e altre impostazioni e gestisce in maniera autonoma i meccanismi di antipassback che coinvolgono le 8 porte da esso controllate.



Terminale per gestione antipassback APBManager



Quando i meccanismi di antipassback hanno interazioni tra porte il cui database è gestito da LonServer diversi, si deve ricorrere a una delle due seguenti soluzioni:

- 1) Tenere il software di gestione sempre attivo sul server
- 2) Installare un APB manager in modo che il funzionamento del sistema sia indipendente dal funzionamento del server.

APBManager si installa in un punto qualsiasi della rete EN14908 ed è in grado di coordinare in tempo reale l'interazioni di antipassback tra i database di 10 LonServer diversi.

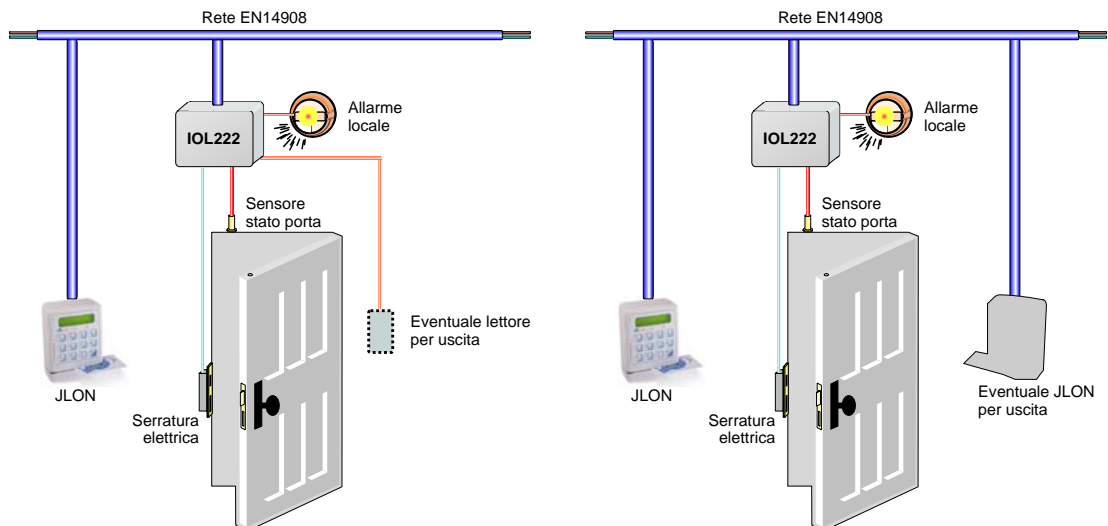
Terminale identificatore JLON



Terminale dotato di lettore di tessere per varie tecnologie (carta magnetica, lettore di prossimità EM, HID, MIFARE ...) da collegare direttamente alla rete EN14908.

Funziona come punto di identificazione evoluto e permette l'accesso con solo PIN, sola tessera o tessera + PIN in funzione della programmazione del sistema.

Ne può essere installato uno per porta (solo ingresso o solo uscita) oppure due per porta (ingresso e uscita).



Terminale per gestione differenziata livelli di sicurezza



Il sistema di controllo accessi funziona in modalità di default in media sicurezza. Questo terminale consente di modificare i livelli di sicurezza del sistema di controllo accessi in maniera dinamica, e automatizzare alcune funzioni come l'inserimento e disinserimento del sistema d'allarme, lo spegnimento delle luci e dell'impianto termico.

Normalmente si utilizza un dispositivo per ciascuna zona, dove questa è gestita da un LonServer.

Nota per identificazione tessera + PIN

Quando è necessaria una identificazione tessera + PIN, oltre alla possibilità di ricorrere ad un terminale di identificazione evoluto come JLON, si può connettere al terminale IOL332 un lettore con tastiera incorporata, anziché un semplice lettore.

Sono disponibili lettori + tastiera per trasponder EM e HID PROX e i.CLASS.



Per trasponder EM



Per PROX HID



Per i.CLASS HID

Software di controllo accessi (AxWin)



E' un potente software di controllo accessi che nasce dalla più che decennale esperienza e specializzazione principale di APICE. Funziona con i sistemi operativi Windows 2000 e Windows XP e non richiede un PC appositamente dedicato. Quando AxWin è in funzione, scarica automaticamente gli eventi dalla memoria dei LonServer e invia a quest'ultimi qualsiasi variazione sui diritti di accesso degli utenti che vengono eseguite dall'operatore.

La comunicazione tra AxWin e i LonServer avviene in sottofondo e in maniera del tutto automatica in modo che l'operatore del software non deve preoccuparsi di fare alcuna operazione manuale per garantire l'allineamento. Vedere la documentazione specifica di AxWin per approfondimenti. Grazie al modulo di portineria è possibile gestire gli accessi dei visitatori, il rilascio a questi dei badge e la compilazione automatica del registro delle visite. Principali caratteristiche:

- Gestione diretta dei LonServer
- Archivio utenti, tessere, ditte, fasce orarie, giorni festivi, presenti, livelli di accesso, tipologie di utenti e numerose altre impostazioni.
- Visualizzazione, ricerca, stampa ed esportazione dei movimenti in formato excell.
- Stampa diretta del badge anche con nome, cognome e fotografia ripresa direttamente da web-cam USB.
- Esportazione dei movimenti per software di gestione presenze/paghe.
- Apertura manuale delle porte.
- Funzioni di diagnostica e di utilità.
- Procedure automatiche di backup e recupero archivi.
- Modulo aggiuntivo per la gestione dei visitatori.
- Moduli client per avere più postazioni di lavoro.

Esempi di utilizzo di AxWin

La portineria lo può utilizzare per la registrazione dei visitatori ed il rilascio del badge. AxWin gli snellisce il lavoro in quanto registra i visitatori abituali, semplifica le operazioni di rilascio e di ritiro del badge utilizzando un lettore locale e riempie automaticamente il registro delle visite.

L'addetto alla security può generare qualsiasi livello di accessi desiderati ed assegnarlo a ciascun utente del sistema in modo da restringere l'accesso di persone in aree in cui non sono autorizzati. Inoltre, grazie alla registrazione di tutti gli eventi, c'è un completo controllo sui movimenti fatti dalle persone nella struttura, nel presente e nel passato.

L'ufficio paghe può estrapolare i dati delle timbrature effettuate sul sistema dagli orologi marcatempo, oppure confrontare i dati dell'acquisizione delle timbrature con quelli degli accessi per controlli incrociati.

L'ufficio acquisti può far calcolare dal sistema i tempi di permanenza all'interno della struttura dei lavoratori di ditte esterne per verificare la fatturazione della manodopera.

Il responsabile della safety può conoscere in caso di emergenza le persone all'interno di un'area che deve essere evacuata.

Infrastruttura di rete

L'infrastruttura di rete utilizzata per il controllo accessi è standard EN14908 e può essere condivisa con qualsiasi altra apparecchiatura che funziona sul medesimo standard, anche se d'altro costruttore.

La rete è costituita da un doppino twistato, può essere utilizzata una coppia del cavo UTP cat V.

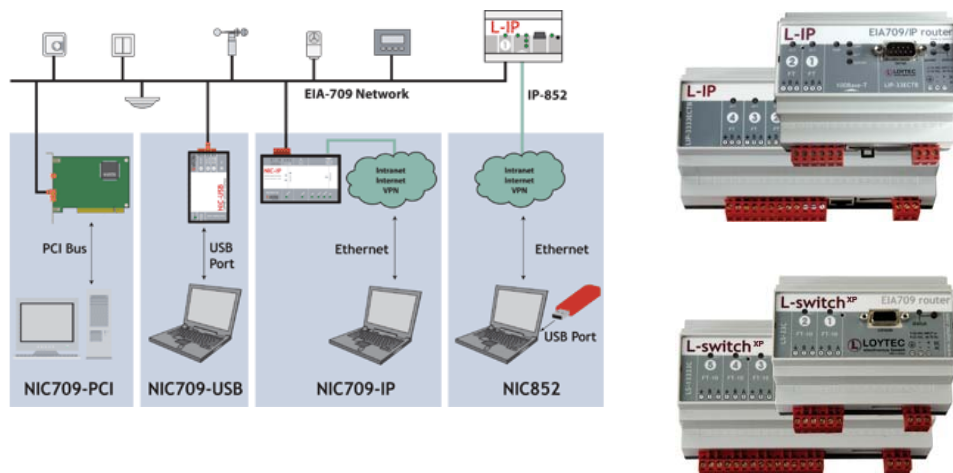
I terminali APICE funzionano con interfaccia di rete certificata del tipo FTT-10 (EN14908.2 – ANSI/EIA 709.3).

Il cablaggio del doppino di rete può essere a tipologia libera o a bus⁵.

L'infrastruttura di rete Ethernet esistente nell'edificio, può essere utilizzata come dorsale per la comunicazione della rete EN14908, diventandone parte integrante (EN14908.4 – ANSI/EIA 852).

Una rete piccola⁶ necessita di una sola interfaccia di rete per connettere il PC ai terminali, una rete più estesa necessita di router per amplificare il segnale ed isolare il traffico locale nelle singole sottoreti. Ciascuna sottorete può collegare fino a 64 terminali con un cablaggio massimo a bus di 900 metri oppure 450 metri se in tipologia libera⁷.

Nel catalogo di building automation APICE si possono trovare tutti i componenti necessari per realizzare una infrastruttura di rete EN14908.



⁵ Cablaggio a BUS: Una linea che ha un inizio e una fine e che connette i dispositivi senza effettuare derivazioni.

⁶ Con meno di 64 dispositivi e con lunghezza di cavo inferiore alle massima capacità di una sottorete.

⁷ Dati riferiti al cavo UTP cat V. 450 metri in tipologia libera = lunghezza totale del cavo steso, sempre in tipologia libera la massima distanza tra due terminali non deve superare i 200 metri.

APICE s.r.l.

Via G.B. Vico 45/B

50053 EMPOLI FI

Tel +39 05 71 92 04 42

Fax +39 05 71 92 04 74

Web: www.apice.org

e-mail: apice@apice.org