

TecnoRS

Ricerca e Sviluppo di Innovazioni Tecnologiche

TecnoaXess© – Manuale Utente



Sistema di controllo accessi TecnoaXess by TecnoRS



Manuale di Uso e manutenzione

Indice

1	Generalità	5
1.1	Dichiarazione di conformità	5
1.2	Premessa	6
1.3	Simbologia.....	7
1.4	Descrizione del dispositivo	7
1.5	Richiesta di assistenza	8
1.6	Caratteristiche tecniche del terminale	8
1.7	Dimensioni meccaniche.....	9
1.8	Istruzioni per la richiesta di intervento di assistenza	9
1.9	Elenco ricambi ed accessori.....	9
1.10	Garanzia	9
2	Prescrizioni di sicurezza	10
2.1	Usi non consentiti	10
2.2	Normativa	10
2.3	Prescrizioni d'uso	10
3	Collegamenti e descrizione del prodotto.....	10
3.1	Fissaggio del terminale.....	11
3.2	Collegamento e installazione del terminale	11
3.2.1	Collegamento alla linea di alimentazione	13
3.2.2	Collegamento delle uscite a relay	14
3.2.3	Collegamento del bus esterno rs232.....	15
3.2.4	Collegamento degli ingressi di supervisione	17
3.2.5	Collegamento del terminale su bus Wiegand.....	18
3.2.6	Collegamento dell'interfaccia RS422 su bus di trasmissione dati	20
3.2.7	Collegamento del terminale su rete LAN.....	26
3.2.8	Collegamento del terminale su rete WiFi	28
4	Configurazione del terminale	29
4.1	Configurazione seriale del terminale	29
4.2	Configurazione mediante messaggi dal server	33
4.3	Riepilogo parametri di configurazione	34
4.4	Configurazione dell'interfaccia WiFi	35
4.5	Configurazione dell'interfaccia Ethernet PoE	38
5	Uso del dispositivo	42
5.1	Terminale Presenze	42
5.1.1	Descrizione terminale	42
5.1.2	Indicazioni del display	42
5.1.3	Utilizzo dei tasti Ingresso / Uscita.....	43
5.1.4	Utilizzo del lettore RFID.....	44
5.1.5	Gestione delle fasce orarie.....	44
5.1.6	Gestione della sirena di inizio/fine turno.....	45
5.2	Terminale accessi.....	46
5.2.1	Descrizione del terminale	46
5.2.2	Indicazione del display	46
5.2.3	Utilizzo del lettore RFID.....	47
5.2.4	Definizione delle politiche di accesso.....	47
5.2.5	Gestione dell'anti pass-back	49
5.2.6	Gestione della supervisione dell'accesso.....	50

1 GENERALITÀ

1.1 DICHIARAZIONE DI CONFORMITÀ

DICHIARAZIONE DI CONFORMITÀ'

Nome del fabbricante: **TecnoRS s.r.l.**

Indirizzo: Via XXV Aprile
Z.I. Pietrarossa
06032 Trevi (PG)
Italy

Dichiara che il prodotto:

Dispositivo elettronico: **TecnoaXess**

Con opzioni: tutte quelle previste dal presente manuale

è conforme a:

- Norme EN61000-6-1:2001 e EN61000-6-3:2001 in base a quanto previsto dalle direttive 2004/108/CE (compatibilità elettromagnetica)
- Norme EN300 328-2 v1.2.1 in base a quanto previsto dalla direttiva R&TTE (equipment operating the 2,4 GHz ISM band)
- Norme EN60950-1:2006 Safety Information technology equipment in base alla direttiva 73/23 CEE (bassa tensione)

Sul prodotto è stata apposta la marchiatura CE.

Trevi, 15 aprile 2008

Il Legale Rappresentante

Vincenzo Saracini

1.2 PREMESSA

Il presente manuale è il documento di riferimento per l'installatore e utilizzatore del terminale in cui sono presenti informazioni per l'installazione, uso e manutenzione del terminale. Data la presenza di più versioni del terminale che si differenziano in termini di funzionalità e di installazione, il presente manuale sarà diviso in più sezioni, una per ogni modello e in una sezione introduttiva in cui verranno descritte le caratteristiche comuni a tutti i modelli.

In ogni caso occorre fare riferimento a quanto segue per un corretto uso del terminale:

- ✓ Scopo del presente manuale è di portare a conoscenza dell'operatore con testi e figure di chiarimento, le prescrizioni ed i criteri fondamentali per l'installazione, il corretto impiego in sicurezza del dispositivo nelle sue modalità di funzionamento.
- ✓ Tenere sempre a portata di mano il presente manuale! Rispettare sempre le istruzioni riportate!
- ✓ La sicurezza di funzionamento del dispositivo affidata in prima persona all'operatore che riteniamo debba avere conoscenze dettagliate su di esso.
- ✓ E' responsabilità dell'utente assicurarsi che l'installazione sia conforme alle disposizioni vigenti in materia.
- ✓ L'apparecchiatura deve essere installata solo da personale specializzato che deve aver letto e compreso il presente manuale.
- ✓ Con "**personale specializzato**" si intende personale che, in seguito alla formazione ed esperienza professionale maturata, è stato espressamente autorizzato dal "Responsabile alla sicurezza dell'impianto" ad eseguirne l'installazione, l'uso e la manutenzione.
- ✓ E' vietato qualsiasi tentativo di smontaggio, modifica e manomissione del dispositivo da parte dell'utente o personale non autorizzato; in tal caso decade immediatamente la garanzia e la TecnoRS si esime dal rispondere ad ogni eventuale danno causato a persone o a cose.
- ✓ La TecnoRS non risponde di danni derivanti da una incauta movimentazione del dispositivo.
- ✓ Le informazioni e le illustrazioni di seguito riportate sono aggiornate alla data di edizione.
- ✓ La TecnoRS è impegnata nella continua ottimizzazione dei propri prodotti con conseguenti possibili modifiche a qualche componente del dispositivo, sia hardware che software.
- ✓ Tutte le informazioni tecniche contenute nel presente manuale sono di esclusiva proprietà della ditta costruttrice e devono essere considerate di natura riservata.
- ✓ E' vietata la riproduzione e divulgazione, anche parziale, del presente manuale su carta, su supporto informatico e su WEB senza autorizzazione scritta della TecnoRS.
- ✓ Inoltre è vietato utilizzare il presente manuale per scopi diversi da quelli strettamente legati all'installazione, all'utilizzo e alla manutenzione del dispositivo.

1.3 SIMBOLOGIA

Di seguito si riportano le simbologie utilizzate nel manuale per richiamare l'attenzione del lettore sui diversi livelli di pericolo nelle operazioni di "Uso e manutenzione" dello strumento.



PERICOLO

Informazione o procedura che, se non scrupolosamente eseguita, provoca la morte o gravi lesioni personali.



ATTENZIONE

Informazione o procedura che, se non scrupolosamente eseguita, potrebbe causare modeste lesioni personali o danni al dispositivo.



AVVERTENZA

Informazione o procedura che consiglia l'operatore sull'utilizzo ottimale dell'impianto per allungarne la durata, evitarne danneggiamenti o perdita della programmazione, ottimizzarne il lavoro nel rispetto delle normative metriche.

Le schermate ed i messaggi che compaiono sul display del terminale sono riportati in un carattere speciale.

Per i messaggi adotteremo la seguente simbologia:

"Questo è un messaggio riportato sul display."

1.4 DESCRIZIONE DEL DISPOSITIVO

Il terminale TecnoaXess è un dispositivo nato e progettato per implementare un sistema di controllo accessi innovativo che offre oltre alle soluzioni standard, già presenti nel campo dei controlli accessi, anche soluzioni innovative sia in termini di interfacce di connessione lato server che in termini di interfaccia utente avendo un display grafico 64x128 pixel in grado di adattarsi al design dell'ambiente che lo ospita. E' possibile inoltre richiedere eventuali personalizzazioni che l'integratore vuole customizzare sulle specifiche del cliente.

Le principali caratteristiche che lo contraddistinguono si possono elencare come:

- ✓ Funzionamento stand-alone (senza collegamento al server) sia in termini di politiche di accesso che di memorizzazione transiti gestendo un numero teoricamente illimitato di card e memorizzando in locale fino a 5460 transiti espandibili a richiesta.
- ✓ Gestione delle politiche di accesso con un massimo numero di gruppi pari a 1000 e un massimo numero di politiche memorizzabili nel terminale pari a 1000.
- ✓ Display Grafico 64x128 pixel con possibilità di personalizzazione della schermata principale o logo aziendale; il display è disponibile con retroilluminazioni nelle colorazioni blu, giallo, grigio, o nelle combinazioni RGB desiderate.

- ✓ Lettura di card RFID operanti alla frequenza di 13,56MHz nel formato più comune come MIFARE (ISO 14443 A/B) ed opzionalmente è possibile avere la possibilità di utilizzo di card del tipo I-CODE2 (ISO 15693).
- ✓ Possibilità di scelta tra le interfacce di trasmissione dati quali Wiegand, RS422, USB, WiFi e Ethernet con possibilità di alimentazione tramite cavo LAN (PoE – Power over Ethernet).
- ✓ Possibilità di utilizzo di batteria tampone al Litio per un'elevata autonomia.
- ✓ Gestione fino a 15m di antenne di ribattuta da esterno IP65.
- ✓ Chassis plastico con design proprietario e colori personalizzabili.
- ✓ Due relay interni per la gestione completa di varchi in termini di gestione di serrature elettriche e di sirene o lampeggianti di allarme.
- ✓ E' dotato di 3 ingressi analogici bilanciati per la supervisione di contatti reed e pulsanti di emergenza per la supervisione completa dei varchi.
- ✓ Gestione di due livelli di anti pass-back.
- ✓ Possibilità di implementazione della gestione di ingressi a scalare.
- ✓ Compatibilità con altri sistemi di controllo accessi su bus Wiegand (26bit e 34 bit)
- ✓ Possibilità di integrazione su sistemi di controllo accessi su protocollo di comunicazione lato server.

1.5 RICHIESTA DI ASSISTENZA

In caso di anomalie di funzionamento o di guasti per i quali è necessario l'intervento di tecnici specializzati rivolgersi all'installatore o al rivenditore del sistema.

1.6 CARATTERISTICHE TECNICHE DEL TERMINALE

Tensione di alimentazione:	12 ÷ 24 Vdc
Consumo massimo:	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Dimensioni (HxLxP):	10 cm x 16,5 cm x 9 cm
Contenitore	ABS (plastico) con colori personalizzabili
Range di temperatura di stoccaggio:	- 40°C ÷ + 150 °C
Range di temperatura di funzionamento:	- 10°C ÷ + 85 °C
Umidità:	85% @ 40 °C (non condensante)
Grado di protezione:	IP 54
Standard card RFID	ISO14443A/B (MIFARE) (I-CODE2 opzionale)
Distanza di lettura card	3 ~ 6 cm (*)
Uscite a relay	2 relay con contatti NO (2A @ 24V)
Ingressi di supervisione	3 ingressi analogici.
Display grafico	64 x 128 pixel, blu/giallo/grigio/RGB
Segnalazione sonora	Buzzer interno
Interfacce di trasmissione dati	- USB (programmatore di card RFID) - WiFi (802.11b/g, WEP 64/128bit,WPA,AES) - Ethernet LAN (alimentazione tramite PoE) - Wiegand (26bit/34 bit specification) - RS422 (9600 bps 8N1 – non fotoaccoppiato) - RS422 versione con fotoaccoppiatori
Distanze di trasmissione dati	Vedere sez relative alle interfacce di trasmis.

Cap. di memorizzazione transiti	5460 (espandibile a richiesta)
Massimo numero di gruppi di accesso gestiti	1000
Massimo numero di regole di accesso gestite	1000
Massimo numero di card bloccabili	100
Gestione anti pass-back	Nessuno, Hard, Soft
Batteria tampone al litio	Opzionale
Durata della batteria tampone	Dipendente dalla configurazione.
Gestione antenna di ribattuta	Su bus RS232.
Distanza massima antenna di ribattuta	~ 15 m
Configurazione terminale	RS232, interfacce di comunicazione

(*)La distanza di lettura può dipendere dalla tecnologia di fabbricazione della card e dalle sue dimensioni.

1.7 DIMENSIONI MECCANICHE

1.8 ISTRUZIONI PER LA RICHIESTA DI INTERVENTO DI ASSISTENZA


In caso di anomalie di funzionamento o di guasti per i quali è necessario l'intervento di tecnici specializzati rivolgersi all'installatore del sistema o al rivenditore. Per una più veloce risoluzione dei problemi comunicare il serial number dello strumento che compare sull'etichetta di bollatura. Comunicare inoltre le caratteristiche del sistema in cui è installato il terminale.

1.9 ELENCO RICAMBI ED ACCESSORI

Descrizione	Codice
Scheda relay/connessione	TRS0030002
Scheda backpanel + display	TRS0030001
Scheda di connessione RS422 non fotoacc.	TRS0030005
Scheda di connessione RS422 fotoaccoppiata	TRS0030010
Scheda di connessione Ethernet LAN	TRS0003
Scheda di connessione WiFi (802.11b/g)	TRS0030003
Antenna di ribattuta ISO14443A/B (MIFARE)	TRS0090
Modulo RFID ISO14443A/B (MIFARE)	TRS0030009
Batteria tampone al Litio	BT1LTI07V2001
Contenitore TecnoaXess completo	TRS0030006
Card RFID MIFARE 512K	
Cavo di programmazione seriale	TRS0030011

1.10 GARANZIA

Le clausole di garanzia sono quelle specificate nel contratto di vendita.

 <p>TecnoRS Ricerca e Sviluppo di Innovazioni Tecnologiche</p>	<p align="center">MANUALE UTENTE MANUALE USO E MANUTEZIONE TERMINALI TECNOAXESS</p>	<p>Rev.N. 00 del 14/04/2008 Pagina 10</p>
--	--	---

2 PRESCRIZIONI DI SICUREZZA

2.1 USI NON CONSENTITI

Il dispositivo è un prodotto progettato per assolvere esclusivamente le funzioni prescritte all'interno del presente manuale.

- ✓ E' vietato utilizzare il dispositivo da personale non specializzato.
- ✓ E' vietato utilizzare il dispositivo per il controllo esclusivo di uscite di emergenza.
- ✓ E' vietato utilizzare il dispositivo in luoghi con atmosfera potenzialmente esplosiva o in luoghi dove esiste pericolo di incendio.

Altri utilizzi sono consentiti solo se espressamente autorizzati dalla TecnoRS.

2.2 NORMATIVA

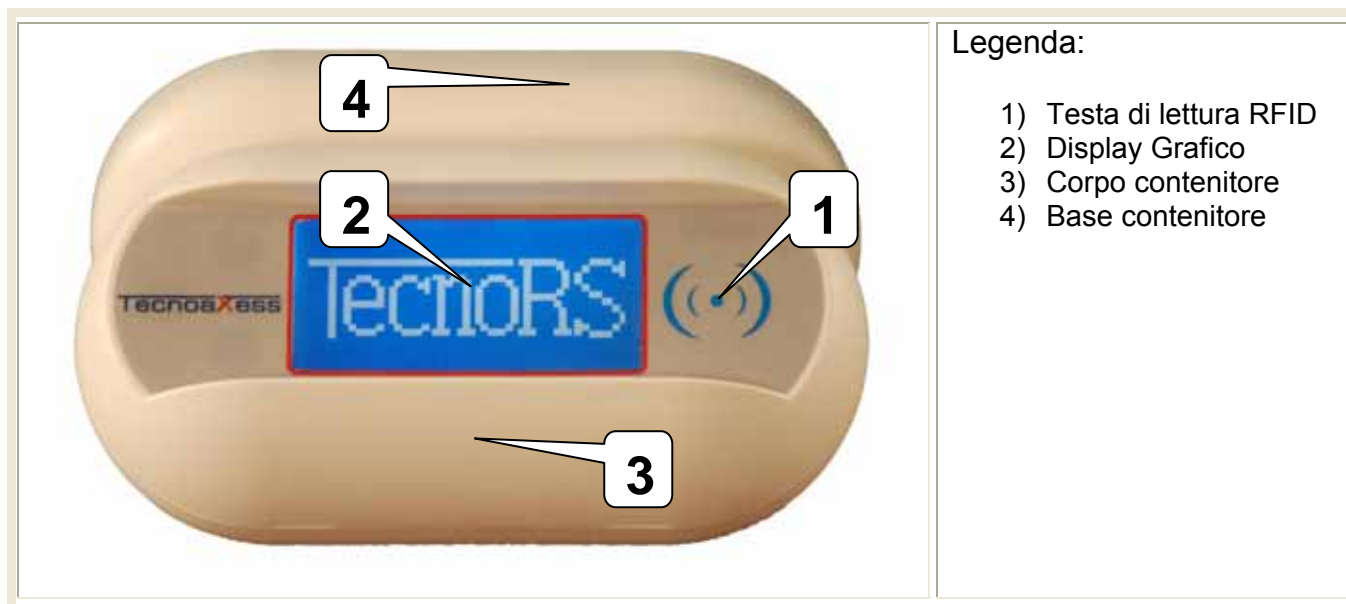
Le condizioni di utilizzo del terminale per controllo accessi sono regolamentate dalle normative in vigore nel paese di utilizzo. Il soggetto installatore dovrà garantire il rispetto a tali norme e sono pertanto vietati gli usi in condizioni non conformi a tali norme.

2.3 PRESCRIZIONI D'USO

- ✓ Durante l'uso seguire scrupolosamente il presente manuale.
- ✓ Nel caso si riscontrino discordanze tra quanto descritto all'interno del presente manuale e l'apparecchiatura in Vs. possesso, chiedere chiarimenti al vostro Rivenditore o al Servizio Post-Vendita della TecnoRS.
- ✓ Assicurarsi che il terminale sia completo di tutti i carter di copertura e di protezione e verificare l'integrità dei cavi e la loro corretta connessione.
- ✓ Se il dispositivo deve essere collegato ad altri apparecchi come computer o altro, scollegarli dalla presa elettrica prima di effettuare il collegamento.
- ✓ Ogni intervento di manutenzione e/o riparazione deve essere eseguito esclusivamente da personale autorizzato.

3 COLLEGAMENTI E DESCRIZIONE DEL PRODOTTO

Di seguito viene riportata una rappresentazione del terminale con indicazione delle varie parti così come si presenta all'utente finale una volta installato. Per semplicità si riporta la foto nel caso di installazione su parete, per quanto riguarda la procedura di installazione fare riferimento alla sezione del presente manuale che descrive il particolare modello di interesse.



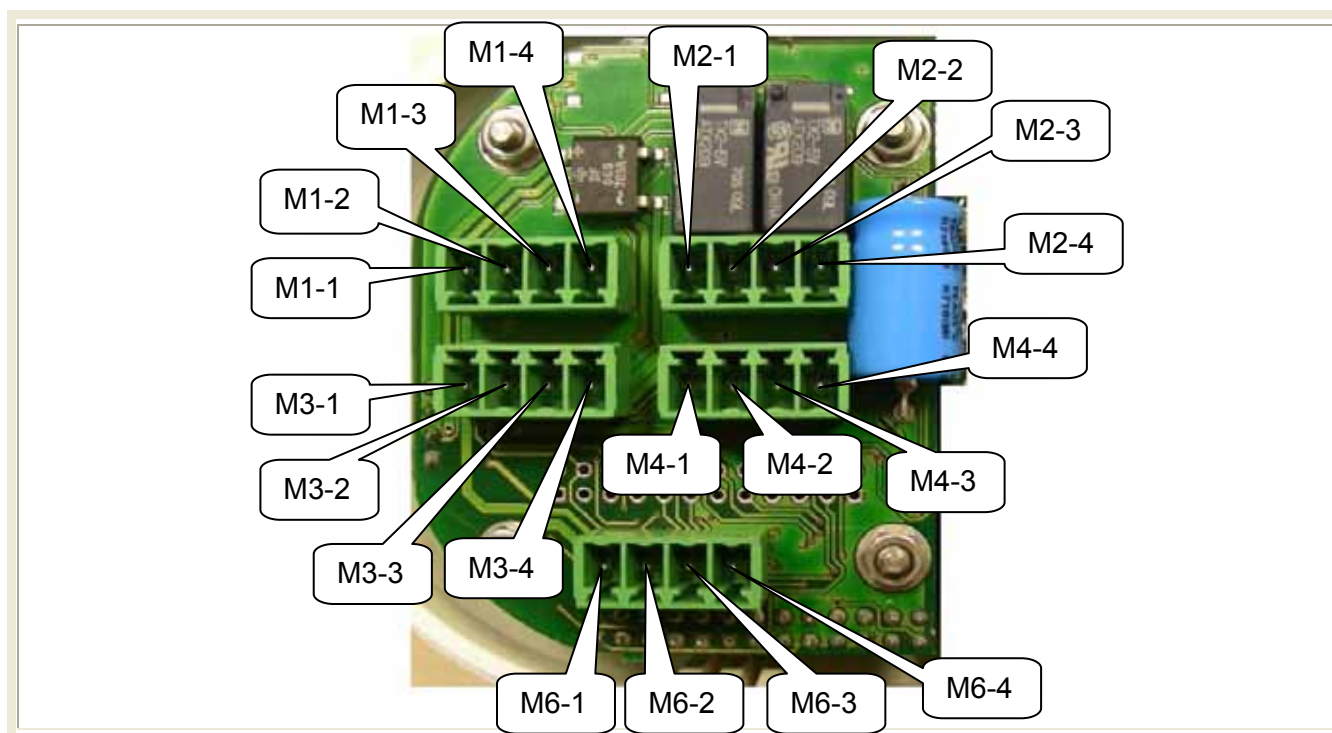
3.1 FISSAGGIO DEL TERMINALE

Per fissare il terminale su una parete verticale seguire le indicazioni riportate di seguito:



3.2 COLLEGAMENTO E INSTALLAZIONE DEL TERMINALE

Di seguito si riporta il layout della scheda connessioni in cui sono alloggiati i morsetti di collegamento del terminale:



Posizione	Funzione	Descrizione
M1-1	Data 0	Bus Wiegand Data 0
M1-2	Data 1	Bus Wiegand Data 1
M1-3	Beeper	Controllo del buzzer interno su bus Wiegand
M1-4	Ground	Massa di riferimento per bus Wiegand
M2-1	C1	Comune Contatto – Accesso Consentito (relay 1)
M2-2	NA1	Contatto Normalmente aperto – Accesso Consentito (relay 1)
M2-3	C2	Comune Contatto – Accesso Negato (relay 2)
M2-4	NA2	Contatto Normalmente aperto – Accesso Negato (relay 2)
M3-1	Led Red	Controllo di segnalazione su bus Wiegand led rosso
M3-2	Led Green	Controllo di segnalazione su bus Wiegand led verde
M3-3	VCC1	Pin1 di alimentazione positiva del terminale (+24V)
M3-4	VCC2	Pin2 di alimentazione negativa del terminale (GND)
M4-1	GND	Massa per ingressi analogici di supervisione SV
M4-2	SV2 (N.O)	Ingresso 2 di supervisione accesso - richiesta di uscita di emergenza
M4-3	SV1 (N.C)	Ingresso 1 di supervisione accesso - contatto reed di apertura porta
M4-4	SV3 (N.O)	Ingresso 3 di supervisione accesso - Ingresso supervisione generico
M6-1	5V	Tensione di servizio 5V (200mA Max)
M6-2	RS232 RX	Pin di ricezione per bus esterno RS232
M6-3	RS232 TX	Pin di trasmissione per bus esterno RS232
M6-4	GND	Riferimento di massa per bus esterno RS232

3.2.1 COLLEGAMENTO ALLA LINEA DI ALIMENTAZIONE



PERICOLO

Verificare che:

- la linea elettrica di alimentazione abbia voltaggio idonea al funzionamento del dispositivo. Tensioni più elevate possono provocare danni a cose o persone oltre che danneggiare irreversibilmente il dispositivo.
- Non vi sia una differenza di potenziale tra la terra della macchina o quadro elettrico e il neutro di alimentazione.

E' possibile alimentare il terminale utilizzando tensione continua. Collegare la linea di alimentazione ai morsetti M3-3 (12V÷24V) e M3-4 (GND) rispettando in ogni caso il range di tensione minima e massima pari a 12 ÷ 24 Vdc. Per un corretto collegamento del terminale procedere nel seguente modo:

- ✓ Effettuare tutti gli altri collegamenti come relay, ingressi ed eventuale rete di trasmissione dati (RS422 o Ethernet non PoE)
- ✓ Estrarre il morsetto e serrare i cavi di alimentazione tra i morsetti corrispondenti a M3-3 e M3-4.
- ✓ Infilare nuovamente il morsetto con i cavi collegati sul connettore M3 della scheda di connessione.

Solo nel caso in cui si utilizza un terminale con interfaccia Ethernet connesso ad un Hub con porte PoE non è necessario la connessione del terminale alla rete di alimentazione.

Il terminale rispetta la normativa sulla compatibilità elettromagnetica ma è tuttavia buona norma tenere separata la linea di alimentazione da quella di potenza.

Nel progetto della linea di alimentazione dei terminali occorre tenere in considerazione la sezione del cavo utilizzato in relazione al numero di terminali collegati sulla stessa tratta e quindi all'assorbimento totale a in relazione alla lunghezza del cavo. Per un corretto dimensionamento si riportano i consumi massimi in ogni configurazione; per ottenere l'assorbimento massimo alla tensione di funzionamento occorre dividere la potenza massima espressa in W per la tensione V:

Configurazione	Consumo massimo
TecnoaXess Ver. RS422	
TecnoaXess Ver. 802.11b/g (WiFi)	
TecnoaXess Ver. Ethernet (no PoE)	
TecnoaXess Ver. Wiegand	



AVVERTENZA

Nel caso in cui si collegano più terminali connessi alla stessa linea di alimentazione tenere in considerazione la sezione dei cavi utilizzati in relazione alla lunghezza della tratta di alimentazione, all'assorbimento totale dei terminali e alla temperatura di esercizio dei cavi stessi.

In ambienti particolarmente rumorosi si consiglia l'uso di cavi schermati.



AVVERTENZA

Nel caso in cui si utilizza un terminale con interfaccia Ethernet con tecnologia PoE (Power over Ethernet) non si deve collegare il terminale alla normale alimentazione.

3.2.2 COLLEGAMENTO DELLE USCITE A RELAY



ATTENZIONE

Prima di procedere al collegamento delle uscite a relay verificare che:

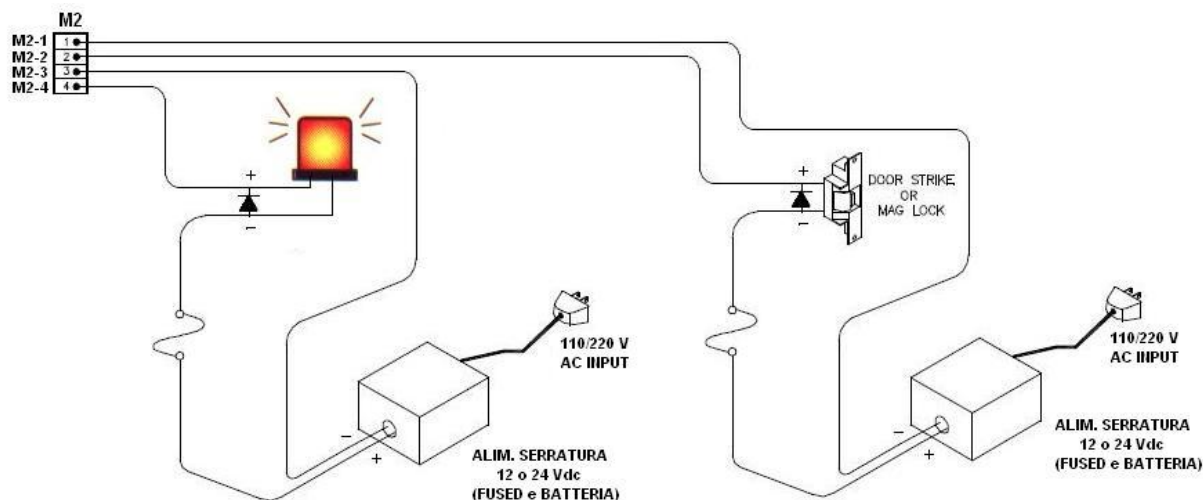
- *le potenze che i relay dovranno commutare non superino le specifiche riportate di seguito*
- *Il terminale sia scollegato dalla linea di alimentazione.*
- *Tutti gli apparecchi connessi al terminale siano scollegati dalla linea di alimentazione.*

Il terminale è dotato di due relay per la gestione completa di un varco. Nelle versioni del TecnoXess esclusa quella Wiegand, è possibile infatti collegare sia l'azionamento della serratura elettrica che viene azionata nel caso in cui l'accesso è consentito che il collegamento di una sirena o lampeggiante che viene attivata nel caso in cui si verifica un accesso negato. Questa seconda opzione è configurabile via software e non sempre potrebbe essere necessaria.

Di seguito si riportano le caratteristiche elettriche dei due relay:

Relay	Morsetti	Caratteristiche elettriche
RL1 – Relay di accesso consentito (azionamenti di accesso)	M2-1 / M2-2	Tensione e corrente nom. 2A – 30Vdc
		Massima Potenza commutabile 60W
		Massima tensione commutabile 220Vdc
		Massima corrente commutabile 2A
		Resistenza di contatto massima 100mΩ
RL2 – Relay di accesso negato (azionamenti di allarmi)	M2-3 / M2-4	Tensione e corrente nom. 2A – 30Vdc
		Massima Potenza commutabile 60W
		Massima tensione commutabile 220Vdc
		Massima corrente commutabile 2A
		Resistenza di contatto massima 100mΩ

Di seguito si riporta una schematizzazione di un possibile collegamento dei due relay:



Come si può vedere dallo schema precedente occorre inserire:

- ✓ Diodo di protezione del tipo 1N4002, 1N4003 e 1N4004 nel caso di serrature elettriche che hanno un'alimentazione in continua. Inserire il catodo del diodo contrassegnato dalla barra bianca sul positivo dell'alimentazione della serratura
- ✓ Un varistore di tipo MOV (metal oxide varistor) nel caso di serrature alimentate a tensione alternata. Scegliere un MOV con una tensione di lavoro maggiore di quella della serratura.
- ✓ Utilizzare alimentatore a 12 o 24Vdc se si vuole connettere direttamente al relay interno del TecnoXess. Se si vuole permettere l'utilizzo del varco in assenza di tensione di rete, utilizzare solo alimentatori con batteria di backup.

Come vedremo in seguito il relay collegato al sistema di allarme è attivato nel caso si voglia supervisionare un varco utilizzando gli ingressi dedicati; in caso di infrazione, ovvero di apertura non autorizzata della porta il terminale rileva una situazione di allarme attivando il relativo relay e comunicando al server la situazione rilevata.



AVVERTENZA

Evitare di utilizzare il terminale come unico sistema di allarme poiché non è progettato per soddisfare le normative tipiche dei sistemi di allarmi. La supervisione dell'accesso è da intendersi come protezione da eventuali accessi non autorizzati.

3.2.3 COLLEGAMENTO DEL BUS ESTERNO RS232



AVVERTENZA

Prima di collegare alcun dispositivo al bus RS232 verificare che il terminale e tutti gli apparecchi ad esso connesso siano scollegati dalla linea di alimentazione.

Il terminale ha la possibilità di essere direttamente connesso ad un PC o un terminale remoto mediante una bus ausiliario di tipo RS232. Esso è utilizzato sia per consentire una più agevole configurazione o manutenzione in fase di installazione; che per il collegamento della antenna di ribattuta (Cod. TRS0090) che come vedremo più avanti nel presente manuale, è un accessorio utile nel caso si voglia monitorare un varco gestendo entrambe le direzioni (ingresso / uscita).

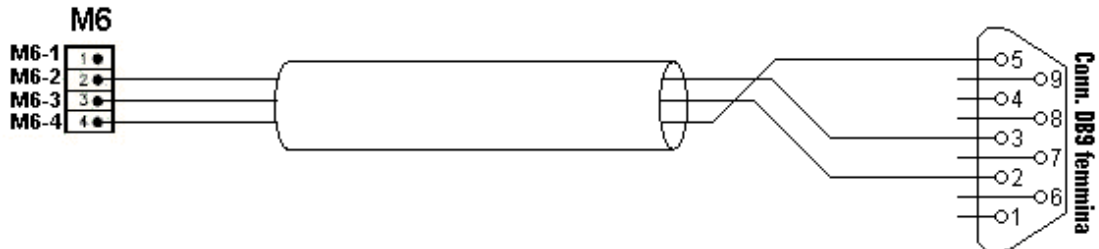


Condizioni di massimo utilizzo previste dallo standard RS232:

- *Massima distanza di trasmissione = 15 m*
- *Massima tensione ai capi = ± 12 Vdc*

Per il collegamento verso dispositivi esterni si consiglia di utilizzare un cavo schermato con l'avvertenza di collegare lo schermo alla parte metallica del guscio del connettore a 9 poli.

Per la connessione del terminale alla porta seriale del PC o terminale utilizzare il cavo di programmazione Cod. TRS0030011 oppure seguire il seguente schema di connessione:



Connessione lato terminale	Connessione DB9
M6-2 RS232 ricezione dati	Pin 3 - RS232 TXD
M6-3 RS232 trasmissione dati	Pin 2 - RS232 RXD
M6-4 GND	Pin 5 - RS232 GND

Nel caso in cui si deve collegare l'antenna di ribattuta al terminale TecnoaXess fare riferimento al manuale di installazione dell'antenna stessa.

3.2.4 COLLEGAMENTO DEGLI INGRESSI DI SUPERVISIONE



AVVERTENZA



Prima di collegare i sensori agli ingressi di supervisione verificare che il terminale e tutti gli apparecchi ad esso connesso siano scollegati dalla linea di alimentazione.

In tutte le versioni del TecnoaXess ad esclusione della versione Wiegand, il terminale dispone di 3 ingressi dedicati alla supervisione completa del varco relativo a un particolare terminale. I tre ingressi, come vedremo successivamente, possono essere bilanciati con delle resistenze per evitare che tagli di cavi o corto circuiti possano inibire il controllo del varco.

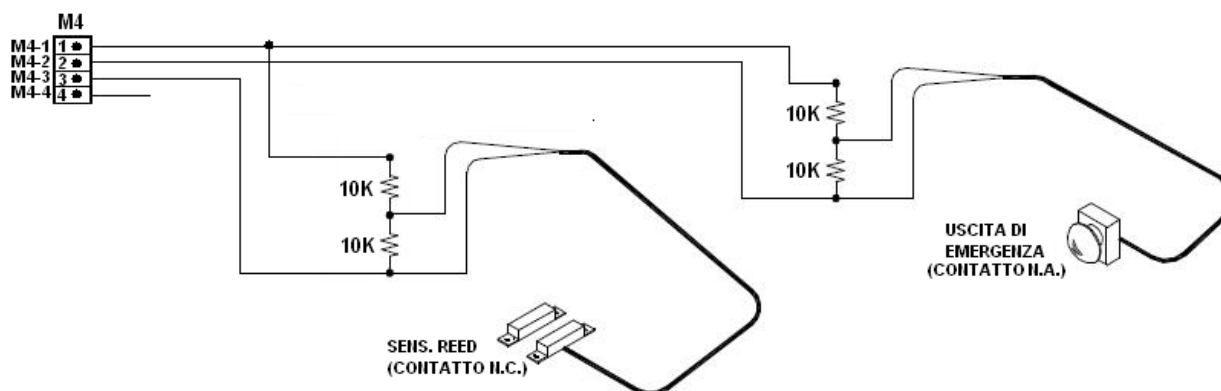
Seppur protetti contro manomissioni o sabotaggi evitare di utilizzare il sistema di controllo accessi e quindi i terminali TecnoaXess come unico sistema di allarme poiché non è stato progettato per soddisfare le normative in termini di centrali di allarmi.

Nella tabella che segue si esplicita il significato dei tre ingressi di supervisione:

Connessione lato terminale	Descrizione
M4-3 SV1 (N.C)	Ingresso di supervisione del contatto reed della porta
M4-2 SV2 (N.O)	Ingresso di supervisione della richiesta di uscita di emergenza
M4-4 SV3 (N.O)	Ingresso di supervisione generico.
M4-1 GND	Ritorno di massa per gli ingressi di supervisione

Per rendere immune il terminale da manomissioni quali cortocircuiti o taglio di cavi dei sensori di supervisione si consiglia di effettuare il doppio bilanciamento degli ingressi posizionando dalla parte del sensore, una resistenza in parallelo al contatto e una in serie a tutto come mostrato nella figura che segue. Il valore della resistenza non incide sul funzionamento del terminale tuttavia si consiglia l'uso di resistenze di 10K Ω .

Per un corretto collegamento seguire lo schema riportato di seguito con cui si mostra come collegare un sensore reed e un pulsante di uscita di emergenza:





AVVERTENZA



Gli unici sensori utilizzabili negli ingressi di supervisione sono contatti puliti o sensori magnetici normalmente utilizzati per impianti di allarme. Evitare di collegare sensori attivi o ingressi in tensione per evitare danni irreversibili del terminale stesso.



AVVERTENZA



Nel caso in cui si utilizzano solo alcuni dei 3 ingressi di supervisione occorre comunque collegare una resistenza da 20K tra gli ingressi inutilizzati e il pin di massa M4-1.

3.2.5 COLLEGAMENTO DEL TERMINALE SU BUS WIEGAND



ATTENZIONE



Al fine di evitare danneggiamenti ad altri dispositivi, prima di collegare il terminale sul bus Wiegand, scollegare dall'alimentazione tutti gli apparecchi ad esso collegato.



ATTENZIONE



Per un corretto collegamento del terminale a centrali di tipo Wiegand fare riferimento anche al proprio manuale di installazione per quanto riguarda le specifiche tecniche dei lettori Wiegand ad esse compatibili e sulle specifiche di realizzazione del bus Wiegand.



AVVERTENZA



Solo i TecnoAXess in versione Wiegand possono essere collegati sul bus Wiegand. Collegando le altre versioni su bus Wiegand si potrebbero verificare malfunzionamenti al sistema di controllo accessi.

Solo nel caso in cui si dispone di un TecnoAXess in versione Wiegand è possibile collegare il terminale al bus Wiegand seguendo le indicazioni presenti in questo paragrafo.

A seconda del tipo di centrale a cui si vuole collegare il terminale è possibile che alcune funzionalità previste non possano essere utilizzate. Per il collegamento alla centrale di controllo accessi in possesso fare riferimento al manuale di installazione; di seguito si riportano le nomenclature più comuni del bus Wiegand.

I morsetti della scheda connessione interessati dalla connessione su bus Wiegand sono:

Morsetto	Funzione	Descrizione
M1-1	Data 0	Bus di trasmissione Data0 su bus Wiegand
M1-2	Data 1	Bus di trasmissione Data1 su bus Wiegand
M1-3	Beeper	Controllo del buzzer interno su bus Wiegand
M1-4	Ground	Massa di riferimento per bus Wiegand
M3-1	Led Red	Controllo di segnalazione su bus Wiegand (accesso negato)
M3-2	Led Green	Controllo di segnalazione su bus Wiegand (accesso consentito)

Molte centrali di controlli accessi forniscono un'alimentazione a 5V per normali lettori RFID collegare il TecnoaXess alla rete di alimentazione come descritto nel par. 3.2.1 poiché l'assorbimento del terminale è tipicamente superiore a quello massimo permesso dalle centrali Wiegand.

Per quanto riguarda i cavi da utilizzare per il bus Wiegand e le massime lunghezze ammesse fare riferimento al manuale di installazione della centrale.

I collegamenti minimi ammessi per l'interoperabilità del terminale con centrali Wiegand sono quelli relativi ai morsetti "Data0" e "Data1" per quanto riguarda la trasmissione alla centrale del serial number della card RFID che ha richiesto l'accesso; quello di "Green Led" che è utilizzato dal terminale per segnalare l'accesso consentito; e il riferimento di massa "Ground" di tutti i segnali del bus. Gli altri due segnali di controllo "Red Led" e "Beeper" sono utilizzati rispettivamente per la segnalazione di accesso negato e per la gestione di un segnale sonoro. Questi ultimi due segnali di controllo a volte non vengono utilizzati dalle centrali Wiegand.

**AVVERTENZA**

Solo per i TecnoaXess in versione Wiegand non si devono effettuare i collegamenti relativi alla serratura e ad eventuali sirene di allarme poiché queste sono gestite direttamente dalla centrale Wiegand così come eventuali supervisioni del varco.

Il TecnoaXess provvederà solamente alla lettura della card RFID e dell'invio del serial number (UID card) alla centrale. Eventuali avvisi di accesso consentito o negato provenienti dalla centrale vengono visualizzati sul display grafico.

3.2.6 COLLEGAMENTO DELL'INTERFACCIA RS422 SU BUS DI TRASMISSIONE DATI



AVVERTENZA



Prima di collegare il terminale al bus RS422 verificare che il terminale e tutti gli apparecchi connesso allo stesso bus siano scollegati dalla linea di alimentazione.



AVVERTENZA



Condizioni di massimo utilizzo previste dallo standard RS422:

Massima distanza di trasmissione = 1220 m

Massima tensione ai capi = +/- 7V

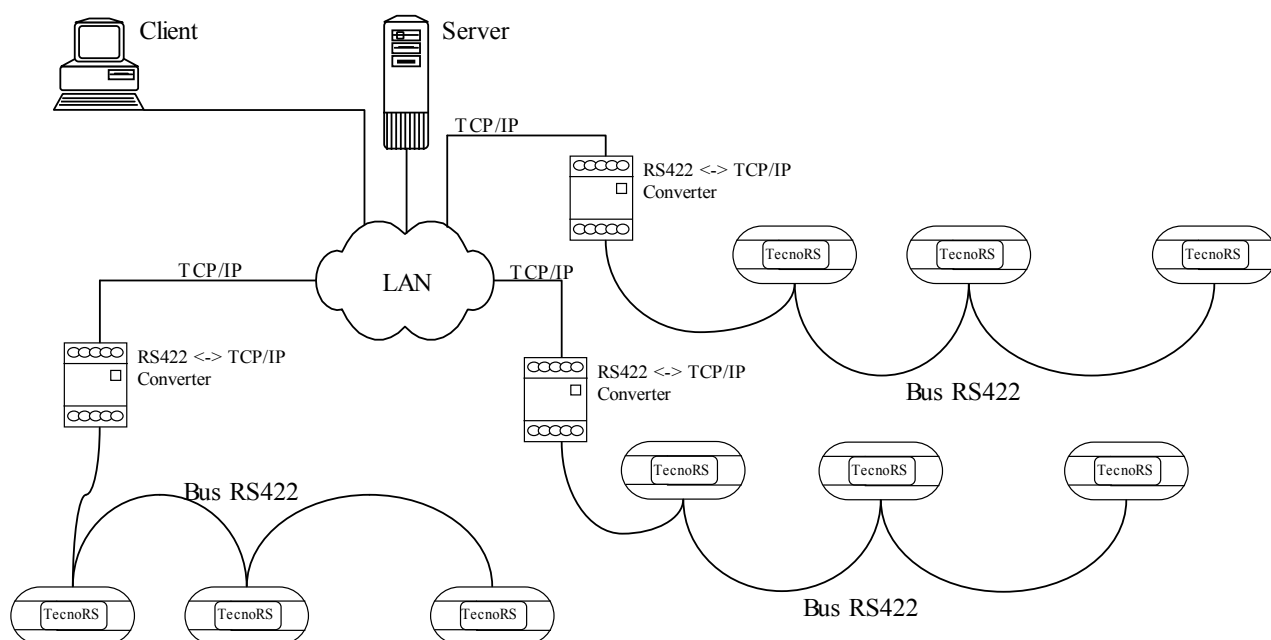
Massimo numero di dispositivi sulla stessa linea = 32

Per un corretto collegamento verso dispositivi esterni si consiglia di seguire scrupolosamente le indicazioni nel presente paragrafo.

3.2.6.1 CONFIGURAZIONE DELLE RETE

Prima di indicare la modalità di collegamento del modulo RS422 sul bus di trasmissione viene illustrata una possibile configurazione della rete RS422.

Poiché i terminali TecnoaXess devono comunicare con l'applicativo lato server su interfaccia Ethernet occorre inserire un convertitore da bus RS422 a Ethernet (Cod. TRS0060) in grado di connettersi via TCP ad un preciso socket di ascolto dell'applicativo lato server. Una possibile configurazione generale della rete RS422 può essere del tipo mostrato in figura:



dove ad all'inizio di ogni ramo del bus RS422 deve essere installato un convertitore RS422 – Ethernet che funziona da master mentre tutti i terminali ad esso collegati assumono la funzionalità di slave. Ogni convertitore che fa capo a un ramo a cui sono connessi N terminali si conatterà via TCP/IP all'applicativo lato server con cui si possono gestire tutti i terminali.

Il massimo numero di terminali collegabili per ogni ramo è pari a 32 mentre complessivamente si può arrivare fino a 65535.

3.2.6.2 COLLEGAMENTO CONVERTITORE - TECNOAXESS

Il protocollo di trasmissione di ogni singolo ramo è di tipo ad interrupts in cui sia il convertitore RS422-Ethernet (master) che i terminali (slave) possono trasmettere in modo asincrono. I collegamenti lato master e lato slave da effettuare sono:

Pin Lato Master (Convertitore RS422-TCP)	Pin Lato Slave (TecnoaXess)
T+	R+
T-	R-
R-	T-
R+	T+
GND	GND
EARTH	EARTH

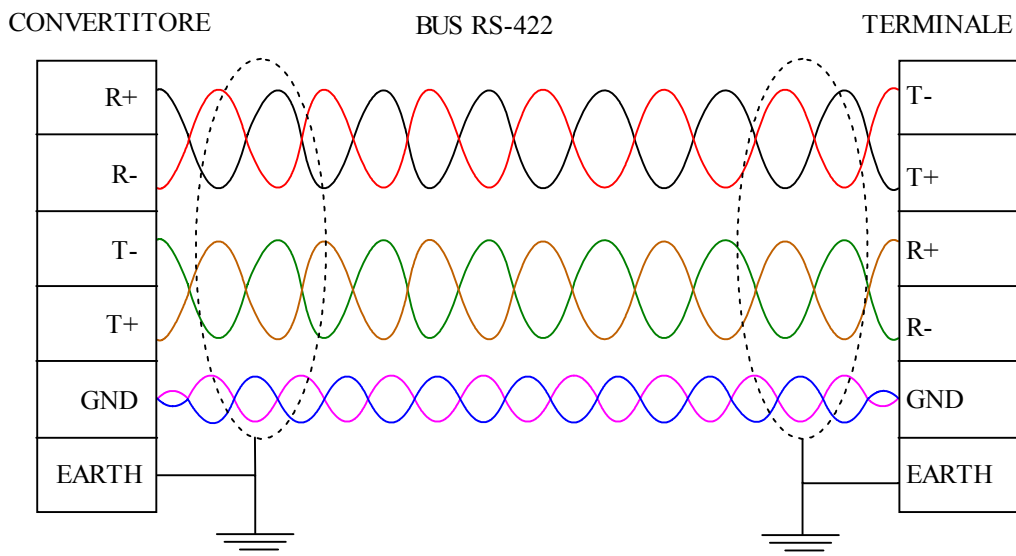
mentre per quanto riguarda la scelta del cavo da utilizzare occorre tener conto che:

- ✓ In ogni caso la lunghezza del bus non deve superare i 1220m
- ✓ Per bus lunghi complessivamente qualche decina di metri è sufficiente un cavo twistato del tipo UTP Cat. 5e
- ✓ Per bus con lunghezza compresa tra i 10 m e i 100 m è consigliabile utilizzare un cavo schermato del tipo STP Cat. 5e
- ✓ Per bus lunghi oltre i 100m si raccomanda l'utilizzo di un cavo schermato specifico per bus RS422/485 con impedenza caratteristica di 120Ω e con 3 coppie twistate come ad es. Belden 9843

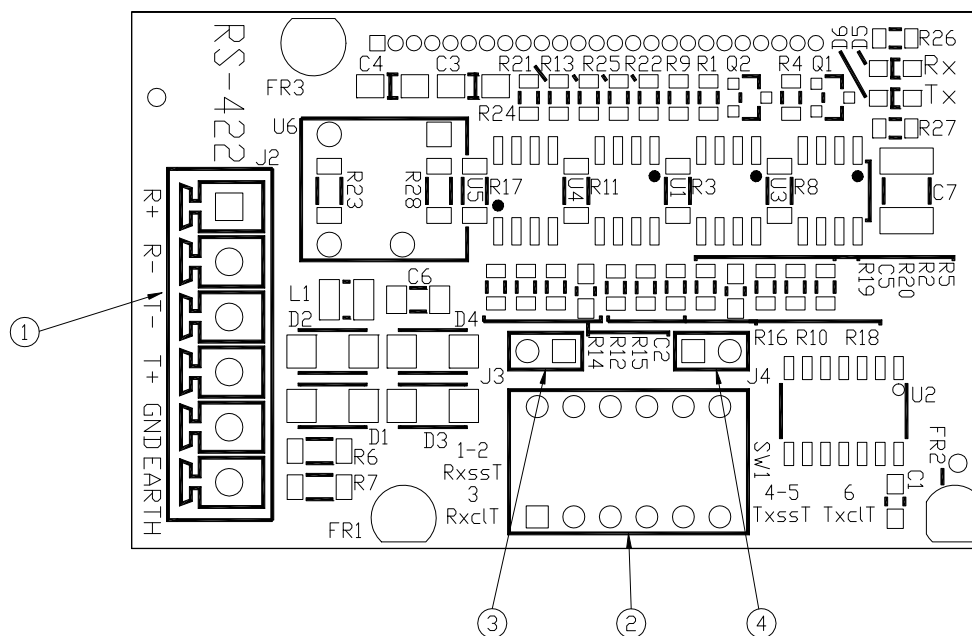
Nel caso in cui si utilizza un cavo UTP o STP utilizzare 3 delle 4 coppie facendo attenzione ad usare una delle 4 coppie per quanto riguarda i segnali T+ e T- , un'altra coppia per i segnali R+ ed R- e la terza coppia per il segnale di massa GND.

Nel caso in cui si utilizza un cavo schermato collegare la schermatura al morsetto di EARTH in almeno un punto della linea.

La figura che segue illustra meglio quanto detto:



Il layout del modulo RS422 su cui collegare il bus si presenta come mostrato in figura:



dove i riferimenti riportati in figura sono:

Riferimento	Descrizione
1	Connettore a morsetti estraibili per collegamenti su bus RS422
2	Dip-switch per la configurazione delle terminazioni di linea
3	Jumper 3 per la configurazione delle terminazioni di linea (J3)

4	Jumper 4 per la configurazione delle terminazioni di linea (J4)
---	---

per quanto riguarda il connettore di connessione RS422 (rif. 1) si hanno i seguenti significati:

Pin	Descrizione
T+	Pin Ricezione non invertente
T-	Pin Ricezione invertente
R-	Pin Trasmissione invertente
R+	Pin Trasmissione non invertente
GND	Pin per collegamento del segnale GND bus RS-422
Earth	Pin per collegamento a terra

mentre per i Dip-Switch:

Pin	Descrizione
1-2(*)	ON/OFF terminazione fail-safe per canale Rx
3	ON-OFF terminazione con resistenza 120 Ω e condensatore per canale Rx
4-5(**)	ON/OFF terminazione fail-safe per canale Tx
6	ON-OFF terminazione con resistenza 120 Ω e condensatore per canale Tx

(*) Per abilitare o disabilitare le terminazioni fail-safe sul canale Rx è necessario portare a ON oppure a OFF sia lo switch 1 che lo switch 2.

(**) Per abilitare o disabilitare le terminazioni fail-safe sul canale Tx è necessario portare a ON oppure a OFF sia lo switch 4 che lo switch 5.

3.2.6.3 TERMINAZIONI SU BUS RS422 E CONFIGURAZIONE DEL BUS

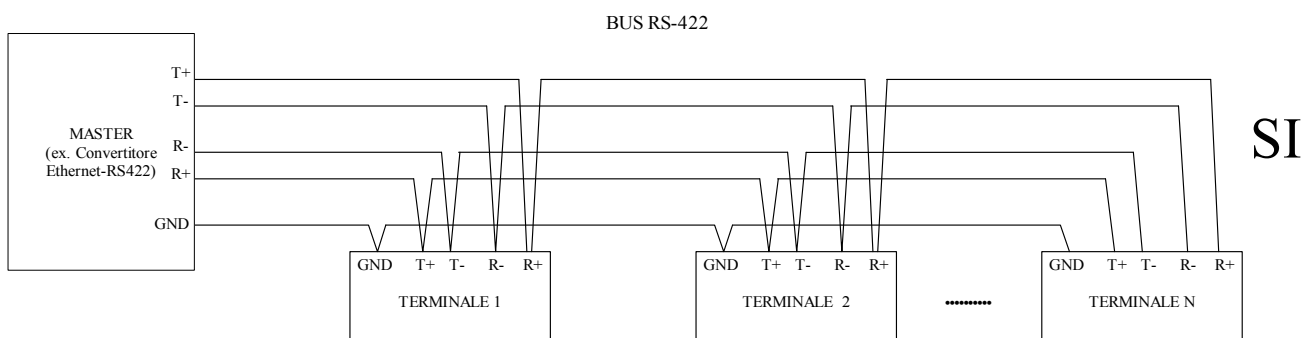
Nel caso in cui il bus ha una lunghezza che eccede la decina di metri è necessario attivare le terminazioni di linea per evitare errori di trasmissione.

Ogni modulo RS422 presente nel TecnoaXess ha un Dip-Switch dedicato alla configurazione delle terminazioni oltre che due jumper J3, J4.

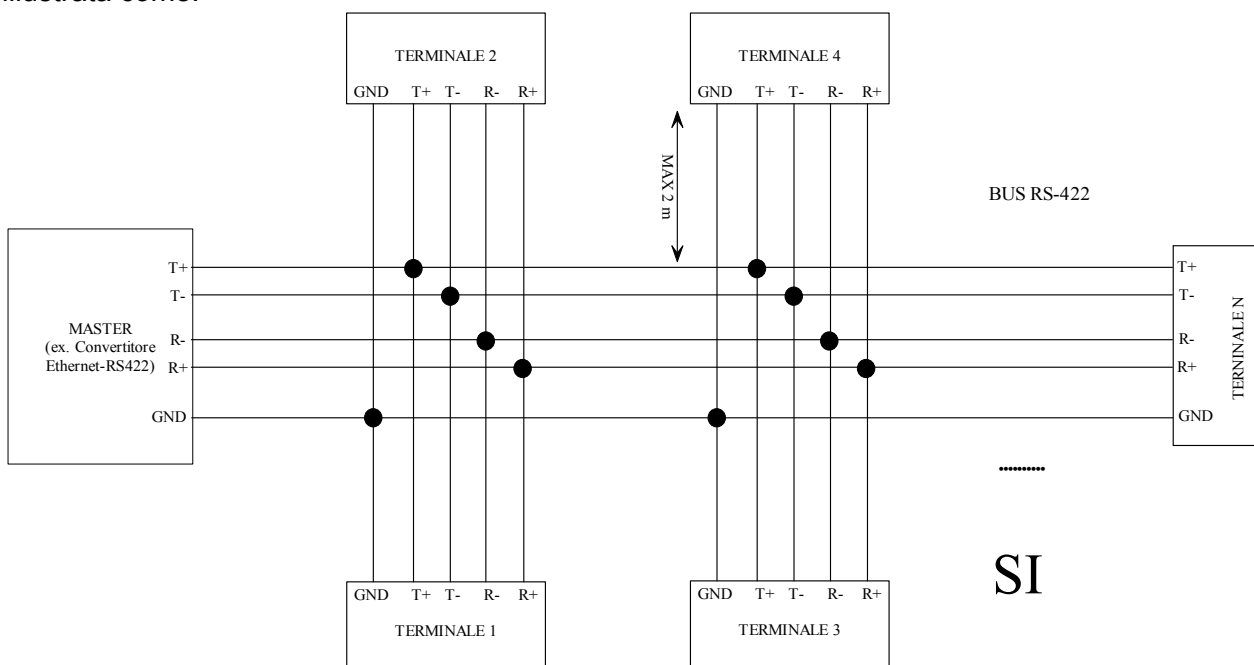
Più precisamente il jumper J3 permette di escludere il condensatore dalla terminazione sul canale Rx, mentre il jumper J4 permette di escludere il condensatore dalla terminazione sul canale Tx. Normalmente questi jumper non vanno inseriti. Essi possono essere usati per aumentare la velocità di trasmissione nel caso di collegamenti a breve distanza ed in ambienti non rumorosi.

La lunghezza massima di un collegamento su bus RS-422 non può essere definita a priori ma dipende dalla velocità di comunicazione, dal rapporto fra segnale e disturbo e dalla qualità del cavo.

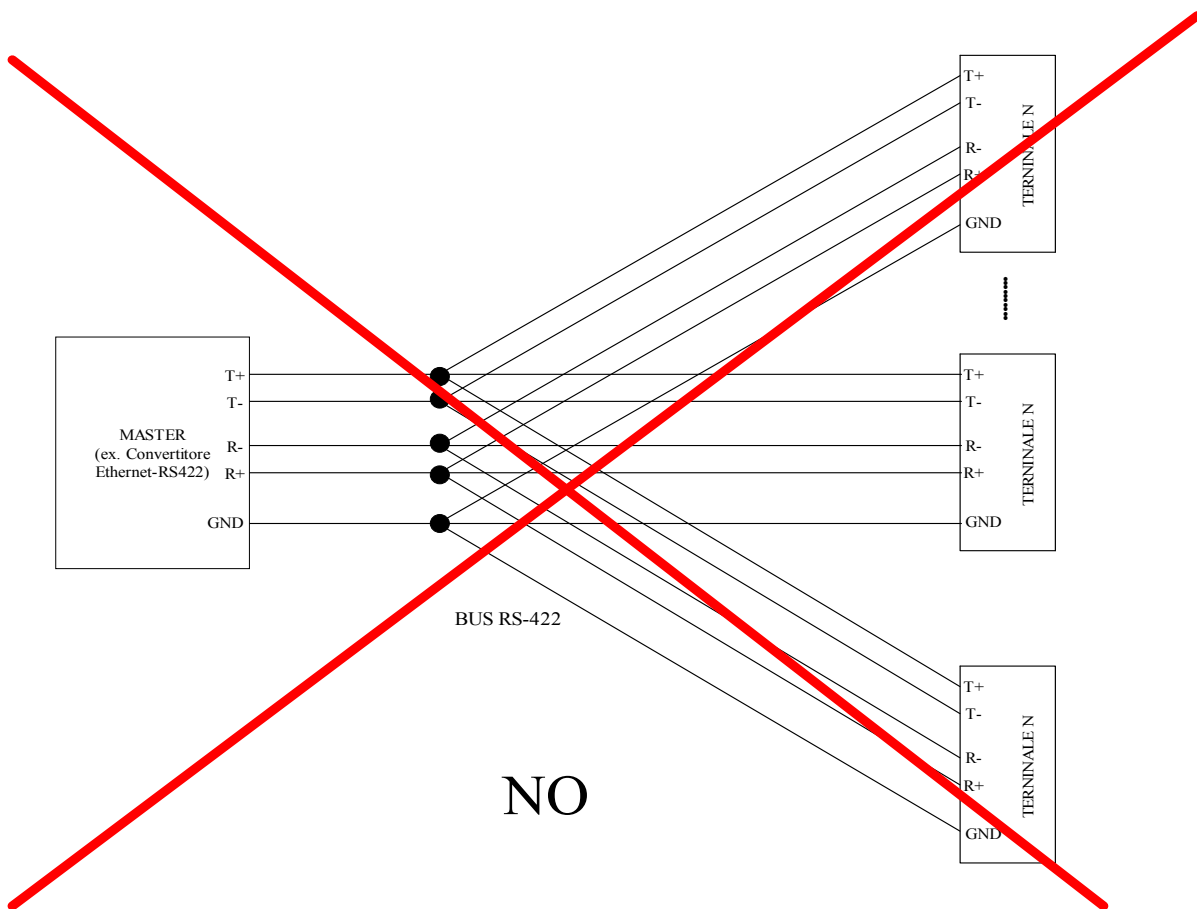
Per quanto riguarda la configurazione di ogni singolo ramo del bus RS422 si consiglia di cablare il bus di comunicazione senza derivazione praticando per ogni terminale l'ingresso sul rispettivo pin e la partenza dello stesso verso i terminali che lo seguono. Tale tipo di connessione detta a catena ed è illustrata in figura.



se strettamente necessario, si possono ammettere alcune derivazioni che non devono tuttavia avere una lunghezza complessiva maggiore di 2 metri. In questo caso la connessione viene illustrata come:



in fine quello che se deve assolutamente evitare sono le configurazioni a stella come quelle di fig:



Gli estremi della linea dovranno essere opportunamente terminati.

Ad esempio nel caso illustrato nella prima delle figure precedenti dovranno essere attivate le terminazioni da 120Ω sia sulla coppia T+ e T- che sulla coppia R+ R- dei dispositivi che si trovano all'estremità della linea; nel caso in figura quindi sul convertitore RS422-TCP/IP e sul terminale N. Nel caso in cui il convertitore trova lungo il ramo avremo alle estremità due terminali e in tal caso le terminazioni vanno attivate su di essi.

Per attivare le terminazioni da 120Ω sulla coppia TX portare a ON lo switch 6 mentre per le terminazioni della coppia RX portare ad ON lo switch 3.

Nel caso in cui si usi un convertitore Ethernet-RS422 TecnoRS, per attivare le terminazioni da 120Ω sulla coppia RX portare a ON lo switch 3 mentre per la coppia TX portare a ON lo switch 6 del dip-switch interno.

Si consiglia inoltre di attivare in almeno un dispositivo del ramo le terminazioni dette fail-safe per evitare false detezioni nel caso in cui tutti i dispositivi sono in alta impedenza.

Per attivare tale terminazioni sui terminali portare ad ON gli switch 1,2,3,4 del dip-switch.

Nel caso in cui si usi un convertitore Ethernet-RS422 TecnoRS per abilitare le terminazioni sail-safe su quest'ultimo portare ad ON gli switch 1,2,3,4 del dip-switch al suo interno (naturalmente in questo caso non abilitarle sullo slave N).

Nel caso in cui si usi un cavo schermato, lo schermo del cavo deve essere collegato al morsetto GND su tutti i componenti della rete RS422 e preferibilmente collegato a terra almeno in un componente della rete.

3.2.7 COLLEGAMENTO DEL TERMINALE SU RETE LAN

Il terminale in versione Ethernet ha internamente un modulo di comunicazione su bus Ethernet con la possibilità di gestire anche l'alimentazione del terminale tramite cavo LAN grazie alla tecnologia Power Over Ethernet (PoE).

3.2.7.1 ALIMENTAZIONE DEL TERMINALE MEDIANTE HUB PoE



AVVERTENZA

Prima di collegare il cavo LAN all'HUB PoE assicurarsi che il terminale non sia alimentato tramite linea di alimentazione collegata ai morsetti M3-3 ed M3-4.

Nel caso in cui si dispone di un terminale con interfaccia Ethernet è possibile alimentarlo direttamente da cavo LAN avendo il grosso vantaggio di ridurre ad 1 numero di cavi da cablare per l'intero sistema di controllo accessi.

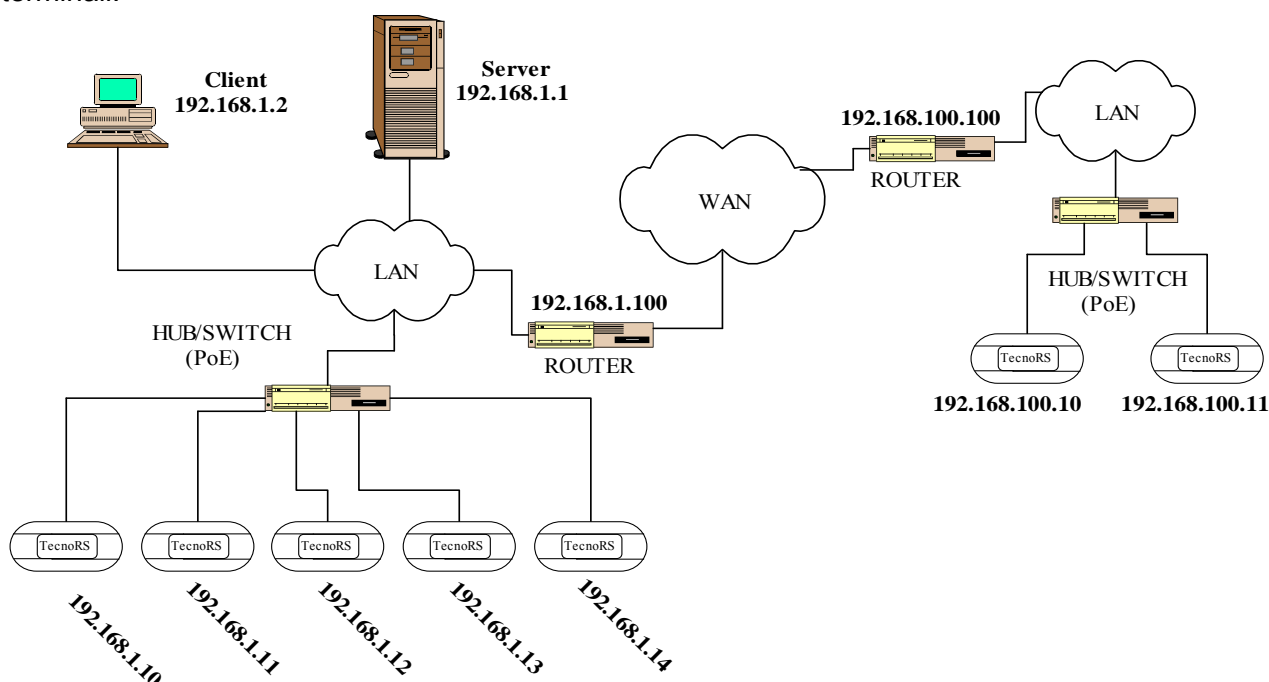
Per alimentare il terminale mediante il cavo LAN è sufficiente collegare il modulo Ethernet interno al terminale, ad un HUB o SWITCH che supporta lo standard PoE IEEE 802.3af.

E' importante evitare che un singolo terminale riceva l'alimentazione sia dalla rete LAN che dalla normale linea di alimentazione connessa ai morsetti M3-3 ed M3-4 della scheda di connessione.

3.2.7.2 CONFIGURAZIONE DELLA RETE

Nel caso in cui si dispone di TecnoaXess con interfaccia di rete LAN è sufficiente collegare ogni singolo terminale ad un HUB o SWITCH di rete in modo che il terminale possa raggiungere l'indirizzo IP del server su è installato l'applicativo di gestione del sistema.

La figura che segue illustra una possibile configurazione più generale possibile della rete dei terminali:



Nel caso in cui il terminale si trova nella stessa rete del server è sufficiente inserire un indirizzo IP della stessa classe di quello del Server (ad es. 192.168.1.x se il server ha indirizzo 192.168.1.y) in modo che i terminali possono raggiungere il server mediante il protocollo TCP/IP.
Se invece la rete di terminali è diversa da quella del server (classe di indirizzi IP diversa) occorre inserire un router (o gateway) che consenta di raggiungere il server a partire da una diversa rete.



AVVERTENZA

Prima di stabilire l'architettura di rete che si intende instaurare si consiglia di rivolgersi all'amministratore della rete LAN esistente per ottenere indicazioni dettagliate sugli indirizzi disponibili e sulla configurazione più idonea all'installazione.

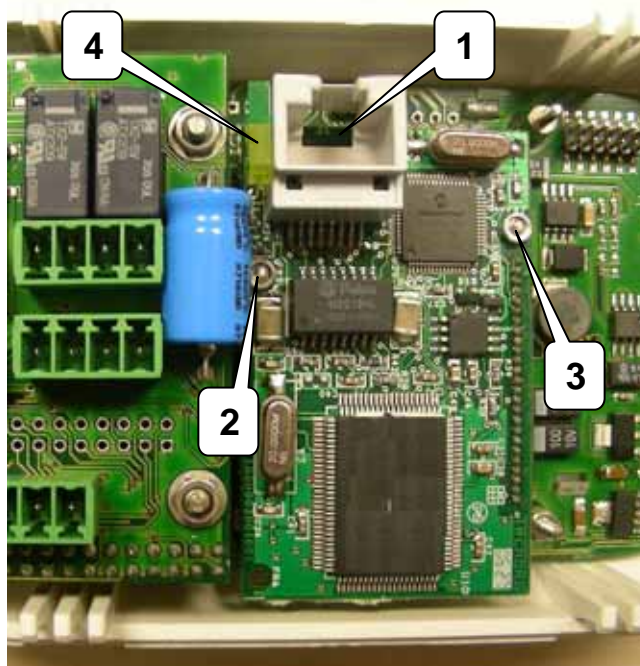
3.2.7.3 COLLEGAMENTO DELL'INTERFACCIA DI RETE

Il modulo Ethernet presente all'interno del terminale in versione Ethernet ha le seguenti specifiche tecniche:

- ✓ Supporto dei protocolli ARP, ICMP, DHCP, UDP, TCP/IP, HTTP, SMTP
- ✓ Velocità di trasmissione 10Mbit
- ✓ Compatibilità standard PoE , IEEE 802.3af
- ✓ Configurazione Web based

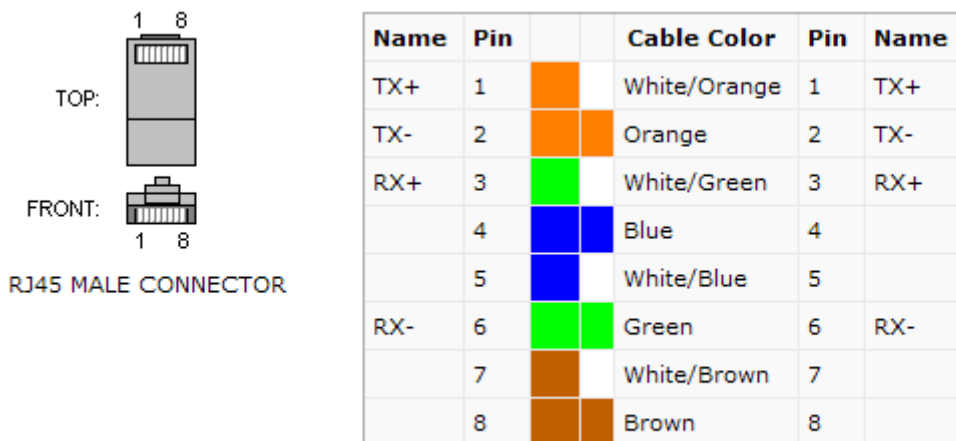
e si presenta come in figura seguente:

- 1) Connettore RJ45 (cavo LAN)
- 2) Dado di fissaggio modulo LAN
- 3) Dado di fissaggio modulo LAN
- 4) Led LINK/ACT rete LAN



Al momento dell'accensione il led contrassegnato dal riferimento numero 4 si accende in modo fisso mentre il lampeggio indica la presenza di dati in ricezione e trasmissione sulla rete LAN a cui è connesso.

Per permettere un agevole cablaggio del cavo di rete all'interno del terminale si consiglia di NON utilizzare cavi di rete stampati ma di crimpare cavi LAN in modo da avere la possibilità di flettere il cavo come illustrato nelle figure seguenti.



Inserire il cavo crimpato secondo la specifica precedente come illustrato nella figura seguente:

INSERIRE FOTO CON CAVO CRIMPATO E PIEGATO

Per quanto riguarda la configurazione dell'indirizzo IP, velocità di trasmissione ecc. fare riferimento alla sezione di configurazione del terminale presente nel manuale.

3.2.8 COLLEGAMENTO DEL TERMINALE SU RETE WiFi

Nel caso in cui si dispone di un terminale in versione WiFi non è necessario effettuare alcun collegamento fisico verso il server.

Occorre tutta via una configurazione delle rete analoga a quella vista nel paragrafo 3.2.7 per la versione Ethernet con l'unica differenza che al posto di del HUB/SWITCH si avrà un access point WiFi compatibile con lo standard IEEE 802.11b/g.

Per una maggior dettaglio sulla configurazione del terminale in versione WiFi fare riferimento alla sezione del presente manuale relativa alla configurazione del TecnoaXess.

Si riportano per completezza le caratteristiche tecniche dell'interfaccia WiFi.

- ✓ Wireless standard: IEEE 802.11b/g
- ✓ Frequenza: 2,412 – 2,484 GHz
- ✓ Distanza di trasmissione ~ 100m
- ✓ Protocolli supportati: ARP,UDP,TCP,Telnet,ICMP,SNMP,DHCP,BOOTP, Auto IP, HTTP, SMTP, TFTP
- ✓ Security: IEEE 802.11i – PSK con AES-CCMP Encryption, WPA – PSK, TKIP Encryption, 64/128 bit WEP

4 CONFIGURAZIONE DEL TERMINALE

Il presente paragrafo descrive le modalità di configurazione dei terminali nelle versioni RS422, Ethernet e WiFi.

Il terminale di controllo accessi TecnoaXess ha la possibilità di essere configurato sia offline mediante una configurazione seriale, che on line mediante specifici messaggi inviati dal server.

In ogni caso per accedere a specifiche funzionalità cambiandone le impostazioni occorre necessariamente utilizzare la configurazione via seriale.

4.1 CONFIGURAZIONE SERIALE DEL TERMINALE

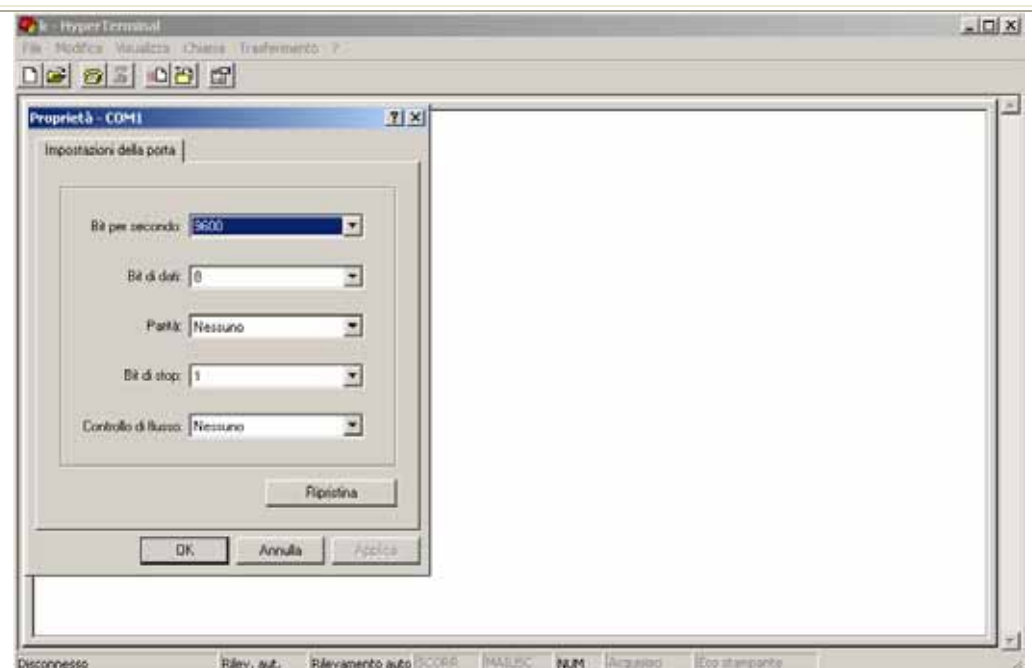
Prima di procedere con l'installazione è consigliabile configurare i terminali come illustrato di seguito in modo da rendere l'installazione più agevole possibile. Per configurare un terminale occorre dotarsi di:

- ✓ Un Personal Computer dotato di porta seriale RS232 e S.O. Windows 2000 o superiore
- ✓ Cavo seriale di programmazione del terminale (Cod. TRS0030011)
- ✓ Il terminale da programmare
- ✓ Un alimentatore 12 – 24 Vdc/Vac

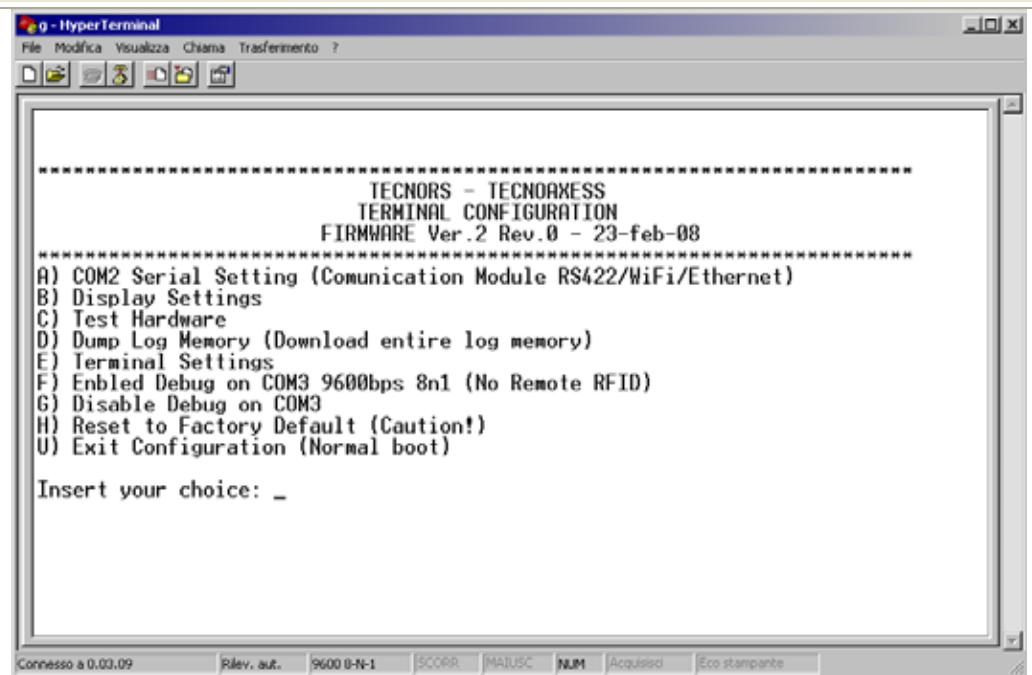
collegare il terminale al computer seguendo gli step mostrati di seguito:

<p>Collegare il cavo di programmazione seriale Cod. TRS0030011 (o equivalente) alla porta del PC (normalmente COM1).</p>	
<p>Aprire il programma Hyper Terminal da Start->Programmi->Accessori->Comunicazioni</p>	

Configurare la porta a cui è connesso il terminale (normalmente COM1) come 8N1 ovvero:
-baud rate: 9600 bps
-bit dati: 8
-bit stop: 1
-bit parity: nessuno
-ctr flusso: nessuno



Alimentare il terminale mediante un alimentatore 12-24Vdc/Vac mentre si tiene pigiato il tasto '+' sulla tastiera del PC. Se la schermata riportata a fianco non appare entro 5 secondi dall'accezione, ripetere l'operazione controllando che le impostazioni della porta sono corrette.



Dal menù principale di configurazione è possibile scegliere:

- A) Per settare l'interfaccia di comunicazione con il server. Scegliendo A è possibile cambiare la velocità di comunicazione dell'interfaccia scegliendo tra 1200, 2400, 4800, 9600(default), 19200, 38400, 57600, 115200. Il valore di default non dovrebbe essere mai cambiato tranne il caso in cui si rilevano problemi di trasmissione su bus RS422 dovuti a rumore presente sulla linea o all'utilizzo di cavi/configurazioni diverse da quelle consigliate. In questo caso occorre configurare tutti i terminali sullo stesso bus e il convertitore con la stessa velocità di trasmissione. Cambiando invece tale velocità su terminali Ethernet e WiFi

occorre modificare anche la configurazione delle interfacce mediante la relativa pagina web di configurazione.



AVVERTENZA



Modificare la velocità di trasmissione solo nel caso di terminali RS422 qualora si verificano problemi di trasmissione sul bus RS422. In tal caso tutti i terminali compreso il convertitore Eth-422 devono avere la stessa velocità di trasmissione.

B) Selezionando il menu "B" si possono visualizzare i settaggi correnti del terminale in cui vengono mostrati i seguenti parametri di configurazione:

- *Communication Module:* (LAN/WiFi/RS422) indica il tipo di interfaccia di trasmissione
- *Terminal ID:* (1 to 65535) indica il numero del terminale che deve essere univoco all'interno del sistema di controllo accesso.
- *Terminal Type:* (Uscita/Ingresso/Presenze) indica se si tratta di un terminale di Ingresso ad una certa area oppure di uscita o se si tratta di terminale di rilevazione presenze.
- *Anti Passback Settings:* (disabile,soft,hard) indica il livello di anti passback selezionato
- *Area of Terminal:* (1 - 255) indica il codice area di appartenenza del terminale
- *Stop when acces memory log full:* (ON/OFF) indica se il terminale blocca o meno l'accesso quando la memoria dei log è piena.



AVVERTENZA



Selezionando ad OFF il parametro "Stop when access memory log full" quando la memoria dei log è piena verranno sovrascritti i log a partire dal meno recente.

- *Relay1 and Relay2 settings:* indica la gestione dei relay interni; è possibile infatti settare l'utilizzo di nessuno, uno od entrambi i relay. In particolare il relay1 è relativo all'accesso consentito mentre il 2 all'accesso negato.
 - *Access Supervision:* Indica se il varco relativo al terminale è supervisionato o meno dal terminale stesso. In tal caso occorre collegare anche gli ingressi di supervisione (vedi par. 3.2.4).
 - *Timing Relays:* Indica il tempo espresso in decimi di secondo della durata di chiusura dei relay interni. (es 20 indica una durata di 2 sec).
 - *Timing Display Message:* Indica il tempo espresso in secondi della durata dei tempi di Visualizzazione dei messaggi sul display grafico.
- C) Selezionando il sotto menù contrassegnato dalla lettera C è possibile eseguire un test hardware del terminale in cui verrà testata la memoria a bordo, l'audio del terminale, i due relay a bordo, il modulo di lettura RFID e il funzionamento del real time clock.



AVVERTENZA



*Prima di effettuare il test hardware del terminale verificare che:
- le uscite relay siano sconnesse.*

Effettuando il test hardware l'ora viene resettata ed è necessario attendere che il terminale sincronizzi l'ora con il server.

D) Selezionando “*Dump Log Memory*” il terminale effettua una lettura completa di tutta la memoria in cui normalmente bufferizza i log che vengono rilevati. Questa operazione deve essere effettuata solo in caso di malfunzionamento in cui il terminale non riesce a comunicare i log al server; in questo modo si ha la possibilità di ricostruire gli eventi dell'ultimo periodo. Le stringhe relative ai log che ha in memoria vengono inviate su seriale nel seguente formato:

```
<0x13><0x10>Log N° 0001; TagID 0000000001;Gruppo 10;Transito 1,hh:mm:ss gg/mm/aa <0x13><0x10>
```

dove con *TagID* si intende il numero identificativo della card espresso in decimale, *Gruppo* è il codice del gruppo che ha avallato l'accesso, *Transito* indica il tipo di transito effettuato (1→ Ingresso negato; 2→ Ingresso consentito; 3→ Uscita negata; 4→ Uscita consentita) e infine viene riportata l'ora e il giorno di rilevazione del transito.

E) Scegliendo il menù contrassegnato dalla lettera E è possibile configurare il terminale. In particolare è possibile impostare:

- a. *Selezionare l'interfaccia di comunicazione: (A→LAN, B→WiFi, C→RS422)*: permette di selezionare il tipo di interfaccia utilizzata per la comunicazione con il server. Non modificare mai tale settaggio se non a seguito della sostituzione del modulo di comunicazione con il server.
- b. *Enter COM2 serial baud rate*: permette di impostare la velocità di comunicazione con il modulo di comunicazione. Per default è impostato a 9600bps e si consiglia di abbassarlo solo nel caso in cui si hanno problemi di trasmissione su bus RS422; con le altre interfacce tale parametro non influisce sulle velocità di comunicazione.
- c. *ID Terminale*: permette di inserire il numero identificativo del terminale che deve essere univoco in tutto il sistema di controllo accessi. I valori permessi di tale parametro sono da 1 a 65535. (non inserire per alcun motivo il numero terminale 0 poiché è utilizzato per l'invio di messaggi speciali da parte del server)
- d. *Tipo Terminale (I→Ingresso, U→Uscita, P→Presenze, V→Varco)*: permette di settare il tipo di terminale scegliendo tra un terminale di ingresso ad una certa area in cui vengono sempre controllate le politiche di accesso, un terminale di uscita da una certa area in cui non si controllano le politiche di accesso e un terminale per la rilevazione di presenze (tale settaggio è significativo solo nel caso in cui il terminale è predisposto per funzionare come rilevamento presenze). In fine un terminale settato come Varco si limita a registrare i transiti senza gestire il varco.
- e. *Setup Relay*: permette di selezionare la gestione dei relay a bordo. In particolare è possibile scegliere se non gestire il relay (inserire il carattere 0) se gestire solo il relay di accesso consentito a cui è connessa la serratura (inserire il carattere 1) oppure gestirli entrambi quando si vuole anche gestire un attuatore nel caso di accesso negato o di allarme di supervisione (inserire il carattere 2).
- f. *Setup anti passback*: permette di selezionare il livello di anti passback voluto. Si può scegliere tra 0,1,2 dove rispettivamente si avrà l'assenza di anti passback, anti passback Hard e Soft. Per una descrizione dettagliata fare riferimento al relativo paragrafo.
- g. *Access Supervision*: permette di disabilitare (inserire il carattere 0) o abilitare (inserire il carattere 1) la supervisione del varco. Abilitandola occorre collegare gli ingressi di supervisione come mostrato al par. 3.2.4

- h. *Tempo di chiusura Relay*: permette di inserire in decisimi di secondo la durata di chiusura del relay di accesso consentito. Impostando il valore 20 ad esempio si avrà una chiusura del contatto di 2 secondi.
 - i. *Tempo visualizzazione messaggi*: permette di inserire la durata in secondi del tempo di visualizzazione delle scritte sul display. Tale tempo ha effetto sui messaggi temporanea mostrati a video come ad esempio le schermate di avviso di accesso consentito, negato o i messaggi inviati dal server.
 - j. *Area di appartenenza*: permette di settare l'area di appartenenza del terminale. Tale parametro ha un'importanza rilevante nel caso in cui si attivi l'anti passback infatti nel caso di terminale di ingresso questo parametro indica l'area a cui il terminale permette l'accesso mentre nel caso di terminale di uscita indica l'area da cui il terminale consente l'uscita. (vedere il par. relativo alla gestione dell'anti passback per maggiori dettagli).
- F) Selezionando *Enable Debug on COM3* si abilitano le tracce di Debug del terminale che le invierà sulla seriale dei morsetti M6. Tale opzione non deve essere selezionata se non dal servizio di assistenza per verificare eventuali malfunzionamenti.

**AVVERTENZA**

L'utente finale non deve mai abilitare le tracce di Debug poiché:

- *rallentano l'esecuzione delle operazioni.*
- *disabilita il controllo di eventuali antenne di ribattuta.*

- G) Selezionando questa opzione si disabilitano le tracce di debug abilitate con il menù "E".
H) Selezionando "Reset to Factory Default" si riportano tutti i settaggi al valore di default.

**AVVERTENZA**

Attenzione resettando i valori di fabbrica si perdono eventuali settaggi e log memorizzati e non ancora inviati al server. Effettuare tale operazione solo prima della fase di installazione.

- U) Selezionando tale menù si esce dalla configurazione e il terminale si avvia con la configurazione salvata.

4.2 CONFIGURAZIONE MEDIANTE MESSAGGI DAL SERVER

Successivamente all'installazione dei terminali nel sistema è possibile comunque accedere ad alcune funzionalità per modificarne di volta in volta i parametri.

Di seguito si riporta solo l'elenco dei parametri settabili da remoto e si rimanda per i dettagli al manuale di uso del software AsyaXess qualora fosse utilizzato nel sistema; o al manuale di integrazione in cui vengono descritti i pacchetti e il protocollo di comunicazione tra server e terminale.

Accedendo da remoto è possibile configurare o modificare:

- ✓ Numero Terminale (ID Terminale da 1 a 65535)
- ✓ Tipo terminale (ingresso,uscita,presenze)
- ✓ Area di appartenenza del terminale
- ✓ Modalità di gestione della memorizzazione dei transiti
- ✓ Modalità di gestione dei due relay di accesso/allarme
- ✓ Durata dell'impulso di chiusura della serratura
- ✓ Attivazione/Disattivazione della funzionalità di supervisione
- ✓ Programmazione delle politiche di accesso
- ✓ Programmazione delle fasce orarie e della gestione della sirena per i terminali Presenze
- ✓ Impostazione della scritta di default visualizzata dal display grafico

E' inoltre possibile gestire altri comandi per i quali si rimanda alle relative sezioni del manuale di uso e manutenzione.

Di seguito si riporta un riepilogo dei vari parametri di configurazione e la modalità seriale/remota per accedervi.

4.3 RIEPILOGO PARAMETRI DI CONFIGURAZIONE

Nella tabella che segue si possono trovare tutti i parametri di configurazioni e la modalità con cui modificarli. E' riportata anche la modalità consigliata per evitare difficoltà in fase di utilizzo del sistema di controllo accessi:

Parametro da configurare/modificare	Config. Seriale	Config. Remota	Modalità di config. consigliata
Numero Terminale	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Seriale(*)
Tipo Terminale (ing/usc/pres/varco)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Indifferente
Area di appartenenza	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Indifferente
Modalità di gestione mem. transiti	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Indifferente
Modalità di gestione dei relay interni	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Indifferente
Durata di chiusura relay	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Indifferente
Attivazione/Disattivazione supervisione	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Seriale
Programmazione politiche di accesso	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Remota
Programmazione fasce orarie e sirena	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Remota
Ipostazione scritta default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Remota
Selezione interfaccia di connessione	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Seriale
Velocità di comunicazione con interf.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Seriale
Tempo di visualizzazione messaggi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Seriale
Gestione Anti Pass-Back	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remota
Enable/Disable Debug su COM3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Seriale

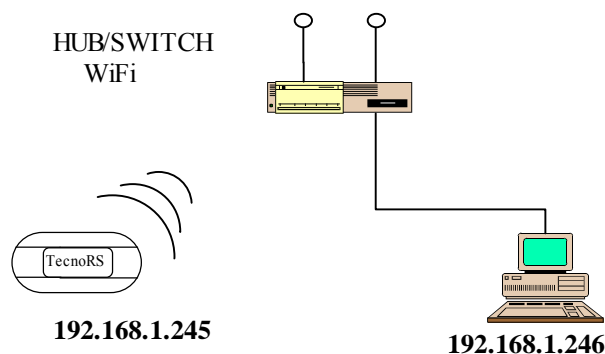
(*)Al fine di evitare duplicazioni del ID terminale si consiglia di settare per la prima volta, il numero terminale prima della sua installazione in modo da evitare l'esistenza di terminali con lo stesso ID. Successivamente all'installazione la modifica può avvenire anche da remoto evitando di assegnare ad un terminale un numero già assegnato ad un altro terminale.

4.4 CONFIGURAZIONE DELL'INTERFACCIA WIFI

Nel caso in cui si utilizza come interfaccia di comunicazione con il server la tecnologia wireless IEEE802.11b/g (WiFi) occorre configurare l'interfaccia di comunicazione interna al TecnoaXess in modo tale che possa agganciarsi alla rete WiFi pre-esistente nel luogo di installazione.

Per poter accedere alla pagina web di configurazione interna all'interfaccia occorre seguire i passi riportati di seguito:

- ✓ Collegare un access point WiFi (non necessariamente connesso alla rete esistente o alla rete definitiva che ospiterà i terminali di controllo accessi) accertandosi che non abbia alcuna politica di sicurezza attiva. I terminali infatti sono inizialmente configurati per accedere a reti wireless aperte (no Authentication o Encryption come WEP, WPA, WPA2 ecc) in modo da facilitare la configurazione degli stessi. Se si tratta di un router WiFi assegnarli un indirizzo di rete nella classe 192.168.1.x evitando di assegnarli il 192.168.1.245 che tipicamente è quello assegnato al Terminale prima della sua configurazione.
- ✓ Allo stesso access point o mediante hub/switch collegare un PC utilizzando un cavo di rete ethernet oppure sfruttando la stessa rete WiFi; assegnare al PC un indirizzo nella classe 192.168.1.x ad eccezione del 192.168.1.245 e dell'indirizzo dell'eventuale router/access point.





- ✓ Dopo aver acceso il terminale aprire un qualsiasi browser web (es. Windows Internet Explorer) e digitare nella barra di indirizzo il seguente link:

<http://192.168.1.245>

se il terminale è connesso all'access point si potrà entrare nel web configurator e seguire i passi riportati nella tabella che segue:

Descrizione	Screen Shot
-------------	-------------

1	<p>Alla prima configurazione accedere al web configurator senza inserire alcun nome utente e passo word cliccando quindi direttamente su "OK"</p>	
2	<p>Cliccare sulla sezione "Network" per impostare i parametri relativi alla rete su cui andrà poi inserito il terminale.</p>	

3

Impostare i parametri di rete desiderati per quanto riguarda

- "IP Address"
- "Subnet Mask"
- "Default Gateway"

Dopo aver selezionato i parametri voluti cliccare su "OK" per salvare le impostazioni.

Al termine occorre selezionare "Apply Settings" per riavviare l'interfaccia con i nuovi parametri

LANTRONIX® Firmware Version: V6.3.0.2
MAC Address: 00-20-4A-96-57-ED

Network Settings

Network Mode:

IP Configuration

Obtain IP address automatically

Use the following IP configuration:

Auto Configuration Methods

BOOTP: Enable Disable

DHCP: Enable Disable

AutoIP: Enable Disable

DHCP Host Name:

IP Address:

Subnet Mask:

Default Gateway:

Ethernet Configuration

Auto Negotiate

Speed: 100 Mbps 10 Mbps

Duplex: Full Half

4

Cliccando sulla sezione "WLAN" è possibile accedere alla pagina di configurazione della sicurezza di accesso e trasmissione dati sulla rete WireLess impostando:

- SSID
- Security
- Authentication
- Encryption
- Key Type
- Key

Dopo aver selezionato i parametri voluti cliccare su "OK" per salvare le impostazioni.

Al termine occorre selezionare "Apply Settings" per riavviare l'interfaccia con i nuovi parametri

LANTRONIX® Firmware Version: V6.3.0.2
MAC Address: 00-20-4A-96-57-ED

Wireless Network Configuration

Network Name (SSID):

Network Type: Infrastructure Ad Hoc

Channel: United States

Wireless Network Security

Security:

Authentication:

Encryption:

Key Type: Hex Passphrase

Key:

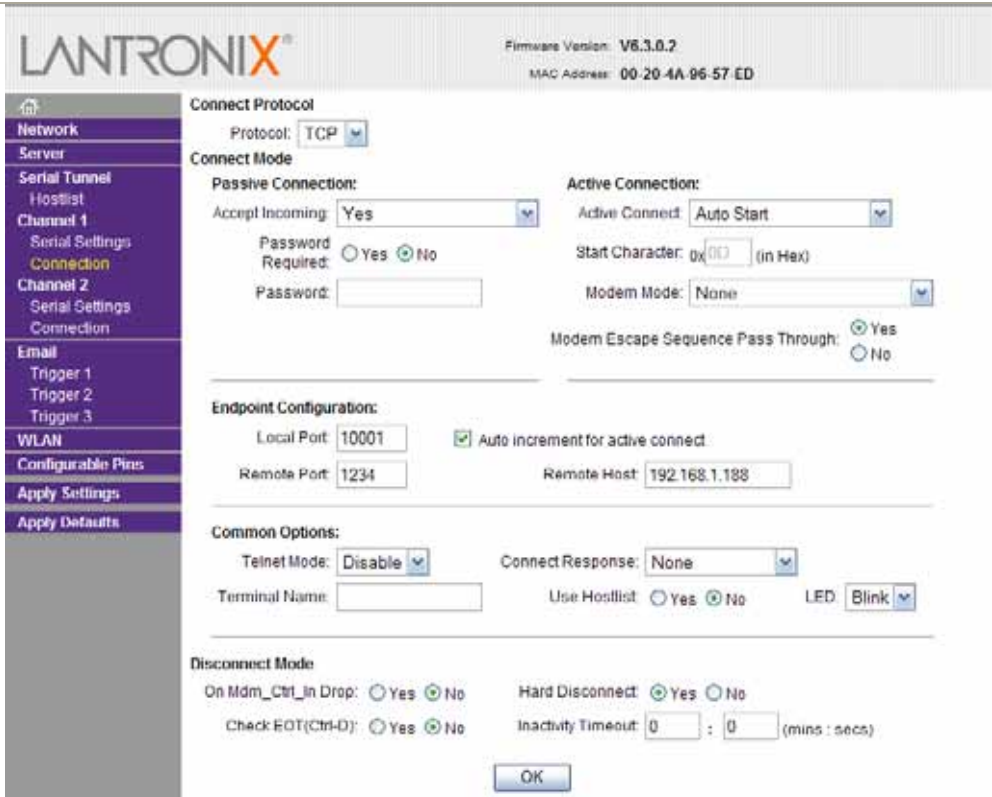
Retype Key:

TX Key:

Advanced Settings

TX Data rate: Auto fallback

Radio Power Management: Enable Disable

<p>5</p> <p>In fine cliccare sulla sotto menù "Connection" del menù "Channel 1" e selezionare i parametri voluti per quanto riguarda il server a cui il terminale deve connettersi:</p> <p>-Remote Host</p> <p>Inserendo l'indirizzo IP del server al quale il terminale dovrà connettersi.</p> <p>Dopo aver selezionato i parametri voluti cliccare su "OK" per salvare le impostazioni.</p> <p>Al termine occorre selezionare "Apply Settings" per riavviare l'interfaccia con i nuovi parametri</p>	
--	---

Di seguito si riportano alcune caratteristiche dell'interfaccia di comunicazione WiFi relativamente alla rete e alla sicurezza:

- ✓ Wireless standard IEEE 802.11b; 802.11g
- ✓ Protocolli supportati: ARP, UDP, TCP, Telnet, ICMP, SNMP, DHCP, BOOTP, Auto IP, HTTP, SMTP, TFTP
- ✓ Security: IEEE 802.11i - PSK with AES-CCMP Encryption, WPA – PSK, TKIP Encryption, 64/128-bit WEP.



AVVERTENZA

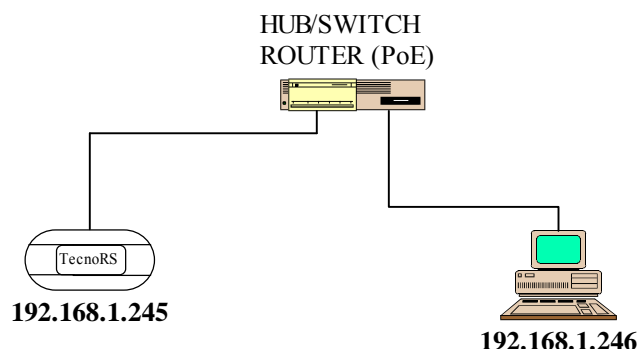
A richiesta è possibile avere i più recenti standard di sicurezza come WPA2- Enterprise (EAP, PEAP, LEAP), WPA2-PSK, WPA - PSK 64/128-bit WEP.

4.5 CONFIGURAZIONE DELL'INTERFACCIA ETHERNET PoE

Nel caso in cui si utilizza come interfaccia di comunicazione con il server la rete ethernet, occorre configurare l'interfaccia di comunicazione interna al TecnoXess in modo tale che possa connettersi al server.

Per poter accedere alla pagina web di configurazione interna all'interfaccia occorre seguire i passi riportati di seguito:

- ✓ Collegare un Hub/Switch/Router al terminale (se non dotato di porta PoE occorre alimentare il terminale separatamente come mostrato al par. 3.2.1). Se si tratta di un router assegnarli un indirizzo di rete nella classe 192.168.1.x evitando di assegnarli il 192.168.1.245 che tipicamente è quello assegnato al Terminale prima della sua configurazione.
- ✓ Collegare allo stesso hub/switch/router a cui è connesso il terminale, un PC utilizzando un cavo di rete ethernet; assegnare al PC un indirizzo nella classe 192.168.1.x ad eccezione del 192.168.1.245 e dell'indirizzo dell'eventuale hub/switch/router.



- ✓ Dopo aver atteso l'avvio del terminale, aprire il browser Windows Internet Explorer e digitare nella barra di indirizzo il seguente link:

<http://192.168.1.245/login.html>

se il terminale è connesso si potrà entrare nel web configurator e seguire i passi riportati nella tabella che segue:

<p>1</p>	<p>Alla prima configurazione e inserire il nome utente e password di default ovvero</p> <p>-admin -admin</p> <p>Si consiglia di modificare i dati di accesso e di conservarli in un luogo sicuro</p>	<p>TecnoXess Home TecnoRS Contact</p> <p>Esegui Login</p> <p>Nome Utente <input type="text"/></p> <p>Password <input type="text"/></p> <p>Login</p> <p>Login</p> <p>Per poter accedere alla configurazione è necessario inserire il nome utente e la password.</p> <p>© 2007 TecnoRS Home Contact</p>
----------	--	--

<p>2</p> <p>Cliccando sulla sezione "LAN Setup" è possibile accedere alla sezione di configurazione e dei parametri di rete. In particolare impostare:</p> <ul style="list-style-type: none"> - Ind. IP - Net Mask - Gateway - Client Mode <p>-Ind IP Host -remote port</p> <p>Dopo aver impostato i parametri volute cliccare su "Salva"</p> <p>IMP.: Se è stato modificato l'ind IP occorre tornare al punto 1</p>	
<p>3</p> <p>Dopo il primo accesso si consiglia di modificare i dati di accesso Nome utente e Password mediante la form riportata in figura.</p> <p>Nome utente e password devo essere composti da 8 caratteri alfanumerici.</p> <p>Cliccare su "salva" per rendere effettive le modifiche</p>	

Nel configurare l'interfaccia ethernet è importante ricordare quanto segue:

- ✓ Inserire nel campo "Indirizzo IP host remoto" l'indirizzo IP del server che ospiterà il programma di gestione da remoto dei terminali di controllo accessi.
- ✓ Inserire nel campo "remote port" il numero di porta TCP/IP su cui il programma di gestione è in ascolto. Nel caso di utilizzo del pacchetto AsyaXess il numero da impostare è 1234.



AVVERTENZA



Nel caso in cui nella rete è presente un firewall assicurarsi che la porta 1234 o quella impostata nel capo "remote port" non sia bloccata dal router/firewall.

- ✓ Nel momento in cui si modifica l'indirizzo IP del terminale mediante il campo "Indirizzo IP" assicurarsi che non vi siano altri dispositivi, inclusi terminali, che abbiano già lo stesso indirizzo.



AVVERTENZA



Nel caso in cui si modifica l'indirizzo IP del terminale occorre aprire nuovamente il browser ed effettuare il login inserendo il nuovo indirizzo salvato.

- ✓ Nella Sezione "COMSetup" è possibile modificare i parametri relativi alla seriale di comunicazione dell'interfaccia con la scheda a microprocessore. Tali parametri devono essere modificati solo da utenti esperti sotto l'indicazione del centro di assistenza o della ditta costruttrice.

5 USO DEL DISPOSITIVO

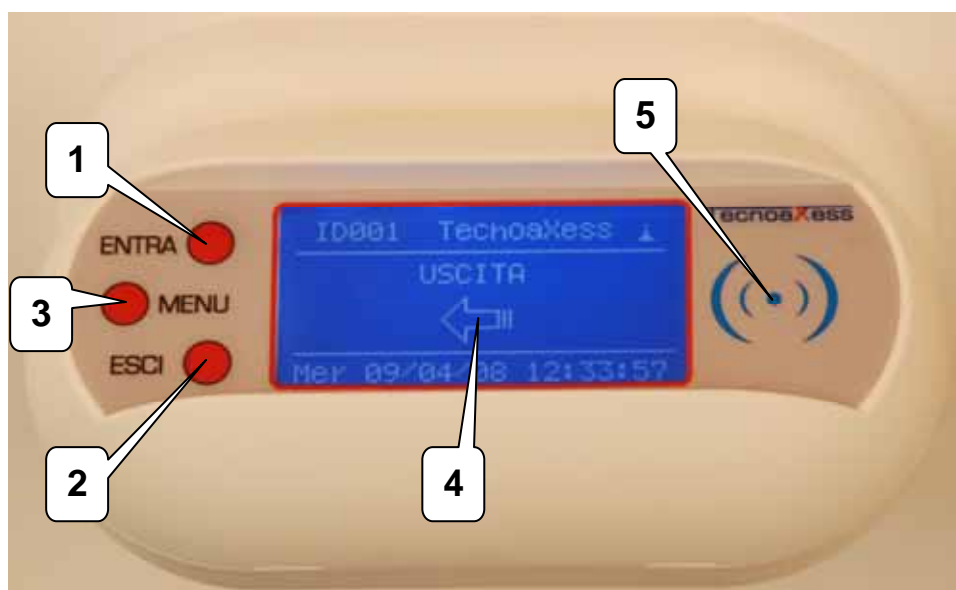
Di seguito verranno illustrate le operazioni che consentono l'utilizzo del terminale nel normale esercizio per il quale è stato configurato. La modalità con vengono eseguite può cambiare a seconda del software utilizzato per la gestione del sistema di controllo accessi. Per informazioni specifiche si rimanda al manuale di uso del software AsyaXess oppure alla descrizione del protocollo di comunicazione del terminale con l'host remoto.

5.1 TERMINALE PRESENZE

Nel paragrafo seguente si descrive l'uso del terminale configurato come rilevazione presenze. Verranno descritte le varie funzionalità in modo generico rimandando nello specifico al manuale di uso del software di gestione AsyaXess oppure al manuale che descrive il protocollo di interfacciamento del terminale su rete ethernet.

5.1.1 DESCRIZIONE TERMINALE

Nella figura che segue si riporta un terminale presenze in cui possiamo individuare:

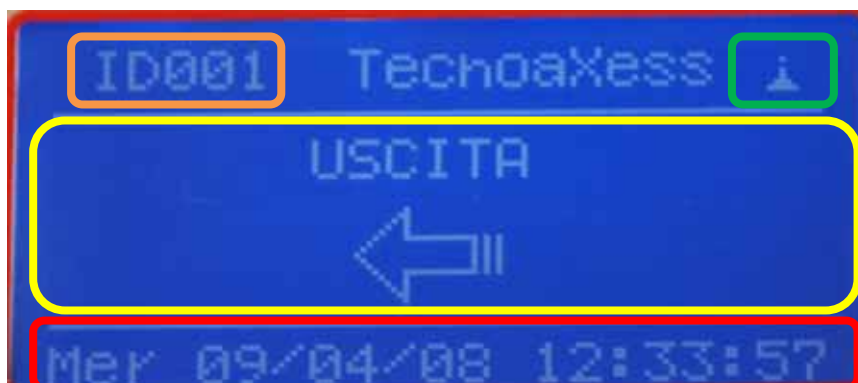


- 1) Tasto "ENTRA" per la selezione della timbratura in ingresso che si vuole registrare
- 2) Tasto "ESCI" per la selezione della timbratura in uscita che si vuole registrare
- 3) Tasto "MENU".
- 4) Display grafico 64x128 pixel per interazione con l'utente.
- 5) Testa di lettura RFID per il riconoscimento delle card RFID.

5.1.2 INDICAZIONI DEL DISPLAY

Vengono illustrati i vari campi del display specificando nel dettaglio il loro significato.

Si riporta, a titolo esemplificativo, l'immagine del display di un terminale configurato come presenze e con interfaccia WiFi:



dove si evidenzia in arancione l'indicazione del numero terminale (*ID Terminale*) impostato. Tale parametro è fondamentale per il corretto funzionamento del sistema poiché individua in modo univoco un terminale all'interno del sistema di controllo accessi / rilevazione presenze. Il numero terminale deve essere necessariamente stabilito e configurato mediante configurazione seriale prima dell'installazione in modo da poter successivamente configurare i vari terminali da remoto.

In verde è evidenziata un'icona che indica il tipo di terminale, nel caso di interfaccia wireless troviamo l'icona visualizzata nella figura precedente mentre nel caso di terminale LAN o RS422 l'icona raffigura lo schermo di un PC connesso ad una rete. Tali icone indicano anche se il terminale è connesso o meno al server; nel caso di terminali wireless se l'icona è fissa come in figura significa che il terminale non è connesso al server remoto mentre nel caso di terminali cablati se il monitor stilizzato nell'icona è "spento" indica la mancanza della rete. In condizioni di standby il terminale effettua un controllo della presenza del server remoto ogni 5 minuti circa quindi l'indicazione della presenza o meno della rete può avvenire con un leggero ritardo.

In giallo invece viene raffigurata la sezione del display (4 righe da 21 caratteri) dedicata ai messaggi all'utente. Nel caso di terminali presenze la visualizzazione di default è quella relativa alla fascia oraria; in base alla configurazione delle fasce orarie, il terminale si predispose alla rilevazione di una timbratura in uscita o in entrata e sul display si riporta tale indicazione.

Durante la timbratura invece, sul display viene riportata l'indicazione di *INGRESSO REGISTRATO* o di *USCITA REGISTRATA* a seconda che si tratti di una timbratura in ingresso oppure in uscita. Se il terminale è normalmente connesso al server, successivamente alla timbratura verrà visualizzato un messaggio a video in cui viene riportato un messaggio inviato dal server in cui si visualizza il nome e l'ora della persona appena registrata.

In fine in rosso viene evidenziata la data corrente del terminale che sarà la data effettiva con cui vengono rilevati i transiti.

5.1.3 UTILIZZO DEI TASTI INGRESSO / USCITA

Sul terminale sono presenti tre tasti identificati come *MENU*, *ENTRA*, *ESCI* che rispettivamente assumono i seguenti significati:

- *MENU*: di uso specifico per alcune personalizzazioni non è associato ad alcuna funzione nelle versioni base del terminale.

- *ENTRA*: è utilizzato per la selezione del tipo di timbratura che l'utente sta per effettuare. In particolare, come vedremo in seguito, il terminale in base alla sua configurazione si predispose ad accettare timbrature in ingresso oppure in uscita in base alla particolare ora del giorno in cui ci troviamo. Con il tasto in *Ingresso* è possibile cambiare tale configurazione e indipendentemente dall'ora effettuare una timbratura in ingresso. Pigiando tale tasto sul display viene visualizzata l'icona relativa all'ingresso per un tempo pari al valore impostato su "*Tempo visualizzazione messaggi*" durante il quale un eventuale timbratura viene registrata come ingresso.

- *ESC/*: è utilizzato per la selezione del tipo di timbratura che l'utente vuole effettuare. In particolare, come vedremo in seguito, il terminale in base alla sua configurazione si predispone ad accettare timbrature in ingresso oppure in uscita in base alla particolare ora del giorno in cui ci troviamo. Con il tasto in *Uscita* è possibile cambiare tale configurazione e indipendentemente dall'ora effettuare una timbratura in uscita. Pigiando tale tasto sul display viene visualizzata l'icona relativa all'uscita per un tempo pari al valore impostato su "*Tempo visualizzazione messaggi*" durante il quale un eventuale timbratura viene registrata come uscita.

5.1.4 UTILIZZO DEL LETTORE RFID

L'antenna RFID che consente la lettura delle card assegnate agli utenti si trova in corrispondenza al logo raffigurato nella figura di par. 5.5.1 rif. 5.

Per effettuare una timbratura occorre avvicinare la card tenendola orizzontalmente rispetto al piano dove è raffigurato il logo e centrata rispetto ad esso. La distanza di lettura può variare a seconda del tipo di card da 2 a 4 cm. Una volta avvicinata la card attendere l'avvenuta lettura indicata dal display come *INGRESSO REGISTRATO* oppure con *USCITA REGISTRATA*.



AVVERTENZA

Nel caso la card venga allontanata prima della completa lettura o ci sono errori in lettura, occorre attendere 4~5 secondi prima di riavvicinare la card per effettuare un nuovo tentativo di lettura.

5.1.4.1 TIMBRATURA IN INGRESSO

Per effettuare una timbratura in ingresso, se sul display è già presente la freccia rivolta verso destra con la scritta "*INGRESSO*" è sufficiente avvicinare la card al lettore in corrispondenza del logo ed attendere l'avvenuta registrazione; se il terminale è predisposto per le timbrature in uscita (freccia verso sinistra e scritta *USCITA*) occorre prima pigiare il tasto *ENTRA* e successivamente avvicinare la card al lettore.

5.1.4.2 TIMBRATURA IN USCITA

Per effettuare una timbratura in uscita, se sul display è già presente la freccia rivolta verso sinistra con la scritta "*USCITA*" è sufficiente avvicinare la card al lettore in corrispondenza del logo ed attendere l'avvenuta registrazione; se il terminale è predisposto per le timbrature in ingresso (freccia verso destra e scritta *INGRESSO*) occorre prima pigiare il tasto *ESC/* e successivamente avvicinare la card al lettore.

5.1.5 GESTIONE DELLE FASCE ORARIE

Come precedentemente accennato il terminale in configurazione di rilevazione presenze ha la possibilità di gestire delle fasce orarie adattandosi al normale flusso di ingresso e uscita dato dai turni presenti nella azienda. Impostando le fasce orarie in modo corretto permette un veloce utilizzo del terminale infatti l'utente nel momento in cui deve effettuare la timbratura già trova il terminale impostato su ingresso o su uscita.

Ad esempio in una azienda in cui turni di lavoro sono:

Primo Ingresso	ore 07:30
Prima Uscita	ore 12:30
Secondo ingresso	ore 14:30

Seconda uscita ore 17:30

È conveniente impostare le fasce orarie in modo che i dipendenti non devono agire sui tasti ENTRA / ESCI quindi avremo per esempio:

Fascia N°1 Ingresso → dalle ore 05:00 alle ore 11:30
Fascia N°2 Uscita → dalle ore 11:30 alle ore 13:30
Fascia N°3 Ingresso → dalle ore 13:30 alle ore 16:00
Fascia N°4 Uscita → dalle ore 16:00 alle ore 05:00

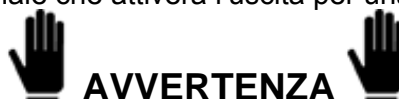
In ogni caso se un dipendente si trova a dover uscire oppure entrare quando la fascia impostata non è corretta è sufficiente agire sui tasti ENTRA/ESCI prima di effettuare la lettura della propria card.

Il massimo numero di fasce orarie impostabili nell'arco della giornata è pari a 24.

Per i dettagli su come impostare le fasce orarie fare riferimento al manuale del software AsyaXess oppure al protocollo di comunicazione con l'host remoto.

5.1.6 GESTIONE DELLA SIRENA DI INIZIO/FINE TURNO

Il terminale TecnoaXess in configurazione di rilevazione presenze può gestire autonomamente anche una segnalazione sonora e/o visiva per scandire l'inizio o la fine di un turno di lavoro. In particolare è possibile collegare al contatto NO del relay N°2 (pin M2-3 e M2-4) una sirena e/o un lampeggiante e programmare il terminale che attiverà l'uscita per una durata e nell'istante voluto.



AVVERTENZA

Prima di collegare un carico al contatto del relay come una sirena e/o un lampeggiante, assicurarsi che tensione e potenza siano supportate dal relay interno. In caso contrario utilizzare un relay esterno pilotato dal terminale.

Si riportano di seguito le caratteristiche principali del relay interno:

- Tensione e corrente nominale: 2A – 30Vdc
- Max potenza commutabile: 60W
- Max tensione commutabile: 220Vdc
- Max corrente commutabile 2A

Il massimo numero di istanti programmabili nell'arco delle 24 ore è pari a 24 dove per ogni istante è possibile definire l'ora e il minuto in cui il terminale chiuderà il relay e la durata in secondi di chiusura.

Per i dettagli su come impostare il terminale fare riferimento al manuale di uso del software AsyaXess oppure al protocollo di comunicazione con l'host remoto.

5.1.7 SINCRONIZZAZIONE DELL'OROLOGIO DI SISTEMA

Il terminale di rilevazione presenze possiede internamente un orologio al alta precisione con batteria di backup che garantisce il funzionamento anche in assenza di alimentazione generale (terminale spento). Tuttavia per garantire una maggiore precisione, il terminale mediante appositi messaggi inviati al server si sincronizza con esso con una periodicità di 2 ore circa. Si consiglia

pertanto di assicurarsi che l'ora di sistema del server a cui il terminale è connesso sia sincronizzata mediante protocollo NTP su rete internet.



AVVERTENZA

Assicurarsi che il server a cui il terminale è connesso, ha una sincronizzazione giornaliera tramite servizio NTP offerto dalla rete internet. Evitare lunghi periodi di disconnessione del terminale dal server o del server dalla rete internet.

5.2 TERMINALE ACCESSI

Nel paragrafo seguente si descrive l'uso del terminale configurato come accessi. Verranno descritte le varie funzionalità in modo generico rimandando nello specifico al manuale di uso del software di gestione AsyaXess oppure al manuale che descrive il protocollo di interfacciamento del terminale su rete ethernet.

5.2.1 DESCRIZIONE DEL TERMINALE

Nella figura che segue si riporta la foto di un terminale configurato come controllo accessi:



in cui si evidenziano il display grafico 64x128 pixel (rif.1) e la testa di lettura RFID (rif. 2)
Rispetto al terminale presenze non vengono utilizzati i tasti poiché in questo caso l'interfacciamento con l'utente non prevede alcuna selezione.

5.2.2 INDICAZIONE DEL DISPLAY

Nel caso di terminali configurati come accessi (Ingresso/Uscita) i campi visualizzati dal display sono leggermente diversi come si può riscontrare nell'immagine che segue:

INSERIRE FOTO DISPLAY

in particolare il campo che indica in numero terminale contiene 5 caratteri per permettere la visualizzazione di numeri fino a 65535 che il massimo numero di terminali utilizzabili.

Al posto della scritta TecnoAXess troviamo invece l'indicazione se si tratta di un terminale di *Ingresso* oppure di uno di *Uscita*.

Riguardo alla sezione centrale invece la differenza con i terminali di presenze sta nel fatto che in condizioni di standby nelle 4 righe è possibile visualizzare una scritta di default come il nome dell'azienda o lo slogan mentre nel momento di verificare l'accesso consentito o negato, un messaggio comparirà ad indicare se l'accesso è avvenuto oppure è stato negato. Anche nel caso dei terminali di controllo accessi, il server può inviare stringhe che vengono temporaneamente visualizzate sul display per una durata pari a quella impostata.

5.2.3 UTILIZZO DEL LETTORE RFID

L'antenna RFID che consente la lettura delle card assegnate agli utenti si trova in corrispondenza al logo raffigurato nella figura di par. 5.2.1 rif. 2.

Per effettuare un accesso occorre avvicinare la card tenendola orizzontalmente rispetto al piano dove è raffigurato il logo e centrata rispetto ad esso. La distanza di lettura può variare a seconda del tipo di card da 2 a 4 cm. Una volta avvicinata la card attendere l'esito del controllo delle politiche di accesso secondo le quali viene stabilito se l'utente è autorizzato ad entrare oppure no. Un messaggio sul display e un'indicazione sonora, riporteranno l'esito dell'accesso come *ACCESSO CONSENTITO* oppure con *ACCESSO NEGATO*.



AVVERTENZA

Nel caso la card venga allontanata prima della completa lettura o se ci sono errori in lettura, occorre attendere 4~5 secondi prima di riavvicinare la card per effettuare un nuovo tentativo di lettura.

Il tempo che il terminale impiega per la verifica della card dipende dal numero di politiche memorizzate nel terminale, in ogni caso il tempo massimo non eccede mai i 1~2 secondi.

Al verificarsi della condizione di accesso consentito, a seconda della configurazione dei relay impostata si attiva la chiusura del relay per una durata pari al valore impostato in fase di configurazione.

5.2.4 DEFINIZIONE DELLE POLITICHE DI ACCESSO

Le politiche di accesso dette anche regole o policy sono il parametro chiave per i terminali di controllo accessi. Infatti da tale configurazione deriva la sicurezza voluta dal sistema che si sta installando. E' importante perciò leggere attentamente questa sezione e prevedere le politiche di accesso prima dell'installazione o della programmazione delle card.



AVVERTENZA

Prima di programmare le card e assegnarle agli utilizzatori si consiglia di definire con precisione quali saranno le diverse aree di accesso, i gruppi e le persone appartenenti ad un dato gruppo come viene descritto nel paragrafo 5.2.4.

Prima di passare alla definizione delle policy occorre definire con attenzione quelle che saranno le *aree* che il sistema di controllo accessi andrà a regolare e quali saranno i *Gruppi* a cui saranno assegnate una o più persone.

Il sistema TecnoaXess basa le proprie politiche sui gruppi nel senso che una politica viene definita per uno o più gruppi e non per singola card. Ovviamente come vedremo in seguito definendo un gruppo per ogni card è possibile estendere il sistema alla gestione delle policy per card.

Le persone che vengono assegnate ad un dato gruppo ereditano le politiche di accesso del gruppo; tuttavia una data persona può essere associata a più gruppi ereditando quindi tutte le policy di tutti i gruppi a cui appartiene.

Supponiamo che in un'azienda siano presenti le seguenti *aree* delimitate in ogni varco da un terminale di Ingresso e uno di Uscita:

- Uffici amministrazione
- Ufficio tecnico
- Uffici dirigenza
- Spogliatoio operai
- Stabilimento 1
- Stabilimento 2
- Mensa
- Ingresso pedonale azienda

Mentre l'insieme di tutti i dipendenti ed operatori vengono così suddivisi:

- Dirigenza
- Personale amministrativo
- Personale ufficio Tecnico
- Operai gruppo 1
- Operai gruppo 2
- Impresa Pulizie
- Vigilanza
-

Una volta definite le aree e i gruppi si può passare alla definizione delle politiche di accesso.

Poiché le politiche sono associate ad un gruppo si deve prima decidere a quale gruppo applicare la regola che si va a definire; successivamente si stabilisce per quale/i area/e deve valere la regola che si sta definendo.

Ad esempio supponiamo che si voglia definire una regola di accesso per il gruppo definito come "*Operai gruppo1*" che avranno accesso solo nelle ore del proprio turno e nelle aree desiderate come ad esempio *Stabilimento 1, Spogliatoi, ingresso pedonale azienda*; la regola sarà costituita dai seguenti campi:

Regola 1:

Gruppi a cui è applicata la regola → *Operai gruppo1*

Area o aree a cui deve essere applicata la regola → *Stabilimento 1, Spogliatoi, ingresso pedonale*

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → dal Lunedì al Venerdì dalle ore 05:00 alle ore 22:00

In questo caso tutte le card che avranno come gruppi di appartenenza *Operai gruppo 1* ereditano la regola appena definita e per tutto l'anno potranno entrare alle aree definite dal lunedì al venerdì dalle ore 5:00 alle ore 22:00.

Se ad esempio si volesse far entrare il gruppo *Operai gruppo 1* anche il sabato dalle ore 05:00 alle 14:00 occorre definire una nuova regola del tipo:

Regola 2:

Gruppi a cui è applicata la regola → *Operai gruppo1*

Area o aree a cui deve essere applicata la regola → *Stabilimento 1, Spogliatoi, ingresso pedonale*

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → ogni sabato dalle ore 05:00 alle ore 14:00

Per quanto riguarda la vigilanza per esempio supponiamo che sia presente in azienda la notte e nei giorni festivi; si avrà

Regola 3:

Gruppi a cui è applicata la regola → *Vigilanza*

Area o aree a cui deve essere applicata la regola → Tutte le aree

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → dal lunedì al venerdì dalle ore 22:00 alle ore 05:00

Regola 4:

Gruppi a cui è applicata la regola → *Vigilanza*

Area o aree a cui deve essere applicata la regola → Tutte le aree

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → ogni sabato dalle ore 14:00 alle ore 05:00

Regola 5:

Gruppi a cui è applicata la regola → *Vigilanza*

Area o aree a cui deve essere applicata la regola → Tutte le aree

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → ogni domenica dalle ore 00:00 alle ore 24:00

Se ad esempio un gruppo ha delle politiche che contengono per interno quelle già definite, non è necessario che vengano ridefinite nuovamente ma sarà sufficiente assegnare alla card anche il gruppo di cui contiene le policy. Nel esempio precedente se il gruppo *Personale Ufficio tecnico* ha le stesse politiche di accesso dei gruppi *Operaio Gruppo 1* e *Operaio Gruppo 2* più delle politiche per quanto riguarda l'area *Ufficio Tecnico* è sufficiente definire solo le nuove regole:

Regola 6:

Gruppi a cui è applicata la regola → *Personale ufficio tecnico*

Area o aree a cui deve essere applicata la regola → *Ufficio tecnico*

Periodo di validità della regola → dal 01 gennaio al 31 dicembre

Fasce Orarie → dal Lunedì al Venerdì dalle ore 05:00 alle ore 22:00

e al momento dell'associazione del dipendente Mario Rossi dell'ufficio tecnico ai gruppi è sufficiente assegnarli i gruppi *Personale ufficio tecnico*, *Operai gruppo1*, *Operai gruppo2*; in questo modo Mario Rossi avrà come politiche di accesso *Regola1*, *Regola2*, *Regola6* più le eventuali regole definite per il gruppo *Operai gruppo2*. Il terminale che leggerà la card di Mario Rossi processerà tutte le regole associate a ciascun gruppo memorizzato nella card consentendo l'accesso se almeno una politica è soddisfatta.

5.2.5 GESTIONE DELL'ANTI PASS-BACK

Il sistema di controllo accessi TecnoXess ha la possibilità di gestire due livelli di anti pass-back che di seguito verranno indicati come *anti pass-back hard* e *anti pass-back soft*. Nel primo caso una card che ha effettuato un accesso in una data area non può accedere a nessun'altra area se

prima non transita in un terminale di uscita appartenente all'area in cui si trova. Nel secondo caso invece il terminale di ingresso controlla solo che la card che sta tentando di accedere all'area a cui il terminale appartiene non sia la stessa in cui la card si trova. Nel caso di anti pass-back di tipo hard se una card ha varcato l'accesso all'area 1, finché non varca un terminale di uscita dall'area 1 non può entrare in nessun'altra area; nel caso di anti pass-back soft invece la card che ha avuto accesso all'area 1 può accedere ai varchi che danno accesso a tutte le aree diverse dalla 1 a cui appartiene. Il livello minore di anti pass-back quindi è usato solo per evitare che una persona che si trova in una determinata area, passando la sua card ad altre persone, permetta l'accesso alla stessa area. Il livello maggiore di sicurezza offerto dall'anti pass-back di tipo hard invece obbliga una data persona ad uscire dall'area in cui si trova per poter accedere alla successiva.

Segue una tabella riassuntiva dei casi di accesso consentito o negato nel caso dei due livelli di anti pass-back:

Condizione rilevata dal terminale di ingresso all'area X	Anti pass-back hard	Anti pass-back soft
Ultimo accesso della card come ingresso all'area X	Accesso Negato	Accesso Negato
Ultimo accesso della card come ingresso all'area Y	Accesso Negato	Accesso Consentito
Ultimo accesso della card come uscita dall'area X o da aree ≠ da X	Accesso Consentito	Accesso Consentito

5.2.6 GESTIONE DELLA SUPERVISIONE DELL'ACCESSO

I terminali TecnoXess hanno la possibilità di gestire fino a tre ingressi bilanciati per supervisionare un varco segnalando con un messaggio di allarme e con l'attivazione di sirene o lampeggianti un eventuale forzatura del varco.

Attivando la supervisione dell'accesso il terminale controlla gli ingressi a cui sono collegati sensori di prossimità posti sul varco; nel momento in cui viene rilevato un'apertura non autorizzata o un tentativo di sabotaggio il terminale invia un messaggio al server e contestualmente attiva il relay 2 (pin M2-3 M2-4) a cui può essere collegato un dispositivo di segnalazione come una sirena o un lampeggiante.

In tale condizione apparirà un messaggio sul display "ACCESSO VIOLATO" e il terminale bloccherà il varco evitando successivi accessi finché l'host remoto non invia una segnalazione al terminale di aver processato l'allarme.

Nel caso della supervisione dell'ingressi SV1 (M4-3) il terminale controlla l'apertura del varco e non genera l'allarme solo se rileva un'apertura a seguito di un accesso consentito.

Nel caso della supervisione dell'ingresso relativo alla richiesta di uscita di emergenza SV2 (M4-2) il terminale controlla in ogni caso che non si verificano tagli o corto circuiti e nel momento in cui rileva una richiesta di emergenza (contatto aperto) provvede ad inviare un messaggio di allarme al server e contestualmente mantiene il varco aperto per consentire l'uscita indiscriminata attraverso il varco. Nel momento in cui viene rilevata la pressione del tasto di emergenza si attiva anche il relay 2 a cui può essere collegato un dispositivo di segnalazione della situazione di emergenza.

In fine anche il terzo ingresso di supervisione come il secondo (richiesta di emergenza) funziona con logica normalmente aperta e genera un messaggio generico che può essere gestito a seconda delle esigenze.

Per il collegamento dei sensori fare riferimento al par. 3.2.4 mentre per la gestione software fare riferimento al manuale di AsyaXess oppure al protocollo di comunicazione con l'host remoto.

Utilizzando come mostrato nel paragrafo 3.2.4 due resistenze da 10K Ω è possibile rilevare oltre alla chiusura o apertura del contatto anche eventuali tagli del cavo che collega il sensore al terminale oppure eventuali corto circuito ai capi del sensore.



AVVERTENZA

Per evitare manomissione dei contatti di supervisione si consiglia di inserire le due resistenze in prossimità del contatto e protette da eventuali manomissioni.

5.2.7 SINCRONIZZAZIONE DELL'OROLOGIO DI SISTEMA

Il terminale di rilevazione presenze possiede internamente un orologio al alta precisione con batteria di backup che garantisce il funzionamento anche in assenza di alimentazione generale (terminale spento). Tuttavia per garantire una maggiore precisione, il terminale mediante appositi messaggi inviati al server si sincronizza con esso con una periodicità di 2 ore circa. Si consiglia pertanto di assicurarsi che l'ora di sistema del server a cui il terminale è connesso sia sincronizzata mediante protocollo NTP su rete internet.



AVVERTENZA

Assicurarsi che il server a cui il terminale è connesso, ha una sincronizzazione giornaliera tramite servizio NTP offerto dalla rete internet. Evitare lunghi periodi di disconnessione del terminale dal server o del server dalla rete internet.

5.3 TERMINALE CONTROLLO ACCESSI WIEGAND

Nel paragrafo seguente si descrive l'uso del terminale per controllo accessi con uscita Wiegand. Essendo il terminale un lettore di card RFID Mifare, per informazioni relative al funzionamento del sistema di controllo accessi occorre fare riferimento al manuale di uso e manutenzione del sistema installato.

5.3.1 INDICAZIONE DEL DISPLAY

Nel caso di terminali configurati come lettori RFID Wiegand i campi visualizzati dal display sono rappresentati nell'immagine che segue:

INSERIRE FOTO DISPLAY+DESCRIZIONE CAMPI

5.3.2 UTILIZZO DEL LETTORE RFID

L'antenna RFID che consente la lettura delle card utenti si trova in corrispondenza al logo raffigurato nella figura di par. 5.2.1 rif. 2.

Per effettuare un accesso occorre avvicinare la card tenendola orizzontalmente rispetto al piano dove è raffigurato il logo e centrata rispetto ad esso. La distanza di lettura può variare a seconda del tipo di card da 2 a 4 cm. Una volta avvicinata la card attendere il segnale acustico che indica l'avvenuta lettura della card e il corrispondente invio su bus wiegand del ID card alla centrale di controllo accessi. L'esito del controllo delle politiche di accesso secondo le quali viene stabilito se l'utente è autorizzato ad entrare oppure no avviene a livello di centrale a cui il lettore è connesso. L'eventuale accesso verrà direttamente consentito o negato dalla centrale stessa.

Nel caso in cui la segnalazione "Led Green" è gestita dal sistema di controllo accessi a cui il lettore è connesso, un messaggio sul display, riporteranno l'esito dell'accesso come *ACCESSO CONSENTITO*.

Nel caso in cui la segnalazione "Led Red" è gestita dal sistema di controllo accessi a cui il lettore è connesso, un messaggio sul display, riporteranno l'esito dell'accesso come *ACCESSO NEGATO*. Infine se la segnalazione "Beeper" è gestita dalla centrale, il buzzer interno suonerà in corrispondenza dell'avvenuta abilitazione o meno a seconda della configurazione della centrale accessi.

5.3.3 CONFIGURAZIONE DEL TERMINALE WIEGAND

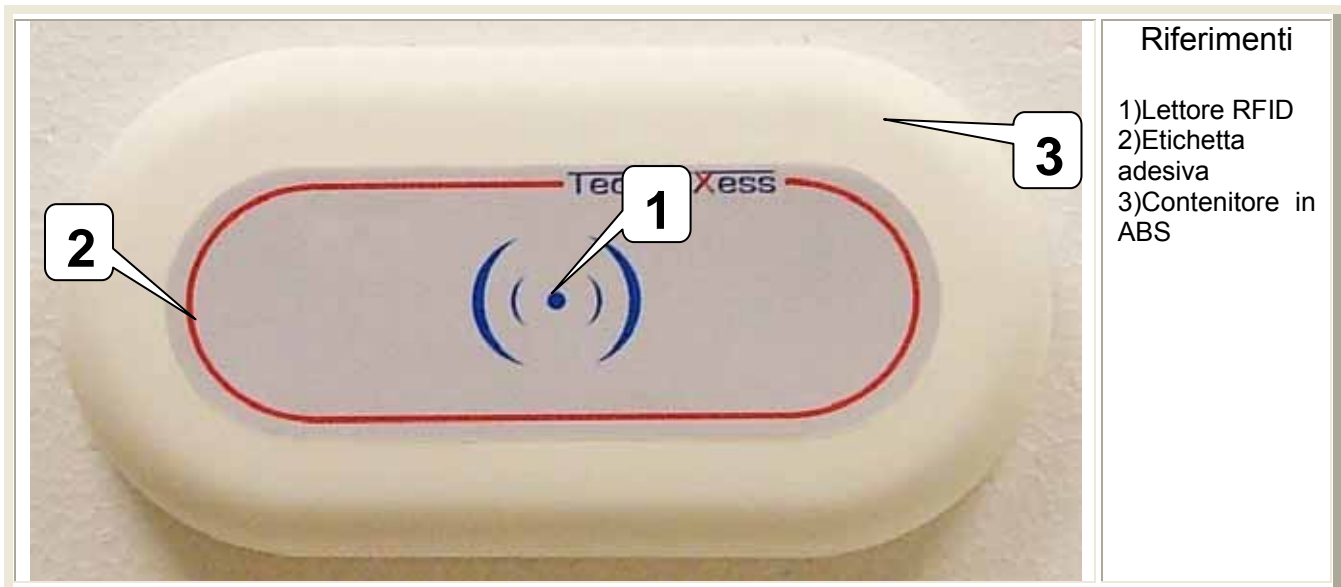
asdsad

6 ANTENNA DI RIBATTUTA

6.1 DESCRIZIONE DEL PRODOTTO

L'antenna di ribattuta individuata dal codice TRS0090 è un accessorio al sistema di controllo accessi TecnoaXess utile nel caso in cui si voglia controllare un varco che delimita l'edificio verso l'esterno. Le caratteristiche del dispositivo come il grado di protezione IP65 e l'assenza di relay interni che abilitano l'accesso ne caratterizzano l'uso in situazioni dove si deve controllare un varco esterno dove si deve assicurare la massima resistenza agli agenti atmosferici e la massima sicurezza alle manomissioni.

In questo caso infatti, un terminale della famiglia TecnoaXess può essere installato nei pressi del varco e all'interno dell'edificio; collegando l'antenna di ribattuta fissata all'esterno dell'edificio al terminale interno, questo è in grado di gestire i transiti sia in ingresso che in uscita. Di seguito si riporta una foto del dispositivo con indicazione dei vari componenti:



Riferimenti

- 1) Lettore RFID
- 2) Etichetta adesiva
- 3) Contenitore in ABS

6.2 CARATTERISTICHE TECNICHE

Tensione di alimentazione:	5 Vdc (±5%)
Consumo massimo:	120mA
Dimensioni (HxLxP):	8,5 cm x 16,5 cm x 2 cm
Contenitore	ABS (plastico)
Range di temperatura di stoccaggio:	- 40°C ÷ + 150 °C
Range di temperatura di funzionamento:	- 10°C ÷ + 85 °C
Umidità:	85% @ 40 °C (non condensante)
Grado di protezione:	IP 65
Standard card RFID	ISO14443A/B (MIFARE)
Distanza di lettura card	3 ~ 8cm (*)
Segnalazione sonora	Buzzer interno
Interfacce di trasmissione dati	- RS232
Distanze di trasmissione dati	15m.
Batteria tampone al litio	Opzionale
Durata della batteria tampone	Dipendente dalla configurazione.
Gestione antenna di ribattuta	Su bus RS232.
Distanza massima antenna di ribattuta	~ 15 m

(*)La distanza di lettura può dipendere dalla tecnologia di fabbricazione della card e dalle sue dimensioni.

6.3 DIMENSIONI MECCANICHE

6.4 FISSAGGIO DELL'ANTENNA

Per fissare l'antenna su una parete verticale seguire le indicazioni riportate di seguito:



6.5 COLLEGAMENTO E INSTALLAZIONE DELL'ANTENNA

L'antenna viene fornita con un cavo quadri polare già assemblato di lunghezza 2 metri circa. Essendo l'antenna resinata al suo interno non è possibile sostituire il cavo fornito in dotazione pertanto nel caso in cui la lunghezza sia insufficiente occorre giuntare con un cavo equivalente in termini di numero di poli e di sezione del cavo.

Per il collegamento dell'antenna al terminale di accessi utilizzare il morsetto fornito all'interno della scatola ed effettuare i seguenti collegamenti:



AVVERTENZA



Prima di collegare l'antenna al bus RS232 verificare che il terminale e tutti gli apparecchi ad esso connesso siano scollegati dalla linea di alimentazione.



ATTENZIONE



Condizioni di massimo utilizzo previste dallo standard RS232:

- *Massima distanza di trasmissione = 15 m*
- *Massima tensione ai capi = ± 12 Vdc.*

Connessione lato terminale	Cavo di collegamento antenna
M6-1 +5V (VCC)	Rosso
M6-2 RS232 ricezione dati	-
M6-3 RS232 trasmissione dati	-
M6-4 GND	Nero

6.6 CONFIGURAZIONE DEL TERMINALE

Come espresso nel paragrafo 4.1 ai punti G ed H, il terminale di default all'accensione controlla l'eventuale presenza di un'antenna di ribattuta e nel caso di riconoscimento si predispose per il suo utilizzo senza alcuna necessità di configurazione.

Al termine del collegamento pertanto è sufficiente accendere il terminale e attendere il suo avvio per testare l'antenna.

Nel caso in cui non venisse rilevata, controllare i collegamenti effettuati e controllare che non siano state abilitate le tracce di Debug in fase di configurazione (Par. 4.1 punto G).

6.7 UTILIZZO DELL'ANTENNA

Nel paragrafo seguente si descrive l'uso dell'antenna una volta collegata ad un terminale.

6.7.1 UTILIZZO DEL LETTORE RFID

L'antenna RFID che consente la lettura delle card assegnate agli utenti si trova in corrispondenza al logo raffigurato nella figura di par. 6.1 rif. 1.

Per effettuare una timbratura occorre avvicinare la card tenendola orizzontalmente rispetto al piano dove è raffigurato il logo e centrata rispetto ad esso. La distanza di lettura può variare a seconda del tipo di card da 3 a 6 cm. Una volta avvicinata la card attendere l'avvenuta lettura indicata dal suono del buzzer interno. Due tipi di segnalazioni sonore identificano l'ingresso consentito e l'ingresso negato.



AVVERTENZA

Nel caso la card venga allontanata prima della completa lettura o ci sono errori in lettura, occorre attendere 4~5 secondi prima di riavvicinare la card per effettuare un nuovo tentativo di lettura.

Nel caso in cui il terminale è configurato come terminale di ingresso, l'antenna assumerà la funzione di uscita pertanto registrerà l'avvenuto passaggio senza applicare le politiche di accesso. Viceversa nel caso in cui il terminale è configurato come uscita, l'antenna di ribattuta assume la funzione di ingresso controllando l'effettivo rispetto delle politiche memorizzate sul terminale.