



 **NOTIFIER**<sup>®</sup>  
by Honeywell



# CS600

Manuale di  
Programmazione

# INDICE

<b>1. INTRODUZIONE</b>	<b>4</b>
1.1. PROCEDURA DI PRIMA ACCENSIONE DELLA CENTRALE CS600.	4
1.2. GENERALITÀ	5
1.3. PROGRAMMAZIONE	6
1.3.1. Condizioni	8
1.3.2. Attivazioni	8
1.3.3. Stati	8
1.3.4. Comandi	8
<b>2. INSTALLAZIONE ED AVVIO</b>	<b>9</b>
2.1. INSTALLAZIONE DEL SOFTWARE DI CONFIGURAZIONE	9
2.2. AVVIO DEL SOFTWARE DI CONFIGURAZIONE	17
2.3. PAGINA PRINCIPALE	18
<b>3. PK SECURITY 600 – MENÙ E CONFIGURAZIONI</b>	<b>20</b>
3.1. LOG IN	20
3.2. CONNESSIONE MANUALE	20
3.2.1. Connessione Diretta	20
3.2.2. Connessione Remota via Modem	21
3.2.3. Connessione Remota via TCP-IP	21
3.2.3.1. Settaggio dell'indirizzo IP di centrale	21
3.2.3.2. Connessione manuale su rete ETH	22
3.3. SET-UP NUMERO MACRO-IMPIANTO	23
3.4. RUBRICA CONNESSIONI	25
3.5. DISCONNETTI	26
3.6. INVIA A CPU	26
3.7. RICEVI DA CPU	26
3.8. SINCRONIZZA CPU	26
3.9. RICEZIONE EVENTI	26
3.10. VISUALIZZAZIONE EVENTI	27
3.11. RICEZIONE EVENTI EN50131	27
3.12. VISUALIZZAZIONE EVENTI EN50131	27
3.13. GESTIONE CLIENTI E IMPIANTI	28
3.13.1. Inserisci Cliente	28
3.13.2. Apri Impianto Esistente	28
3.13.3. Apri Come...	29
Esporta Impianto	29
3.13.4. Importa Impianto	29
3.14. SETUP RUBRICA CONNESSIONI	30
3.15. SETUP PERIFERICHE DI CONNESSIONE	31
3.16. GESTIONE STAMPA	32
3.17. CONFIGURAZIONE OPERATORI PC	32
3.18. CONFIGURAZIONE CENTRALE	33
3.18.1. Setup	33
3.18.2. Programmazione	44
3.18.2.1. Attivazioni Uscite / Zone Uscite	45
3.18.2.2. Sinottici / Segnalazioni aggiuntive	46
3.18.2.3. Comandi	47
3.18.3. Dettagli	47
3.18.4. Comandi	48
3.18.5. Binding	48
3.18.6. Diagnostica	49
3.18.7. Upgrade Firmware Periferiche	49
3.18.8. Upgrade Firmware CPU	50
3.19. CONFIGURAZIONE IMPIANTI	51
3.19.1. MacroZone Ingressi Associate	52
3.19.2. MacroZone Uscite Associate	52
3.19.3. Usato In...	52
3.20. CONFIGURAZIONE MACROZONE E ZONE INGRESSI	53
3.20.1. Macro Zone – Zone Ingressi/Uscite Associate	55
3.21. CONFIGURAZIONE PERIFERICHE INGRESSI / USCITE	56

3.21.1.	<i>Configurazione Periferica IND</i>	57
3.21.1.1.	Generale	57
3.21.1.2.	Diagnostica	58
3.21.1.3.	Ingressi/Uscite	58
3.21.2.	<i>Configurazione periferica LCD/AEI/RXE</i>	59
3.21.2.1.	Generale Terminale	59
3.21.2.2.	Configurazione Terminale	60
3.21.2.3.	Controllo Accessi Terminale	61
3.21.2.4.	Profili Terminale	62
3.21.2.5.	Prog.Tasti e LED Terminale	62
3.21.2.6.	MacroZone - Terminale	64
3.21.2.7.	Messaggi - Terminale	64
3.21.2.8.	Diagnostica - Terminale	64
3.21.2.9.	Ingressi/Uscite- Terminale	65
3.21.3.	<i>Automatismi e Azioni</i>	65
3.21.3.1.	Generale	65
3.21.3.2.	Diagnostica	66
3.21.3.3.	Ingressi/Uscite	66
3.21.4.	<i>Configurazione di un'uscita "Automatismo"</i>	66
3.21.5.	<i>Configurazione di un'uscita "Azione"</i>	68
3.21.6.	<i>Configurazione di un'ingresso digitale</i>	69
3.21.7.	<i>Configurazione di un'uscita digitale</i>	72
3.21.8.	<i>PERIFERICA SERV</i>	73
3.21.8.1.	Generale	74
3.21.8.2.	Diagnostica	74
3.21.8.3.	Ingressi/Uscite	74
3.21.9.	<i>PERIFERICA MAB</i>	75
3.21.9.1.	Generale	75
3.21.9.2.	Diagnostica	76
3.21.9.3.	Ingressi/Uscite	76
3.21.10.	<i>PERIFERICA LCV</i>	77
3.22.	PROFILI, OPERATORI E GRUPPI	78
3.22.1.	<i>Operatori</i>	78
3.22.2.	<i>Profili</i>	80
3.22.3.	<i>Livelli</i>	81
3.22.4.	<i>Gruppi</i>	82
3.23.	FASCE ORARIE	83
3.24.	CALENDARIO	84
3.25.	VERIFICA STRUTTURA	85
<b>4.</b>	<b>IMPIANTO BASE</b>	<b>88</b>
4.1.	STRUTTURA LOGICA	88
4.1.1.	<i>Impianto Servizi – Struttura Ingressi</i>	89
4.1.2.	<i>Impianto Servizi – Struttura Uscite</i>	89
4.1.3.	<i>Impianto Antifurto – Struttura Ingressi</i>	90
4.1.4.	<i>Impianto Antifurto – Struttura Uscite</i>	91
4.2.	PREDISPOSIZIONI DEFAULT – LCD600S	91
<b>5.</b>	<b>PASSWORD DEL SISTEMA</b>	<b>92</b>
<b>6.</b>	<b>TIPOLOGIA ED ETICHETTE DEGLI INGRESSI DIGITALI</b>	<b>94</b>
6.1.	TIPOLOGIE DEGLI INGRESSI DIGITALI	94
6.2.	ETICHETTE DEGLI INGRESSI DIGITALI	94
6.2.1.	<i>Manomissione / Tamper</i>	94
6.2.2.	<i>Manca Rete</i>	95
6.2.3.	<i>Batteria</i>	95
6.2.4.	<i>Antintrusione</i>	96
	Eventi Antintrusione / Attivazione Uscite	96
6.2.5.	<i>Antintrusione 24</i>	97
6.2.6.	<i>Porte di Sicurezza C.M.</i>	98
6.2.7.	<i>Porte di Sicurezza Blocchi</i>	98
6.2.8.	<i>Rapina</i>	98
6.2.9.	<i>Panico</i>	99
6.2.10.	<i>Incendio</i>	100
6.2.11.	<i>Servizio</i>	101
6.2.12.	<i>Tecnologici</i>	101

6.2.13.	<i>Fusibili</i> -----	101
6.2.14.	<i>Sirena</i> -----	101
6.2.15.	<i>Riserva</i> -----	102
6.2.16.	<i>ATS</i> -----	102
<b>7.</b>	<b>TABELLE DI RIFERIMENTO</b> -----	<b>102</b>
7.1.	LIVELLI DI ACCESSO-----	102
7.2.	FUNZIONALITÀ-----	104
7.2.1.	<i>Fuori Servizio – CS600 Grado 3</i> -----	104
7.2.2.	<i>Fuori Servizio – CS600 Grado 2</i> -----	104
7.2.3.	<i>Reset – CS600 Grado 3</i> -----	105
7.2.4.	<i>Reset – CS600 Grado 2</i> -----	105
7.2.5.	<i>Isolamento – CS600 Grado 3</i> -----	105
7.2.6.	<i>Isolamento – CS600 Grado 2</i> -----	106
7.2.7.	<i>Gestione Installatore – CS600 Grado 3</i> -----	106
7.2.8.	<i>Gestione Installatore – CS600 Grado 2</i> -----	106
7.2.9.	<i>Gestione Utenti Livello 3 – CS600 Grado 3</i> -----	107
7.2.10.	<i>Gestione Utenti Livello 3 – CS600 Grado 2</i> -----	107
7.2.11.	<i>Gestione CARICO dati da CS600 a Grado 3 → verso PK Security600</i> -----	107
7.2.12.	<i>Gestione CARICO dati da CS600 a Grado 2 → verso PK Security600</i> -----	108
7.2.13.	<i>Gestione SCARICO dati da PK Security600 → verso CS600 a Grado 3</i> -----	108
7.2.14.	<i>Gestione SCARICO dati da PKSecurity600 → verso CS600 a Grado 2</i> -----	108
7.3.	CONTACT-ID-----	109
<b>8.</b>	<b>UTILITY</b> -----	<b>114</b>
8.1.1.	<i>Integrazione Euronet</i> -----	114
8.1.2.	<i>Come programmare antintrusione dall'impianto base</i> -----	115
8.1.3.	<i>Configurare un Operatore con Badge/Radiocomando</i> -----	115
8.1.4.	<i>Parametri Accesso DataBase</i> -----	115

Versione Manuale	Data	Vers. PKSecurity600
A16	09-2013	1.0.028 o successivi

## 1. Introduzione

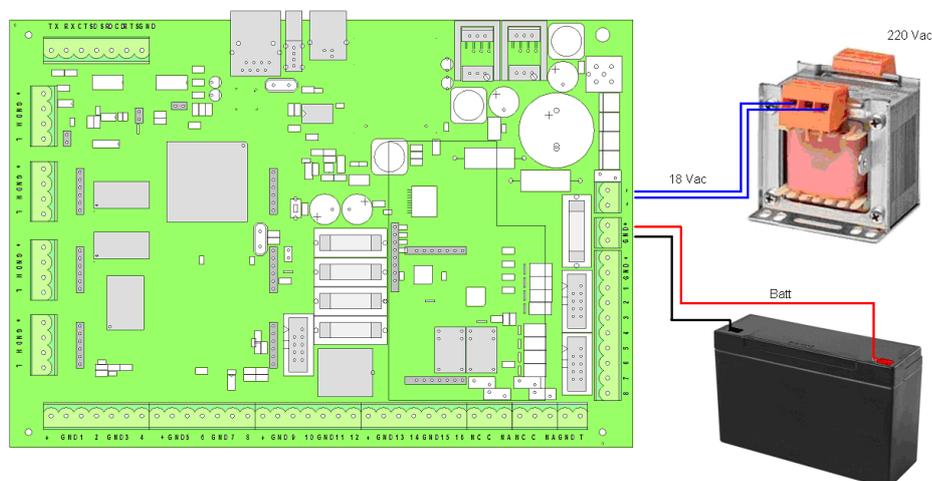
### 1.1. Procedura di prima accensione della centrale CS600.

- Una volta terminata l'installazione delle periferiche di campo e verificati i cablaggi in centrale, collegare la batteria e fornire l'alimentazione di rete 230Vac al trasformatore, attendere circa 15 secondi affinché il sistema sia pronto a ricevere una nuova programmazione tramite il software in dotazione PK-Security600. Tutti i terminali LCD600s, AEI-485, RXE e le periferiche IND8/4, ALI8/8 risultano in questa fase non operative, in quanto non ancora riconosciute dalla centrale.
- A centrale alimentata, il led "L3" sarà di color arancio pulsante durante la ricarica della batteria, se sarà verde fisso, significa che la batteria ha terminato il ciclo di carica. Lo stesso led "L3", risulterà invece rosso fisso in caso mancanza rete 230Vac.

**N.B.:** Se l'alimentazione di rete 230Vac, non è disponibile in fase di start-up impianto, è possibile alimentare la centrale **temporaneamente** solo a batteria. Per poter abilitare la centrale a funzionare solo a batteria (che dovrà essere carica) occorre cortocircuitare per circa 5 secondi, il morsetto +batt (JP13) con uno dei due morsetti 18Vac (JP14 – connessione trasformatore).

Controllare inoltre che la Ram sia tenuta in vita dalla batteria interna da 3,6 V, andando quindi a cortocircuitare i due pin del jumper P4.

Alimentazione della scheda base CS600.



**Prima di procedere alla programmazione da software, eseguire i seguenti passaggi:**

- Mettere in servizio il terminale LCD600S n°121 (linea 1 – terminale 1) digitando "121" sul terminale stesso.

- Accedere come utente supervisor (di fabbrica codice **111111**) e premere invio.
- Entrare nel menù “DATA” e aggiornare la data e ora di centrale.
- Entrare successivamente nel menù “Operatori > Installatore” e metterlo in servizio. In questo modo, verrà abilitato l’operatore coi criteri d’accesso necessari alla configurazione e connessione verso la centrale tramite il programma di configurazione PKSecurity600. L’operatore installatore (PIN di fabbrica = 999999) sarà abilitato fino alle 24:00 del corrente giorno dopodiché la CS600 lo metterà automaticamente “fuori servizio”.
- Eseguire la procedura di messa in servizio/binding delle periferiche installate sulle 4 linee di centrale.
- Accedere come Installatore da terminale LCD600S e comandare lo stato di “In servizio” sulle periferiche TAMPER di ogni linea, questa procedura memorizzerà automaticamente tutti gli indirizzi delle periferiche IND8/4, ALI8/8, e RX-E; per mettere in servizio gli inseritori trasponder AEI-485, collegarne uno alla volta ed impartire il comando di “In servizio” sulla periferica di linea per ogni AEI-485 collegato in successione. Per mettere in servizio gli LCD600S presenti, digitare direttamente l’indirizzo dalla tastiera. E’ possibile cancellare il binding delle periferiche manualmente (vedi scheda tecnica) o impartendo il comando di Cancella binding da terminale LCD600S.
- Procedere alla configurazione della CS600 tramite software PKSecurity600 consultando il manuale di programmazione.

## 1.2. Generalità

La centrale CS600 è una centrale antintrusione con funzionalità estese all'antirapina, al controllo accessi e agli allarmi tecnologici e incendio.

Sia l'hardware che il software sono strutturati per rispondere alle normative EN50131, permettendone il funzionamento a grado di sicurezza 3 e in funzione delle impostazioni anche a grado 2 o 1.

La flessibilità della struttura permette di realizzare rapidamente dal semplice impianto con poche zone fino a gestioni complesse con integrazioni con più centrali e con il sistema Euro-net.

I terminali LCD600S forniscono un'interfaccia utente semplice e completa già nella configurazione base, grazie alla programmazione dei tasti funzione e dei relativi led sinottici è possibile semplificare ulteriormente l'interazione col sistema.

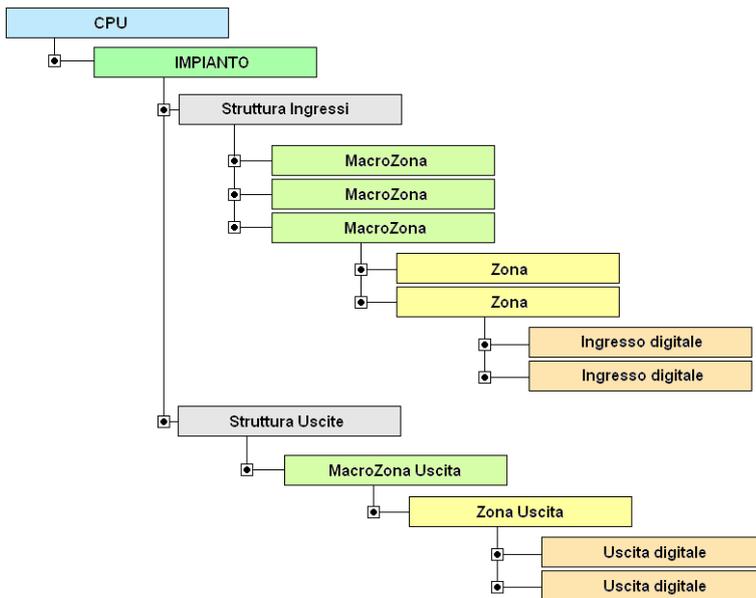
La gestione delle abilitazioni degli utenti basata su Profili configurabili permette di personalizzare secondo le necessità il funzionamento del sistema.

La programmazione della CS600 può essere eseguita esclusivamente da PKsecurity600.

Le modalità di configurazione sono molteplici e applicabili in base alle necessità.

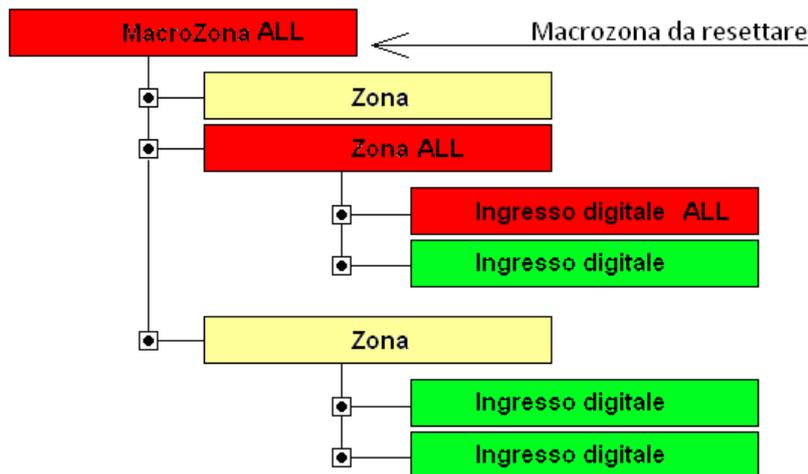
## 1.3. Programmazione

Il funzionamento della centrale si basa sulle strutture gerarchiche degli ingressi e delle uscite. Gli ingressi e le uscite fisiche vengono associate a Zone logiche, che a loro volta sono associate a una o più Macrozone logiche, le quali sono contenute in uno degli otto impianti disponibili, che fanno capo direttamente alla CPU.



Gli stati ovvero la condizione che un oggetto può assumere (es: un ingresso digitale può assumere lo stato di ALLARME, TAGLIO, MANOMISSIONE, CORTO) si estendono attraverso la struttura dal figlio al padre ( da Ingresso Digitale verso la propria Zona, poi da Zona verso la propria MacroZona e di conseguenza alla CPU ) e i comandi viceversa dal padre al figlio ( da MacroZona come primo livello a scendere fino all'ingresso o uscita digitale ). Intervenendo ai vari livelli della struttura si ottengono:

Per gli stati, informazioni già aggregate e per i comandi la propagazione a tutti gli oggetti sottostanti, fino ad arrivare agli ingressi e alle uscite fisiche.



Le attivazioni delle uscite digitali vengono garantite dalle programmazioni di attivazione per allarme o stato, configurate direttamente dalle proprietà della CPU o Zone/Macrozone di ingresso.

I comandi, essendo estendibili dal Padre al figlio possono essere effettuati direttamente sull'ingresso digitale o da Zona/Macrozona padre.

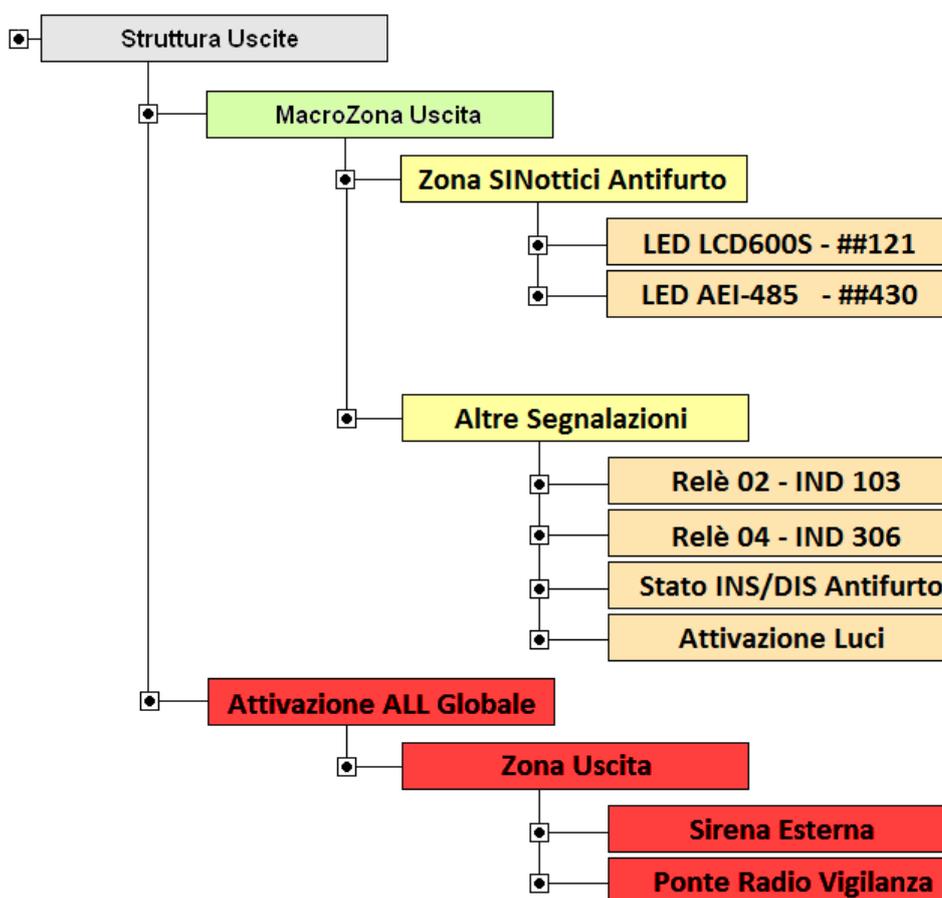
Nell'esempio in figura sopra viene riportata la suddivisione logica della struttura ingressi attraverso una MacroZona contenuta in uno degli 8 impianti disponibili, che identifica la struttura da proteggere nel suo complesso (es.: capannone, abitazione ...) suddivisa a sua volta in nr° 3 Zone che possono identificare stanze/locali o sezioni da proteggere.

All'interno delle zone troviamo gli ingressi digitali (volumetrici, contatti magnetici, barriere...).

Gli stati degli ingressi dipendono dalla condizione fisica che assumono in funzione del tipo di bilanciamento scelto tra Singolo, Doppio, Quadruplo o normalmente aperti o chiusi, dell'etichetta assegnata che ne identifica la funzionalità (es.: Panico, Antincendio, Rapina, Antintrusione, 24H...) e dalla condizione di inserimento / disinserimento della zona alla quale appartengono.

Le etichette permettono di associare ad un'unica zona più ingressi con diverse funzionalità, semplificando la struttura e la gestione del sistema. Ad esempio nella stessa zona possono coesistere ingressi etichettati come Antintrusione, Tamper, Manca Rete, ecc., senza creare problemi di segnalazioni indesiderate in quanto la CS600 è in grado di gestire segnalazioni differenti e mantenendo il rispetto della normativa EN50131 in merito alla gestione dell'inibizione all'inserimento, alle esclusioni, al reset e tutte le parzializzazioni configurate nel sistema.

Sempre in figura, attraverso la colorazione rossa delle caselle viene identificata come la condizione di allarme generata da un ingresso digitale venga estesa alla Zona e MacroZona alla quale è associato. Una volta che la condizione di allarme è cessata per resettare la condizione di memoria di allarme è possibile effettuare il reset manuale o automatico da LCD600S o sulla MacroZona o sull'ingresso digitale.



Nell'immagine sopra viene riportata la modalità in cui è consigliato gestire le attivazioni, le segnalazioni e i sinottici che servono a riportare sui LED tricolori dei terminali LCD600S lo stato degli oggetti di campo della centrale CS600.

Dalla figura si può notare che nella Struttura Uscite sono state create n°2 MacroZone Uscite, che servono ad identificare le Macro attivazioni, per esempio "Segnalazioni di allarme" oppure "Segnalazioni Sinottiche".

All'interno delle MacroZone troviamo rispettivamente 2 e 1 Zona-uscite che vengono utilizzate per suddividere e personalizzare le Macro attivazioni.

Come ultimo livello troviamo le uscite digitali che fisicamente subiscono i comandi impartiti in modo manuale o automatico alle MacroZone o alle Zone uscita.

Questa suddivisione gerarchica viene utilizzata principalmente per semplificare e ridurre il numero delle programmazioni da eseguire.

Prendiamo per esempio la zona uscita che comanda le segnalazioni sinottiche da riportare su tutti i terminali LCD600S installati in campo.

Eseguendo la programmazione direttamente sulla Zona Uscita sarà necessario solo associare alla zona programmata i LED dei terminali interessati.

In questo modo non sarà necessario effettuare le programmazioni sul singolo LED riducendo i tempi di programmazione.

E' possibile quindi effettuare o eseguire dei comandi come per esempio Inserimento/Disinserimento o Attivazione/Riposo direttamente sulla Zona o MacroZona ingresso/uscita capostipite.

### **1.3.1. Condizioni**

Per tutti gli oggetti dell'impianto sono disponibili delle condizioni/stati grazie ai quali è possibile comandare uscite / zone uscite. Questi comandi sono di due tipi: "Attivazioni" e "Stati".

Per le Zone e Macrozone ingressi sono disponibili anche delle associazioni ad Ingressi / Zone Ingressi utilizzati come comandi (tale parametro degrada la centrale a Fuori Norma, quindi non conforme EN50131).

### **1.3.2. Attivazioni**

Le attivazioni attivano l'uscita / zona uscita al verificarsi della condizione scelta ma non la mettono a riposo quando la condizione non è più presente.

Il riposo delle Zone uscite/uscite associate ad una condizione di attivazione può avvenire in tre modi:

- al reset di uno degli eventi che ha generato la condizione, se abilitato il riposo con reset
- alla scadenza del tempo di attivazione impostato nelle proprietà dell'uscita
- con un comando di riposo impartito da terminale LCD600S, da supervisione o da altra azione programmata.

### **1.3.3. Stati**

Gli stati attivano l'uscita / zona uscita al verificarsi della condizione scelta e la mettono a riposo quando la condizione non è più presente. Un tipo particolare di stato è il sinottico, normalmente usato per comandare dei LED tricolore, comanda l'uscita secondo una logica più complessa, nella quale sono previsti modalità di attivazione diverse, ad esempio lampeggio in colorazioni differenti.

In funzione dell'oggetto da gestire sono disponibili sinottici specifici già configurati che vanno scelti in base delle segnalazioni richieste.

### **1.3.4. Comandi**

Permettono di utilizzare un ingresso di una periferica IND8/4 o ALI8/8 per impartire un comando all'oggetto che si sta programmando, dato che non possibile riconoscere l'utente che lo attiva, questi comandi non sono conformi alla normativa EN50131.

I comandi disponibili sono:

- Chiavi di Inserimento / Disinserimento, con funzionamento impulsivo o segue stato
- Reset Memorie
- Tacitazione Uscita

## 2. Installazione ed avvio

### 2.1. Installazione del software di configurazione

La centrale CS600 viene fornita con DVD di installazione Software (PKsecurity600) e documentazione tecnica necessaria all'utilizzo degli apparati.

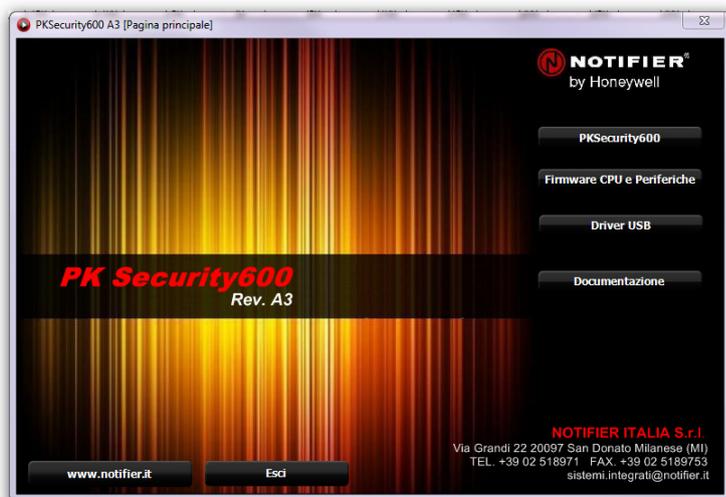
I sistemi Operativi compatibili sono:

- **XP Sp3 (32 bit)**
- **Windows 7 Sp1 Professional/Enterprise/Ultimate (32/64 bit)**

Caratteristiche minime:

- **4Gb di spazio libero su HDD**
- **2Gb di RAM**
- **Processore 2,5 Ghz**

Il DVD parte in "autorun" e viene mostrata la schermata principale.



#### DVD rev A.xx:

- **PKSecurity600:** Installazione SW di configurazione CS600
- **Firmware:** contiene eventuali upgrade di FW delle periferiche e CPU
- **Driver USB:** contiene i driver necessari per la configurazione/connesione con la CS600, da utilizzare in caso di necessità dopo l'installazione.



- **Documentazione:** contiene tutti datasheet, manuali, schemi di collegamento, presentazioni inerenti alla CS600.
- **Risorse WEB:** contiene i link ai video tutorial di installazione degli articoli che compongono il sistema CS600, LCD, Centrale, IND ....



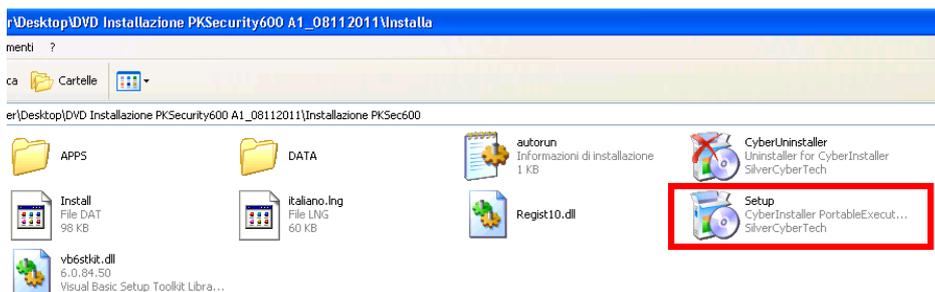
### Installazione:

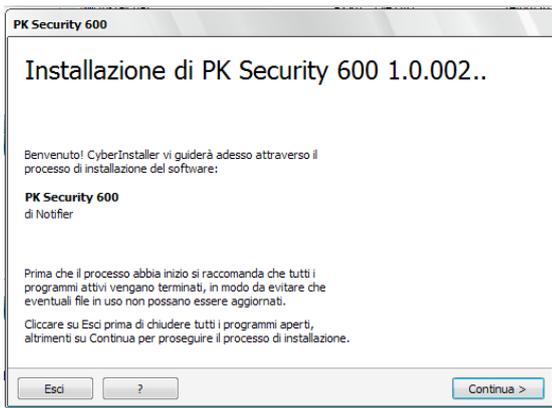
- **Installa PKSecurity600:** Apre un'ulteriore maschera che indica la sequenza di azione per eseguire l'installazione nel modo corretto. La procedura richiede
- **NOTA:** Per S.O. XP **e' necessario** avere installato Windows Installer 4.5 e Power Shell 2.0, se non installati è possibile farlo dal DVD.



- **Installa PKSecurity600:** verrà creata una cartella direttamente sul PC che si sta utilizzando dove verranno inseriti i file necessari per eseguire l'installazione del Software

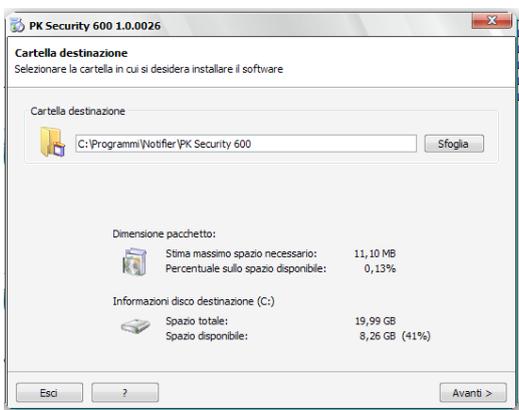
Nella directory creata cliccare su Setup:





### Installazione:

- **Installa PKSecurity600:** Premere Continua.

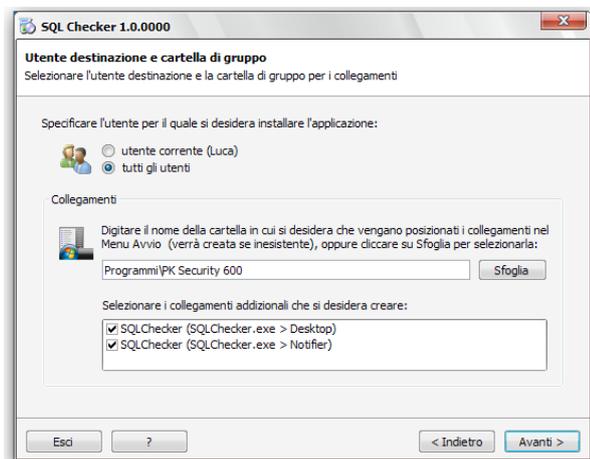


### Installazione:

- **Installa PKSecurity600:** Premere Avanti.

### **NOTA:**

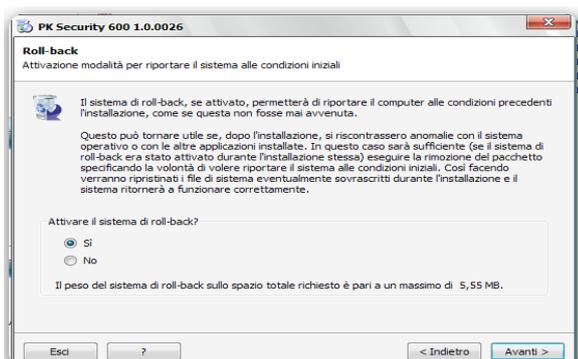
Lasciare la directory d'installazione di default.



### Selezionare :

- A quali utenti Windows rendere disponibile il PKsecurity600.
  - o Consigliato: Tutti gli utenti
- La directory dove installare il Software
  - o Consigliato: Lasciare quella di default
- Quali collegamenti verranno creati in automatico dall'installazione.

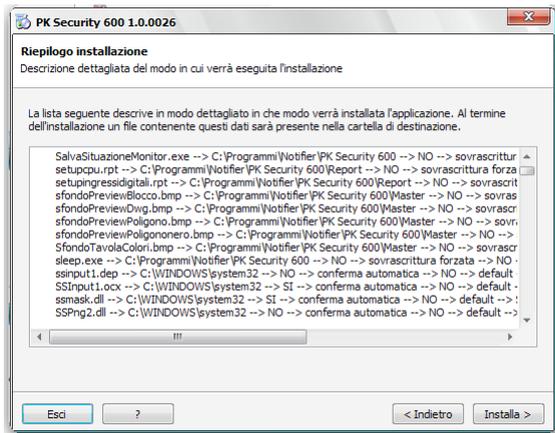
Premere "Avanti"



La schermata presenta l'abilitazione dell'utility Roll-Back

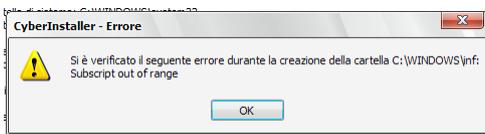
- Consigliato: Sì

Premere "Avanti"

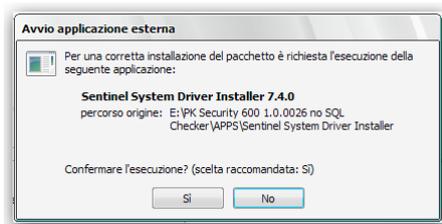


La schermata presenta l'elenco dei file che verranno installati.

Premere “**Installa**”



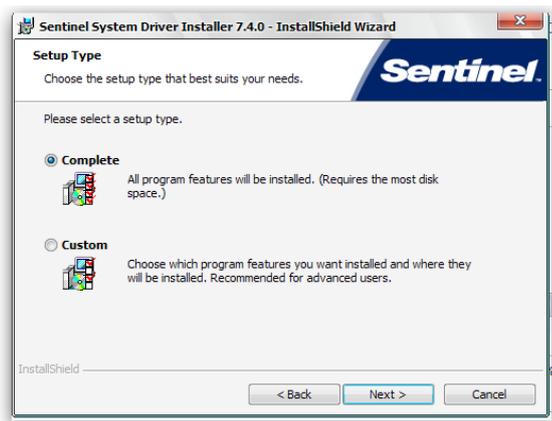
**NOTA:** Per sistemi operativi XP se si genera un errore: **CyberInstaller-Error** (errore nella creazione della cartella C:\Windows\inf) cliccare su **OK**, ignorando la segnalazione. L'installazione procede senza problemi.



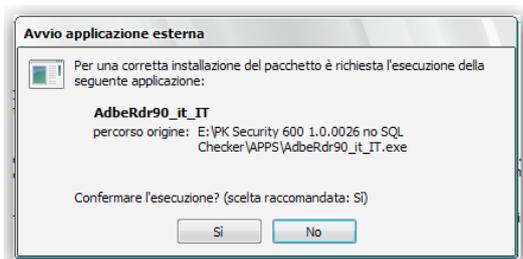
La schermata presenta la richiesta di installazione dei driver Sentinel. Premere “**SI**”



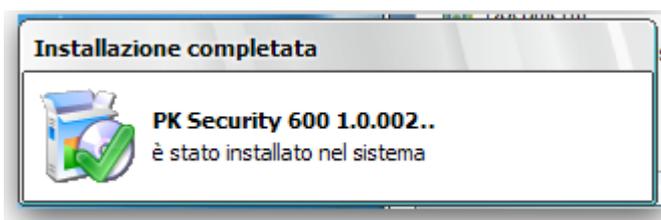
Accettare i termini di Licenza



Premere “SI” e seguire la procedura guidata. In caso di Driver già presenti nella procedura guidata premere “**Modify**” e proseguire fino alla fine.



Se già presente un reader Acrobat premere su **NO** altrimenti procedere con l'installazione premendo **SI**.

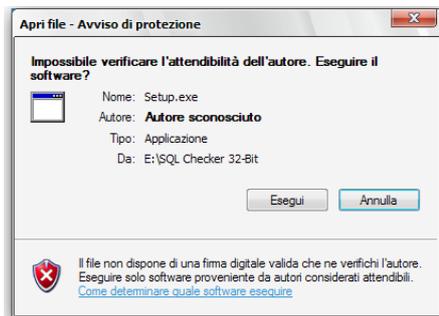


Una volta terminata l'installazione del PKSecurity600 è necessario procedere con quella del DataBase SQL.

Selezionare la versione in base al sistema Operativo in uso (per XP è sempre a 32Bit) e procedere come segue:

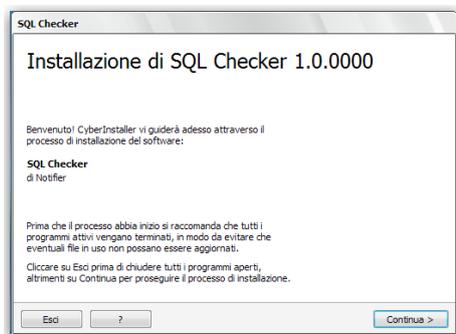


Selezionare la directory dove copiare il file d'installazione dal DVD al PC in uso.  
Cliccare sul file Setup.exe

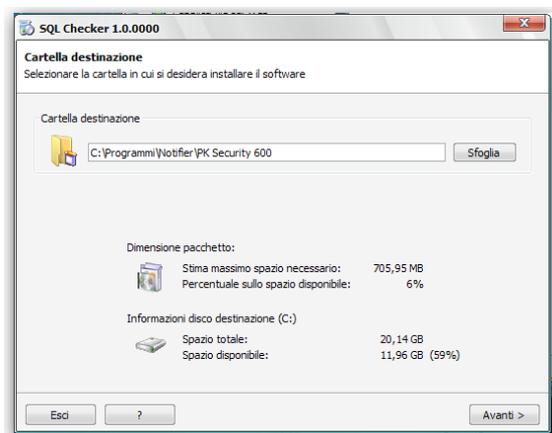


Premere “Esegui” per procedere con l'installazione della nuova istanza SQLNotifier.

Se invece viene trovata una istanza già nominata SQLNotifier verrà mostrato il messaggio “Istanza Già Presente” premere Avanti per installare la base di dati.



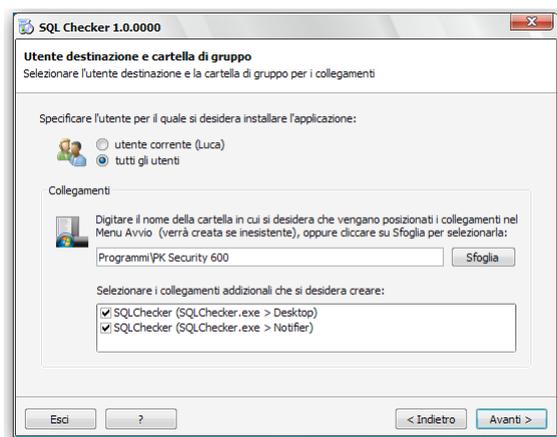
Premere “Continua”



Premere “Continua”

**NOTA:**

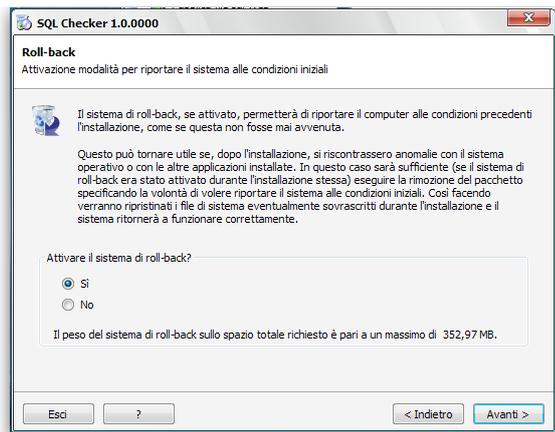
Lasciare la directory d'installazione di default.



**Selezionare :**

- A quali utenti Windows rendere disponibile il PKsecurity600.
  - o *Consigliato: Tutti gli utenti*
- La directory dove installare il Software
  - o *Consigliato: Lasciare quella di default*
- Quali collegamenti verranno creati in automatico dall'installazione.

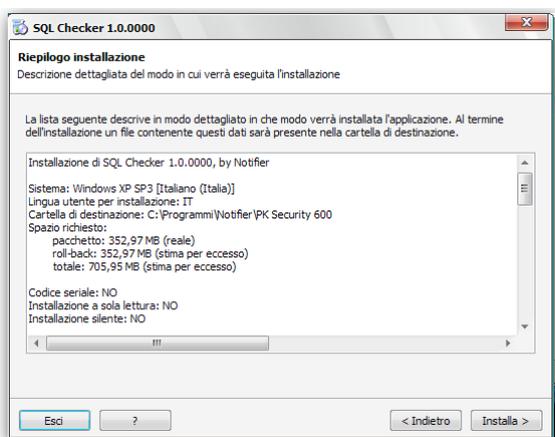
Premere “Avanti”



La schermata presenta l'abilitazione dell'utility Roll-Back

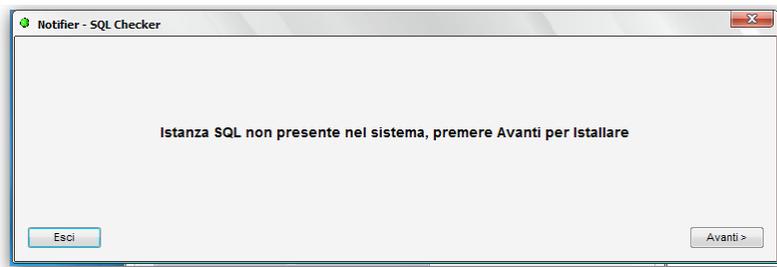
- *Consigliato: Sì*

Premere “Avanti”

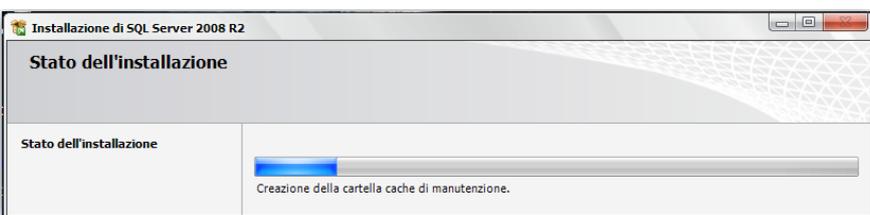
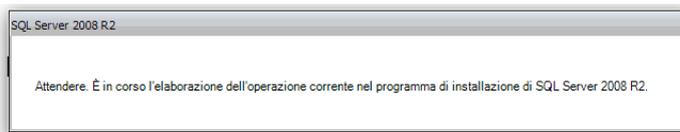
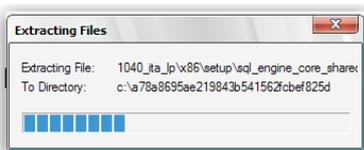


La schermata presenta l'elenco dei file che verranno installati.

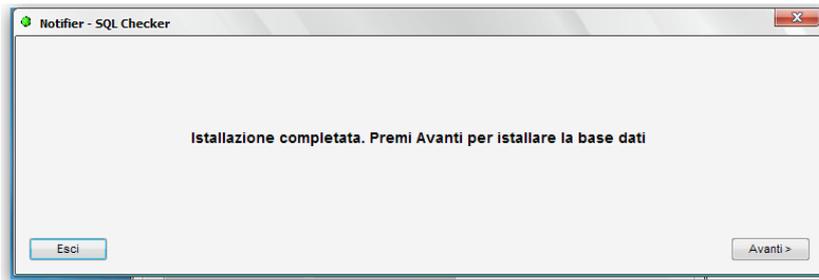
Premere “Installa”



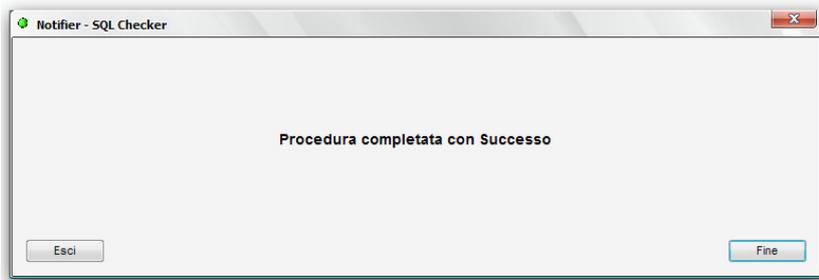
Il Software esegue una ricerca per verificare se ci sono Istanze SQL già presenti. Se non vengono trovate premere “Avanti”



Attendere il termine dell'installazione di SQL Server



Premere “Avanti”

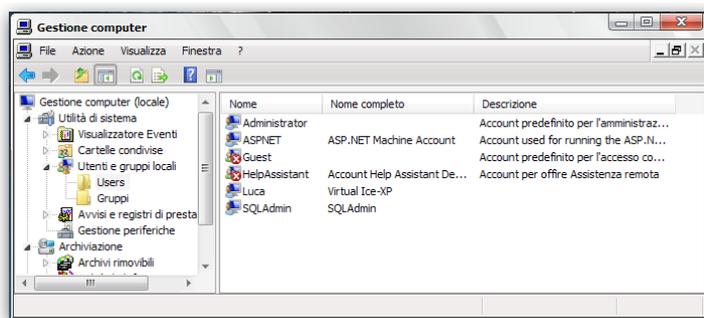


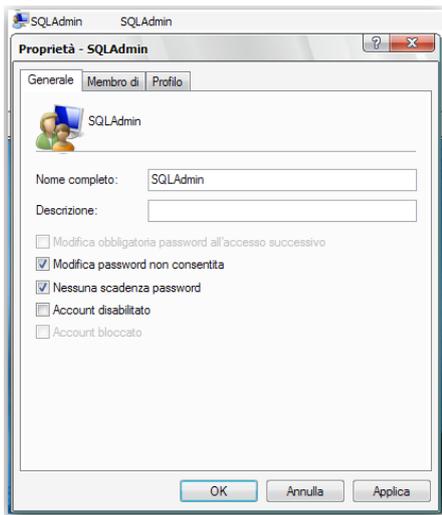
Attendere il termine dell’installazione della “MonitorData” e premere “Fine”.

Al termine dell’installazione è necessario togliere la scadenza della Password per l’operatore creato “SQLAdmin”.



Dall’icona “Risorse del Computer” per S.O. *Win XP* o “Computer” per S.O. *Win 7* tasto DX **Gestione**, selezionare *Utenti e gruppo o Utenti Locali*, l’utente *SQLAdmin*.





Premere **Tasto DX Proprietà** e nella finestra **Generale** mettere il flag:

- *Nessuna scadenza Password*
- *Modifica Password non consentita*

Riavviare la macchina

NOTA: Nel caso di installazioni dove sono già presenti istanze di SQL in versione Compact o Standard è necessario al termine dell'installazione verificare nei "Servizi" di Windows sotto Pannello

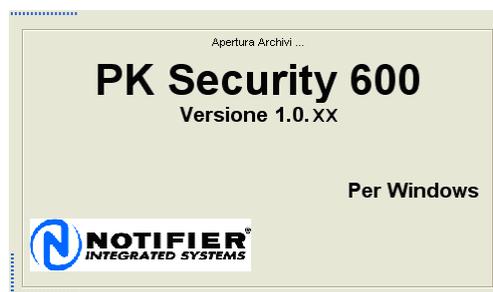


di controllo "Strumenti di Amministrazione" che l'attivazione del Servizio di SQL sia configurato come "Manuale" e non "Automatico" in modo da poter gestire di volta in volta quale Istanza di SQL abilitare per il buon funzionamento dei Software.

## 2.2. Avvio del software di configurazione

A seguito di una corretta installazione del software e conseguente riavvio della macchina PC, sarà possibile procedere eseguendo il collegamento del file **PK600Security 1.0.00xx.exe** posizionato sul desktop.

All'avvio verrà mostrata una finestra di controllo compatibilità database indicante la versione del software.



All'apertura del software PKSecurity600 verrà mostrata la pagina iniziale del Software PK.

## 2.3. Pagina Principale



La pagina principale del software si presenta intuitiva e di facile gestione grazie alle icone dinamiche suddivise in 5 categorie logiche nominate “Aree”:

- **Area Login/Connessione**

A seconda del login effettuato sarà possibile sbloccare i diversi menù del PKSecurity600.

- **Area Invia/Ricevi Dati**

Da quest’area è possibile caricare/scaricare tutte le configurazioni da o verso la centrale CS600, oppure è possibile aggiornare parzialmente le configurazioni tramite la funzione (**Sincronizza CPU**) selezionando solo le voci interessate.

- **Gestione Eventi**

Permette il carico e la visualizzazione dell’archivio eventi di una centrale CS600 o del sistema. La gestione degli eventi è ottimizzata grazie a particolari filtri di tipologie, Impianto, Data, ID oggetto, Tipo Oggetto, Operatore o Descrizione. Inoltre è disponibile un menù a parte capace di filtrare i soli eventi propri richiesti dalla normativa EN50131.

- **Area Impianti / Configurazione PK**

Riguarda la configurazione del software residente nella macchina PC. Permette la gestione e configurazione delle anagrafiche dei diversi impianti (o siti), degli Operatori PC, configurazione delle rubriche di connessione, Setup delle periferiche di comunicazione (schede di rete, porte COM, modem...) e stampe filtrate delle configurazioni del sistema.

- **Area Configurazione Sistema**

Quest’area è dedicata alla configurazione della centrale di sicurezza, da qui è possibile configurare i parametri e le molteplici proprietà della centrale CS600.

Nel DVD del Software PKsecurity600 è presente un DataBase di un “**Impianto Base**” completo, utilizzabile come linea guida per la creazioni di impianti più complessi.

Vedi cap. **3.13.4**

Alla prima connessione con la centrale CS600 come mostrato nei paragrafi successivi viene creata in automatico la rubrica di connessione che viene utilizzata per non dover fornire manualmente le credenziali di accesso per le connessioni successive.

Una volta connessi con la CS600 avendo già inserito i dati nell'anagrafica e identificato il numero di MacroImpianto è possibile iniziare la programmazione della centrale, che può essere eseguita in varie modalità.

Viene di seguito riportata una linea guida per le prima programmazione:

- 1. Configurazione Periferiche Ingressi/uscite:** Programmare le periferiche esistenti tramite la selezione del FLAG “Programmata” presente nelle proprietà di ogni singola periferica IND8/4 – ALI8/8 – AEI/485 – RXE485 – LCD600S.  
Sarà così possibile mettere IN SERVIZIO le periferiche installate sulle linee 485.  
Successivamente sarà possibile modificarne la descrizione, le proprietà degli ingressi/uscite eventualmente utilizzati e i vari parametri di funzionamento impostabili dalla proprietà della singola periferica. (vedi cap 3.21).
- 2. Configurazione MZZ/SZZ:** permette la definizione della suddivisione logica del sistema, creando MacroZone e Zone a cui dovranno essere associati poi gli ingressi/uscite digitali, precedentemente nominati e configurati con tutti i parametri necessari al loro funzionamento. Sempre in questa sezione vanno definite le Zone Uscite che dovranno avere la funzione di sinottico, in modo da dover solo associare successivamente i LED tricolore dei LCD600S e AEI-485, o di segnalazione come Allarmi, Guasti o altro richiesto dall'installazione.  
*E' necessario in questo passaggio associare le Zone Ingressi e/o Uscite alle MacroZone Ingressi e/o Uscite, in base alla logica creata (vedi cap 3.20).*
- 3. Configurazione Centrale:** In questa sezione vengono definiti tutti i parametri di funzionamento della centrale CS600.  
Grado di Sicurezza della norma EN50131 (default configurato al 3 livello), la gestione delle attivazioni generali delle uscite come le uscite relè od O/C della scheda madre e delle periferiche di campo.  
Questa funzionalità permette di avere la gestione delle segnalazioni direttamente gestite dalla centrale e non dalla singole MacroZone/SottoZone di ingresso/uscite, semplificando e limitando la quantità di programmazioni da eseguire nel software PKSecurity600 (vedi cap 3.18)
- 4. Configurazione Periferiche Ingressi/uscite:** Ritornando nel menu selezionare i terminali che dovranno avere il riporto dei sinottici di MacroZona / Zona e andare nel menù di programmazione Tasti/Led presente all'interno delle proprietà dei terminali (LCD600S o AEI-485), e associare le uscite LED alle Zone uscite programmate come gestione sinottici. (vedi cap 3.21.2.5).
- 5. Configurazione Impianti:** in questa sezione viene data la descrizione e l'associazione all'impianto delle MacroZone Ingressi/Uscite precedentemente configurate. (vedi cap 3.19)
- 6. Profili e Utenti:** in questa sezione si configurano gli utenti che utilizzeranno il sistema, definendo i Profili, Gruppi, PIN e i Livelli con le varie associazioni di funzionamento. (vedi cap 3.22).
- 7. Verifica Struttura:** Serve per poter visualizzare la programmazione realizzata.  
Inoltre se si è connessi alla CS600 è possibile visualizzare i vari stati dell'impianto.

## 3. PK Security 600 – menù e configurazioni

### 3.1. Log In

Permette l'accesso di un Operatore PC preconfigurato.

All'avvio del Software PK Security 600 tutte le icone si trovano in stato disabilitato, solo dopo aver eseguito un Login sarà possibile accedere ai diversi menù.



La password di default assegnata all'operatore **101** (Supervisor Tecnico) è: **1111**.

**Nota:** Per ulteriori informazioni sulle password di default vedi **cap. 5 – Password di sistema**.

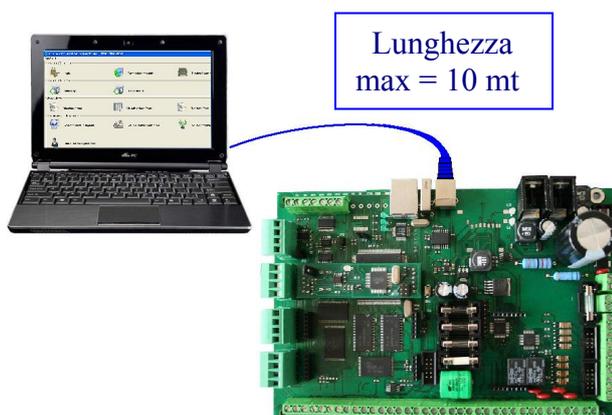
### 3.2. Connessione Manuale

Da questa finestra è permessa la richiesta di connessione tra PC e centrale in molteplici tipologie di comunicazione.



#### 3.2.1. Connessione Diretta

Se opportunamente configurata da menù “Setup periferiche di Comunicazione”, è possibile richiedere una connessione diretta (max 10 mt.) tra PC e CS600, ovvero una connessione via cavo standard USB sulla porta JP16 montata direttamente sulla scheda base della centrale.

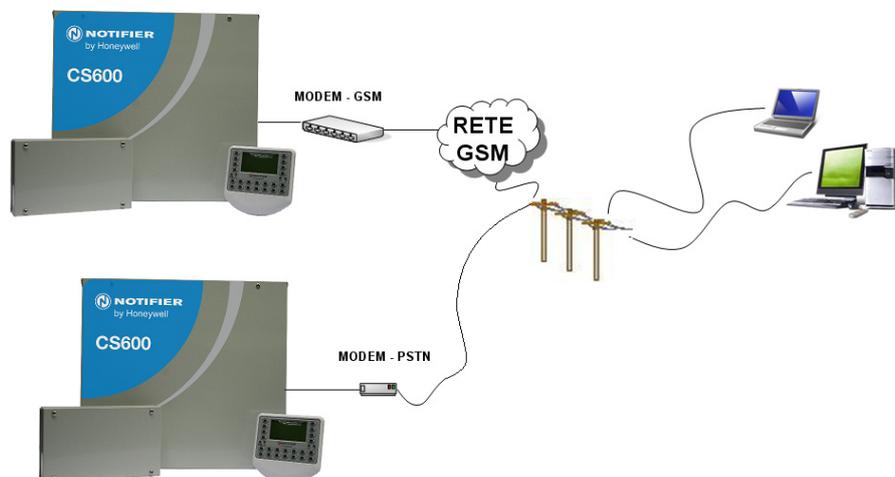


**Nota:** Il cavo standard USB fornito con la centrale, viene individuato dal sistema operativo come una normale porta di comunicazione seriale (COM 2, COM 7...). Non è necessario installare alcun driver di comunicazione perché già presente in centrale ed auto-installante alla prima connessione.

E' importante però accertarsi del corretto indirizzamento della porta dal menu Hardware/Gestione Periferiche di Windows.

### 3.2.2. Connessione Remota via Modem

Esegue una connessione via modem. E' necessario che sugli slot JP11 e 12 sia installato il combinatore telefonico e modulo digitale M-CONTACT-ID oppure sulla porta JP20 sia un modem (es: MDM-GSM Notifier), configurato e connesso alla linea telefonica.



### 3.2.3. Connessione Remota via TCP-IP

Permette la connessione via Ethernet tramite protocollo TCP-IP inserendo l'indirizzo della scheda di rete integrata nella scheda base della CS600 (JP18).



#### 3.2.3.1. Settaggio dell'indirizzo IP di centrale

La CS600 dispone di una scheda di rete 10/100 MB integrata direttamente nella scheda base, è possibile settarne IP Address, Gateway e Netmask direttamente da software PKSecurity600. Utilizzare il cavetto USB standard tipo A-B in dotazione alla centrale per effettuare la connessione .

#### Procedura di settaggio:

- 1 Connettere il cavo USB alla porta JP16 della CPU.
- 2 Non è necessario installare alcun driver in quanto già presenti nell'installazione del PKSecurity600, in caso contrario è possibile reperire il driver di comunicazione dal DVD di installazione del software.
- 3 Controllare dal menù Hardware/Gestione Periferiche di Windows quale porta di comunicazione è stata assegnata (es: COM5).

- 4 Eseguire il software di configurazione PKSecurity600 e loggarsi con user Supervisor Tecnico.
- 5 Accedere al menù **Setup Periferiche di Comunicazione**, selezionare la porta di comunicazione interessata e, come mostrato in figura sotto, mettere il flag sulla voce **Abilita** e selezionare **Interfaccia Ethernet**:



- 6 Selezionare **OK**.
- 7 Accedere al menù **Connessione Manuale/Remota Via TCP-IP/Scheda di rete RS**.
- 8 Compilare le voci riguardanti le **Proprietà Scheda Locale** (IP address, Mask e Gateway).
- 9 **Indirizzo di Fabbrica:**
  - a. IP: 192.168.2.150
  - b. Subnet Mask: 255.255.255.0
  - c. Gateway: 192.168.2.200

### 3.2.3.2. Connessione manuale su rete ETH

Accertarsi della corretta abilitazione del canale ETH dal menu **Setup Periferiche di Comunicazione**. Durante la richiesta di connessione vengono proposte 2 tipologie di connessione.

- 1 **Scheda di Rete / RS** (inserimento manuale dell'indirizzo IP della scheda di rete, vedi figura sotto).
- 2 **Accesso Remoto** (apre una connessione remota preconfigurata da Windows).

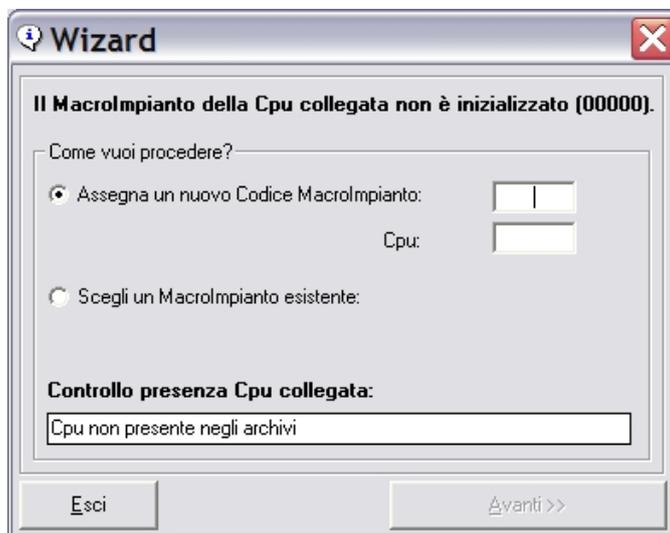
**N.B.:** inserimento dell'IP-Address della scheda di rete CS600.

Il flag "manuale" o "Nat" determina la modalità di connessione e la tipologia di rete LAN o WAN.

### 3.3. Set-up Numero Macro-Impianto

**IMPORTANTE:** Prima di stabilire la connessione con la centrale effettuare l'import del DataBase (impianto base 0001) presente nell'installazione del PKSecurity600 (vedi 3.14.4).

Alla prima connessione verso la CS600 se non è stata precedentemente configurata verrà mostrata una finestra sotto che richiede di dare un numero identificativo alla centrale alla quale si è connessi.



All'apertura della finestra le scelte possibili sono 2:

**Soluzione 1.** (da utilizzare quando si vuole eseguire una programmazione di una CS600 nuova e all'interno dell'installazione del PK troviamo solo l'impianto di default Notifier **00001**).

- Assegnare un nuovo codice MacroImpianto (5cifre – Es. 95100) e un numero di Cpu (2 cifre – Es. 00 ) e premere “Avanti”.
- Se la procedura di inizializzazione è andata a buon fine verrà mostrata la finestra con la descrizione di Procedura Terminata.



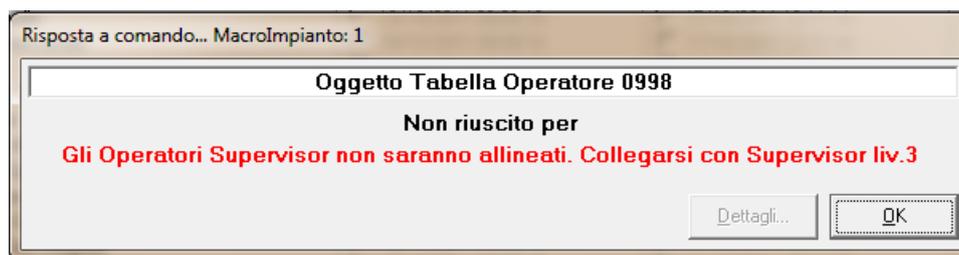


E' indispensabile accedere con utente **Installatore** per caricare le configurazioni esistenti in centrale.

Per codici utenti PK/CPU vedi cap.5.

- A questo punto sarà possibile effettuare una nuova connessione con la CS600 e caricare dalla Centrale il programma di default presente.

Attenzione: l'utente Supervisor, a differenza dell'Installatore (999), consente il solo carico e invio dei dati della tabella Operatori (nello specifico PIN, codici Trasponder, codici Radiocomando e Password di connessione). Se viene richiesto l'allineamento tabella operatori con utente Installatore, viene mostrata la seguente finestra d'avviso:



**NB:** Il software PKSecurity600 viene fornito con una programmazione di base, definita in questo manuale nel capitolo 4 "Impianto Base – 00001 V2".

Quando la connessione è andata a buon fine verrà mostrato un messaggio di impianto inesistente, a questo punto il PKSecurity600 caricherà la programmazione presente nella centrale CS600 oppure permetterà l'invio del Programma Base 00001 presente nel software.

**Soluzione 2.** (da utilizzare quando si vuole eseguire una programmazione di una CS600 nuova e all'interno dell'installazione del PK troviamo non solo l'impianto di default Notifier 00001, ma anche programmi precedentemente creati).

- Alla prima connessione con la CS600 verrà mostrata la figura di inizializzazione CPU.
- Selezionare Scegli un Macro Impianto Esistente figura sotto.
- Aprire il menù a tendina e identificare il numero che si vuole assegnare a questa CS600.



I MacroImpianti nel menù a tendina saranno disponibili solo dopo aver creato in precedenza un DataBase, o averne importato uno da un altro impianto.

Se la procedura di inizializzazione è andata a buon fine verrà mostrata la finestra con la descrizione di Procedura Terminata.

Dal menù di connessione sarà possibile effettuare una nuova connessione con la CS600 e nel momento che la connessione è andata a buon fine verrà mostrato un messaggio “*Vuoi procedere all’allineamento delle Tabelle?*”.

Selezionare il Tasto NO e dalla finestra principale del PK premere INVIA a Cpu.

In questo modo si scaricheranno all’interno della CS600 tutte le configurazioni presenti nel PKSecurity600.

**Soluzione 3.** (da utilizzare quando si vuole eseguire una programmazione di una CS600 che al suo interno ha già configurato un impianto).

**NOTA:** questa procedura comporta la cancellazione di tutti i dati residenti nella CS600 (operatori, PIN, Badge, Sinottici, segnalazioni esterne ecc)

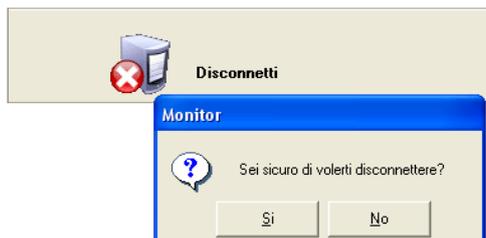
- Alla prima connessione con la CS600 sarà necessario accedere con utente **Installatore** per poter modificare le configurazioni della centrale esistente  
NB: l’utente installatore dovrà essere abilitato dall’utente **Supervisor**
- Una volta connessi accedere al menu **Configurazione Centrale** e dalla pagina **Comandi Cambia MacroImpianto e Cpu**.
- Alla successiva connessione la centrale avrà il nuovo codice MacroImpianto inserito. Sarà possibile eseguire il **Sincronizza CPU** scaricando la nuova configurazione presente nel PKSecurity600 oppure prelevare dalla CS600 il nuovo MacroImpianto.

### 3.4. Rubrica Connessioni

Apri l’elenco delle connessioni preconfigurate. Se presente una sola connessione creata, il software procede direttamente alla connessione della centrale.

### 3.5. Disconnetti

Interrompe la connessione attiva.



### 3.6. Invia a CPU

Se connessi, permette di inviare tutto il DataBase del PK alla CPU.

### 3.7. Ricevi da CPU

Se connessi, permette di caricare tutto il DataBase della CPU con tutte le programmazioni esistenti.

### 3.8. Sincronizza CPU



Se connessi, permette di selezionare quali modifiche allineare.

Il comando Sincronizza visualizza una finestra di allineamento riportante tutte le tabelle che compongono i database di sistema della CS600. Sarà quindi possibile confermare le informazioni presenti in centrale fleggando le voci di tabella sotto la colonna “Centrale” (es colonna 1) oppure selezionare quali tabelle modificare con quelle fatte dal software PKSecurity600 abilitando il flag sotto la colonna “PC” (es colonna 2).

### 3.9. Ricezione Eventi

Viene mostrata una finestra a tutto schermo indicante l’archivio eventi completo della centrale connessa.

MI - Cpu	Confirma	Data	Impianto	Oper	Descrizione Operatore	Tipo Evento	Oggetto	IDOgg.	Descrizione
55555 - 00	##	25/07/2011 15:17.49	mpianto Notifier	0999	Installatore	Reset Eventi Important	Operatore Cpu		KD - Elenco generale 121 - Terminale Furto 121
55555 - 00	##	25/07/2011 15:18.06	mpianto Notifier	0999	Installatore	Disabilitato	Operatore Cpu	0999	Installatore 121 - Terminale Furto 121
55555 - 00	##	25/07/2011 15:18.06	mpianto Notifier	0999	Installatore	Reset Eventi Important	Operatore Cpu		KD - Elenco generale 121 - Terminale Furto 121
55555 - 00	##	25/07/2011 15:18.16	mpianto Notifier	0000	Operatore Centrale	Taglio	Ingresso Digitale	0012101	Tamper Termin. Furto 127 - Zona Tamper Sistema
55555 - 00	##	25/07/2011 15:18.35	mpianto Notifier	0000	Operatore Centrale	Riposo	Ingresso Digitale	0012101	Tamper Termin. Furto 127 - Zona Tamper Sistema
55555 - 00	##	25/07/2011 15:18.37	mpianto Notifier	0000	Operatore Centrale	Forzatura Porta	Operatore Cpu	121	Terminale Furto 121 - Password Errata
55555 - 00	##	25/07/2011 15:22.06	nerali ed Allarmi	0999	Installatore	Abilitato da Monitor	Operatore Cpu	0999	Installatore - Monitor - 10.0.0.202
55555 - 00	##	25/07/2011 15:31.25	nerali ed Allarmi	0999	Installatore	Disabilitato da Monitor	Operatore Cpu	0999	Installatore - Monitor - 10.0.0.202
55555 - 00	##	26/07/2011 00:00.00	nerali ed Allarmi	0000	Operatore Centrale	Fsv per scadenza tessei	Operatore Cpu	0999	Installatore

Il tasto aggiorna richiede ulteriori eventi e li incolonna in sequenza cronologica.

**Nota:** Gli eventi non vengono visualizzati on-line, lo scarico dei nuovi record avviene solo su richiesta tramite il comando “Aggiorna” o chiusura e riapertura della finestra.

In fase di caricamento eventi, il PKSecurity600 visualizzerà, in basso a sinistra, il messaggio “Trasferimento eventi in corso”.

### 3.10. Visualizzazione eventi

Mostra gli eventi precedentemente caricati dopo aver eseguito la procedura al cap 3.9. Da questo menù sarà possibile consultare gli eventi in stato Off-line, filtrarli, stamparli o archivarli in multiformato digitale.

Procedere alla stampa tramite il tasto



**Nota:** Una volta visualizzati i fogli d’anteprima di stampa avremo la possibilità di stampare gli eventi direttamente su stampante predefinita da Windows oppure esportarli in multiformato digitale



### 3.11. Ricezione Eventi EN50131

Carica e mostra i soli eventi classificati secondo normativa EN50131 con possibilità di filtro secondo categorie.

**N.B.:** Gli eventi non vengono visualizzati on-line, lo scarico dei nuovi record avviene solo su richiesta tramite il comando “Aggiorna” o chiusura e riapertura della finestra.

In fase di caricamento eventi, il PKSecurity600 visualizzerà, in basso a sinistra, il messaggio “Trasferimento eventi in corso”.

### 3.12. Visualizzazione eventi EN50131

Mostra gli eventi EN50131 precedentemente caricati. Da questo menù è possibile consultare gli eventi in stato Off-line, filtrarli, stamparli o archivarli in multiformato digitale.

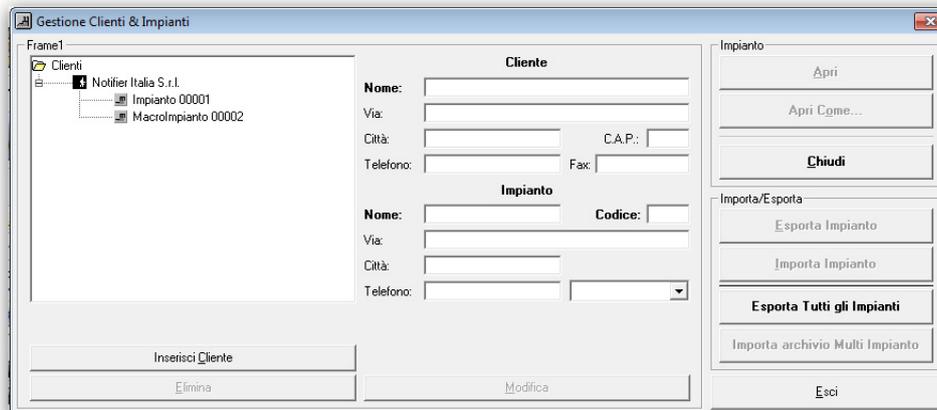
Procedere alla stampa tramite il tasto



**N.B.:** Una volta visualizzati i fogli d’anteprima di stampa avremo la possibilità di stampare gli eventi direttamente su stampante predefinita da Windows oppure esportarli in multiformato digitale



## 3.13. Gestione Clienti e Impianti



La finestra di **Gestione Clienti e Impianti** visualizza l'elenco completo dei Macroimpianti (o siti) gestiti dal PKSecurity600. Ogni volta che ci collegheremo ad una nuova CS600, essa andrà associata ad un cliente (possibilmente completo nelle sue parti anagrafiche) e ad un impianto.

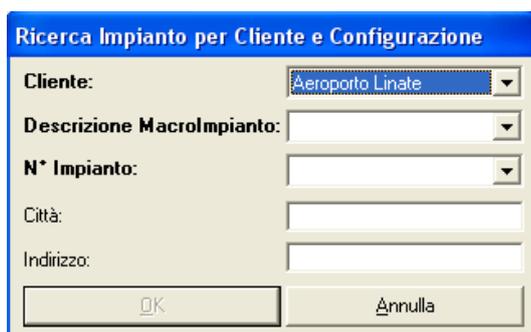
### 3.13.1. Inserisci Cliente

Dalla finestra “Inserisci Cliente” verranno compilati tutti i dati anagrafici dei clienti gestiti dal PK Security 600.

### 3.13.2. Apri Impianto Esistente

Il tasto “Apri Impianto Esistente” permette l’apertura off-line di un impianto precedentemente realizzato.

### 3.13.3. Apri Come...



La funzione “**Apri Come...**” serve a creare cloni di un impianto realizzato.

Un buon metodo di partenza, nella creazione di un nuovo impianto è appunto caricare l’impianto Base 00001 (o un’altro esistente) e personalizzarlo nelle descrizioni, associazioni, operatori, terminali etc. mantenendo valide le configurazioni di base quali Struttura Logica, Impianti e logiche di attivazione programmate.

Per esempio, è possibile creare molteplici impianti attribuiti a diversi clienti, mantenendo le stesse logiche di funzionamento.

### Esporta Impianto

Permette l’esportazione, quindi il salvataggio completo di un impianto selezionato.

#### Procedura di esportazione di un impianto:

- 1 Accedere al menù **Gestione Clienti e Impianti**.
- 2 Selezionare il cliente e l’impianto interessato all’esportazione.
- 3 Premere il pulsante **Esporta Impianto**.
- 4 Viene mostrata la finestra nominata **Cartella di Esportazione**, selezionare quindi una directory a piacere, nominando il file che di default viene chiama “Export.zip”, premere Ok.
- 5 Viene mostrata un finestra di avviso indicante **Esportazione avvenuta con successo**.

### 3.13.4. Importa Impianto

Permette l’importazione di un impianto precedentemente esportato.

#### Procedura di importazione di un impianto:

- 1 Accedere al menù **Gestione Clienti e Impianti**.
- 2 Selezionare il cliente interessato all’importazione.
- 3 Premere il pulsante **Importa Impianto**.
- 4 Viene mostrata la finestra nominata **Cartella di Importazione**, selezionare quindi la directory residente del file.zip da importare (di default nominato Export.zip):

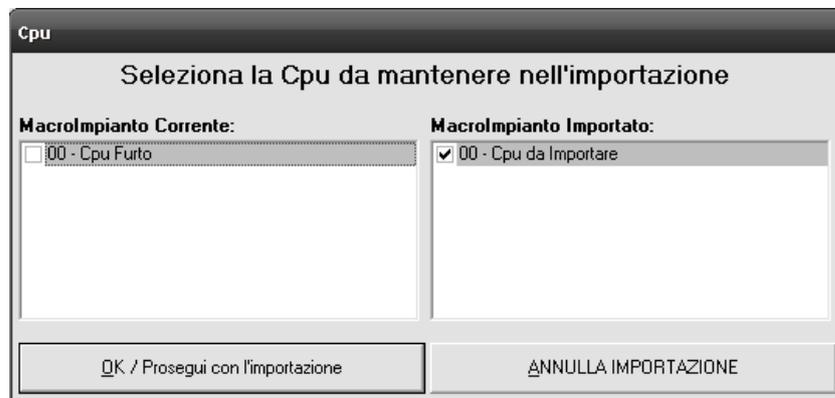


- 5 Attendere la decompressione del file selezionato.
- 6 Successivamente verrà visualizzata la schermata dove nel caso sia già presente un impianto con lo stesso ID Impianto assegnato, chiederà se mantenere il programma esistente nel PKSecurity600 oppure eseguire un’importazione del file selezionato, come in figura successiva.

7 Selezionare:

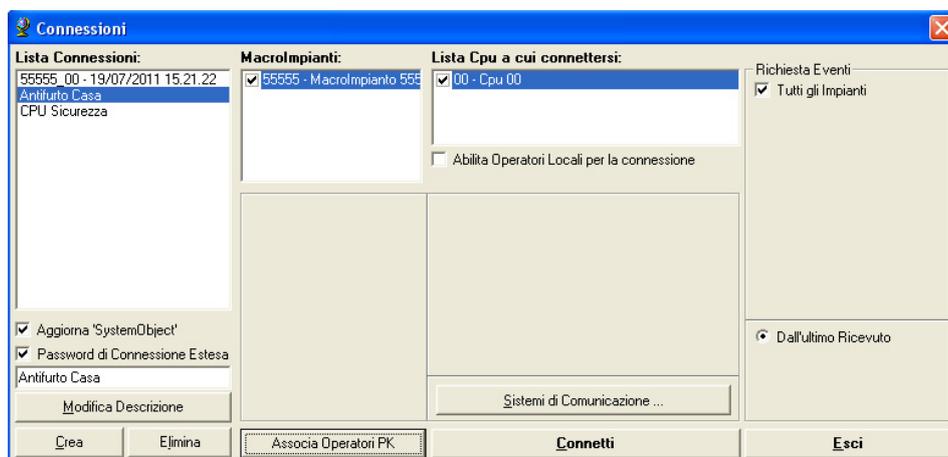
**OK / Proseguì con l'importazione:** e attendere il messaggio di **Importazione avvenuta con successo.**

**ANNULLA IMPORTAZIONE:** la procedura d'importazione viene terminata e ripristinato l'operatore di connessione di default.



### 3.14. Setup Rubrica Connessioni

Il menù Setup Rubrica Connessioni è l'elenco delle configurazioni di connessione alle diverse centrali CS600 caricate.



E' possibile personalizzare la ricezione degli eventi filtrando i singoli impianti che compongono il sistema dal menù **Richiesta Eventi.**

#### Settare una Rubrica di Connessione.

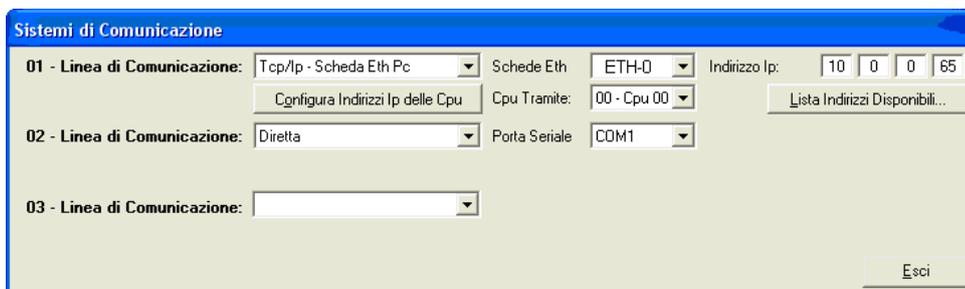
**N.B.:** Durante la fase della prima connessione manuale il PK Security 600 crea in automatico una rubrica di connessione identificata con n° MacroImpianto\_NR CPU\_ Data/ora.

Quindi sarà necessario solo modificare la descrizione.

#### Procedura di creazione di una nuova connessione:

- 1 Con il tasto **Crea** s'inserta la nuova connessione.
- 2 Selezionare la nuova connessione e modificare la descrizione tramite il tasto **Modifica.**
- 3 Dalla colonna **Macroimpianti** selezionare quale macroimpianto si desidera connettere.
- 4 Selezionare da **Lista CPU** quale centrale dello stesso Macroimpianto si desidera connettere di norma è sempre la 00.

- 5 Selezionare dall'apposito menù **Richiesta Eventi** da quali impianti si potranno visualizzare una volta connessi gli eventi generati.
- 6 Dal tasto **Associa Operatori PK** viene creata, attraverso la Password di connessione, un'associazione che autorizza l'operatore PK in login ad assumere le proprietà di un operatore CPU - Installatore (999), ottenendo così le opportune autorizzazioni che gli permetteranno di agire sulle configurazioni di centrale.
- 7 Premendo il tasto Sistemi di Comunicazione appare la finestra mostrata in figura sotto. Da qui verrà settata una o più tipologie di connessione.



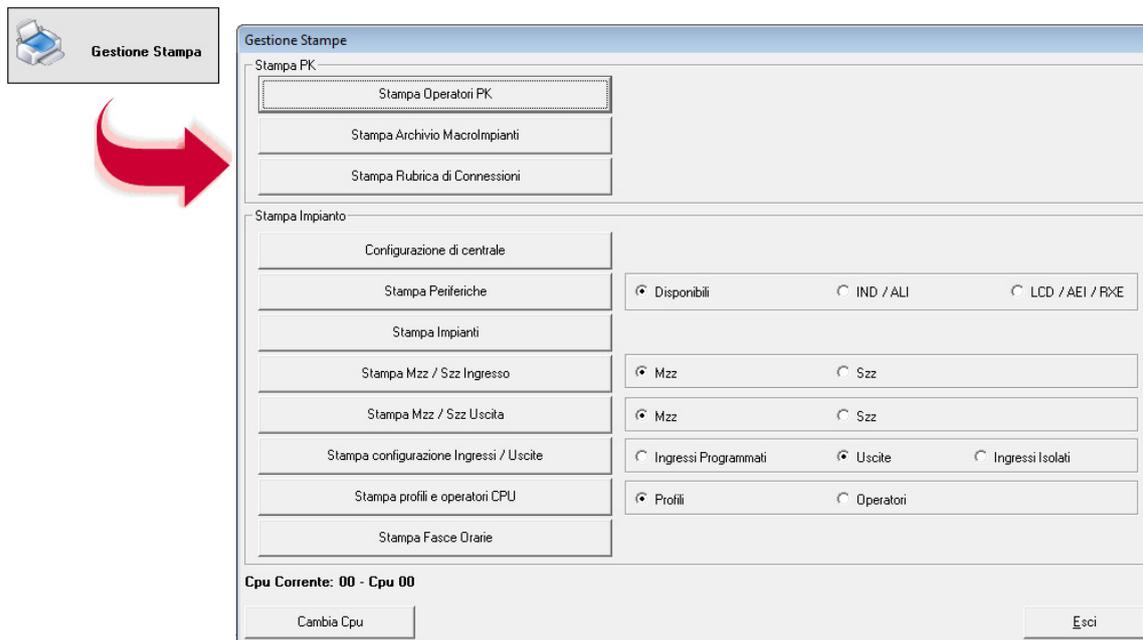
### 3.15. Setup Periferiche di Connessione

La finestra **Setup periferiche di Connessione** permette la configurazione delle diverse porte di comunicazione della macchina PC dove risiede il PKSecurity600.

Sotto, due esempi che mostrano una configurazione *tipo* di una connessione diretta (1) e una connessione tramite scheda di rete IP wireless (2).



## 3.16. Gestione Stampa



Il PKSecurity600 è in grado di stampare le configurazioni dell'impianto aperto in formato.txt, le stampe vengono generate e filtrate per tipologia selezionata.

La directory di default dove vengono salvate le stampe:

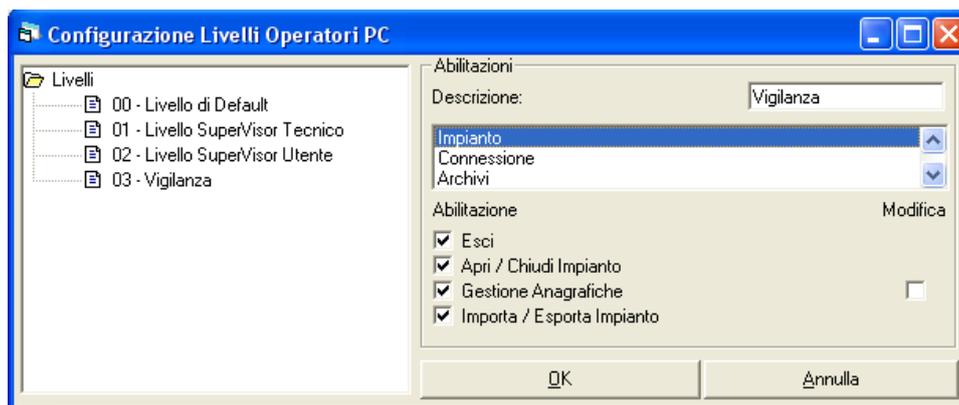
***C:\Programmi\notifier\pksecurity600\Stampe.***

## 3.17. Configurazione Operatori PC

Permette la personalizzazione degli operatori abilitati all'accesso del PKSecurity600, completi di nome, cognome e password d'accesso.

Per semplificare la procedura di configurazione dei singoli operatori esiste la possibilità di creare dei **Livelli** tramite l'apposito menù **Configurazione Livelli**.

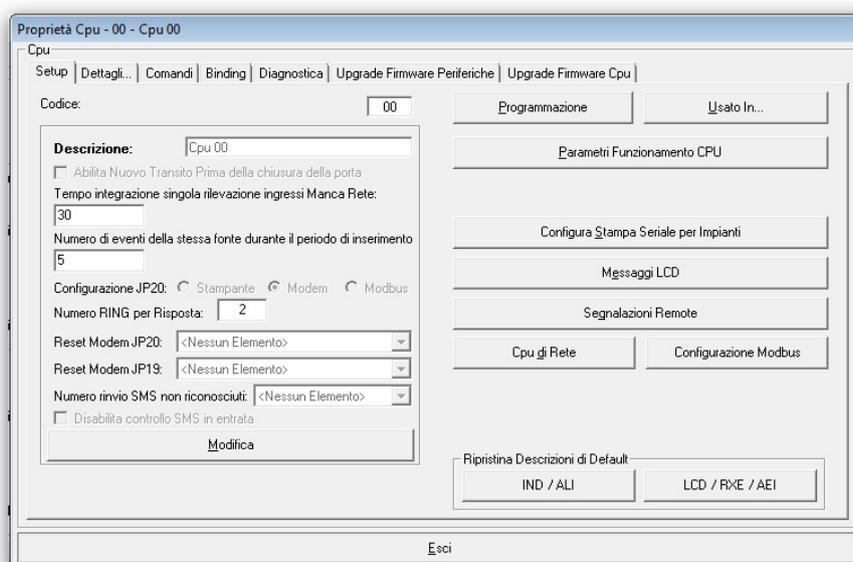




Il **Livello** definisce le funzionalità dell'operatore sul PKSecurity600.

## 3.18. Configurazione Centrale

Una volta aperto l'impianto è possibile procedere alla configurazione della CS600, cominciando dalle proprietà della CPU.



### 3.18.1. Setup

La pagina di **Setup** permette la configurazione di funzionamento logico della CPU selezionata quali:

- 1 **Codice:** Indirizzo identificativo della centrale CS600, in caso d'impianto MultiCPU verranno identificate le centrali con un indirizzo sequenziale 00, 01, 02...
- 2 **Descrizione:** Label d'intestazione della centrale.
- 3 **Abilita nuovo transito prima della chiusura della porta:** Permette il transito di più operatori attraverso un varco prima di eseguire il controllo di chiusura porta.
- 4 **Tempo di integrazione Mancanza Rete;** espresso in secondi indica il ritardo sulla segnalazione di Mancanza rete, necessaria ad evitare false segnalazioni in caso di rete 230 Vac instabile. Nel tempo inserito è possibile configurare delle segnalazioni aggiuntive con la funzionalità di ingresso **Pre Manca rete** nei parametri di funzionamento delle CPU.
- 5 **Numero di eventi della stessa fonte:** indica il n° max di eventi che possono essere generati in modo ripetuto da un qualsiasi elemento del sistema ad impianto inserito.

- 6 **Configurazione JP16:** permette il settaggio di una stampante seriale (Modulo continuo tipo EPSON ST04A) o di un Modem (MDM-GSM) collegato alla porta di comunicazione JP16 della CPU.
- 7 **Numero RING per risposta:** E' il numero massimo di squilli che il combinatore M-CONT-ID accetta prima di impegnare la linea durante l'interrogazione di un numero telefonico esterno.
- 8 **Reset Modem JP16:** permette l'associazione di un ingresso digitale incaricato di eseguire la funzione di Reset Modem sulla porta di comunicazione JP16.
- 9 **Reset Modem JP19:** permette l'associazione di un ingresso digitale incaricato di eseguire la funzione di Reset Modem sulla porta di comunicazione JP19.
- 10 **Numero rinvio SMS non riconosciuti:** E' possibile associare ad un indirizzo di rubrica delle chiamate remote dove inoltrare tutti gli sms inviati al numero di SIM card (presente nel M-CONTACT-ID) da parte di utenti non presenti nella rubrica. In questo modo gli SMS di avviso del gestore telefonico (per esempio "il credito sta per esaurire") o di pubblicità potranno essere inoltrati all'indirizzo di rubrica selezionato.
- 11 **Disabilita Controllo SMS in entrata:** Disabilita il rinvio configurato nel punto precedente.
- 12 **Programmazione;** questa finestra determina il funzionamento/programmazione della CS600, da qui infatti possono essere configurate le principali attivazioni di sistema (es: attivazione delle uscite d'allarme, attivazioni logiche differenziate in base agli innumerevoli stati della CPU) Cap 3.18.2
- 13 **Usato in:** Non utilizzato.
- 14 **Parametri Funzionamento CPU;** permette di stabilire il grado di conformità della normativa EN50131, di default fissato a 3.

La centrale darà la possibilità di programmare logiche funzionamento differenti se viene modificato tale parametro, ad esempio abbassando il grado di funzionamento a 2 sarà possibile utilizzare ingressi digitali come comando di inserimento/disinserimento di zone logiche del sistema altrimenti impedito dalla conformità a grado 3.

**Parametri Funzionamento CPU**

GRADO EN 50131  
 Grado 3    Grado 2    Grado 1    Fuori Norma

LIMITA SOLO A SUPERVISOR DI LIVELLO 2 E 3

**Fuori Servizio**

<input type="checkbox"/> Ingresso Antintrusione in Allarme	<input type="checkbox"/> Guasto Batteria
<input type="checkbox"/> Ingresso Antirapina in Allarme	<input type="checkbox"/> Altri Guasti (tranne ATS e Sir.)
<input type="checkbox"/> Ingresso Antintrusione in Mask	<input type="checkbox"/> Manomissione
<input type="checkbox"/> Ingresso Antintrusione Guasto	<input type="checkbox"/> Guasto ATS
<input type="checkbox"/> Guasto Manca Rete	<input type="checkbox"/> Guasto Sirena

**Reset**

<input type="checkbox"/> Intrusione	<input type="checkbox"/> Guasto ATS
<input type="checkbox"/> Rapina	<input type="checkbox"/> Manomissione
<input type="checkbox"/> Guasto Manca Rete	<input type="checkbox"/> Altri Guasti (tranne Manca Rete e ATS)

**Isolamento**

Isola

**PIN**

Centrale con Pin a 4 Cifre

**FUNZIONAMENTO SIRENE**

	Manomissione		Guasto		Rapina	
	Inserito	Disinserito	Inserito	Disinserito	Inserito	Disinserito
Interna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Esterna	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Annula Ritardo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Panico		Incendio	
	Inserito	Disinserito	Inserito	Disinserito
Interna	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Esterna	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Annula Ritardo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**PARAMETRI FUORI NORMA**

<input type="checkbox"/> Abilita Utente Supervisor alla modifica degli utenti	<input type="checkbox"/> Abilita comando Inserimento Forzato
<input type="checkbox"/> Abilita Utente Supervisor al comando test	<input type="checkbox"/> Disabilita controlli 50131

Modifica   Esci

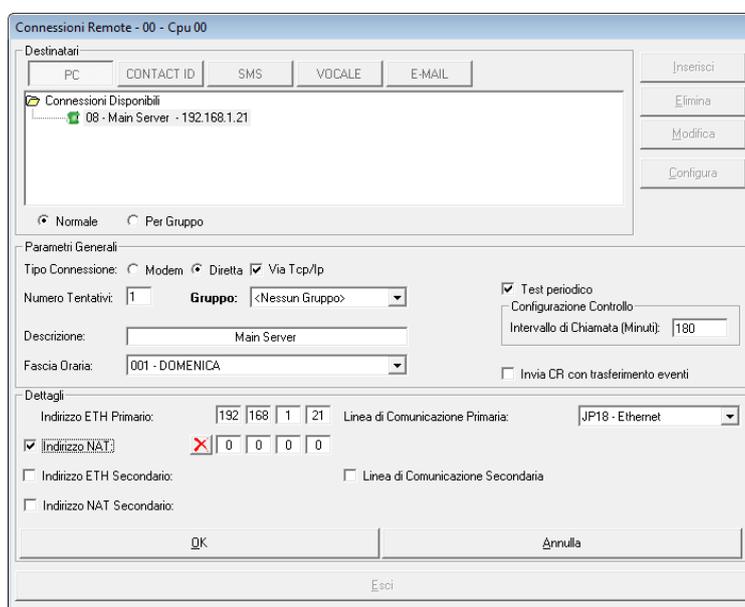
**Nota:** E' possibile, a prescindere dal grado di funzionamento della CPU, modificare il *FUNZIONAMENTO SIRENE* ovvero settare la possibilità di attivare le uscite 50131 ed eventualmente annullare i ritardi di attivazione a seconda degli eventi di **Manomissione**, **Guasto**, allarmi **Rapina**, allarmi **Panico** e allarmi **Incendio** sia da *Inseriti* che *Disinseriti*. Il settaggio proposto in figura sopra è lo stesso predisposto per l'**Impianto Base 00001**.

- 15 **Configura Stampa seriale per Impianti;** la centrale CS600 è dotata di uscita seriale RS-232 su **JP20**, da questo menù è pertanto possibile selezionare quali degli 8 impianti disponibili in ogni programma saranno sottoposti a stampa seriale in caso di eventi.
- 16 **Messaggi LCD;** permette di rinominare i 20 Messaggi disponibili ad un'eventuale visualizzazione sul display dei terminali **LCD600S**.
- 17 **Segnalazioni Remote:** Da questo menù è possibile accedere ad ulteriori menù di configurazione che riguardano le chiamate remote attivate degli eventi della CPU.



a. **Rubrica;** Permette creazione la configurazione e la gestione (messa in servizio e fuori servizi) degli indirizzi di rubrica configurati.

a.1. **PC:** Definisce a quale indirizzo IP inviare una segnalazione remota (come evento), di norma verso un Software di supervisione Monitor Server (vs 2.07 e succ) .



- **Inserisci:** abilita la creazione del nuovo numero di Rubrica
- **Elimina:** Permette la cancellazione della voce selezionata
- **Modifica:** Permette la modifica delle configurazioni della voce selezionata
- **Configura:** Permette di selezionare per quali oggetti (MacroZone, Zone, Ingressi Digitali/Analogici ecc ecc è necessario inviare segnalazione remota al SW Monitor Server).
- **Normale – Gruppo:** Definisce la modalità di visualizzazione e raggruppamento dei numeri inseriti nella rubrica.

- **Tipo di connessione:** Identifica la modalità con cui verranno inviate le segnalazioni.
  - **Numero tentativi:** Definisce il numero di volte che la centrale CS600 tenta di inviare la chiamata remota al Software di Supervisione ogni volta che si verifica un evento configurato per eseguire tale procedura.
  - **Gruppo:** Da 1 a 16. Permette l'assegnazione ad un gruppo del numero selezionato
  - **Test Periodico:** intervallo espresso in minuti che la centrale CS600 invia una chiamata di "Live/Test in Vita" al Software di Supervisione.
  - **Descrizione:** Identificativo del numero di rubrica.
  - **Fascia Oraria:** Se presente stabilisce l'arco temporale in cui il numero selezionato riceverà le chiamate da parte della centrale CS600.
  - **Indirizzo ETH Primario:** Inserire l'indirizzo IP del PC dove installato il Software di supervisione Monitor
  - **Linea di Comunicazione Primaria:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata)
  - **Indirizzo NAT:** Inserire l'indirizzo IP della rete Privata quando la chiamata è indirizzata verso un PC che risiede in una sottorete.
- NOTA: se si utilizza "Indirizzo NAT" quello ETH Primario dovrà essere l'IP pubblico del router principale.
- **Indirizzo ETH Secondario:** Inserire l'indirizzo IP secondario del PC dove installato il Software di supervisione Monitor
  - **Linea di Comunicazione Secondaria:** Identifica l'interfaccia secondaria utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata)
  - **Indirizzo NAT secondario:** Inserire l'indirizzo IP della rete Privata quando la chiamata è indirizzata verso un PC che risiede in una sottorete.
- NOTA: se si utilizza "Indirizzo NAT" quello ETH Primario dovrà essere l'IP pubblico del router principale.

**a.2. CONTACT ID:** Definisce a quale numero telefonico (ricevitore digitale) inviare la chiamata in formato Contact-ID.

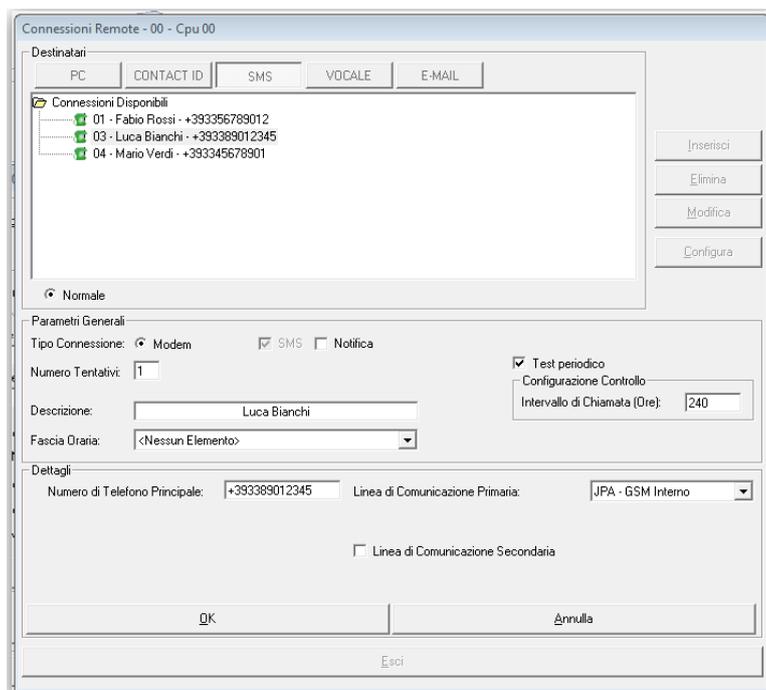
The screenshot shows the 'Connessioni Remote - 00 - Cpu 00' configuration window. It has a 'Destinatari' section with tabs for PC, CONTACT ID, SMS, VOCALE, and E-MAIL. A list contains '08 - Istituto Vigilanza - 025178665'. Below are 'Parametri Generali' and 'Dettagli' sections with various input fields and checkboxes for configuring the remote connection.

- **Inserisci:** abilita la creazione del nuovo numero di Rubrica
- **Elimina:** Permette la cancellazione della voce selezionata
- **Modifica:** Permette la modifica delle configurazioni della voce selezionata

- **Configura:** Permette di selezionare per quali oggetti (MacroZone, Zone, Ingressi Digitali ecc ecc è necessario inviare segnalazione remota al ricevitore digitale).
- **Normale:** Definisce la modalità di visualizzazione dei numeri inseriti nella rubrica
- **Tipo di connessione:** Identifica la modalità con cui verranno inviate le segnalazioni (non modificabile).
- **Numero tentativi:** Definisce il numero di volte che la centrale CS600 tenta di inviare la chiamata remota al ricevitore digitale ogni volta che si verifica un evento configurato per eseguire tale procedura.
- **Descrizione:** Identificativo del numero di rubrica (es. Istituto vigilanza)
- **Fascia Oraria:** Se presente stabilisce l'arco temporale in cui al numero selezionato verranno inviate le chiamate da parte della centrale CS600.
- **Numero di telefono Principale:** Inserire il numero telefonico del ricevitore digitale al quale verranno inoltrate le chiamate.
- **Linea di Comunicazione Primaria:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata).
- **Numero di telefono Secondario:** Inserire il numero telefonico secondario del ricevitore digitale dove inviare le chiamate.
- **Linea di Comunicazione Secondario:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata)

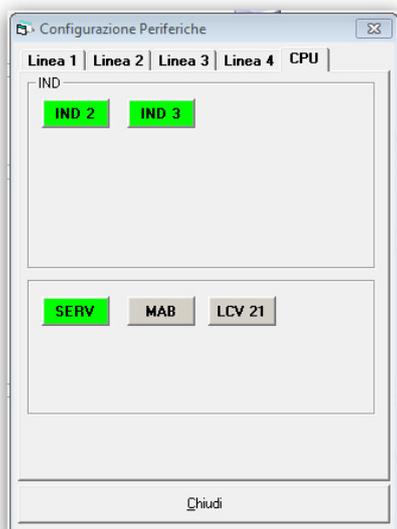
NOTA: per lo standard Contact-ID l'istituto di vigilanza rilascerà un codice identificativo del sito chiamante, che dovrà essere inserito nel menù "Configurazione Impianti" selezionando ogni singolo impianto "nella voce Codice CID" che dovrà generare la chiamata verso il ricevitore digitale.

**a.3. SMS:** Definisce a quale numero telefonico inviare il messaggio di segnalazione in formato SMS.



- **Inserisci:** abilita la creazione del nuovo numero di Rubrica
- **Elimina:** Permette la cancellazione della voce selezionata
- **Modifica:** Permette la modifica delle configurazioni della voce selezionata

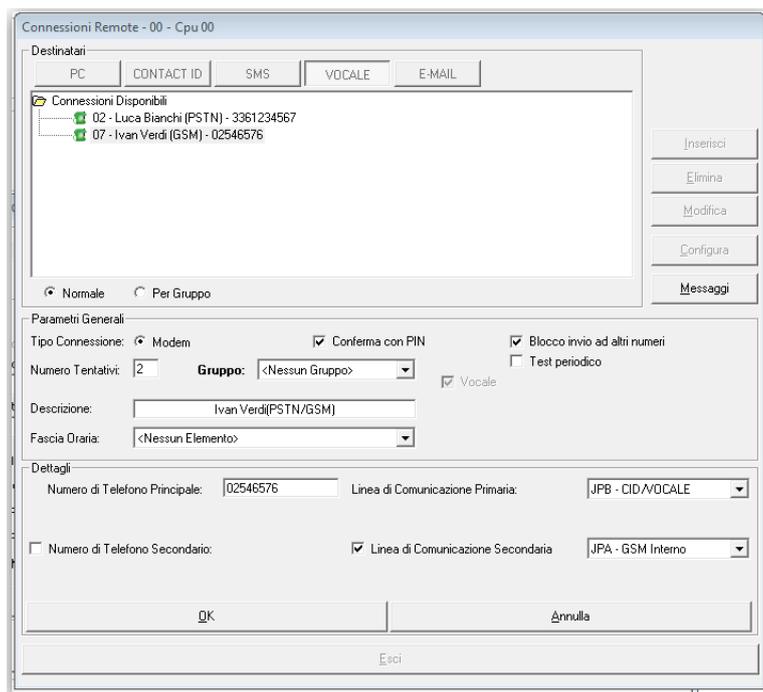
- **Configura:** Permette di selezionare per quali oggetti (MacroZone, Zone, Ingressi Digitali ecc ecc è necessario inviare l'SMS al numero selezionato).
- **Normale:** Definisce la modalità di visualizzazione dei numeri inseriti nella rubrica
- **Tipo di connessione:** Identifica la modalità con cui verranno inviate le segnalazioni (non modificabile).
- **Test Periodico:** intervallo espresso in ore, al termine del quale la centrale CS600 invia un SMS di "Live/Test in Vita" al numero di telefono selezionato.
- **Numero tentativi:** Definisce il numero di volte che la centrale CS600 tenta di inviare l'SMS al numero di telefono selezionato ogni volta che si verifica un evento configurato per eseguire tale procedura.
- **Descrizione:** Identificativo del numero di rubrica (es. Fabio Rossi)
- **Fascia Oraria:** Se presente stabilisce l'arco temporale in cui al numero selezionato verranno inviate gli SMS da parte della centrale CS600.
- **Numero di telefono Principale:** Inserire il numero telefonico del ricevitore digitale dove inviare le chiamate.
- **Linea di Comunicazione Primaria:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata).
- **Linea di Comunicazione Secondario:** Identifica l'interfaccia secondaria utilizzata per effettuare la chiamata (es: modem esterno MDM-GSM collegato alla JP16)



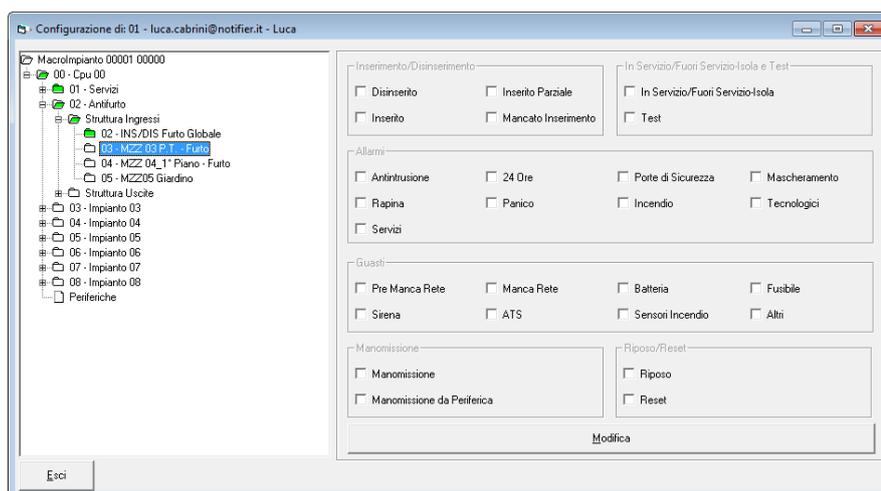
**a.3.1 SMS:** E' possibile attraverso una configurazione della periferica virtuale **LVC 21** (*cap 3.21.10*) presente nella *configurazione periferiche\_cpu* (dalla versione Firmware CS600 vs 7.07 o sup) inviare SMS alla centrale CS600 per eseguire dei comandi (es Inserimento/Disinserimento Macrozona, Aperture cancello, Accensione Luci .....).

I comandi disponibili attraverso SMS sono 32 e possono essere lanciati da un operatore abilitato presente in centrale e in condizione di In Servizio.

**a.4. Vocale:** Definisce a quale numero telefonico inviare la chiamata di segnalazione in formato vocale.



- **Inserisci:** abilita la creazione del nuovo numero di Rubrica
- **Elimina:** Permette la cancellazione della voce selezionata
- **Modifica:** Permette la modifica delle configurazioni della voce selezionata
- **Configura:** Permette di selezionare per quali oggetti (MacroZone, Zone, Ingressi Digitali/Analogici etc.) è necessario inviare l'SMS al numero selezionato.



- **Messaggi:** Permette la configurazione e la registrazione dei messaggi vocali.
- **Normale – Gruppo:** Da 1 a 32. Definisce la modalità di visualizzazione e raggruppamento dei numeri inseriti nella rubrica.

**Nota:**

**Gruppo:** Quando si inseriscono dei numeri suddivisi per “Gruppo” la sequenza delle chiamate avverrà partendo dal 1° numero presente nella lista.

Se durante la fase di chiamata il 1° numero risponde e conferma la ricezione (in base alle configurazioni sotto citate), la coda delle chiamate verrà interrotta in quanto nella

suddivisione a **Gruppo** è sufficiente che la chiamata remota venga gestita da un utente presente nell'elenco.

Se il 1° numero invece non è raggiungibile o non può rispondere la chiamata verrà inviata al secondo della lista e così via fino a quando un utente risponde e conferma il messaggio.

I tentativi e le conferme di chiamata vengono registrate nell'archivio eventi della CS600

**Normale:** Quando si inseriscono dei numeri suddivisi per "**Normale**" la sequenza delle chiamate avverrà partendo dal numero con ID più basso presente nella lista.

Se durante la fase di chiamata il numero con ID più basso risponde e conferma la ricezione (*in base alle configurazioni sotto citate*), la coda delle chiamate verrà interrotta in quanto nella suddivisione a **Normale** è sufficiente che la chiamata remota venga gestita da almeno un utente presente nell'elenco.

Se il numero con ID più basso invece non è raggiungibile o non può rispondere la chiamata verrà inviata a quello successivo della lista e così via fino a quando un utente risponde e conferma il messaggio.

I tentativi e le conferme di chiamata vengono registrate nell'archivio eventi della CS600.

- **Tipo di connessione:** Identifica la modalità con cui verranno inviate le segnalazioni (non modificabile).

- **Conferma PIN** (*senza Blocco invio ad altri numeri*): se abilitato, durante la fase di ricezione chiamata necessita l'inserimento del proprio PIN operatore (6 cifre) preceduto dal "#" per terminare la coda delle chiamate e far considerare la chiamata remota andata buon fine.

Parametro abilitabile per singolo Numero di telefono.

- **Blocco Invio ad altri numeri** (*senza Conferma con PIN*): se abilitato, permette di terminare la coda delle chiamate per l'evento che ha generato la chiamata ricevuta con la pressione di "# + \*".

Parametro abilitabile per singolo Numero di telefono.

- **Conferma PIN + Blocco invio ad altri numeri:** Se abilitati durante la fase di ricezione della chiamata per terminarne la coda e confermare la ricezione della chiamata diventa necessario premere "# + PIN Operatore (a 6 cifre) + \*"

Parametro abilitabile per singolo Numero di telefono.

Es: # (attendere bip) + PIN Operatore (a 6 cifre) + \* (attendere bip per avere conferma avvenuto blocco).

- **Numero tentativi:** Definisce il numero di volte che la centrale CS600 tenta di inviare la chiamata remota al numero di telefono selezionato ogni volta che si verifica un evento configurato per eseguire tale procedura.

- **Gruppo:** permette l'assegnazione successiva ad un gruppo del numero selezionato

- **Test Periodico:** intervallo espresso in minuti, al termine del quale la centrale CS600 invia una chiamata di "Live/Test in Vita" al Software di Supervisione.

- **Descrizione:** Identificativo del numero di rubrica (es: Luca Bianchi).

- **Fascia Oraria:** Se presente stabilisce l'arco temporale in cui il numero selezionato riceverà le chiamate da parte della centrale CS600.

- **Numero di Telefono principale:** Inserire il numero di telefono a cui inviare la chiamata.

- **Linea di Comunicazione Primaria:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata)

- **Linea di Comunicazione Secondaria:** Identifica l'interfaccia secondaria (back-up in caso di disservizio della primaria) utilizzata per effettuare la chiamata al numero di telefono Principale (di default viene selezionata quella corretta per il tipo di chiamata).

- **Numero di Telefono secondario:** Inserire il numero di telefono secondario a cui inviare la chiamata, con i riferimenti della stessa persona fisica.

#### a.4.1 MESSAGGI: Menù di programmazione e configurazione messaggi vocali:

In questo menù è possibile definire per ogni messaggio, di tipo vocale, per quali eventi sarà inviato.

- **Descrizione:** Identificazione testuale del messaggio

- **File Audio:**

- **Ascolta:** mette in Play la traccia audio registrata in formato wave 16 bit.
- **Elimina:** elimina la traccia audio selezionata.
- **Registra:** avvia la modalità di registrazione attraverso le periferiche audio del PC su cui è installato il PKSecurity600.

**NOTA:**

- Il messaggio vocale “COMUNE” deve essere sempre configurato e registrato.

- La traccia audio ha una durata max di 10 secondi per messaggio che viene mostrata durante la fase di registrazione.

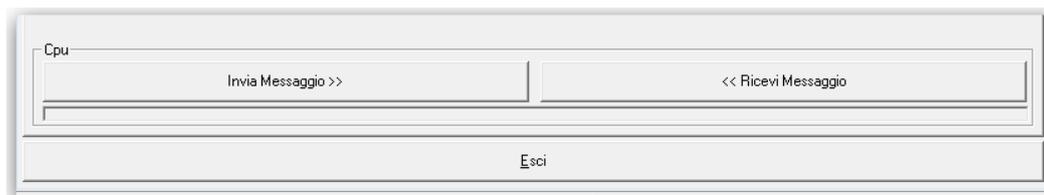
Alla fine della registrazione verrà visualizzata la directory nella quale verrà salvato il file (default: MessaggiVocali).

I messaggi vocali vengono esportati durante la fase di Export dell’impianto

- I messaggi registrabili ed utilizzabili sono nr° 9 + nr° 1Messaggio Comune + nr° 1 - Messaggio per manomissione M-Contact-ID.

- Ogni singolo messaggio può essere configurato all’inoltro a fronte di differenti condizioni/eventi (Allarme, Rapina, Tecnologico, Manca rete, etc) Si consiglia che la traccia audio sia registrata per non creare confusione ma che identifichi la segnalazione ricevuta nel modo più appropriato possibile.

**a.4.2 COMANDI RUBRICA:** dal menù Proprietà Cpu – Comandi è necessario inviare o ricevere le tracce audio.



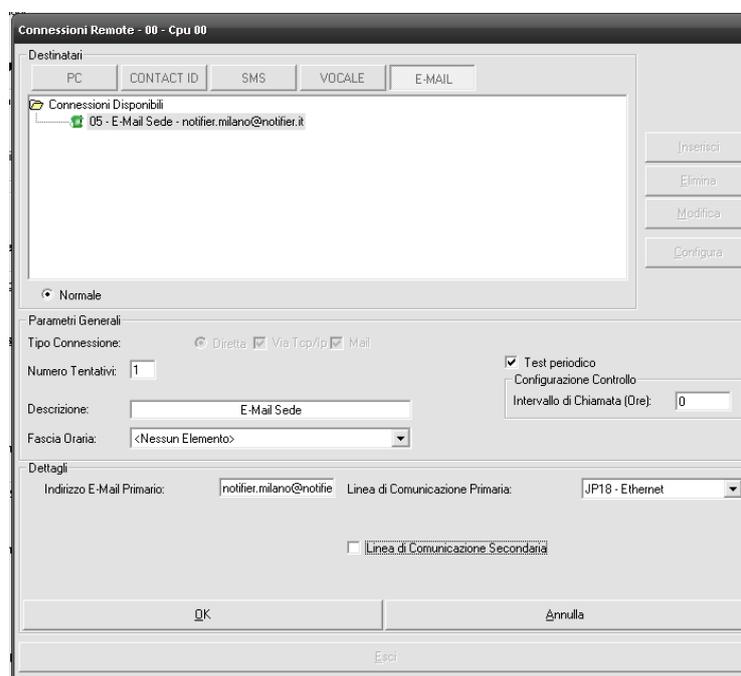
**Invia Messaggio:** durante la fase di connessione invia la traccia audio del messaggio selezionato all'interno della CS600.

Sarà necessario eseguire questa operazione su ogni messaggio.

**Ricevi Messaggio:** durante la fase di connessione riceve la traccia audio del messaggio selezionato dalla CS600 per essere salvato nel PKSecurity600.

Sarà necessario eseguire questa operazione su ogni messaggio.

**a.5 E-MAIL:** Definisce a quale numero indirizzo @email inviare la segnalazione.



- **Inserisci:** abilita la creazione del nuovo indirizzo di Rubrica
- **Elimina:** Permette la cancellazione della voce selezionata
- **Modifica:** Permette la modifica delle configurazioni della voce selezionata
- **Configura:** Permette di selezionare per quali oggetti (MacroZone, Zone, Ingressi Digitali ecc ecc è necessario inviare l'SMS al numero selezionato).
- **Normale:** Definisce la modalità di visualizzazione dei numeri inseriti nella rubrica
- **Tipo di connessione:** Identifica la modalità con cui verranno inviate le segnalazioni (non modificabile).
- **Test Periodico:** intervallo espresso in ore, al termine del quale la centrale CS600 invia un E-mail di "Live/Test in Vita" all'indirizzo selezionato.
- **Numero tentativi:** Definisce il numero di volte che la centrale CS600 tenta di inviare una e-mail all'indirizzo selezionato ogni qualvolta si verifichi un evento configurato per eseguire tale procedura.
- **Descrizione:** Identificativo del numero di rubrica (es. Fabio Rossi).
- **Fascia Oraria:** Se presente, stabilisce l'arco temporale in cui al numero selezionato verranno inviate gli SMS da parte della centrale CS600.
- **Indirizzo E-Mail Primario:** Inserire l'indirizzo email del destinatario della chiamata remota.

- **Linea di Comunicazione Primaria:** Identifica l'interfaccia utilizzata per effettuare la chiamata (di default viene selezionata quella corretta per il tipo di chiamata).
- **Linea di Comunicazione Secondaria:** Non utilizzata.

**B.6 SERVER DI POSTA;** Definisce i parametri utilizzati dalla CS600 per inviare le chiamate remote in formato e.mail.

- **Indirizzo IP:** Identifica l'indirizzo del Provider o del server SMTP che fornisce il servizio @email.
- **Hostname:** Identifica il nome del Provider o del server SMTP che fornisce il servizio @email.
- **Porta (SMTP):** porta di rete utilizzata dal Provider o dal server SMTP
- **Autenticazione:** Definisce i parametri di accesso al servizio di invio mail, rilasciati dal provider durante la registrazione dell'account o dall'amministratore di rete.
- **Crittografia:** Parametri di sicurezza per l'accesso al servizio di invio mail
- **Destinatario:** Spazio dedicato all'inserimento manuale di un indirizzo e-mail utilizzabile per fare un test di invio di una mail da parte della CS600.

**18 Cpu di Rete:** Definisce i parametri di associazione/integrazione ad una CPU E-net ,

- **Indirizzo IP Privato:** Identifica l'indirizzo IP della sottorete (configurato sulla CS600)
- **Indirizzo IP Pubblico:** Identifica l'indirizzo IP pubblico del router
- **Operatore di connessione:** Definisce quale utente utilizzare per la connessione verso la cpu E-net.
- **Password di connessione:** Definisce quale password utilizzare per la connessione verso la cpu E-net.

## 19 Configurazione ModBus: Permette la configurazione delle porte di comunicazioni della centrale a rendere disponibile il protocollo ModBus.



**Seriale:** *Abilita la porta seriale JP20 – RS232*

**USB:** *Abilita la porta JP16 - USB-A*

**TCP/IP:** *Abilita la porta JP18 - ETH*

- **Porta TCP/IP:** *permette di modificare la porta TCP su cui inviare il protocollo (default 502).*

**Accesso con Login:** *Definisce le modalità in cui dovrà essere stabilita la connessione da parte del sistema terzo verso la CS600.*

- **Con Flag:** *l'operatore deve essere definito nel sistema di supervisione e può essere dinamico.*
- **Senza Flag:** *L'operatore di connessione è definito dalla CS600 ed è fisso con l'operatore Supervisor.*

NOTA:

Gli Operatori che saranno utilizzati per la connessione dovranno avere la Password di connessione abilitata.

L'Operatore 9999 Installatore non può essere utilizzato come Utente di connessione.

Configurazione disponibile da Firmware CS600 – Centrale\_furto\_711.mot e PKSecurity600 versione 1.0.0036 o sup

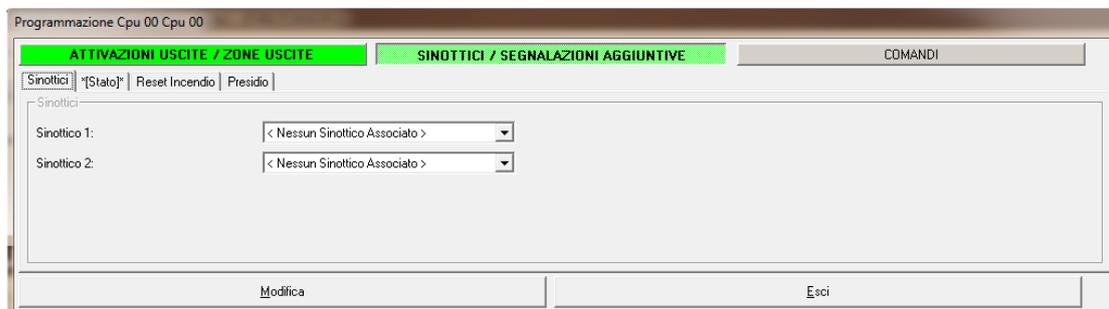
## 20 Ripristina Descrizioni di Default:

- IND/ALI;** Riporta tutte le descrizioni modificate delle periferiche IND8/4 o ALI8/8 al valore di fabbrica.
- zLCD/RXE/AEI;** Riporta tutte le descrizioni modificate delle periferiche LCD600s, RXE o AEI-485 al valore di fabbrica.

### 3.18.2. Programmazione

Cliccando sul tasto **Programmazione** viene visualizzata la finestra di gestione, Figura sotto, dove risiedono tutte le attivazioni in base ai differenti stati dell'oggetto selezionato (in questo caso la centrale CS600).

Negli impianti dove le configurazioni/attivazioni non devono essere personalizzate per MacroZona/Zona/Ingresso è sufficiente eseguire la programmazione della sola centrale CS600 attraverso questo menù.



**Nota:** Per dare maggior libertà di configurazione, tale finestra di programmazione viene riproposta sia per le Macrozone Ingresso che per le Macrozone di Uscita, le Zone Ingressi, le Zone uscita, gli Ingressi Digitali e le Uscite digitali.

Anche questi elementi hanno infatti la possibilità di gestire sinottici, comandi e attivazioni particolari in base ai diversi stati in cui si trovano.

La finestra si presenta suddivisa in tre principali blocchi nominati:

- 21 **SINOTTICI / SEGNALAZIONI AGGIUNTIVE** (rif 1.3.1).
- 22 **ATTIVAZIONI USCITE / ZONE USCITE** (rif 1.3.2).
- 23 **COMANDI** (rif 1.3.3).

### 3.18.2.1. Attivazioni Uscite / Zone Uscite

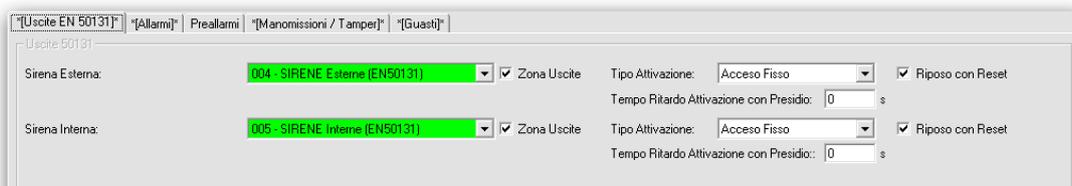
Le attivazioni innescano l'uscita / zona uscita al verificarsi della condizione selezionata, ma non la mettono a riposo quando tale condizione non è più presente.

Il riposo delle uscite/zona uscite associate ad una condizione di attivazione può avvenire in tre modi:

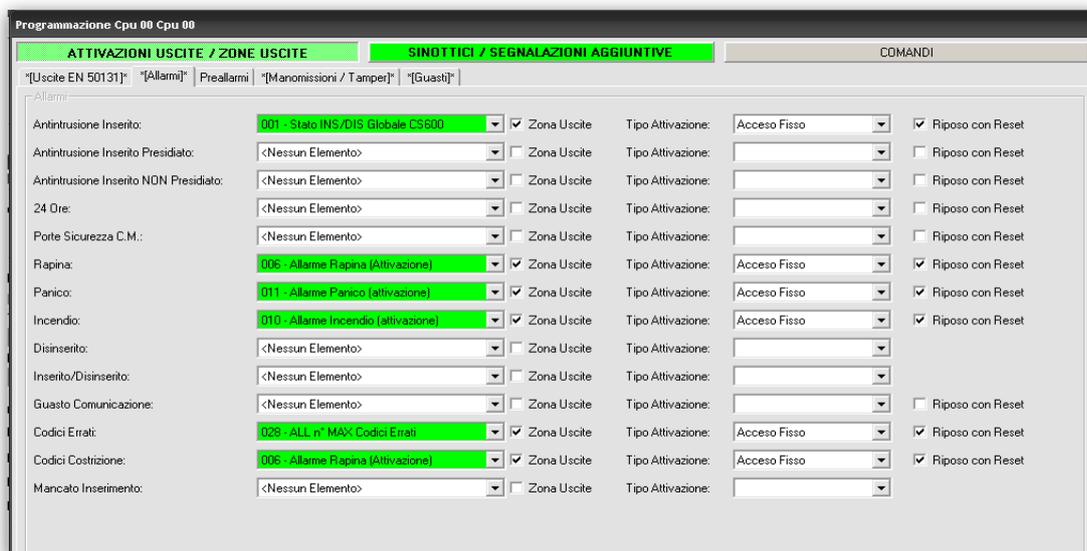
- al reset di uno degli eventi che ha generato la condizione, se abilitato al tipo di attivazione il flag “riposo con reset”.
- alla scadenza del tempo di attivazione (OND configurato alle uscite digitali) impostato nelle proprietà dell'uscita.
- Con un comando di riposo impartito da terminale, supervisore o altre azioni programmate.

Le immagini di seguito riportano la configurazione standard che viene eseguita nell'impianto Base 0001\_V2.

#### ➤ Configurazione Attivazioni: Uscite EN50131



#### ➤ Configurazione Attivazione: Allarmi



#### ➤ Configurazione Attivazione: PreAllarmi



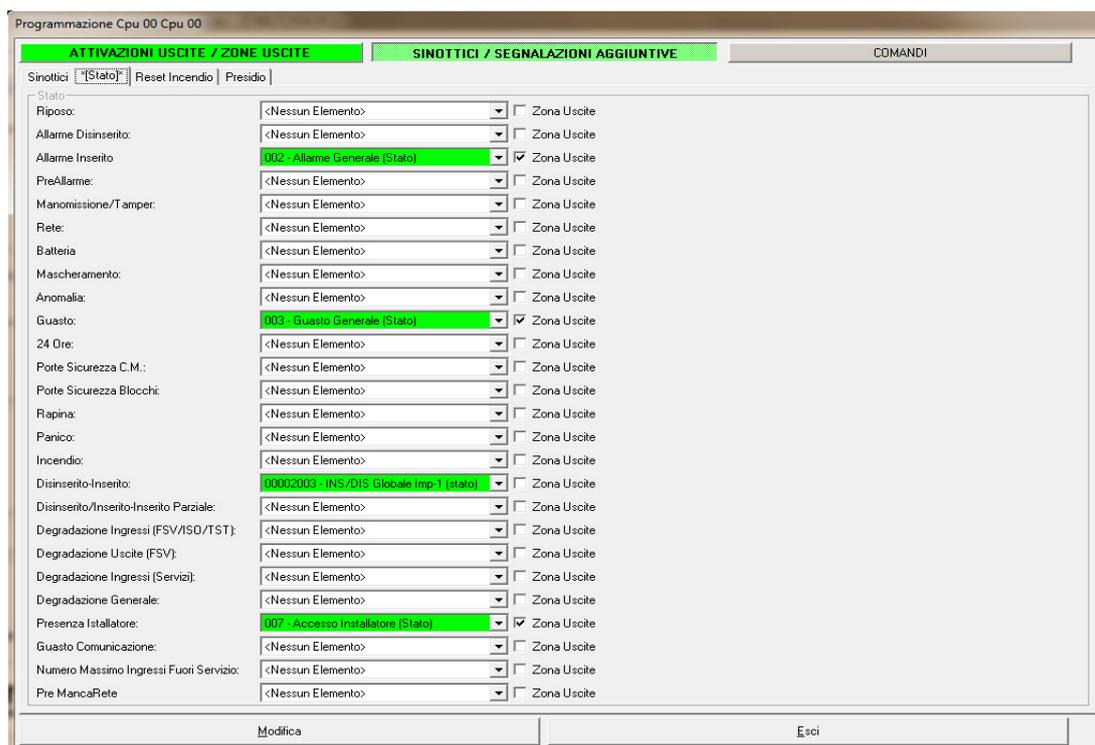
➤ Configurazione Attivazione: Manomissione/Tamper



➤ Configurazione Attivazione: Guasti



### 3.18.2.2. Sinottici / Segnalazioni aggiuntive



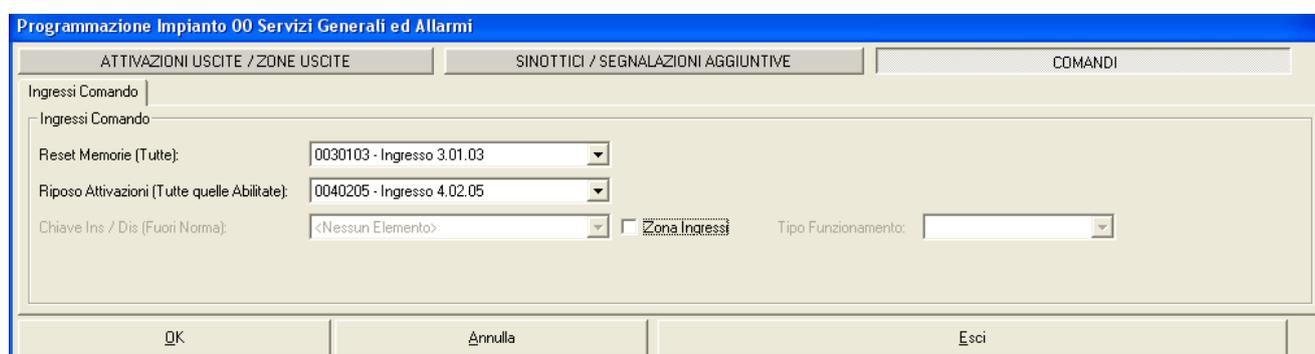
Gli stati attivano l'Uscita o Zona di uscita al verificarsi della condizione e la mettono a riposo quando la condizione non è più presente. Un tipo particolare di stato è il sinottico, normalmente usato per comandare LED tricolore degli LCD600S/AEI-485, secondo una logica più complessa, nella quale sono previsti modalità di attivazione diverse.

In funzione dell'oggetto sono disponibili sinottici specifici che vanno scelti in funzione delle segnalazioni richieste.

**Esempio di gestione STATO:** Se all'apertura di una porta a Zona/MacroZona disinserita c'è la necessità di attivare una segnalazione (Cicalino/Led/Lampeggiante) è possibile farlo utilizzando nella pagina STATO nella sezione Sinottici/Segnalazioni Aggiuntive la voce Allarme Disinserito.

Questa Uscita/Zona Uscita rimarrà in stato di attivata fino a che la condizione scatenante (in questo caso l'apertura della porta) non torni in normalità (chiusura porta).

### 3.18.2.3. Comandi



I comandi permettono di utilizzare un ingresso digitale di una periferica IND8/4 o ALI8/8 per impartire un comando all'oggetto che si sta programmando. Dato che non è possibile riconoscere l'utente che lo attiva, questi comandi non sono conformi a normativa EN50131.

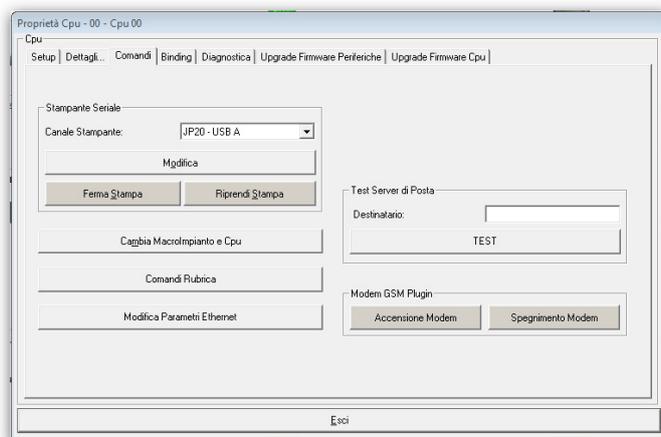
I comandi disponibili sono:

- Chiavi di Inserimento / Disinserimento, con funzionamento impulsivo o segue stato.
- Reset Memorie.
- Tacitazione Uscite.

### 3.18.3. Dettagli

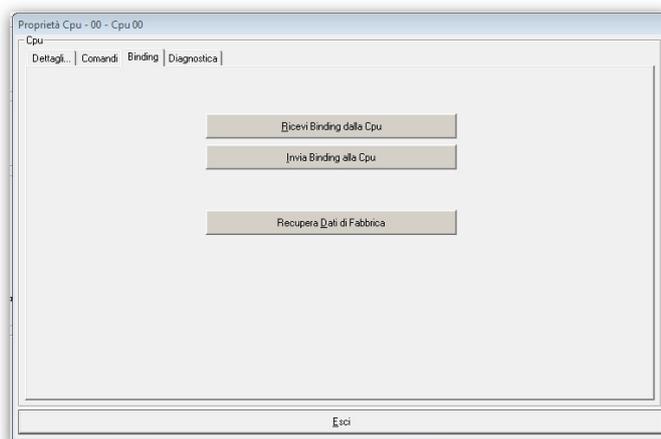
Mostra dati relativi alla versione di Firmware presente in centrale e data/ora dell'ultima modifica.

### 3.18.4. Comandi



- Abilita o interrompe la stampa seriale RS-232 abilitata sulla porta JP20 di centrale.
- Permette la modifica del numero Macroimpianto e/o ID-CPU.
- Permette la modifica di indirizzo IP, netmask e gateway della centrale connessa.
- Permetti comandi allineare i messaggi di rubrica ( cap 3.18.1 punto 16.a.4.2)

### 3.18.5. Binding

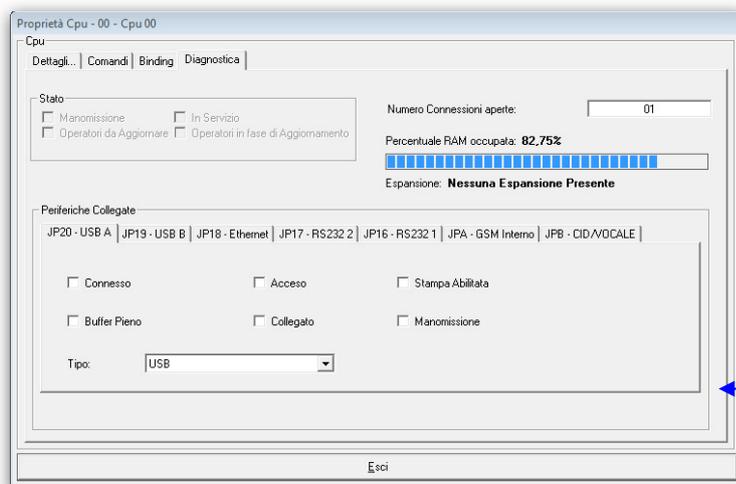


Il comando **Ricevi Binding dalla Cpu** permette il salvataggio del binding delle periferiche connesse alle 4 linee di centrale.

Il comando **Invia Binding alla Cpu** permette il ripristino del binding precedentemente salvato nel momento di una sostituzione di una CPU.

In caso di sostituzione di una scheda madre CS600 su un impianto in funzione, si rende necessario l'invio del comando **Recupera dati di Fabbrica** con lo scopo di ripristinare il valore della chiave di criptatura del protocollo di comunicazione al valore di fabbrica, permettendo così una nuova configurazione automatica per il nuovo impianto.

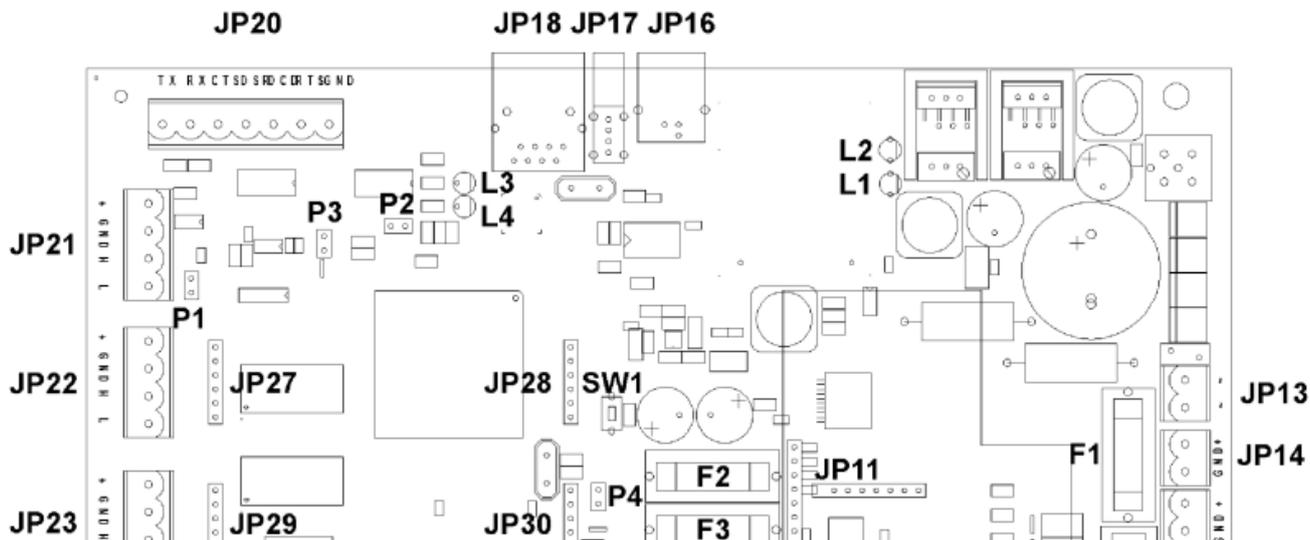
### 3.18.6. Diagnostica



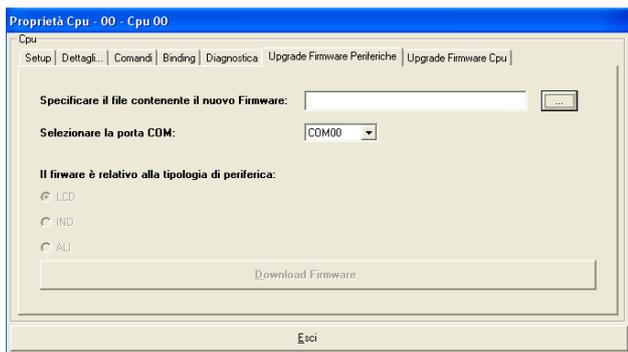
Nella parte superiore vengono mostrate le connessioni attive e la percentuale di RAM utilizzata.  
NB: il menù Diagnostica presenta comandi e opzioni differenti se si è on-line con la CS600, rispetto alla modalità off-line.

L'area **Periferiche Collegate** mostra le caratteristiche delle porte di comunicazione di centrale, di default settate come segue:

- |    |             |                            |   |
|----|-------------|----------------------------|---|
| 24 | <b>JP20</b> | (morsettiera RS_232)       | Tipo: <b>Stampante.</b>                                 |
| 25 | <b>JP19</b> | (connettore disponibile)   | Tipo: Non utilizzato.                                   |
| 26 | <b>JP18</b> | (connettore RJ-45)         | Tipo: <b>Connessione Ethernet.</b>                      |
| 27 | <b>JP17</b> | (morsettiera USB class. A) | Tipo: non disponibile in questa versione di FW.         |
| 28 | <b>JP16</b> | (connettore USB class. B)  | Tipo: <b>USB</b> , Utilizzato come connessione diretta. |



### 3.18.7. Upgrade Firmware Periferiche



Il software di gestione PK Security 600 è dotato di un sistema semplificato per la gestione degli aggiornamenti firmware delle periferiche di campo.

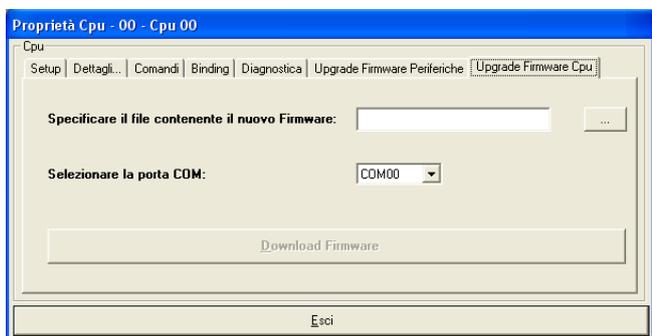
Una volta selezionato il file (es: LCD\_0x\_0105\_20xxxx.hex) e la porta di comunicazione, s'invia il file in centrale tramite il tasto **Download Firmware**. Successivamente sarà possibile, da un terminale *LCD600s*, aggiornare se stesso o tutte le periferiche di linea LCD che necessitano di tale upgrade firmware.

### Procedura:

- 1 Da disconnessi, impostare la COMxx assegnata alla connessione di centrale (cavo USB) come "Connessione Diretta" dal menù *Setup Periferiche di Comunicazione* del PKSecurity600.
- 2 Loggarsi da LCD600s con utente Installatore e abilitare lo scarico del Firmware CPU da *Menù/Tecnico/Impostaz.Tecniche/Abil.Scarico FW Per.*
- 3 Accedere al menù Configurazione Centrale/Upgrade del PKSecurity600.
- 4 Selezionare il file da caricare in centrale e impostare la porta di comunicazione.
- 5 Attendere il termine dell'operazione.
- 6 Accertarsi della corretta scrittura del Firmware Periferiche in centrale consultare il menù *Menù/Tecnico/Impostaz.Tecniche/Elenco FW Perif. Da terminale LCD600s.*
- 7 Selezionare le periferiche che richiedono aggiornamento firmware dal menù *Menù/Tecnico/Impostaz.Tecniche/Agg. FW Periferiche/Perif. Da aggiornare*

**Nota:** con la stessa procedura è possibile eseguire l'up-grade anche le periferiche ALI8/8 - IND8/4 – AEI485 – RXE485.

### 3.18.8. Upgrade Firmware CPU



La finestra **Upgrade Firmware Cpu** è dedicata alla gestione dell'aggiornamento della versione di centrale.

Come precedentemente mostrato per le periferiche, è sufficiente caricare il file di aggiornamento e inviare il nuovo firmware alla CPU tramite la porta di comunicazione selezionata.

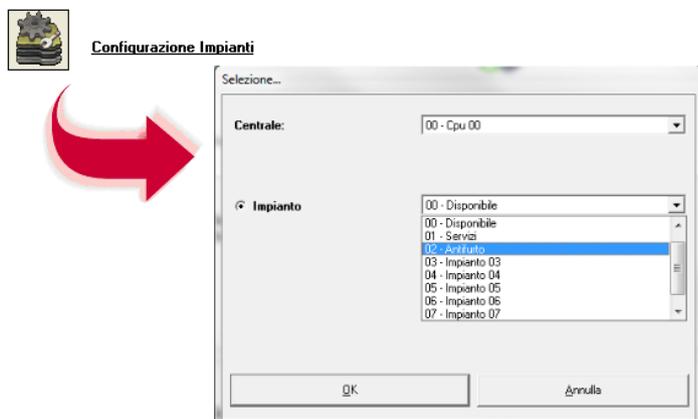
### Procedura:

- 1 Da disconnessi, impostare la COMxx assegnata alla connessione di centrale (cavo USB) come "Connessione Diretta" dal menù *Setup Periferiche di Comunicazione* del PKSecurity600.
- 2 Loggarsi da LCD600s con utente Installatore e abilitare lo scarico del Firmware CPU da *Menù/Tecnico/Impostaz.Tecniche/Agg.FW Centrale.*
- 3 Accedere al menù Configurazione Centrale/Upgrade Firmware CPU del PKSecurity600.
- 4 Selezionare il file da caricare in centrale e impostare la porta di comunicazione.

- 5 Attendere il termine dell'operazione.
- 6 Si renderà necessario eseguire un comando **Invia a CPU** (vedi cap.3.6) delle configurazioni del PK per ripristinare la precedente situazione.

Si consiglia di collegare la CPU al PC tramite l'apposito cavo USB prima dell'apertura del PKSecurity600.

## 3.19. Configurazione Impianti

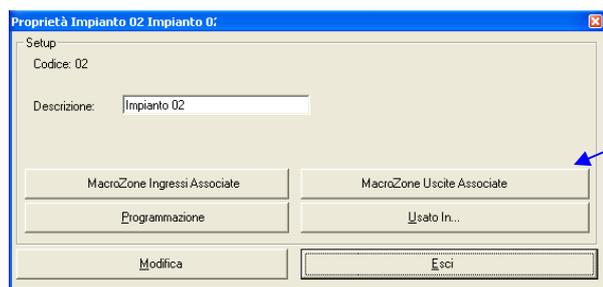


Nel sistema di sicurezza CS600 per **Impianto** s'intende un contenitore logico nel quale vengono associate le Macrozone ingresso/uscite che a loro volta permettono un'ulteriore suddivisione dell'impianto stesso. Ogni centrale può contenere max 8 Impianti (Impianto 00 non modificabile, 01 Servizi utilizzato per la gestione e diagnostica del sistema).

NOTA: La suddivisione per impianti può essere utile per la gestione attraverso un'unica centrale di uno stabile che contiene più appartamenti/uffici o unità separate.

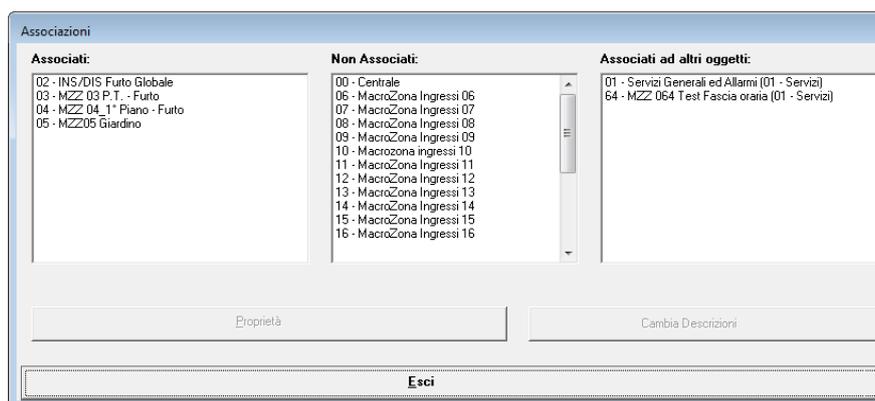
Ogni singola unità abitativa è un impianto che con la sua gestione separata sia di eventi, allarmi, attivazioni, inserimenti e disinserimenti dalla propria tastiera LCD è indipendente dai restanti impianti della CS600.

Una volta selezionato l'impianto desiderato e premuto **OK** si accede alla finestra di configurazione mostrata in figura sotto.



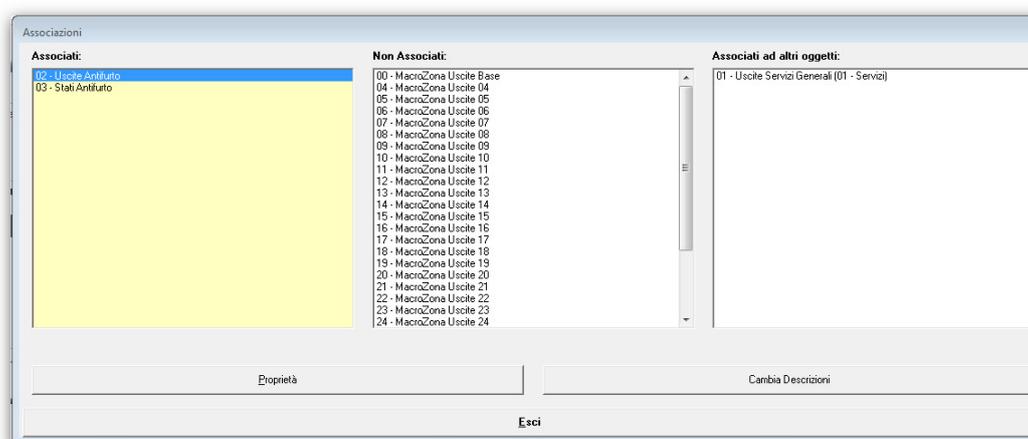
Prima di modificare la descrizione dell'impianto premere il tasto **Modifica**.

### 3.19.1. MacroZone Ingressi Associate



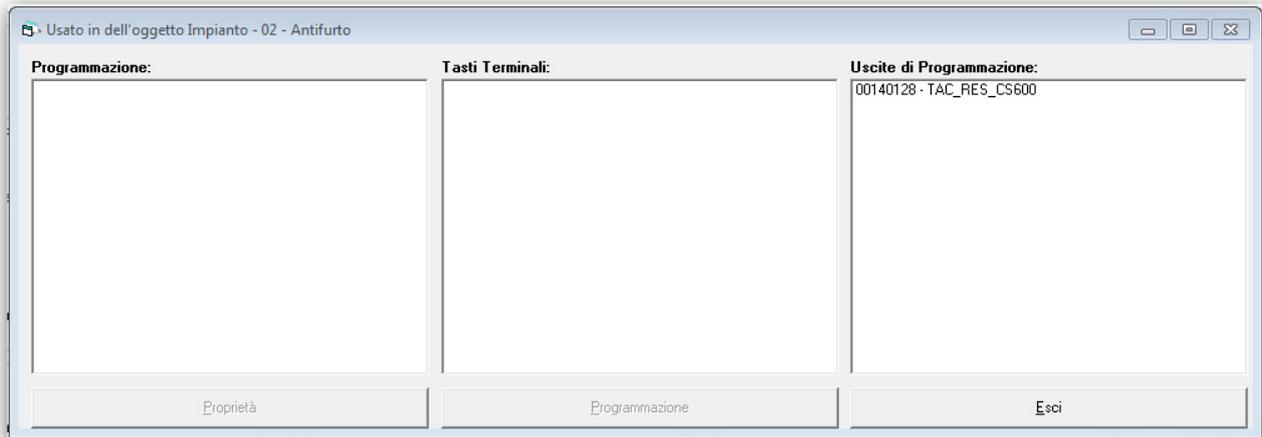
**Tasto Macrozone Ingressi Associate:** Permette la visualizzazione delle MacroZone associate all'impianto selezionato e/o presenti in altri impianti (le singole MacroZone possono essere associate ad un solo Impianto, quindi non può esistere la stessa MacroZona sotto due impianti differenti). Nell'esempio riportato in figura sopra viene mostrato un l'Impianto Antifurto con nr 4 Mzz associate, quelle disponibili "Non Associate" ad eccezione della MacroZona 01 "Servizi Generali ed Allarmi" e "MZZ 064 Test Fascia Oraria" riportate nella colonna di destra, significando che questa risiede nell'impianto 01 - Servizi.

### 3.19.2. MacroZone Uscite Associate



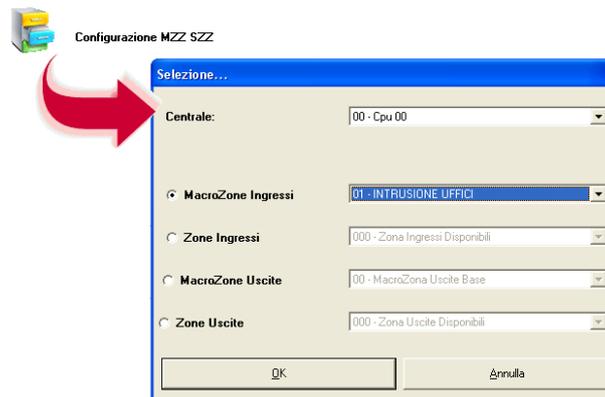
**Tasto Macrozone Uscite Associate:** Permette la visualizzazione delle MacroZone Uscite associate all'impianto selezionato (le singole MacroZone possono essere associate ad un solo Impianto, quindi non può esistere la stessa MacroZona sotto due impianti differenti). Nell'esempio riportato in figura sopra viene mostrato che l'impianto selezionato ha le MacroZone – 02-03 associate mentre la 01 – Uscite servizi generali risiede nell'impianto e presente nell'impianto 01 - Servizi.

### 3.19.3. Usato In...

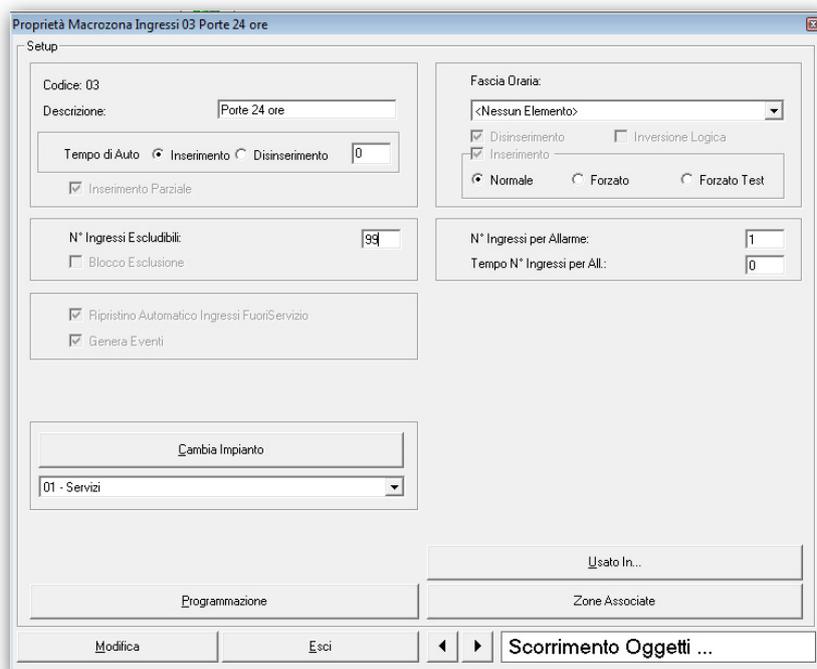


Visualizza una finestra di controllo che riporta gli elementi del sistema che comandano o subiscono l'azione dell'oggetto selezionato semplificando la ricerca a posteriori.

### 3.20. Configurazione MacroZone e Zone ingressi



Una volta selezionata la MZZ o SZZ di Ingresso/Uscita dalla finestra riportata in figura sopra, si accede al menù di configurazione dell'oggetto selezionato, viene di seguito riportato un esempio di configurazione di una Macrozona di ingresso con tutte le sue proprietà editabili:



### I parametri disponibili nella configurazione sono:

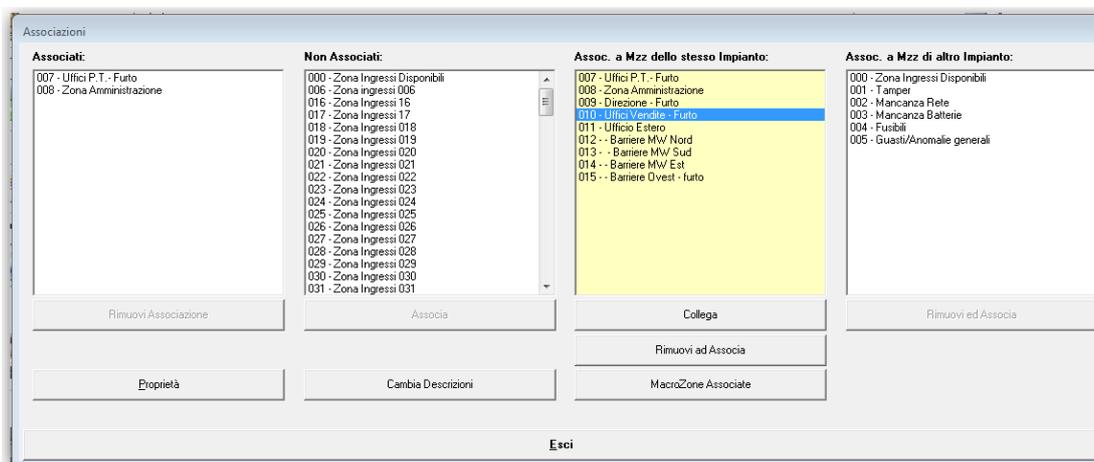
- **Descrizione:** Label descrittiva della Macrozona o Zona.
- **Tempo di Auto Inserimento / Disinserimento:** Se impostato, permette un Inserimento o Disinserimento automatico allo scadere di un tempo impostato espresso in secondi.
- **Inserimento Parziale:** Se abilitato permette un inserimento parziale della Zona o Macrozona.
- **Numero ingressi escludibili:** Se impostato, fissa un limite d'ingressi escludibili. Se all'interno della Zona o Macrozona si tenta di escludere ingressi in numero superiore al limite impostato, viene generato un evento di *n° max Ingressi Fuori Servizio*, al quale attraverso programmazione di STATO è possibile associare un attivazione.
- **Blocco esclusione:** Se abilitato impedisce l'esclusione di ulteriori ingressi rispetto al *n° ingressi escludibili* impostato. Se Numero ingressi escludibili è a 0 il blocco inibisce la possibilità di esclusione anche di un singolo oggetto.
- **Ripristino Automatico ingressi fuori servizio:** Con questo parametro abilitato, al Disinserimento della Zona o Macrozona, vengono rimessi automaticamente in servizio gli ingressi esclusi in modalità automatica o manuale.
- **Genera eventi:** Se disabilitato inibisce la generazione degli eventi della Zona o Macrozona.
- **Fascia Oraria associata:** In caso di associazione ad una fascia oraria la Zona o Macrozona cambia di stato (INS/DIS) a seconda della variazione degli intervalli configurati nella fascia. Se la Fascia oraria = ON allora la Zona o Macrozona ingressi verrà Inserita automaticamente (se abilitato il relativo Flag *Inserito*), se la fascia orarie = OFF la Zona o Macrozona ingressi verrà disinserita (se abilitato il relativo flag *Disinserimento*). In caso di abilitazione del flag *Inversione Logica*, la zona o Macrozona assumerà uno stato inverso rispetto al normale funzionamento sopra descritto. (Es: se associata ad una MacroZona Uscite l'associazione della fascia potrà essere utilizzata per gestire delle attivazioni temporali definite come per esempio irrigazione o delle luci nei parcheggi).
- **N° Ingressi per Allarme:** Corrisponde al n° minimo di ingressi in stato di allarme per poter generare l'evento di Allarme Zona o Macrozona.
- **Tempo n° Ingressi per Allarme:** Corrisponde al tempo max in cui si debbano verificare un n° max di ingressi in allarme per poter determinare lo stato di Allarme della Zona o Macrozona.
- **Cambia Impianto:** Modifica l'associazione di una Zona o Macrozona ingressi ad un Impianto logico.

- **Programmazione:** Apre la finestra di configurazione delle attivazioni particolari della Zona o Macrozona selezionata (vedi par. 3.18.3 – Programmazione Impianto).
- **Usato In.:** Visualizza una finestra di controllo che riporta gli elementi del sistema che comandano o subiscono l'azione dell'oggetto selezionato semplificando la ricerca a posteriori.
- **Zone Associate:** disponibile nelle proprietà delle sole Macrozone, visualizza le zone associate alla Macrozona selezionata, ne permette la rimozione o l'associazione di nuove.
- **Macrozone Associate:** disponibile nelle proprietà delle sole Zone, visualizza a quali Macrozone è stata associata la Zona selezionata.
- **Ingressi Associati:** disponibile nelle proprietà delle sole Zone, visualizza a quali ingressi digitali sono associati alla Zona selezionata e ne permette la rimozione o l'associazione di nuovi.
- **< > Scorrimento Oggetti:** Permette di spostarsi alla MacroZona successiva o precedente, senza necessita di chiudere e riaprire la finestra.

### 3.20.1. Macro Zone – Zone Ingressi/Uscite Associate

Le creazione di Macro Zone e Zone Associate facilita per esempio la gestione degli inserimenti globali di Zone appartenenti a Macrozone diverse o attivazioni di più gruppi di uscite che riportano stati, accendono delle luci o effettuano controlli tecnologici. E' fondamentale che tali Zone o Macrozone appartengano comunque allo stesso impianto.

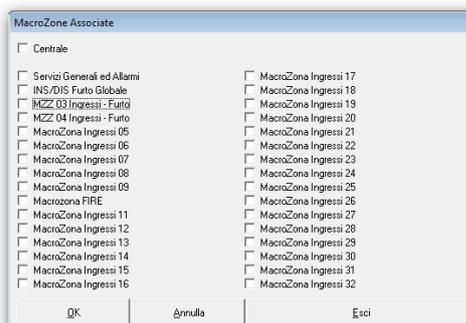
L'abilitazione delle zone associate va eseguita dall'apposito tasto *Zone Associate* presente nelle proprietà della Macrozona



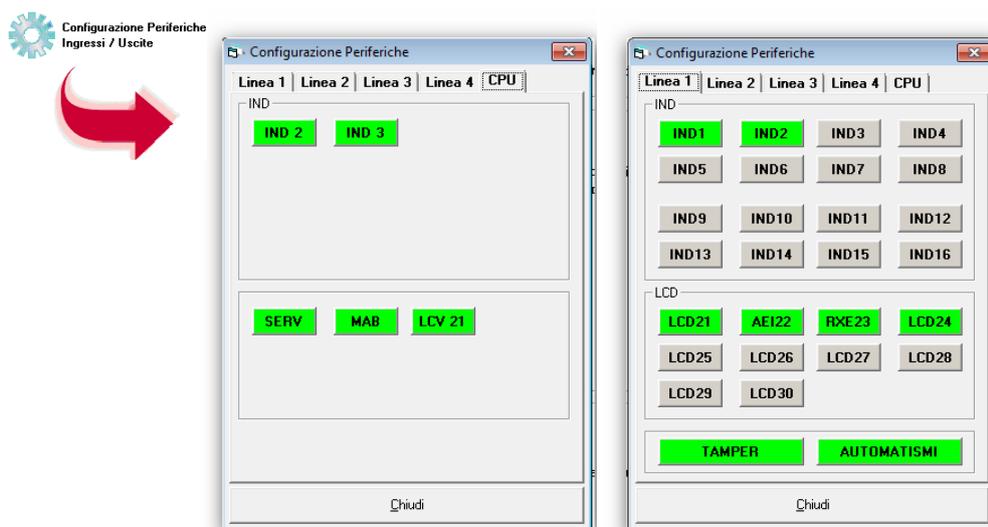
Una volta entrati nelle proprietà della Macrozona che avrà la funzione di collegamento, andranno selezionate le Zone precedentemente associate ad altre Macrozone ma presenti nello stesso impianto che si desidera collegare, premere il tasto **Collega**, le zone selezionate verranno portate nella prima colonna nominata **Associati**, in questo modo si è effettuato il collegamento delle Zone Ingresso. Dal menù **Verifica Struttura** si potrà verificare la nuova architettura con i collegamenti appena effettuati.

Il Tasto MacroZone Associate permette di visualizzare quali di queste sono Associate e collegate.

La finestra mostrerà solo quelle associate.



## 3.21. Configurazione Periferiche Ingressi / Uscite



Dalla finestra di selezione periferiche mostrata in figura sopra, viene identificata la struttura fisica della centrale CS600, ovvero l'insieme delle periferiche quali: schede di ingresso/uscita digitale, ingressi analogici, alimentatori di campo e terminali che compongono il sistema.

E' possibile consultare quali periferiche si trovano in stato "disponibile" oppure "in servizio" semplicemente accedendo al menu "**Configurazione Periferiche Ingressi/Uscite**" posizionato sulla pagina principale del software, noteremo infatti che le periferiche con icona verde corrispondono alle periferiche effettivamente programmate e/o Binding.

Il menù Configurazione Periferiche Ingressi/Uscite è stato suddiviso in 5 pagine per identificare le periferiche integrate nella scheda base di centrale (CPU) e tutte le altre, appartenenti alle rispettive 4 linee RS-485 di ampliamento.

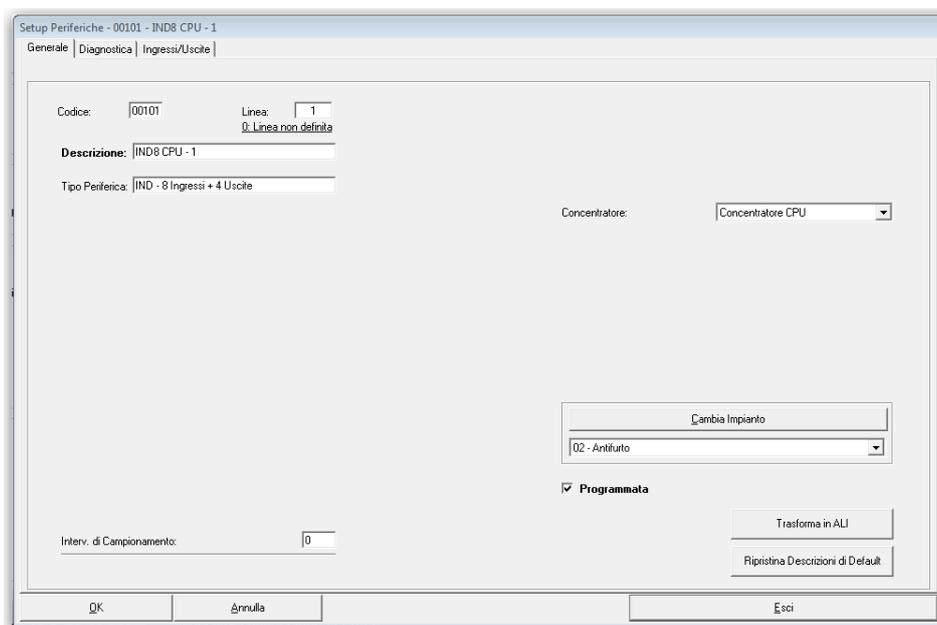
### La CPU dispone di:

- 1 Periferica IND 02 - 8 IN, 8 Out – identificati dall'1 all'8.
- 1 Periferica IND 03 - 8 IN, 8 Out – identificati dal 9 al 16.
- 1 Periferica SERV (periferica virtuale ATS e IN/OUT stato CONTACT-ID, stato stampante, stato Modem...).
- Periferica MAB (dedicata al controllo fusibili, temperatura e alimentazioni).

### Ogni linea RS485 dispone di:

- Max **16** Periferiche **IND** di Ingresso/Uscita (IND 8/4 oppure ALI8/8).
- Max **10** **LCD** (terminali di tipo LCD600S - AEI-485 - RXE).
- **Nr°1** Periferica **Linea** tutti gli ingressi tamper del sistema CS600 si trovano in questa periferica virtuale, che andranno poi associati secondo la struttura logica creata (es: Servizi generali ed allarmi). Questa periferica virtuale può anche essere utilizzata per comandare il binding automatico di tutte le periferiche (IND 8-4/ALI 8-8/LCD600/RXE) installate sulla linea. Il comando di In Servizio viene impartito dalla LCD600S nel menù Struttura Periferiche.
- Periferica **AUTOMATISMI**, composta da 128 uscite virtuali, utilizzabili come uscite di controllo o azioni per automazioni complesse e/o integrazione con il sistema Euronet. Ogni uscita virtuale può comandare fino ad un max di 8 Azioni contemporanee, impostate dalle proprietà dell'uscita.

### 3.21.1. Configurazione Periferica IND



Ogni periferica di Ingresso/Uscita viene configurata dalle 3 pagine principali:

- **Generale**
- **Diagnostica**
- **Ingressi/Uscite**

#### 3.21.1.1. Generale

La pagina **Generale** permette di modificare la *descrizione* della periferica selezionata, l'*associazione* ad un Impianto del sistema con *cambia Impianto*, mentre il tasto **Trasforma in ALI** posizionato in basso a destra ha la funzione di trasformare un indirizzo di periferica, precedentemente assegnato ad una periferica tipo **IND8/4** in una periferica tipo Alimentatore **ALI8/8**, modificandone quindi caratteristiche di funzionamento e configurazione come i fusibili, controllo alimentazioni e ulteriori Uscite digitali (per un totale di 8 OC + 2 Relè programmabili).

**Ripristina descrizioni di default:** riporta tutte le descrizioni degli ingressi/uscite della periferica selezionata alla descrizione di fabbrica (*es: Ingresso Digitale 1.01.01 - Uscita 1.01.01*).

**Concentratore** consente di suddividere in modo logico il posizionamento della periferica all'interno di un impianto. Questo permette di non compromettere i piani d'inserimento, gli eventi e gli allarmi di altri impianti in caso di anomalie/manomissioni, ma viene limitato solo alla porzione d'impianto a cui fa parte il concentratore.

**Nota:** Il flag "**Programmata**" identificherà la periferica di colore verde di figura cap 3.21, permettendo la configurazione degli ingressi e uscite nel menù di programmazione.

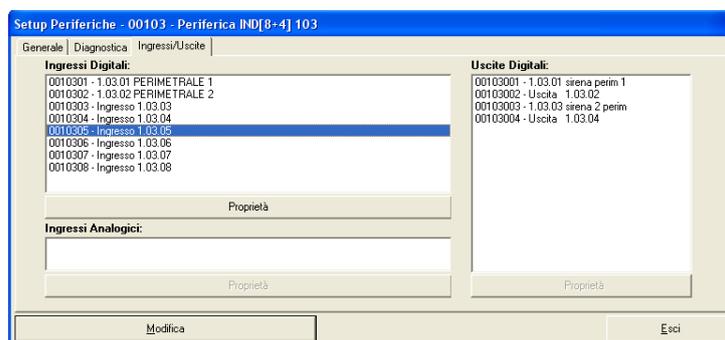
### 3.21.1.2. Diagnostica

La pagina **Diagnostica** mostra uno storico del tempo di attività della periferica selezionata, versione di firmware, numero di restart e altre informazioni utili al monitoraggio delle periferiche di campo. **N.B.:** Menù disponibile solo quando si è connessi con la CS600, i contatori vengono resettati ogni volta che viene cancellato il binding della periferica selezionata.

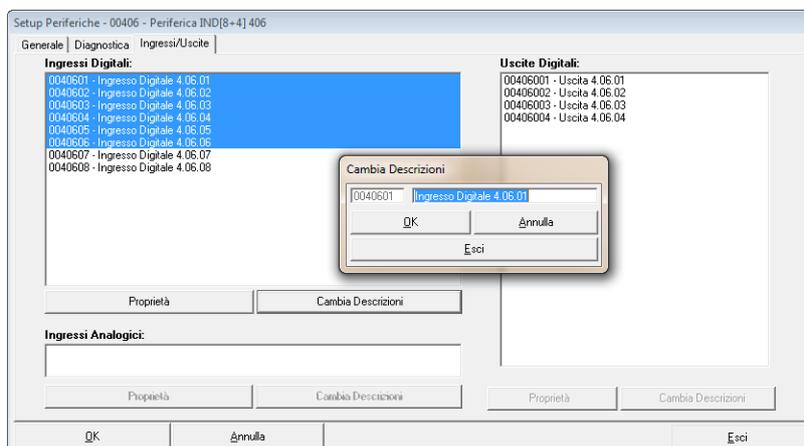


### 3.21.1.3. Ingressi/Uscite

Sotto viene mostrata la finestra di gestione **Ingressi/Uscite** di una periferica tipo IND8/4, il tasto **Proprietà** permette la configurazione specifica di ogni singolo Ingresso o Uscita appartenente alla periferica selezionata, meglio descritta nei paragrafi 3.21.6 e 3.21.7.



**Nota:** Tenendo premuto il click sinistro del mouse è possibile modificare le descrizioni in multi selezione come mostrato in figura sotto:



## 3.21.2. Configurazione periferica LCD/AEI/RXE

Setup Periferiche - 00121 - Terminale Furto 121

Generale | Configurazione | Controllo Accessi | Profili | Prog. Tasti e Led | MacroZone | Messaggi | Diagnostica | Ingressi/Uscite

Codice: 00121 Linea: 1  
0. Linea non definita

Descrizione: Terminale Furto 121

Tipo Periferica: Terminale LCD

Fascia: <Nessun Elemento>

Tipo Terminale: Furto

Tastiera Disabilitata

Pin Disabilitato

Concentratore: Concentratore CPU

Numero Max Tentativi d'Accesso Errati: 5

Periodo di Blocco per Tentativi d'Accesso Errati: 90

Cicalino Timbratura Disabilitato

Cicalino Terminale Disabilitato

Doppia Timbratura: Disabilitata

TimeOut Operatore: 90

Cambia Impianto

02 - Antifurto

Programmata

Trasforma in AEI

Trasforma in RXE

Ripristina Descrizioni di Default

Modifica

Esci

I settaggi di un terminale LCD600s vengono distribuiti nelle pagine di gestione presenti nelle finestre di configurazione.

### 3.21.2.1. Generale Terminale

Le pagine Generali permettono la configurazione di:

- **Descrizione:** Descrizione del terminale.
- **Fascia Oraria:** Il comportamento del terminale dipenderà dalla fascia oraria associata, quindi dallo stato degli intervalli configurati. (Es. quando la fascia oraria associata avrà un intervallo in stato di ON, il terminale permetterà il log-in degli operatori, viceversa con l'intervallo in stato di OFF il terminale negherà il login dell'operatore).
- **Cicalino Timbratura Disabilitato:** Disabilita il funzionamento del buzzer interno solo al momento del riconoscimento da parte dell'operatore con il Trasponder.
- **Cicalino terminale Disabilitato:** Disabilita il funzionamento del buzzer interno.
- **Disabilita Led Stato L3 (solo per RXE e AEI):** Disabilita la gestione del LED L3 dal terminale (live di comunicazione con CS600) ma ne rende configurabile l'utilizzo per segnalazioni varie.
- **TimeOut Operatore:** definisce il tempo di logout, espresso in secondi, di qualsiasi operatore dal terminale.
- **Tipo Terminale:** Seleziona la modalità Furto o Controllo Accessi.
- **Disabilita Tastiera:** Disabilita il funzionamento della tastiera lasciando abilitato solo l'antenna trasponder.
- **Disabilita PIN:** disabilita la possibilità di eseguire il Login tramite codice PIN.
- **N° max tentativi PIN errati:** Identifica il numero max di tentativi di immissione di un Pin errato, superato questo limite, il terminale entra in stato di Blocco per il tempo impostato nel Periodo di Blocco.
- **Periodo di Blocco per PIN errati:** identifica il periodo di persistenza di un Terminale in stato di Blocco espresso in secondi, da utilizzare in associazione del precedente.
- **Doppia Timbratura:** Funzione che rende obbligatorio l'utilizzo della doppia riconoscimento dell'operatore (Pin + Trasponder).

- **Cambia Impianto:** Permette l'associazione di un terminale ad un impianto. Utilizzato nella visualizzazione degli eventi differenziata per impianto e nella gestione delle MacroZone e Zone ingressi e Azioni associate ai tasti dell'LCD600S.
- **Trasforma in AEI:** ha la funzione di trasformare un indirizzo di periferica, precedentemente assegnato ad una periferica tipo **LCD** in una periferica tipo **AEI**, modificandone quindi caratteristiche di funzionamento, proprietà e configurazione; come per esempio la gestione degli ingressi e delle uscite digitali.  
Il terminale AEI-485 dispone di: 1 ingressi digitale e 5 OUT digitali (Cicalino del terminale, uscita OC disponibile, due uscite LED tricolore, un'uscita LED di stato terminale).
- **Trasforma in RXE:** ha la funzione di trasformare un indirizzo di periferica, precedentemente assegnato ad una periferica tipo **LCD** o **AEI** in una periferica tipo **RXE** (terminale abilitato a ricevere codici da Radiocomando 2 o 3 tasti), modificandone quindi caratteristiche di funzionamento e configurazione come, per esempio, gli Ingressi/Uscite digitali e la gestione dei tasti del telecomando.  
Anche in questo caso verranno modificati i menù della periferica in oggetto in modo tale da rendere disponibili le modifiche delle sole caratteristiche proprie del terminale RXE.  
Il terminale RXE dispone di due ingressi e due uscite digitali configurabili.
- **< > Scorrimento Oggetti:** Permette di spostarsi al terminale successivo o precedente, senza necessità di chiudere e riaprire la finestra.

### 3.21.2.2. Configurazione Terminale

#### La pagina di Configurazione rende disponibili i seguenti settaggi:

- **Presenza Eventi:** in caso di presenza eventi il terminale ha la possibilità di: far lampeggiare il display, attivare il cicalino (buzzer interno), visualizzare un messaggio di presenza eventi sul display. e/o rendere visibili gli eventi Rapina e Panico normalmente nascosti.
- **Tempo di Visualizzazione Sinottici:** esistono 4 pagine sinottiche visualizzabili ciclicamente con diversi tempi programmabili di permanenza.
- **Fuori Norma EN50131:** Disabilita il timeout indicazioni, le informazioni mostrate dai messaggi in primo piano rimarranno visualizzati fino a che un operatore non confermi la visualizzazione.
- **Visualizzazione Eventi senza Login:** visualizzare la pagina degli eventi importanti e l'accesso alle liste del terminale senza effettuare Login.

- **Time Out Operatore:** Tempo di permanenza operatore dopo inattività tasti, espresso in secondi.
- **Cicalino Timbratura Disabilitato:** Disabilita il Buzzer, al riconoscimento dell'operatore.

### 3.21.2.3. Controllo Accessi Terminale

La finestra di set-up mostra le configurazioni specifiche di un terminale impostato in modalità Controllo Accessi.

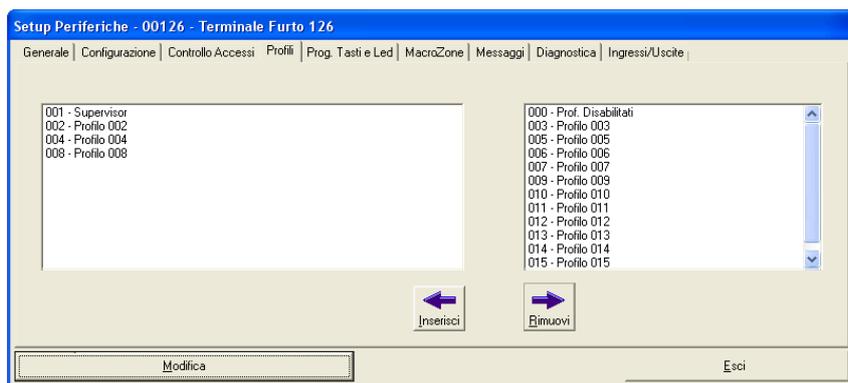
- **Uscita Comando serratura 1/2:** le uscite associate verranno attivate in caso di timbratura valida.
- **Uscita allarme forzatura:** l'uscita selezionata si attiverà in caso di una timbratura non valida o in caso di apertura del varco senza timbratura.
- **Riposo a chiusura porta:** Mette in stato di riposo l'uscita di allarme forzatura in automatico quando l'ingresso Sensore porta torna in stato di riposo (porta chiusa).
- **Tempo per apertura Porta:** tempo massimo in cui la porta deve essere aperta dopo che è avvenuta l'attivazione della serratura 1 o 2. Se la porta resta chiusa, alla scadenza del tempo apertura porta verrà generato l'evento di *Forzatura per Mancanza Apertura*.
- **Tempo per Chiusura Porta:** tempo massimo in cui la porta deve essere chiusa. Se l'*Ingresso sensore porta* non torna a riposo prima della scadenza del *Tempo per chiusura Porta*, verrà generato l'evento di *Forzatura per Mancanza Chiusura*.
- **Ingresso sensore Porta:** associare il contatto magnetico per la gestione del controllo porta. A Impianto Inserito, il sensore porta genera un allarme e potrà essere utilizzato, associato ad una Zona ingresso, in un normale impianto di Antintrusione.
- **Ingresso Pulsante Apertura:** l'allarme dell'ingresso associato genera l'attivazione dell'*uscita Comando Serratura 1/2*.
- **Disabilita Forzature:** disabilita la generazione degli eventi di *Forzatura Porta, Mancanza Apertura, Mancanza Chiusura*.
- **Area Terminale:** indica l'Area logica di partenza degli Operatori che effettuano il login sul terminale.
- **Tempo di Antiritorno Area Terminale:** definisce il tempo, espresso in secondi, entro il quale l'utente non può entrare nell'area in cui è configurato il terminale (Area Terminale)
- **Area Destinazione:** indica l'Area di destinazione degli operatori dopo il Login.

- **Tempo di Antiritorno Area Destinazione:** definisce il tempo, espresso in secondi, entro il quale l'utente non può rientrare nell'area in cui viene spostato dopo la timbratura dell'Area Terminale.
- **Modalità Antipassback:** se abilitata, permette la selezione **HARD e SOFT** Antipassback tra le due aree.

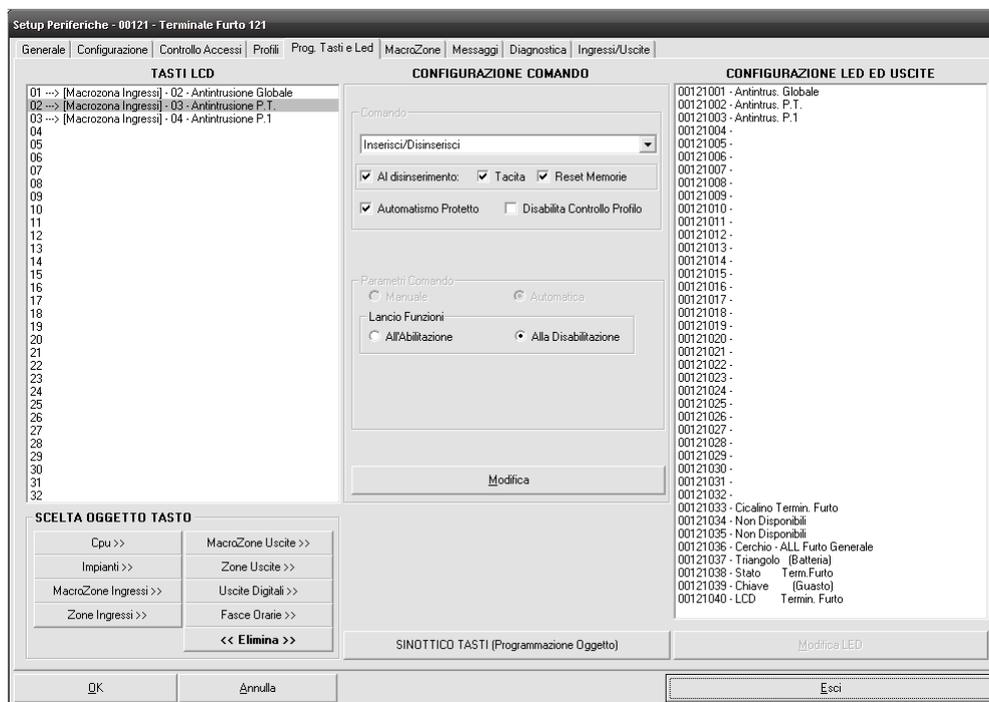
### 3.21.2.4. Profili Terminale

Mostra i Profili Operatore associati al terminale selezionato e ne permette l'inserimento di nuovi o la rimozione dei presenti.

**Nota:** La configurazione Profili/Terminali viene eseguita nel menù Profili/Utenti.



### 3.21.2.5. Prog.Tasti e LED Terminale



**Programmazione Tasti e LED:** è il menù che permette la configurazione dei tasti dei terminali LCD600S.

Nella colonna di sinistra vengono mostrati i 32 tasti disponibili; una volta associato l'oggetto desiderato ( *Zona, Macrozona...* ) sarà possibile selezionare il tipo di Comando che si dovrà eseguire (es: *Inserire/Disinserire, fare Reset memorie, Tacitare uscite...*).

I comandi disponibili sono differenziati e dipendenti dal tipo oggetto selezionato per i 32 tasti e possono essere eseguiti come:

- **Automatismo Protetto:** necessita il riconoscimento dell'operatore sulla tastiera/antenna/radiocomando.
  - **Manuale:** Il comando deve essere eseguito manualmente dall'operatore premendo il tasto.
  - **Automatico:** Il comando verrà eseguito automaticamente al riconoscimento dell'operatore.

**NOTA:** In base alla tipologia di configurazione (*Furto o Controllo Accessi*) del terminale/antenna/ricevitore radio saranno disponibili differenti modalità di esecuzione del comando:

- **Prima dell'apertura della porta:** per la modalità controllo Accessi
- **All'Abilitazione/Disabilitazione:** per la modalità Furto
- **Automatismo non Protetto:** Senza il flag di protezione permette l'esecuzione dei comandi liberamente senza la necessità di riconoscersi sul terminale/antenna/radiocomando semplicemente con la pressione del tasto.
- **Disabilita Controllo Profilo:** Permette di eseguire il comando indipendentemente dal profilo associato all'operatore che si riconosce sul terminale.

Per i terminali configurati come AEI e RXE ci sono parametri aggiuntivi che definiscono le modalità di gestione dei comandi che potranno essere eseguiti solo in modalità Automatica.

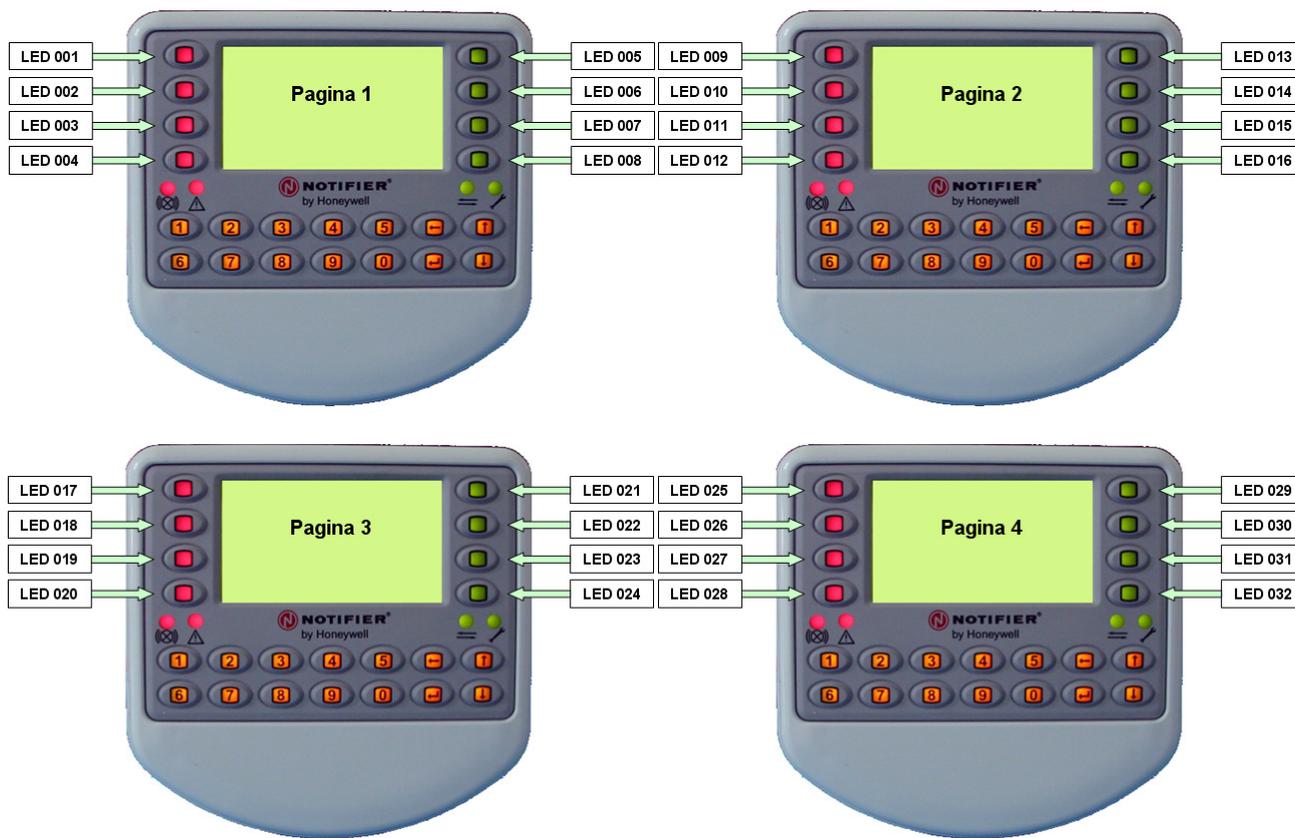
- **AEI:** Permette l'esecuzione di comandi singoli o multipli mantenendo il transponder in posizione di lettura, tutti i led lampeggiano per tre secondi: prima Giallo, poi Rosso, poi Verde. Togliendo il transponder dalla posizione di lettura, in funzione del colore attivo, viene lanciato il comando corrispondente, confermato all'accensione fissa per due secondi del colore.
  - *Lettura 1:* Passaggio e riconoscimento con led di colore Giallo
  - *Lettura 2:* Passaggio e riconoscimento con led di colore Rosso
  - *Lettura 3:* Passaggio e riconoscimento con led di colore Verde
- **RXE:** Permette l'esecuzione di comandi singoli o multipli con la pressione dei Tasti del radiocomando.
  - *TastoTX 1:* Pressione Tasto 1
  - *TastoTX 2:* Pressione Tasto 2
  - *TastoTX 3:* Pressione Tasto 3

Nella colonna di destra vengono mostrati i 32 LED multicolore corrispondenti al tasto della colonna di sinistra.

Una volta selezionate le uscite LED del terminale selezionato è possibile modificarne la descrizione, anche in multiselezione, tramite.

Il Led sarà programmabile dal tasto **Modifica LED** dove sarà possibile associarlo ad una Zona Uscita precedentemente configurata come zona di gestione Sinottici, attraverso la maschera di configurazione Sinottici/Segnalazione aggiuntive della Macrozona/zona a cui il led dovrà riportare lo stato.

Nell'immagine sotto vengono riportate le 4 pagine sinottiche configurabili sui terminali LCD600S:



### 3.21.2.6. MacroZone - Terminale

Visualizza e permette l'associazione o la rimozione di Macrozone associate al terminale selezionato, solo le Macrozone associate infatti saranno soggette ai comandi del terminale selezionato.

**Nota:** la configurazione MacroZone/Terminali viene eseguita nel menù Profili/Utenti.

### 3.21.2.7. Messaggi - Terminale

Permette di selezionare dei messaggi preimpostati, visualizzabili sulle 8 righe del display del Terminale LCD600S.

### 3.21.2.8. Diagnostica - Terminale

Visualizza una finestra indicante dati relativi allo stato di vita del terminale, indicando versione Firmware ed eventuali problemi di comunicazione.

Nello specifico:

- Giorni, ore, minuti e secondi di vita della periferica selezionata
- N° di Restart
- N° di manomissioni
- Tempo Manomissioni
- Errori di trasmissione alla prima richiesta
- Errori di trasmissioni all'ultima richiesta
- Versione

**Nota:** Menù disponibile solo quando si è connessi con la CS600, i contatori vengono resettati ogni volta che viene cancellato il binding della periferica selezionata.

### 3.21.2.9. Ingressi/Uscite- Terminale

Permette la configurazione completa di tutti gli Ingressi e Uscite (fisiche e sinottiche) del Terminale. Vedi par. 3.21.6. *Configurazione di un ingresso digitale* e par. 3.21.7 *Configurazione di un'uscita digitale*.

Se le periferiche sono configurate come AEI o RXE il numero di ingressi e uscite varia a seconda del Tipo Terminale.

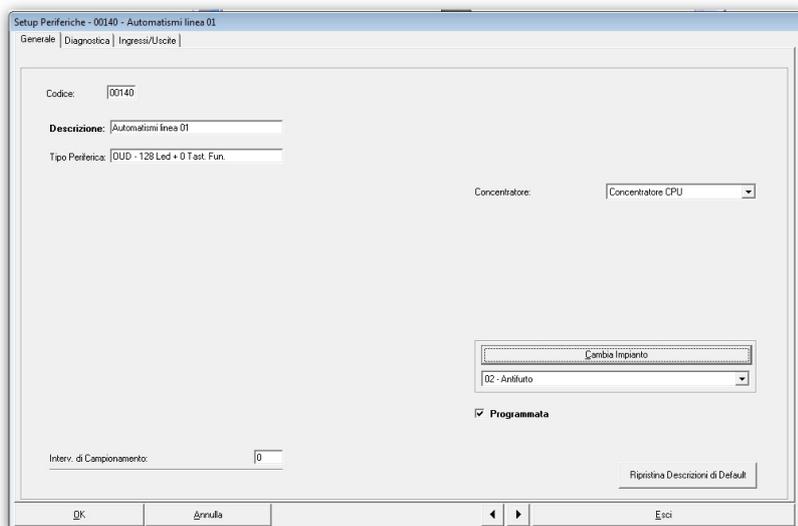
	<i>Ingressi</i>	<i>Uscite</i>	<i>Note</i>
<i>LCD</i>	<i>1</i>	<i>40</i>	<i>33 Uscite liberamente configurabili 7 Uscite di sistema non utilizzabili</i>
<i>AEI</i>	<i>1</i>	<i>5</i>	<i>4 Uscite liberamente configurabili, 1 Uscita di sistema non utilizzabile</i>
<i>RXE</i>	<i>2</i>	<i>2</i>	

### 3.21.3. Automatismi e Azioni

Periferica **AUTOMATISMI**, composta da 128 uscite virtuali, utilizzabili come uscite di controllo o/e azioni per automazioni complesse e/o integrazione con il sistema Euronet.

Ogni uscita virtuale può comandare fino ad un max di 8 Azioni contemporanee, impostate dalle proprietà dell'uscita.

Una volta selezionata la periferica, cliccando sul tasto **AUTOMATISMI** viene mostrata la finestra di setup sotto riportata



Ogni periferica Automatismi viene configurata dalle 3 pagine principali:

- **Generale**
- **Diagnostica**
- **Ingressi/Uscite**

#### 3.21.3.1. Generale

La pagina **Generale** permette di modificare la *descrizione* della periferica selezionata, l'*associazione* ad un Impianto del sistema con *cambia Impianto* e l'associazione ad un *Concentratore*.

**Ripristina descrizioni di default:** riporta tutte le descrizioni delle uscite della periferica selezionata alla descrizione di fabbrica (es: *Uscita 1.01.01*).

**Concentratore** consente di suddividere in modo logico il posizionamento della periferica all'interno di un impianto. Questo permette di non compromettere i piani d'inserimento, gli eventi e gli allarmi di altri impianti in caso di anomalie/manomissioni, ma viene limitato solo alla porzione d'impianto a cui fa parte il concentratore.

< > **Scorrimento Oggetti:** Permette di spostarsi alla periferica Automatismi della linea successiva o precedente, senza necessita di chiudere e riaprire la finestra.

**Nota:** Il flag **“Programmata”** sempre abilitato di default identificherà la periferica di colore verde, permettendo così la configurazione delle uscite nel menù di programmazione.

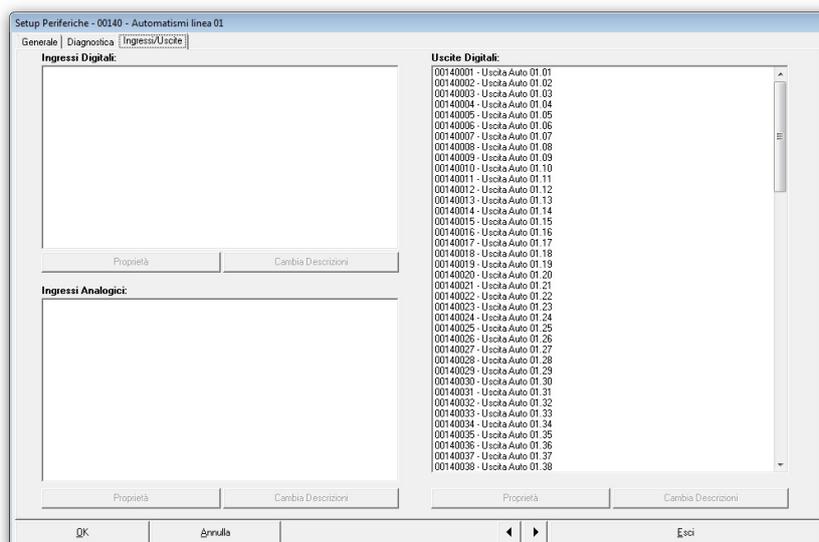
### 3.21.3.2. Diagnostica

La pagina **Diagnostica** mostra uno storico del tempo di attività della periferica selezionata, versione di firmware, numero di restart e altre informazioni utili al monitoraggio delle periferiche di campo.

**N.B.:** Menù disponibile solo quando si è connessi con la CS600.

### 3.21.3.3. Ingressi/Uscite

Sotto viene mostrata la finestra di gestione **Ingressi/Uscite** di una periferica tipo AUTOMATISMI, il tasto **Proprietà** permette la configurazione specifica di ogni singola Uscita appartenente alla periferica selezionata.



### 3.21.4. Configurazione di un'uscita “Automatismo”

Le uscite Automatismo sono degli oggetti virtuali a cui non è possibile collegare per esempio un relè. Queste vengono utilizzate dal sistema CS600 per effettuare delle automazioni logiche (AND/OR/NOT) senza ricorrere alla movimentazione fisica di apparati come sirene, combinatori, lampeggianti ecc ecc.

#### Configurazioni disponibili di un'uscita digitale:

- **Descrizione.** Modifica la descrizione dell'uscita selezionato.
- **Descrizione come zona appartenenza:** se selezionato permette all'uscita digitale di ereditare la descrizione della Zona Uscite a cui è associata.
- **Zona Associata:** Permette di selezionare la Zona Uscite a cui associare logicamente l'uscita digitale.

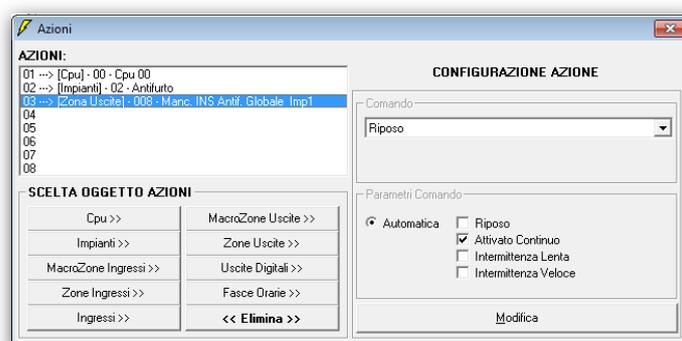
- **Tipo Attivazione:** definisce la modalità di attivazione dell'uscita che di Default viene gestita in base alla programmazione di zona, altrimenti è possibile selezionare; Attivata (attiva fissa), Lampeggiante Lenta (ON/OFF Freq. = 1 Hz), Lampeggiante Veloce (ON/OFF Freq. = 2 Hz).
  - **Setup Uscite:**
    - o **Tempo di OND:** Espresso in secondi definisce il tempo di attivazione continua dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscita a cui è associata. (es: se l'uscita viene utilizzata per comandare una sirena Ext il tempo da impostare è 180 sec).
    - o **Tempo di ritardo di attivazione:** espresso in secondi definisce il tempo di ritardo che l'uscita dovrà considerare prima di attivarsi a fronte di un comando diretto o dalla Zona Uscita a cui è associata. (es: se l'uscita viene utilizzata per comandare una un ponte radio/combinatore telefonico è possibile con il ritardo evitare di mandare segnalazioni remote in caso di errore di gestione dell'impianto).
    - o **Tempo di puls. Veloce (PUV):** Espresso in secondi definisce il tempo di attivazione pulsante veloce (ON/OFF Freq. = 2 Hz) dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscita a cui è associata. (es: utilizzata per comandare una sirena INTERNA per avere il suono l'attivazione intermittente per il tempo impostato).
    - o **Tempo di puls. Lento (PUL):** Espresso in secondi definisce il tempo di attivazione pulsante lento (ON/OFF Freq. = 1 Hz) dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscita a cui è associata. (es: utilizzata per comandare un lampeggiante di segnalazione per il tempo impostato).
  - **Cicli Attivazioni:**
    - o **Tempo di ON:** Espresso in secondi definisce il tempo che l'uscita rimarrà attivata all'interno del tempo definito in "Tempo di OND".
    - o **Tempo di OFF:** Espresso in secondi definisce il tempo che l'uscita rimarrà disattivata all'interno del tempo definito in "Tempo di OND".
- Nota:** Sono parametri legati tra di loro che definiscono dei cicli di attivazione e riposo dell'uscita digitale da eseguire all'interno del tempo totale dichiarato nel "Tempo di OND".  
(es Tempo di OND =180 sec, Tempo di ON=30 sec, Tempo di OFF=30 sec, questo significa che l'uscita all'interno dei 180 sec eseguirà nr°3 cicli di ON e nr°3 cicli di OFF.
- **Abilita Autoreset:** Con il flag disabilitato definisce se l'uscita dovrà arrivare alla scadenza del tempo di OND/PUV/PUL con un unico comando di attivazione diretto o dalla Zona Uscita a cui è associata. Con il flag abilitato l'uscita ricaricherà il tempo di OND/PUV/PUL ogni volta che viene rigenerata la causa dell'attivazione diretta o della zona uscita associata.
  - **Sicurezza Positiva: Parametro non utilizzato**
  - **Genera Eventi:** abilita la generazione degli eventi dell'oggetto selezionato. (*default disabilitato*).
  - **Inversione funzionamento:** inverte il funzionamento logico dell'uscita digitale, se Attiva = OFF se Disattiva = ON.
  - **Invia a Cpu di rete:** parametro da configurare per l'integrazione con il sistema Euronet. Invia i cambi di stato delle oggetto all'indirizzo della cpu di rete configurata nelle proprietà della centrale.
  - **Usato In:** Visualizza una finestra di controllo che riporta gli elementi del sistema che comandano o subiscono l'azione dell'oggetto selezionato semplificando la ricerca a posteriori.
  - **Programmazione:** configurazione completa delle attivazioni/segnalazione sinottiche/comandi generati dell'uscita digitale. Vedi par. **3.17.3. Programmazione Impianto**
  - **Azioni:** vedi paragrafo successivo
  - **<> Scorrimento Oggetti:** Permette di spostarsi all'uscita successiva o precedente, senza necessita di chiudere e riaprire la finestra.

### 3.21.5. Configurazione di un uscita “Azione”

Le uscite Azioni sono delle configurazioni avanzate delle uscite Automatismo.

Queste permettono di gestire in modo simultaneo o differenziato una serie di “Azioni” con il variare di stato ( Riposo, Attivata Continua, Intermittenza Lenta, Intermittenza Veloce) dell’uscita Automatismo associata.

Le Azioni disponibili per singola uscita Automatismo sono max.8, e possono essere eseguite su qualsiasi oggetto della CS600 (CPU, MacroZone, SottoZone, Ingressi/Uscite digitali, Fasce Orarie ecc ecc.).



Le configurazioni disponibili sono

**Scelta dell’oggetto Azioni:** permette di selezionare quale oggetto può essere comandato e quindi subire l’azione che verrà configurata.

**Parametri Comando:** definisce in base allo stato dell’uscita Automatismo associata quando dovrà essere eseguito il comando dell’Azione.

**Comando:** Specifica il comando che verrà eseguito sull’oggetto selezionato nella finestra AZIONI e i comandi disponibili sono:

- **Cpu>>**
  - o Tacita
  - o Reset Memorie
- **Impianti>>**
  - o Tacita
  - o Reset Memorie
- **MacroZone – ZoneIngressi e Ingressi digitali>>**
  - o Tacita
  - o Reset memorie
  - o Inserisci/Disinserisci\*\*
  - o Inserisci Forzato/Disinserisci\*\*
  - o Inserisci Forzato Test/Disinserisci\*\*
  - o Inserisci
  - o Inserisci forzato
  - o Inserisci forzato Test
  - o Disinserisci\*\*

\*\* : Il comando Disinserisci permette di eseguire ulteriori funzioni legate sulla MacroZona , Zona Ingressi associata, come:

- Tacita
- Reset Memorie

- **MacroZone – ZoneUscite e Uscite Digitali>>**
  - o Attiva/Riposo
  - o Attiva
  - o Riposo
  - o Ond/Pul/Puv/Riposo

- **Fasce Orarie>>**
  - o Attiva/Riposo
  - o Attiva
  - o Riposo
  - o Posticipa

### 3.21.6. Configurazione di un ingresso digitale

Una volta selezionato un ingresso digitale appartenente ad una periferica, cliccando sul tasto **Proprietà** viene mostrata la finestra di setup sotto riportata:

The screenshot shows a software window titled "Proprietà Ingresso Digitale 0010101 Sensore 1". It contains the following fields and options:

- Setup:**
  - Indirizzo: 0010101, Zona: 008
  - Indirizzo CID: 1
  - Codice CID: 130
  - Descrizione: Sensore 1
  - Zona Associata: 008 - Sensori
  - Da Salvare nel Registro Eventi 50131:
- Tipo Ingresso:**
  - Tipo Ingresso: Normale
  - Etichettatura: Antintrusione
  - Normalmente Aperto:
  - Tecnologico:
  - Singolo Bilanciamento:
  - Doppio Bilanciamento:
  - Quadruplo Bilanciamento:
  - Esclusione Manomissione:
  - Sensore Interno:
- Setup Ingressi:**
  - Ritardo Inserimento: 0
  - Ritardo Allarme: 0
  - AutoEsclusione:
  - Reinserimento Ingresso AutoEscluso:
  - Rilevazioni per AutoEsclusione: 99
  - Tempo Rilevazioni per AutoEsclusione: 0
  - Numero Rilevazioni per Integrazione: 0
  - Tempo Integrazione Numero Rilevazioni: 0
  - Tempo Integrazione Singola Rilevazione: 0
  - Abilita Allarme per Singola Rilevazione:
  - Rigenera Allarmi:
  - Genera Eventi:  Riposo:  Guasto:
  - Allarme:  Mascheramento/Anomalia:
  - Taglio:  Corte:
- Ingresso Per Allarme:**
  - Ingresso Per Allarme: <Nessun Elemento>
  - Tempo: 0

Buttons at the bottom: Programmazione, Usato In..., Modifica, Esci.

#### Configurazioni disponibili di un ingresso digitale:

- **Descrizione.** Modifica la descrizione dell'ingresso selezionato.
- **Zona Associata:** associazione logica obbligatoria di un ingresso digitale ad una Zona Ingressi.
- **Tipo Ingresso:** permette di selezionare se l'ingresso è di tipo "Normale" (utilizzabile per contatti magnetici, volumetrici....) di Tipo "Tapparella" (impiegabile per contatti veloci tipo tapparella in associazione ai parametri Tempo e Numero rilevazioni e ritardo di allarme) oppure di Tipo "Contatore" (utilizzabile per campionare il numero di rivelazioni prima di eseguire una determinata azione, in associazione ai parametri Numero rilevazioni).
- **Etichettatura:** l'ingresso assumerà comportamenti differenti di funzionamento a seconda del tipo scelto (rif 6.2).
- **Selezione Bilanciamento:** gli ingressi di default vengono configurati come Quadruplo-bilanciamento, ma possono essere variati selezionando la casella specifica.

Le resistenze per la configurazione a quadruplo bilanciamento sono:

- 1KΩ fine linea
- 1,2 KΩ Mascheramento
- 6,8 KΩ Guasto
- 2,2 KΩ Allarme

La configurazione software di default (quadruplo bilanciamento) permette anche la gestione del doppio bilanciamento installando solo le resistenze di fine linea (1K $\Omega$ ) in serie e quella di allarme (2,2K $\Omega$ ) in parallelo al contatto.

In questo modo si avranno solo le segnalazioni di Allarme, Riposo, Corto e Taglio.

Vedi approfondimento per l'etichetta di funzionamento al **Cap.6 Tipologia Ingressi Digitali**.

- **Sensore Interno:** La funzionalità di questo parametro è legata alla presenza nella stessa zona di almeno un ingresso con impostato il ritardo dall'allarme.

**Esempio:**

L'ingresso **A** ha il parametro sensore interno abilitato, l'ingresso **B** ha il ritardo d'allarme.

Se l'ingresso **A** rileva un allarme prima di **B**, esegue immediatamente la chiamata d'allarme.

Se l'ingresso **A** rileva un allarme dopo **B**, esegue la chiamata d'allarme contemporaneamente a **B**.

Se nella zona esistono più ingressi con impostato un ritardo dall'allarme, la chiamata d'allarme di **A** viene eseguita contemporaneamente alla chiamata del primo ingresso in allarme del quale scade il ritardo.

Per un funzionamento efficace l'ingresso **A** non deve aver impostato nessun ritardo.

- **Setup Ingressi** - tempistiche di comportamento dell'ingresso digitale:
  - o **Ritardo di Inserimento:** Immette un ritardo nell'inserimento dell'ingresso espresso in secondi. (default 0)
  - o **Ritardo Allarme:** Immette un ritardo nella generazione della condizione di allarme dell'ingresso espresso in secondi. (default 0)
  - o **Autoesclusione:** Permette l'autoesclusione automatica degli ingressi in allarme al momento dell'inserimento della Zona ( a cui sono associati) effettuata da LCD600 o attraverso fascia Oraria.
  - o **Reinserimento Ingresso AutoEscluso:** permette l'inclusione automatica dell' ingresso escluso.
  - o **Rivelazioni per Autoesclusione:** Valore che indica dopo quante rilevazioni ad impianto inserito l'ingresso deve autoescludersi. (default 99 = mai)
  - o **Tempo Rivelazione per AutoEsclusione:** Valore espresso in secondi che indica entro quanto tempo devono essere effettuate il numero rilevazioni configurate nel parametro precedente. (default 0)
  - o **Numero Rivelazioni per Integrazione:** Valore che indica quante rilevazioni l'ingresso deve effettuare prima di attivare le programmazioni di allarme.
  - o **Tempo Integrazione Numero Rivelazioni:** Valore espresso in secondi entro il quale il Numero di rivelazioni per integrazioni devono verificarsi.
  - o **Tempo Integrazione Singola Rivelazione:** Valore espresso in secondi che indica per quanto tempo deve rimanere presente la rilevazione per essere considerata valida e generare le programmazioni di allarme

**Nota:** Gli ultimi 3 parametri possono essere tutti configurati per gestire delle situazioni con ingressi posizionati in ambienti con condizioni molto variabili per evitare falsi allarmi.

- **Abilita Allarme per Singola Rivelazione:** modifica il funzionamento dei parametri "Numero Rivelazioni Per Integrazione", "Tempo Integrazione Numero Rivelazioni", "Tempo Integrazione Singola Rivelazione".

Quando è abilitato, la centrale :

- o Non considera il "Tempo Integrazione Singola Rivelazione" ma utilizza quello Hardware della periferica IND/ALI (= **250 ms**).
- o Nel caso di allarme continuo di un ingresso (*ovvero rimane costantemente in allarme senza tornare a mai riposo*) usa il "Tempo Integrazione Singola Rivelazione" invece del "Tempo Integrazione Numero Rivelazioni".

ESEMPIO:

- Numero Rivelazioni Per Integrazione                   **3**
- Tempo Integrazione Numero Rivelazioni               **10 sec**
- Tempo Integrazione Singola Rilevazione               **2 sec**

**L'ingresso** genera la condizione di allarme quando:

**A. senza Flag:**

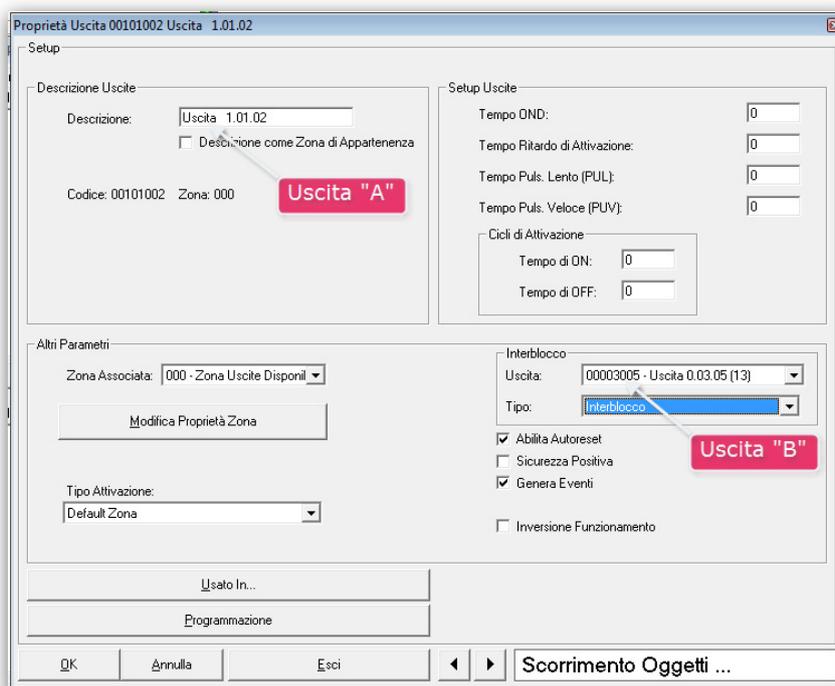
1. dopo che ha generato **3** allarmi/aperture nei **10 sec** e per ogni allarme/apertura è stato in quella condizione per almeno **2 sec**.
2. se l'ingresso rimane costantemente in allarme senza tornare a mai riposo per almeno 10 s

**B. con Flag:**

1. dopo che ha generato **3** allarmi/aperture nei **10 sec** e per ogni allarme/apertura è stato in quella condizione per almeno **250 ms**
2. se l'ingresso rimane costantemente in allarme senza tornare a mai riposo per almeno 2 s

- **Rigenera Allarmi:** permette all'ingresso di rigenerare la condizione di allarme (quindi anche le attivazioni di sirene e segnalazioni varie) quando passa dallo stato di allarme a riposo e poi di nuovo in allarme.  
**NB:** questa condizione può essere generata anche dopo un tentativo di reset memorie di un ingresso ancora in allarme (es: porta/finestra aperta).
- **Genera Eventi:** definisce quali eventi genererà l'ingresso e che verranno mostrati sul display LCD600S e nel DataBase eventi della CS600.
- **Ingresso per allarme:** se viene configurato questo parametro l'ingresso selezionato andrà in allarme solo se l'ingresso associato come per allarme sarà già nella condizione di allarme.
- **Programmazione:** configurazione completa delle attivazioni/segnalazione sinottiche/comandi generati dell'ingresso digitale. Vedi par. **3.17.3. Programmazione Impianto.**

### 3.21.7. Configurazione di un'uscita digitale



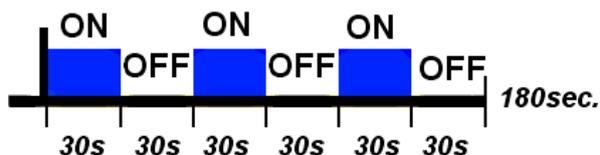
#### Configurazioni disponibili di un'uscita digitale:

- **Descrizione.** Modifica la descrizione dell'uscita selezionato.
- **Descrizione come zona appartenenza:** se selezionato permette all'uscita digitale di ereditare la descrizione della Zona Uscite a cui è associata.
- **Zona Associata:** Permette di selezionare la Zona Uscite a cui associare logicamente l'uscita digitale.
- **Tipo Attivazione:** definisce la modalità di attivazione dell'uscita che di Default viene gestita in base alla programmazione di zona, altrimenti è possibile selezionare; Attivata (attiva fissa), Lampeggiante Lenta (ON/OFF Freq. = 1 Hz), Lampeggiante Veloce (ON/OFF Freq. = 2 Hz).
- **Setup Uscite:**
  - o **Tempo di OND:** Espresso in secondi definisce il tempo di attivazione continua dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscite a cui è associata. (es: se l'uscita viene utilizzata per comandare una sirena Ext il tempo da impostare è 180 sec).
  - o **Tempo di ritardo di attivazione:** espresso in secondi definisce il tempo di ritardo che l'uscita dovrà considerare prima di attivarsi a fronte di un comando diretto o dalla Zona Uscite a cui è associata. (es: se l'uscita viene utilizzata per comandare una un ponte radio/combinatore telefonico è possibile con il ritardo evitare di mandare segnalazioni remote in caso di errore di gestione dell'impianto).
  - o **Tempo di puls. Veloce (PUV):** Espresso in secondi definisce il tempo di attivazione pulsante veloce (ON/OFF Freq. = 2 Hz) dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscite a cui è associata. (es: utilizzata per comandare una sirena INTERNA per avere il suono l'attivazione intermittente per il tempo impostato).
  - o **Tempo di puls. Lento (PUL):** Espresso in secondi definisce il tempo di attivazione pulsante lento (ON/OFF Freq. = 1 Hz) dell'uscita dopo che è stata attivata da un comando diretto o dalla Zona Uscite a cui è associata. (es: utilizzata per comandare un lampeggiante di segnalazione per il tempo impostato).
- **Cicli Attivazioni:**

- **Tempo di ON:** Espresso in secondi definisce il tempo che l'uscita rimarrà attivata all'interno del tempo definito in "Tempo di OND".
- **Tempo di OFF:** Espresso in secondi definisce il tempo che l'uscita rimarrà disattivata all'interno del tempo definito in "Tempo di OND".

**Nota:** Sono parametri legati tra di loro che definiscono dei cicli di attivazione e riposo dell'uscita digitale da eseguire all'interno del tempo totale dichiarato nel "Tempo di OND".

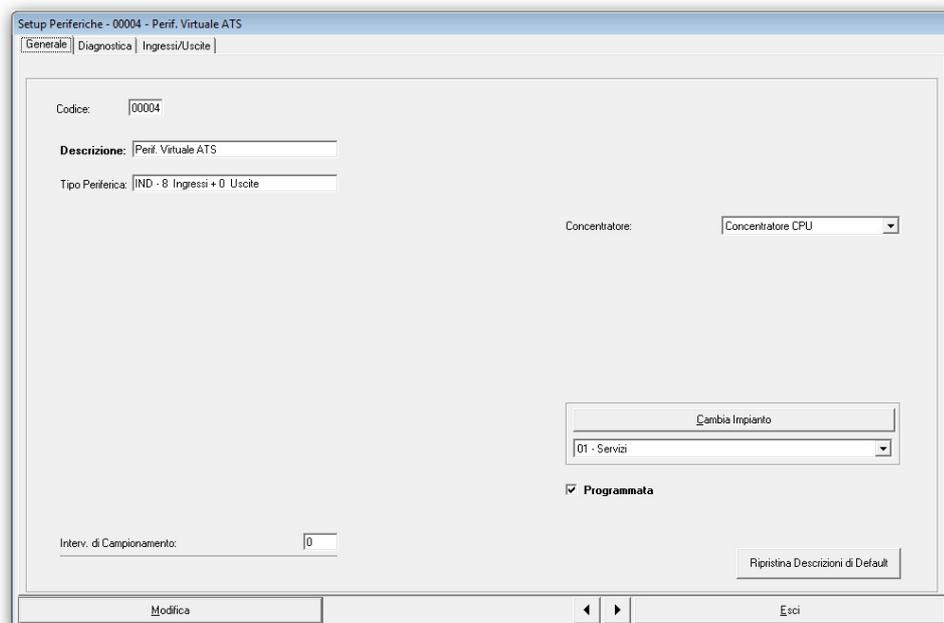
(es Tempo di OND =180 sec, Tempo di ON=30 sec, Tempo di OFF=30 sec, questo significa che l'uscita all'interno dei 180 sec eseguirà nr°3 cicli di ON e nr°3 cicli di OFF.



- **Interblocco:**
  - **Tipo "Interblocco":** l'uscita associata B non può attivarsi fino a quando l'uscita A che si sta configurando è attiva.  
*Esempio:* Se l'uscita A è attivata, l'uscita B non può attivarsi; se l'uscita B è attivata, l'uscita A non può attivarsi.
  - **Tipo "Interblocco scambio":** Quando l'uscita B associata è attivata, l'attivazione dell'uscita A che si sta configurando provoca automaticamente il riposo dell'uscita associata B.  
*Esempio:* Se l'uscita A è attivata, l'attivazione dell'uscita B provoca il riposo dell'uscita A; se l'uscita B è attivata, l'attivazione dell'uscita A provoca il riposo dell'uscita B.
- **Abilita Autoreset:** Con il flag disabilitato definisce se l'uscita dovrà arrivare alla scadenza del tempo di OND/PUV/PUL con un unico comando di attivazione diretto o dalla Zona Uscita a cui è associata. Con il flag abilitato l'uscita ricaricherà il tempo di OND/PUV/PUL ogni volta che viene rigenerata la causa dell'attivazione diretta o della zona uscita associata.
- **Sicurezza positiva:** se abilitata, mantiene l'uscita normalmente eccitata per un maggiore livello di sicurezza. Non utilizzare in abbinato alla **Inversione Funzionamento**.
- **Inversione Funzionamento:** inverte il funzionamento logico dell'uscita digitale, se Attiva = OFF se Disattiva = ON. Non utilizzare in abbinato a **Sicurezza Positiva**.
- **Genera eventi:** abilita la generazione degli eventi dell'oggetto selezionato. (*default abilitato*)
- **Programmazione:** configurazione completa delle attivazioni/segnalazione sinottiche/comandi generati dell'uscita digitale. Vedi par. **3.17.3. Programmazione Impianto**.
- **<> Scorrimento Oggetti:** Permette di spostarsi all'uscita successiva o precedente, senza necessita di chiudere e riaprire la finestra.

### 3.21.8. PERIFERICA SERV

Periferica **SERV**, comprende gli ingressi di segnalazione e stato di tutti i dispositivi di comunicazione della CS600 verso fonti esterne (telefono, ricevitori digitali computer ecc. ecc.) e la segnalazione di allarmi speciali come Costrizione e blocco tastiera per PIN errati.



Ogni periferica Serv viene configurata dalle 3 pagine principali:

- **Generale**
- **Diagnostica**
- **Ingressi/Uscite**

### 3.21.8.1. Generale

La pagina **Generale** permette di modificare la *descrizione* della periferica selezionata, l'*associazione* ad un Impianto del sistema con *cambia Impianto* e l'associazione ad un *Concentratore*.

**Ripristina descrizioni di default:** riporta tutte le descrizioni delle uscite della periferica selezionata alla descrizione di fabbrica (*es: Stato CID, Stato Modem ecc. ecc.*).

**Concentratore** consente di suddividere in modo logico il posizionamento della periferica all'interno di un impianto. Questo permette di non compromettere i piani d'inserimento, gli eventi e gli allarmi di altri impianti in caso di anomalie/manomissioni, ma viene limitato solo alla porzione d'impianto a cui fa parte il concentratore.

< > **Scorrimento Oggetti:** Permette di spostarsi alla periferica successiva o precedente, senza necessita di chiudere e riaprire la finestra.

**Nota:** Il flag "**Programmata**" sempre abilitato di default identificherà la periferica di colore verde, permettendo così la configurazione delle uscite nel menù di programmazione.

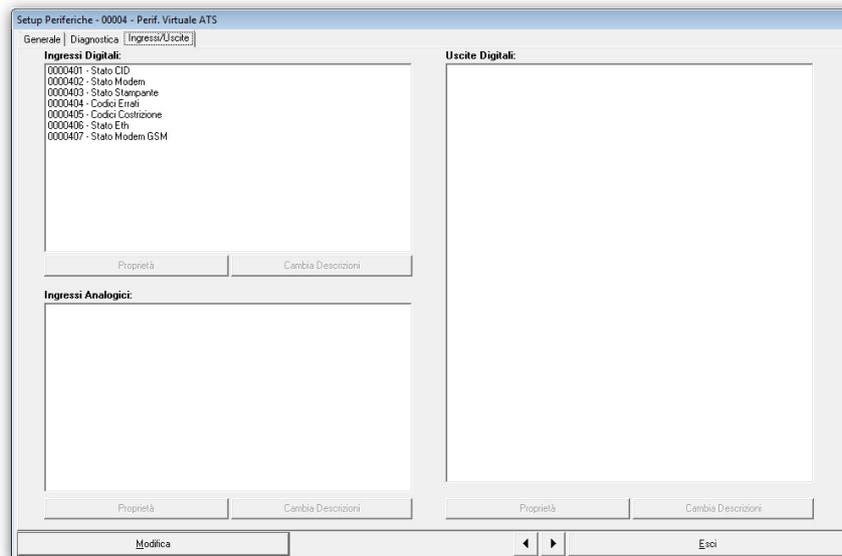
### 3.21.8.2. Diagnostica

La pagina **Diagnostica** mostra uno storico del tempo di attività della periferica selezionata, versione di firmware, numero di restart e altre informazioni utili al monitoraggio delle periferiche di campo.

**N.B.:** Menù disponibile solo quando si è connessi con la CS600.

### 3.21.8.3. Ingressi/Uscite

Sotto viene mostrata la finestra di gestione **Ingressi/Uscite** di una periferica tipo AUTOMATISMI, il tasto **Proprietà** permette la configurazione specifica di ogni singola Uscita appartenente alla periferica selezionata.



Gli ingressi contenuti in questa periferica hanno i parametri di configurazione fissi, ma possono essere solo associati e/o spostati in zone Logiche differenti.

- **Stato CID:** verifica la presenza della linea PSTN e lo stato del modulo M-contact-ID nei confronti della CS600
- **Stato Modem:** verifica lo stato del modem esterno seriale collegato sulla JP20
- **Stato Stampante:** verifica lo stato della stampante seriale collegata sulla JP20
- **Codici Errati:** Genera una segnalazione di Manomissione /Tamper nella condizione in cui vengono inseriti PIN errati in base alla configurazione nella proprietà della centrale CS600.
- **Codici Costrizioni:** Genera un allarme di tipo Rapina se attivato alla combinazione del PIN + nr identificativo costrizione.
- **Stato ETH:** Verifica la presenza della portante di rete sulla porta ETH JP18
- **Stato Modem GSM:** Verifica la copertura del segnale GSM

### 3.21.9. PERIFERICA MAB

#### 3.21.9.1. Generale

La pagina **Generale** permette di modificare la *descrizione* della periferica selezionata, l'*associazione* ad un Impianto del sistema con *cambia Impianto* e l'*associazione* ad un *Concentratore*.

**Ripristina descrizioni di default:** riporta tutte le descrizioni delle uscite della periferica selezionata alla descrizione di fabbrica (*es: Tamper Centrale, F002/RS485L1-L2 CPU ecc. ecc.*).

**Concentratore** consente di suddividere in modo logico il posizionamento della periferica all'interno di un impianto. Questo permette di non compromettere i piani d'inserimento, gli eventi e gli allarmi di altri impianti in caso di anomalie/manomissioni, ma viene limitato solo alla porzione d'impianto a cui fa parte il concentratore.

<> **Scorrimento Oggetti:** Permette di spostarsi alla periferica successiva o precedente, senza necessita di chiudere e riaprire la finestra.

**Nota:** Il flag "**Programmata**" sempre abilitato di default identificherà la periferica di colore verde, permettendo così la configurazione delle uscite nel menù di programmazione.

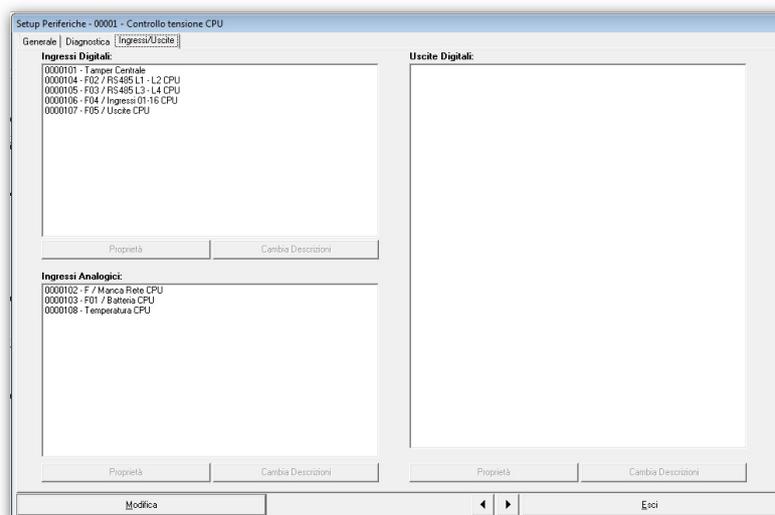
### 3.21.9.2. Diagnostica

La pagina **Diagnostica** mostra uno storico del tempo di attività della periferica selezionata, versione di firmware, numero di restart e altre informazioni utili al monitoraggio delle periferiche di campo.

**N.B.:** Menù disponibile solo quando si è connessi con la CS600.

### 3.21.9.3. Ingressi/Uscite

Sotto viene mostrata la finestra di gestione **Ingressi/Uscite** di una periferica tipo AUTOMATISMI, il tasto **Proprietà** permette la configurazione specifica di ogni singola Uscita appartenente alla periferica selezionata.



Gli ingressi analogici contenuti in questa periferica hanno parametri di configurazione fissi, ma possono essere solo associati e/o spostati in zone Logiche differenti.

Gli ingressi Digitali invece hanno le parametrizzazioni delle integrazioni sugli allarmi abilitate.

#### **INGRESSI DIGITALI**

- **Tamper Centrale:** Si riferisce all'ingresso della morsettiera JP7
- **F02 / RS485 L1 - L2 CPU:** Fusibile a protezione dell'integrità delle linee RS485 1 e 2
- **F03 / RS485 L1 - L2 CPU:** Fusibile a protezione dell'integrità delle linee RS485 1 e 2
- **F04 / Ingressi 01-16 CPU:** Fusibile a protezione dell'integrità dei 16 ingressi delle CS600
- **F05 / Uscite CPU:** Fusibile a protezione dell'integrità delle uscite della CS600

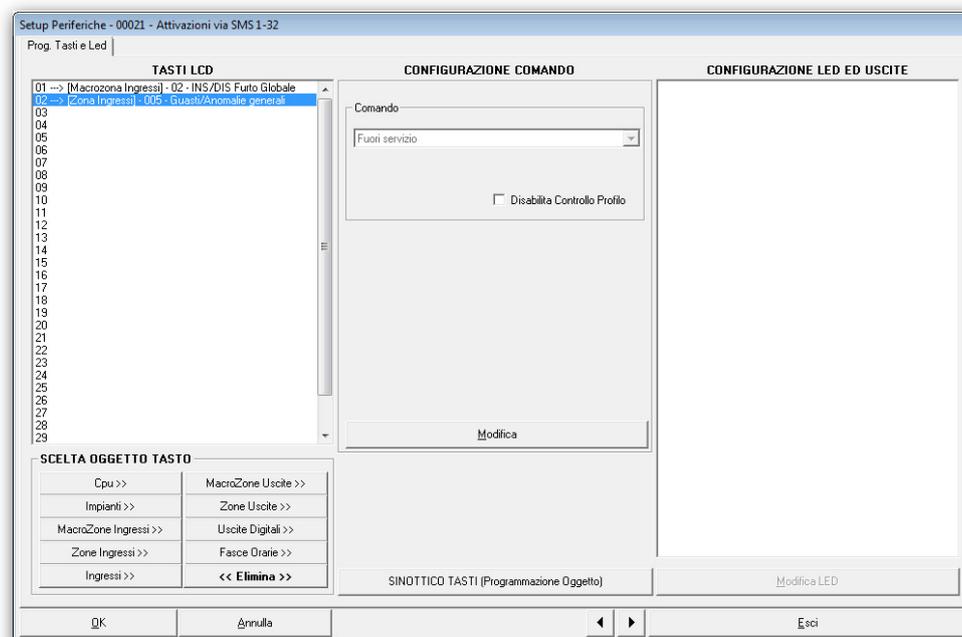
#### **INGRESSI ANALOGICI**

- **F / Manca Rete CPU:** Ingresso Integrato a controllo dell'alimentazione della CS600
- **F01 / Batteria CPU:** Fusibile a protezione e verifica stato Batteria CS600
- **Temperatura CPU:** Ingresso Integrato a controllo della temperatura della CS600

### 3.21.10. PERIFERICA LCV

La periferica LCV viene utilizzata dalla CS600 come terminale virtuale di configurazione dei possibili comandi eseguibili mediante SMS da apparati mobili (telefonini, palmari ecc).

E' possibile attraverso la configurazione della periferica virtuale LCV (dalla versione Firmware CS600 vs 7.07 o sup) inviare SMS alla CS600 per eseguire dei comandi (es Inserimento/Disinserimento Macrozona, Aperture cancello, Accensione Luci .....).



I comandi disponibili attraverso SMS sono nr°32 e possono essere lanciati solo da un operatore abilitato e presente in centrale nella condizione di In Servizio.

Le proprietà della tastiera virtuale LCV 21, sono limitate alla configurazione "Prog. Tasti e Led".

Nella programmazione "Tasti e Led" si creano le associazioni ai tasti virtuali disponibili (da 1 a 32) dei tipo "comando" che si vuole impartire tramite SMS.

Il sistema controlla il PIN operatore contenuto nel test dell'SMS, occorre quindi associare i PROFILI alla tastiera virtuale LCV 21 e anche alle Macrozone che si vorranno gestire.

La sintassi corretta dell'SMS per eseguire un comando è la seguente:

- **PIN operatore (composto da 6 cifre)** [spazio] **n°comando (nr°tasto LCV21)** - 22222 1

Attraverso l'invio di un SMS è possibile eseguire più comandi nella centrale CS600.

Questo è possibile aggiungendo dopo il comando un [punto] e il numero del comando successivo da eseguire.

La sintassi del messaggio è la seguente:

- **PIN operatore (composto da 6 cifre)** [spazio] **n°comando**[punto]**n°comando (nr°tasto LCV21)** - 22222 1.5

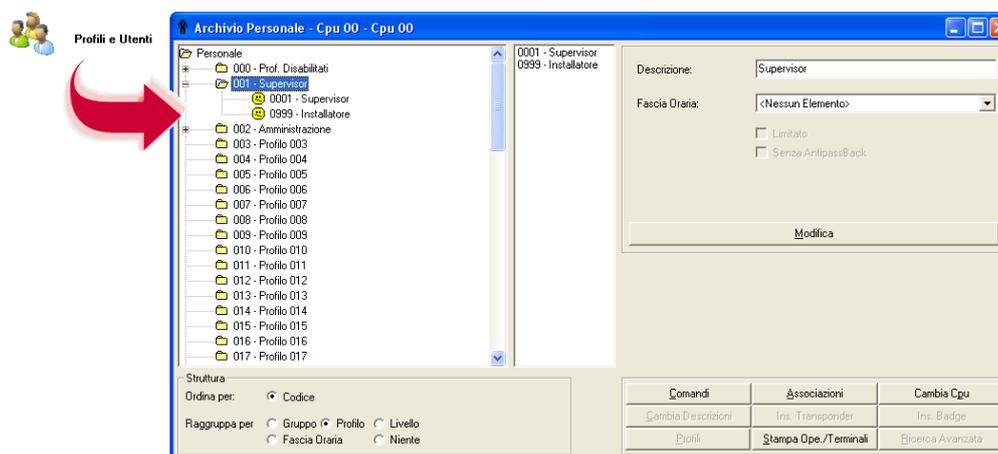
**Nota:** Per avere un riscontro sull'esito dei comandi, si consiglia di configurare le opportune chiamate remote, così da avere un feedback sul comando impartito.

Ad esempio se comandiamo un Inserimento di Macrozona verso la Centrale, sarà opportuno configurare le chiamate remote in modo tale da poter ricevere, lo stato di INS/DIS della Macrozona comandata.

## 3.22. Profili, Operatori e Gruppi

Permette la configurazione e gestione dei codici Utente, Profili, Gruppi e Livelli degli operatori della CS600.

Gli operatori della CS600 sono il personale che utilizza Pin/Tessera/Radiocomando per accedere all'impianto o eseguire automazioni attraverso le periferiche del sistema. (LCD, Antenne ....)



La divisione degli operatori è strutturata in questo modo:

- **Gruppo:** suddivisione Logica senza associazioni (*es Impiegati, Magazzinieri, Dipendenti...*)
- **Livello:** modalità di funzionamento sugli oggetti che compongono il sistema (*es cambio PIN, comandi da tastiera, reset memorie....*)
- **Profilo:** Insieme di autorizzazioni legate alle funzionalità dell'operatore e identificano su quali oggetti che compongono il sistema hanno la possibilità di operare.
- **Operatore:** Identificano il personale che tramite Pin, Tessere, Radiocomandi, interagiscono con il sistema.

L'apertura del menù carica in visualizzazione tutti i 1000 operatori disponibili suddivisi per Profilo/Gruppo/Livello/Fascia Oraria/Niente ovvero elenco completo senza raggruppamenti.

**Nota:** La connessione alla centrale (se mantenuta a grado 3 di sicurezza) per configurare gli operatori deve essere realizzata da un utente **Supervisor** e non da un utente **Installatore**.

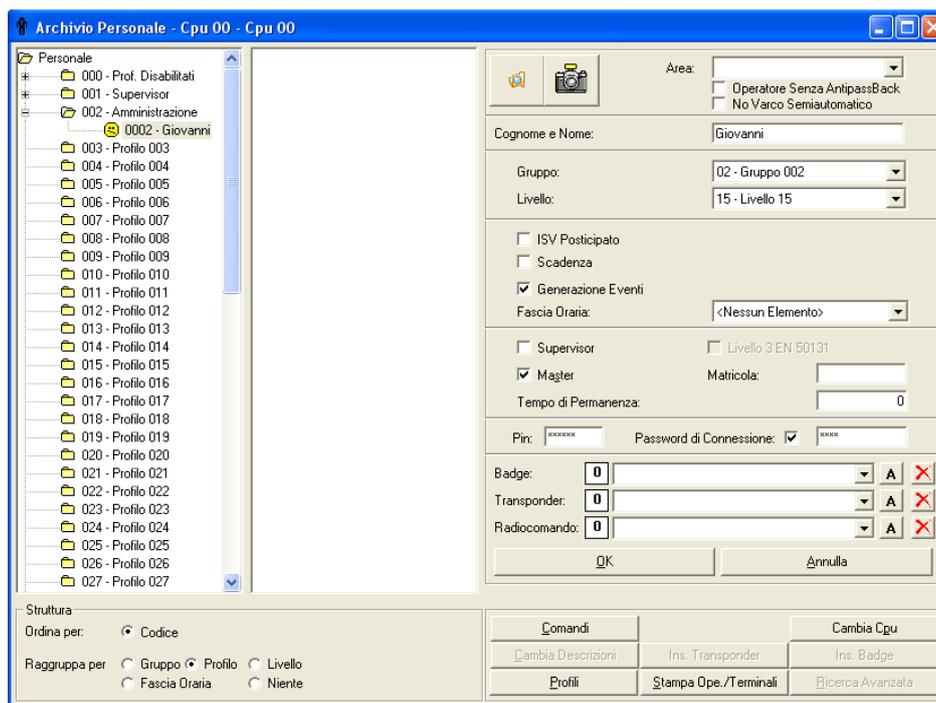
### 3.22.1. Operatori

Identificano il personale che tramite Pin, Tessere, Radiocomandi, interagisce con il sistema attraverso i dispositivi di campo ( LCD600, AEI-485, RXE...).

Dalla finestra **Archivio Personale** selezionando un operatore viene aperta sulla destra la maschera con tutte le parametrizzazioni degli utenti.

Gli operatori possono assumere due stati:

- **In servizio:** Operatore abilitato e funzionante sul sistema, icona di gestione su PKSecurity600 di colore Verde 😊 0002 - Operatore 0002
- **Fuori Servizio:** Operatore disabilitato e non funzionante sul sistema, icona di gestione su PKSecurity600 di colore Grigio 😞 0003 - Operatore 0003
- **Non Aggiornato:** Il Software non ha ancora lo stato degli operatori, (premere tasto "Aggiorna" per avere stato) icona di gestione su PKSecurity600 di colore Giallo 😟 0002 - Operatore 0002



-  Permette di assegnare ad un Operatore una foto salvata (formato compatibile JPEG) nella directory predefinita del programma **C:\Programmi\Notifier\PkSecurity600\Foto**.
-  Permette di acquisire la foto da una risorsa video esterna.
- **Area:** Definisce l'area di appartenenza dell'operatore nella gestione del antipassback del controllo accessi (*default non selezionata*).
- **Operatore senza antipassback:** se selezionato permette all'operatore di non avere il controllo antipassback (modalità in cui viene vietata l'accesso multiplo dello stesso utente nello stesso varco) sui terminali configurati come controllo accessi. Verificare se l'operatore è associato ad un Profilo/Gruppo che possiede già questa abilitazione. (*default non selezionata*).
- **Cognome Nome:** Dati anagrafici operatore.
- **Gruppo:** Definisce solo una suddivisione logica degli utenti, non ha associazioni, non influisce sul funzionamento dell'operatore. (Es: Personale uffici, Magazzinieri, Dirigenti ecc etc).
- **Livello:** Definisce la modalità di funzionamento sugli oggetti che compongono il sistema CS600. (es cambio PIN, comandi da tastiera, reset memorie.....) (*paragraf. 3.22.3*)
- **ISV Posticipato:** permette di dare una data dalla quale l'operatore entrerà in funzione sul sistema con PIN e/o Tessera registrata. (*default non selezionata*).
- **Scadenza:** permette di dare una data da cui l'operatore non potrà più accedere al sistema. (*default non selezionata*).
- **Generazione Eventi:** Abilita la generazione eventi dell'operatore selezionato, ovvero la registrazione nel DataBase della CS600 di tutte le operazioni eseguite. (*default selezionato*).
- **Fascia Oraria:** definisce se all'operatore viene associata una fascia Oraria, quindi questo sarà abilitato alle sue associazioni solo se l'intervallo della fascia oraria associata sarà in fase di ON (es: associata ad un utente specifico che ha accesso a determinate aree solo in momenti stabiliti della giornata).
- **Supervisor:** Attribuisce all'utente le credenziali di Supervisor di Livello 2 (rif tabella 7).
- **Livello 3 En50131:** Attribuisce all'utente le credenziali di Supervisor Livello 3, di norma utilizzato dal responsabile dell'impianto. (*default non selezionato*).
- **Master:** Dà le credenziali di Utente Master nella logica della gestione aree del controllo accessi.

- **Matricola:** Identificativo aggiuntivo ai parametri anagrafici dell'operatore (utilizzato nelle esportazioni dati nel sistema di supervisione Monitor).
- **Pin:** Numerico composto da 6 cifre (non è possibile associare lo stesso PIN a più utenti)
- **Password di connessione:** Utilizzata dal sistema di supervisione Monitor qualora l'operatore che si sta configurando viene utilizzato come tramite di connessione per limitare le possibilità di esecuzione da centri di controllo remoto. (es: Istituto di vigilanza che possiede il Software Monitor Notifier).
- **Badge:** Non utilizzato.
- **Trasponder:** Valore che identifica in modo criptato i trasponder associati all'operatore. E' possibile associare più trasponder per ogni utente.
  - o Premendo il tasto "A" e selezionando un LCD600S in binding sarà possibile utilizzarlo come terminale di acquisizione tessere.
- **Radiocomando:** Valore che identifica in modo criptato i telecomandi associati all'operatore. E' possibile associare più telecomandi per ogni utente.
  - o Premendo il tasto "A" e selezionando un LCD600S in binding sarà possibile utilizzarlo come terminale di acquisizione tessere.
- **Profili:** permette di associare all'operatore uno o più profili configurati nel menù 3.21.2.
- **Cambia Descrizioni:** Selezionando più utenti è possibile modificarne la descrizione in sequenza.

I comandi disponibili per gli utenti attraverso LCD sulla gestione degli operatori sono:

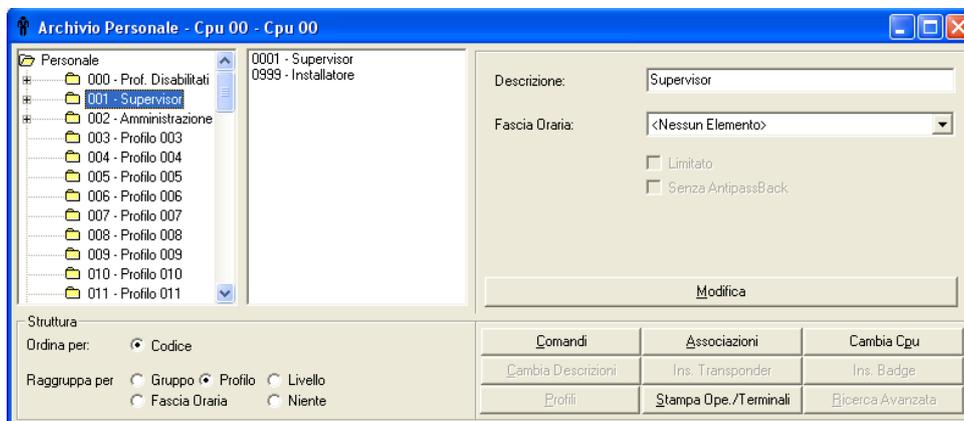
- **Operatori:** *In Servizio e/o Fuori Servizi, cambia PIN, Telecomando, Password connessione*
- **Gruppi:** *In Servizio e/o Fuori Servizio*
- **Profili:** *In Servizio e/o Fuori Servizio*

**Nota:** L'operatore una volta configurato e allineato con la centrale, deve essere messo "In Servizio" perché di default parte in disabilitato (*Fuori Servizio*).

### 3.22.2. Profili

E' un insieme di autorizzazioni legate alle funzionalità dell'operatore e identificano su quali oggetti che compongono il sistema hanno la possibilità di operare.

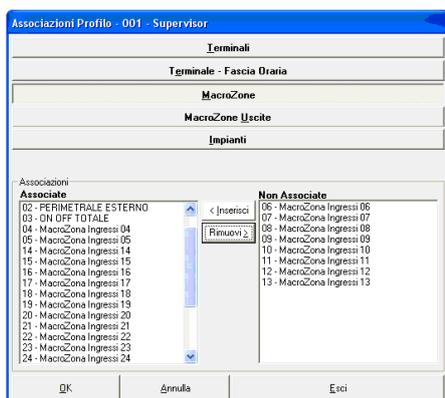
Un operatore può avere più Profili associati e questi possono contenere anche una sola associazione ad accedere ad un solo LCD dell'impianto.



All'apertura del menù nella colonna di sinistra sono elencati i 20 profili e 1000 operatori presenti di default. Nella colonna centrale sono mostrati invece gli operatori associati al profilo selezionato. Tutti gli operatori disponibili alla configurazione sono posizionati nel Profilo Disabilitati.

- **Struttura:**

- **Raggruppa per:** definisce la visualizzazione degli utenti divisi per
  - Gruppo
  - Profilo
  - Livello
  - Fascia oraria
  - Niente
- **Descrizione:** descrizione per identificare il Profilo (es: Amministrazione, Impiegati...)
- **Fascia oraria:** definisce se al profilo viene associata una fascia Oraria, quindi il profilo sarà attivo di conseguenza anche gli utenti associati potranno avere attive le abilitazioni configurate. (es: associata al profilo del personale che ha accesso a determinati luoghi solo in determinati momenti della giornata).
- **Limitato:** Funzionalità utilizzabile solo con sistema di supervisione Monitor.  
**N.B.:** Questo parametro viene utilizzato associato alla presenza di un software di supervisione Monitor. Se flaggato, permette al solo profilo selezionato l'allineamento sul sistema di supervisione del DataBase Utenti.
- **Senza Antipassback:** se selezionato permette a tutti gli utenti associati a questo profilo di non avere il controllo antipassback sui terminali configurati come controllo accessi.
- **Comandi:** Permette di mettere in servizio/fuori servizio il profilo selezionato (funzione disponibile solo con connessione attiva verso CS600).
- **Associazioni:** tasto di configurazione associazioni logiche al profilo. Qui vengono selezionati tutti gli Impianti/MacroZone/Zone/LCD600 che un utente associato a questo profilo potrà gestire, Figura sotto.



Ogni profilo può avere associazioni differenziate di Terminali, Terminali associati a fascia oraria, Macrozone, Macrozone di uscita e Impianti.

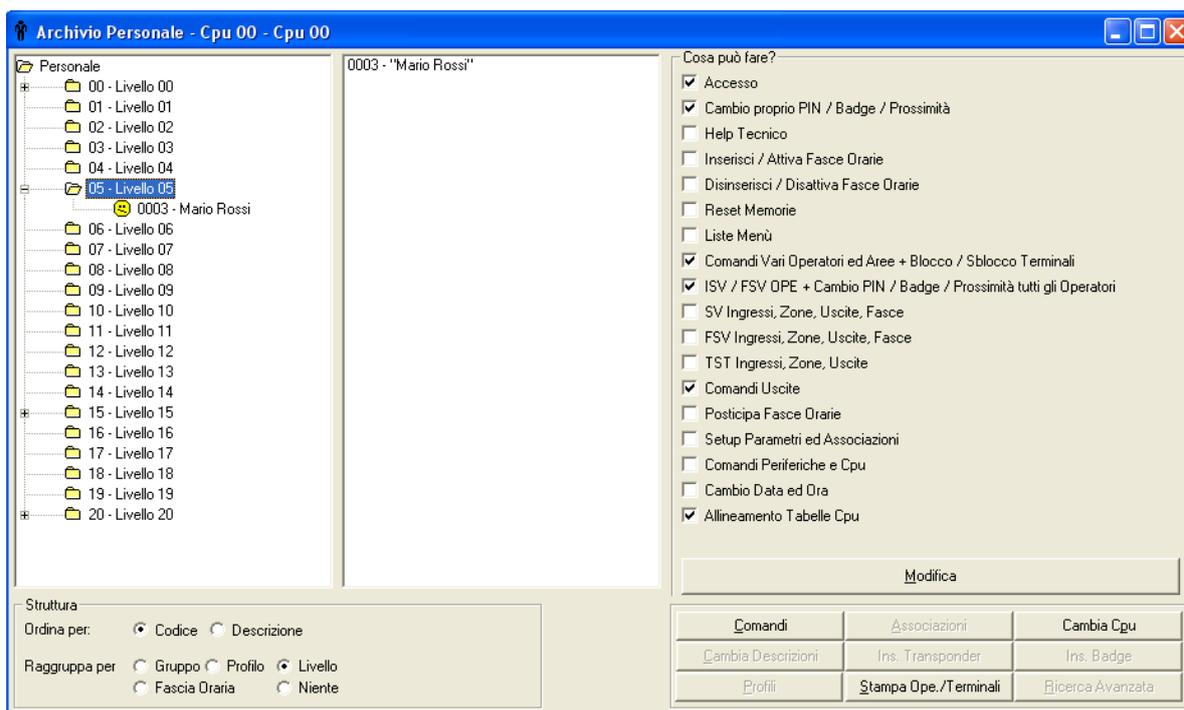
Una volta premuto il tasto Modifica è possibile selezionare o deselegionare gli elementi tramite i tasti <Inserisci o Rimuovi>.

- **Cambia Cpu:** tasto di selezione centrale in impianti di grosse dimensioni composti da più centrali CS600.
- **Stampa Ope/Terminali:** Permette la stampa e/o archiviazione tramite Database Access 2.0 degli Operatori e Terminali con le relative associazioni.



### 3.22.3. Livelli

E' la modalità con cui gli operatori interagiscono con gli oggetti (*LCD – AEI – RXE*) che compongono il sistema (es: *cambio PIN, comandi da tastiera, reset memorie...*).



Esistono 20 Livelli liberamente programmabili ma di default già pre-configurati, il **Livello** determina le diverse funzionalità degli oggetti (LCD/AEI...) che compongono il sistema CS600.

A differenza dei Profili ogni operatore può essere associato ad un solo Livello e di default sono tutti associati al livello 15.

**Nota:** Durante la fase di Sincronizzazione e aggiornamento dati, l'operatore "Installatore" utilizzato per la connessione con la CS600 non avrà le credenziali per la modifica di alcune parametrizzazioni (PIN e Password di connessione degli Operatori).

Il Software PKsecurity600 mostrerà in automatico un messaggio che richiama la necessità di allineare PIN e Password di connessione, connettendosi con operatore di tipo Supervisor liv.3 abilitato a eseguire le variazioni richieste.

Le restrizioni definite dalla norma per una centrale a Grado 3 e/o 2 di sicurezza sono riportate nelle tabelle di funzionalità nel capitolo 7 di questo manuale.

### 3.22.4. Gruppi

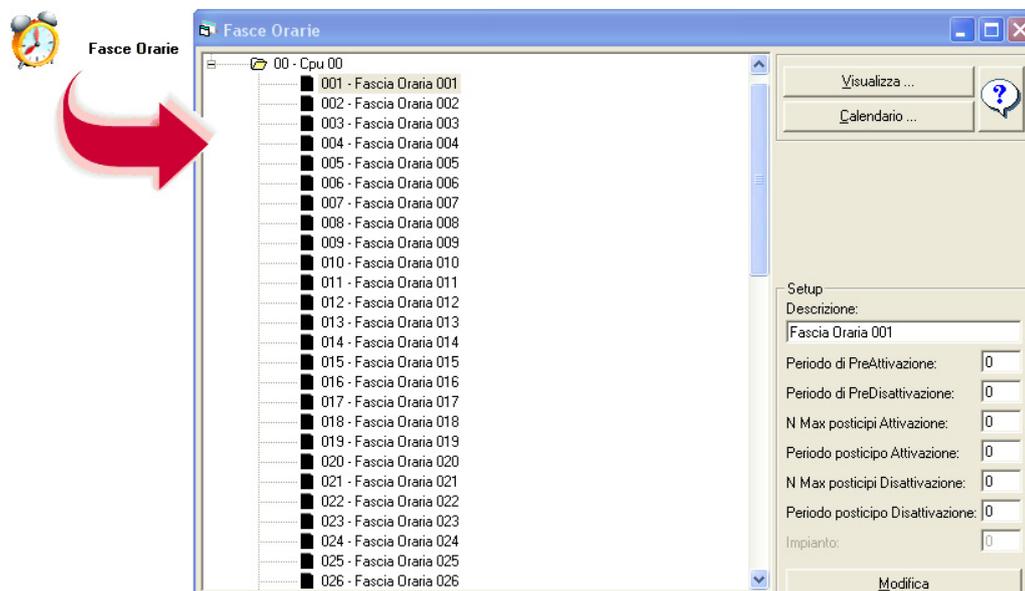
E' una suddivisione Logica, per raggruppare operatori in diversi team di lavoro (*es Impiegati, Magazzinieri, Dipendenti...*).

Questa suddivisione non ha ne associazione di funzionamento con il sistema, ma permette l'abilitazione/disabilitazione attraverso un unico comando di tutti gli operatori appartenenti al gruppo selezionato.

Gli operatori appartenenti allo stesso gruppo possono avere Profili e/o Livelli differenziati.

*ES: Se nell'azienda ci sono più gruppi e uno di questi contiene dipendenti che sono dei prestatori di manodopera in modo saltuario, è possibile eseguire un comando dalla tastiera LCD che agisca direttamente sul gruppo per escludere e/o includere in un'unica azione tutti gli operatori associati senza dover operare sul singolo utente, semplificandone la gestione.*

## 3.23. Fasce Orarie



Esistono 64 **Fasce Orarie** nella centrale CS600, liberamente programmabili e associabili a Operatori, Terminali, Macrozone etc.

Settaggi disponibili sulla fascia Oraria:

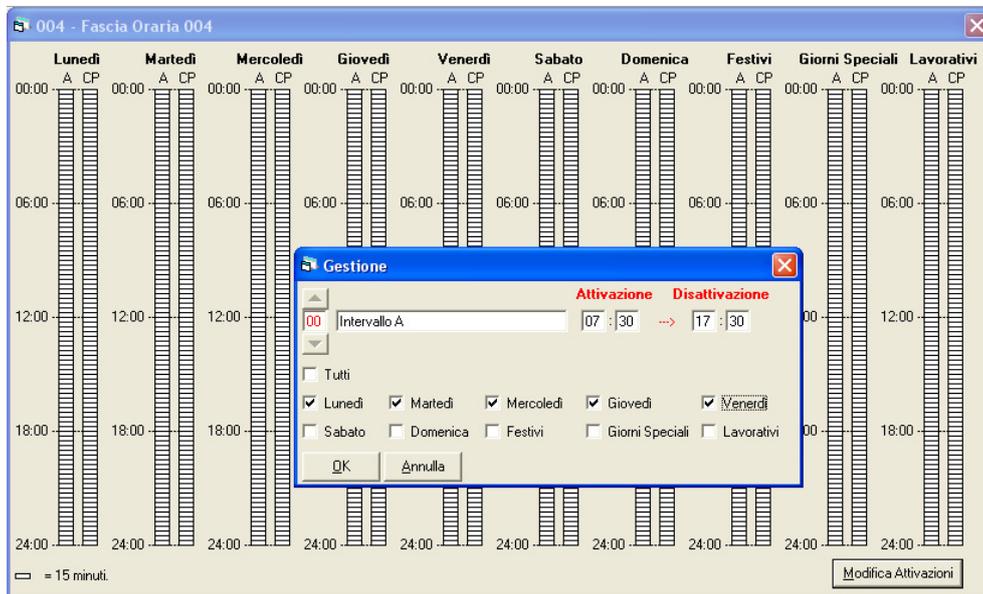
- **Descrizione:** Nome personalizzabile da attribuire alla fascia.
- **Periodo di PreAttivazione:** Espresso in secondi, corrisponde al tempo che anticipa l'Attivazione della fascia. Es: è possibile attivare un'uscita digitale (un buzzer di un LCD600S o un LED..) in fase di PreAttivazione in modo tale da avvisare il personale residente in un ambiente che il sistema entrerà nella fase d'Inserimento. (*default =0*)
- **Periodo di PreDisattivazione:** espresso in secondi corrisponde al periodo che intercorre prima che la fascia venga messa a riposo. Es è possibile attivare un'uscita digitale (un buzzer di un LCD600 o un Led..) in fase di PreDisattivazione fascia in modo tale da avvisare il personale residente in un ambiente che allo scadere della segnalazione non potrà essere più realizzata una determinata operazione. (*default =0*)
- **N° Max Posticipi Attivazione:** n° massimo consentito di posticipi attivazione fascia. (*default =0*)
- **Periodo Posticipo Attivazione:** espresso in secondi, corrisponde alla durata del periodo di posticipo Attivazione (*default =0*)
- **N° Max Posticipi Disattivazione:** n° massimo consentito di posticipi disattivazione fascia. (*default =0*)
- **Periodo Posticipo Disattivazione:** espresso in secondi corrisponde alla durata del periodo di posticipo Disattivazione. (*default =0*).

Quando si clicca su una delle fasce orarie viene visualizzato il telecomando di gestione che permette l'invio di comandi alla fascia oraria se connessi alla CS600:



Il tasto di setup  mostra la finestra di configurazione della fascia oraria dove vengono creati gli intervalli ON/OFF della fascia, l'associazione a giorni settimanali che si dividono in Lavorativi, Speciali e Festivi.

E' possibile creare più intervalli fino a n°9 max per singola fascia oraria.

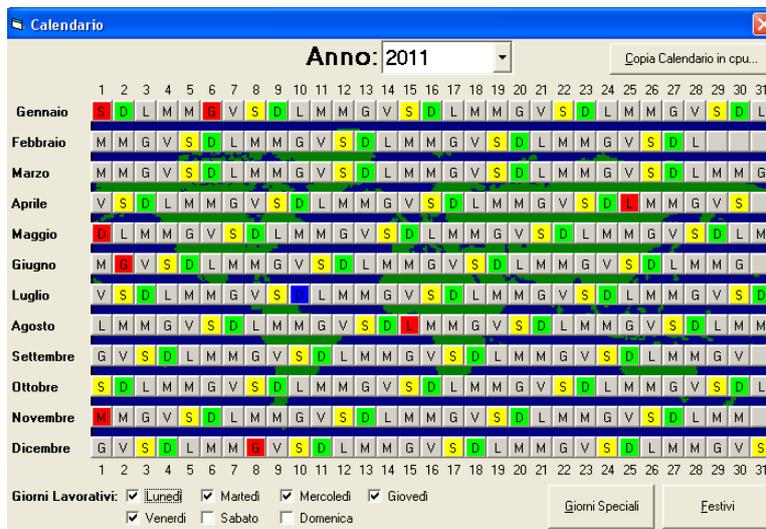


Il tasto  visualizza e permette la modifica del calendario presente in centrale. (vedi Cap. 3.23 Calendario).



: Permette la visualizzazione di una legenda stati delle icone della struttura impianto.

### 3.24. Calendario

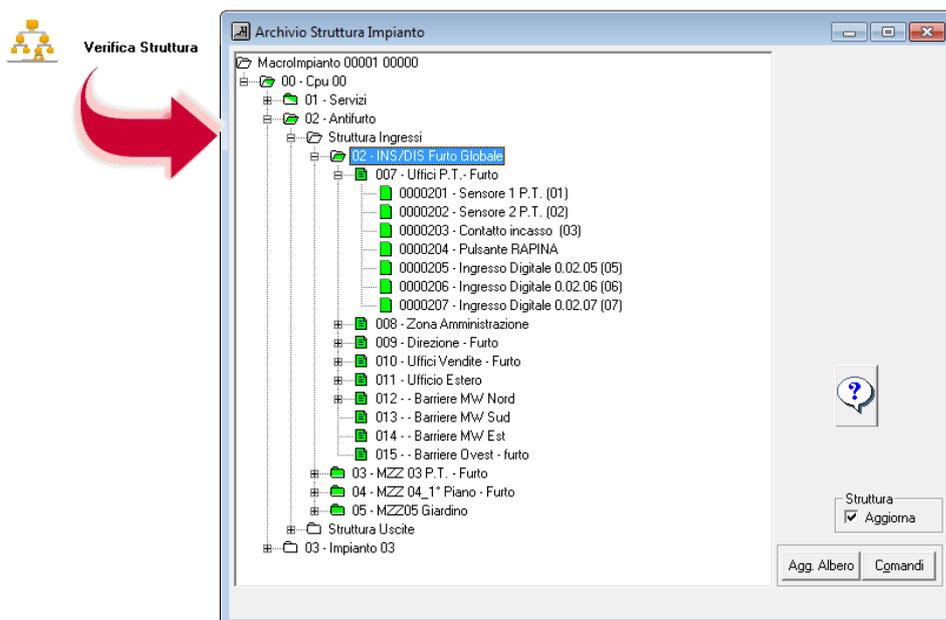


Il menù Calendario permette la configurazione suddivisa per anno (biennale) dei giorni Lavorativi, Festivi e Speciali attraverso i tasti dedicati.

Il menù Calendario permette la configurazione biennale (anno corrente e successivo in modo perpetuo) dei giorni Lavorativi, Festivi e Speciali attraverso i tasti dedicati.

## 3.25. Verifica struttura

Una volta eseguita la programmazione della centrale CS600 e quindi associati gli Ingressi alle varie Zone Logiche, le Zone alle Macrozone e le Macrozone dei vari impianti è utile controllare le corrette associazioni tramite il menù “**Verifica Struttura**”, tale menù visualizza una struttura ad albero che identifica l'appartenenza logica degli elementi che compongono il sistema.



Una volta connessi con la centrale CS600 attraverso il tasto **Aggiorna** dopo aver aperto “**Verifica Struttura**” sarà possibile avere la visualizzazione in tempo reale gli stati degli oggetti collegati e configurati.

E' consentito altresì inviare comandi agli elementi selezionati dall'apposito tasto **Comandi**.

I comandi sono disponibili in base all'oggetto selezionato e si dividono in:

### ➤ MacroZone Ingressi



- **Reset memorie:** Cancella tutte le memorie (Allarme, Guasto ecc ecc) di tutti gli oggetti associati (MacroZone, Zone, Ingressi).
- **Inserisci:** Inserisce la MacroZona e tutti gli oggetti associati (Zone, Ingressi), considerando gli eventuali tempi di ritardo configurati sui singoli oggetti.
- **Inserisci !:** Inserisce immediato della MacroZona e tutti gli oggetti associati (Zone, Ingressi), NON considerando gli eventuali tempi di ritardo configurati sui singoli ingressi.
- **Disinserisci:** Disinserisce la MacroZona e tutti gli oggetti associati (Zone, Ingressi).

### ➤ Zone Ingressi



- **Reset memorie** Cancella tutte le memorie (Allarme, Guasto ecc ecc) di tutti gli oggetti associati (Ingressi).
- **Inserisci:** Inserisce la Zona e tutti gli oggetti associati (Ingressi), considerando gli eventuali tempi di ritardo configurati sui singoli oggetti.
- **Inserisci !:** Inserisce immediato della MacroZona e tutti gli oggetti associati (Ingressi), NON considerando gli eventuali tempi di ritardo configurati sui singoli ingressi.
- **Disinserisci:** Disinserisce la MacroZona e tutti gli oggetti associati (Ingressi)
- **In Servizio:** Mette In Servizio tutti gli oggetti associati (Ingressi).
- **Fuori Servizio:** Mette Fuori Servizio tutti gli oggetti associati (Ingressi).

- **Test:** Mette in stato di verifica tutti gli oggetti associati (Ingressi), che in caso di allarme da Inseriti, generano eventi di “Allarme in test” senza generare la condizione di allarme che attiva le uscite EN50131
- **InizioWalk Test Totale:** Mette in stato di controllo tutti gli oggetti associati (Ingressi), per effettuare controlli manutentivi.  
**NOTA:** Il WalkTest ha una durata max di 20min entro i quali tutti i dispositivi (Sensori, Contatti, Barriere ecc ecc) associati alla Zona in cui è stato attivato il comando dovranno generare almeno una condizione di allarme.
  1. Tutti i dispositivi della Zona hanno generato almeno un allarme nei 20 min, la condizione di WalkTest verrà terminata in automatico dalla centrale, generando un evento di WalkTest OK.
  2. Alcuni dispositivi non hanno generato almeno una condizione di allarme nei 20min la centrale termina la condizione di Controllo e genera un evento di WalkTest KO con l’elenco dei dispositivi che NON sono andati in Allarme.
- **Fine Walk Test:** Termina in modo manuale la condizione di controllo, generando un evento di Walktest KO con l’elenco dei dispositivi che NON sono andati in allarme.

### ➤ Ingressi Digitali



- **Reset memorie:** Cancella tutte le memorie (Allarme, Guasto ecc ecc) dell’oggetto in gestione.
- **In servizio** Mette In Servizio l’oggetto in gestione.
- **Fuori Servizio:** Mette Fuori Servizio l’oggetto in gestione.
- **Test:** Mette in stato di verifica l’oggetto in gestione, in caso di allarme da Inserito, genererà un evento di “Allarme in test” senza generare la condizione di allarme che attiva le uscite EN50131
- **Isola:** Mette l’oggetto in gestione in una condizione per cui la centrale non ne considererà più le variazioni di stato. Il numero totale di oggetti “Isolati” viene visualizzato dal menu della tastiera LCD.

### ➤ MacroZone Uscite



- **Lampeggio lento:** Mette in condizione di Attivato, Lampeggiante Lento tutti gli oggetti associati (Zone Uscite e Uscite digitali).
- **Lampeggio veloce:** Mette in condizione di Attivato, Lampeggiante Veloce tutti gli oggetti associati (Zone Uscite e Uscite digitali).
- **Accesso fisso:** Mette in condizione di Attivato Fisso tutti gli oggetti associati (Zone Uscite e Uscite digitali).
- **Riposo:** Mette in condizione di Riposo tutti gli oggetti associati (Zone Uscite e Uscite digitali).

NOTA: Colorazione del Led: Di default le attivazioni manuali prevedono la colorazione ROSSA delle uscite Led tricolori. E’ possibile modificare la colorazione temporaneamente selezionando con il mouse la striscia tricolore. Il colore selezionato verrà visualizzato in “Selezione Corrente”.

- Zone Uscite
- Uscite Digitali



- **In servizio** Mette In Servizio l’oggetto in gestione.
- **Fuori Servizio:** Mette Fuori Servizio l’oggetto in gestione.
- **Lampeggio lento:** Mette in condizione di Attivato, Lampeggiante Lento tutti gli oggetti associati o in gestione (Uscite digitali).
- **Lampeggio veloce:** Mette in condizione di Attivato, Lampeggiante Veloce tutti gli oggetti associati o in gestione (Uscite digitali).
- **Acceso fisso:** Mette in condizione di Attivato Fisso tutti gli oggetti associati o in gestione (Uscite digitali).
- **Riposo:** Mette in condizione di Riposo tutti gli oggetti associati o in gestione (Uscite digitali).

NOTA: Colorazione del Led: Di default le attivazioni manuali prevedono la colorazione ROSSA delle uscite Led tricolori. E’ possibile modificare la colorazione temporaneamente selezionando con il mouse la striscia tricolore. Il colore selezionato verrà visualizzato in “Selezione Corrente”.

**Nota:** Gli oggetti non configurati non saranno visualizzati in questa struttura, e gli oggetti non

comandabili avranno un messaggio di comandi non disponibili



: Permette la visualizzazione di una legenda stati delle icone della struttura impianto.



Gli Ingressi digitali e/o analogici di un impianto visibili dal menù “verifica Struttura” assumo delle colorazioni differenti in base allo stato. Sotto le legende identificative.

### Legenda stati ingressi

<u>Colorazione</u>	<u>Stato</u>
<b>Rosso</b>	Allarme
<b>Bianco</b>	Riposo
<b>Giallo</b>	Manomissioni Varie*
<b>Verde</b>	Inserito
<b>Viola</b>	Pre-Allarme**
<b>Arancione</b>	Isolato
<b>Blu</b>	Memoria Manomissioni
<b>Giallo con bordo Blu</b>	Memoria Pre-Allarme
<b>Giallo con “X” Rossa</b>	Fuori Rete
<b>Bianco con “X” Rossa</b>	Periferica non in Binding
<b>Nota:</b> -* Alcuni stati nella tabella sono accompagnati da una lettera “Legenda Stati Ingressi” che specifica la condizione dell’ingresso. -** Solo per Ingressi Analogici/Zone/MacroZone	

### Definizione stati Ingressi

<u>Definizione</u>	<u>Stato</u>
<b>C</b>	Corto
<b>T</b>	Taglio
<b>W</b>	WalkTest
<b>G</b>	Guasto
<b>I</b>	Isolato
<b>V</b>	Memorie Varie (Guasto Mascheramento, Anomalia...)
<b>M</b>	Mascheramento
<b>Nota:</b> Le lettere della colonna “Definizione” si trovano sulle Icone degli Ingressi digitali/analogici sul Software PkSecurity600 del menu Verifica Struttura	

## 4. Impianto Base

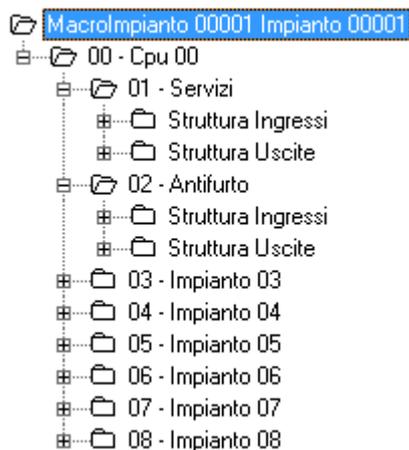
Il Software PKSecurity600 è rilasciato completo di un programma di default (impianto Base) identificato con numerazione 00001.

Questo può essere modificato, espanso, rinumerabile, ma comunque preconfigurato in tutti gli aspetti e logiche di funzionamento.

E' possibile creare nuovi impianti o cloni dell'impianto di default tramite la funzione **Apri come**. (vedi par. 3.11.3), questo comando permette la copia multipla degli impianti caricati rinumerandoli semplicemente. In questo modo sarà possibile personalizzare infiniti impianti, mantenendo inalterate le logiche di funzionamento basilari, con un notevole risparmio in termini di tempo di programmazione.

### 4.1. Struttura Logica

- **8 Impianti:** suddivisi in Struttura ingressi e Struttura Uscite. 2 dei quali ottimizzati alle funzioni di Servizi Generali (**01**) e Antifurto (**02**), gli altri 6 liberamente programmabili



L'impianto **Servizi** è dedicato alla gestione di tutte le segnalazioni e attivazioni generiche del sistema, che escludono quelle dei singoli impianti come per esempio le segnalazioni (Allarmi generali, Tamper del sistema, Mancanza rete, Codici errati, allarmi Rapina....

L'Impianto **Antifurto** invece è predisposto per il funzionamento come impianto di Antintrusione con tutte le logiche e prerogative di un impianto di sicurezza.

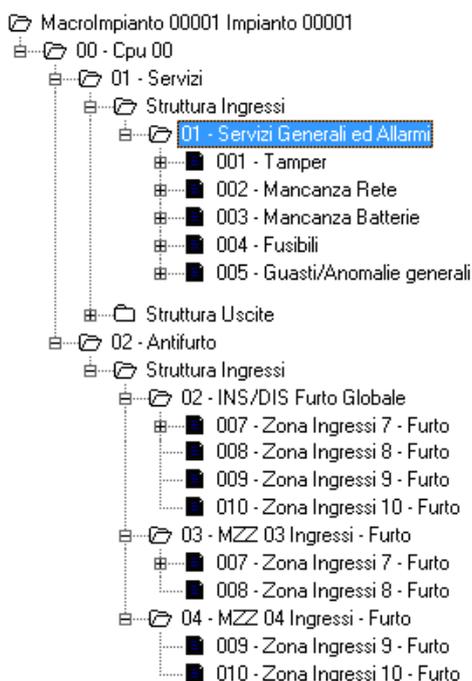
La struttura mostrata è richiamabile dal tasto



**Verifica Struttura**

presente sulla pagina principale del **PKSecurity600**.

### 4.1.1. Impianto Servizi – Struttura Ingressi



Alla **Struttura Ingressi** dell'impianto **Servizi** è stata associata una Macrozona (01- Servizi Generali ed allarmi) completa di 8 Zone preconfigurate con alcuni ingressi già associati quali: Tamper delle periferiche della linea 1, Fusibili di centrale e controlli di Mancanza Rete / Mancanza Batteria.

Sono inoltre presenti Zone logiche di uscita già preconfigurate all'attivazione di: **Guasti e Anomalie** generiche di sistema, **Allarmi generali**, **Allarmi Panico/Rapina**, **Codici errati**.

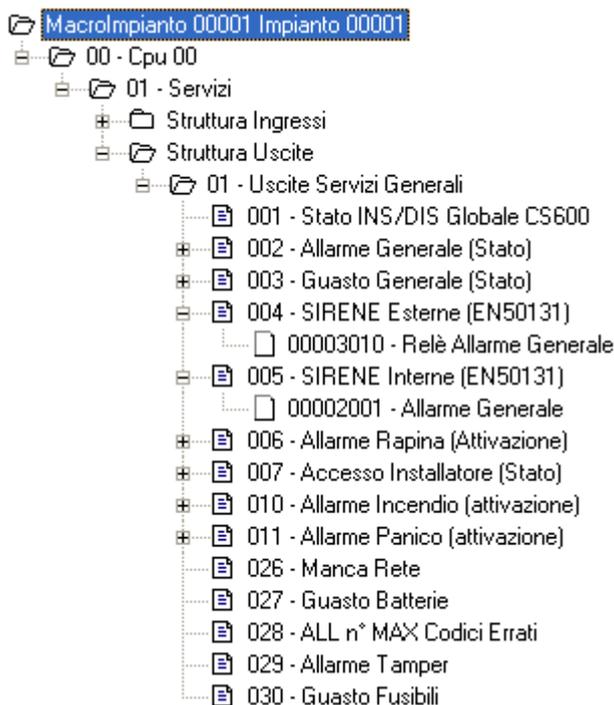


**Verifica Struttura**

La struttura mostrata è richiamabile dal tasto del **PKSecurity600**.

presente sulla pagina principale

### 4.1.2. Impianto Servizi – Struttura Uscite

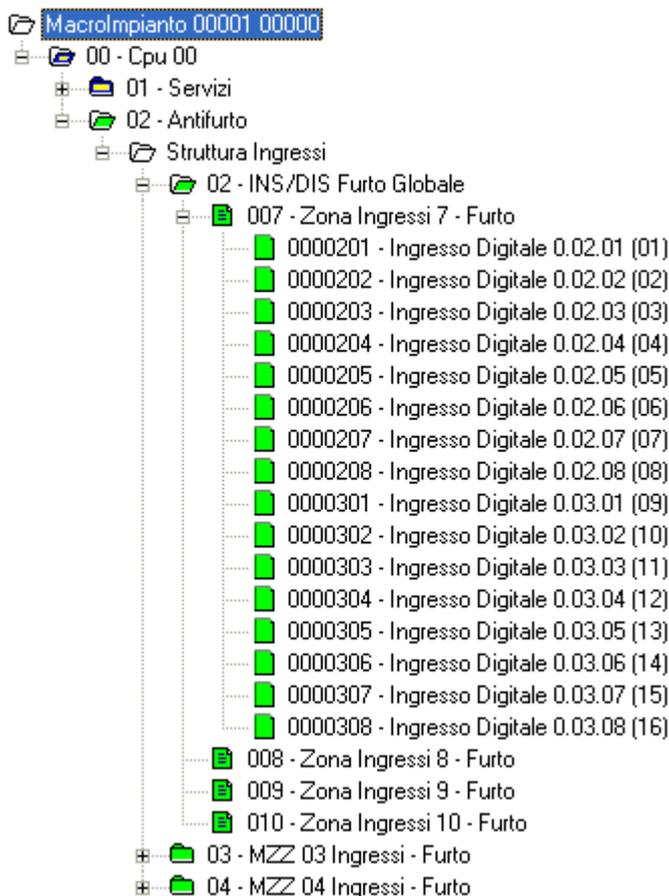


La struttura Uscite dell'Impianto **Servizi** è costituita da 8 Zone di uscita diversificate per tipologia:

- **Zona Sinottici** : associare le uscite LED dei terminali LCD600S, che riporteranno una segnalazione generica con LED tricolore dello stato della MacroZona 01- Servizi Generali ed allarmi
  - **Allarmi Generali**: Associare le uscite digitali che andranno attivate in caso di allarme generale del sistema.
  - **Uscite (Stato)**: Si ripristinano, ovvero tornano a riposo quando la condizione che le ha attivate non è più presente.
  - **Guasti Generali**: la zona viene attivata da un qualsiasi Guasto del sistema.
- **Attivazioni di servizio**: Contiene di default 8 uscite digitali associate che corrispondono ai relativi 8 Open Collector presenti sulla morsettiera JP8 della scheda Base CS600 .

- **Mancanza Rete:** la zona viene attivata dall'evento di Mancanza Rete primaria (220Vac) della CPU o degli ALI8/8 di campo, (verificare tempo integrazione Pre-Manca Rete (rif 3.17.1)).
- **Guasto Batterie:** la zona viene attivata dall'evento Mancanza Batterie della CPU.
- **ALL nr MAX codici errati:** le uscite associate verranno attivate alla generazione dell'evento n° max codici errati impostato dalle proprietà dei Terminali (rif 3.20.1).
- **Allarme Tamper:** le uscite associate si attiveranno in corrispondenza di una manomissione generato dall'apertura di un Tamper associato alla zona di ingresso **001 Tamper**.

#### 4.1.3. Impianto Antifurto – Struttura Ingressi

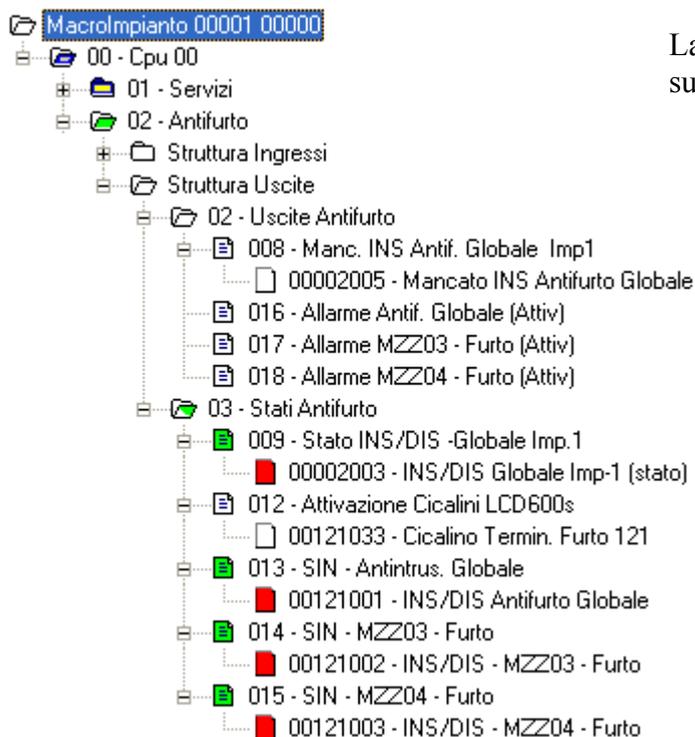


La **struttura ingressi** dell'impianto **Antifurto** è suddivisa in 3 Macrozone:

- **INS/DIS Furto Globale:** Oggetto Logico creato per gestire i comandi di INS/DIS Totale delle MacroZone d'ingresso **03** e **04**.
- **MZZ 03 Ingressi - Furto:** contiene nr° 2 zone Ingressi disponibili all'associazione di ingressi digitali di controllo dell'impianto Antifurto (es: Perimetrale e Volumetrico).
- **MZZ 04 Ingressi - Furto:** contiene nr° 2 zone Ingressi disponibili all'associazione di ingressi digitali di controllo dell'impianto Antifurto (es: Perimetrale e Volumetrico).

**Nota:** La MZZ 02 è una MacroZona “*Collegata*”, creata per facilitare le procedure d’Inserimento e Disinserimento globale delle diverse Zone appartenenti alle Mzz (in questo caso MZZ 03 e MZZ04) che compongono un impianto. Vedi cap. 3.20.1 “Zone Ingressi/uscite Associate”.

#### 4.1.4. Impianto Antifurto – Struttura Uscite



La **struttura uscite** dell'impianto **Antifurto** è suddivisa in 2 Macrozone essenziali:

- **02 Uscite Antifurto:** Contiene le zone di uscita che verranno attivate a fronte di Allarmi Antintrusione, Guasti/Anomalie Furto, Sinottici Antifurto, Stati Antifurto Collegamento e Mancati Inserimento, e vengono messe a riposo in seguito ad un comando manuale o automatico oppure da un tempo impostato nelle proprietà delle uscite stesse (es: sirena esterna con 180°)
- **03 Stati Antifurto:** contiene le zone di uscita attivate da condizioni specifiche, suddivise in relazione alle diverse Zone/MacroZone di ingresso ad esse legate nella programmazione e vengono messe a riposo non appena la causa che le ha attivate termina (*rif 3.19*).  
**ES:** Impianto Antifurto (ALLARME Antifurto1, ALLARME Antifurto 2, Stato INSERITO/DISINSERITO Antifurto1, Stato INSERITO/DISINSERITO Antifurto2, SINOTTICO Antifurto 1 (che riporta nelle specifico attraverso segnalazione tricolore lo stato dell'impianto.

Colorazione sinottico di default associato MacroZona Antifurto						
<i>Stato MacroZona</i>	<i>Riposo</i>	<i>Allarme</i>	<i>Memoria Allarme</i>	<i>Guasto</i>	<i>Memoria Guasto</i>	
<b>INSERITO</b>	Rosso Fisso	Rosso Lamp Veloce	Rosso Lamp Lento	Giallo Fisso	Giallo Lamp Lento	
<b>DISINSERITO</b>	Verde Fisso	Verde Lamp Veloce	Verde Lamp Lento	Giallo Fisso	Giallo Lamp Lento	

#### 4.2. Predisposizioni default – LCD600s

Ogni LCD600S dispone di nr°3 pagine sinottiche configurabili che possono essere visualizzate ciclicamente sul display (rif 3.20.2.2).

Nell'impianto Base 00001, le pagine sinottiche con comandi di INS/DIS del terminale LCD600S con indirizzo 121 (Linea 1 Indirizzo 21) si presenta configurato in questa modalità:

##### Pagina 1:

Indirizzo	Funzione Tasto	Descrizione LED
<b>01</b>	Inserimento / Disinserimento della Macrozona <b>02 Furto Globale</b>	<b>INS/DIS Furto Globale</b>
<b>02</b>	Inserimento / Disinserimento della Macrozona <b>03 Ingressi Furto</b>	<b>INS/DIS MZZ 03 Ingressi Furto</b>
<b>03</b>	Inserimento / Disinserimento della Macrozona	<b>INS/DIS MZZ 04 Ingressi Furto</b>

	<b>04 Ingressi Furto</b>	
<b>04</b>		
<b>05</b>		
<b>06</b>		
<b>07</b>		
<b>08</b>		

**Pagina2:**

<b>Indirizzo</b>	<b>Descrizione</b>	<b>LED</b>
<b>01</b>		
<b>02</b>		
<b>03</b>		
<b>04</b>		
<b>05</b>		
<b>06</b>		
<b>07</b>		
<b>08</b>		

**Pagina3:**

<b>Indirizzo</b>	<b>Descrizione</b>	<b>LED</b>
<b>01</b>		
<b>02</b>		
<b>03</b>		
<b>04</b>		
<b>05</b>		
<b>06</b>		
<b>07</b>		
<b>08</b>		

**LED LA:** (⊗) Rosso fisso – Allarme Generale.

**LED LB:** △ Giallo Fisso – Guasto Generale.

**LED LD:** ✎ Rosso Fisso – Accesso Installatore.

## 5. Password del sistema

Per poter operare con il software PKSecurity600, occorre eseguire un login con un operatore Supervisor Tecnico o Supervisor Utente precedentemente configurato.  
Di default è presente il Supervisor Tecnico, che accede con codice operatore 101 e password 1111.

### Operatori PC - Password di accesso PKSecurity600 - Default.

<b>Descrizione</b>	<b>User</b>	<b>Password</b>
Supervisor Tecnici	101	1111

### **Password di connessione:**

Tutti gli operatori PK, di default assumono la stessa password di connessione = **0000**.

**N.B.:** Verificare la configurazione della Rubrica di Connessione e tramite il tasto “**Associa Operatori PK**” viene creata, attraverso la Password di connessione, un’associazione che autorizza l’operatore PK in login ad assumere le proprietà di un operatore CPU - Installatore (999), ottenendo così le opportune autorizzazioni che gli permetteranno di agire sulle configurazioni di centrale.

### **Connessione tramite Rubrica di connessione.**

Quando ci si connette alla CS600 con l’operatore PK “101” tramite la rubrica, otterremo la connessione con la centrale sfruttando le credenziali dell’operatore Installatore 999.

### **Connessione tramite Connessione Manuale.**

Se invece si richiede la connessione tramite “Connessione Manuale”, ci verrà chiesto di inserire User e Password dell’operatore CPU; inserire quindi “999 – 0000” per connettersi come installatore e avere il pieno controllo sulla programmazione e modifica dei dati; connettersi invece con operatore “1 – 0000” per accedere come Supervisor Utente. In questo caso potremo prendere visione di tutto ma non abbiamo l’autorità per modificare i dati in centrale, ad esclusione dei PIN degli operatori.

### **Operatori CPU – Pin e Password di connessione (Default)**

<b>Descrizione</b>	<b>User</b>	<b>Pin</b>	<b>Password di connessione</b>
<b>Supervisor</b>	0001	111111	0000
<b>Installatore</b>	0999	999999	0000
<b>Supervisione Remota</b>	0998	-	-

### **N.B.:**

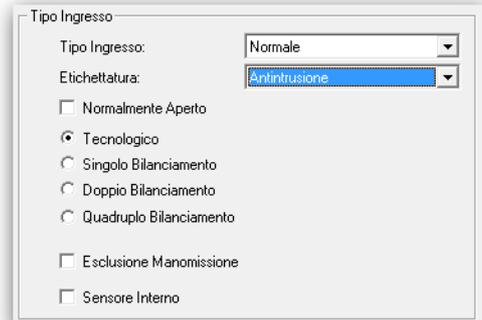
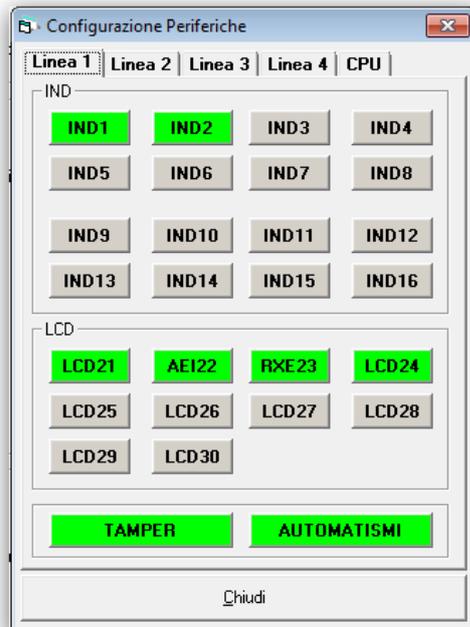
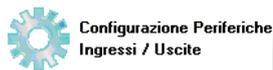
- La connessione alla centrale CS600 da parte di un utente installatore può avvenire in modalità singola, ovvero due installatori non si possono collegare alla centrale in simultanea.
- L’operatore 0997 viene utilizzato dal Software PK e dal Software Monitor di supervisione per effettuare connessioni temporanee per eseguire modifiche agli operatori di Livello 2 come da paragrafo 7.

## 6. Tipologia ed Etichette degli Ingressi digitali

### 6.1. Tipologie degli Ingressi digitali

Esistono diverse tipologie di Ingressi digitali, configurabili direttamente dal menù **Configurazione Periferiche Ingressi/Uscite**.

A seconda della tipologia selezionate l'ingresso assumerà diversi comportamenti.



A seconda della tipologia selezionata l'ingresso assumerà diversi comportamenti.

#### Tipologia Ingresso:

- **Normale:** Per tutti i gli ingressi di tipo digitale ad esclusione di quelli veloci per tapparelle.
- **Tapparella:** Per contatti veloci tipo tapparelle , senza la necessità di schede di analisi aggiuntive.

### 6.2. Etichette degli Ingressi Digitali

#### 6.2.1. Manomissione / Tamper

Da utilizzare per tutti gli ingressi destinati a proteggere i componenti del sistema contro l'accesso non autorizzato.

Allo stato di allarme viene sostituito lo stato di Taglio / Tamper.

Il Taglio / Tamper di un ingresso Manomissione / Tamper inibisce l'inserimento della Zona/MacroZone che lo contengono e deve essere escluso e/o resettato da un operatore Installatore.

E' possibile abilitare gli utenti standard di Livello 2 alla loro esclusione e al reset portando la CS600 a livello di sicurezza 2.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- La loro esclusione col parametro Manomissione selezionato.
- Il loro reset col parametro Manomissione selezionato.

## 6.2.2. Manca Rete

Da utilizzare per tutti gli ingressi destinati a segnalare la mancanza della sorgente di alimentazione primaria (230V).

Allo stato di Allarme viene sostituito lo stato di Guasto.

Nel caso in cui venga utilizzato il “*Tempo d'integrazione ingressi manca rete*” della centrale o il tempo integrazione singola rivelazione direttamente sull'ingresso, viene generato immediatamente un evento di Pre Manca Rete, se la condizione persiste, il Guasto al termine dell'integrazione.

Per rispettare la Norma EN50131 il tempo d'integrazione non deve superare i 3600 secondi.

Se questa etichetta viene assegnata ad un ingresso analogico (Es: manca rete CS600/ ALI8/8), lo stato di **Preallarme 1** genera un evento di tensione bassa e lo stato di **Preallarme 2** un evento di Tensione Alta.

Il Guasto di un ingresso Manca Rete inibisce l'inserimento della Zona/MacroZone che lo contengono e può essere escluso da un Utente.

L'evento di Guasto Manca Rete può essere resettato da un Utente Standard di Livello 2.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- La loro esclusione col parametro Guasto manca rete selezionato.
- Il loro reset col parametro Guasto manca rete selezionato.

USCITE SUPPLEMENTARI Manca Rete			
Inserito		Disinserito	
ATTIVAZIONI	STATI	ATTIVAZIONI	STATI
Pre MancaRete	Pre MancaRete	Pre MancaRete	Pre MancaRete
Rete	Rete	Rete	Rete

EVENTI SUPPLEMENTARI Manca Rete				
STATO	Inserito		Disinserito	
	EVENTO	RESET	EVENTO	RESET
<b>PREALLARME PER INTEGRAZIONE</b>	PRE MANCA RETE	Grado 3: Utente	PRE MANCA RETE	Grado 3: Utente
<b>PRE1</b>	TENSIONE BASSA	Grado 3: Utente	TENSIONE BASSA	Grado 3: Utente
<b>PRE2</b>	TENSIONE ALTA	Grado 3: Utente	TENSIONE ALTA	Grado 3: Utente

## 6.2.3. Batteria

Da utilizzare per tutti gli ingressi destinati a segnalare la mancanza o l'insufficienza della sorgente di alimentazione secondaria (generalmente le batterie).

Allo stato di allarme viene sostituito lo stato di Guasto.

Se è assegnata ad un ingresso analogico (Es: Batteria CS600/ ALI8/8), lo stato di **Preallarme 1** genera un evento di tensione bassa e lo stato di **Preallarme 2** un evento di Tensione Alta.

Il Guasto di un ingresso Batteria inibisce l'inserimento della Zona/MacroZone che lo contengono e può essere escluso da un Utente non Supervisor.

L'evento di Guasto Batteria deve essere resettato da un operatore Installatore.

E' possibile abilitare agli Utenti non Supervisor il reset portando la centrale a livello di *Sicurezza 2*.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- La loro esclusione col parametro Guasto Batteria selezionato.
- Il loro reset col parametro Altri Guasti selezionato.

<b>EVENTI SUPPLEMENTARI Batteria</b>				
<b>STATO</b>	<b>Inserito</b>		<b>Disinserito</b>	
	<b>EVENTO</b>	<b>RESET</b>	<b>EVENTO</b>	<b>RESET</b>
<b>PRE1</b>	TENSIONE BASSA	Grado 3: Utente	TENSIONE BASSA	Grado 3: Utente
<b>PRE2</b>	TENSIONE ALTA	Grado 3: Utente	TENSIONE ALTA	Grado 3: Utente

<b>USCITE SUPPLEMENTARI Batteria</b>			
<b>Inserito</b>		<b>Disinserito</b>	
<b>ATTIVAZIONI</b>	<b>STATI</b>	<b>ATTIVAZIONI</b>	<b>STATI</b>
Batteria	Batteria	Batteria	Batteria

#### 6.2.4. Antintrusione

Da utilizzare per tutti gli ingressi destinati a segnalare un tentativo d'intrusione in area protetta soggetta a variazione di stato Inserito/Disinserito.

<b>Eventi Antintrusione / Attivazione Uscite</b>				
<b>STATO</b>	<b>INSERITO</b>		<b>DISINSERITO</b>	
	<b>ATTIVAZIONI</b>	<b>STATI</b>	<b>ATTIVAZIONI</b>	<b>STATI</b>
<b>CORTO / TAGLIO</b>	Sirena Interna 50131 (OPZ)	Manomissione	Sirena Interna 50131 (OPZ)	Manomissione
	Sirena Esterna 50131 (OPZ)		Manomissione	
	Manomissione		Manomissione Disinserito	
	Manomissione Inserito		Remota (ATS)	
	Remota (ATS)			

<b>ALLARME</b>	Sirena Interna 50131	Allarme Inserito	Allarme Inserito / Disinserito	Allarme Disinserito
	Sirena Esterna 50131		Allarme Disinserito	
	Allarme Inserito / Disinserito			
	Allarme Inserito			
	Allarme Inserito Presidiato (vedi Presidio)			
	Allarme Inserito Non Presidiato (vedi Presidio)			
	Remota (ATS)			
<b>GUASTO</b>	Sirena Interna 50131 (OPZ)	Guasto		Guasto

	Guasto		Guasto	
	Remota (ATS)		Remota (ATS)	
<b>MASCHERAMENTO</b>	Sirena Interna 50131	Allarme Inserito		Mascheramento
	Sirena Esterna 50131	Mascheramento		
	Allarme Inserito / Disinserito			
	Allarme Inserito			
	Allarme Inserito Presidiato (vedi Presidio)			
	Allarme Inserito Non Presidiato (vedi Presidio)			
	Remota (ATS)			
<b>ANOMALIA</b>	Anomalia	Anomalia	Anomalia	Anomalia
	Remota (ATS)(OPZ)		Remota (ATS)(OPZ)	

<b>PREALLARME</b>	Preallarme	Preallarme		
	Preallarme Presidiato (vedi Presidio)			
	Preallarme Non Presidiato (vedi Presidio)			
	Remota (ATS)(OPZ)			

### 6.2.5. Antintrusione 24

Da utilizzare per tutti gli ingressi destinati a segnalare un tentativo d'intrusione in area protetta che devono generare una segnalazione anche quando la Zona/MacroZona che li contengono sono Disinserite.

<b>1.6.2.5.1.1. EVENTI SUPPLEMENTARI Antintrusione 24</b>				
<b>STATO</b>	<b>INSERITO</b>		<b>DISINSERITO</b>	
	<b>EVENTO</b>	<b>RESET</b>	<b>EVENTO</b>	<b>RESET</b>
<b>ALLARME</b>			Allarme	Grado 3: Utente

<b>1.6.2.5.1.2. USCITE SUPPLEMENTARI Antintrusione 24</b>			
<b>INSERITO</b>		<b>DISINSERITO</b>	
<b>ATTIVAZIONI</b>	<b>STATI</b>	<b>ATTIVAZIONI</b>	<b>STATI</b>
24 H	24 H	24 H	24 H
		Remota (ATS)	

## 6.2.6. Porte di Sicurezza C.M.

Da utilizzare per tutti gli ingressi, collegati al sensore di apertura delle porte di sicurezza, destinati a segnalare un tentativo d'intrusione nell'area protetta che devono generare una segnalazione anche quando la Zona/MacroZona che li contengono sono Disinserite.

1.6.2.6.1.1. EVENTI SUPPLEMENTARI Porte di Sicurezza C.M.				
STATO	INSERITO		DISINSERITO	
	EVENTO	RESET	EVENTO	RESET
ALLARME			Allarme	Grado 3: Utente

1.6.2.6.1.2. USCITE SUPPLEMENTARI Porte di Sicurezza C.M.			
INSERITO		DISINSERITO	
ATTIVAZIONI	STATI	ATTIVAZIONI	STATI
Porte Sicurezza C.M.	Porte Sicurezza C.M.	Porte Sicurezza C.M.	Porte Sicurezza C.M.
		Remota (ATS)	

## 6.2.7. Porte di Sicurezza Blocchi

Da utilizzare per tutti gli ingressi, collegati al sensore di apertura del blocco meccanico delle porte di sicurezza, destinati a segnalare l'allarme antintrusione quando aperti con impianto inserito.

A Impianto disinserito senza blocco meccanico l'ingresso sarà costantemente in allarme, genererà un *Allarme Porte di Sicurezza Blocchi* al momento del ripristino di tale blocco. In questa condizione non attiverà ne le uscite di allarme disinserito ne quelle di stato, ma solo la sua uscita dedicata nella programmazione.

1.6.2.7.1.1. EVENTI SUPPLEMENTARI Porte di Sicurezza Blocchi				
STATO	INSERITO		DISINSERITO	
	EVENTO	RESET	EVENTO	RESET
RIPOSO			Allarme	Grado 3: Utente

1.6.2.7.1.2. USCITE SUPPLEMENTARI Porte di Sicurezza Blocchi			
INSERITO		DISINSERITO	
ATTIVAZIONI	STATI	ATTIVAZIONI	STATI
		Porte Sicurezza Blocchi	Porte Sicurezza Blocchi
		Remota (ATS)	

## 6.2.8. Rapina

Da utilizzare per tutti gli ingressi destinati a segnalare un tentativo di rapina.

**N.B.:** Di default sia da inseriti che disinseriti attivano solo le sirene EN50131 nella menù di programmazione , **NON ATTIVANO** le uscite Allarme Antintrusione nel menù attivazioni sia in condizione presidiato, che non).

<b>1.6.2.8.1.1. EVENTI SUPPLEMENTARI Rapina</b>				
<b>STATO</b>	<b>INSERITO</b>		<b>DISINSERITO</b>	
	<b>EVENTO</b>	<b>RESET</b>	<b>EVENTO</b>	<b>RESET</b>
<b>ALLARME</b>			Allarme	Grado 3: Utente

<b>1.6.2.8.1.2. USCITE SUPPLEMENTARI Rapina</b>			
<b>INSERITO</b>		<b>DISINSERITO</b>	
<b>ATTIVAZIONI</b>	<b>STATI</b>	<b>ATTIVAZIONI</b>	<b>STATI</b>
Rapina	Rapina	Rapina	Rapina
		Remota (ATS)	
Sirena Interna 50131		Sirena Interna 50131	
Sirena Esterna 50131		Sirena Esterna 50131	

<b>1.6.2.8.1.3. PARAMETRI OPZIONALI Rapina</b>	
DISABILITA Sirena Interna 50131 da Disinserito	
DISABILITA Sirena Esterna 50131 da Disinserito	
ANNULLA RITARDO SIRENE	

## 6.2.9. Panico

Da utilizzare per tutti gli ingressi destinati a segnalare una condizione di panico.

**Nota:** Di default sia da inseriti che disinseriti attivano solo le sirene EN50131 nella menù di programmazione , **NON ATTIVANO** le uscite Allarme Antintrusione nel menù attivazioni sia in condizione presidiato, che non).

<b>1.6.2.9.1.1. EVENTI SUPPLEMENTARI Panico</b>				
<b>STATO</b>	<b>INSERITO</b>		<b>DISINSERITO</b>	
	<b>EVENTO</b>	<b>RESET</b>	<b>EVENTO</b>	<b>RESET</b>
<b>ALLARME</b>			Allarme	Grado 3: Utente

<b>1.6.2.9.1.2. USCITE SUPPLEMENTARI Panico</b>			
<b>INSERITO</b>		<b>DISINSERITO</b>	
<b>ATTIVAZIONI</b>	<b>STATI</b>	<b>ATTIVAZIONI</b>	<b>STATI</b>
Panico	Panico	Panico	Panico

		Remota (ATS)	
		Sirena Interna 50131	
		Sirena Esterna 50131	

### 1.6.2.9.1.3. PARAMETRI OPZIONALI Panico

DISABILITA Sirena Interna 50131 da Disinserito
DISABILITA Sirena Esterna 50131 da Disinserito
ANNULLA RITARDO SIRENE

## 6.2.10. Incendio

Da utilizzare per tutti gli ingressi destinati a segnalare una condizione di Incendio.

**Nota:** Di default sia da inseriti che disinseriti attivano solo le sirene EN50131 nella menù di programmazione , **NON ATTIVANO** le uscite Allarme Antintrusione nel menù attivazioni sia in condizione presidiato, che non).

Come parametri opzionali al ripristino viene attivata l'uscita Reset Incendio per tagliare l'alimentazione dei sensori incendio e quindi resettarli (utilizzare il contatto N.C. del relè scelto). Impostare il tempo di attivazione del relè (OND).

Durante il ripristino gli allarmi dei sensori vengono ignorati per un tempo pari al tempo di OND + 5 secondi.

### 1.6.2.10.1.1. EVENTI SUPPLEMENTARI Incendio

STATO	INSERITO		DISINSERITO	
	EVENTO	RESET	EVENTO	RESET
ALLARME			Allarme	Grado 3: Utente

### 1.6.2.10.1.2. USCITE SUPPLEMENTARI Incendio

INSERITO		DISINSERITO	
ATTIVAZIONI	STATI	ATTIVAZIONI	STATI
Incendio	Incendio	Incendio	Incendio
		Remota (ATS)	
		Sirena Interna 50131	
		Sirena Esterna 50131	
Reset Incendio			

### 1.6.2.10.1.3. PARAMETRI OPZIONALI Incendio

DISABILITA Sirena Interna 50131 da Disinserito
DISABILITA Sirena Esterna 50131 da Disinserito
ANNULLA RITARDO SIRENE

### 6.2.11. Servizio

Gli ingressi Servizio funzionano come gli ingressi Antintrusione, ma non attivano le uscite delle Zone, Macrozone, Impianti, Cpu. Attivano solo le uscite associate direttamente all'ingresso, che vanno a riposo configurando il tempo di OND o da comando manuale.

**N.B.:** Se utilizzato su ingressi dedicati all'antintrusione il sistema non è conforme alla EN50131.

### 6.2.12. Tecnologici

Gli ingressi Tecnologici funzionano come gli ingressi Antintrusione, ma non attivano le uscite degli Impianti e Cpu, la condizione di allarme si estende solo alla Zona.

**Nota:** Se utilizzato su ingressi dedicati all'antintrusione e con le sirene programmate a livello di impianto o cpu, il sistema non è conforme alla EN50131

### 6.2.13. Fusibili

Da utilizzare per tutti gli ingressi destinati a segnalare l'interruzione di un fusibile.

Allo stato di allarme viene sostituito lo stato di Guasto.

Il Guasto di un ingresso Fusibile inibisce l'inserimento della Zona/MacroZone che lo contengono e può essere escluso da un Utente non Supervisor.

L'evento di Guasto Fusibile deve essere resettato da un operatore installatore.

E' possibile abilitare gli utenti non Supervisor al reset portando la centrale a livello di sicurezza 2.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- La loro esclusione col parametro Guasto Batteria selezionato.
- Il loro reset col parametro Altri Guasti selezionato.

### 6.2.14. Sirena

Da utilizzare per tutti gli ingressi destinati a segnalare il Guasto di una sirena.

Allo stato di allarme viene sostituito lo stato di Guasto.

Il Guasto di un ingresso Sirena inibisce l'inserimento della zona/macrozone che lo contengono e deve essere escluso da un Operatore Installatore.

L'evento di Guasto Sirena deve essere resettato da un operatore Installatore.

E' possibile abilitare gli Utente non Supervisor all'esclusione e al reset portando la centrale a livello di sicurezza 2.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- La loro esclusione col parametro Guasto Sirena selezionato.
- Il loro reset col parametro Altri Guasti selezionato.

## 6.2.15. Riserva

Da utilizzare per tutti gli ingressi che pur rimanendo associati ad una zona operativa del sistema non devono generare nessuna segnalazione, gli ingressi settati come Riserva restano isolati e non possono essere messi In Servizio / Fuori Servizio.

## 6.2.16. ATS

Da utilizzare per tutti gli ingressi destinati a segnalare il Guasto di un sistema di trasmissione allarmi. Allo stato di allarme viene sostituito lo stato di Guasto.

Il Guasto di un ingresso ATS inibisce l'inserimento della zona/macrozone che lo contengono e deve essere escluso da un Operatore Installatore.

L'evento di Guasto Batteria può essere resettato da un Utente non Supervisor.

E' possibile abilitare gli utenti Utente non Supervisor all'esclusione portando la centrale a livello di sicurezza 2.

A grado sicurezza 2, nella finestra di configurazione Parametri Funzionamento CS600, è possibile limitare ai soli utenti Supervisor:

- A grado 2, la loro esclusione col parametro Guasto Sirena selezionato.
- A grado 2 e 3, il loro reset col parametro Altri Guasti selezionato.

# 7. Tabelle di riferimento

In questa sezione vengono definite le modalità di funzionamento della centrale e degli Operatori in base al grado di sicurezza scelto per la centrale CS600.

## 7.1. Livelli di accesso

L'accesso al sistema da parte degli operatori è definito in quattro Livelli.

Mentre le funzionalità operative vengono differenziate a seconda del Grado di sicurezza impostato sulla CS600.

### Livello 2

Accesso da parte dell'operatore.

Questo livello di accesso si divide in due sezioni, Standard e Supervisor.

Esegue funzioni che influenzano lo stato operativo, Inserimenti/Disinserimenti ma che non variano la configurazione dell'impianto di sicurezza e rapina.

L'accesso alle funzioni di livello 2 devono avvenire per mezzo di una chiave logica o da codici del livello indicato che non devono consentire l'accesso alle funzionalità dei livelli superiori 3 o 4.

La differenza di funzionalità dipende dalle configurazioni date nel menù Parametri funzionamento CPU.

Un Operatore di Livello 2 Supervisor può mettere in servizio un Operatore di livello 3\*.

### Livello 3

Accesso da parte del Supervisor,

Esegue funzioni che influenzano lo stato operativo, Inserimenti/Disinserimenti e che possono variare i dati dell'impianto di sicurezza e rapina, ma senza variarne le configurazioni.

L'accesso alle funzioni di livello 3 deve avvenire per mezzo di una chiave logica, o codici del livello indicato che non devono consentire l'accesso alle funzionalità dei livello superiore 3 Installatore o 4.

L'utente di livello 3 deve essere messo in servizio da un utente Livello 2 Supervisor, e può mettere in servizio un Operatore Installatore\*.

### Installatore

Accesso da parte dell'installatore,

Esegue funzioni che influenzano lo stato operativo, Inserimenti/Disinserimenti e che possono variare la configurazione e le funzionalità dell'impianto di sicurezza e rapina.

L'accesso alle funzioni di livello 3 deve avvenire per mezzo di una chiave logica, o codici del livello indicato che non devono consentire l'accesso alle funzionalità del livello superiore 4.

L'utente Installatore deve essere messo in servizio da un utente Livello 3 Supervisor.\*  
Livello 4.

Accesso da parte dell'utilizzatore, ad esempio, da parte del costruttore dell'apparecchiatura.

Accesso ai componenti per modificare il progetto dell'apparecchiatura.

L'accesso alle funzioni prescritte per essere accessibili al livello 4 deve essere limitato per mezzo di una chiave, di un interruttore o di una serratura a combinazione, o di altri dispositivi equivalenti.

**Nota:** L'accesso al livello 4 si applica alla variazione del software del programma operativo senza che sia stato attivato un dispositivo di manomissione.

(rif. Norma Tecnica CEI EN 50131-1:2008-02):

- L'accesso ai livelli 3 e 4 deve essere impedito finché l'accesso non sia stato consentito da parte di un operatore con livello 2. L'accesso al livello 4 deve richiedere anche l'autorizzazione da parte di un Operatore di livello 3.

- L'accesso ai livelli 2,3,4 può essere effettuato a distanza. A condizione che siano soddisfatti i livelli di autorizzazione equivalenti a quelli specificati nella schema sotto.

PRESCRIZIONE DEI CODICI DI AUTORIZZAZIONE				
Livelli di accesso 2,3,4	Combinazioni in base al Grado di sicurezza della centrale			
	1	2	3	4
Chiave Logica	1.000	10.000	100.000	1.000.000
Chiave Fisica	300	3.000	15.000	50.000
NOTE: Il riferimento alle chiavi fisiche e logiche nella tabella non escludono l'uso di altri mezzi di autorizzazione, come per es: Biometria ecc...				

Funzioni eseguite sulla CS600	Livello di accesso			
	2	3*	4**	Installatore
Inserimento	A	A	NA	A
Disinserimento	A	A	NA	A
Ripristino sistema Sicurezza/Rapina	A	A	NA	A
Verifica funzioni Sicurezza/Rapina	A	A	NA	A
Interrogazione registro eventi	A	A	NA	A
Inibizione/Isolamento/Forzatura ***	A	A	NA	A
Aggiunta/variazione dei codici di autorizzazione individuale	A	A	A	A
Aggiunta/eliminazione di utilizzatori e codici di livello 2	NA	A	NA	NA
Aggiunta/variazione dati specifici del sito	NA	A	NA	A
Variazione/sostituzione programma base	NA	NA	A	A

**Legenda:**

A= Abilitato

NA= Non Abilitato

\*= solo se abilitato dall'Operatore livello 2

\*\*= solo se abilitato dall'Operatore livello 2 e 3

\*\*\*= in funzione del grado di sicurezza selezionato

## 7.2. Funzionalità

In questa tabella vengono evidenziate le funzionalità degli operatori in base al grado di sicurezza della CS600, del livello di appartenenza e della caratteristica (Standard o Supervisor) dell'operatore.

### 7.2.1. Fuori Servizio – CS600 Grado 3

Fuori servizio**	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Ingresso Antintrusione in allarme	SI*	SI	SI	SI
Ingresso Antirapina in allarme	SI*	SI	SI	SI
Ingresso Antintrusione in mascheramento, anomalia	SI*	SI	SI	SI
Ingresso Antintrusione in guasto	SI*	SI	SI	SI
Guasto Manca Rete	SI*	SI	SI	SI
Guasto Batteria	SI*	SI	SI	SI
Altri Guasti (tranne ATS e Sirene)	SI*	SI	SI	SI
Manomissioni	NO	NO	SI	SI
Guasto Ats	NO	NO	SI	SI
Guasto Sirena (dalla vers FW 7.04)	NO	NO	SI	SI

**NOTE:**  
 \* Agli Operatori di Livello 2 Standard è possibile limitare alcune funzionalità abilitando il parametro dal menù di Configurazione Centrale / Parametri funzionamento CPU.  
 \*\* Il Fuori servizio s'intende sia durante la fase di Inserimento che nella modalità di impianto Disinserito, quindi con comandi diretto da LCD600S.

### 7.2.2. Fuori Servizio – CS600 Grado 2

Fuori servizio**	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Ingresso Antintrusione in allarme	SI*	SI	SI	SI
Ingresso Antirapina in allarme	SI*	SI	SI	SI
Ingresso Antintrusione in mascheramento, anomalia	SI*	SI	SI	SI
Ingresso Antintrusione in guasto	SI*	SI	SI	SI
Guasto Manca Rete	SI*	SI	SI	SI
Guasto Batteria	SI*	SI	SI	SI
Altri Guasti (tranne ATS e Sirene)	SI*	SI	SI	SI
Manomissioni	SI*	SI	SI	SI
Guasto ATS	SI*	SI	SI	SI
Guasto Sirena (dalla vers FW 7.04)	SI*	SI	SI	SI

**NOTE:**

\* Agli Operatori di Livello 2 Standard è possibile limitare alcune funzionalità abilitando il parametro nel menù di Configurazione Centrale / Parametri funzionamento CPU.

\*\* Il Fuori servizio si intende sia durante la fase di inserimento che nella modalità di impianto disinserito, quindi con comandi diretto da LCD600S.

**7.2.3. Reset – CS600 Grado 3**

Reset**	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Intrusione (Allarme, Mascheramento, Anomalie)	SI*	SI	SI	SI
Rapina	SI*	SI	SI	SI
Guasto Manca Rete	SI*	SI	SI	SI
Guasto ATS	SI*	SI	SI	SI
Manomissione (Corto, Taglio, Manomis. Periferica)	NO	NO	SI	SI
Altri Guasti (tranne ATS e Sirene)	NO	NO	SI	SI

**NOTE:**

\* Agli Operatori di Livello 2 Standard è possibile limitare alcune funzionalità abilitando il parametro nel menù di Configurazione Centrale / Parametri funzionamento CPU.

\*\* Il Reset s'intende come operazione eseguita dopo una verifica sul display LCD600S attraverso il menù eventi importanti e con la condizione che lo ha generato tornata a riposo.

**7.2.4. Reset – CS600 Grado 2**

Reset**	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Intrusione (Allarme, Mascheramento, Anomalie)	SI*	SI	SI	SI
Rapina	SI*	SI	SI	SI
Guasto Manca Rete	SI*	SI	SI	SI
Guasto ATS	SI*	SI	SI	SI
Manomissione (Corto, Taglio, Manomis. Periferica)	SI*	SI	SI	SI
Altri Guasti (tranne ATS e Sirene)	SI*	SI	SI	SI

**NOTE:**

\* Agli Operatori di Livello 2 Standard è possibile limitare alcune funzionalità abilitando il parametro nel menù di Configurazione Centrale / Parametri funzionamento CPU.

\*\* Il Reset si intende come operazione eseguita dopo una verifica sul display LCD600S attraverso il menù eventi importanti e con la condizione che lo ha generato tornata a riposo.

**7.2.5. Isolamento – CS600 Grado 3**

Isolamento**	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore

Isola Ingressi	NO	NO	SI	SI
----------------	----	----	----	----

**NOTE:**  
**\*\*** L'isolamento s'intende come operazione eseguita su ingressi digitali/analogici da terminale LCD600S attraverso il menù Comandi.  
L'ingresso in questa condizione non sarà più controllato dalla CS600 fino a quando non sarà messo di nuovo nello stato di In Servizio.  
La condizione d'isolamento viene mantenuta sia a impianto Inserito che Disinserito.

### 7.2.6. Isolamento – CS600 Grado 2

Isolamento**	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Isola Ingressi	SI*	SI	SI	SI

**NOTE:**  
\* Agli Operatori di Livello 2 Standard è possibile limitare alcune funzionalità abilitando il parametro nel menù di Configurazione centrale\_Parametri funzionamento CPU.  
**\*\*** L'isolamento s'intende come operazione eseguita su ingressi digitali/analogici da terminale LCD600S attraverso il menù Comandi.  
L'ingresso in questa condizione non sarà più controllato dalla CS600 fino a quando non sarà messo di nuovo nello stato di In Servizio.  
La condizione d'isolamento viene mantenuta sia a impianto Inserito che Disinserito.

### 7.2.7. Gestione Installatore – CS600 Grado 3

In servizio operatore Installatore	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Installatore	NO	SI	SI[*]	NO

**NOTE:**  
Il comando di In Servizio dell'operatore Installatore è permesso solo agli operatori Supervisor di Livello 2.  
[\*] Mettendo fuori norma la centrale CS600 è possibile far eseguire ad un operatore di Livello 3 Supervisor il comando di In Servizio dell'installatore.

### 7.2.8. Gestione Installatore – CS600 Grado 2

In servizio operatore Installatore	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Installatore	NO	SI	SI[*]	NO

**NOTE:**

Il comando di In Servizio dell'operatore Installatore è permesso solo agli operatori Supervisor di Livello 2.

[\*] Mettendo fuori norma la centrale CS600 è possibile far eseguire ad un operatore di Livello 3 Supervisor il comando di In Servizio dell'installatore.

**7.2.9. Gestione Utenti Livello 3 – CS600 Grado 3**

In servizio operatore Livello 3	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Utenti Livello 3	NO	SI	SI[*]	NO

**NOTE:**

Il comando di In Servizio dell'operatore Installatore è permesso solo agli operatori Supervisor di Livello 2.

[\*] Mettendo fuori norma la centrale CS600 è possibile far eseguire ad un operatore di Livello 3 Supervisor il comando di In Servizio dell'installatore.

**7.2.10. Gestione Utenti Livello 3 – CS600 Grado 2**

In servizio operatore Livello 3	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Utenti Livello 3	NO	SI	SI[*]	NO

**NOTE:**

Il comando di In Servizio dell'operatore Installatore è permesso solo agli operatori Supervisor di Livello 2.

[\*] Mettendo fuori norma la centrale CS600 è possibile far eseguire ad un operatore di Livello 3 Supervisor il comando di In Servizio dell'installatore.

**7.2.11. Gestione CARICO dati da CS600 a Grado 3 → verso PK Security600**

Questa sezione si riferisce alla gestione del carico dei dati da parte del Software di configurazione PK Security 600 e del sistema di supervisione Monitor nei confronti della centrale CS600.

Allineamento/sincronizzazione dati	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Dati Installatore	NO	NO	SI*	SI
Programmazione	NO	NO	NO	SI
Altri dati	NO	NO	SI	SI

**NOTE:**

\* i dati dell'utente sono archiviati in modo criptato all'interno dei database del PKSecurity600 durante la fase di programmazione e allineamento dati.

### 7.2.12. Gestione CARICO dati da CS600 a Grado 2 → verso PK Security600

Questa sezione si riferisce alla gestione del carico dei dati da parte del Software di configurazione PKSecurity600 e del sistema di supervisione Monitor nei confronti della centrale CS600.

Allineamento/sincronizzazione dati	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Dati Installatore	NO	NO	SI*	SI
Programmazione	NO	NO	NO	SI
Altri dati	NO	NO	SI	SI

**NOTE:**  
\* i dati dell'utente sono archiviati in modo criptato all'interno dei database del PKSecurity600 durante la fase di programmazione e allineamento dati.

### 7.2.13. Gestione SCARICO dati da PK Security600 → verso CS600 a Grado 3

Questa sezione si riferisce alla gestione dello scarico dei dati da parte del Software di configurazione PKSecurity600 e del sistema di supervisione Monitor nei confronti della centrale CS600.

Allineamento/sincronizzazione dati	Grado 3 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Dati Installatore	NO	NO	SI*	SI*
Programmazione	NO	NO	NO	SI
Operatori e Associazioni	NO	NO	SI	SI
Descrizione, Gruppo, livello Operatori Liv. 3	NO	NO	SI	SI
Altri Parametri Operatori Liv. 3	NO	NO	SI	NO

**NOTE:**  
\* i dati dell'utente sono archiviati in modo criptato all'interno dei database del PKSecurity600 durante la fase di programmazione e allineamento dati.

### 7.2.14. Gestione SCARICO dati da PKSecurity600 → verso CS600 a Grado 2

Questa sezione si riferisce alla gestione dello scarico dei dati da parte del Software di configurazione PKSecurity600 e del sistema di supervisione Monitor nei confronti della centrale CS600.

Allineamento/sincronizzazione dati	Grado 2 EN50131			
	Livello 2 EN50131		Livello 3 EN50131	
	Standard	Supervisor	Supervisor	Installatore
Dati Installatore	NO	NO	SI*	SI*
Programmazione	NO	NO	NO	SI
Operatori e Associazioni	NO	NO	SI	SI
Descrizione, Gruppo, livello Operatori Liv. 3	NO	NO	SI	SI
Altri Parametri Operatori Liv. 3	NO	NO	SI	NO

**NOTE:**  
\* i dati dell'utente sono archiviati in modo criptato all'interno dei database del PKSecurity600 durante la fase di programmazione e allineamento dati.

## 7.3. Contact-ID

La CS600 attraverso il modulo M-Contact-ID è in grado di inviare verso un ricevitore digitale dei messaggi/codici che sono definiti e identificati come segue.

La tabella sotto identifica la suddivisione per linea e conseguente ID di riconoscimento.

	CPU	1 Linea	2 Linea	3 Linea	4 Linea
Ingressi <b>IND/ALI/RXE/AEI/LCD/CPU</b>	Da B00 a B50	Da 1 a 250	Da 251 a 500	Da 501 a 750	Da 751 a 999

### Metodo di calcolo ID:

- Ingressi 16 periferiche **IND/ALI**:  $[(\text{num\_perif} - 1) * 13 + \text{Num Ing}] = \text{valore compreso tra 001 e 208}$   
*Es: Linea 1, IND 14, Ingresso 3* →  $01.14.03 = 13 * 13 + 3 = \text{ID } 172$
- Ingressi 10 periferiche **LCD/RXE/AEI**:  $[(\text{num\_perif} - 21) * 2 + \text{Num Ing} + 210] = \text{valore compreso tra 211 e 230}$   
*Es: Linea 1, LCD 25, Ingresso 1* →  $01.25.01 = 4 * 2 + 1 + 210 = \text{ID } 219$
- Ingressi di centrale **CS600**:  $[(\text{num\_perif} - 1) * 8 + B00] = \text{valore compreso tra B00 e B50}$   
*Es: Linea 0, IND 2, Ingresso 3 (ing. 00.02.03)* =  $1 * 8 + 3 + B00 = B11$

Ingressi 16 periferiche **TAMPER**:  $(230 + \text{Num Ing}) = \text{valore compreso tra 231 e 247}$

Ingressi 10 periferiche **TAMPER**:  $(211 + \text{Num Ing}) = \text{valore compreso tra 211 e 230}$

Formato del messaggio: "1234 18 1,3 130 01 015 CHK"

Dove

1234 = Numero account dato dall'istituto di vigilanza da inserire in ogni Impianto

18 = Identificativo codice messaggio tipo Contact-ID (non modificabile)

1,3 = 3 ripristino e 1 attivazione

130 = Codice identificativo evento (vedi tabella Norma)

01 = Identificativo MacroZona programmata

015 = Identificativo Ingresso (ID ingresso vedi tabella sopra)

CHK = Checksum gestita dal sistema

Eventi associati agli ingressi delle IND:

Evento	1,3	XYZ (codice)	Descrizione
Ins/Dis	1,3	401	Open/Close by User
ISV/FSV	1,3	570	Zone/Sensor Bypass
Mancato inserimento	3	454	Failed to Close
InsParziale o con Ing Fsv	3	456	Partial Arm
Allarme generico (default)	1,3	130	BURG-Burglary-#
Guasti/Mascheramenti/Allarmi/MAN	1,3	XXX	Etichetta CID Ingresso

Tabella identificatrice codici Contact-ID in base al doc:

- SIA DC-05-1999.09
- Publication Order Number: 14085

Event	Data Type	Event	Data Type
<b>ALARMS</b>			
<b>Medical Alarms -100</b>		<b>General Alarm - 140</b>	
100 Medical	Zone	140 General Alarm	Zone
101 Personal Emergency	Zone	141 Polling loop open	Zone
102 Fail to report in	Zone	142 Polling loop short	Zone
		143 Expansion module failure	Zone
<b>Fire Alarms -110</b>		144 Sensor tamper	
		145 Expansion module tamper	
110 Fire	Zone	146 Silent Burglary	
111 Smoke	Zone	147 Sensor Supervision Failure	
112 Combustion	Zone		
113 Water flow	Zone	<b>24 Hour Non-Burglary - 150 and 160</b>	
114 Heat	Zone		
115 Pull Station	Zone	150 24 Hour Non-Burglary	
116 Duct	Zone	151 Gas detected	
117 Flame	Zone	152 Refrigeration	
118 Near Alarm	Zone	153 Loss of heat	
		154 Water Leakage	
<b>Panic Alarms -120</b>		155 Foil Break	
		156 Day Trouble	
120 Panic	Zone	157 Low bottled gas level	
121 Duress	User	158 High temp	
122 Silent	Zone	159 Low temp	
123 Audible	Zone	161 Loss of air flow	
124 Duress - Access granted	Zone	162 Carbon Monoxide detected	
125 Duress - Egress granted	Zone	163 Tank level	
<b>Burglar Alarms -130</b>		<b>SUPERVISORY</b>	
130 Burglary		<b>Fire Supervisory - 200 and 210</b>	
131 Perimeter			
132 Interior		200 Fire Supervisory	
133 24 Hour (Safe)		201 Low water pressure	
134 Entry/Exit		202 Low CO2	
135 Day/night		203 Gate valve sensor	
136 Outdoor		204 Low water level	
137 Tamper		205 Pump activated	
138 Near alarm		206 Pump failure	
139 Intrusion Verifier			

<b>TROUBLES</b>		341 Exp. Module Tamper	Zone
		342 Exp. Module AC Loss	Zone
<b>System Troubles -300 and 310</b>		343 Exp. Module self-test fail	Zone
		344 RF Receiver Jam Detect	Zone
300 System Trouble	Zone		
301 AC Loss	Zone	<b>Communication Troubles -350 and 360</b>	
302 Low system battery	Zone		
303 RAM Checksum bad	Zone	350 Communication trouble	Zone
304 ROM checksum bad	Zone	351 Telco 1 fault	Zone
305 System reset	Zone	352 Telco 2 fault	Zone
306 Panel programming changed	Zone	353 Long Range Radio xmitter fault	Zone
307 Self-test failure	Zone	354 Failure to communicate event	Zone
308 System shutdown	Zone	355 Loss of Radio supervision	Zone
309 Battery test failure	Zone	356 Loss of central polling	Zone
310 Ground fault	Zone	357 Long Range Radio VSWR problem	Zone
311 Battery Missing/Dead	Zone		
312 Power Supply Overcurrent	Zone	<b>Protection Loop -370</b>	
313 Engineer Reset	User		
		370 Protection loop	Zone
<b>Sounder / Relay Troubles -320</b>		371 Protection loop open	Zone
		372 Protection loop short	Zone
320 Sounder/Relay	Zone	373 Fire trouble	Zone
321 Bell 1	Zone	374 Exit error alarm (zone)	Zone
322 Bell 2	Zone	375 Panic zone trouble	Zone
323 Alarm relay	Zone	376 Hold-up zone trouble	Zone
324 Trouble relay	Zone	377 Swinger Trouble	Zone
325 Reversing relay	Zone	378 Cross-zone Trouble	Zone
326 Notification Appliance Ckt. # 3	Zone		
327 Notification Appliance Ckt. #4	Zone		
		<b>Sensor Trouble -380</b>	
<b>System Peripheral Trouble -330 and 340</b>			
		380 Sensor trouble	Zone
330 System Peripheral trouble	Zone	381 Loss of supervision - RF	Zone
331 Polling loop open	Zone	382 Loss of supervision - RPM	Zone
332 Polling loop short	Zone	383 Sensor tamper	Zone
333 Expansion module failure	Zone	384 RF low battery	Zone
334 Repeater failure	Zone	385 Smoke detector Hi sensitivity	Zone
335 Local printer out of paper	Zone	386 Smoke detector Low sensitivity	Zone
336 Local printer failure	Zone	387 Intrusion detector Hi sensitivity	Zone
		388 Intrusion detector Low sensitivity	Zone
<b>Event</b>	<b>Data Type</b>	389 Sensor self-test failure	Zone
337 Exp. Module DC Loss	Zone	391 Sensor Watch trouble	Zone
338 Exp. Module Low Batt.	Zone	392 Drift Compensation Error	Zone
339 Exp. Module Reset	Zone	393 Maintenance Alert	Zone

<b>OPEN/CLOSE/REMOTE ACCESS</b>			
<b>Open/Close -400, 440,450</b>		<b>Access control -420,430</b>	
400 Open/Close	User	421 Access denied	User
401 O/C by user	User	422 Access report by user	User
402 Group O/C	User	423 Forced Access	Zone
403 Automatic O/C	User	424 Egress Denied	User
404 Late to O/C (Note: use 453, 454 instead )	User	425 Egress Granted	User
405 Deferred O/C (Obsolete- do not use )	User	426 Access Door propped open	Zone
406 Cancel	User	427 Access point Door Status Monitor trouble	Zone
407 Remote arm/disarm	User	428 Access point Request To Exit trouble	Zone
408 Quick arm	User	429 Access program mode entry	User
409 Keyswitch O/C	User	430 Access program mode exit	User
441 Armed STAY	User	431 Access threat level change	User
442 Keyswitch Armed STAY	User	432 Access relay/trigger fail	Zone
450 Exception O/C	User	433 Access RTE shunt	Zone
451 Early O/C	User	434 Access DSM shunt	Zone
452 Late O/C	User		
453 Failed to Open	User	<b>BYPASSES / DISABLES</b>	
454 Failed to Close	User		
455 Auto-arm Failed	User	<b>System Disables -500 and 510</b>	
456 Partial Arm	User		
457 Exit Error (user)	User	501 Access reader disable	Zone
458 User on Premises	User		
459 Recent Close	User	<b>Sounder / Relay Disables -520</b>	
461 Wrong Code Entry	Zone		
462 Legal Code Entry	User	520 Sounder/Relay Disable	Zone
463 Re-arm after Alarm	User	521 Bell 1 disable	Zone
464 Auto-arm Time Extended	User	522 Bell 2 disable	Zone
465 Panic Alarm Reset	Zone	523 Alarm relay disable	Zone
466 Service On/Off Premises	User	524 Trouble relay disable	Zone
		525 Reversing relay disable	Zone
<b>Remote Access -410</b>		526 Notification Appliance Ckt. # 3 disable	Zone
		527 Notification Appliance Ckt. # 4 disable	Zone
411 Callback request made	User		
412 Successful download/access	User	<b>System Peripheral Disables -530 and 540</b>	
413 Unsuccessful access	User		
414 System shutdown command received	User	531 Module Added	Zone
415 Dialer shutdown command received	User	532 Module Removed	Zone
416 Successful Upload	Zone		

<b>Communication Disables -550 and 560</b>			
551 Dialer disabled	Zone	627 Program mode entry	Zone
552 Radio transmitter disabled	Zone	628 Program mode exit	Zone
553 Remote Upload/Download disabled	Zone	629 32 Hour Event log marker	Zone
<b>Bypasses -570</b>		<b>Scheduling -630</b>	
570 Zone/Sensor bypass	Zone	630 Schedule change	Zone
571 Fire bypass	Zone	631 Exception schedule change	Zone
572 24 Hour zone bypass	Zone	632 Access schedule change	Zone
573 Burg. Bypass	Zone		
574 Group bypass	User	<b>Personnel Monitoring -640</b>	
575 Swinger bypass	Zone		
576 Access zone shunt	Zone	641 Senior Watch Trouble	Zone
577 Access point bypass	Zone	642 Latch-key Supervision	User
<b>TEST / MISC.</b>		<b>Misc. -650</b>	
<b>Test/Misc. -600, 610</b>		651 Reserved for Ademco Use	Zone
		652 Reserved for Ademco Use	User
601 Manual trigger test report	Zone	653 Reserved for Ademco Use	User
602 Periodic test report	Zone	654 System Inactivity	Zone
603 Periodic RF transmission	Zone		
604 Fire test	User		
605 Status report to follow	Zone		
606 Listen-in to follow	Zone		
607 Walk test mode	User		
608 Periodic test - System Trouble Present	Zone		
609 Video Xmitter active	Zone		
611 Point tested OK	Zone		
612 Point not tested	Zone		
613 Intrusion Zone Walk Tested	Zone		
614 Fire Zone Walk Tested	Zone		
615 Panic Zone Walk Tested	Zone		
616 Service Request	Zone		
<b>Event Log -620</b>			
621 Event Log reset	Zone		
622 Event Log 50% full	Zone		
623 Event Log 90% full	Zone		
624 Event Log overflow	Zone		
625 Time/Date reset	User		
626 Time/Date inaccurate	Zone		

## 8. Utility

### 8.1.1. Integrazione Euronet

La centrale CS600 può essere integrata, gestita e supervisionata da un sistema EuroNet.

L'integrazione avviene attraverso rete Ethernet (LAN/WAN), senza abilitazioni di licenze, hardware aggiuntivo, ma con delle semplici configurazioni eseguibile attraverso PkSecurity600.

La CS600 in configurazione integrata, invia/riceve dalla centrale E-net dei comandi/attivazioni che sono configurati nelle proprietà delle ZoneUscita e/o Uscite Digitali.

La comunicazione tra i due sistemi è costantemente monitorata attraverso dei controlli sui tempi di risposta delle informazioni scambiate.

La CS600 se non riceve risposta da parte della E-net entro le tempistiche previste (max 10 sec) genera un evento di “Guasto comunicazione con CPU di rete”.

Questo significa che dalla centrale E-net non ha ricevuto nessuna risposta durante la fase di comunicazione

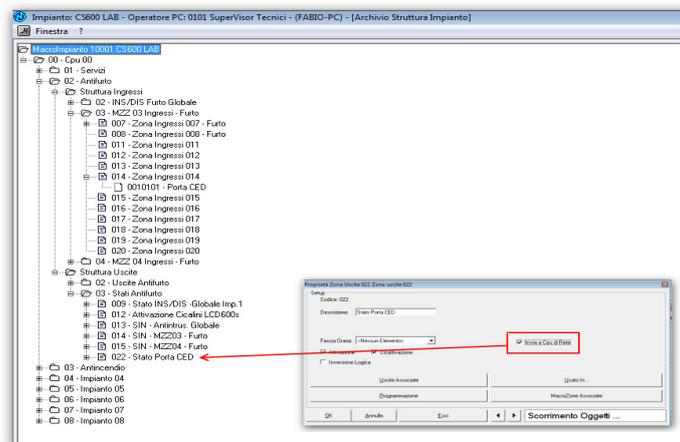
ESEMPIO: In un impianto dove c'è la necessità di segnalare lo stato/apertura di una porta (tramite Led, Lampeggianti, Luci o altro) collegate alla centrale E-net e non alla CS600 è possibile eseguirlo in questo modo.

Lo stato di porta aperta viene dato da un Contatto Magnetico collegato ad una IND8/4 associato ad una Zona Ingressi (es Szz 014 - ingresso 00110101) .

Per inviare alla centrale E-net l'informazione di cambio di stato della zona interessata è necessario abilitare nella ZonaUscita (es Szo 022) che riporta lo stato della Zona Ingressi (Szz 014, quella da monitorare) il Flag “Invia a CPU di Rete”.

Nella centrale E-net sarà necessario verificare che la ZonaUscita Uscita 022 sia disponibile e che venga utilizzata per attivare le uscite interessate (Luci, Led, Lampeggianti ecc) .

Da questo momento in poi la CS600 invierà alla E-net sia lo stato di attivazione che di riposo della ZonaUscita 022,



NOTA:

Per il corretto funzionamento dell'interazione è fondamentale che gli ID oggetti nelle due centrale siano uguali.

- ZonaUscita 022 - CS600 = ZonaUscita 022 - E-net
- UscitaDigitale 00140003 – CS600 = UscitaDigitale 0014003 – E-net

Non è possibile eseguire comandi direttamente su MacroZone, Zone Ingresso e Ingressi Digitali

### 8.1.2. Come programmare antintrusione dall'impianto base

La centrale CS600 viene fornita corredata di Software PK security600 utilizzato per la programmazione e configurazione completa del sistema.

Il Software al suo interno contiene un database di un impianto funzionante e già configurato per essere velocemente scaricato e messo in servizio.

Il programma 00001\_V2 ha già configurato tutte le logiche funzionali di un impianto Antintrusione, quindi la messa in servizio di una centrale risulta semplice e veloce.

Le configurazioni aggiuntive da eseguire a carico dell'installatore sono esclusivamente quelle di inserire le descrizioni degli oggetti presenti nel sistema e verificare attraverso il menù "verifica Struttura" che le interconnessioni della sensoristica di campo sia stata realizzata a regola d'arte.

### 8.1.3. Configurare un Operatore con Badge/Radiocomando

La centrale CS600 ha la possibilità di gestire fino a 1000 operatori, questi possono utilizzare per essere riconosciuti dal sistema, un PIN, un TRASPONDER, un RADIOCOMANDO.

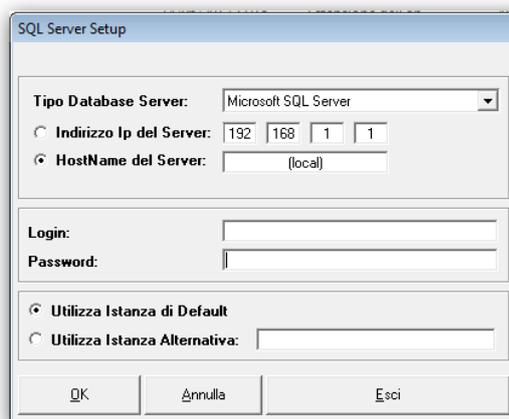
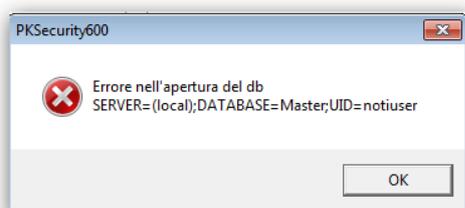
Ad eccezione del PIN gli operatori possono avere associato più Transponder di prossimità e Radiocomandi.

La configurazione degli operatori avviene in due fasi, la prima inerente ai gruppi, alle associazioni e ai profili che viene realizzata mediante software PKSecurity600 dal menù "Profili e Utenti".

La seconda invece attraverso LCD600S o RXE per la registrazione del Transponder e/o Radiocomando.

### 8.1.4. Parametri Accesso DataBase

E' possibile che dopo un aggiornamento automatico di Windows il servizio SQL Server Notifier venga arrestato e l'utente SQLADMIN venga temporaneamente disabilitato dal Sistema Operativo. Questa condizione genera all'avvio del PKSecurity600 una finestra di richiesta di inserimento parametri di connessione (User, Password, Istanza e Indirizzo server)



Chiudere le finestre sopra e verificare nei servizi di Windows lo stato del servizio SQLNotifier, e i parametri dell'operatore SQLAdmin come riportato nel capito iniziale d'installazione software.

Una volta eseguite tutti i passaggi sopra citati, entrare nella directory

C:\Programmi\notifier\PkSecurity600 verificare la presenza del file SQL.ini ed eliminarlo, e riavviare l'applicazione PKSecurity600.

NOTIFIER international offices



20097  
San Donato Milanese  
(MILANO)  
Via Grandi, 22

Tel: 02/518971  
Fax: 02/5189730  
www.notifier.it  
E-mail: notifier@notifier.it  
A Honeywell company



Every care has been taken in the preparation of this data sheet but no liability can be accepted for the use of the information therein. Design features may be changed or amended without prior notice.

**NOTIFIER ITALIA S.r.l.**

NOTIFIER ITALIA S.r.l. - A socio unico - 20097 San Donato Milanese (MI) - Via Grandi, 22 - Tel.: 02/518971 - Fax: 02/5189730 - E-mail: notifier@notifier.it Capitale Sociale € 2.700.000,00 i.v. - C.C.A.A. 1456164 - Trib. Milano Reg. Soc. 348608 - Vol. 8549 Fasc. 8 Codice Fiscale 05108880153 Partita IVA IT 11319700156 (informativa privacy art. 3 Digs 196/03)

**UFFICI REGIONALI:**

**Uffici Regionali:** 10143 **Torino** - Corso Potenza, 6 - Tel.: 011/0650611 - Fax: 011/4531183 E-mail: notifier.torino@notifier.it - 35010 **Limena (PD)** Via IV Novembre, 6/c Int. 9 - Tel.: 049/7663511 - Fax: 049/7663550 E-mail: notifier.padova@notifier.it 40050 **Funo di Argelato (BO)** - Asta Servizi, Bl. 3B, Gall. B n. 85, Centergross - Tel.: 051/0432211 - Fax: 051/6647638 - E-mail: notifier.bologna@notifier.it - 50136 **Firenze** Via B. Telesio, 15 - Tel.: 055/696706 - Fax: 055/6529294 - E-mail: toscana@notifier.it - 00118 **Roma** - Via Del Casale Santarelli, 51 - Tel.: 06/7988021 Fax: 06/79880250 - E-mail: notifier.roma@notifier.it - 80143 **Napoli** - Via G. Porzio, 4 - Centro Direzionale, Isola E2, Scala B, Piano 5° - Int. 19 - Tel.: 081/19493111 Fax: 081/7879159 - E-mail: notifier.napoli@notifier.it - 70125 **Bari** - Via Della Costituente, 29 - Tel.: 080/6180700 - Fax: 080/5648114 - E-mail: notifier.bari@notifier.it - 95126 **Catania** - Viale A. De Gasperi, 187 - Tel.: 095/2279511 - Fax: 095/7120753 - E-mail: notifier.catania@notifier.it

M-8253.2-CS-600-ITA Rev A.16 10/2013