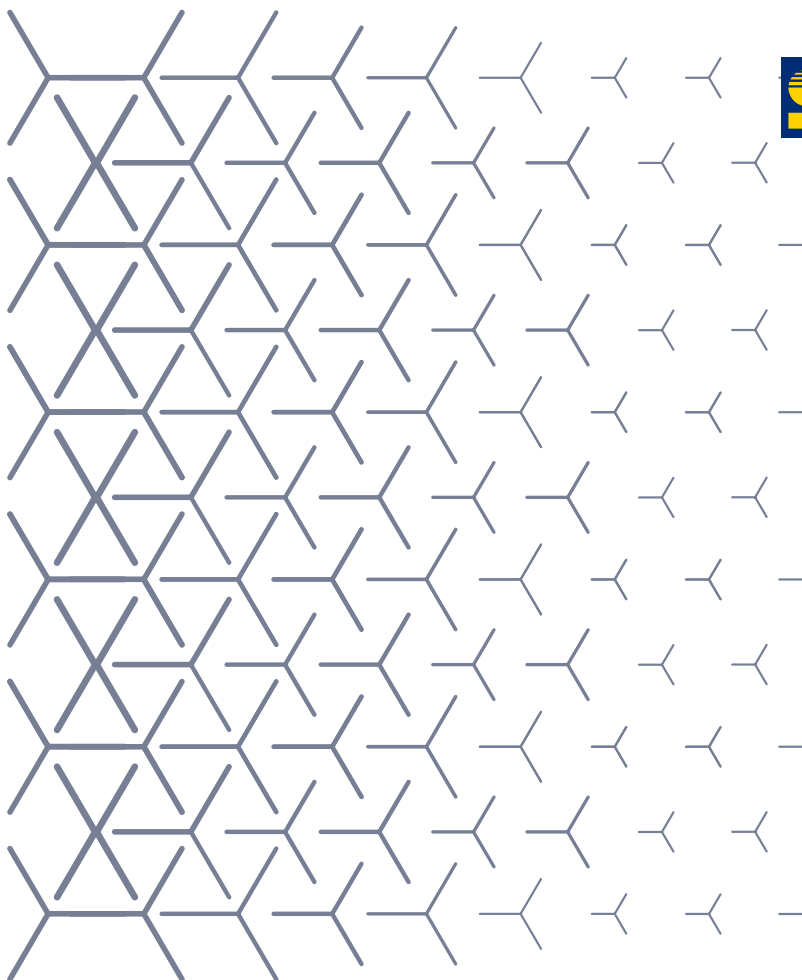
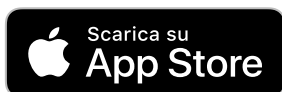




DG-432

MANUALE DI INSTALLAZIONE E PROGRAMMAZIONE



CE
23494.8

Sommario

1. Generalità	1
1.1 Generalità	1
1.2 Funzione del manuale	1
1.3 Termini convenzionali utilizzati nel manuale	1
1.4 Definizioni e abbreviazioni	1
2. Introduzione e caratteristiche	2
2.1 Cos'è il sistema antintrusione DOGMA	2
2.2 Caratteristiche della Centralina	2
2.2.1 Comunicatore	3
2.3 Comunicazione wireless a 868MHz (BiTech)	3
2.3.1 Elevata sicurezza	3
2.3.2 Consumi ridotti e velocità di risposta	3
2.3.3 Facilità di installazione e manutenzione	3
2.4 Sensori wireless compatibili con centralina DOGMA	4
2.4.1 BT-DTCX, BT-DTVX, BT-MDCX, BT-MDWX sensore infrarosso da interno doppia tecnologia con antimascheramento e telecamera	4
2.4.2 BT-IRWX sensore infrarosso da interno standard	4
2.4.3 BT-MX2P, BT-MX2PC, BT-MX3T, BT-MX3TC sensore infrarosso da esterno doppio PIR e doppia tecnologia con antimascheramento e telecamera	4
2.4.4 BT-IRE2 sensori da esterno	4
2.4.5 BT-CMXW sensore magnetico multifunzionale	5
2.4.6 BT-CMXE sensore magnetico multifunzionale economico	5
2.4.7 BT-SMK2 sensore di fumo wireless	5
2.4.8 BT-KPXW tastiera wireless	5
2.4.9 BT-KT radiocomando	5
2.4.10 BT-ER2 espansioni wireless	5
2.4.11 BT-NI Generatore di fumo NIMBUS	6
2.4.12 IF-URFOG	6
2.4.13 BT-ALMA sirena da esterno	6
2.4.14 BT-REP2 ripetitore di segnale radio	6
2.5 Accessori del sistema Sicep BiTech DOGMA	6
2.5.1 BT-WIFI - Interfaccia WiFi	6
2.6 Descrizione hardware	7
2.7 Conformità di Conformità UE semplificata	8
3. Caratteristiche elettriche e dimensionali centralina	9
4. Gestione sistema di sicurezza	10
4.1 Aree	10
4.1.1 Inserimento Totale - Perimetrale/Notte	10
4.1.2 Tempi Ingresso / uscita Aree: zone ritardate	10
4.1.3 Auto esclusione zone	10
4.1.4 Riattivazione automatica delle zone/dispositivi esclusi	11
4.1.5 Disabilitazione zone	11
4.1.6 Varchi	11
4.1.7 Aree di competenza - Aree predefinite	11
4.1.8 Condivisione Aree	12

4.1.9	Area 24h	13
4.1.10	Funzione Reinserimento Automatico Aree	13
4.2	Accessi e Password	13
4.2.1	Blocco Tastiera	14
4.2.2	Blocco Accesso da Remoto	14
4.2.3	Disinserimento con Coercizione	14
4.3	Eventi (descrizione dettagliata)	14
4.4	Programmatore orario	20
4.5	Scenari	20
4.6	Sirena	20
4.7	Uscita On Board	20
4.8	Riduzione dei Falsi Allarmi	21
4.9	Comunicatore	21
4.9.1	Comunicazioni verso il gestionale MvsNET	21
4.9.2	Comunicazione verso gestionale con protocollo standard SIA-IP DC09	21
4.9.3	Comunicazioni verso gli utenti	21
4.9.4	Configurazione dei dispositivi di rete	22
4.10	Cloud Sicep	22
4.11	Gestione della centralina da MvsNET	23
4.12	Gestione Teleassistenza	23
4.12.1	Teleassistenza tramite LAN	23
4.12.2	Teleassistenza tramite LTE/GPRS	23
4.13	Il protocollo di comunicazione radio BiTech	23
4.13.1	Come funziona	23
4.13.2	Gestione dei dispositivi registrati	24
4.13.3	Codice Impianto o Serial Number	24
4.13.4	Test qualità del collegamento radio	24
4.13.5	Test del livello di batteria dei dispositivi radio	24
5.	Installazione	25
5.1	Scelta del luogo per l'installazione della centralina	25
5.2	Come aprire e chiudere la centralina	25
5.3	Installazione dispositivi opzionali	25
5.3.1	Installazione scheda interfaccia BT-WIFI	25
5.4	Fissaggio e cablaggio Centralina DOGMA	26
5.4.1	Fissaggio magneti antistrappo	26
5.4.2	Cablaggio centralina	26
5.5	Installazione dispositivi wireless	27
5.6	Registrazione dei dispositivi wireless	27
5.6.1	Registrazione da software Sicep Cloud Connect	27
5.6.2	Registrazione da App SICEP	28
5.6.3	Registrazione Tastiera BT-SKW	28
5.6.4	Registrazione sensore di fumo BT-SMK2	28
5.6.5	Registrazione Radiocomando BT-KT	28
5.7	Cancellazione di un dispositivo wireless dalla centralina	29

6. Programmazione	30
6.1 App SICEP	30
6.1.1 Login	30
6.1.2 Prima configurazione	31
6.1.3 Pagina principale HOME	32
6.1.4 Icone di stato	33
6.1.5 Pagina Impostazioni Centralina	33
6.2 Sicep Cloud Connect	33
6.2.1 Login	33
6.2.2 Collegamento locale tramite porta USB	33
6.2.3 Primo collegamento con cavo USB	34
6.2.4 Primo collegamento tramite LAN	34
6.2.5 Collegamento da remoto tramite LAN/WiFi	34
6.2.6 Requisiti centralina per l'accesso da parte installatore	34
6.2.7 Collegamento da remoto in LTE/GPRS	34
6.3 Parametri di programmazione con software Sicep Cloud Connect	35
6.3.1 Pagina Sinottico	35
6.3.2 Pagina Sistema	36
6.3.3 Aree	40
6.3.4 Pagina Utenti	41
6.3.5 Pagina Ingressi	45
6.3.6 Pagina Zone AND	48
6.3.7 Pagina Dispositivi RF	50
6.3.8 Parametri di configurazione specifici per ogni dispositivo.	54
6.3.9 IpCamera	69
6.3.10 Pagina Comandi	72
6.3.11 Pagina Comunicatore	74
6.3.12 Cloud	83
6.3.13 Pagina Eventi	84
6.3.14 Pagina Controllo dissuasori	88
6.3.15 Pagina Programmi	90
6.3.16 Pagina Scenari.	92
6.3.17 Pagina Storico	93
6.4 Impostazioni Cloud Sicep	93
7. Operazioni speciali	94
7.1 Riprogrammare la centralina ai valori di default (impostazioni di fabbrica)	94
7.2 Aggiornamento firmware	94
7.3 Installazione dei driver USB	94

1. Generalità

1.1 Generalità

Si invita prima di tutto a leggere attentamente le Informazioni sulla Sicurezza che sono state fornite in formato cartaceo a corredo del prodotto al momento della vendita.

Sicep decina ogni responsabilità in caso di non osservanza delle Informazioni sulla Sicurezza presenti sul prodotto.

1.2 Funzione del manuale

Il prodotto ed il presente manuale devono essere esaminati prima di effettuare qualsiasi operazione.

Le informazioni contenute in questo manuale sostituiscono quanto precedentemente pubblicato. Sicep si riserva il diritto di modificare e di effettuare miglioramenti sul prodotto in qualsiasi momento e senza alcun preavviso.

Nessuna parte di questo documento può essere riprodotta in alcuna forma senza autorizzazione scritto di Sicep.



1.3 Termini convenzionali utilizzati nel manuale

ESEMPIO	Riporta un caso particolare utile a chiarire ulteriormente il concetto
NOTA.	Riporta delle considerazioni aggiuntive utili a chiarire ulteriormente il particolare argomento
ATTENZIONE!	Identifica una situazione da gestire con attenzione; eseguire attentamente le istruzioni in quanto si potrebbe pregiudicare il corretto funzionamento dell'apparato
PERICOLO! 	Identifica una condizione o una pratica che potrebbe arrecare un danno fisico o provocare la perdita di vita

1.4 Definizioni e abbreviazioni

Area	Si intende il termine tecnico relativo alla centralina che indica un raggruppamento di zone filari o dispositivi radio
Centralina	Si riferisce al prodotto DOGMA.
Default	Indica il valore che hanno i parametri nella configurazione di fabbrica.
Evento	Qualsiasi variazione di uno degli stati logici interni o esterni alla centralina; esso può provocare un'azione locale (es. attivazione della sirena) e/o generare un allarme o un ripristino che può essere trasmesso dal comunicatore.
Firmware	Indica il software di gestione della centralina, memorizzato nella memoria non volatile della scheda logica.
	MvsNET: Sistema realizzato da Sicep per la gestione degli allarmi in Centrale Operativa.
	Sicep Cloud Connect: Software Client per PC sviluppato da Sicep per l'installazione, la configurazione e l'aggiornamento dei prodotti Sicep.
Zona o Ingresso	Indica un morsetto di ingresso per il collegamento a un sensore.

Dispositivo	Un sensore o un dispositivo wireless connesso alla centrale d'allarme.
	BiTech: Protocollo proprietario di comunicazione radio bidirezionale fra la centralina ed i dispositivi wireless
	Vtech: Protocollo proprietario di comunicazione radio bidirezionale per l'invio delle immagini di videoverifica.
	Sicep: Applicazione per smartphone o tablet per sistemi operativi iOS e Android
TAG e CARD	Dispositivo portatile con tecnologia RFID in dotazione all'utente per la gestione del sistema di allarme

2. Introduzione e caratteristiche

2.1 Cos'è il sistema antintrusione DOGMA

Dogma è un sofisticato sistema di sicurezza facilmente installabile che garantisce una protezione totale della proprietà. Il sistema DOGMA si compone di una centrale antifurto con interfaccia wireless completamente bidirezionale con protocollo BiTech, estremamente compatta, con possibilità di video-verifica integrata su richiesta o allarme (tecnologia V-Tech). La video-verifica permette di inviare i fotogrammi dell'evento direttamente sul cellulare dell'utente oppure in Centrale Operativa di monitoraggio consentendo di verificare la situazione ed autorizzare l'invio della pattuglia e/o delle forze dell'ordine. La centrale DOGMA rappresenta l'epicentro dell'intero sistema, un HUB capace di monitorare tutti i dispositivi wireless registrati e garantire un elevato standard di sicurezza. Attraverso i suoi organi di comando e la App SICEP è possibile gestire il sistema DOGMA in maniera semplice, efficace e funzionale. DOGMA può comunicare informazione alle Centrali Operative degli Istituti di Vigilanza o agli utenti privati, attraverso vari canali di comunicazione ed in varie modalità: IP, LTE/GPRS, notifiche a mezzo Cloud, e-mail, SMS.

2.2 Caratteristiche della Centralina

Le caratteristiche della centralina DOGMA possono essere così riassunte:

- 4 aree indipendenti, che possono gestire anche zone/dispositivi condivisi
- 2 tipologie di inserimento per ciascuna area (Totale, Perimetrale/Notte)
- Programmatore orario su base annuale con definizione giornaliera che consente un elevato grado di personalizzazione secondo le proprie esigenze (con gestione delle festività)
- Area 24h
- Tempi Ingresso/Uscita programmabili separatamente per ciascuna area
- Auto esclusione zone (inserimento forzato)
- Esclusione manuale zone (disabilitazione)
- Reinserimento automatico a tempo delle aree
- 1 uscita programmabile open collector, statica o impulsiva
- Controllo motori per apertura/chiusura tapparelle, tende ecc.
- Test batteria continuo e periodico per la verifica dell'efficienza della stessa.
- 28 dispositivi radio fra sensori infrarossi, magnetici, tastiere LCD, lettori RFID, sensori fumo, sirene, espansioni radio.
- Funzioni di test per l'utente: Walk Test sensori, test sirena, richiesta immagine video dai sensori BT-DTCX / BT-MDCX.
- 4 IpCamera Dahua serie WizSense con AI e per rilevazione Motion Detector programmabile per eventi Furto, Allarme 24H o Tecnologico.
- 4 ripetitori radio (REP) con possibilità di doppio salto

- Funzione Rilevazione Acccecamento radio
- 16 utenti (di cui uno Amministratore) più 2 utenti speciali: Installatore, Vigilanza
- Gestione dei varchi tramite CODICI, PASSWORD, TAG, CARD.
- Funzioni Incendio, Soccorso e Panico
- Storico Eventi contenente fino a 1024 eventi, consultabile da App SICEP o software Sicep Cloud Connect.
- Configurazione tramite software Sicep Cloud Connect: locale / remoto, USB/ Ethernet/WiFi / LTE
- App SICEP per Android e iOS, scaricabili gratuitamente dallo store.
- Alimentatore switching da 3W
- Sirena interna piezoelettrica
- Contenitore plastico con Tamper sull'apertura e antistrappo
- Collegamento al PC: porta USB integrata (porta Device) / Ethernet / Wi-Fi (opzionale)
- Aggiornamento firmware da remoto

2.2.1 Comunicatore

- 8 destinatari di tipo utente, con protocollo SMS Testo, e-mail, chiamata con squillo.
- Destinatario Centrale operativa (MvsNet o standard SIA-IP DC09), con gestione dell'invio multivettore: LAN (Ethernet/Wi-Fi), SIA-IP Contact-ID su IP (protocolli SIA DC09/SIA DC05), LTE/GPRS, SMS dati
- 74 eventi di sistema di cui 8 programmabili
- Teleassistenza tramite vettori LAN e LTE/GPRS

2.3 Comunicazione wireless a 868MHz (BiTech)

2.3.1 Elevata sicurezza

Tutti i dispositivi radio, in caso di mancata conferma da parte della centralina effettuano molteplici tentativi di trasmissione in modo da assicurare la riuscita della comunicazione. E' riconosciuta l'assenza prolungata di comunicazioni di ciascun dispositivo con un tempo programmabile da 20 a 720 minuti, inoltre un apposito controllo rileva i tentativi di acccecamento sulla rete radio.

Le comunicazioni fra i dispositivi wireless e la centralina avvengono mediante un protocollo proprietario con crittatura dinamica ad alta velocità; tale tecnologia consente tempi di trasmissione estremamente brevi, assenza di collisioni e distribuzione ottimale del traffico radio.

2.3.2 Consumi ridotti e velocità di risposta

Con la tecnologia bidirezionale BiTech è stato possibile ridurre notevolmente i consumi; ogni sensore infatti resta "a riposo" quando l'area di appartenenza è disinserita, allungando così il tempo medio di durata della batteria. All'inserimento dell'impianto tutti i sensori vengono riattivati nel giro di pochi secondi, assicurando una prontezza equiparabile ad un classico impianto filare.

2.3.3 Facilità di installazione e manutenzione

L'installazione dei sensori radio è rapida e semplice: una volta registrati sull'impianto, la programmazione dei parametri si effettua dalla centralina. I parametri operativi possono essere modificati in qualsiasi momento, anche da remoto (per esempio per modificare la sensibilità di un sensore); in questo modo la manutenzione è molto semplificata ed evita di dover tornare fisicamente sull'impianto.

Il test di installazione permette di stabilire in fase di installazione la qualità del segnale radio; può essere eseguito comunque in qualsiasi momento. Inoltre per ciascun sensore, sono conteggiate tutte le comunicazioni fornendo delle statistiche settimanali in modo da poter tenere sotto controllo tutta la rete radio e rilevare i malfunzionamenti.

2.4 Sensori wireless compatibili con centralina DOGMA

Ogni centralina DOGMA dispone di un numero identificativo assegnato in modo univoco e non modificabile (Serial Number). Questo numero codifica la rete radio e fa sì che ogni sensore con tecnologia radio BiTech registrato sull'impianto, possa funzionare solo su questo. I sensori apprendono il numero dell'impianto in fase di registrazione.

2.4.1 BT-DTCX, BT-DTWX, BT-MDCX, BT-MDWX sensore infrarosso da interno doppia tecnologia con antimascheramento e telecamera



Questo dispositivo è un sensore infrarosso wireless doppia tecnologia, integra cioè un rivelatore termico passivo (PIR) e un rivelatore di movimento a microonde. Una telecamera incorporata scatta automaticamente fino a 5 fotogrammi quando viene rivelata un'intrusione; l'allarme è valido quando sia l'infrarosso che la microonda hanno segnalato la condizione di allarme. Il sensore dispone di un illuminatore a LED bianchi ed è dotato di funzione anti mascheramento.

Questa linea di sensori sono disponibili nelle seguenti versioni:

- BT-DTCX doppia tecnologia + Anti-mask e telecamera grandangolare
- BT-DTWX doppia tecnologia + Anti-mask
- BT-MDCX solo infrarosso + Anti-mask e telecamera grandangolare
- BT-MDWX solo infrarosso + Anti-mask

Il sensore è alimentato da una o due batterie al Litio da 3,6V e ha un' autonomia tipica di 2 anni in base all'utilizzo.

2.4.2 BT-IRWX sensore infrarosso da interno standard



È un sensore infrarosso passivo con portata 12m. L'elaborazione digitale del segnale di rilevamento rende il dispositivo particolarmente immune ai falsi allarmi. Sono disponibili più tipi di lenti in funzione dell'utilizzo. Il sensore è alimentato da una batteria al Litio da 3,6V e ha un'autonomia stimata di 2 anni.

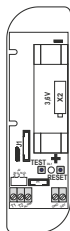
2.4.3 BT-MX2P, BT-MX2PC, BT-MX3T, BT-MX3TC sensore infrarosso da esterno doppio PIR e doppia tecnologia con antimascheramento e telecamera



I sensori della serie MATRIX (BT-MX) sono proposti in un'ampia gamma di versioni che integrano diverse tecnologie di rilevamento (PIR, MW e video-verifica), la cui combinazione permette una sofisticata analisi dell'ambiente monitorato.

Il sensore è alimentato da due o tre batterie al Litio da 3,6V e ha un' autonomia stimata che va da 2 a 5 anni in base al modello ed all'utilizzo.

2.4.4 BT-IRE2 sensori da esterno



Sono sensori infrarosso per esterno disponibili in più modelli. Ciascun sensore è alimentato da una batteria al litio da 3,6V AA.

Tutti questi sensori sono ottimizzati per l'uso in esterno e sono quindi particolarmente immuni ai falsi allarmi. In questi sensori alcuni parametri come la sensibilità, il numero di impulsi e la geometria del fascio possono essere modificati solo intervenendo sul sensore stesso, facendo riferimento al manuale di istruzioni fornito con il sensore stesso.

In ognuno di questi sensori è presente il modulo di comunicazione radio BiTech mod. BT-IRE2 alimentato da una batteria al Litio da 3,6V e ha un'autonomia stimata di 2 anni.

2.4.5 BT-CMXW sensore magnetico multifunzionale



Contatto magnetico radio con sensore inerziale (accelerometro) integrato.

Ogni sensore aggiunge 2 ingressi alla centralina configurabili per ingressi NO, NC e per ingressi conta-impulsi (sensori Tapparella e Inerziali esterni), senza circuiti ausiliari. Dispone di protezione Tamper e antirimozione.

Alimentato da batteria Litio CR123A

2.4.6 BT-CMXE sensore magnetico multifunzionale economico

Contatto magnetico radio. Ogni sensore aggiunge 2 ingressi alla centralina per il collegamento ad un contatto ausiliario N.C.

Dispone di protezione Tamper e antirimozione.

Alimentato da batteria Litio CR123A.

2.4.7 BT-SMK2 sensore di fumo wireless



Sensore autonomo di fumo di tipo a camera ottica (effetto Tyndall) che permette di rilevare un principio d'incendio.

È alimentato da una batteria da al Litio da 3,6V.

ATTENZIONE!

Questo rilevatore di fumo ha la funzione di ausilio al sistema antifurto segnalando eventi che possono essere connessi ad attività criminose quali l'utilizzo di strumenti a fiamma (lancia termica, fiamma ossidrica) e/o strumenti in grado di generare calore senza sviluppo di fiamma viva, ma con produzione di fumo. Non va, quindi, considerato come componente di un sistema antincendio.

2.4.8 BT-KPXW tastiera wireless



Tastiera wireless alimentata a batterie.

La tastiera dispone di LED di stato e di lettore Tag RFID integrato e permette l'esecuzione di tutte le normali operazioni di gestione dell'impianto (inserimento e disinserimento delle aree). Dispone di 4 led di servizio per le segnalazioni visive.

2.4.9 BT-KT radiocomando



È un radiocomando bidirezionale da utilizzare come organo di comando per la centralina che può operare su una o più aree. È dotato di pulsanti per le operazioni di inserimento totale e perimetrale/notte, disinserimento, e 4 combinazioni di pulsanti configurabili, più alcuni led per la visualizzazione dello stato delle aree nonché per segnalare condizioni di anomalia (zone in allarme, batteria scarica). Ai pulsanti configurabili può essere associato un evento programmabile sia se premuti singolarmente sia premuti in combinazione con il tasto disinserimento. L'alimentazione del radiocomando avviene tramite una batteria a 3V di tipo CR2032 che garantisce 2 anni di autonomia (uso tipico).

2.4.10 BT-ER2 espansioni wireless



Questo modulo viene visto come una espansione di Ingressi/Uscite nel sistema radio BiTech. Ogni contatto aggiunge due ingressi configurabili a cui possono essere collegati via cavo contatti magnetici, sensori per tapparelle, sensori inerziali ecc. e due uscite anch'esse configurabili e utilizzabili per l'attivazione di tapparelle, tende, cancelli, luci ecc. Nella centralina possono essere installati 8 moduli di espansione radio. Il modulo può essere alimentato dalla rete elettrica da 100 a 240Vac 50-60Hz, oppure mediante batteria al litio da 3,6 V. E' anche possibile alimentare da rete il modulo e lasciare la batteria al litio come backup in assenza di rete elettrica.

2.4.11 BT-NI Generatore di fumo NIMBUS



NIMBUS è un dispositivo di dissuasione per sistemi di allarme che fa uso di un fumogeno per proteggere gli ambienti contro ogni tentativo di furto, innalzando il livello di efficacia del sistema di sicurezza. È in grado di saturare un ambiente di 100 metri cubi in 35 secondi. Il dispositivo viene alimentato tramite due batterie al litio da 3,6V che garantiscono un'autonomia di 2 anni. La centralina può gestire massimo 8 fumogeni. Dispone di una sirena interna per intensificare l'effetto panico, della doppia conferma per evitare attivazione accidentali, attivazione anche da telecomando. Consultare il manuale allegato per ulteriori informazioni e programmazione.

2.4.12 IF-URFOG

Questa interfaccia permette la gestione di un dissuasore per sistemi di allarme di tipo nebbiogeno. Consultare il manuale del produttore per caratteristiche ed utilizzo.

2.4.13 BT-ALMA sirena da esterno



È una sirena da esterno per centrali BiTech. Alimentata da 2 batterie al Litio 3V 2800mA con connettore, ha una potenza sonora di 110dB(A) a 1m. Include le protezioni per Tamper sull'apertura del contenitore e sulla rimozione, rilevamento schiuma, controllo temperatura e protezione antiscazzo.

2.4.14 BT-REP2 ripetitore di segnale radio



Il sistema radio BiTech permette l'utilizzo di appositi ripetitori radio "REP" per raggiungere facilmente anche dispositivi posti in zone sfavorevoli rispetto alla centralina. La centralina può utilizzare fino a 4 BT-REP2 utilizzabili anche come doppio salto. Il BT-REP2 consente di ripetere segnali radio (BiTech) e video (VTech). Può essere alimentato da rete elettrica a 230Vac o tramite collegamento con BUS RS-485 alta velocità. Comprende una batteria di backup agli ioni di litio ricaricabile da 3,7V 1100mAh.

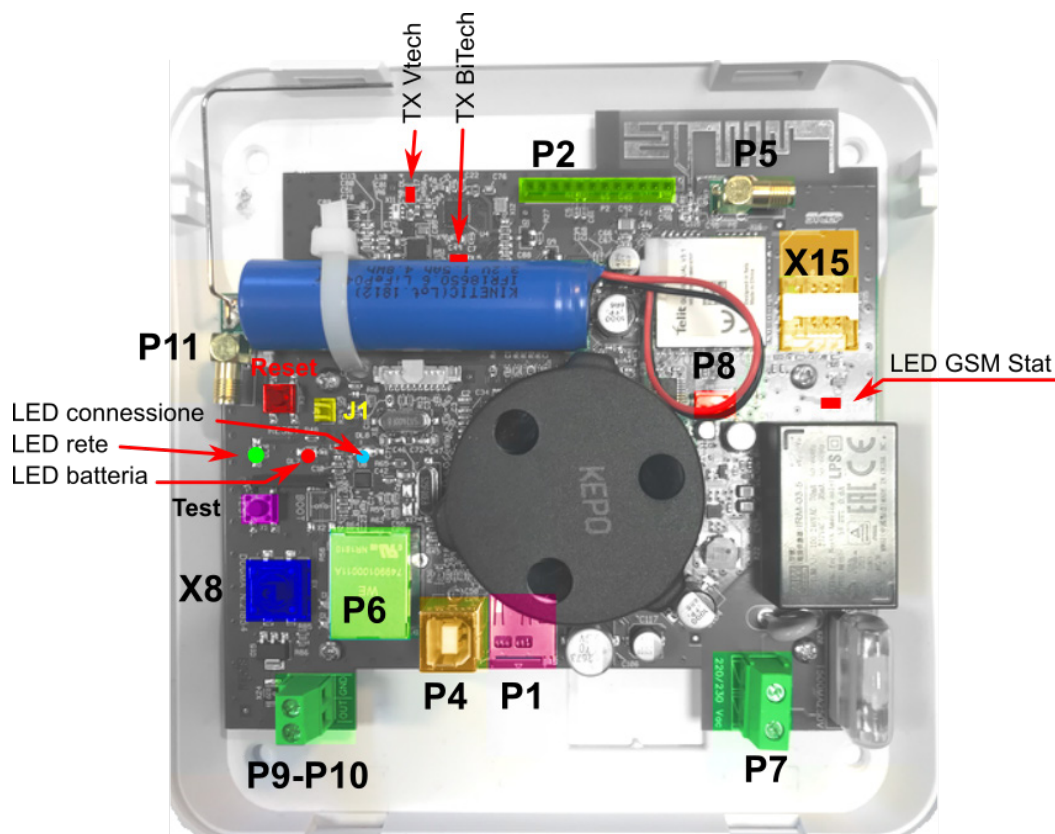
2.5 Accessori del sistema Sicep BiTech DOGMA

2.5.1 BT-WIFI - Interfaccia WiFi

Questo modulo consente un collegamento ad Internet alternativo alla connessione Ethernet tramite cavo. Per il suo utilizzo è necessario un Access Point in grado di supportare i protocolli di cui alle specifiche.

Una volta che il modulo viene abilitato, la connessione Ethernet viene esclusa da qualsiasi utilizzo in modo automatico.

2.6 Descrizione hardware



Connettore	Descrizione
P7	Morsettiera per alimentazione da rete elettrica
P8	Connettore per l'alimentazione della batteria di backup
P4	Connettore USB di tipo B (device) per programmazione da Sicep Cloud Connect
P11	Connettore SMA per antenna BiTech / VTech esterna
P5	Connettore SMA per antenna GSM esterna
P2	Connettore per modulo opzionale WLAN
X15	Alloggiamento SIM CARD
P6	Connettore Ethernet 10/100 Mbit
P1	Alloggiamento memoria MicroSD 8GB
P9 - P10	Morsettiera per uscita programmabile

Pulsante/Jumper	Descrizione
RESET	Premuto esegue un reset del microcontrollore principale
TEST	Permette il ripristino alla programmazione di default. Per l'utilizzo fare riferimento all'apposita sezione.
X8	Switch Tamper (apertura contenitore)
J1	Jumper per cancellazione processore

Led	Colore	Descrizione
RETE(DL6)	Verde	Acceso indica che l'alimentazione di rete è presente
BATTERIA (DL7)	Rosso	Acceso indica batteria scarica / guasta
CONNESSIONE (DL8)	Blu	Acceso o lampeggiante indica una connessione in corso
GSM STAT (DL3)	Verde	I lampeggi indicano l'attività del modulo GSM
TX BiTech(DL5)	Rosso	Si accende durante la trasmissione dei pacchetti dati
TX VTech(DL4)	Rosso	Si accende durante la trasmissione dei pacchetti dati
Traffico dati (DL9)	Verde	Comunicazione su rete LAN
Traffico dati (DL10)	Giallo	Comunicazione su rete LAN

2.7 Conformità di Conformità UE semplificata



Sicep S.r.l. dichiara che il tipo di apparecchiatura radio DG-432, Centralina di allarme wireless 868MHz è conforme alla Direttiva 2014/53/UE.

Il testo completo della Dichiarazione di Conformità UE è disponibile al seguente indirizzo Internet: www.sicep.it

3. Caratteristiche elettriche e dimensionali centralina

Alimentazione da rete:	100 -240 VAC, 50/60Hz
Assorbimento a 230V:	40 mA max.
Assorbimento a 115V:	70 mA max.
Fusibile:	800 mA.
Batteria backup:	LiFePO4 3.2V 1.5Ah 4.8Wh
	NOTA. La batteria deve essere sostituita da personale esperto.
Assorbimento a 3,6V da batteria:	350 mA max. / 70 mA in risparmio energetico
Livello batteria scarica:	<3V
Ripristino da batteria scarica:	>3,35V
Blocco di sicurezza della batteria:	<2V
Verifica continua livello batteria	Si
Verifica periodica efficienza batteria:	Ogni 240 ore
Autonomia in assenza rete elettrica:	> 12 ore (no LTE/GPRS, no WI-FI)
Tempo di ricarica batteria all'80%:	4 ore circa
Protocolli radio:	BiTech, VTech
Frequenze radio:	868.2 - 869.8MHz (3 canali disponibili) CEPT/ERC/REC 70-03 Classe 3
Potenza:	<10mW ERP con antenna integrata
Duty cycle:	<1%
Antenna:	Integrata / connettore SMA per antenna esterna.
Connessione di rete:	RJ45 Ethernet IEEE 802.3 10/100 LANport
Connessione LTE/GPRS:	Modulo LTE CAT1 Bande: EGSM900MHz, DCS1800MHz, LTE-FDD B1, B3, B5, B7, B8, B20
Antenna:	Integrata / connettore SMA per antenna esterna.
Porta SIM:	Mini-SIM(2FF)
Connessione USB:	2.0 (Hi-Speed) , connettore tipo B
Connessione WI-FI (opzionale):	802.11 b/g/n Wireless LAN (2.4GHz)
Uscita programmabile:	Tipo Open Collector con riferimento a GND corrente max. 200 mA.
Memoria rimovibile:	micro SD 8GB
Sirena locale:	Integrata, piezoelettrica, potenza > 85dB @ 1 metro
Antimanomissione:	Tamper apertura contenitore e antistrappo di tipo magnetico.
Dimensioni (LxHxP):	180 x 180 x 36 mm.
Peso:	430 g comprensivo di batteria
Temperatura (funzionamento):	Da 5° a +40°
Temperatura (immagazzinamento):	Da -10° a +45°
Umidità:	Da 20% a 80%
Grado di protezione contenitore:	IP40

4. Gestione sistema di sicurezza

In questo capitolo sono descritte in dettaglio tutte le funzioni della centralina.

4.1 Aree

La centralina DOGMA gestisce 4 aree. Ciascuna area può utilizzare sensori immediati o ritardati, sensori condivisi fra più aree e può utilizzare due diversi tipi di inserimento.

4.1.1 Inserimento Totale - Perimetrale/Notte

E' possibile definire in fase di programmazione se ciascuna zona/dispositivo è interna oppure non interna (perimetrale). In questo modo si può inserire l'impianto in due modalità diverse: totale o Perimetrale. Inserendo l'area in modo totale, tutte le zone sono attive; inserendo l'area in modo perimetrale, le zone interne non sono attive. Tipicamente i sensori posti sulle porte e finestre sono perimetrali mentre i sensori infrarossi e rivelatori di movimento sono interni.

- **Inserimento Totale** - In questo tipo di inserimento tutte le zone appartenenti all'area sono attive (si suppone di non avere aree condivise); questo tipo di inserimento è quello che si effettua quando si esce dall'abitazione.
- **Inserimento Perimetrale** - In questo tipo di inserimento sono attive solo le zone perimetrali (si suppone di non avere aree condivise). Questo tipo di inserimento consente di muoversi dentro l'abitazione mantenendo la protezione perimetrale (porte e finestre) attiva.
- **Inserimento Notte** - In alternativa all'inserimento Perimetrale è possibile configurare l'area per l'inserimento di tipo Notte. E' come l'inserimento Perimetrale ma ignora i tempi di Ingresso e di Uscita.

4.1.2 Tempi Ingresso / uscita Aree: zone ritardate

Le zone/dispositivi ritardate utilizzano i tempi programmati in base all'area di appartenenza; in altre parole tutte le zone ritardate hanno tempi di ingresso e uscita uguali.

Una zona/dispositivo deve essere ritardata se è necessario allarmarla durante le operazioni di Inserimento e disinserimento dell'area.

Esempio: se la centralina è posta nel corridoio d'ingresso ed è presente un contatto magnetico sulla porta, una volta inserita l'area, la porta deve essere necessariamente aperta per uscire dall'abitazione; quando si rientra nell'abitazione, prima di disinserire l'impianto la porta viene nuovamente aperta.

I tempi di ingresso e uscita agiscono in questo modo:

- **Tempo d'uscita:** si attiva all'inserimento dell'area; i sensori ritardati sono ignorati (non sono attivi) fino al termine di questo tempo.
- **Tempo d'ingresso:** si attiva quando una zona/dispositivo ritardata va in allarme; questa condizione viene memorizzata e genera l'allarme allo scadere di questo tempo, a meno che l'area non venga disinserita prima dello scadere del tempo di ingresso.

4.1.3 Auto esclusione zone

Ci sono situazioni in cui è necessario poter escludere una zona/dispositivo che si trova in allarme quando si va a inserire l'impianto.

Esempi:

- *Un sensore guasto è rimasto permanentemente in allarme e si vuole comunque inserire l'impianto, in attesa della sostituzione del sensore;*
- *Si desidera, d'estate, inserire l'impianto lasciando volutamente una finestra aperta che è protetta da un contatto.*

Quando si esegue un inserimento con una o più zone/dispositivi in allarme si deve effettuare un Inserimento **forzato** per poter procedere all'esclusione.

Il sistema notificherà in qualche modo che sono presenti una o più zone/dispositivi in allarme e per inserire si deve eseguire nuovamente l'operazione di Inserimento. A questo punto possono presentarsi varie situazioni, in funzione del tipo di zona/dispositivo in allarme:

- **Zona / dispositivo non ritardato escludibile:** La zona viene esclusa al secondo tentativo di inserimento. Se l'inserimento avviene tramite programmatore orario, la zona/dispositivo viene esclusa automaticamente.
- **Zona / dispositivo non ritardato non escludibile:** La zona/dispositivo non

può essere escluso per cui l'area non viene mai inserita, l'unico modo di inserire l'impianto è riportare a riposo la zona o il dispositivo in allarme. Fa eccezione la condizione in cui l'inserimento avviene tramite programmatore orario: se è presente questa condizione l'impianto viene inserito e l'area va immediatamente in allarme.

- **Zona / dispositivo ritardato:** La zona/dispositivo non viene escluso e non viene segnalato il suo eventuale stato di allarme. E' tassativo però il suo ripristino entro la fine del tempo d'uscita. Una zona/dispositivo ritardato non può essere anche escludibile; in fase di programmazione un apposito controllo la rende non escludibile.
- **Zona / dispositivo condiviso escludibile:** La zona/dispositivo viene escluso solo a fronte dell'inserimento dell'ultima area di condivisione. All'inserimento delle aree precedenti la zona in allarme viene notificata e l'inserimento diventa di tipo forzato; la zona però non viene esclusa. L'area inserita è visualizzata come in attesa.
- **Zona / dispositivo condiviso non escludibile:** La zona/dispositivo non viene mai escluso. A fronte dell'inserimento dell'ultima area di condivisione, viene negato l'inserimento. L'inserimento è permesso solo se la zona o il dispositivo è riportata a riposo. All'inserimento delle aree precedenti la zona/dispositivo in allarme viene notificata e l'inserimento diventa di tipo forzato; la zona però non viene esclusa. L'area inserita è visualizzata come in attesa. Se l'ultima area di condivisione viene inserita tramite programmatore orario, l'impianto viene inserito e l'area va immediatamente in allarme.

NOTA. *Le zone che si trovano nello stato di Sabotaggio non sono considerate in allarme;*

Tutte le volte che una zona / dispositivo viene escluso, viene generato un apposito evento.

4.1.4 Riattivazione automatica delle zone/dispositivi esclusi

Le zone o dispositivi immediati escludibili possono ritornare attivi in due modi diversi, a seconda della programmazione scelta:

- **Singolo:** la zona/dispositivo, una volta escluso a seguito di un inserimento forzato, resta escluso fino al prossimo inserimento.
- **Auto:** la zona/dispositivo, una volta escluso a seguito di un inserimento forzato, ritorna attivo automaticamente appena torna a riposo.

Queste modalità sono disponibili per le sezioni "Porta" e "Aux" dei contatti magnetici BT-CMXW / BT-CMXE.

4.1.5 Disabilitazione zone

L'esclusione manuale di una zona/dispositivo, o disabilitazione, è una operazione compiuta da una tastiera o da programmazione tramite Sicep Cloud Connect con la quale si rende un zona / dispositivo permanentemente non attivo. Una zona/dispositivo disabilitato può essere reso di nuovo attivo eseguendo l'operazione inversa. Quando si disabilita una zona/dispositivo viene generato un apposito evento.

4.1.6 Varchi

La centralina DOGMA utilizza la gestione dei varchi in base alla programmazione. Per varco si intende un punto di accesso all'impianto, che può essere costituito da una tastiera LCD, un lettore RFID, o un radiocomando. Quando si accede all'impianto tramite un determinato varco l'impianto eseguirà l'azione programmata in base al codice introdotto nella tastiera, al TAG presentato o al radiocomando ricevuto:

- Visualizzazione dello stato di una o più aree di competenza;
- Possibilità di eseguire l'operazione sul gruppo di aree di competenza o su un'area specifica (fra quelle di competenza);
- Nessuna operazione, se il tipo di identificazione non risulta valido per quel varco.

4.1.7 Aree di competenza - Aree predefinite

Il concetto di aree di competenza si può riassumere così:

Nel caso di TAG o radiocomandi, le aree di competenza sono quelle su cui sono eseguite le operazioni contemporaneamente e questo dipende dal varco.

Esempio: se un TAG associato a un determinato utente ha associate le aree 1, 2 per un determinato varco, presentato a quel determinato varco opererà sempre e solo su tutte le aree 1 e 2 contemporaneamente.

Nel caso delle tastiere, le aree di competenza sono le aree su cui l'utente può operare. Le aree predefinite invece rappresentano quelle su cui la tastiera opera contemporaneamente appena si inserisce il codice.

Esempio: un utente ha associato per una tastiera le aree di competenza 1 e 2 e ha come area predefinita la 2. Ciò significa che se inserisce il codice e preme l'icona "disinserimento" disinserisce direttamente e soltanto l'area 2. In alternativa, una volta inserito il codice può operare sulle aree 1, e 2 anche separatamente.

Nel caso in cui le aree di competenza coincidono con le aree predefinite (es. competenza 1 e 2 e predefinite 1 e 2), facendo un'operazione di inserimento / disinserimento si attivano contemporaneamente entrambe le aree.

Riassumendo:

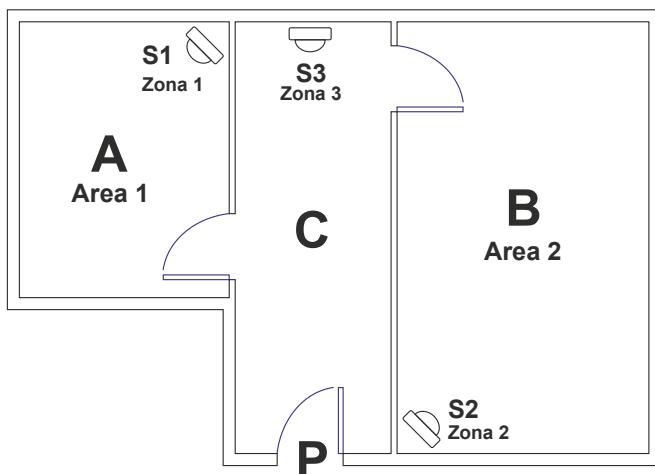
- **Aree Visibili:** vale per le tastiere fisiche e gli altri dispositivi di inserimento. Non sono assegnate all'utente ma al dispositivo (nella pagina di configurazione dello stesso).
- **Aree di Competenza:** sono le aree assegnate all'utente su quel varco. Sono le aree che l'utente da quel varco può inserire e disinserire.
- **Aree Predefinite:** sono le aree fra quelle di competenza che sono assegnate alle operazioni rapide.

Normalmente su una tastiera si vede lo stato delle aree visibili, dal momento che si inserisce un codice si vedono quelle di competenza.

Sul client si vedono da subito quelle di competenza per l'accesso remoto (in quanto l'accesso è già stato autenticato con la password).

4.1.8 Condivisione Aree

La centralina DOGMA permette l'utilizzo e la gestione di zone condivise fra più aree. Vediamo come funziona mediante un semplice esempio.



Due uffici A e B hanno il corridoio C in comune; per semplicità in questo impianto abbiamo solo 3 sensori: uno nell'ufficio A, uno nell'ufficio B e uno nel corridoio.

L'impianto è suddiviso in due aree: area 1 (ufficio A) e area 2 (ufficio B); il sensore 1 (zona 1) è assegnato solo all'area A, il sensore 2 solo all'area B mentre la zona 3 (sensore 3) è condivisa, cioè è assegnata sia all'area A che all'area B.

Ciascun utente (A e B) può inserire / disinserire solo la propria sezione dell'impianto.

Supponiamo di partire dalla condizione in cui entrambe le aree sono disinserite.

Supponiamo che tutte le zone siano non ritardate.

L'utente A esce e inserisce l'area 1 (totale). Visto che la zona 3 appartiene anche ad un'area non inserita, la zona 3 non viene attivata. L'area 1, avendo aree condivise non

attivate è nella condizione di attesa. In questo modo l'utente B può attraversare il corridoio senza generare allarmi. L'utente B esce ed inserisce l'area 2 (totale). A questo punto anche la zona 3 viene attivata.

NOTA. *Se un intruso fa scattare il sensore zona 3, risulteranno in allarme sia l'area 1 che la 2.*

4.1.9 Area 24h

Appartengono all'area 24h tutti i controlli che sono sempre attivi e in grado di generare un evento di allarme, indipendentemente dall'inserimento delle aree. Questi controlli sono:

- Disabilitazione zone/dispositivi
- Tamper dispositivi wireless
- Tamper apertura coperchio centralina
- Incendio
- Panico
- Soccorso
- Stato batteria centralina
- Batteria sensori e dispositivi wireless
- Assenza tensione di rete
- Malfunzionamento sensori wireless
- Accecamento RF sensori
- Coercizione
- Inserimento password errata, TAG non registrato
- Esclusione zone
- Accecamento GSM
- Segnale GSM insufficiente
- SIM prepagata: credito basso o SIM in scadenza
- Assenza LAN
- Zone Disabilitate
- Allarme zone 24H

Questi controlli non generano allarme soltanto quando la centralina si trova nella condizione di manutenzione.

4.1.10 Funzione Reinserimento Automatico Aree

Tutte le aree possono essere impostate per effettuare un inserimento in automatico dopo un tempo programmato. Per questa funzione è necessario programmare il parametro "T.Autoins." (tempo auto inserimento) nella pagina Sistema → Aree.

Se al reinserimento automatico di un'area una o più zone / dispositivi di appartenenza si trovano in allarme, la centralina si comporta in modo un po' diverso rispetto all'inserimento manuale:

- Se ci sono zone / dispositivi immediati in allarme auto escludibili, la centralina forza l'inserimento dell'area escludendo automaticamente le zone / dispositivi.
- Se ci sono zone / dispositivi immediati in allarme non escludibili, la centralina inserisce l'area e fa scattare subito l'allarme; la zona o dispositivo resta attivo.
- Se ci sono zone / dispositivi ritardati in allarme la centralina inserisce normalmente; se la zona / dispositivo non si ripristina, al termine del tempo di ingresso scatta l'allarme.

In tutti i casi, se ci sono zone / dispositivi ritardati ed è prevista la segnalazione acustica del tempo di uscita, questo viene notificato normalmente, come per l'inserimento manuale.

4.2 Accessi e Password

La centralina DOGMA utilizza vari organi di comando permettendo diversi tipi di accesso. Localmente si può accedere tramite le tastiere, lettori chiave RFID o radiocomando.

Da remoto possono essere utilizzati sia l'App SICEP, che il software Sicep Cloud Connect; questo ultimo integra la parte dedicata all'installatore per la configurazione dell'impianto.

Nella centralina DOGMA ci sono due tipi di codici di accesso:

Le **PASSWORD** che servono per la connessione da remoto tramite Sicep Cloud Connect o Sicep e i **CODICI** tastiera a 5 cifre, che servono per accedere localmente al sistema tramite le tastiere.

Ciascun utente, può modificare il proprio codice tastiera tramite le tastiere o tramite App.

La modifica della password può essere fatta solo da App SICEP o da Sicep Cloud Connect. L'amministratore può fare singolarmente il default della password o l'azzeramento del codice tastiera di tutti gli utenti, da App SICEP o da Sicep Cloud Connect. L'amministratore può inoltre abilitare o disabilitare tutti gli utenti compreso l'installatore tramite Sicep o Sicep Cloud Connect.

Programma Sicep Cloud Connect: l'accesso da locale con collegamento USB o da remoto tramite LAN o LTE/GPRS è permesso solo all'installatore e all'Amministratore che devono utilizzare la propria password per entrambi i tipi di collegamento.

Quando la centralina esce con le impostazioni di fabbrica sono abilitati solo gli accessi Amministratore e Installatore con le password e i codici di default riportati qui di seguito.

Nome Utente	Codice tastiera	Password Sicep Cloud Connect	Abilitazione
Utente 1 (amministratore)	12301	amministratore	Si
Utente 2	12302	utente2	No
...	...	...	No
Utente 15	12315	utente15	No
Installatore	11100	installatore	Si

NOTA. *Le password e i codici tastiera di default non sono utilizzabili come nuovi codici. Esempio: l'utente 3 (default 12303) non può modificare il proprio codice tastiera in 12314, che è il codice di default dell'utente 14, neppure se l'utente 14 è disabilitato.*

4.2.1 Blocco Tastiera

Se si inserisce per 5 volte consecutive un codice tastiera non valido, la tastiera si blocca per 5 minuti. Qualsiasi accesso alla tastiera durante questo tempo, verrà visualizzato il messaggio sul display "Fuori Servizio".

4.2.2 Blocco Accesso da Remoto

Se si inserisce per 5 volte consecutive una password non valida, l'accesso da remoto viene bloccato per 5 minuti e viene generato l'evento "REMOTO: PW FALSA".

4.2.3 Disinserimento con Coercizione

È possibile disinserire ed inviare una segnalazione di Coercizione solamente dalle tastiere.



Su BT-KPXW,

il disinserimento dell'impianto sotto coercizione avviene premendo prima il pulsante dedicato al disinserimento e successivamente effettuando la procedura di disinserimento, ovvero inserendo il proprio codice utente e premendo nuovamente il pulsante dedicato.



Su BT-SKW,

se si inserisce un qualsiasi codice tastiera valido preceduto dal tasto "***", viene effettuata l'operazione richiesta e contemporaneamente viene generato l'evento Coercizione.

4.3 Eventi (descrizione dettagliata)

Per evento si intende qualsiasi variazione di uno degli stati logici esterni o interni alla centralina. Ciascun evento può provocare un'azione in loco e/o generare una trasmissione di allarme o di ripristino da parte del sistema di comunicazione della centralina. Alcuni eventi non trasmettono il ripristino. Per la trasmissione in CONTACT-ID ciascun evento ha già assegnato un codice di default che comunque può essere modificato in configurazione da Sicep Cloud Connect. Ciascun evento trasmesso in questo formato include il codice periferica a 4 cifre più l'eventuale zona, area o utente che ha effettuato l'operazione. Una descrizione dettagliata dei vettori di trasmissione è riportata nella sezione Comunicatore. Segue la descrizione di tutti gli eventi generati dalla centralina DOGMA.

1. Zone / dispositivi disabilitati

Questo evento indica che uno o più dispositivi wireless sono stati disabilitati manualmente. L'evento si ripristina quando non ci sono più dispositivi disabilitati. Questo evento serve principalmente per ricordare che nell'impianto è presente uno o più sensori (o dispositivi) volutamente disabilitati.

Codice CONTACT-ID di default: 570.

Il codice identificativo del dispositivo (zona / dispositivo) trasmesso nel messaggio CONTACT-ID è il seguente: 1 ... 16 per gli ingressi filari e 201 ... 236 Sensori e dispositivi wireless.

2. Sabotaggio dispositivi RF (wireless)

Questo evento indica che un dispositivo wireless ha il contenitore aperto o è stato rimosso dal muro. L'evento torna nello stato di riposo quando il sensore viene ripristinato o disabilitato manualmente.

Codice CONTACT-ID di default: 383.

Il codice identificativo del dispositivo trasmesso nel messaggio CONTACT-ID è 201 ... 236.

3. Tamper e Antistrappo Centrale

Questo evento indica che la centralina ha il contenitore aperto o è stata asportata dal muro. L'evento si ripristina quando il contenitore della centralina viene fissato alla parete ed il coperchio viene chiuso. Per poter aprire il contenitore senza mandare in allarme l'impianto, si dovrà precedentemente impostare lo stato di MANUTENZIONE. Questo stato si disattiva automaticamente dopo 60 secondi da quando viene chiuso il contenitore (Tamper). Nello storico viene riportato il motivo che ha generato l'evento: Tamper o Antistrappo.

Codice CONTACT-ID di default: 137.

4. Incendio

Questo evento può essere provocato da più cause:

- un sensore di fumo BT-SMK2 ha rilevato del fumo o un aumento anormale della temperatura ambientale;
- è stato premuto l'apposito tasto su una tastiera o un radiocomando.

L'evento non ha ripristino; se è associata l'attivazione di una uscita, questa deve essere sempre impulsiva. I sensori BT-SMK2 possono essere programmati per suonare anche quando l'allarme incendio è provocato da un'altra causa (per es. dal pulsante sulla tastiera) o da un altro sensore BT-SMK2. Questa funzione è chiamata Ripetitore allarme sonoro.

Codice CONTACT-ID di default: 110.

NOTA.

Se le sirena BT-ALMA e BT-SIR rileva un aumento anormale della temperatura, questo evento è segnalato come Sabotaggio dispositivo RF e non come Incendio.

5. Panico

Questo evento può essere provocato premendo l'apposito tasto su una tastiera o un radiocomando.

L'evento non ha ripristino; se è associata l'attivazione di una uscita, questa deve essere impulsiva.

Codice CONTACT-ID di default: 120.

6. Soccorso

Questo evento può essere provocato premendo l'apposito tasto su una tastiera o un radiocomando.

L'evento non ha ripristino; se è associata l'attivazione di una uscita, questa deve essere impulsiva.

Codice CONTACT-ID di default: 101

7. Batteria centrale

Questo evento indica che la batteria di backup della centralina è scarica o da sostituire. In particolare, nel primo caso è assente l'alimentazione di rete e la tensione di alimentazione è scesa sotto 3V; nel secondo caso l'evento è stato generato dal test periodico di efficienza della batteria e in tal caso deve essere sostituita. Il ripristino dell'evento è diverso in base alla causa che lo ha provocato; nel primo caso avviene quando la tensione di alimentazione risale oltre 3,35V, nel secondo caso quando il test periodico indica che la batteria è tornata efficiente.

Codice CONTACT-ID di default: 302.

8. Batteria dispositivi RF

Questo evento indica che il dispositivo wireless corrispondente ha la batteria scarica, ovvero al di sotto della tensione di guardia. Le soglie di scarica sono le seguenti:

- 2,7V per tutti i dispositivi eccetto il radiocomando, il sensore di fumo e il ripetitore
- 2,5V per il radiocomando; la tensione nominale di questa batteria è 3V.
- 7,5V per il sensore di fumo; la tensione nominale di questa batteria è 9V.
- 3,5V per il ripetitore; la tensione nominale complessiva di questa batteria è 3,7V.

Il ripristino dell'evento si ha quando la batteria del dispositivo è stata sostituita e questo ha trasmesso un messaggio verso la centralina contenente il nuovo valore corretto della tensione.

Codice CONTACT-ID di default: 384.

Il codice identificativo del dispositivo trasmesso nel messaggio CONTACT-ID è 201 ... 236.

9. Assenza Rete

Questo evento indica che l'alimentazione di rete è assente o l'alimentatore è guasto. L'evento viene generato se la rete rimane assente per un tempo superiore a quello programmato.

Il ripristino avviene al ritorno dell'alimentazione da rete. Impostando il tempo di ritardo a zero l'evento è immediato.

Codice CONTACT-ID di default: 301.

10. Malfunzionamento dispositivo RF

Questo evento indica che un dispositivo wireless presenta una criticità nel collegamento con la centralina DOGMA. L'evento può essere generato da tre condizioni diverse:

- **CRITICO.** Il dispositivo ha trasmesso meno di 1000 presenze nell'ultima settimana (contro le 1344 nominali), oppure una percentuale significativa delle trasmissioni (25%) è effettuata nella modalità di emergenza "Mesh", oppure la centralina non ha ricevuto trasmissioni consecutive per un tempo superiore a quello programmato (da 20 a 720 minuti).
- **ASSENTE.** La centralina non ha ricevuto trasmissioni consecutive dal dispositivo per un tempo superiore a 12 ore.
- **CONSUMO ECCESSIVO.** Il dispositivo ha effettuato più di 2400 trasmissioni nell'ultima settimana. Questo controllo può essere disabilitato per ciascun dispositivo.

Il conteggio delle trasmissioni per le soglie di "critico" e "consumo eccessivo" è eseguito ogni 24 ore e inizia dopo 3 giorni dall'installazione del dispositivo.

Il ripristino dell'evento avviene quando la condizione che ha creato l'evento non c'è più:

- Nei casi di dispositivo CRITICO o CONSUMO ECCESSIVO il ripristino avviene entro la settimana successiva alla risoluzione del problema;
- Nel caso di dispositivo ASSENTE, appena il collegamento con la centralina viene ripristinato.

Codice CONTACT-ID di default: 380.

Il codice identificativo del dispositivo trasmesso nel messaggio CONTACT-ID è 201 ... 236.

11. Accciamento RF

Questo evento indica che la centralina sta rilevando un disturbo prolungato sul canale radio della rete wireless BiTech (868MHz); l'evento viene generato se il disturbo persiste per un tempo superiore a quello impostato.

L'evento può essere rilevato anche da un ripetitore BT-REP.

Entrambi i controlli possono essere abilitati o disabilitati separatamente. L'evento si

ripristina quando il disturbo non è più presente.
Codice CONTACT-ID di default: 344.

12. Accecamento GSM

Questo evento indica che la centralina sta rilevando un disturbo prolungato sulla rete GSM che potrebbe compromettere il canale di comunicazione. Questo controllo può essere abilitato o disabilitato in fase di configurazione del GSM.
L'evento si ripristina quando il disturbo non è più presente.
Codice CONTACT-ID di default: 344.

13. Coercizione

Questo evento indica che l'operazione di inserimento/disinserimento da tastiera è avvenuta sotto coercizione (l'inserimento del codice è stato preceduto dall'apposito tasto “*”).

Questo evento non può attivare la sirena.

L'evento non ha ripristino; se è associata l'attivazione di una uscita, questa deve essere impulsiva.

Codice CONTACT-ID di default: 121.

14. Password falsa

Questo evento indica che su una tastiera è stata inserita consecutivamente per 5 volte un codice non valido; la tastiera viene resa inattiva per 5 minuti.

L'evento non ha ripristino; se è associata l'attivazione di una uscita, questa deve essere impulsiva.

Codice CONTACT-ID di default: 461.

15. Prova automatica

Questo evento serve a generare una comunicazione di sopravvivenza ad intervalli di tempo prestabiliti. E' lo stesso messaggio che viene generato premendo i pulsanti TEST nella pagina Comunicatore → Gestionale. L'evento non ha ripristino.

Codice CONTACT-ID di default: 602.

16. Ignorata Richiesta Assistenza

Questo evento indica che nella fase di inserimento impianto una o più zone / dispositivi o anomalie del sistema sono presenti, ma ignorate tramite un inserimento forzato.

Questo evento viene generato a prescindere dallo stato del flag di configurazione *Non richiedere di forzare l'inserimento con Richiesta Assistenza*.

Codice CONTACT-ID di default: 570.

17. Assenza comm. LAN/WIFI

Questo evento indica che il collegamento della rete ethernet via LAN o WiFi è assente. L'evento viene generato se il collegamento rimane assente per un tempo superiore a quello programmato e il ripristino avviene al ripristino dello stesso. Impostando il tempo a zero l'evento è disabilitato.

Codice CONTACT-ID di default: 350.

18. Manutenzione

Questo evento indica che la centralina si trova nello stato di manutenzione. In questa condizione sono disabilitate le sirene e il comunicatore telefonico; le tastiere e i lettori RFID emettono un “bip” ogni 10 secondi.

I sensori wireless attivano i led per segnalare le comunicazioni con la centralina e il riconoscimento di uno stato di allarme, dove previsto.

La centralina può essere posta nello stato di manutenzione in vari modi:

- Automaticamente, se si preme il bottone RESET sul circuito mantenendo il contenitore aperto;
- Manualmente, entrando in programmazione da Sicep Cloud Connect con password installatore;
- Da tastiera, entrando con codice installatore e accedendo all'apposita funzione.
- Tramite Sicep

Anche l'uscita dallo stato di manutenzione può avvenire in vari modi:

- Automaticamente, dopo un minuto dalla chiusura del contenitore;
- Manualmente, entrando in programmazione da Sicep Cloud Connect con password installatore;
- Da tastiera, entrando con codice installatore e accedendo all'apposita funzione.
- Tramite Sicep.

Codice CONTACT-ID di default: 466.

19. Assenza linea GSM

Questo evento indica che il GSM non è registrato in rete per un tempo superiore a quello programmato. Impostando il tempo a zero l'evento è disabilitato.

Codice CONTACT-ID di default: 353.

20. Credito - Scadenza SIM

Se si utilizza per il GSM una SIM prepagata ricaricabile, la centralina DOGMA ogni 48 ore controlla il credito residuo nella SIM e ogni giorno incrementa il parametro "giorni trascorsi dall'ultima ricarica".

L'evento genera una segnalazione di allarme nei seguenti casi:

- Il credito residuo è sceso sotto 4 euro;
- Il credito residuo è sceso sotto 2 euro;
- I giorni trascorsi dall'ultima ricarica sono 320.

La centralina riporta automaticamente a 1 il valore "giorni trascorsi dall'ultima ricarica" quando rileva che il credito è maggiore di quello letto in precedenza.

Codice CONTACT-ID di default: 350.

L'utente può in qualsiasi momento richiedere il credito attuale inviando un SMS da un cellulare verso la SIM installata nella centralina contenente il testo "INFO SIM".

ATTENZIONE!

Il controllo è supportato solo per gli operatori TIM e Wind. Questi operatori possono modificare in qualsiasi momento senza preavviso l'SMS di risposta, pertanto non si garantisce il corretto funzionamento.

21. Allarme 24H

Questo evento indica che una zona di tipo 24H è in allarme. L'evento si ripristina quando la zona torna a riposo.

Codice CONTACT-ID di default: 150.

Il codice identificativo della zona trasmesso nel messaggio CONTACT-ID è 001 – 016.

22. Apriporta

Questo evento indica che l'utente ha aperto la porta (elettroserratura) tramite l'apposita funzione del lettore RFID BT-PRW. Questo evento non può essere associato ad azioni locali e serve soltanto per trasmettere l'informazione al gestionale MvsNET della Centrale Operativa.

Codice CONTACT-ID di default: 422.

Il codice identificativo dell'utente trasmesso nel messaggio CONTACT-ID è compreso tra 501 e 516.

23. Assenza connessione Internet

Evento generato in caso di problemi di collegamento in internet sia via TCP/IP che via LTE/GPRS.

Codice CONTACT-ID di default: 350.

24. Fumogeni cartuccia scaduta

Evento che indica la scadenza della cartuccia di uno dei fumogeni.

Codice CONTACT-ID di default: 315.

25. Fumogeni cartuccia esaurita

Evento che indica che una cartuccia dei fumogeni è stata utilizzata, quindi esaurita.

Codice CONTACT-ID di default: 316.

26. Malfunzionamento IPCamera

Evento generato in caso di problemi le IPCamera associate.

Codice CONTACT-ID di default: 333.

27 – 38 . Allarme Area 1 ... Area 4 (Totale / Perimetrale / Notte)

Questo evento indica che l'area corrispondente è in allarme e provoca l'attivazione delle sirene. L'evento può essere generato solo se l'area corrispondente è inserita. Il ripristino può avvenire in due modi: al termine del ciclo di allarme, cioè allo spegnimento delle sirene, oppure al ripristino della zona che ha provocato l'allarme. Il modo viene scelto in programmazione ed è lo stesso per tutte le aree. Nel caso che si sia scelto il ripristino sulla zona, questo è effettivo solo nel caso di allarme provocato da un contatto magnetico BT-CMXW/BT-CMXE (sezioni Porta e Ausiliario) o da zone filari; per le altre sezioni il ripristino è immediato.

Se all'evento è associata l'attivazione di una uscita avremo il seguente comportamento: in ogni caso si attiva nel momento dell'evento; se è statica si disattiva quando l'evento si ripristina, mentre se è impulsiva si disattiva dopo il tempo impostato per l'impulso.

Codice CONTACT-ID di default: 130.

39 – 54. Ins./Dis. Area 1 ... Area 4 (Ins. Totale, Ins. Perimetrale, Ins. Notte, Disinserim.)

Questo evento indica che l'area relativa è inserita in modo totale, perimetrale, notte o disinserita.

Se all'evento è associata l'attivazione di una uscita avremo il seguente comportamento: in ogni caso si attiva nel momento dell'evento; se è statica si disattiva quando l'evento si ripristina, mentre se è impulsiva si disattiva dopo il tempo impostato per l'impulso.

Codice CONTACT-ID di default: 400.

Il codice identificativo dell'utente trasmesso nel messaggio CONTACT-ID è compreso tra 501 e 516.

55 – 58 Tempo Uscita Area1 ... Area4

Questo evento viene generato all'inizio del Tempo di Uscita a fronte di un inserimento dell'area e viene ripristinato al termine del tempo impostato. Se durante questo periodo di tempo viene effettuata una forzatura per ottenere l'inserimento immediato, nello stesso momento si ripristina anche l'evento.

Se all'evento è associata l'attivazione di una uscita avremo il seguente comportamento: in ogni caso si attiva nel momento dell'evento; se è statica si disattiva quando l'evento si ripristina, mentre se è impulsiva si disattiva dopo il tempo impostato per l'impulso.

Codice CONTACT-ID di default: << Da Impostare >>.

59 – 62 Tempo Ingresso Area1 ... Area4

L'evento è generato all'inizio del Tempo di Ingresso, nel momento in cui si allarma un sensore o una zona ritardata e viene ripristinato allo scadere del tempo impostato e scatta l'allarme, oppure nel momento in cui viene disinserita l'area.

Se all'evento è associata l'attivazione di una uscita avremo il seguente comportamento: in ogni caso si attiva nel momento dell'evento; se è statica si disattiva quando l'evento si ripristina, mentre se è impulsiva si disattiva dopo il tempo impostato per l'impulso.

Codice CONTACT-ID di default: << Da Impostare >>.

63 – 66 Mancato Inserimento Area1 ... Area4

Questo evento indica che l'inserimento dell'area è fallito per qualche motivo, normalmente per una zona o dispositivo in allarme NON ESCLUDIBILE. L'evento non prevede ripristino, se è associata l'attivazione di una uscita, questa deve essere impulsiva.

Codice CONTACT-ID di default: 454.

67 – 70 Esclusione Zone Area1 ... Area4

Questo evento indica che una o più zone / dispositivi sono state esclusi in fase di inserimento tramite un inserimento forzato. L'evento si ripristina quando l'ultima zona / dispositivo esclusa ritorna attiva oppure quando l'area di appartenenza viene disinserita.

Se all'evento è associata l'attivazione di una uscita avremo il seguente comportamento: in ogni caso si attiva nel momento dell'evento; se è statica si disattiva quando l'evento si ripristina, mentre se è impulsiva si disattiva dopo il tempo impostato per l'impulso.

Codice CONTACT-ID di default: 570.

Il codice identificativo del dispositivo trasmesso nel messaggio CONTACT-ID è il seguente:
1 ... 16 per gli ingressi filari, 209 – 236 Sensori wireless

61 – 78 Eventi programmabili

Sono una serie di eventi generici, programmabili e assegnabili ad alcune funzioni legate ai sensori o agli organi di comando della centrale. A differenza di quelli predefiniti, è possibile assegnare una etichetta all'evento per facilitare la comprensione del significato. Le operazioni da eseguire sull'evento sono totalmente configurabili come per gli eventi predefiniti e il comportamento dipende in parte dal tipo di organo da cui viene generato.

4.4 Programmazione orario

La centralina DOGMA dispone di un programmatore orario estremamente flessibile che consente di configurare le operazioni automatiche in maniera rapida per un intero anno.

Le sue caratteristiche sono le seguenti:

- fino a 4 programmi diversi.
- Ciascun programma può essere associato a una o più aree, a una o più uscite, a uno o più utenti per limitarne l'accesso.
- Ciascun programma consente di specificare, per ogni giorno dell'anno, due inserimenti e due disinserimenti, oppure due attivazioni e due disattivazioni, o due fasce di accessibilità all'impianto per l'utente.
- Possono essere definiti fino a 12 giorni "Tipo" diversi da assegnare al singolo giorno dell'anno oppure ad un periodo di tempo nell'anno.
- Possono essere definite fino a 4 settimane diverse, componendole con i giorni "Tipo" da assegnare ad un periodo di tempo nell'anno.
- Gestione delle festività fisse e mobili con 12 giorni per ciascun tipo.

La programmazione o eventuali modifiche si effettuano esclusivamente dal software Sicep Cloud Connect.

Se al reinserimento automatico di un'area una o più zone / dispositivi di appartenenza si trovano in allarme, la centralina si comporta in modo diverso rispetto all'inserimento manuale:

- Se ci sono zone / dispositivi immediati auto escludibili in allarme, la centralina forza l'inserimento dell'area escludendo automaticamente le zone o dispositivi allarmati.
- Se ci sono zone / dispositivi immediati non auto escludibili in allarme, la centralina inserisce l'area e fa scattare immediatamente l'allarme; le zone ed i dispositivi restano attivi.
- Se ci sono zone / dispositivi ritardati in allarme, la centralina inserisce normalmente; se la zona / dispositivo non si ripristina entro il tempo di uscita, scatta l'allarme.

In ogni caso se ci sono zone / dispositivi ritardati in allarme ed è prevista la segnalazione acustica del tempo di uscita, questa segnalazione verrà notificata normalmente come per l'inserimento manuale.

4.5 Scenari

Possono essere creati fino a 8 diversi scenari, che consistono in operazioni multiple, anche temporizzate, registrabili in configurazione. Esempio: inserire un'area e successivamente comandare una uscita tramite un evento programmabile.

Una volta creato uno scenario è azionabile da radiocomando o da App SICEP.

4.6 Sirena

La centralina DOGMA dispone di sirena interna di tipo piezoelettrico. Un' apposita funzione limita il tempo massimo di attivazione della sirena a 20 minuti cumulativi. Una volta raggiunto questo limite la sirena non suona più; per riattivarla è necessario disinserire e reinserire una qualsiasi area.

4.7 Uscita On Board

E' disponibile un'uscita di tipo open collector riferita a massa (GND) in grado di pilotare un carico massimo di tipo resistivo di 200mA. L'uscita è programmabile come statica (bistabile) o impulsiva (monostabile) e può essere attivata in più modi:

- In base a un qualsiasi evento del sistema (batteria scarica sensori, area 1 inserita, ecc.);
- Manualmente dall'utente, da una tastiera o da un radiocomando mediante l'utilizzo di "eventi".

4.8 Riduzione dei Falsi Allarmi

Al fine di evitare falsi allarmi, il sistema DOGMA comprende una serie di funzioni programmabili come ad esempio:

- Zone in "AND". Solo l'attivazione di due zone entro un intervallo programmabile causano la condizione di allarme.
- Conteggio impulsi entro una finestra temporale applicabile ad ogni singola zona o dispositivo.
- Esclusione automatica delle zone/dispositivi, dopo un numero programmabile di attivazioni, la zona o dispositivo viene automaticamente escluso dal sistema e non vengono più generati allarmi su sirena e comunicazioni telefoniche fino al prossimo inserimento dell'area di appartenenza.
- Tempi di Ingresso e Uscita riprodotti tramite toni acustici dagli organi di comando.
- Tempo di ritardo sulla comunicazione telefonica degli allarmi. Se il sistema viene inserito entro il tempo di ritardo la comunicazione telefonica dell'allarme non viene effettuata.

4.9 Comunicatore

La centralina DOGMA integra un sistema di comunicazione programmabile che può inviare le informazioni relative agli eventi a vari destinatari con più vettori.

La comunicazione utilizza vettori diversi a seconda se il destinatario è l'Istituto di Vigilanza oppure un utente privato.

I vettori di comunicazione principali sono la rete LAN o WI-FI. Se il collegamento con questi vettori non è possibile, viene tentato un collegamento di backup tramite il modulo GSM LTE/GPRS sempre che sia fornito di carta SIM. Il primo tentativo di comunicazione con la Centrale Operativa viene effettuato in LTE/GPRS e successivamente, se anche questo fallisce, in SMS dati.

4.9.1 Comunicazioni verso il gestionale MvsNET

La comunicazione può essere inviata tramite tre vettori alternativi. La priorità è fissa. Se l'invio tramite un vettore non ottiene conferma, la centralina passa al vettore successivo.

Il primo vettore è l'invio tramite LAN (ethernet) se la connessione LAN è presente, la rete è configurata per l'accesso a Internet ed è stato programmato l'indirizzo IP o l'hostname della Centrale Operativa. La comunicazione con questo vettore/protocollo può essere diretta solo a Centrali Operative che utilizzano il gestionale Sicep MvsNET (dalla versione 1.05.1622).

Il secondo vettore è l'invio tramite LTE/GPRS, se è presente una SIM che permetta l'accesso a Internet e se è stato programmato l'indirizzo IP o l'hostname della Centrale Operativa. Come sopra, la comunicazione con questo vettore/protocollo può essere diretta solo a Centrali Operative che utilizzano il gestionale Sicep MvsNET.

Il terzo vettore è l'invio di un SMS dati (binario) verso il modulo GSM della Centrale Operativa, sempre se è presente una SIM nella centralina. La comunicazione con questo vettore/protocollo può essere diretta solo a Centrali Operative che utilizzano il gestionale Sicep MvsNET.

4.9.2 Comunicazione verso gestionale con protocollo standard SIA-IP DC09

La centralina DOGMA, grazie al suo sistema di comunicazione programmabile, permette anche l'invio delle varie segnalazioni e la ricezione delle conferme utilizzando il protocollo standard Contact-ID su IP (protocolli SIA DC09/SIA DC05). La comunicazione può avvenire via LTE/GPRS o LAN. La centrale trasmette i codici programmati nella pagina *Gestione Eventi* Contact-ID. Tramite questo protocollo non è possibile effettuare alcuna interrogazione dalla Centrale Operativa. La comunicazione da e verso la Centrale Operativa può essere crittografata con la chiave crittografica personalizzabile a 32 o 64 caratteri esadecimali (0-9 A-F).

4.9.3 Comunicazioni verso gli utenti

Sono disponibili 8 destinatari telefonici e 8 destinatari e-mail. Ogni evento può essere inviato a uno o più utenti, scelti in base all'evento stesso; il vettore è associato a ciascun numero impostato.

I protocolli/vettori possibili sono i seguenti:

- SMS testo. Può essere inviato solo tramite GSM e consiste in un messaggio di testo contenente la descrizione dell'evento, così come viene riportata nello storico della centralina.

- E-mail. Possono essere inviate sia tramite LAN (ethernet) che LTE/GPRS; l'invio tramite LAN è prioritario. Sono disponibili 8 diversi destinatari; poiché le e-mail non possono avere conferma, se sono programmati due indirizzi, l'invio avviene sempre verso entrambi i destinatari. La centralina DOGMA può gestire l'autenticazione e l'uso del protocollo di crittografia se il server SMTP utilizzato lo richiede.

Per mezzo del Cloud Sicep è possibile notificare una selezione di eventi personalizzabile per ogni singolo utente. La notifica verrà così inoltrata a quei dispositivi mobili che l'utente stesso ha provveduto a registrare sul Cloud.

4.9.4 Configurazione dei dispositivi di rete

Qui di seguito è descritta una situazione di utilizzo tipica per il collegamento di rete della centralina Sicep DOGMA, tenendo presente che il grado di complessità può essere diverso in base al tipo di utilizzo e situazione.

Questi i possibili scenari:

- La centralina DOGMA è collegata in una rete locale (LAN) che si interfaccia a Internet tramite un router ADSL/DSL. L'indirizzo IP esterno del router è di tipo dinamico e assegnato dall'ISP (Internet Service Provider); è la tipica configurazione domestica.
- La Centrale Operativa dispone di un router ADSL/DSL con almeno un IP statico; tale router interfaccia la rete interna alla Centrale Operativa, dove è presente il server MvsNET e uno o più computer client.
- L'installatore dispone di PC in rete locale (LAN) interfacciata a Internet tramite un router ADSL/DSL con IP dinamico; è la stessa situazione in cui è installata la centralina DOGMA.

Cosa si deve configurare nella rete locale dove è installata la centralina DOGMA

Il router ADSL/DSL non deve essere configurato per la comunicazione con la Centrale Operativa in quanto la centralina stessa tramite un processo denominato "Keep Alive" aprirà automaticamente le porte per la comunicazione verso l'esterno. Deve invece essere configurato per poter permettere l'accesso dall'esterno tramite Sicep ed il software Sicep Cloud Connect. In questi casi si dovranno aprire le porte di comunicazione **8000 per Sicep Cloud Connect e 8002 per Sicep**; si dovrà inoltre impostare il percorso delle comunicazioni dalla rete esterna alla rete interna che utilizzano queste porte, verso l'indirizzo IP interno assegnato alla centralina.

Cosa si deve configurare nella rete locale della Centrale Operativa

Sul router della Centrale Operativa devono essere aperte le porte 9001 UDP e 9016 TCP; il traffico in arrivo verso queste porte deve essere inviato all'indirizzo IP del server MvsNET. Tutte le periferiche e centraline Sicep utilizzano questa configurazione.

Cosa si deve configurare nella rete locale dell'installatore

Poiché l'installatore di solito non dispone di IP statico, si deve ricorrere a un servizio esterno che gestisca l'IP dinamico, ad esempio DynDNS. Tramite questo servizio è possibile disporre di un hostname a scelta (es. mariobianchi45) che sarà inserito nella periferica (parametro Hostname Installatore).

Nel router è presente una pagina di configurazione (Dynamic DNS o simili) in cui dovrà essere configurato l'accesso a tale servizio; normalmente sono richiesti i dati per l'accesso autenticato, cioè username e password.

Dovranno essere aperte le porte 9001 UDP e 9016 TCP; il traffico in arrivo verso queste porte deve essere inviato all'indirizzo IP del PC nel quale si utilizza il software Sicep Cloud Connect.

4.10 Cloud Sicep

La centralina è già predisposta per una connessione al server Cloud Sicep.

Una volta installata e collegata in rete, tramite interfaccia LAN / Wi-Fi o LTE/GPRS, la centralina si collegherà automaticamente. Se la connessione è avvenuta con successo, visualizzeremo lo Stato della connessione nella pagina *Comunicatore* → *Cloud* → *Impostazioni Cloud* in VERDE con la dicitura "Connesso".

Per poter registrare Sicep o Sicep Cloud Connect sulla centralina, si dovrà richiedere il codice OTP mediante il pulsante "Richiedi codice" e successivamente copiare il codice

sull'applicazione.

Il codice OTP formato da 8 cifre, consente la registrazione dell'APP in modo sicuro in quanto ha una scadenza di 120" dopodiché non è più utilizzabile e deve essere effettuata una nuova richiesta.

4.11 Gestione della centralina da MvsNET

La centralina DOGMA è sempre in grado di inviare gli allarmi spontanei (eventi) con tutti i protocolli disponibili, mentre l'interrogazione avviene in modi diversi:

- L'interrogazione via LAN avviene verso l'ultimo indirizzo IP trasmesso dalla centralina stessa;
- L'interrogazione via LTE/GPRS avviene con uno "squillo di risveglio" tramite l'interfaccia GSMTA;
- L'interrogazione tramite SMS avviene tramite l'invio di un SMS di tipo MVS.

ATTENZIONE!

Gli SMS sono in genere a pagamento e possono incidere sui costi del sistema.

Nel caso di comunicazioni dirette sia verso MvsNET che verso gli utenti, le trasmissioni seguono l'ordine riportato qui di seguito:

1. Evento su LAN
2. Evento in LTE/GPRS
3. Evento in SMS verso il gestionale
4. Utenti della lista iniziando dal primo
5. E-mail, iniziando dal destinatario 1

4.12 Gestione Teleassistenza

Per teleassistenza si intende la possibilità che ha l'installatore o l'Amministratore di collegarsi alla centralina da una postazione remota e poter modificare la configurazione. L'accesso dell'installatore può essere abilitato/disabilitato dall'utente Amministratore.

Ci sono due possibilità per effettuare la teleassistenza: tramite LAN o tramite LTE/GPRS. In entrambi i casi si deve utilizzare il software Sicep Cloud Connect.

4.12.1 Teleassistenza tramite LAN

Per questo tipo di collegamento è richiesto nel PC dell'installatore un IP statico pubblico, oppure l'utilizzo di un servizio Dynamic DNS (consultare la relativa sezione di questo manuale).

4.12.2 Teleassistenza tramite LTE/GPRS

Anche per questo tipo di collegamento è richiesto nel PC dell'installatore un IP statico pubblico, oppure l'utilizzo di un servizio Dynamic DNS, inoltre deve essere effettuato uno squillo di risveglio per attivare il collegamento. Questo squillo deve avvenire tramite un telefono fisso o mobile il cui numero chiamante deve essere stato inserito nella centralina (*Comunicatore → Teleassistenza → Numero telefonico teleassistenza LTE/GPRS*).

4.13 Il protocollo di comunicazione radio BiTech

La centralina DOGMA utilizza un' apposita gamma di sensori e dispositivi wireless con protocollo di comunicazione radio proprietario Sicep denominato "BiTech".

4.13.1 Come funziona

Tutte le comunicazioni fra centralina DOGMA e dispositivi wireless, avvengono in modo bidirezionale e sincrone, ovvero ogni dispositivo ha un proprio intervallo di tempo in cui può dialogare con la centralina all'interno di un ciclo di 2 secondi. In questo modo si hanno particolari vantaggi:

- Un notevole risparmio della batteria, perché ogni sensore attiva la parte ricevente (e trasmittente) solo per un piccolo intervallo di tempo;
- Reale supervisione dei sensori e funzionamento "intelligente" di quest'ultimi: quando l'area di appartenenza è disinserita, una parte del circuito può essere spenta per risparmiare ulteriormente il consumo della batteria;
- Totale assenza di collisioni e quindi utilizzo ottimale del canale radio.
- Scelta fra 3 canali radio di comunicazione

La centralina DOGMA può gestire un massimo di 28 dispositivi wireless generici più un massimo di 4 ripetitori di segnale radio.

Ciascun dispositivo wireless è alimentato da una o due batterie al Litio.

4.13.2 Gestione dei dispositivi registrati

La centralina instaura periodicamente un dialogo con tutti i dispositivi. Quando un dispositivo non riesce a comunicare con la centralina per almeno due minuti, innesca una procedura automatica di ripristino della comunicazione. La centralina considera mal funzionante un dispositivo se non c'è scambio dati con questo ultimo per un tempo programmabile da 20 a 720 minuti. La centralina è in grado di rilevare la presenza di un qualsiasi disturbo sul canale radio utilizzato che potrebbe influenzare il corretto funzionamento del sistema e generare l'evento Accecamento Radio.

4.13.3 Codice Impianto o Serial Number

Ogni centralina BiTech contiene un numero di serie identificativo (generato in modo casuale ma non sequenziale) che viene assegnato in modo univoco in fase di costruzione. Questo numero che identifica l'impianto non è modificabile e fa sì che ogni dispositivo possa funzionare solo sulla centralina su cui è stato registrato. E' comunque sempre possibile cancellare un dispositivo da un impianto e registrarlo su un altro. I dispositivi si registrano sulla centralina seguendo una semplice procedura; non deve essere effettuata nessuna programmazione sul sensore perché tutti i parametri di funzionamento vengono programmati nella centralina e al termine della programmazione, premendo un pulsante, vengono trasferiti nel dispositivo.

4.13.4 Test qualità del collegamento radio

Il sistema radio BiTech dispone, in fase di installazione o programmazione, di uno strumento diagnostico per misurare la qualità del collegamento radio di ogni singolo dispositivo. Il funzionamento del test è il seguente:

- La centralina trasmette una serie di messaggi di test verso il sensore in prova, diminuendo via via la potenza su 4 livelli. In base ai messaggi confermati viene assegnata una valutazione.
- Nel caso di test di un dispositivo ripetuto da un REP (o mediante due REP in cascata), viene eseguito il test della tratta radio fra il dispositivo e il REP a lui più vicino; per il test delle tratte intermedie basta ripetere la stessa prova sui due REP.

Qualità Segnale RF
ASSENTE
SCARSO
SUFFICIENTE
BUONO
OTTIMO

Comunicazione

Connessione **Connesso**

Qualità Segnale RF **OTTIMO**

Test Segnale

4.13.5 Test del livello di batteria dei dispositivi radio

Ogni dispositivo BiTech comunica periodicamente alla centralina il livello della batteria di cui è dotato. Il test di efficienza della batteria viene effettuato da ogni singolo dispositivo andando a misurare il livello di tensione presente nel momento di massimo assorbimento. Il livello di tensione batteria riportato in centralina, consente a questa di stabilire le condizioni di "Batteria Scarica" o "Batteria Carica".

5. Installazione

Di seguito sono descritte le operazioni per l'installazione della centralina DOGMA e di tutto il sistema antifurto Sicep BiTech; è preferibile svolgere le operazioni nella sequenza descritta.

5.1 Scelta del luogo per l'installazione della centralina

La centralina DOGMA è progettata per essere installata nelle abitazioni o in edifici industriali con condizioni ambientali simili agli ambienti residenziali. In ogni caso il luogo scelto deve rispettare quanto riportato nelle Caratteristiche Tecniche del presente manuale (requisiti ambientali) e deve essere asciutto, esente da infiltrazioni d'acqua, polveri e fonti di calore. Se si utilizzano i dispositivi wireless non installare la centralina in luoghi molto schermati perché ciò potrebbe pregiudicare la portata radio dei sensori. Evitare di installare la centralina nei seguenti ambienti: cantine, stanze o ripostigli con pareti interamente in cemento armato, box metallici.

La centralina DOGMA integra un comunicatore GSM LTE/GPRS che è soggetto alle stesse limitazioni imposte per l'uso dei telefoni cellulari. Tali limitazioni possono essere applicate ad ambienti particolari, come ospedali, cliniche e tutti i luoghi in cui è obbligatorio spegnere i telefoni cellulari. In queste situazioni devono essere rispettate le limitazioni richieste pertanto il comunicatore GSM non può essere utilizzato.

5.2 Come aprire e chiudere la centralina

Il coperchio della centralina è incernierato nella parte alta del contenitore e bloccato con due agganci nella parte bassa. Per aprirla, premere contemporaneamente sui due agganci nella parte bassa del coperchio frontale.

Per la chiusura del contenitore, agganciare le cerniere superiori per poi ruotare fino al blocco a scatto inferiore.

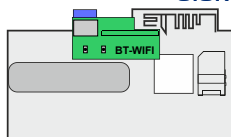


5.3 Installazione dispositivi opzionali

Prima di fissare al muro la centralina si consiglia di installare i dispositivi opzionali.

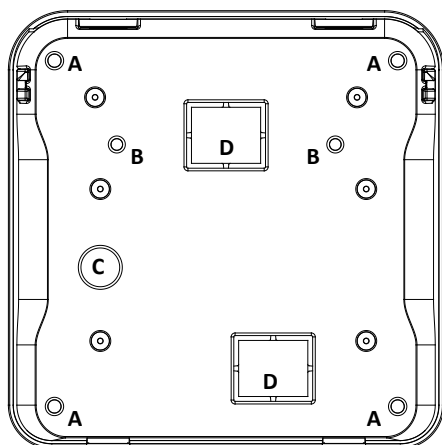
5.3.1 Installazione scheda interfaccia BT-WIFI

- Assicurarsi che la centralina non sia alimentata.
- Inserire il modulo radio nel connettore "P2" come mostrato in figura.
- Alimentare nuovamente la centralina.



5.4 Fissaggio e cablaggio Centralina DOGMA

Fissare al muro la centralina utilizzando 4 viti di diametro 4mm e appositi tasselli. Per migliorare le comunicazioni con i dispositivi wireless, evitare di installare la centralina nelle immediate vicinanze di strutture metalliche o rispettare una distanza minima di un metro.



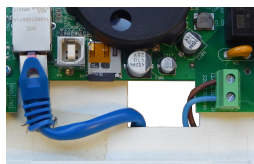
- A Fori di fissaggio a parete
- B Fori di fissaggio per scatola da incasso mod. 503
- C Foro per antistrappo
- D Aperture per passaggio cavi

5.4.1 Fissaggio magnete antistrappo

Fissare il magnete antistrappo alla parete in corrispondenza del foro circolare "C". Fare attenzione a non stringere troppo la vite di fissaggio per evitare la rottura del magnete. Nel caso non si intenda fissare il magnete alla parete, è comunque possibile disabilitare la funzione "antistrappo" nella pagina di configurazione della centralina.

5.4.2 Cablaggio centralina

1. In assenza della scheda BT-WIFI, connettere il cavo di rete ethernet sul connettore P6.
2. Inserire la carta SIM nel connettore X15
3. Cablare il cavo di alimentazione sul connettore P7
4. Connettere la batteria al connettore P8.
5. Alimentare la centralina da rete elettrica.
6. Premere e rilasciare il pulsante di RESET.
7. Assicurarsi che la procedura di avvio sia completata:
 - 3 lampeggi led Verde di alimentazione RETE,
 - Accensione per 2 secondi del led Rosso TX BiTech,
 - Nuova accensione del led Verde RETE.
 - Se installato cavo ethernet, verificare accensione led DATI LAN.



ATTENZIONE!

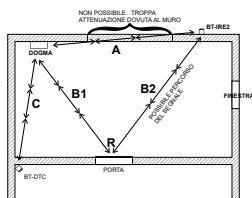
Apparecchio in categoria di sovratensione II (CAT II 2500 V). Se l'apparecchio, una volta installato, fosse soggetto a tensioni transitorie superiori a quelle della categoria di sovratensione di progetto, allora necessita dell'installazione di una protezione supplementare dalle tensioni transitorie esterna all'apparecchiatura.

ATTENZIONE!

Poiché la centralina non è dotata di interruttore di alimentazione da rete. Se necessario, per interrompere l'alimentazione, prevedere un interruttore bipolare conforme alle norme sugli impianti e sui lavori elettrici del Paese di impiego.

5.5 Installazione dispositivi wireless

La rete radio BiTech funziona a 868MHz. A questa frequenza il segnale radio si propaga in linea retta, può attraversare i muri ma in base allo spessore e al tipo di muro stesso, il segnale viene più o meno attenuato. Può venire riflesso principalmente da oggetti metallici. Quando si installano i sensori o gli altri dispositivi wireless bisogna sempre tenere presente questo comportamento per evitare di fare una installazione critica nel tempo. Cerchiamo di vedere cosa può succedere con un semplice esempio. Nel disegno è rappresentata la pianta parziale di una abitazione dove è installata una centralina DOGMA e due sensori. Il sensore BT-DTCX è raggiunto dalla centralina attraversando il muro su cui è installato; il percorso del segnale radio è diretto ed è indicato con C. Ciò è possibile perché lo spessore del muro attraversato è piccolo. Il sensore BT-IRE2 invece è posto in una tipica posizione difficile da raggiungere. Il percorso diretto, contrassegnato con A, non è possibile: il segnale non può attraversare il muro lungo il suo spessore perché in questo modo viene troppo attenuato. Se il test radio indica che il sensore è raggiungibile dalla centralina, il segnale radio sfrutta almeno una riflessione. Molto probabilmente il percorso è quello indicato da B1-B2, dove il segnale viene riflesso da qualche oggetto metallico posto in prossimità del punto R. Questa è una situazione a rischio: se la superficie riflettente è come nell'esempio una porta metallica, quando questa viene aperta, la riflessione cambia e può darsi che in questa condizione il sensore non raggiunga più la centralina e viceversa. In una installazione di questo tipo il controllo delle Statistiche del dispositivo si rivela molto utile, perché fornisce l'andamento delle condizioni nell'ultima settimana di funzionamento. Quando il sensore non raggiunge la centralina quest'ultima non riceve più i messaggi di "presenza"; dopo poco tempo il sensore è dichiarato "critico". Per risolvere una situazione del genere è opportuno utilizzare un REP posto in prossimità della presunta riflessione; in questo caso potrebbe essere collocato sopra la porta.



5.6 Registrazione dei dispositivi wireless

Per effettuare la registrazione dei dispositivi wireless sulla centrale Dogma è necessario entrare in programmazione con il software Sicep Cloud Connect o da App SICEP.

5.6.1 Registrazione da software Sicep Cloud Connect

Per stabilire il collegamento ed entrare in programmazione fare riferimento alla sezione "6.2 Sicep Cloud Connect" a pagina 33.

Da Sicep Cloud Connect, una volta stabilito il collegamento:

- Aprire il contenitore del sensore/dispositivo (consultare le istruzioni dello stesso) ed inserire la batteria rispettando la polarità.
- Aprire la pagina "Sistema", sotto-pagina *Impostazioni e Tempi*; porre la centralina nello stato di *Manutenzione* = ON mediante l'apposito bottone. Questo escluderà l'azionamento della sirena e del comunicatore.
- Scegliere il canale radio da utilizzare per l'impianto. Tenere presente che una volta registrati i dispositivi wireless, se si vorrà cambiarlo sarà necessario ripetere la registrazione di tutti i dispositivi.
- Aprire la pagina "Dispositivi RF". Verrà visualizzata la mappa, cioè l'elenco di tutti i dispositivi RF registrati sulla centrale.
- Premere il pulsante "Aggiungi dispositivo" nella mappa dispositivi RF.
- Premere il pulsante TEST sul sensore/dispositivo e tenerlo premuto fino all'accensione dei led. Appena registrato, apparirà la voce corrispondente con accanto l'indicazione del tipo (KPXW, IRWX, IRE, CMW, DTCX, DTWX...).
- Ripetere l'operazione per registrare tutti gli altri sensori/dispositivi.
- La procedura di registrazione può variare in base al dispositivo.

ATTENZIONE!

Prima di procedere con la registrazione dei dispositivi radio, assicurarsi che la centralina sia in manutenzione altrimenti, nel momento in cui viene registrato il sensore, scatterà l'allarme Tamper dello stesso.

NOTA.

- I codici da 1 a 8 sono riservati ai REP; tutti gli altri dispositivi vengono registrati assegnando loro un numero progressivo che inizia da 9.
- La prima lettura della tensione della batteria di un sensore può dare un valore errato.

ATTENZIONE!

Se il sensore è già stato registrato su un altro impianto, è necessario eseguire un reset della configurazione: con il tamper aperto, premere contemporaneamente i tasti Test e Reset, rilasciare il reset mantenendo premuto il Test a lungo fino all'accensione dei due led rosso e verde.

5.6.2 Registrazione da App SICEP

Da App SICEP, una volta stabilito il collegamento:



- Aprire il contenitore del sensore/dispositivo (consultare le istruzioni dello stesso) ed inserire la batteria rispettando la polarità.
- Tramite l'App SICEP, accedere alle Impostazioni con il pulsante dedicato.
- Dalla pagina *Centrale / Generale* attivare il flag *Manutenzione* per escludere l'azionamento delle sirene e del comunicatore.
- Tornare alla pagina principale delle impostazioni ed accedere alla sezione dedicata ai *Dispositivi RF*.
- Premere il pulsante *Aggiungi Dispositivo*.
- Premere il pulsante **TEST** sul sensore/dispositivo e tenerlo premuto fino all'accensione dei led. Appena registrato, apparirà la voce corrispondente con accanto l'indicazione del tipo (KPXW, IRWX, IRE, CMW, DTCX, DTWX...).
- Ripetere l'operazione per registrare tutti gli altri sensori/dispositivi.
- La procedura di registrazione può variare in base al dispositivo.
- Valgono le note riportate nel precedente paragrafo.

5.6.3 Registrazione Tastiera BT-SKW

- Aprire la tastiera (consultare le istruzioni dello stesso) ed inserire le batterie rispettando la polarità.
- Avviare la richiesta di registrazione di un nuovo dispositivo da Sicep Cloud Connect o da App SICEP come descritto nei paragrafi "5.12.1 Registrazione da software Sicep Cloud Connect" a pagina 35 e "5.12.2 Registrazione da App SICEP" a pagina 35.
- Risvegliare la tastiera premendo sul tasto . Premere il tasto **MENU** sulla tastiera; scorrere l'elenco utilizzando le frecce , selezionare **REG./CANC** Tastiera e premere .
- Appena registrata, apparirà la voce corrispondente nella Mappa "Dispositivi RF" con accanto l'indicazione del tipo (SKW).

5.6.4 Registrazione sensore di fumo BT-SMK2

- Avviare la richiesta di registrazione di un nuovo dispositivo da Sicep Cloud Connect o da App SICEP come descritto nei paragrafi "5.6.1 Registrazione da software Sicep Cloud Connect" a pagina 27 e "5.6.2 Registrazione da App SICEP" a pagina 28.
- Entro alcuni secondi, inserire la batteria nel sensore BT-SMK2. All'avvio il sensore invia il comando di registrazione.
- Il sensore deve apparire nella lista dei dispositivi registrati con l'identificativo SMK2.

5.6.5 Registrazione Radiocomando BT-KT

Registra telecomando +

Registra

- Questo dispositivo è già dotato di batteria installata. Il radiocomando è l'unico dispositivo wireless che deve essere assegnato direttamente agli utenti.
- **Tramite l'App SICEP,**
 - Accedere alle Impostazioni con il pulsante dedicato.
 - Dalla pagina *Utenti*, selezionare l'utente a cui associare il telecomando.
 - Premere **Registra Telecomando**.
- **Da Sicep Cloud Connect,**
 - Aprire la pagina *Utenti* e selezionare l'utente a cui associare il telecomando.
 - Nella sezione *Radiocomando*, premere il pulsante **Registra**.



- Premere sul radiocomando i tasti **INSERIMENTO PERIMETRALE** e **INSERIMENTO TOTALE** e tenerli premuti fino all'accensione del led; l'accensione del led **P** unita al segnale acustico conferma l'avvenuta registrazione.
- Ripetere l'operazione per registrare tutti gli altri radiocomandi.

NOTA.



Se il radiocomando è stato già registrato su un altro impianto e si desidera eseguire un reset della configurazione: tenere premuti a lungo i tasti indicati a lato; quando tutti i 4 led si accendono contemporaneamente, la configurazione è stata cancellata. Questo modello di radiocomando consente di registrare fino a 4 impianti diversi contemporaneamente.

5.7 Cancellazione di un dispositivo wireless dalla centralina

Può succedere di dover rimuovere un dispositivo wireless dalla centralina. Nel caso in cui si voglia solo disabilitare **temporaneamente** il dispositivo, è sufficiente disabilitarlo nella sua pagina di configurazione da Sicep Cloud Connect o da App SICEP; deve essere tolta la spunta dal flag **"Abilitato"**. Nel caso invece si abbia necessità di rimuovere **permanentemente** il dispositivo dall'impianto è necessario procedere come segue:

Se il dispositivo è ancora funzionante,



- **Tramite l'App SICEP,**
 - Accedere alle Impostazioni con il pulsante dedicato.
 - Dalla pagina **Generale** attivare il flag **Manutenzione** per escludere l'azionamento delle sirene e del comunicatore.
 - Tornare alla pagina principale delle impostazioni ed accedere alla sezione dedicata ai **Dispositivi**, quindi **Dispositivi RF**.
 - Premere il pulsante **Cancella Dispositivo**.



- **Da Sicep Cloud Connect,**
 - Aprire la pagina **"Sistema"**, sotto-pagina **Impostazioni e Tempi**; porre la centralina nello stato di **Manutenzione** = ON mediante l'apposito bottone. Questo escluderà l'azionamento della sirena e del comunicatore.
 - Aprire la pagina **"Dispositivi RF"**. Verrà visualizzata la mappa, cioè l'elenco di tutti i dispositivi registrati sulla centrale.
 - Premere il pulsante **"Cancella dispositivo"** nella mappa dei dispositivi.
- Premere il pulsante **TEST** sul dispositivo da cancellare e tenerlo premuto fino alla scomparsa dall'elenco dei dispositivi. Nel caso della tastiera BT-SKW, del sensore di fumo BT-SMK2 o del telecomando BT-KT, utilizzare la stessa procedura usata per la registrazione.
- Togliere la centrale di allarme dallo stato di **Manutenzione** dalla pagina **Generale** (per App SICEP) o dalla pagina **Sistema** (per Sicep Cloud Connect).

Se il dispositivo non è funzionante,



- **Tramite l'App SICEP,**
 - Accedere alle Impostazioni con il pulsante dedicato.
 - Dalla sezione dedicata ai **Dispositivi**, accedere a **Dispositivi RF**.
 - Accedere al dispositivo da disabilitare e quindi alle **Impostazioni dispositivo**.
 - Premere il pulsante **Scollega dispositivo**.

Scollega dispositivo

- **Da Sicep Cloud Connect,**
 - Aprire la pagina **"Dispositivi RF"**. Verrà visualizzata la mappa, cioè l'elenco di tutti i dispositivi registrati sulla centrale.
 - Selezionare il dispositivo da cancellare e quindi deselezionare il flag **Abilitato/a**.
 - Premere il pulsante **Cancella** per scollegare il dispositivo dalla centrale di allarme.

Cancella

6. Programmazione

La programmazione può avvenire tramite App SICEP o tramite PC con software Sicep Cloud Connect. La programmazione della centralina è disponibile solamente agli utenti Installatore e Amministratore (se abilitato).

6.1 App SICEP

App SICEP è l'applicazione che consente agli utenti la gestione da remoto delle centrali di allarme di ultima generazione di Sicep comodamente dal proprio smartphone o tablet. E' disponibile sia per sistema operativo Android che per iOS ed è scaricabile gratuitamente dai rispettivi Store.

Attraverso questa applicazione, l'utente può controllare varie funzionalità dell'impianto di allarme dipendenti dal modello di centrale installata.

In elenco le funzionalità principali:

- Visualizzare lo stato, inserire e disinserire le singole aree dell'impianto;
- Verificare la presenza di guasti o anomalie;
- Verificare la presenza e cancellare la memoria degli allarmi;
- Visualizzare lo stato dei comandi ed attivarle;
- Scattare foto nel caso vi siano sensori dotati di fotocamera;
- Visualizzare i video in diretta delle telecamere;
- Accedere allo storico degli eventi, e visualizzare eventuali foto associate;
- Visualizzare lo stato delle zone e dispositivi del sistema e eventualmente abilitarli e disabilitarli;
- Visualizzare informazioni sulla SIM e il livello del segnale GSM della centrale;
- Gestire gli utenti: abilitare accessi da tastiera e da remoto, registrare telecomandi/Tag.

NOTA. *Alcune funzioni possono non essere disponibili per ogni utente.*

6.1.1 Login

L'utilizzo dell'App SICEP necessita di un account a cui collegare gli impianti di allarme. Lo stesso account può essere utilizzato sul software Sicep Cloud Connect o su altre App SICEP: questo permette la sincronizzazione più dispositivi e la possibilità di trasferire i propri dati su un nuovo dispositivo semplicemente inserendo le credenziali di accesso.

Se non si dispone già di un account, è possibile crearlo inserendo un indirizzo e-mail valido, una password e premere Registrati e seguire la procedura.

SICEP

Accedi
Effettua l'accesso inserendo le tue credenziali

Email

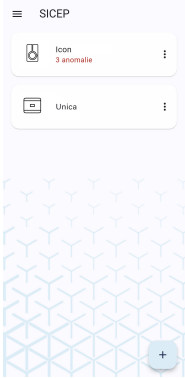
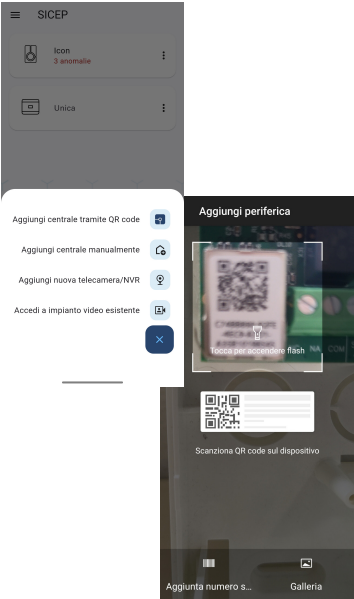
Password

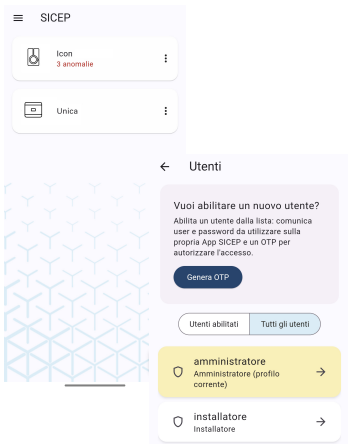
[Recupera password](#)

Entra

[Non hai un account? Crea ora](#)

6.1.2 Prima configurazione

Operazione Utente	Risposta App	Simbolo
Prima configurazione Eseguire l'applicazione cliccando sull'icona presente sullo smartphone. Alla voce configurazione è possibile abilitare il Login automatico (che disabilita la richiesta PIN), oppure modificare il codice del PIN per il prossimo accesso. Se lo smartphone dispone di identificazione biometrica (lettore di impronte digitali o riconoscimento facciale), l'App richiederà l'abilitazione per utilizzarlo in alternativa al PIN.		
Nella schermata successiva, "Periferiche" toccare il tasto + per l'inserimento di un nuovo impianto di ALLARME o di VIDEOSORVEGLIANZA. In caso di prima configurazione è possibile registrare il dispositivo scansionando il QR Code che è all'interno della Centrale. Aggiungere successivamente: • Il nome impianto • L'ubicazione (non obbligatorio) Se già configurata scegliere l'inserimento manuale dei dati: • Il nome impianto • L'ubicazione (non obbligatorio) • Il nome utente per l'accesso da remoto¹ • La password per l'accesso da remoto¹ • Il codice di autenticazione (OTP) fornito da un Amministratore o un Installatore. ¹ è consigliato non utilizzare il nome utente e la password di default. Poi premere "Associa impianto" per salvare.		

Selezionando la centrale desiderata si instaura un collegamento verso quella centrale come programmato. La richiesta di un nuovo codice OTP per la registrazione di una nuova app può essere fatta dalla pagina <i>Impostazioni / Utenti</i> con il pulsante <i>Genera OTP</i> o dall'elenco delle periferiche tramite il breve menu contestuale alla centrale di allarme.		Genera OTP
--	---	--------------------------

6.1.3 Pagina principale HOME

Una volta instaurato il collegamento, appare la pagina principale per l'utilizzo delle funzioni base e la visualizzazione dei parametri principali dell'impianto di allarme.

Stato aree disponibili e pulsanti di gestione		Pulsante impostazioni Pulsanti per Inserimento e Disinserimento area Eventi programmabili preferiti Pagine disponibili
--	--	--

6.1.4 Icone di stato

In alto sono presenti delle piccole icone; è importante sapere cosa significano. Alcune icone sono sempre presenti, altre solo in certe condizioni.

	Alimentazione a 220V dalla rete elettrica presente.
	Anomalia: Alimentazione a 220V è assente.
	Batteria della centrale antifurto è carica e in buono stato.
	Anomalia: la batteria è presente ma è da sostituire (esaurita).
 Attività	Memoria allarme: una o più aree sono andate in allarme.
	Anomalia: indica che è presente almeno una condizione di guasto pertanto è necessario l'intervento del tecnico installatore per la sua risoluzione. Esempi: un sensore ha la batteria scarica o il contenitore aperto, la batteria della centralina è da sostituire, il collegamento verso l'istituto di vigilanza è assente, ecc.
	Indica che la centralina si trova nella condizione di manutenzione : gli allarmi non azionano le sirene e le comunicazioni verso gli utenti non vengono inviate. In questa condizione i dispositivi di comando emettono un "bip" ogni 10 secondi come promemoria. Durante il funzionamento normale la centralina non deve trovarsi in questa condizione.

6.1.5 Pagina Impostazioni Centralina



Per accedere alle impostazioni della Centralina, premere il pulsante dedicato.

Quest'area varia a seconda dell'utente collegato: l'Installatore e l'Amministratore avranno pieno accesso alla programmazione di base. Per la spiegazione delle funzioni disponibili di configurazione della centralina, consultare la sezione successiva dedicata al software Sicep Cloud Connect ricercando i parametri contrassegnati con il logo dell'App SICEP.

6.2 Sicep Cloud Connect

Questo software di tipo client in connessione con il dispositivo, permette di configurare in modo semplice ed intuitivo tutte le funzionalità della centrale antifurto. Consente inoltre, di verificare in tempo reale mediante spie luminose o messaggi, tutte le funzionalità della centralina.

Per il suo utilizzo, occorre installare il software scaricabile gratuitamente dal sito www.sicep.it su di un PC con sistema operativo Windows (7/8/10/11) avente una porta USB oppure un collegamento Ethernet.

6.2.1 Login



Sicep Cloud Connect utilizza un account dove salvare i dati. Lo stesso account può essere utilizzato su App SICEP o su altri software Sicep Cloud Connect: questo permette la sincronizzazione tra più dispositivi e la possibilità di trasferire i propri dati su un nuovo dispositivo semplicemente inserendo i propri dati di accesso.

Se non si dispone già di un account, è possibile crearlo inserendo un indirizzo e-mail valido, una password e premere Registrati e seguire la procedura.

6.2.2 Collegamento locale tramite porta USB

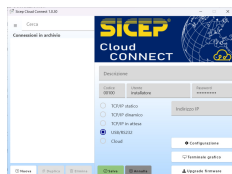
Per la connessione verso la centralina deve essere utilizzato un cavo di tipo A/B che andrà collegato sul connettore USB interno alla centralina.

Alla prima connessione, verrà chiesta l'installazione dell'apposito driver; i sistemi da Windows 7 in poi tentano l'installazione in automatico ma bisogna procedere manualmente. Per l'installazione vedi paragrafo "7.3 Installazione dei driver USB" a pagina 94.

6.2.3

Primo collegamento con cavo USB

- Collegare la centralina al PC tramite il cavo USB.
- Lanciare il programma Sicep Cloud Connect e impostare i seguenti parametri per la connessione:
 - Codice: 0100
 - Utente: installatore o amministratore
 - Password: installatore o amministratore
 - Vettore: USB/RS232



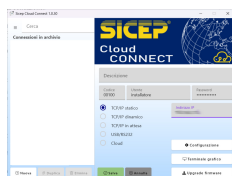
6.2.4

Primo collegamento tramite LAN

La centralina può essere programmata per la prima volta anche tramite collegamento Ethernet (non Wi-Fi). È necessario in questo caso che la centralina sia collegata su una rete locale dove è presente un server DHCP che assegnerà automaticamente un indirizzo IP alla centralina.

Diversamente l'unica modalità di accesso alla programmazione è tramite USB dove è possibile configurare i parametri relativi alla rete (indirizzo IP, subnet mask, eventuale gateway, eventuale hostname).

- Collegare la centralina alla rete locale tramite un cavo Ethernet.
- Alimentare la centralina o premere il pulsante Reset.
- Lanciare il programma Sicep Cloud Connect e impostare i seguenti parametri per la connessione:
 - Codice: 0100
 - Utente: installatore o amministratore
 - Password: installatore o amministratore
 - Vettore: TCP/IP statico
 - Indirizzo IP: dogma



6.2.5

Collegamento da remoto tramite LAN/WiFi

Questo collegamento è utilizzabile solo con centraline già programmate e collegate su una rete con accesso ad Internet. Le centrali di allarme possono essere state programmate con IP statico o dinamico.

6.2.6

Requisiti centralina per l'accesso da parte installatore

- L'accesso Installatore deve essere abilitato per il collegamento da remoto.
- La centralina deve essere stata programmata con l'indirizzo del router dell'installatore, che può essere un indirizzo IP statico o l'hostname relativo a un servizio tipo dyndns, nel caso che l'installatore non disponga di un indirizzo IP statico pubblico.

6.2.7

Collegamento da remoto in LTE/GPRS

Requisiti della centrale di allarme

- La SIM utilizzata nella centrale di allarme deve permettere il collegamento a Internet (LTE/GPRS).
- L'accesso Installatore deve essere abilitato per il collegamento da remoto.
- La centrale di allarme deve essere stata programmata con l'indirizzo del router dell'installatore, che può essere un indirizzo IP statico o l'hostname relativo a un servizio tipo dyndns, nel caso che l'installatore non disponga di un indirizzo IP statico pubblico.
- Deve essere programmato il numero di telefono dell'installatore dal quale verrà effettuata la chiamata (squillo di risveglio).

Requisiti per l'installatore

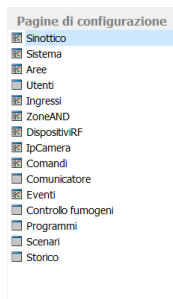
- Deve disporre di un PC collegato a Internet.
- Il router che utilizza per il collegamento a internet deve avere un IP statico, oppure deve utilizzare un servizio di risoluzione dinamica dell'indirizzo come Dyndns o simili.
- Deve disporre di un telefono per effettuare lo squillo di risveglio per attivare la connessione.

ATTENZIONE!

L'accesso alla programmazione da remoto è possibile solo se tutte le aree sono disinserite a meno che non sia stato abilitato l'apposito parametro nella pagina Sistema.

6.3 Parametri di programmazione con software Sicep Cloud Connect

Tutti i parametri di programmazione sono organizzati in pagine di configurazione di tipo dinamico. Per accedere alla pagina desiderata, selezionare l'icona corrispondente con il mouse. Una volta entrati in configurazione e modificati i parametri necessari, premere il tasto TAB per il suo salvataggio. Si è preferito presentare le pagine secondo un ordine di programmazione, in modo da guidare l'installatore passo passo per una rapida e logica configurazione dell'impianto.

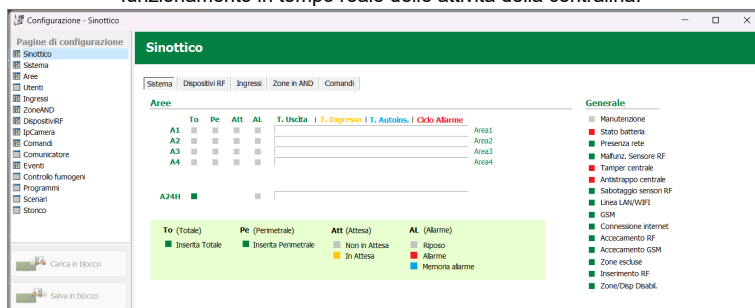


ATTENZIONE!

La modifica dei parametri della pagina Dispositivi RF forza lo stato delle aree nella condizione DISINSERITO. Pertanto nel caso di teleassistenza permessa con aree inserite sia in modo Perimetrale che Totale, una modifica ai parametri di queste pagine forzerà tutte le aree nello stato di Disinserito e si renderà necessario ripristinare manualmente lo stato precedente. Tutto questo non può accadere se il relativo parametro di accesso è disabilitato: in questo caso l'entrata in programmazione da remoto è possibile solo se tutte le aree sono disinserite. Per default l'accesso con aree inserite è disabilitato.

6.3.1 Pagina Sinottico

Questa pagina, composta da più sotto-pagine, ha lo scopo di mostrare lo stato ed il funzionamento in tempo reale delle attività della centralina.



6.3.2 Pagina Sistema

Questa pagina raggruppa i parametri che definiscono la configurazione base della centralina DOGMA.

Impostazioni / Tempi



Tempistiche, Tempo ciclo di allarme

Stabilisce la durata di un ciclo di allarme, ovvero il suono della sirena.

Valori programmabili: 0 - 600 secondi

Default: 20

Tempistiche, Riconoscimento assenza rete

Imposta il ritardo prima di generare l'allarme Mancanza Rete. Inserendo 0 l'evento è immediato.

Valori programmabili: 0 - 240 minuti

Default: 60

Tempistiche, Riconoscimento assenza comunicazione su LAN/WIFI

Imposta il ritardo prima di generare l'allarme Assenza LAN. Inserendo 0 l'evento è disabilitato

Valori programmabili: 0 - 240 minuti

Default: 0

Tempistiche, Riconoscimento assenza linea GSM

Imposta il ritardo prima di generare l'allarme assenza linea GSM. Inserendo 0 l'evento è disabilitato.

Valori programmabili: 0 / 5 - 240 minuti

Default: 0

Tempistiche, Riconoscimento assenza connessione internet

Imposta il ritardo prima di generare l'allarme Assenza connessione ad Internet. Inserendo 0 l'evento è disabilitato.

Valori programmabili: 0 - 240 minuti

Default: 0

Tempistiche, Prova Automatica

Stabilisce l'intervallo di tempo fra l'invio di due segnalazioni successive di Prova Automatica. Impostando 0 la funzione è disabilitata.

Valori programmabili: 0 - 14400 minuti

Default: 0

Tempistiche, Riconoscimento comunicazione assente con dispositivo RF

Quando un dispositivo RF non comunica più con la centralina, questo parametro imposta

il ritardo prima di generare l'evento Malfunzionamento dispositivo RF.

Valori programmabili: 20 / 45 / 60 / 90 / 120 / 720 minuti

Default: 45

Tempistiche, Riconoscimento accecamento Radio

Imposta il tempo di persistenza dell'oscuramento radio prima di generare l'allarme per Accecamento Radio.

Valori programmabili: Disab. / 1 / 2 / 4 / 8 / 10 minuti

Default: Disab

Tempistiche, Ripristino allarme furto

Questa impostazione stabilisce il comportamento del comunicatore per quanto riguarda il ripristino dell'allarme Furto; la disattivazione della sirena e dell'uscita eventualmente associata all'evento avvengono sempre al termine del tempo di ciclo allarme impostato.

Su fine ciclo allarme: il ripristino viene trasmesso al termine del tempo ciclo allarme, cioè allo spegnimento della sirena.

Su ripristino zona: il ripristino viene trasmesso quando la zona o il sensore torna a riposo. Nel caso di un sensore infrarosso wireless il ripristino è immediato.

Default: su fine ciclo allarme

Notifiche e Impostazioni Generali, Logo

Questo descrizione permette di assegnare un nome all'impianto di allarme. Questa informazione viene riportata sull'intestazione delle notifiche.

Default: Dogma System

Notifiche e Impostazioni Generali, Abilita segnalazione "Richiesta Assistenza" su tastiere

Se abilitato, in caso di necessità le tastiere notificheranno tramite un apposito messaggio che sono presenti una o più anomalie sul sistema e che quindi è necessario l'intervento di un tecnico (installatore) per risolvere il problema.

Default: Disabilitato

Notifiche e Impostazioni Generali, Disattivare le notifiche visive secondo i requisiti EN50131

Se abilitato le tastiere non visualizzano lo stato delle aree associate.

Default: Abilitato

Notifiche e Impostazioni Generali, Consenti l'accesso in teleassistenza a impianto inserito

Se abilitato permette all'installatore di accedere alla configurazione anche quando l'impianto è inserito.

Default: Disabilitato

Notifiche e Impostazioni Generali, Non richiedere di forzare l'inserimento con richiesta assistenza

Se abilitato consente di inserire senza forzare l'inserimento nel caso vi sia una richiesta di assistenza.

Default: Disabilitato

Notifiche e Impostazioni Generali, Inibisci riconoscimento comunicazione critica con dispositivi RF per statistiche

Se abilitato, non effettua il riconoscimento dei dispositivi critici. Questo parametro risulta essere la disabilitazione del controllo "Riconoscimento comunicazione critica con dispositivi RF".

Default: Abilitato

Notifiche e Impostazioni Generali, Disinserimento rapido all'autenticazione da tastiera

Se abilitato, permette il disinserimento dell'impianto al solo inserimento del PIN o al riconoscimento del TAG. Attivo solamente sulle tastiere BT-KPXW e BT-SKW.

Default: Disabilitato

Impostazione RF, Serial Number

Indica il codice univoco dell'impianto assegnato alla centralina.

Impostazione RF, Canale RF assegnato

Stabilisce il canale radio utilizzato dall'impianto nella gamma 868MHz. Si suggerisce di

lasciare il valore di default e di variarlo solo in caso di necessità, per esempio se il canale è disturbato.

Valori programmabili: 0 / 1 / 2

Default: 0

ATTENZIONE!

Se si cambia il canale radio su un impianto con sensori già registrati, questi devono essere registrati nuovamente.

Controllo antistrappo centralina, Abilitazione antistrappo

Se abilitata, attiva la protezione antistrappo. Questo controllo prevede il fissaggio alla parete del magnete in dotazione.

Default: Abilitato



Utilità di installazione, Stato di Manutenzione

Indica lo stato attuale di operatività della centralina:

- Manutenzione OFF = centralina con tutte le funzioni attive,
- Manutenzione ON = le funzioni suono sirena e comunicazione sono inibite.

Lo stato di Manutenzione viene impostato nel momento in cui si deve accedere alla installazione o configurazione dell'impianto senza la necessità di far suonare le sirene o comunicare l'allarme. Lo stato di manutenzione può essere attivato/disattivato con i seguenti organi di comando: Sicep Cloud Connect (pulsante Cambia), tastiera radio BT-SKW (menù installatore), Sicep. Inoltre lo stato di manutenzione si attiva in automatico quando la centralina DOGMA viene alimentata con il contenitore aperto e si disattiva in automatico dopo 60 secondi che il contenitore viene chiuso.

Sostituzione centralina, Codice

Il codice per la "sostituzione della centralina" serve per la sua sostituzione in caso di guasto con un modello identico senza dover ripetere l'intera procedura di acquisizione dei dispositivi radio. Infatti, tramite questo sistema viene clonato il Serial Number, quindi ripristinando la configurazione precedentemente salvata, si ottiene una copia esatta delle funzionalità dell'impianto di allarme con esclusione delle password e codici tastiera.

Per assicurare la massima sicurezza sull'operazione, la modifica del codice dell'impianto viene effettuata soltanto per mezzo di un codice di sblocco inviato dall'assistenza di Sicep dietro richiesta del titolare dell'impianto o dell'installatore di fiducia tramite email.

Il codice di sblocco, con validità temporale limitata ed utilizzabile una sola volta, dovrà essere inserito nell'apposito campo e premuto il pulsante "Applica". Al termine dell'operazione si avrà il reset della centralina con il cambio del Serial Number.

Nella richiesta dovranno essere riportati i seguenti parametri:

1. Richiedente procedura,
2. Il Serial Number da clonare (della centralina da sostituire),
3. Il Serial Number della nuova centralina,
4. La data riferita al giorno dell'intervento.

Nella stessa richiesta può anche essere specificata la necessità dell'azzeramento della password dell'Amministratore.

Data e Ora



Data (GG/MM/AAAA) Ora (hh:mm)

Impostare la data e l'orario negli appositi campi; questi dati sono essenziali per una corretta memorizzazione degli eventi nello storico. Il giorno della settimana viene impostato automaticamente dal calendario interno.

Data /ora di default all'accensione: 1 gennaio 2019, ore 00:00



Fuso orario

Impostare il fuso orario del Paese di utilizzo; questa impostazione viene utilizzata per il cambio automatico dell'ora solare/legale.

Valori programmabili: da GMT -12 a GMT +13.

Default: (GMT +1.99 h) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna



Fuso orario, Passa automaticamente all'ora legale

Se abilitato la centralina DOGMA rimette automaticamente l'ora solare/legale in base al calendario interno e al fuso orario selezionato.

Default: Abilitato

Fuso orario, Forza l'applicazione dell'ora legale

Se abilitato, la centralina applica l'ora legale; se non abilitato, la centralina applica l'ora solare. Questo parametro è accessibile solo se la rimessa automatica è disabilitata.

Default: Disabilitato

Lingua

Lingua, Selezione Lingua

Consente di impostare la lingua in uso.

Il cambiamento da una lingua all'altra comporta l'azzeramento di tutti i parametri registrati e il ripristino della configurazione di fabbrica. Per procedere nell'operazione occorre confermare con il tasto "OK".

Default: Italiano.

Utilità sistema

Configurazione, Esporta configurazione

Configurazione, Carica configurazione

Esporta ed importa localmente su file la configurazione della centralina DOGMA.

Default Configurazione, Abilita

Consente di ripristinare tutti i parametri alla configurazione di fabbrica. Per procedere nell'operazione occorre prima impostare il flag "Abilita" e quindi premere il pulsante "Ricarica configurazione di default".

Log, Esporta log di sistema

Salva in un file in formato testo il log di sistema.

Log, Indirizzo IP

Utilizzato in fase di assistenza tecnica.

Log, Abilita log remoto

Utilizzato in fase di assistenza tecnica.



Reset Centralina, Esegui reset

Consente di effettuare un reset della centralina tramite collegamento da remoto.

Aggiornamento firmware, Carica aggiornamento

Permette di aggiornare il firmware della centrale DOGMA ad una versione più recente.

Info

Mostra la versione firmware della centralina, la versione firmware del bootloader, il numero di matricola, il numero identificativo della centralina e la data di collaudo del prodotto.

6.3.3 Aree



Descrizione

Le aree sono le sezioni dell'impianto che riuniscono le zone e dispositivi e che possono essere inserite/disinserite. Assegnare un nome di riferimento a quelle utilizzate, massimo 18 caratteri spazi inclusi.

Default: Area1 - Area4



Tempistiche, Tempo di ingresso

Stabilisce il tempo di ritardo delle zone o dei sensori nel generare l'allarme. E' il tempo che intercorre fra l'allarme della zona o dispositivo e l'attivazione della sirena e del comunicatore. Il tempo agisce solo sulle zone o dispositivi che sono state programmate come ritardate.

Valori programmabili: da 0 a 4000 secondi (circa 66 minuti).

Default: 0



Tempistiche, Tempo di uscita

Stabilisce il tempo in cui le zone e dispositivi sono ignorate dal momento dell'inserimento dell'area; il tempo agisce soltanto sulle zone e dispositivi che sono stati programmati come ritardati.

Valori programmabili: da 0 a 4000 secondi (circa 66 minuti).

Default: 0

Tempistiche, Tempo di autoinserimento

Se programmato diverso da zero, l'area una volta disinserita si reinserisce automaticamente al termine del tempo impostato.

Valori programmabili: 0 - 720 minuti (12 ore).

Default: 0

Tempistiche, Inserimento istantaneo (tempo di uscita azzerato) da APP

Se configurato azzerà il tempo di uscita quando l'inserimento è effettuato da APP.

Default: Disabilitato

Inserimento parziale, Tipo inserimento parziale

Consente di scegliere che tipo di inserimento parziale è predefinito sull'area in questione. I valori possibili sono:

- **Perimetrale:** l'inserimento parziale da qualsiasi organo di comando inserisce l'area in modo perimetrale, ovvero attende i tempi di ingresso e di uscita prima di allarmare o di inserire.
- **Notte:** l'inserimento parziale da un qualsiasi organo di comando inserisce l'area in modo notte, ovvero non attende i tempi di ingresso e uscita prima di allarmare e di inserire. In caso di inserimento notte si presuppone che, chi inserisce l'impianto, non allarmerà le zone o i dispositivi coinvolti, quindi non sono necessari ulteriori ritardi.

Default: Perimetrale

Inserimento parziale, Attivazione sirene ritardata di 30 secondi su allarme con impianto inserito parziale

Ritarda di 30 secondi l'attivazione delle sirene quando l'impianto è inserito parziale (perimetrale o notturno)

Default: Disabilitato

Inserimento/Disinserimento automatico, Programma

Permette di assegnare un programma per l'inserimento /disinserimento automatico a orario dell'area.

Valori programmabili: Disabilitato / Programma1 ... Programma4. Default: Disabilitato

Inserimento/Disinserimento automatico, Tipo inserimento

Consente di decidere la modalità di inserimento dell'area dal programma selezionato. Attiva soltanto se è stato selezionato un programma.

Valori programmabili: Totale / Perimetrale / Notte.

Default: Totale

Segnalazioni acustiche, Abilitate

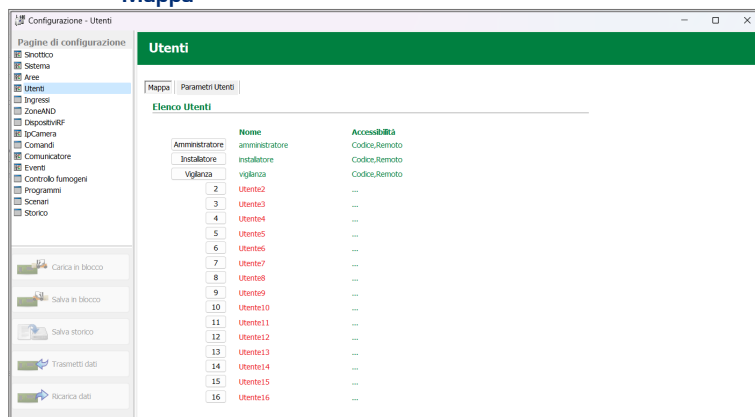
Se è abilitata l'area genera una segnalazione acustica durante il tempo di ingresso e di uscita.

La segnalazione avviene anche se non ci sono zone di tipo ritardato, è sufficiente che i tempi di ingresso e/o di uscita siano programmati diversi da zero.

Default: Abilitata

6.3.4 Pagina Utenti

Mappa



Lista Utenti

Questa mappa riporta l'elenco degli utenti; per selezionare un utente da programmare premere sul pulsante relativo.

Accanto a ciascun utente è riportato il nome programmato e i tipi di accesso assegnati; se la dicitura è verde l'utente è abilitato, se è rossa l'utente è disabilitato.

Qui di seguito è riportata come esempio la pagina relativa all'utente amministratore; le altre pagine sono simili oppure non contengono alcuni parametri.

Parametri Utenti



Abilitato

Abilita o disabilita l'Utente. L'Amministratore è l'unico che non può essere disabilitato.
Default: Amministratore, Installatore, Vigilanza sono abilitati



Nome Utente

Assegnare il nome di riferimento per l'utente che viene utilizzato tutte le volte che si effettuano le operazioni sull'impianto: viene utilizzato sull'APP per verificare insieme alla password l'accesso al sistema, viene utilizzato nello storico eventi per contraddistinguere le operazioni effettuate dall'utente. Possono essere inseriti fino a 18 caratteri alfanumerici, spazi inclusi.

*Default: Amministratore
 Utente1 ... Utente16
 Installatore
 Vigilanza*

Accessibilità

Limita l'accesso alle aree per l'utente. Definire un programma nell'apposita pagina ed assegnarlo in questo campo. Il programma definisce fino a 2 fasce orarie al giorno durante le quali l'utente è autorizzato ad effettuare manovre di inserimento/disinserimento impianto nell'area protetta assegnata. Utilizzare questa funzionalità per consentire l'accesso a un utente che generalmente non ha consenso di accedere ai locali protetti. (es. maestranze per un lavoro occasionale, personale di servizio ecc.)

Default: Disabilitato

Abilitazione comandi

Questo parametro permette all'utente di attivare/disattivare le uscite dall'App SICEP.
Default: Abilitato

Abilitazione controllo fumogeni

Questo parametro permette all'utente l'attivazione manuale dei fumogeni gestiti dalla centralina via App SICEP

Default: Disabilitato

Abilitazione servizi OnDemand

Questo parametro permette all'utente di utilizzare i servizi OnDemand.

Default: Disabilitato



Abilitazione configurazione centrale da APP

Questo parametro, se disabilitato, limita le capacità dell'Amministratore.

Default: Abilitato

Abilitazione registrazione nuove APP

Questo parametro permette all'utente non amministratore di generare codici OTP per registrare nuovi dispositivi al Cloud.

Default: Abilitato per Amministratore



Utente attivo solo per inserimento/disinserimento

Questo parametro, se abilitato, limita ulteriormente le funzioni dell'Utente.

Default: Disabilitato



Codice tastiera

E' il codice a cinque cifre per le operazioni da tastiera. Premendo i relativi pulsanti è possibile compiere le seguenti operazioni:

- **Default** per abilitare il codice ed impostarlo al valore di default, o riportarlo al valore di default. Nel caso che il codice sia stato modificato dall'utente la visualizzazione del codice è nascosta.
- **Elimina** per disattivare l'accesso da tastiera all'utente.

I nuovi codici scelti dagli utenti devono essere tutti di 5 cifre numeriche; non possono essere scelti come nuovi codici quelli di default.

Valori di Default: Amministratore 12301
Utente2 12302

... ..
Utente15 12315
Installatore 11100



Tag

Ad ogni utente può essere associata una sola chiave TAG da utilizzare con i lettori RFID mod. BT-PRW. I pulsanti permettono di compiere le seguenti operazioni:

- **Registra:** permette di acquisire una nuova chiave TAG. Per compiere l'operazione premere il pulsante e avvicinare il TAG al lettore RFID.
- **Elimina:** permette di cancellare il TAG dall'utente; il dispositivo cancellato può essere associato ad un altro utente.
- **Annulla:** permette di interrompere la fase di registrazione nel caso di impossibilità di registrazione. Il sistema comunque esce dalla fase di registrazione se questa non è avvenuta entro 30 secondi.

NOTA.

Una chiave TAG può essere registrata su più centraline della serie DOGMA, ICON oppure UNICA.



Radiocomando

All'Amministratore e ad ogni utente può essere associato un solo radiocomando.

I pulsanti permettono di compiere le seguenti operazioni:

- **Registra:** permette di associare il radiocomando desiderato all'utente. Per compiere l'operazione premere il pulsante "Registra" e successivamente premere e mantenere premuti i pulsanti INSERIMENTO PERIMETRALE e INSERIMENTO TOTALE sul radiocomando.
- **Elimina:** permette di rimuovere l'associazione del radiocomando dall'utente in questo modo il radiocomando può essere assegnato ad un altro utente. Questa operazione non cancella la programmazione del BT-KT che deve essere cancellato manualmente premendo e tenendo premuti i due tasti programmabili in basso fino a che non si accendono tutti i led.
- **Annulla:** permette di interrompere la fase di registrazione nel caso di impossibilità di registrazione del radiocomando. Il sistema comunque esce dalla fase di registrazione se questa non è avvenuta entro 30 secondi.
- **Configura tasti funzioni:** premere questo pulsante per accedere alla scheda di configurazione dei tasti programmabili. In questa scheda si può scegliere se associare un evento al tasto o alla combinazione di tasti fra quelli disponibili per il tasto scelto.
- **Abilitato:** dopo la registrazione e l'assegnazione all'utente il pulsante è abilitato. E' però possibile sempre disabilitarlo per renderlo temporaneamente inutilizzabile.

Disabilitare il radiocomando in caso sia stato perduto o se non si vuole consentire l'accesso all'utente per un determinato periodo di tempo. Riabilitando il radiocomando questo torna ad essere utilizzabile.

- **Aree di competenza:** elenco delle aree di competenza del radiocomando. Le operazioni di inserimento e disinserimento verranno eseguite contemporaneamente sulle aree selezionate.

Per ogni tasto o combinazione di tasti è possibile configurare le seguenti azioni:

- Nessuno
- Panico
- Soccorso
- Evento programmabile da 1 a 8
- Gestione aree da Area1 a Area4



Accesso da remoto

E' la password alfanumerica per l'accesso con il programma Sicep Cloud Connect o con Sicep tramite collegamento USB, Ethernet o LTE/GPRS.



Accesso da remoto, Default

Abilitare la password impostandola al valore di default, o riportarla al valore di default; la parola viene visualizzata di fianco. Nel caso che la password sia stata modificata dall'Utente la visualizzazione è nascosta.



Accesso da remoto, Elimina

Eliminare la password. In questo modo l'accesso da remoto per questo Utente non è più possibile.



Accesso da remoto, Aree di competenza

Accesso da remoto, Aree Ins./Dis. Pred.

Impostano rispettivamente le aree su cui l'utente può compiere operazioni e quelle su cui tali operazioni sono compiute simultaneamente appena eseguito l'accesso.

Default: nessuna



Accesso da remoto, Notifiche eventi APP

Permette di scegliere fra 8 gruppi di tipologie di eventi da notificare all'utente tramite il servizio di Cloud Sicep.

Lista Varchi

Per ogni varco (punto di accesso agli organi di comando) vengono definite le operazioni consentite all'utente.

Lista Varchi, Aree di competenza / Aree Ins./Dis. Pred.

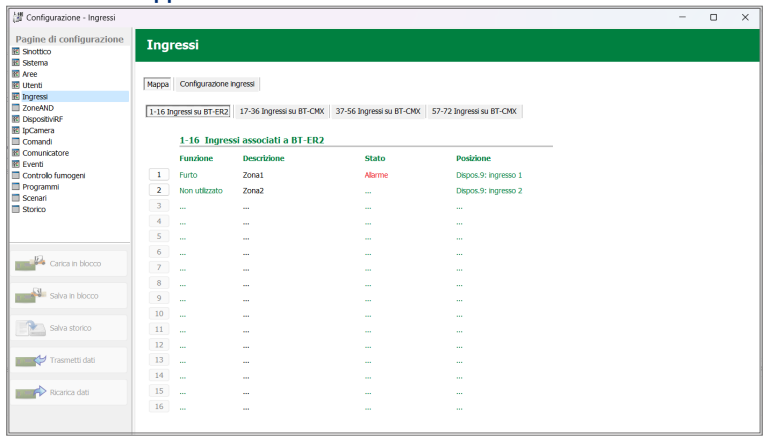
Impostano rispettivamente le aree su cui l'utente può compiere operazioni e quelle su cui tali operazioni sono compiute simultaneamente appena eseguito l'accesso. Nel caso di lettori RFID mod. BT-PRW le due impostazioni coincidono non permettendo di fare scelte.

Apriporta

Stabilisce se l'utente può attivare la funzione apriporta. È disponibile solo per i lettori RFID modello BT-PRW.

6.3.5 Pagina Ingressi

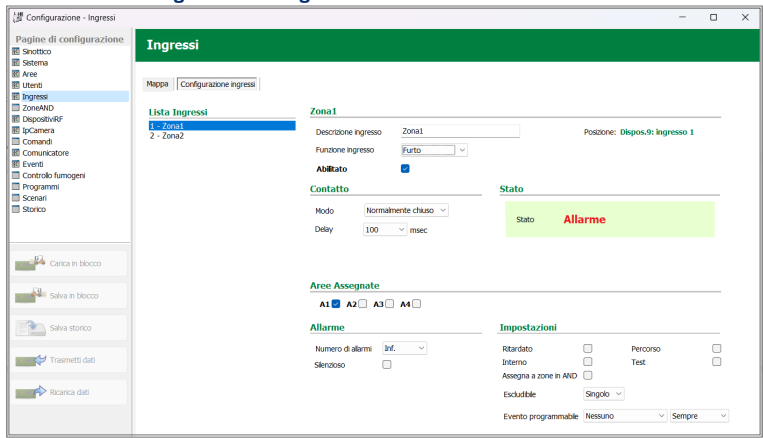
Mappa



1-16 Ingressi su BT-ER2
17-36 Ingressi su BT-CMX
37-56 Ingressi su BT-CMX
57-72 Ingressi su BT-CMX

Questa mappa riporta l'elenco degli ingressi filari o zone. Nella centralina DOGMA per ingressi o zone filari si intendono quelle presenti sulle espansioni radio installate opzionalmente.
Per selezionare la configurazione di un ingresso da programmare premere sul pulsante relativo. Accanto a ciascun ingresso è riportata la descrizione e lo stato reale.
Qui di seguito è riportata come esempio la pagina relativa all'ingresso 1, le altre pagine sono identiche a quella in esempio.

Configurazione Ingressi



Descrizione ingresso

Inserire una descrizione che sia attinente all'utilizzo dell'ingresso (massimo 18 caratteri, spazi inclusi).

Default: ---



Funzione ingresso

Imposta il funzionamento dell'ingresso. E' possibile scegliere fra le seguenti tipologie:

Furto	L'ingresso genera allarme solo quando l'area (o le aree) di appartenenza è inserita.
Incendio, Panico, Soccorso	L'ingresso è attivo 24h e genera l'evento relativo.
Inserimento	L'ingresso è usato per inserire e disinserire l'area selezionata. Il cambio dello stato avviene sul passaggio da stato normale ad allarme.
Allarme 24h	L'ingresso è attivo 24h e genera l'apposito evento "Allarme 24h".
Tecnologico	L'ingresso è attivo 24h e genera l'evento programmabile selezionato.
Non utilizzato	L'ingresso non è attivo e a differenza di una zona disabilitata non richiede tutte le volte un inserimento forzato.

Default: Furto



Abilitato

Questo flag stabilisce se l'ingresso è abilitato o disabilitato; ha senso solo se l'ingresso è di tipo diverso da "non utilizzato". Un ingresso disabilitato attiva l'apposito evento; l'operazione che compie l'utente da tastiera (disabilitazione) equivale a togliere la spunta da questo flag in programmazione.

Default: Abilitato



Contatto, Modo

Stabilisce lo stato di riposo dell'ingresso. In base alla programmazione del parametro *Funzione ingresso*, alcune modalità possono non essere disponibili.

Normalmente chiuso	L'ingresso è a riposo quando è chiuso a massa (GND)
Normalmente aperto	L'ingresso è a riposo quando è aperto
Tapparella	L'ingresso conta gli impulsi trasmessi da un contatto per tapparelle
Inerziale	L'ingresso è regolamentato dai parametri sensibilità e integrazione

Valori programmabili: NC, NA, Tapparella, Inerziale

Default: NC



Contatto, Delay

Stabilisce il valore di tempo minimo necessario per ritenere valida la variazione dello stato dell'ingresso in modo da ridurre l'effetto di eventuali disturbi. Il tempo è in millisecondi.

Valori programmabili: 100 / 200 / 500 / 1000 / 2000 / 4000 msec

Default: 100msec

Tapparella, Impulsi

Stabilisce il numero di impulsi necessari ad un ingresso "tapparella" a provocare l'allarme in una finestra temporale impostata dal parametro Tempo Reset. Il numero di impulsi è proporzionale allo spostamento della tapparella e dipende dal tipo di sensore.

Valori programmabili: 4, 10, 20, 30.

Default: 10

Tapparella, Tempo reset

Determina il tempo (in secondi) entro il quale sono conteggiati gli impulsi.

Valori programmabili: 3, 6, 12, 16 sec

Default: 6

Inerziale, Sensibilità

Imposta la sensibilità ad un ingresso "inerziale". Eseguire delle prove per trovare il valore più adatto.

Valori programmabili: 1 (poco sensibile) ...4 (molto sensibile)

Default: 1

Inerziale, Integrazione

Imposta la velocità di ritorno a riposo dopo un impulso. Una serie di impulsi ad un ingresso "inerziale" in un tempo, determinato anche dal parametro Integrazione, provoca l'allarme. *Valori programmabili: 1 (ritorno veloce a riposo) ...4 (ritorno lento a riposo) Default: 1*

Stato

Questo messaggio indica lo stato dell'ingresso in tempo reale in base alla configurazione (Modo) scelta.

Messaggio	Colore	Descrizione
OK	Verde	Ingresso a riposo
Allarme	Rosso	Ingresso in allarme



Aree Assegnate

Assegna l'ingresso all'area o alle aree desiderate. Nel caso che un ingresso sia assegnato a due o più aree l'ingresso è condiviso fra le aree.

Gli ingressi non di tipo Furto non hanno area assegnata

Valori impostabili: A1 - A4

Default: A1



Allarme, Numero di allarmi

Questa impostazione agisce solo per gli ingressi Furto. Stabilisce il numero di cicli allarme (ovvero attivazioni della sirena) che l'ingresso può generare tra un inserimento e il successivo disinserimento; una volta raggiunto il limite l'ingresso non è più attivo e per riarmarlo è necessario disinserire e reinserire l'area. Questa impostazione è utilizzabile solo per gli ingressi Furto, per tutti gli altri il parametro è forzato a Infinito e l'ingresso può generare infiniti cicli di allarme.

Questa impostazione non limita il numero di eventi trasmessi dal comunicatore: durante un ciclo allarme se l'ingresso va ripetutamente in allarme vengono trasmessi tutti i nuovi eventi. Le trasmissioni non vengono più effettuate solo al termine dei cicli.

Valori programmabili (solo per zone Furto): Infinito / 1 / 3 / 5

Default: Inf.

Allarme, Silenzioso

Questa impostazione agisce solo per gli ingressi Furto. Inibisce l'attivazione della sirena in caso di allarme.

Default: Disabilitato



Impostazioni, Ritardato

Questa impostazione agisce solo per gli ingressi Furto. Se abilitato l'ingresso è ritardato e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: Disabilitato



Impostazioni, Interno

Questa impostazione agisce solo per gli ingressi Furto. Se abilitato l'ingresso è interno e pertanto non è attivo quando l'area di appartenenza è inserita in modo perimetrale.

Default: Disabilitato

Impostazioni, Assegna a zone in AND

La zona è assegnata al funzionamento in combinazione con altre zone. Da configurare nella pagina Zone in AND dedicata.

Default: Disabilitato

Impostazioni, Percorso

Questa impostazione agisce solo per gli ingressi Furto. Evita che l'ingresso generi un allarme quando nell'area di appartenenza è attivo il "tempo di ingresso"

Default: Disabilitato

Impostazioni, Test

Questa impostazione è utilizzabile per operazioni di test: se abilitato, l'allarme dell'ingresso viene solo registrato nello storico, mentre la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata. Non disponibile per ingressi tipo Inserimento e Tecnologico.

Default: Disabilitato



Impostazioni, Escludibile

Questa impostazione agisce solo per gli ingressi Furto. Stabilisce se un ingresso in allarme può essere escluso all'inserimento (inserimento forzato) e la modalità con cui ritorna attivo dopo l'esclusione.

NO L'ingresso non è escludibile.

Singolo L'ingresso può essere escluso e viene riattivato al successivo reinserimento dell'area.

Auto L'ingresso può essere escluso e viene riattivato non appena torna a riposo, senza necessità di disinserire l'area.

Valori programmabili: No/Singolo/Auto

Default: No

Impostazioni, Evento programmabile

Questa impostazione agisce solo per gli ingressi Furto e Tecnologico.

L'allarme generato dall'ingresso può attivare un evento programmabile fra quelli disponibili, è possibile inoltre selezionare quando è attiva questa funzione (solo per la funzione Furto):

Sempre

Se non attivo (Area/e di appartenenza disinserita)

Se attivo (Area/e di appartenenza inserita)

Valori programmabili: Nessuno, Programmabile 1 ... 8

Default: Nessuno

6.3.6 Pagina Zone AND

Oltre al normale utilizzo di una zona o di un sensore è possibile assegnare la possibilità di operare in combinazione fra loro. Questa configurazione consente di ridurre i possibili disturbi e di conseguenza diminuire la probabilità di falsi allarmi. In configurazione AND una zona genera allarme solo se anche altre zone sono state, o verranno allarmate.

La centralina permette di configurare fino a 8 zone in AND, ognuna delle quali consente di combinare fra loro fino a 4 sensori fra quelli registrati e assegnati a questo modo di funzionamento.

Descrizione

Nome assegnato alla zona in AND attualmente selezionata. La centrale farà riferimento al nome qua assegnato per ogni operazione che riguardano questa zona.

Default: ZonaAND1..8.

Scheda Attributi Zona AND

Abilitata

Abilita la Zona in AND. Per Default: tutte le zone in AND sono disabilitate. Configurarle e abitarle quando si ha intenzione di utilizzarle.

Default: non abilitata

Allarmi

Stabilisce il numero di cicli allarme (ovvero attivazioni della sirena) che la zona può generare tra un inserimento e il successivo disinserimento; una volta raggiunto il limite la zona non è più attiva e per riarmarla è necessario disinserire e reinserire l'area.

Questa impostazione non limita il numero di eventi trasmessi dal comunicatore: durante un ciclo allarme se la zona va ripetutamente in allarme vengono trasmessi tutti i nuovi eventi. Le trasmissioni non vengono più effettuate solo al termine dei cicli.

Valori programmabili (solo per zone Furto): Infinito / 1 / 3 / 5

Default: 5

Silenzioso

Inibisce l'attivazione della sirena in caso di allarme.

Default: Disabilitata (sirena attiva)

Test

Serve per operazioni di test: se abilitata, l'allarme della zona viene solo registrato nello storico; la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitata (funzionamento normale)

Ritardata

Se abilitato la zona è ritardata e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: non abilitata (non ritardata).

Scheda aree

Aree associate

Assegna la zona all'area o alle aree desiderate. Nel caso che una zona sia assegnata a due o più aree la zona è condivisa.

Default: Area1

Scheda configurazione

Rispetta l'ordine

Se abilitato, per generare allarme, è richiesto che i sensori siano sollecitati nell'ordine di inserimento dall'alto verso il basso.

Default: disabilitato

Validità

Indica il tempo massimo durante il quale, tutti i sensori assegnati alla zona in AND, devono essere sollecitati affinché venga generato un allarme.

Default: 20 sec

Lista sensori

Tutti i sensori che possono essere associati a una zona AND sono elencati in queste liste e possono essere assegnati esclusivamente a una delle zone AND. Per aggiungere elementi alle liste agire sulle apposite configurazioni delle singole zone e sensori.

6.3.7 Pagina Dispositivi RF

Mappa

Configurazione - DispositiviRF

Pagina di configurazione

Sistema

Area

Utenti

Ingressi

ZonaAND

DispositiviRF

IPcamera

Comandi

Comunicatore

Eventi

Controllo fumogeni

Programmi

Scenari

Storico

Carica in blocco

Salva in blocco

Salva storico

Trasmetti dati

Ricarica dati

Dispositivi RF

MappaConfigurazione Dispositivi

Elenco Dispositivi RF

	Tipo	Nome	Stato	Rep	Tipo	Nome
1	...	...	...	...	20	...
2	...	...	...	...	21	...
3	...	...	...	...	22	...
4	...	...	...	...	23	...
					24	...
					25	...
9	ER2	Dispos.9	OK	...	26	...
10	...	...	...	...	27	...
11	...	...	...	...	28	...
12	...	...	...	...	29	...
13	...	...	...	...	30	...
14	...	...	...	...	31	...
15	...	...	...	...	32	...
16	...	...	...	...	33	...
17	...	...	...	...	34	...
18	...	...	...	...	35	...
19	...	...	...	...	36	...

Aggiungi Dispositivo

Cancella Dispositivo

Annulla

Azzerare Statistiche

Legenda	
REP	BT-REP2 Ripetitore
KPXW	BT-KPXW Tastiera
SKW	BT-SKW Tastiera
DTCX	BT-DTCX Sensore DT/Camera
DTWX	BT-DTWX Sensore DT
MDCX	BT-MDCX Sensore Pir/Camera
MDWX	BT-MDWX Sensore Pir
IRWX	BT-IRWX Sensore Pir
IRE	BT-IRE2 Sensore Pir da esterno
CMXW	BT-CMXW Sensore magnetico
CMXE	BT-CMXE Sensore magnetico
CMW	BT-CMW/BT-CME Sensore magnetico
SMK	BT-SMK2 Sensore di fumo
NI	BT-NI Fumogeno
UF	IF-URFOG Nebbiogeno
SIR	BT-SIR Sirena radio
SIR2W	BT-ALMA Sirena radio
PRW	BT-PRW Lettore TAG

Questa pagina serve per la registrazione di tutti i dispositivi wireless ad esclusione del radiocomando BT-KT che viene registrato nella pagina UTENTI. Una volta registrato il singolo dispositivo, premere sul relativo pulsante dell'elenco per accedere alla configurazione specifica. Le prime 8 posizioni sono riservate ai dispositivi REP. Per ogni dispositivo sono elencati:

- Tipo

Sigla di massimo 3 caratteri che identifica il sensore o il dispositivo installato
- Nome

Una descrizione che serve per riconoscere il sensore fra gli altri registrati.
- Stato

Riporta lo stato del dispositivo; è presente il tamper più altre caratteristiche specifiche del dispositivo. Gli stati sono aggiornati in tempo reale.
- Rep

Indica sotto quale ripetitore il dispositivo è registrato.
- Descrizione dei pulsanti presenti sulla mappa:



Aggiungi Dispositivo

Permette di attivare sulla centralina la procedura di registrazione di un dispositivo wireless. Nella barra a fondo pagina viene riportato il messaggio "Registrazione in corso ...". Al termine della registrazione, se questa è andata a buon fine, viene riportato il messaggio "Operazione terminata" e verranno riempiti i campi relativi al sensore aggiunto: Tipo, Nome, Stato.



Cancella Dispositivo

Permette la cancellazione di un dispositivo wireless già registrato. Nella barra a fondo pagina viene riportato il messaggio "Cancellazione in corso ..."

Al termine della cancellazione, se questa è andata a buon fine, viene riportato il messaggio "Operazione terminata", verranno cancellati i campi relativi al sensore cancellato: Tipo, Nome, Stato e verrà azzerata la configurazione del dispositivo wireless.

Annulla

Permette di annullare l'operazione in corso.

Azzera Statistiche

Permette di azzerare le statistiche di tutti i dispositivi wireless. Questa operazione è utile al termine dell'installazione dell'impianto di sicurezza.

Configurazione Dispositivi Radio Parametri comuni

In tutti i dispositivi sono presenti le seguenti sezioni e funzioni:



Abilitato/a

Indica se il sensore o organo di controllo è abilitato

Default: Abilitato



Descrizione dispositivo

È il campo dove impostare il nome del dispositivo. Inserire una breve descrizione del sensore 19 caratteri massimi compresi gli spazi.

Default: Dispos XX

Controllo consumo elevato

Permette di disabilitare questo controllo per quei dispositivi che sono sottoposti a un utilizzo intensivo, cioè diverso da quello tipicamente residenziale (es. BT-CMXW installato sulla porta di un negozio).

Default: Abilitato

Pulsante Allinea

Trasferisce la configurazione da Sicep Cloud Connect al dispositivo per cui le modifiche effettuate diventano attive. A trasferimento avvenuto la spia a fianco del pulsante da rossa diventa verde.

Pulsante Ripristina

Serve per registrare nuovamente sulla centralina un nuovo dispositivo al posto di quello preesistente guasto, conservando tutta la programmazione del sensore eliminato; il sensore deve essere ovviamente dello stesso tipo. Questo pulsante si abilita automaticamente quando il sensore guasto viene disabilitato manualmente.

Pulsante Cancella

Permette di rimuovere dall'impianto un dispositivo guasto; il pulsante è attivo solo se il dispositivo viene disabilitato. La cancellazione con questo pulsante deve essere considerata una procedura di emergenza. Se il sensore è funzionante la cancellazione deve essere eseguita dalla mappa dispositivi RF.

Pulsante Annulla

Permette di interrompere la procedura di ripristino dispositivo. Il pulsante è attivo solo se il dispositivo è stato precedentemente disabilitato.

NOTA.

Se il dispositivo transitava da uno o più REP l'operazione "Ripristina Dispositivo" riconfigura anche il passaggio da REP; in ogni caso l'operazione deve essere eseguita in prossimità della centralina. Una volta terminata la configurazione di ogni dispositivo premere il bottone "Allinea Dispositivo" per trasferire le informazioni al dispositivo.

Stato, Sistema

Stato, Sensore

Visualizza lo stato reale del dispositivo. In genere è presente il tamper più altre caratteristiche specifiche per ogni dispositivo.



Stato, Comunicazione

Riporta l'indicazione sullo stato della comunicazione con la centralina: Connesso, Non Connesso, la Qualità del segnale radio ed è presente il pulsante per effettuare il Test di Comunicazione.

Stato, Batteria

Indica lo stato della batteria e l'ultimo valore di tensione letto dal sensore.

ATTENZIONE!

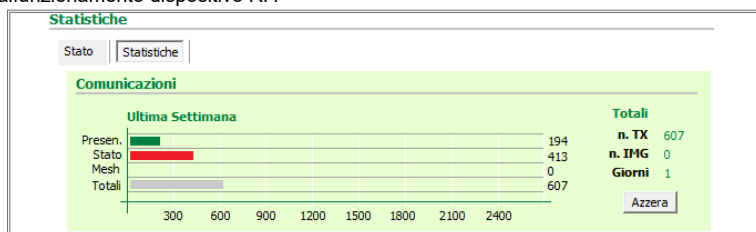
Se la centralina non si trova nello stato di manutenzione, alcune sezioni dei dispositivi possono essere disattivate e quindi l'indicazione riportata può non essere lo stato reale.

Statistiche e controllo periodico dei dispositivi

La centralina DOGMA usa una tecnologia radio bidirezionale che permette di controllare costantemente l'efficienza di tutti i dispositivi, in modo da garantire la massima sicurezza dell'impianto.

In questa ottica, il sistema può mettere in evidenza le criticità dei collegamenti radio fra la centralina e i sensori relativamente all'ambiente in cui è installato.

Per questo motivo ciascun dispositivo radio (con l'esclusione dei REP e dei radiocomandi) ha una pagina di programmazione in cui sono riportate le statistiche sulle comunicazioni. I dati che vengono raccolti consentono di analizzare il funzionamento del dispositivo nell'ultima settimana di funzionamento e sono utilizzati anche per generare l'evento Malfunzionamento dispositivo RF.



Qui di seguito sono descritti i parametri riportati.

- **Presenze.** È il numero di messaggi di "presenza dispositivo" ricevuti dalla centralina DOGMA per il dispositivo considerato. In condizioni ottimali si devono ricevere da 1200 a 1344 trasmissioni alla settimana. Quando il valore conteggiato è inferiore a 1000 il sensore è dichiarato critico.
- **Stato.** È il numero di messaggi trasmessi dal dispositivo per comunicare la variazione di uno stato (esempio: apertura e chiusura del contatto principale sui contatti BT-CMXW, apertura/chiusura del tamper, allarme dell'inerziale, rilevazione movimento di un infrarosso, ecc.). Il valore conteggiato dà un'idea dell'utilizzo del dispositivo e viene utilizzato per generare l'evento sensore critico per consumo eccessivo. Questo controllo è calcolato per un utilizzo tipico in una abitazione residenziale; quando il sensore è necessariamente molto sollecitato (es. la porta di un negozio) il controllo può essere disabilitato.
- **Mesh.** È il numero di messaggi che la centralina ha ricevuto in modalità "emergenza"; il protocollo Bitech permette infatti ai sensori che hanno difficoltà di comunicazione con la centralina di allarme, di essere ripetuto da un qualsiasi altro dispositivo in ascolto che agisce come ripetitore provvisorio. Tale modalità aumenta in modo considerevole il consumo delle batterie dei sensori coinvolti e quindi deve essere utilizzata il meno possibile.
- **Totali.** È la somma dei valori Presenze + Stato + Mesh calcolati nell'ultima settimana.
- **n. TX.** È la somma di tutti i messaggi trasmessi dal dispositivo dal momento dell'installazione.
- **n. IMG.** È il numero di immagini catturate dal sensore (solo per BT-MDCX e BT-DTCX).
- **Giorni.** Indica il numero di giorni trascorsi dall'installazione del dispositivo.
- **Azzera.** Pulsante per l'azzeramento delle statistiche per il singolo dispositivo.

Questi dati sono utilizzati per generare l'evento "malf funzionamento sensore RF", che può essere dovuto alle seguenti cause:

- **CRITICO.** Il dispositivo ha trasmesso nell'ultima settimana meno di 1000 presenze oppure una percentuale uguale o maggiore del 25% è ricevuta tramite messaggi Mesh, oppure non risulta connesso alla centralina per un tempo uguale o superiore a quanto impostato nel parametro Riconoscimento dispositivo RF critico. Il ripristino dell'evento si ha, rispettivamente ai tre casi, o al raggiungimento di 1100 presenze settimanali, oppure quando la percentuale di messaggi "Mesh" scende sotto il 20%, oppure quando il sensore comunica nuovamente con la centralina.
- **ASSELENTE.** Il dispositivo non è connesso alla centralina per un tempo superiore a 12 ore. Il ripristino si ha all'arrivo della prima trasmissione.
- **CONSUMO ECCESSIVO.** Il dispositivo ha effettuato più di 1200 trasmissioni di stato nell'ultima settimana. Può indicare: che il posizionamento è critico e necessita di molte ripetizioni oppure che effettua molte trasmissioni di stato, per esempio perché si tratta della porta di un negozio che viene aperta e chiusa molte volte al giorno. In questo caso, si consiglia di disabilitare tale controllo. Il ripristino si ha quando le trasmissioni settimanali scendono sotto al valore di 1000. In una situazione di "Consumo Eccessivo", la durata della batteria potrebbe essere inferiore a quello dichiarato nelle specifiche del prodotto.

ATTENZIONE!

Si consiglia di controllare periodicamente le statistiche dei dispositivi. La modalità Mesh deve essere considerata una situazione di emergenza che riduce la durata della batteria di tutti i sensori coinvolti. Per questo motivo, quando un sensore invia molti messaggi di questo tipo è consigliabile installare un REP per sopperire ai problemi di comunicazione.

6.3.8 Parametri di configurazione specifici per ogni dispositivo.

BT-DTCX	Sensore infrarosso doppia tecnologia con camera e antimascheramento
BT-DTWX	Sensore infrarosso doppia tecnologia con antimascheramento
BT-MDCX	Sensore infrarosso passivo con camera e antimascheramento
BT-MDWX	Sensore infrarosso passivo con antimascheramento
BT-IRWX	Sensore infrarosso versione base
BT-MX2P	Sensore infrarosso da esterno
BT-MX2PC	Sensore infrarosso da esterno con camera
BT-MX3T	Sensore infrarosso da esterno doppia tecnologia
BT-MX3TC	Sensore infrarosso da esterno doppia tecnologia con camera

NOTA. I parametri descritti in questa sezione si riferiscono alla versione completa (BT-DTCX). Nelle altre versioni alcuni parametri non sono presenti.

PIR camera

Ver. 05

☒ **Abilitata**

Descrizione dispositivo **Dispos.9**

Controllo consumo elevato ☐

Ripristina Cancia Annulla

Allinea ☒

Statistiche

Stato Statistiche

Sistema

Sensore **Fermo**

Tamper **Chiuso**

Anti-Mask **Normale**

Temperatura **0.0 C**

Comunicazione

Connessione **Connesso**

Qualità Segnale RF ...

Test Segnale

Batteria

Ultima Lettura **3.4V**

Condizioni **Carica**

Aree Assegnate

A1 ☒ A2 ☐ A3 ☐ A4 ☐

Modalità Attiva se tutte le aree inserite

Allarme

Numero di allarmi 5 Silenzioso ☐

Controlli

Anti-Mask ☒

Configurazione PIR

Sensibilità L4 (ALTA)

Impulsi 1

Configurazione microonda

Abilitata ☒

Sensibilità L4 (ALTA)

Impulsi 1

Impostazioni

Ritardato ☐ Percorso ☐

Interno (non perimetrale) ☒ Test ☐

Assegna a zone in AND ☒

Fotocamera

Abilitata ☒

Privacy ☐

Risoluzione 640x480

Qualità Alta

Immagini per Allarme 5

Cattura immagine



Aree Assegnate

Assegna il sensore all'area o alle aree desiderate.

Valori programmabili: A1 ... A4

Default: A1



Allarme, Numero di allarmi

Stabilisce il numero di cicli allarme che il sensore può generare tra un inserimento e il successivo disinserimento. Per ciclo allarme si intende l'attivazione della sirena. Una volta raggiunto il limite, il sensore ritorna attivo solo disinserendo e reinserendo l'area. Questa impostazione non limita il numero di eventi trasmessi dal comunicatore: durante un ciclo allarme; se il sensore va ripetutamente in allarme vengono trasmessi tutti i nuovi eventi. Le trasmissioni non vengono più effettuate solo quando è stato raggiunto il limite degli allarmi

Valori programmabili: Infinito / 1 / 3 / 5

Default: 5

Allarme, Silenzioso

Se abilitato l'allarme di questo sensore non attiva la sirena.

Default: Disabilitato



Impostazioni, Ritardato

Se abilitato il sensore è ritardato e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: Disabilitato



Impostazioni, Interno

Se abilitato il sensore è interno e pertanto non è attivo quando l'area di appartenenza è inserita in modo perimetrale o notte.

Default: Abilitato

Impostazioni, Assegna a zone in AND

Il sensore è assegnato al funzionamento in combinazione con altre zone. Da configurare nella pagina Zone in AND dedicata.

Default: Disabilitato

Impostazioni, Percorso

Evita che il dispositivo generi allarme quando nell'area di appartenenza è attivo il tempo di ingresso causato da un dispositivo ritardato.

Default: Disabilitato

Impostazioni, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme del sensore viene soltanto registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato



Parametri sensore, Anti-Mask

Permette di disattivare la sezione relativa qualora non interessi utilizzare la funzione.

Default: Abilitato



Parametri sensore, Sensibilità

Questo parametro imposta la portata massima del rivelatore infrarosso.

Valori programmabili: L4 (alta) / L3 / L2 / L1 (bassa).

Default: L4



Parametri sensore, Impulsi.

Permette di aumentare l'immunità ai falsi allarmi; la condizione di allarme del sensore viene provocata soltanto quando vengono conteggiati il numero di allarmi impostati (impulsi) in un tempo di 10 secondi. Si consiglia di aumentare il numero di impulsi solo in caso di necessità.

Valori programmabili: 1, 2, 3

Default: 1



Microonda, Abilitata.

Permette di disattivare la sezione relativa qualora non interessi utilizzare la funzione.

Default: Abilitato

**Microonda, Sensibilità**

Questo parametro imposta la portata massima del rivelatore a microonda.
Valori programmabili: L4 (alta) / L3 / L2 / L1 (bassa).

Default: L4

**Microonda, Impulsi**

Permette di aumentare l'immunità ai falsi allarmi; la condizione di allarme del sensore viene provocata soltanto quando vengono conteggiati il numero di allarmi impostati (impulsi) in un tempo di 10 secondi. Si consiglia di aumentare il numero di impulsi solo in caso di necessità.

Valori programmabili: 1, 2, 3

Default: 1

**Fotocamera, Abilitata**

Permette di disattivare la sezione della fotocamera qualora non interessi utilizzare la funzione.

Default: Abilitata

**Fotocamera, Privacy**

Se abilitata, su interrogazione il sensore non restituisce immagini quando l'area di appartenenza è disinserita.

Default: Abilitata

Fotocamera, Risoluzione

Imposta il formato dell'immagine, si può scegliere 640x480 oppure 320x240. Il formato più piccolo consente trasmissioni più veloci e minor consumo della batteria.

Default: 640x480

Fotocamera, Qualità

Imposta il livello di compressione dell'immagine per ridurre la quantità dei dati da trasmettere e si può scegliere su 3 livelli (alta/media/bassa). Supponendo che all'immagine di qualità alta corrisponda il 100%, il livello medio riduce i dati al 75% circa, mentre il livello basso riduce al 50% circa.

Valori programmabili: Alta, Media, Bassa

Default: Alta

Camera, Immagini per Allarme

Imposta il numero di fotogrammi scattati per ogni evento Furto.

Valori programmabili: 1, 2, 5.

Default: 5

Immagini (Si accede tramite il pulsante Cattura immagine)**Pulsante Cattura immagine.**

Premuto richiede una immagine dalla telecamera del sensore. Questa immagine non viene salvata nello storico.

Pulsante Configura sensore

Premuto si torna nella pagina di configurazione sensore.

BT-CMXW / BT-CMXE BT-IRE2

sensori magnetici multifunzione
sensori infrarossi da esterno (tutti i modelli)

Magnetico
Ver. 02

☒ **Abilitato**
 Descrizione dispositivo **Dispos.13**
 Controllo consumo elevato ☐

Ripristina
Cancella
Annulla

Alinea

Statistiche

Stato
Statistiche

Sensori

Porta **Aperta**
Inerziale **Disabilitato**
Ingresso 1 associato a **Zona63**
Ingresso 2 associato a **Zona64**
Tamper **Aperto**

Comunicazione

Connessione **Connesso**
Qualità Segnale RF **OTTIMO**

Test Segnale

Batteria

Ultima Lettura **3.1V**
Condizioni **Carica**

Aree Assegnate

Porta e Inerziale
A1 ☒ **A2** ☐ **A3** ☐ **A4** ☐
Modalità Attiva se tutte le aree inserite

Allarme

Numero di allarmi **5** Silenzioso ☐
Evento program. **Nessuno** Sempre ☐

Assegna a Zone in AND

Porta ☐

Porta

Abilitata ☒ Ritardata ☐ Interno ☐ Escludibile **Singolo**
Percorso ☐ Test ☐

Inerziale

Sensibilità **DISABILITATO** Test ☐



Aree Assegnate

Assegna il sensore all'area o alle aree desiderate.

Valori programmabili: A1 ... A4

Default: A1



Allarme, Numero di allarmi

Stabilisce il numero di cicli allarme che il sensore può generare tra un inserimento e il successivo disinserimento. Per ciclo allarme si intende l'attivazione della sirena. Una volta raggiunto il limite, il sensore ritorna attivo solo disinserendo e reinserendo l'area. Questa impostazione non limita il numero di eventi trasmessi dal comunicatore: durante un ciclo allarme; se il sensore va ripetutamente in allarme vengono trasmessi tutti i nuovi eventi. Le trasmissioni non vengono più effettuate solo quando è stato raggiunto il limite degli allarmi

Valori programmabili: Infinito / 1 / 3 / 5

Default: 5

Allarme, Silenzioso

Se abilitato l'allarme di questo sensore non attiva la sirena.

Default: Disabilitato

Allarme, Evento programmabile

L'allarme generato dal sensore può attivare un evento programmabile fra quelli disponibili, è possibile inoltre selezionare quando è attiva questa funzione:

Sempre

Se non attivo Area/e di appartenenza disinserita

Se attivo Area/e di appartenenza inserita

Valori programmabili: Nessuno, Programmabile 1 ... 8

Default: Nessuno, Sempre

Assegna a Zone in AND, Porta e Inerziale

Assegna il contatto Porta al funzionamento in combinazione con altre zone. Da configurare nella pagina Zone in AND dedicata.

Default: Disabilitato

**Porta, Abilitata**

Questo parametro serve per poter disabilitare la sezione "porta" in modo da poter installare il sensore senza il magnete.

Default: abilitata

**Porta, Ritardata**

Se abilitato, la sezione "porta" è ritardata e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: disabilitata

**Porta, Interno (Porta / Inerziale)**

Se abilitato, le sezioni "porta" e "inerziale" sono interne e pertanto non sono attive quando l'area di appartenenza è inserita in modo perimetrale o notte.

Default: Disabilitato

**Porta, Escludibile**

Se abilitato, la sezione "porta" è escludibile tramite inserimento forzato. Una volta escluso, il contatto magnetico principale ritorna attivo in base alla programmazione scelta. Un controllo impedisce l'abilitazione di questo parametro se la sezione è ritardata.

Valori programmabili:

NO	Non è escludibile.
Singolo	Escludibile da inserimento forzato
Auto	Escludibile da inserimento forzato con reinclusione automatica quando torna a riposo

Default: Singolo.

Porta, Percorso

Evita che la sezione "porta" generi allarme quando nell'area di appartenenza è attivo il tempo di ingresso causato da un dispositivo ritardato.

Default: Disabilitato

Porta, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme generato dalla sezione "porta" viene solo registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato

**Inerziale, Sensibilità**

Attiva ed imposta la sensibilità della sezione "inerziale". Il valore più adatto deve essere trovato sperimentalmente aiutandosi con la tabella seguente.

Valori programmabili: Disabilitato, Livello 1 (sensibilità minima) ... Livello 7 (sensibilità max)

Default: Disabilitato

Inerziale, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme generato dalla sezione "inerziale" viene solo registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato

**Ausiliario, Abilitato**

Questo parametro serve per poter disabilitare la sezione "ausiliario" (morsetti AUX), in modo da poter installare il sensore senza dover cortocircuitare questi morsetti.

Default: Disabilitato



Ausiliario, Ritardato

Se abilitato, la sezione "ausiliario" è ritardato e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: Disabilitato



Ausiliario, Escludibile

Se abilitato, la sezione "ausiliario" è escludibile tramite inserimento forzato. Una volta esclusa, questa sezione ritorna attiva in base alla programmazione scelta. Un controllo impedisce l'abilitazione di questo parametro se la sezione è ritardata.

Valori programmabili:

NO	Non è escludibile.
Singolo	Escludibile da inserimento forzato
Auto	Escludibile da inserimento forzato con reinclusione automatica quando torna a riposo

Default: Singolo.

Ausiliario, Percorso

Evita che la sezione "ausiliario" vada in allarme quando nell'area di appartenenza è attivo il tempo di ingresso causato da un dispositivo ritardato.

Default: Disabilitato

Ausiliario, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme generato dalla sezione "ausiliario" viene solo registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato



Tapparella, Impulsi

Stabilisce il numero di impulsi necessari alla sezione "tapparella" a provocare l'allarme in una finestra temporale impostata dal parametro Tempo Reset. Il numero di impulsi è proporzionale allo spostamento della tapparella e dipende dal tipo di sensore.

Valori programmabili: 1, 4, 8, 16, 32.

Default: 4



Tapparella, T. Reset (sec)

Determina il tempo (in secondi) entro il quale sono conteggiati gli impulsi.

Valori programmabili: 1, 3, 5, 8.

Default: 3

Tapparella, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme generato dalla sezione "tapparella" viene solo registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato

NOTA.

Il dispositivo riconosce automaticamente se il sensore tapparella è presente rilevando il cortocircuito (sensore presente) o il circuito aperto (sensore non presente); se la sezione non è utilizzata i morsetti tapparella devono essere lasciati scollegati.

BT-KPXW tastiera capacitiva wireless

KPXW

☒ **Abilitata**

Ver. 00

Descrizione dispositivo

Dispos.9

☐ Controllo consumo elevato

☐ Esterno (Tempo di uscita non attivato all'inserimento)

Ripristina

Cancela

Annula

Alinea

Statistiche

Stato

Statistiche

Sistema

Tamper

Chiuso

Ultimo tag Letto

Non presente

Comunicazione

Connessione

Connesso

Qualità Segnale RF

OTTIMO

Test Segnale

Batteria

Ultima Lettura

6.0V

Condizioni

Carica

Aree visualizzate e segnalazioni sonore con utente non loggato

Area1

☒

Area2

☐

Area3

☐

Area4

☐

☐ Inserimento rapido abilitato

Lettore Tag

Modalità di comunicazione sicura (non compatibile con i vecchi modelli di tag)

☒

Suoni

Livello audio

ALTO

Segnalazione audio su tempo di ingresso e uscita

☒

Funzionalità

Tasto 1

Nessuno

☐ Attivabile senza autenticazione utente

Tasto 2

Nessuno

☐ Attivabile senza autenticazione utente

Tasto 3

Nessuno

☐ Attivabile senza autenticazione utente

Tasto 4

Nessuno

☐ Attivabile senza autenticazione utente

Tasto 5

Nessuno

☐ Attivabile senza autenticazione utente

Tasto 6

Nessuno

☐ Attivabile senza autenticazione utente

Esterno (tempo di uscita non attivato all'inserimento)

Se abilitato, un inserimento effettuato da questa tastiera attiva immediatamente anche i sensori ritardati.

Default: Disabilitato

Aree Visualizzate e segnalazioni sonore con utente non loggato

Permettono di limitare la visibilità dello stato delle aree quando si attiva la tastiera (prima di inserire la password) e contemporaneamente disattivano le segnalazioni acustiche per le aree non visibili.

Valori programmabili: A1 ... A4

Default: A1

Inserimento rapido abilitato

Imposta l'area da inserire con l'operazione Inserimento rapido, cioè senza password.

Default: Disabilitato

Lettore Tag, Modalità di comunicazione sicura (non compatibile con i vecchi modelli di tag)

Se disabilitato, i vecchi modelli di BT-TAG o BT-CARD non verranno letti.

Default: Disabilitato

Luminosità, Spenta con tastiera in stand-by

Se abilitato, quando la tastiera passa in modalità stand-by, spegne display e pulsanti.

Default: Disabilitato

Suoni, Livello audio

Definisce il volume delle segnalazioni audio.

Valori programmabili: ALTO, MEDIO, BASSO

Default: ALTO

Programmazione

SICEP[®]

- 60 -

Suoni, Segnalazione audio su tempo di ingresso e uscita

Abilita o disabilita le segnalazioni audio durante i tempi di Ingresso e di Uscita.

Default: Abilitato

Funzionalità, Tasto X

Ai pulsanti da 1 a 6 è possibile assegnare uno scenario da eseguire alla pressione prolungata del pulsante.

Valori programmabili: Scenario1..Scenario8

Default: Nessuno

Funzionalità, Attivabile senza autenticazione utente

Se abilitato, l'esecuzione dello scenario non necessita di password o TAG di riconoscimento.

Default: Disabilitato

BT-SKW tastiera capacitiva wireless.

Tastiera

☒ **Abilitata**

[Ver. 09]

Descrizione dispositivo

☐ Controllo Consumo Elevato

☐ Esterno (Tempo di uscita non attivato all'inserimento)

☒

Statistiche

Tamper

Tamper **Chiuso**

Comunicazione

Connessione **Connesso**

Qualità Segnale RF ...

Batteria

Ultima Lettura **3.4V**

Condizioni **Carica**

Aree Visibili e Segnalazioni Acustiche

A1 ☒ A2 ☒ A3 ☒ A4 ☒

Funzioni Tastiera

Inserimento Rapido

Tasto funzione

Esterno (tempo di uscita non attivato all'inserimento)

Se abilitato, un inserimento effettuato da questo lettore attiva immediatamente anche i sensori ritardati.

Default: Disabilitato

**Aree Visibili e Segnalazione Acustiche**

Permettono di limitare la visibilità dello stato delle aree quando si attiva la tastiera (prima di inserire la password) e contemporaneamente disattivano le segnalazioni acustiche per le aree non visibili.

Valori programmabili: A1 ... A4

Default: A1, A2, A3, A4

Funzioni Tastiera, Inserimento rapido

Imposta l'area da inserire con l'operazione Inserimento rapido (senza password).

Valori programmabili: Disabilitato, Area 1 ... Area 4.

Default: Disabilitato

Funzioni Tastiera, Tasto funzione

Assegna al tasto "P" un evento programmabile

Valori programmabili: Nessuno, Programmabile 1 ... 8.

Default: Nessuno

BT-PRW Lettore RFID wireless

Lettore tag
[Ver. 02]

☒ **Abilitata**
 Descrizione dispositivo:
☐ Controllo Consumo Elevato
☐ Esterno (Tempo di uscita non attivato all'inserimento)

Statistiche

Sistema		Comunicazione	
Tamper	Chiuso	Connessione	Connesso
Antistrappo	Chiuso	Qualità Segnale RF	...
Ultimo Tag Letto: Non presente		Test Segnale	
Batteria			
Ultima Lettura		3.2V	
Condizioni		Carica	

Configurazione Lettore

Apriporta:
 Area visibile:
 Abilitazione Buzzer: ☒
 Abilitazione Antistrappo: ☒

Esterno (tempo di uscita non attivato all'inserimento)

Se abilitato, un inserimento effettuato da questo lettore attiva immediatamente anche i sensori ritardati.

Default: Disabilitato

Configurazione Lettore, Apriporta

Abilita il relè locale (a bordo del lettore) alla funzione Apriporta.

Valori programmabili: Disabilitato, relè locale

Default: Disabilitato

Configurazione Lettore, Area visibile

Permette di attivare la visibilità continua dello stato dell'area (tramite lampeggio della barra e contemporaneamente attivare le segnalazioni acustiche).

Valori programmabili: Disabilitato, Area1 ... Area4.

Default: Area1

Configurazione Lettore, Abilitazione Buzzer

Permette di disabilitare le segnalazioni acustiche relative ai tempi di ingresso e di uscita

Default: Abilitato

Configurazione Lettore, Abilitazione Antistrappo

Permette di disabilitare l'antistrappo; in questo modo non è necessario fissare al muro l'apposito magnete.

Default: Abilitato

BT-SMK2 Sensore di fumo

Antiincendio
[Ver. 00]

☒ **Abilitata**
 Descrizione dispositivo

Statistiche

Sistema		Comunicazione	
Incendio	Normale	Connessione	Connesso
Rivelatore Fumo	Regolare	Qualità Segnale RF	...
Circuito Controllo	Regolare	Test Segnale	
Temperatura	21,7 °C	Batteria	
		Ultima Lettura	8.8V
		Condizioni	Carica

Configurazione Antiincendio

Ripetitore allarme sonoro ☒

Test Rivelatore

Premuto esegue un test della camera a fumo senza generare un allarme incendio.

Sistema, Incendio

Indica se il sensore si trova nello stato regolare oppure negli stati di allarme per rivelazione fumo o per aumento temperatura. Il ripristino dell'allarme fumo avviene dopo circa 4 minuti dalla fine della rivelazione.

Sistema, Rivelatore Fumo

Indica lo stato della camera ottica (rilevatore fumo). In caso di guasto il sensore emette un segnale acustico ogni 60 secondi circa.

Sistema, Circuito Controllo

Riporta l'eventuale guasto della parte elettronica che segue la camera ottica; tale informazione viene indicata anche dall'assenza del lampeggio periodico del led rosso.

Sistema, Temperatura

Indica l'ultimo valore di temperatura misurato dal sensore.

Batteria

Riporta l'ultima lettura della tensione della batteria. La soglia per avere batteria scarica è 7,5V e in questa condizione il sensore emette un segnale acustico ogni 60 secondi; il sensore ha circa 30 giorni di autonomia dall'inizio della segnalazione.

ATTENZIONE!

I valori temperatura e batteria sono aggiornati ogni 7 minuti e mezzo. È normale che i valori riportati alla registrazione siano 0.0.

Ripetitore allarme sonoro

Se abilitato, il sensore attiva la sua sirena in tutti i casi di allarme incendio cioè anche quelli provocati da altri sensori fumo, allarmi manuali da tastiera, ecc.)

Default: Abilitato

BT-ALMA Sirena da esterno BT-SIR Sirena da esterno

Sirena

☒ **Abilitata**

[Ver. 06]

Descrizione dispositivo

Controllo Consumo Elevato ☐

☒

Statistiche

Sistema		Comunicazione	
Stato	Riposo	Connessione	Connesso
Antischiuma	Riposo	Qualità Segnale RF	...
Tamper	Chiuso		Test Segnale
Sup. Temperatura	Riposo	Batteria	
Antiscasso	Riposo	Ultima Lettura	3.4V
Accciamento	...	Condizioni	Carica

Aree Assegnate

A1 ☒ A2 ☐ A3 ☐ A4 ☐

Suono

Tipo

Volume

Segnalazioni

☒ Lampeggio per allarme
 ☐ Lampeggio per impianto inserito
 ☐ Memoria allarme
 Preallarme

Controlli

Superamento temperatura
 Antischiuma
 Antiscasso

Pulsante Test

Permette di eseguire il test della segnalazione locale (suono + accensione led).

Aree Assegnate

Permette di associare le funzioni Lampeggio per allarme, Memoria allarme, Lampeggio a impianto inserito solo a determinate aree. Questa impostazione non influisce sull'attivazione della sirena in caso di allarme. L'associazione della sirena con l'allarme dell'area viene effettuata nella pagina Eventi.

Default: Area 1

Suono, Tipo

Permette di scegliere il suono associato agli eventi Furto e allarmi 24H fra i 4 disponibili. L'evento Incendio ha un suono dedicato.

Valori programmabili: suono 1 ... 4.

Default: 1

Suono, Volume

Stabilisce il volume del suono su tre livelli.

Valori programmabili: minimo, medio, massimo

Default: massimo

Controlli, Superamento temperatura

Abilita il controllo della temperatura per un tentativo di sabotaggio della sirena con l'incendio del contenitore.

Default: Disabilitato

Controlli, Antischiuma

Abilita il controllo antischiuma (alette laterali attive) per un tentativo di sabotaggio.

Default: Disabilitato

Controlli, Antiscasso

Abilita il controllo del sensore inerziale a bordo della sirena per il riconoscimento di urti sul contenitore.

Valori programmabili: Disabilitato, Sensibilità Bassa / Media / Bassa. Default: Disabilitato

Segnalazioni, Lampeggio per Allarme

Permette di abilitare il flash a led durante l'attivazione per allarme.

Default: Abilitato

Segnalazioni, Lampeggio per impianto inserito

Attiva il lampeggio del led rosso quando almeno una fra le aree associate è inserita. La segnalazione avviene con un doppio lampeggio ogni 6 secondi.

Default: Disabilitato

Segnalazioni, Memoria allarme.

Attiva il lampeggio del led rosso quando un'area fra quelle associate è andata in allarme. La segnalazione avviene con un singolo lampeggio ogni 3 secondi.

Default: Disabilitato

Segnalazioni, Preallarme.

Attiva il lampeggio e il segnale acustico durante il tempo di ingresso, ovvero quando è stato allarmato un sensore o una zona ritardata.

Valori programmabili: Disabilitato, Sonoro, Luminoso, Sonoro + Luminoso

Default: Disabilitato

BT-ER2 Espansioni input/output radio

In/Out radio
[Ver. 00]

☒ **Abilitata**
 Descrizione dispositivo
 Controllo Consumo Elevato ☐

Statistiche

Sistema

Rete: **Assente**

Ingresso 1 associato a: **Zona1**

Ingresso 2 associato a: **Zona2**

Relè 1 associato a: **Uscita1**

Relè 2 associato a: **Uscita2**

Comunicazione

Connessione **Connesso**

Qualità Segnale RF ...

Batteria

Ultima Lettura **2.9V**

Condizioni **Carica**

Sistema, Rete

Mostra la presenza dell'alimentazione da rete: Assente, Presente.

**Sistema, Ingresso X associato a:**

Mostra i due ingressi a bordo scheda a quali ingressi filari sono associati.

Sistema, Relè X associato a:

Mostra i due relè a bordo scheda a quali uscite sono associate.

BT-NI Generatore di fumo

Fumogeno/Nebbiogeno

☒ **Abilitata** Ver. 00

Descrizione dispositivo

☒

Statistiche

Sistema

Stato cartuccia	Regolare
Stato dispositivo	Riposo
Tamper	Chiuso
Antistrappo	Chiuso

Comunicazione

Connessione	Connesso
Qualità Segnale RF	...
Test Segnale	

Batteria

Ultima Lettura	3.0V
Condizioni	Carica

Fumogeno

Impianto in manutenzione, fumogeno non attivo.

Configurazione

Abilitazione antistrappo ☒

Abilitazione lampeggio led stato ☒

Data di scadenza della cartuccia (MM/AA) /

Abilitazione antistrappo

Permette di disabilitare l'antistrappo; da utilizzare in situazioni dove la parete di fissaggio del dispositivo non è perfettamente planare.

Default: Abilitato

Abilitazione lampeggio led stato

Permette di disabilitare il lampeggio del led di stato. Questa funzione aumenta l'autonomia della batteria.

Default: Abilitato

Data di scadenza della cartuccia (MM/AA)

Consente di inserire il mese e l'anno di scadenza del generatore di fumo come indicato sul generatore di fumo.

Ha esclusivamente una funzione di promemoria attivando l'evento ad esso associato.

Default: da assegnare

IF-URFOG interfaccia per nebbiogeno

Fumogeno/Nebbiogeno
Ver. 00

☒ **Abilitato**

Descrizione dispositivo

Statistiche

Sistema		Comunicazione	
Stato cartuccia	Regolare	Connessione	Connesso
Stato dispositivo	Pronto!	Qualità Segnale RF	...
		Test Segnale	
Alimentazione		Batteria	
Perc. Liquido	89%	Ultima Lettura	...
		Condizioni	Carica

Controllo

ATTENZIONE! Dispositivo attivo e pronto all'uso.

Configurazione

Tempo di sparo: (1-50 Secondi)
 Modello: Compact 390

Attenzione! Eseguire solo se la cartuccia è piena

Stato, Sistema

Finestra di sola lettura indicante lo stato del nebbiogeno e delle sue componenti:

- Stato Cartuccia: Regolare / Esaurita
- Stato dispositivo: Pronto! / Attesa riscaldamento
- Alimentazione: Regolare / Allarme
- Perc. Liquido: 1% ÷ 100%

Tempo di sparo:(1-50 Secondi)

Imposta i secondi di attivazione del nebbiogeno.

Valori programmabili: 1 ... 50

Default: 30

Reset contatore spari effettuati

La Percentuale di Liquido della cartuccia è una stima calcolata in base all'utilizzo. Premendo questo pulsante, viene effettuato un reset riportando la percentuale al 100%. Premere esclusivamente ad ogni sostituzione della cartuccia.

BT-REP2 ripetitore

Ripetitore
☒ **Abilitata**
 Descrizione dispositivo

[Ver. 10]

Stato Sistema

Sistema		Comunicazione	
Tamper	Aperto	Connessione	Connesso
Rete	Presente	Qualità Segnale RF	OTTIMO
Carica Batterie	Non attivo	0.0V Test Segnale	
Accensione Radio	Normale		

Batteria
 Ultima Lettura **0.0V**
 Condizioni **Scarica**

Dispositivi Registrati sul Ripetitore



Dispositivi Registrati sul Ripetitore

In questa finestra è riportato l'elenco dei dispositivi registrati sul ripetitore.



Registra dispositivo

Permette di avviare la procedura di registrazione di un nuovo dispositivo che transiterà sul ripetitore.

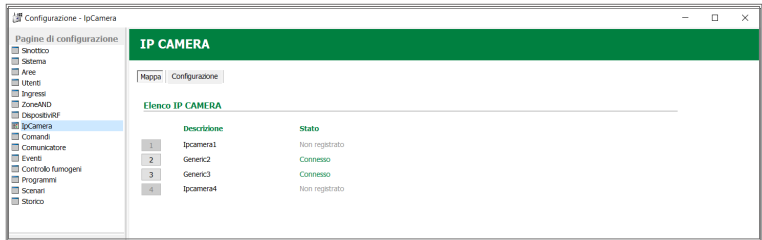


Cancella dispositivo

Permette di avviare la procedura di cancellazione di un dispositivo dal ripetitore.

6.3.9 IpCamera

Mappa



Pagina dedicata alla registrazione e configurazione delle IpCamera Dahua serie WizSense.

Per ogni dispositivo sono elencati:

Descrizione Una descrizione che serve per riconoscere il sensore fra gli altri registrati.

Stato Riporta lo stato del dispositivo; è presente il tamper più altre caratteristiche specifiche del dispositivo. Gli stati sono aggiornati in tempo reale.

Ipcamera1

Abilitato ☒

Descrizione:

Indirizzo IP:

User:

Password:

Serial number:

Motion detection: ☒

Smart motion detection: ☐

Ricezione eventi IVS (Attraversamento linea o intrusione): ☐

Abilitazione controllo assenza connessione: ☐

Funzione:

Aree Assegnate

Area1 ☒ Area2 ☐ Area3 ☐ Area4 ☐

Allarme

Numero di allarmi:

Silenzioso: ☐

Stato

Connessione: **Connesso**

Stato: **Non attivo**

Impostazioni

Ritardata: ☐

Interno: ☐

Assegna a zone in AND: ☐

Percorso: ☐

Test: ☐



Abilitato

Abilita o disabilita l'utilizzo della IpCamera.

Default: Abilitato



Descrizione

È il campo dove impostare il nome della IpCamera. Inserire una breve descrizione con 19 caratteri massimi compresi gli spazi.

Default: Generic X

**Indirizzo IP**

Impostare l'indirizzo IP della IpCamera.

**User**

Impostare il nome utente per accedere alla IpCamera.

**Password**

Impostare la password per accedere alla IpCamera.

**Serial number**

Campo di sola visualizzazione in cui viene riportato il numero seriale della IpCamera.

**Motion detection**

Permette alla Centralina di abilitare/disabilitare la segnalazione di allarme per Motion detection sulla IpCamera. In caso di Funzione *Furto*, il Motion detection dipenderà dallo stato di inserimento dell'area di appartenenza. Per Funzione *Allarme 24h* o *Tecnologico*, il Motion detection sarà sempre attivo.

Default: Disabilitato

**Smart motion detection**

Funzione simile a *Motion detection* ma l'evento viene generato solo al riconoscimento di persone o auto.

Default: Disabilitato

**Ricezione eventi IVS (Attraversamento linea o intrusione)**

Funzione simile a *Motion detection* ma l'evento viene generato solo all'attraversamento di una linea o in caso di intrusione in un'area. La linea e l'area devono essere disegnati tramite la pagina di configurazione web della telecamera.

Default: Disabilitato

**Abilitazione controllo assenza connessione**

Permette di abilitare/disabilitare il controllo di assenza connessione con la IpCamera

Default: Abilitato

**Funzione**

Imposta il tipo di allarme generato dalla IpCamera. E' possibile scegliere fra le seguenti tipologie:

Furto La IpCamera genera allarme solo quando l'area (o le aree) di appartenenza è inserita.

Allarme 24h La IpCamera è attiva 24h e genera l'apposito evento "Allarme 24h".

Tecnologico La IpCamera è attiva 24h e genera l'evento programmabile selezionato.

Default: Furto

**Evento programmabile**

Questa impostazione agisce solo per le IpCamera configurate con la funzione Tecnologico. L'allarme generato dall'ingresso può attivare un evento programmabile fra quelli disponibili
Valori programmabili: Nessuno, Programmabile 1 ... 8

Default: Nessuno

**Aree Assegnate**

Assegna la IpCamera all'area o alle aree desiderate. Nel caso che una IpCamera sia assegnata a due o più aree, genera allarme solo con tutte le aree inserite.

Le IpCamera con funzione Allarme 24h e Tecnologico non hanno aree assegnate.

Valori programmabili: A1 - A4

Default: A1



Allarme, Numero di allarmi

Questa impostazione agisce solo per le IpCamera configurate con la funzione Furto. Stabilisce il numero di cicli allarme (ovvero attivazioni della sirena) che l'ingresso può generare tra un inserimento e il successivo disinserimento; una volta raggiunto il limite l'ingresso non è più attivo e per riarmarlo è necessario disinserire e reinsertire l'area. Questa impostazione è utilizzabile solo per con la funzione Furto, per tutte le altre il parametro è forzato a Infinito.

Questa impostazione non limita il numero di eventi trasmessi dal comunicatore: durante un ciclo allarme se l'ingresso va ripetutamente in allarme vengono trasmessi tutti i nuovi eventi. Le trasmissioni non vengono più effettuate solo al termine dei cicli.

Valori programmabili: Infinito / 1 / 3 / 5

Default: Inf

Allarme, Silenzioso

Inibisce l'attivazione della sirena in caso di allarme.

Default: Disabilitata (sirena attiva)



Allarme, Attiva speaker su allarme area

In caso di allarme Furto, attiva lo speaker della IpCamera per la riproduzione del messaggio di allerta programmato.

Default: Disabilitato



Allarme, Attiva flash su allarme area

In caso di allarme Furto, attiva i lampeggianti integrati nella IpCamera.

Default: Disabilitato



Impostazioni, Ritardata

Se abilitato la IpCamera è ritardata e i tempi di ingresso e di uscita sono quelli programmati per l'area di appartenenza.

Default: Disabilitato

Impostazioni, Percorso

Questa impostazione agisce solo per le IpCamera con funzione Furto. Evita che l'ingresso generi un allarme quando nell'area di appartenenza è attivo il "tempo di ingresso"

Default: Disabilitato



Impostazioni, Interno

Questa impostazione agisce solo per gli ingressi Furto. Se abilitato l'ingresso è interno e pertanto non è attivo quando l'area di appartenenza è inserita in modo perimetrale.

Default: Disabilitato

Impostazioni, Test

Questa impostazione serve per operazioni di test sull'impianto: se abilitato, l'allarme del sensore viene soltanto registrato nello storico, la sirena e il comunicatore non vengono attivati. Nel funzionamento normale questa impostazione deve essere disabilitata.

Default: Disabilitato

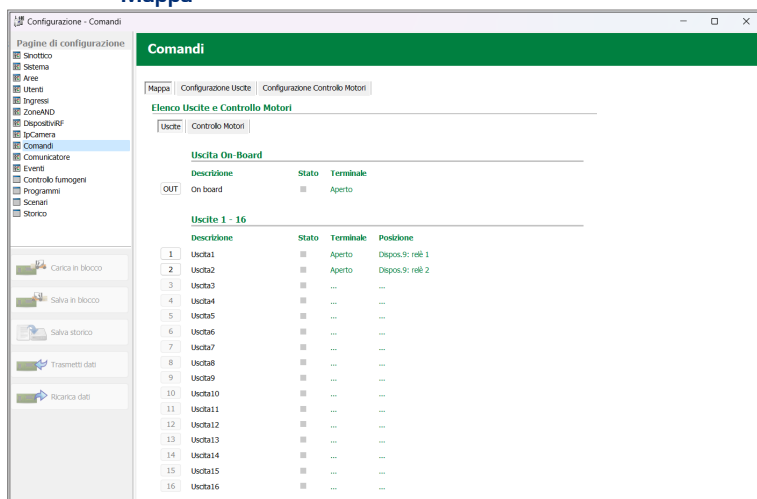
Impostazioni, Assegna a zone in AND

La IpCamera è assegnata al funzionamento in combinazione con altre zone. Da configurare nella pagina Zone in AND dedicata.

Default: Disabilitato

6.3.10 Pagina Comandi

Mappa



Elenco Uscite e Controllo Motori, Uscite Uscita On Board e Uscite 1 - 16

Questa mappa riporta l'elenco delle uscite presenti sulla DOGMA. Nella centralina è disponibile una sola Uscita On Board di tipo open collector, è però possibile aggiungere ulteriori uscite a relè per mezzo dei moduli di espansione radio mod. BT-ER2. Ognuna di queste espansioni aggiunge 2 uscite a relè con scambio libero e 2 ingressi filari.

Per selezionare la configurazione di una uscita premere sul pulsante relativo.

Accanto a ciascuna uscita è riportata la descrizione, lo stato reale, lo stato del terminale fisico ed eventualmente la corrispondenza del modulo di espansione radio a cui appartiene.

Elenco Uscite e Controllo Motori, Controllo Motori Controllo Motori

Questa mappa riporta l'elenco dei "Controllo Motori" presenti sulla DOGMA.

Per "controllo motore" si intende la capacità che ha il dispositivo DOGMA di pilotare attuatori per finestre o tende ecc. mediante l'utilizzo di apposite interfacce.

Ogni "controllo motore" mette a disposizione dell'installatore 2 relè con scambio libero da collegare al motore della tapparella o della tenda. Il "controllo motore" dispone di 3 funzioni programmabili di cui: apertura, chiusura e apertura parziale. La combinazione dell'attivazione dei relè con i tempi di esecuzione, assicurano il funzionamento del sistema. Per selezionare la configurazione di un "controllo motore" premere sul pulsante relativo.

Accanto a ciascun "controllo motore" è riportata la descrizione e la corrispondenza del modulo di espansione radio a cui appartiene.

Configurazione Uscite

Descrizione

Inserire una descrizione che sia attinente all'utilizzo dell'uscita (massimo 18 caratteri, spazi inclusi).
Default: ---

Configurazione, Impulsiva

Se abilitata, l'uscita funziona in modo impulsivo: una volta attivata, si disattiva dopo il Tempo impulso impostato (Durata).
Default: Disabilitato

Configurazione, Durata

Determina il tempo in secondi dello stato attivo per l'uscita impulsiva.
Valori programmabili: 1 / 5 / 10 / 30 / 60 / 120 / 240 / 600 sec.

Default: 5

Configurazione, Invertita

Se abilitata, inverte lo stato fisico del morsetto di uscita.

Default: Disabilitato

Configurazione, Controllabile direttamente da utente

Se abilitata, questo comando sarà disponibile su Sicep.

Default: Disabilitato

Stato

Mostra lo stato logico dell'uscita in tempo reale

Led	Descrizione
Grigio	Stato uscita spenta
Verde	Stato uscita attivata

Stato, Terminale

Riporta lo stato fisico dell'uscita.

Dicitura	Descrizione
Aperto	Uscita a riposo (transistor O.C. non attivo) / relè a riposo
Chiuso	Uscita attiva (transistor O.C. attivo) / relè attivato

Stato e terminale differiscono nel significato attribuito, secondo l'impostazione del parametro 'invertita'. Lo stato uscita spenta indica che il dispositivo connesso all'uscita (qualunque sia) è spento, questo indipendentemente dal fatto che, quest'ultimo, necessiti di un'uscita aperta o di un'uscita chiusa per essere nello stato spento. Così, allo stesso modo, vale per lo stato uscita accesa.

Stato, Funzionamento

Riporta l'utilizzo configurato per l'uscita: Uscita Semplice (singola uscita non legata al "controllo motori", oppure funzione assegnata dal controllo motori ed il riferimento del controllo motore.

Stato, Posizione

Riferimento del dispositivo radio a cui appartiene e riferimento del morsetto.

Controllo automatico, Programma

Associa all'uscita un programma orario per il controllo automatico.

Valori programmabili: Disabilitato / Programma1 - Programma 4 *Default: Disabilitato*

Configurazione Controllo Motori**Descrizione**

Inserire una descrizione che sia attinente all'utilizzo del controllo (massimo 18 caratteri, spazi inclusi).

Default: ---

Configurazione, Uscite utilizzate (APERTURA – CHIUSURA)

Consente di selezionare la coppia di uscite per il "controllo motore"

Default: Disabilitato

Configurazione, Tempo Apertura / Chiusura

Tempo di attivazione dei relè da impostare per garantire le operazioni di apertura / chiusura tapparella. In fase di configurazione, si consiglia di misurare il tempo necessario per le operazioni, quindi aggiungere alcuni secondi di margine di tempo ed assegnare il risultato a questo campo di impostazioni.

Configurazione, apertura Parziale (rispetto al tempo di apertura)

Percentuale calcolata sul tempo di Apertura utile ad ottenere una parzializzazione dell'operazione. Consente, in pratica, di poter aprire parzialmente una tapparella con un comando dedicato.

Valori programmabili: 25%, 50%, 75%.

Default: 25%

Configurazione, Controllabile direttamente da utente

Se abilitata, questo controllo motori sarà disponibile su Sicep.

Default: Disabilitato

Controllo Automatico, Programma

Associa al controllo motori un programma orario per il controllo automatico.

Valori programmabili: Disabilitato / Programma 1 - Programma 4 Default: Disabilitato

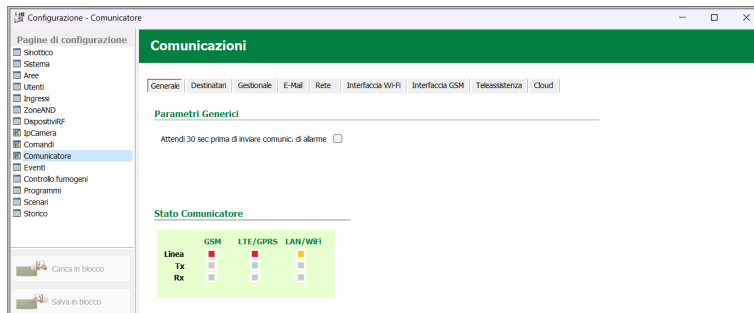
Controllo Automatico, Apertura parziale

Se abilitato, durante l'esecuzione del programma, effettua una apertura Parziale invece che Totale.

Default: Disabilitato

6.3.11 Pagina Comunicatore

Generale



Parametri Generali, Attendi 30 sec prima di inviare comunic. di allarme.

Ritarda di 30 secondi l'invio di una comunicazione di allarme per consentire all'utente di disattivare l'impianto che si è allarmato per errore.

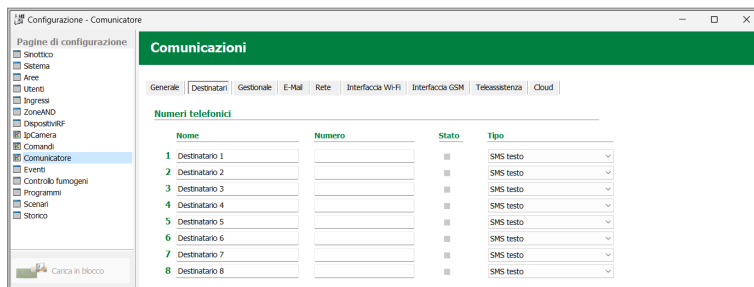
Default: Disabilitato

Stato Comunicatore (indicazioni luminose)

Permettono di controllare l'esito e lo stato delle comunicazioni. I colori hanno il seguente significato:

Led	Descrizione
Verde	Presente ma non in uso / tentativo riuscito
Giallo	In uso / tentativo di comunicazione in corso
Rosso	Non presente / tentativo di comunicazione fallito

Destinatari



Numeri telefonici, Nome

Specificare il nome di riferimento del destinatario. Massimo 19 caratteri, spazi inclusi.



Numeri telefonici, Numero

Specificare il numero del destinatario. Massimo 20 cifre.

Numeri telefonici, Stato

Permette di conoscere l'esito della comunicazione. I colori hanno il seguente significato:

Led	Descrizione
Verde	Tentativo riuscito
Giallo	Tentativo in corso
Rosso	Tentativo fallito



Numeri telefonici, Tipo

Specifica la modalità di contatto con il destinatario.

Valori programmabili: SMS testo, Squillo, Squillo e SMS testo

Default: SMS testo

Gestionale



Gestionale, Codice periferica

Impostare il codice numerico della centralina utilizzato Con la Centrale Operativa della Vigilanza e per la connessione da Sicep Cloud Connect.

Valori programmabili: da 1 a 99999.

Default: 100

Gestionale, Tipo gestionale

Imposta il tipo di Centrale Operativa, se MvsNET o SIA-IP compatibile.

Valori programmabili: MvsNet, SIA-IP

Default: MvsNET

Gestionale, Protocollo di comunicazione (solo per SIA-IP)

Scegliere il protocollo fra UDP e TCP

Valori programmabili: UDP, TCP

Default: UDP



Indirizzi centrale operativa, Indirizzo Primario

Impostare l'indirizzo IP o l'hostname primario del destinatario, in base al vettore disponibile.

Default: ---



Indirizzi centrale operativa, Indirizzo Secondario

Impostare l'indirizzo IP o l'hostname secondario del destinatario, in base al vettore disponibile.

Default: ---

NOTA.

Normalmente gli accessi alla Centrale Operativa vengono effettuati sul primo indirizzo. Solo se esiste e non va a buon fine l'accesso all'indirizzo primario, si passa all'indirizzo secondario.



Indirizzi centrale operativa, Porta TCP (solo per MvsNET)

Porta per la connessione TCP. Modificare solo in caso di utilizzi particolari.

Default: 9016



Indirizzi centrale operativa, Porta UDP (solo per MvsNET)

Porta per la trasmissione di pacchetti UDP. Modificare solo in caso di utilizzi particolari.

Default: 9001

Indirizzi centrale operativa, Porta di comunicazione (solo per SIA-IP)

Porta per la connessione via SIA-IP.

Default: 0



Numero SMS, Numero SMS Dati (solo per MvsNET)

Impostare il numero destinatario del GSM della Centrale Operativa della vigilanza.

Default: vuoto

Sicurezza, Utilizza crittografia (solo per SIA-IP)

Abilitando questa funzione, il collegamento da e verso la Centrale Operativa viene crittografato in base alla chiave crittografica impostata.

Default: Disabilitato

Sicurezza, Chiave crittografica (solo per SIA-IP)

Introdurre la chiave crittografica utilizzata per la comunicazione criptata da e verso la Centrale Operativa. È permesso l'introduzione di una chiave a 32 o 64 caratteri esadecimali (0-9 A-F).

Invio immagini su server FTP, Indirizzo

Invio immagini su server FTP, Porta

Invio immagini su server FTP, User

Invio immagini su server FTP, Password

(solo per SIA-IP)

Parametri di configurazione per accedere ad un server FTP dove trasmettere le immagini.

Stato comunicazioni Gestionale

Utilizzare questo riquadro per testare le comunicazioni con la centrale di vigilanza. Agendo sui tasti è possibile forzare l'invio di un messaggio di prova sul vettore scelto.

In condizioni operative normali il vettore non è selezionabile ma viene scelto automaticamente dalla centralina, che dà priorità ai vettori più veloce fra quelli operativi, e passa a utilizzare gli altri più lenti se la comunicazione fallisce. È importante testare singolarmente i vettori a disposizione perché, anche se le comunicazioni sembrano regolari, non è detto che non ci sia un malfunzionamento su uno dei vettori configurati.

E-Mail

Destinatari E-Mail, E-Mail 1 - 8

Inserire gli indirizzi e-mail dei destinatari.

Destinatari E-Mail, pulsante "Invia Test"

Premuto invia un messaggio di prova al rispettivo destinatario. Durante il test sono visualizzate delle indicazioni nel campo Stato del Test.

Configurazione, Invia email solo tramite LAN

Se abilitato, l'invio delle e-mail avviene solo tramite il vettore LAN e non tramite LTE/ GPRS.

Configurazione, Oggetto

Permette di personalizzare l'oggetto delle e-mail inviate. Massimo 32 caratteri spazi inclusi.

Default: Centralina di allarme

Configurazione, Indirizzo mittente

L'indirizzo mittente è previsto dal protocollo della posta elettronica. Nel caso si utilizzi un server di posta che richiede l'autenticazione, l'indirizzo mittente deve essere compilato e coincidere con quello dell'account per il quale è stata fatta l'autenticazione. In tutti gli altri casi si può lasciare di default.

Default: dogma@sicep.it

Configurazione, Server SMTP**Configurazione, Porta****Configurazione, Utilizza autenticazione****Configurazione, User****Configurazione, Password****Configurazione, Utilizza crittografia (SSL/TLS)**

Inserire i dati relativi al server utilizzato per l'invio della posta elettronica. La porta di default è 25, ma questo valore deve essere lasciato solo se il server non richiede l'autenticazione. Ogni server richiede una propria configurazione; normalmente basta cercare in Internet i parametri necessari digitando nel motore di ricerca "nomeserver configurazione SMTP". Qui di seguito alcuni esempi; alcuni server permettono anche configurazioni alternative. Quando l'autenticazione è richiesta è necessario registrare un account presso il provider scelto, ovvero aprire una casella di posta.

Nome	Server SMTP	Porta	Utilizza Autenticazione	Utilizza Crittografia
Gmail	smtp.gmail.com	465	SI	SI
Gmail	smtp.gmail.com	587/25	SI	NO
Libero	smtp.libero.it	465	SI	SI
Tiscali	smtp.tiscali.it	465	SI	SI
Tiscali	smtp.tiscali.it	25	NO	NO
Yahoo!	smtp.mail.yahoo.it	465	SI	SI
Yahoo!	smtp.mail.yahoo.it	25	SI	NO
Fastweb	smtp.fastwebnet.it	587	SI	SI

ATTENZIONE!

Le informazioni fornite qui sopra sono solo indicative e possono essere modificate dai rispettivi provider in qualsiasi momento senza preavviso.

Rete

Questa pagina configura le impostazioni di rete della centralina. Per default è abilitata la configurazione automatica tramite DHCP.

**Impostazioni di rete locale, Abilita DHCP****Impostazioni di rete locale, Hostname**

Attiva/disattiva il servizio di assegnazione automatica degli indirizzi IP (DHCP) per la centralina e gli assegna un nome per riconoscerla all'interno della rete locale.

Default: dogma

**Impostazioni di rete locale, Indirizzo IP****Impostazioni di rete locale, Net Mask****Impostazioni di rete locale, Gateway**

In caso di DHCP abilitato sono campi in sola lettura e mostrano i parametri assegnati dal servizio di assegnazione indirizzi. Se sono nulli significa che non è stato possibile assegnare un indirizzo automatico di rete alla centralina. Se il DHCP è disabilitato, sono editabili, e vanno impostati con i parametri della propria rete interna.

**Server DNS Esterni, DNS Primario****Server DNS Esterni, DNS Secondario**

Indirizzo dei server di risoluzione degli indirizzi (DNS). Specificare gli indirizzi IP dei server DNS esterni. E' necessario specificare server esterni, non interni alla rete domestica, perché gli stessi indirizzi vengono utilizzati anche dalla connessione dati LTE/GPRS del modem GSM. Si possono utilizzare indirizzi interni solo nel caso che non si ha intenzione di utilizzare la connessione dati LTE/GPRS per le comunicazioni.

KeepAlive, Tempo KeepAlive (min)

Questo parametro imposta il tempo che intercorre fra un invio ed il successivo dei messaggi inviati alla Centrale Operativa su rete LAN/LTE/GPRS allo scopo di mantenere attivo il collegamento.

Valore programmabile: 0 - 9999

Default: 30

Dynamic DNS

Tale servizio è fornito da siti esterni. Entrambi i fornitori selezionabili forniscono un servizio di DNS dinamico previa iscrizione e sotto certe condizioni. In fase di iscrizione sarà richiesto di inserire i propri dati e di accettare le condizioni del servizio. Tali precauzioni, in genere, hanno lo scopo di evitare abusi o l'uso improprio del servizio. Far riferimento ai seguenti siti dei fornitori del servizio.

Fornitore	Descrizione
DynDNS	http://dyndns.it/
No-IP	http://www.noip.com/

Dynamic DNS, Server

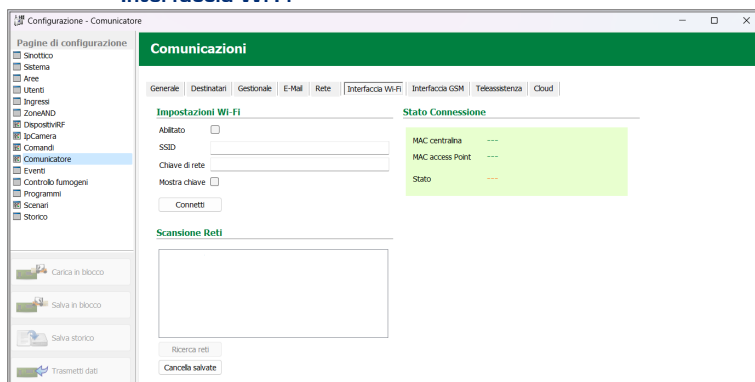
Selezionare il fornitore del servizio di DNS dinamico.

Valori programmabili: Disabilitato, DynDNS, No-IP

Default: Disabilitato

Dynamic DNS, Hostname**Dynamic DNS, Username****Dynamic DNS, Password**

Inserire i parametri che sono stati scelti o assegnati in fase di iscrizione al servizio DNS .

Interfaccia Wi-Fi**Impostazioni Wi-Fi, Abilitato**

Permette di abilitare o meno l'accesso alla rete WLAN. L'abilitazione di questa opzione disabilita l'accesso alla rete via ethernet ed è funzionante solo se è stato installato l'apposito modulo hardware aggiuntivo.

Default: Disabilitato

**Impostazioni Wi-Fi, SSID**

Identifica la rete Wi-Fi scelta per la connessione. In genere, questo parametro, non va inserito a mano ma va scelto fra quelli disponibili come risultato della scansione.

**Impostazioni Wi-Fi, Chiave di rete**

In caso di rete Wi-Fi criptata, identifica la chiave di criptatura dei dati, secondo il metodo scelto per la rete a cui ci stiamo connettendo. La chiave di rete viene scelta al momento dell'installazione della rete WLAN e deve essere conosciuta da tutti gli utenti autorizzati a connettersi alla rete. In caso contrario chiedere al tecnico che ha eseguito l'installazione.

Impostazioni WI-Fi, Mostra chiave

Consente di vedere la chiave di rete, che in condizioni normale è nascosta per motivi di segretezza.

Default: Disabilitato

Stato Connessione, Indirizzo MAC centralina

Mostra l'indirizzo MAC del modulo Wi-Fi installato sulla centralina.

Stato Connessione, Indirizzo MAC dell'access point

Quando la centralina è connessa alla rete, mostra l'indirizzo MAC dell'access point.

Stato Connessione, Stato

Mostra lo stato attuale della connessione.

Stato	Significato
Connesso	Connessa regolarmente alla rete Wi-Fi
Non connesso	Nessuna connessione stabilita
In connessione	Tentativo di connessione in corso
Disconnessione	Disconnessione dalla rete Wi-Fi
Scansione reti...	E' in corso una scansione delle reti Wi-Fi disponibili
Modulo assente	Il modulo Wi-Fi non è installato o non risponde
Rete inesistente	Il SSID inserito è sconosciuto o non appartiene a nessuna rete entro la portata radio
Password errata	La Chiave di rete inserita non è corretta
Conn. fallita	Si è verificato un problema in fase di connessione
---	Nessuna informazione sullo stato o in attesa di elaborazione

**Pulsante Connetti**

Dopo che sono stati inseriti tutti i parametri, premere il pulsante per eseguire un tentativo di connessione oppure per disconnettere una rete già connessa. La connessione alla rete Wi-Fi è automatica ad ogni riavvio dopo che è andata a buon fine la prima volta e se i parametri registrati restano validi.

**Pulsante Ricerca reti**

Esegue una scansione delle reti disponibili. Alla fine della scansione, per ogni rete elencata, si possono leggere: l'SSID, il livello del segnale (valore negativo: più siamo vicini allo zero e migliore è il livello del segnale) e il metodo di crittatura. Agendo sulla lista si seleziona una rete e l'SSID viene riportato nell'apposito campo. Possibile solo se la centrale non è già connessa a una rete Wi-Fi.

Pulsante Cancella salvate

Cancella la lista delle reti e i dati di connessione per le reti salvate.

Interfaccia GSM



Impostazioni GSM, Abilitato

Permette di abilitare o meno il comunicatore GSM LTE/GPRS. Se la SIM card non è presente è preferibile lasciare questo parametro disabilitato.

Default: Disabilitato

Impostazioni GSM, SIM PIN

Permette di utilizzare la SIM con il PIN attivo.

Valore programmabile: 0000 - 9999

Default: ---

ATTENZIONE!

Quando si utilizza una SIM con PIN attivato, se questo è errato o mancante la centralina esegue un solo tentativo di immissione del codice; però se questa viene resettata o spenta e riaccesa il PIN viene reimpresso e al terzo tentativo la SIM si blocca ed è necessario sbloccarla tramite il PUK. In questo caso è necessario togliere la SIM dalla centralina, inserirla in un telefono e digitare il PUK.



Impostazioni GSM, APN

Access Point Name, identifica l'accesso alla rete LTE/GPRS. Inserire il valore corretto del gestore utilizzato; se non è presente fra quelli disponibili è possibile scriverlo manualmente (es. Mio.gestore.net)

Default: ---

Valori programmabili preimpostati:

Vodafone	web.omnitel.it
TIM	ibox.tim.it
Wind	internet.wind.biz
Vodafone	internetm2m.air.com
Telit	nxt17.net

ATTENZIONE!

Le informazioni fornite qui sopra sono solo indicative e possono essere modificate dai rispettivi gestori in qualsiasi momento senza preavviso.

Impostazioni GSM, Abilitazione controllo accecamento

Se abilitato attiva una funzione che crea un apposito evento quando il GSM rileva un tentativo di accecamento. E' sufficiente che il disturbo sia presente per un breve tempo (< 30 secondi).

Default: Disabilitato

Modalità LTE/GPRS sempre connesso, Abilitata

Se abilitata, mantiene una connessione continua in LTE/GPRS verso la Centrale Operativa MvsNET.

Questo metodo di funzionamento (always-on), consente di ottenere delle comunicazioni rapide sia in fase di invio allarmi che in fase di interrogazione della centralina a scapito di un maggior consumo di energia e di dati trasmessi.

Controllo Credito residuo e scadenza SIM

Questa sezione deve essere utilizzata (abilitando il flag Controllo Attivo) solo se si sta utilizzando una SIM card di tipo prepagato ricaricabile.

Il controllo viene effettuato automaticamente ogni 48 ore.

ATTENZIONE!

Questa funzione è utilizzabile solo in Italia con SIM degli operatori TIM e Wind. La funzione si basa sulla richiesta di un SMS che viene letto dalla centralina. I gestori possono variare in qualsiasi momento e senza preavviso il messaggio di risposta e in tal caso la funzione smette di restituire o aggiornare il valore del credito.

Controllo Credito residuo e scadenza SIM, Controllo attivo

Abilita o disabilita il controllo. Se la SIM card non è di tipo prepagato ricaricabile, il controllo deve essere disabilitato.

Default: Disabilitato

Controllo Credito residuo e scadenza SIM, Gestore

Impostare il gestore della SIM card.

Valori programmabili: Sconosciuto / TIM / Wind

Default: TIM

Controllo Credito residuo e scadenza SIM, Giorni dall'ultima ricarica

Campo in cui deve essere riportato il numero di giorni trascorsi dall'ultima ricarica della SIM. La centralina aumenta automaticamente questo valore tutti i giorni e lo azzerà quando rileva un aumento del credito (ricarica). L'allarme viene generato quando si raggiunge 320 (SIM prossima alla scadenza).

Default: ---

Controllo Credito residuo e scadenza SIM, Pulsante Verifica credito

Premuto effettua immediatamente il controllo del credito.

Pannello di stato

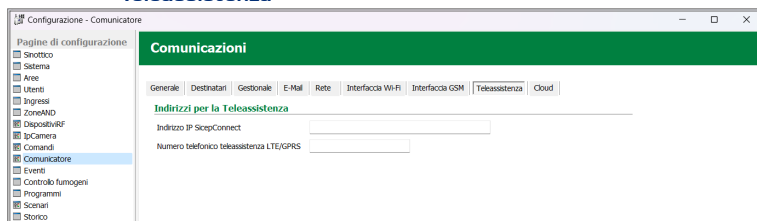
Permette di verificare le impostazioni automatiche del GSM LTE/GPRS e di controllarne lo stato mediante indicatori luminosi che hanno il seguente significato:

Led	Descrizione
Verde	Presente ma non in uso / stato normale o regolare
Giallo	In uso / tentativo in corso
Rosso	Non presente / operazione non riuscita o non possibile

La barra indica l'intensità del campo GSM. I colori indicano:

Led	Descrizione
Verde	Segnale buono /ottimo, comunicazione affidabile
Giallo	Segnale appena sufficiente
Rosso	Segnale scarso, comunicazione non affidabile

Teleassistenza



Indirizzi per la Teleassistenza, Indirizzo IP ScepConnect

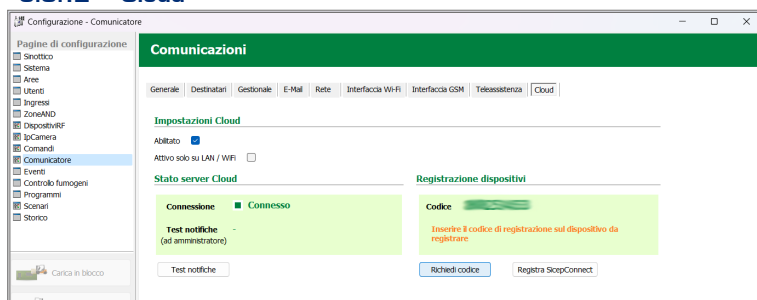
Indirizzo IP o hostname del computer dell'installatore da cui intende effettuare la teleassistenza, tramite LTE/GPRS o LAN. Questi indirizzi devono essere diversi dai rispettivi indirizzi della Centrale Operativa; un controllo automatico impedisce

Default: ---

Indirizzi per la Teleassistenza, Numero telefonico teleassistenza LTE/GPRS

La centralina riconosce questo numero come una chiamata proveniente dall'installatore, termina la chiamata in corso e tenta di stabilire una connessione verso l'indirizzo IP/hostname LTE/GPRS se questo è stato configurato. La chiamata di risveglio per la periferica può essere effettuata da un qualsiasi telefono.

6.3.12 Cloud



Impostazioni Cloud, Abilitato

Permette di abilitare o meno il collegamento con il Cloud Sicep.

Default: Disabilitato

Stato server Cloud, Connessione

Indica lo stato della connessione con il Server.

Stato server Cloud, Test notifiche

Permette, tramite il pulsante "Test notifiche", di inviare una notifica verso il dispositivo mobile dell'amministratore.

Registrazione dispositivi, Codice

Permette, tramite il pulsante "Richiedi codice" di effettuare la richiesta del codice OTP al Cloud per la registrazione di Sicep o Sicep Cloud Connect. Il codice visualizzato dovrà essere inserito sul dispositivo mobile.

Registrazione dispositivi, Registra SicepConnect

Dopo aver effettuato la richiesta del codice, con questo pulsante si abilita automaticamente il software Sicep Cloud Connect al collegamento con la centralina tramite il Cloud Sicep. In alternativa, si può sempre registrare il software Sicep Cloud Connect riportando il codice OTP richiesto, sulla pagina iniziale del software alla voce **CLOUD** → **Non registrato** → **Immetti il codice OTP**.

6.3.13 Pagina Eventi

Configurazione - Eventi

Pagina di configurazione

Sinottico

Systema

Area

Utenti

Ingressi

ZoneAHD

DispositiviRF

IpCamera

Comandi

Comunicatore

Eventi

Controllo fumogeni

Programmi

Sonari

Storico

Carica in blocco

Salva in blocco

Salva storico

Trasmetti dati

Ricarica dati

Gestione Eventi

Mappa

Systema e emergenze

Alarmi aree

Innesco aree

Altri eventi aree

Eventi programmabili

Systema e emergenze

	Numeri	E-mail	Gestionale	App	Segn. locali	Uscite	Controllo motori
1 - Zone/Dispositivi disabilitati	...	...	...	-	-	...	...
2 - Sabotaggio disp. RF	...	...	...	-	sirena	...	...
3 - Sabotaggio centrale	...	...	...	-	sirena	...	...
4 - Incendio	...	...	...	Emergenze	sirena	...	...
5 - Panico	...	...	...	Emergenze	sirena	...	...
6 - Soccorso	...	...	...	Emergenze	...	...	...
7 - Batteria centrale	...	...	...	...	...	...	...
8 - Batteria disp. RF	...	...	...	...	...	...	...
9 - Assenza rete	...	...	...	...	...	...	...
10 - Malfunzionamento disp. RF	...	...	...	...	...	...	...
11 - Accensione RF	...	...	...	...	...	...	...
12 - Accensione GSM	...	...	...	...	...	...	...
13 - Coesione	...	...	...	Emergenze	...	...	...
14 - Password falsa	...	...	...	Emergenze	...	...	...
15 - Prova automatica	...	...	...	-	...	...	...
16 - Ignoranza rich. assistenza	...	...	...	-	...	...	...
17 - Assenza com. LAN/WIFI	...	...	...	-	...	...	...
18 - Manutenzione	...	...	...	-	...	...	...
19 - Assenza linea GSM	...	...	...	-	...	...	...
20 - Credito/scadenza SIM	...	...	...	-	...	...	...
21 - Allarme 24h	...	...	...	-	sirena	...	...
22 - Asportata	...	...	...	-	...	...	...
23 - Assenza conn. internet	...	...	...	-	...	...	...
24 - Fumogeni cartuccia scaduta	...	...	...	-	...	...	...
25 - Fumogeni cartuccia esaurita	...	...	...	-	...	...	...
26 - Malfunz. ipcamera	...	...	...	-	...	...	...

Alarmi aree

	Numeri	E-mail	Gestionale	App	Segn. locali	Uscite	Controllo motori
27 - Allarme Area 1 - Ins. Totale	...	...	...	Alarmi	sirena	...	...
28 - Allarme Area 2 - Ins. Totale	...	...	...	Alarmi	sirena	...	...
29 - Allarme Area 3 - Ins. Totale	...	...	...	Alarmi	sirena	...	...
30 - Allarme Area 4 - Ins. Totale	...	...	...	Alarmi	sirena	...	...
31 - Allarme Area 1 - Ins. Perimetrale	...	...	...	Alarmi	sirena	...	...
32 - Allarme Area 2 - Ins. Perimetrale	...	...	...	Alarmi	sirena	...	...
33 - Allarme Area 3 - Ins. Perimetrale	...	...	...	Alarmi	sirena	...	...
34 - Allarme Area 4 - Ins. Perimetrale	...	...	...	Alarmi	sirena	...	...
35 - Allarme Area 1 - Ins. Notte	...	...	...	Alarmi	sirena	...	...
36 - Allarme Area 2 - Ins. Notte	...	...	...	Alarmi	sirena	...	...

Per evento si intende qualsiasi variazione di uno degli stati logici esterni o interni alla centralina. Ciascun evento può provocare un'azione locale o generare una comunicazione verso destinatari esterni, con le informazioni inerenti all'evento stesso. Ogni evento può attivare l'azione programmata sia nella variazione da stato di riposo a stato di allarme (ALLARME), sia nella variazione da stato di allarme a stato di riposo (RIPRISTINO). Alcuni eventi non hanno il RIPRISTINO per l'attivazione dell'azione programmata.



Mappa

Questa mappa riporta l'elenco di tutti gli eventi suddivisi per categorie. A fianco di ogni evento vengono visualizzati i seguenti parametri:

SMS	I riferimenti dell'elenco destinatari per comunicazioni in SMS
E-Mail	I riferimenti dell'elenco destinatari per comunicazioni in E-Mail
Gestionale	Abilitazione e codice del Contact-ID da inviare in Centrale Operativa
APP	Categoria della notifica a cui è assegnato l'evento.
Segn. Locali	Segnalazioni acustiche locali: sirena interna e sirene radio
Uscite	Elenco delle uscite attivate dall'evento
Controllo Motori	Elenco dei controllo motori attivati dall'evento

Sistemi e emergenze, Allarmi aree, Inserimento aree, Altri eventi aree, Eventi programmabili.

Di seguito la descrizione delle configurazioni comuni a tutti i tipi di evento

Destinatari SMS/SQUILLO, 1 ... 8

Sceita degli utenti a cui inviare l'evento tramite SMS testo.

Default: Disabilitato



Destinatari SMS/SQUILLO, Invia anche Ripristino

Stabilisce se deve essere trasmesso anche l'evento di ripristino.

Default: Disabilitato



Destinatari E-Mail, 1 ... 8

Sceita degli utenti a cui inviare l'evento tramite e-mail

Default: Disabilitato

Destinatari E-Mail, Invia anche Ripristino

Stabilisce se deve essere trasmesso anche l'evento di ripristino.

Default: Disabilitato



Comunicazioni con Gestionale, Abilita

Permette di assegnare all'evento la trasmissione al destinatario "gestionale" che può avvenire anche con più vettori alternativi, se disponibili.

Comunicazioni con Gestionale, Codice CONTACT-ID

Assegna all'evento il codice Contact-ID da comunicare al gestionale della Centrale Operativa. Il codice Contact-ID può essere variato in conformità a quanto richiesto dalla centrale di ascolto.

Default: Vedi tabella



Comunicazioni con Gestionale, Invia anche Ripristino

Stabilisce se deve essere trasmesso anche l'evento di ripristino.

Default: Vedi tabella



Esempio di alcuni codici preimpostati:

Evento	Codice Contact-ID	Ripristino
Zone/Disp. disabil.	570	NO
Allarme A1-A4	130	NO
Ins/dis A1-A4	400	SI
Sabotaggio filari	144	SI
Tamper RS 485	341	NO
Sabotaggio disp. RF	383	NO
Tamper contenitore	137	SI
Incendio	110	NO
Panico	120	NO
Soccorso	101	NO
Batteria Centralina	302	SI
Batteria disp. RF	384	NO
Assenza rete	301	SI
Malfunzionamento disp. RF	380	SI
Perdita RS 485	333	NO
Accecamento RF	344	NO
Coercizione	121	NO
Password errata	461	NO
Chiave falsa	461	NO
Assenza linea telef.	350	NO
Intrusione da remoto	-	-
Prova Automatica	602	NO
Zone escluse	570	NO
Manutenzione	466	NO
Assenza linea GSM	353	SI
Credito-Scadenza SIM	350	NO
Allarme Zone 24H	150	SI
Apriporta	422	NO



Notifiche eventi APP, Categoria Notifica

Permette di assegnare all'evento una categoria di notifiche da utilizzare con Cloud Sicep.



Notifiche eventi APP, Invia anche Ripristino

Stabilisce se deve essere trasmesso anche l'evento di ripristino.

Default: Abilitato



Notifiche eventi APP, Suoneria di allarme

Abilitando questa funzione, la notifica sull'APP sarà prolungata e differente.

Default: Disabilitato



Segnalazioni locali, Sirena interna

Assegna all'evento l'attivazione della segnalazione locale della sirena interna.

Default: dipendente dall'evento



Segnalazioni locali, Cancella comunicazioni

L'evento cancella le comunicazioni in corso.

Default: Disabilitato



Segnalazioni locali, Sirene radio

Assegna all'evento l'attivazione delle segnalazioni delle sirene radio.

Default: Disabilitato

Segnalazioni locali, Suono sirene solo ad impianto inserito

Negli eventi di sistema attivi 24H, limita il suono delle sirene solo ad impianto inserito.

Default: Disabilitato

Uscite, Tipo comando su evento

Consente di scegliere il tipo di comando da effettuare sullo stato di allarme dell'evento:

Nessuna azione	
ON	Attivazione uscita
OFF	Disattivazione uscita
ON/OFF	Cambio di stato dell'uscita

Uscite, Tipo comando su ripristino

Consente di scegliere il tipo di comando da effettuare sullo stato di ripristino dell'evento. Alcuni eventi non avendo il ripristino, hanno questo parametro disabilitato.

Nessuna azione	
ON	Attivazione uscita
OFF	Disattivazione uscita
ON/OFF	Cambio di stato dell'uscita

Uscite, Uscita1..Uscita16

Uscite, Uscita On Board

Assegna alle uscite selezionate il tipo di comando dell'evento.

Default: Disabilitata

Controllo Motori, Tipo comando su evento

Consente di scegliere il tipo di comando da effettuare sullo stato di allarme dell'evento:

Nessun comando	
Apertura	Apertura tapparella, tenda ecc.
Chiusura	Chiusura tapparella, tenda ecc.
Apertura parziale	Apertura parziale tapparella, tenda ecc.

Controllo Motori, Tipo comando su ripristino

Consente di scegliere il tipo di comando da effettuare sullo stato di ripristino dell'evento. Alcuni eventi non avendo il ripristino, hanno questo parametro disabilitato.

Nessun comando	
Apertura	Apertura tapparella, tenda ecc.
Chiusura	Chiusura tapparella, tenda ecc.
Apertura parziale	Apertura parziale tapparella, tenda ecc.

Controllo Motori, Controllo Motori1 .. Controllo Motori8

Assegna ai "controllo motori" selezionati il tipo di comando dell'evento.

Default: Disabilitato

Configurazione Eventi Programmabili

Rispetto agli eventi generati in modo automatico dalle funzioni della centralina, questo tipo di evento generico può essere attivato da radiocomandi, tastiere o stati degli ingressi o dispositivi radio e può aiutare l'installatore a creare delle funzioni particolari per il cliente. I seguenti parametri sono stati aggiunti rispetto agli eventi descritti in precedenza:

Programmabile XX, Nome evento

Inserire una descrizione che sia attinente all'utilizzo dell'evento programmabile (massimo 18 caratteri, spazi inclusi).

Default: ---

Programmabile XX, Controllabile direttamente dall'utente

Se abilitata, questo evento programmabile sarà disponibile su Sicep.

Default: Disabilitato

6.3.14 Pagina Controllo dissuasori
Abilita programmazione

Onde evitare un'attivazione accidentale del dissuasore (fumogeno/nebbiogeno) durante la configurazione, questo flag se abilitato esclude questa possibilità, posizionando il dispositivo nella modalità di TEST.

Questa modalità è segnalata tramite il lampeggio del LED di colore BLU ed un beep periodico sulla sirena. Al termine della configurazione, l'installatore deve abilitare i dissuasori installati al funzionamento normale togliendo questo flag.

Durante la funzione di TEST (flag Abilitato), è possibile testare l'avvio dei dissuasori sapendo che al posto dell'attivazione del generatore di fumo, viene attivata la sirena per 5 secondi.

Default: Disabilitato

Control. dissuasoriX, Abilitato

Abilita / Disabilita il Controllo fumogeno selezionato. Se "Disabilitato" i dissuasori riferiti a questa pagina di configurazione non verranno attivati.

Default: Disabilitato

Control. dissuasoriX, Descrizione

È possibile assegnare un nome al Controllo fumogeno. Questo nome sarà quello riportato sulla App SICEP o MvsNET.

Default: Control. dissuasori1, Control. dissuasori2, ecc.

Control. dissuasoriX, Stato

Indica lo stato del sistema per l'attivazione dei dissuasori:

- "ATTENZIONE! Dispositivi attivi e pronti all'uso"
- "Modalità Test, dispositivi non attivi"

Fumogeni/nebbiogeni associati

Mostra l'elenco dei dispositivi radio registrati e consente di abilitare il flag per il controllo del singolo dissuasore. Con questa configurazione è possibile assegnare al controllo più dispositivi dissuasori che verranno attivati contemporaneamente.

A fianco di ciascun dissuasore viene riportato l'eventuale stato anomalo con l'indicazione di generatore di fumo esaurito nel caso sia stata attivata precedentemente o generatore di fumo scaduto nel caso sia trascorso un periodo di tempo superiore a quello indicato nella

data di scadenza del generatore di fumo.

Default: Disabilitati

Attivazione su allarme area con zona di conferma

Mostra l'elenco delle aree da associare all'attivazione dei dissuasori. È possibile selezionare una o più aree per ogni controllo. L'attivazione dei dissuasori associati, avviene se nel periodo di allarme dell'area o delle aree (tempo di allarme), viene allarmata la zona o il dispositivo di conferma.

Default: Disabilitate

Attivazione su allarme area con zona di conferma, Zona/dispositivo di conferma

È la zona o dispositivo che consente l'attivazione dei dissuasori associati al controllo. L'attivazione avviene solo se la zona o dispositivo passa da uno stato di riposo a quello di allarme. La zona o dispositivo può avere qualsiasi funzione (furto, incendio, 24H, tecnologico ecc.) e la sua variazione ha effetto soltanto se è presente un allarme su almeno un'area fra quelle selezionate.

Default: Nessuna selezione

Attivazione immediata, Zona/dispositivo di attivazione

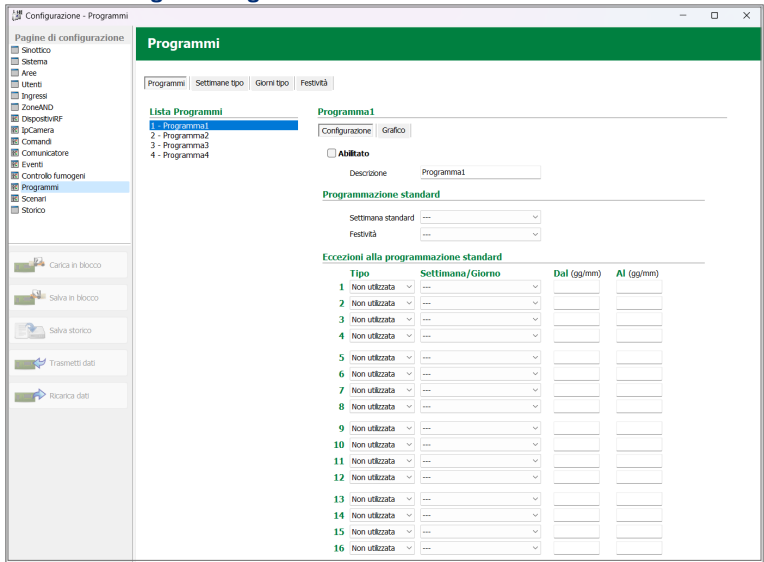
Consente di selezionare una zona o dispositivo per un'attivazione immediata dei dissuasori associati al controllo. Per evitare delle attivazioni indesiderate, la zona o il dispositivo viene filtrato in modo tale che solo 3 variazioni consecutive da uno stato di riposo ad uno stato di allarme in un periodo di tempo di 15 secondi, diano inizio alla procedura di attivazione dei dissuasori.

Nel caso in cui venga cablato un pulsante sulla zona per l'attivazione del controllo, il pulsante deve essere premuto ripetutamente per 3 volte entro 15 secondi.

Nel caso in cui si faccia uso di un sensore volumetrico da installare nell'ambiente, questo dovrà rivelare per 3 volte consecutive entro 15 secondi, una situazione di allarme.

Default: Nessuna selezione

6.3.15 **Pagina Programmi**



Programmi

Lista Programmi

Seleziona il programma da configurare 1 – 4.

Configurazione, Abilitato

Permette di abilitare/disabilitare il programma senza cancellarne la programmazione.

Default: Disabilitato

Configurazione, Descrizione

E' il campo dove è possibile impostare il nome del programma (19 caratteri massimi compresi gli spazi).

Programmazione Standard, Settimana Standard

Il programma selezionato seguirà la programmazione della "Settimana Tipo" assegnata alla settimana standard. E' possibile scegliere fra 4 "Settimane Tipo".

Default: ---

Programmazione Standard, Festività

E' possibile assegnare alle festività un "Giorno Tipo". In questo caso la festività si comporterà come il "Giorno Tipo" assegnato.

Default: ---

Eccezioni alla programmazione standard

E' possibile inserire delle eccezioni al comportamento standard del programmatore per determinati periodi dell'anno.

L'eccezione deve essere impostata programmando una data di inizio ed una data di fine e assegnando il comportamento del programma per questo periodo dell'anno riferito ad un "Giorno Tipo" o ad una "Settimana Tipo".

Grafico

Consente di visualizzare in forma grafica la programmazione effettuata. I giorni dell'anno vengono rappresentati con colori diversi secondo il seguente schema:
Selezionando con il mouse un giorno dell'anno, viene evidenziato nel pannello "informazioni giorno" la programmazione e gli orari del giorno stesso.

Colore	Descrizione
Grigio	Giorno non assegnato nel programma
Giallo	Settimana standard
Rosso	Festività
Verde	Eccezione settimanale
Blu	Eccezione giornaliera

Settimane tipo

Consente di configurare 4 modelli di "Settimana Tipo" distinguibili tramite una breve descrizione di 19 caratteri. Ogni giorno della settimana può essere riempita con un "Giorno Tipo" selezionato fra i 12 disponibili.

Giorni tipo

Il "Giorno Tipo" è la definizione minima impostabile nel programmatore annuale. Ogni giorno dispone di 4 fasce orarie di controllo; 2 per il disinserimento dell'area, l'abilitazione all'accesso di un utente o un comando e 2 per l'inserimento dell'area, la disabilitazione all'accesso di un utente o un comando.

Le caselle devono essere riempite inserendo l'ora ed il minuto del controllo separate dal carattere ":" (es. 08:00, 12:40 ecc.)

Festività

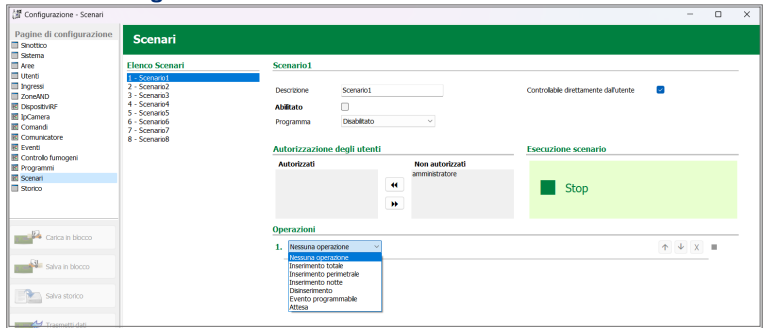
Sono riportate 12 caselle per le festività annuali fisse già precompilate e 12 caselle di festività variabili da compilare. In fase di configurazione, può essere assegnato un "Giorno Tipo" alle festività che consenta di stabilire il comportamento del programmatore orario per questo giorno.

Esempio Configurazione di un programma

Si consiglia di procedere nel seguente modo:

1. *Compilare i "Giorni Tipo" necessari. Ad esempio per la funzione di Inserimento/Disinserimento di un'area, si possono predisporre 3 "Giorni Tipo": giorno feriale, giorno prefestivo, giorno festivo con gli orari di Inserimento/Disinserimento dell'area desiderati. La stessa procedura può essere ripetuta se occorre differenziare questi orari per un periodo dell'anno, ad esempio nel periodo estivo.*
2. *Compilare la o le "Settimane Tipo" con i "Giorni Tipo" precedentemente compilati.*
3. *Abilitare il programma*
4. *Riempire il campo Descrizione (opzionale)*
5. *Assegnare alla settimana standard la "Settimana Tipo" precedentemente compilata.*
6. *Assegnare un "Giorno Tipo" per le festività annuali.*
7. *Riempire le Eccezioni alla programmazione standard se necessario (opzionale).*

6.3.16 Pagina Scenari.



Elenco Scenari

Seleziona lo scenario da configurare.

Descrizione

E' il campo dove è possibile impostare il nome allo scenario (19 caratteri massimi compresi gli spazi)

Abilitato

Permette di abilitare/disabilitare lo scenario senza cancellarne la programmazione.

Default: Disabilitato

Programma

Permette di assegnare allo scenario un programma automatico ad orari e giorni stabiliti nella pagina Programmatore.

Valori programmabili: Disabilitato / Programma1 ... Programma4. Default: Disabilitato

Controllabile direttamente da utente

Se abilitato, questo scenario sarà disponibile su App SICEP e tastiere touch.

Default: Disabilitato

Autorizzazione degli utenti

Tramite i pulsanti   è possibile decidere quali utenti sono abilitati all'attivazione dello scenario in questione.

Esecuzione scenario

Riquadro informativo riportante lo stato attuale dello scenario.

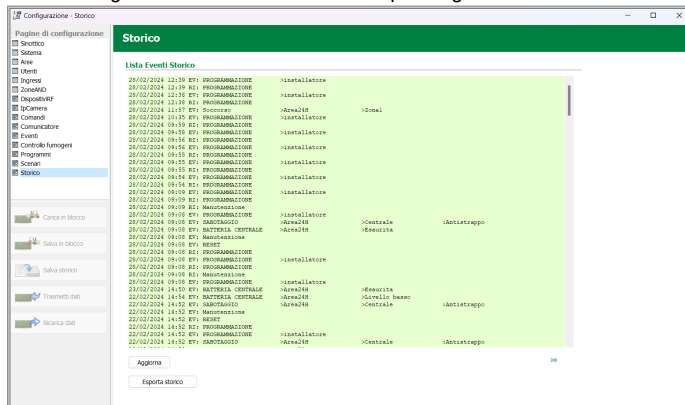
Operazioni

Programmazione delle operazioni da eseguire con lo scenario. È possibile scegliere tra:

Nessuna operazione	Termina l'esecuzione dello scenario
Inserimento totale	Inserimento totale delle aree selezionate
Inserimento perimetrale	Inserimento perimetrale delle aree selezionate
Inserimento notte	Inserimento notte delle aree selezionate
Evento programmabile	Esegue l'evento programmabile selezionato
Attesa	Attende i secondi programmati

6.3.17 Pagina Storico

Pagina di sola lettura in cui sono riportati gli ultimi 1024 eventi della centralina.



Nella Lista Eventi Storico sono riportate le seguenti informazioni:

- Data (giorno, mese, anno)
- Orario Evento (ore, minuti)
- Tipo di evento (EV=evento, RI=ripristino)
- Categoria evento
- Sorgente dell'evento o utente
- Zona, Dispositivo, Utente sorgente evento
- Dettaglio dell'evento

Pulsante Aggiorna / Stop

Permette di effettuare un aggiornamento dell'elenco degli eventi.

6.4 Impostazioni Cloud Sicep

La centralina DOGMA è già predisposta per una connessione al server Cloud Sicep. Una volta installata e collegata in rete, tramite interfaccia LAN o Wi-Fi o LTE/GPRS, si dovrà semplicemente attivare la connessione al Cloud abilitando il FLAG nella pagina *Comunicatore* → *Cloud* → *Impostazioni Cloud*. Se la connessione è avvenuta con successo, visualizzeremo lo Stato della connessione in VERDE con la dicitura "Connesso". Per poter registrare Sicep o Sicep Cloud Connect sulla centralina, si dovrà richiedere il codice OTP mediante il pulsante "Richiedi codice" e successivamente copiare il codice sull'applicazione.

Il codice OTP formato da 8 cifre, consente la registrazione dell'APP in modo sicuro in quanto ha una scadenza di 120" dopodiché non è più utilizzabile e deve essere effettuata una nuova richiesta.

7. Operazioni speciali

7.1 Riprogrammare la centralina ai valori di default (impostazioni di fabbrica)

Per eseguire il default di tutti i parametri procedere come segue:

- Porre la centralina in manutenzione e aprire il contenitore;
- Premere contemporaneamente i pulsanti RESET e TEST;
- Rilasciare il RESET e continuare a tenere premuto il TEST a lungo finché il led blu non smette di lampeggiare.
- Una volta effettuato il default, prima di effettuare una nuova connessione, attendere il reset della centralina (10 secondi circa).
- A questo punto per collegarsi con Sicep Cloud Connect tramite TCP/IP utilizzare i seguenti parametri:
 - Codice: 100
 - Utente: installatore
 - Password: installatore
 - Vettore: TCP/IP statico
 - Indirizzo IP: dogma

7.2 Aggiornamento firmware

L'aggiornamento del firmware della centralina può essere effettuato sia localmente tramite connessione USB, che da remoto tramite connessione a rete LAN, Wi-Fi o LTE/GPRS.

Per effettuare l'aggiornamento procedere come segue:

- Lanciare il software Sicep Cloud Connect
- Inserire il codice della centralina nell'apposito campo
- Digitare il nome utente e password (solo l'utente Installatore o Amministratore possono accedere a questa funzione).
- Selezionare il Vettore di Comunicazione: seriale diretta (USB), TCP/IP statico/dinamico (LAN, Wi-Fi), TCP/IP in attesa (LTE/GPRS), Cloud.
- Selezionare: porta COM (USB), indirizzo IP/ Hostname (altri)
- Premere il pulsante Upgrade Firmware.
- Selezionare il NOMEFILE.UPG
- Premere il pulsante "Apri".

Al termine della procedura chiudere il programma ed attendere il termine dell'aggiornamento segnalato dal lampeggio del led rosso batteria.

7.3 Installazione dei driver USB

Sistemi 2000 / XP

- Scaricare dal sito Sicep nella pagina Download il file contenente i driver USB.
- Estrarre il contenuto del file ZIP in una cartella.
- Collegare la periferica al PC tramite il cavo USB.
- Appena il dispositivo viene riconosciuto viene chiesto un percorso per la ricerca del driver.
- Scegliere la cartella contenente di driver precedentemente estratti cliccando su Sfoglia.

NOTA. *Se il sistema operativo notifica l'avviso che il driver non ha superato il testing del programma WindowsLogo, ignorare e proseguire con l'installazione.*

Una volta terminata l'installazione, questa procedura viene richiesta una seconda volta per l'installazione di un secondo file. Procedere allo stesso modo.

Terminata l'installazione è utile conoscere il numero della porta COM emulata assegnata al dispositivo. Il programma Sicep Cloud Connect può mostrare in un apposito elenco le porte COM effettivamente presenti; in ogni caso per conoscere la porta COM assegnata procedere come segue:

- Il dispositivo deve essere collegato al PC;
- Cliccare su: *Start → Impostazioni → Pannello di controllo → Sistema → Hardware*

→ *Gestione periferiche* → *porte COM* e vedere il numero assegnato a quella denominata "USB CDC serial port emulation".

Sistemi Windows Vista / 7

- Scaricare dal sito Sicep nella pagina Download il file contenente i driver USB.
- Estrarre il contenuto del file ZIP in una cartella.
- Collegare la periferica al PC tramite il cavo USB.
- Il sistema tenterà invano l'installazione riportando l'errore "Installazione del driver del dispositivo non riuscita".
- A questo punto installare il driver procedendo come segue:
- Cliccare su: *Avvio* → *Pannello di controllo* → *Hardware e suoni* → *Gestione dispositivi* → *Altri dispositivi*; *USB serial* → *Aggiorna driver* → *Cerca il software del drive nel computer* → *Specificare il percorso* → *Sfoggia* → *Computer* → *Cartella contenente i Driver estratti* → *Driver Vista/Win7* → *Ok* → *Avanti*.
- Comparirà il messaggio di avvertimento "Impossibile verificare l'autore del software di questo driver"; selezionare *Installa il software del driver*.

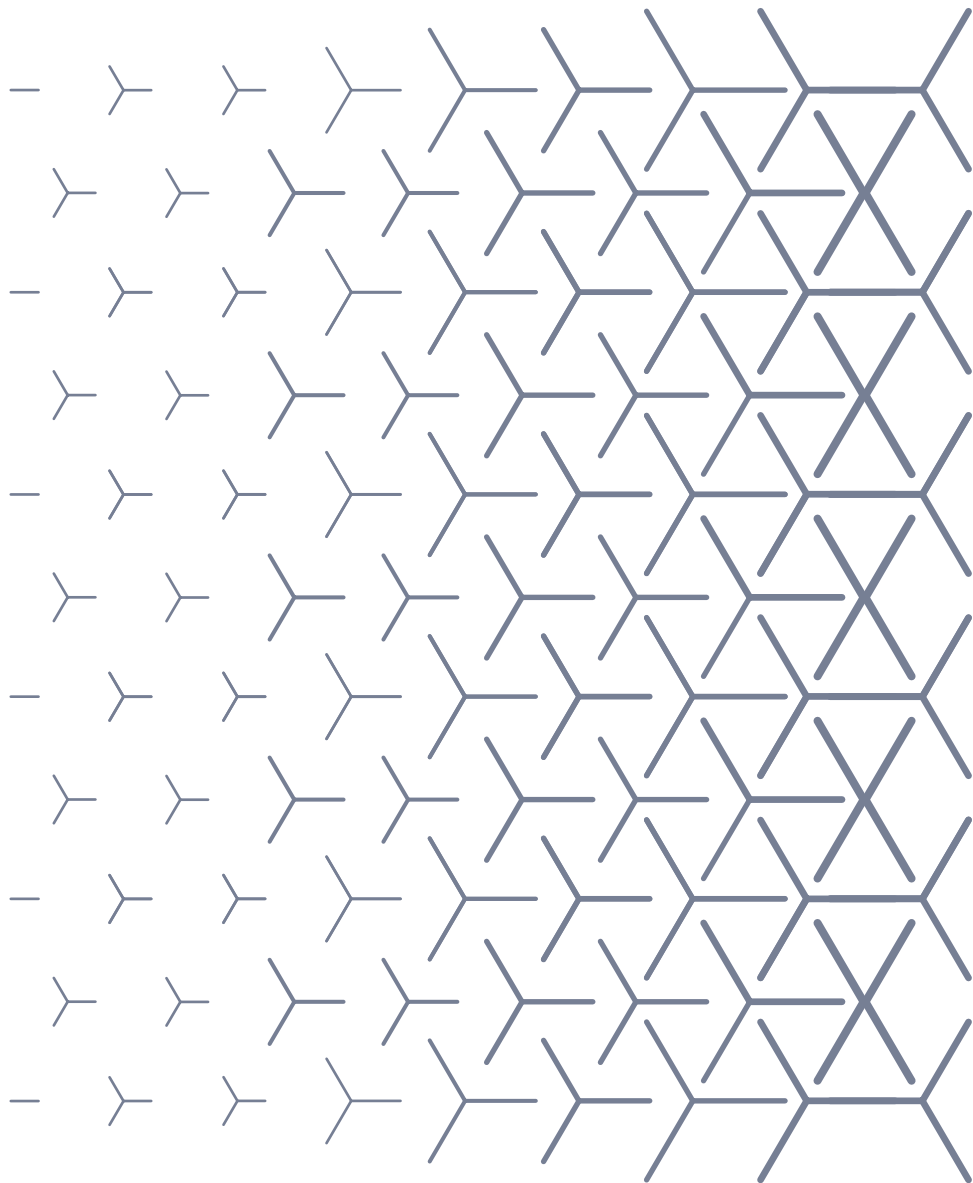
Sistema Windows 8/10/11

L'installazione è simile a quella per Windows 7. Nel caso che il sistema rifiuti l'installazione perché il driver non risulta certificato occorre rimuovere questa protezione procedendo come segue.

- Premere contemporaneamente i tasti *Windows + R* ; si aprirà una finestra di comando (*Esegui*).
- Scrivere nella finestra di comando *shutdown.exe /r /o /f /t 00*
- Premere OK.
- Il sistema si riavvierà.
- All'avvio selezionare la modalità *Risoluzione dei problemi*.
- Selezionare *Opzioni Avanzate*. *Selezionare Impostazioni di avvio* → *Riavvia*.
- Il computer verrà riavviato con la schermata delle opzioni avanzate di avvio.
- Selezionare *Disabilita impostazione firma driver* (scelta n. 7).
- A questo punto installare nuovamente il driver. Il sistema notificherà comunque che il driver non è certificato, ma questa volta si può fare proseguire l'installazione.

GARANZIA

- La garanzia sui prodotti elettrici e/o elettronici di produzione SICEP è di 24 mesi dalla data di acquisto ovvero dalla data indicata dalla fattura.
- La presente garanzia non si estende ai software prodotti e/o commercializzati da SICEP, né copre gli eventuali danni di qualsiasi natura che possono derivare dal loro uso ed utilizzo.
- Qualora i prodotti o parti di essi risultano difettosi per qualità dei materiali o per anomalie di costruzione, la garanzia è limitata alla loro sostituzione. Sono comprese nella garanzia suddetta le prestazioni di manodopera necessarie alle riparazioni.
- Nel caso in cui l'apparato difettoso risulti mancante di una o più parti, verrà riparato e restituito senza integrare le stesse, salvo esplicita richiesta in tal senso.
- La presente garanzia non si estende alle avarie dipendenti dall'usura naturale dei prodotti o di parti di essi (ivi incluse le batterie).
- La presente garanzia non copre i danni causati da negligenza ed incuria, da sinistro, dall'uso improprio dei prodotti, o di parti di essi, e/o dei software; così i danni causati da agenti atmosferici, da esposizione dei medesimi prodotti, o parti di essi, e/o dei software a condizioni ambientali improprie, ivi inclusi i danni direttamente o indirettamente provocati da temperatura eccessiva, umidità, stress fisici od elettrici, mancanza o fluttuazione di energia elettrica, fulmini, elettricità statica, incendi, inondazioni o allagamenti, e da quanto non imputabile alla diretta responsabilità di SICEP.
- Sono esclusi dalla copertura della garanzia anche i danni imputabili a cattiva od erronea installazione – ossia installazione non conforme alle relative istruzioni od in assenza di esse non effettuata a regola d'arte – per errata o carente manutenzione secondo quanto indicato nelle relative istruzioni d'uso o comunque secondo l'usuale manutenzione, per operazioni o uso improprio o errato, per trascuratezza o incapacità d'uso e comunque per cause di ogni genere non dipendenti da SICEP.
- Sono esclusi dalla copertura della presente garanzia tutti quei danni prodotti da difetti originari di componenti o di parti del prodotto assemblate, comunque certificati, che non sia possibile in alcun modo rilevare prima, durante e dopo la realizzazione del prodotto finale da parte di SICEP, secondo le normali e consuete procedure di controllo e di verifica dei componenti o di prodotti e parti di essi esterni; altresì, i danni o i difetti imputabili a riparazioni ed a manutenzioni, così come a sostituzioni o modificazioni, effettuate da soggetti terzi, non autorizzati direttamente dal produttore, in ogni caso da altri con prodotti, o parti di essi, e/o software, diversi, non originali, non conformi e quindi non garantiti, non certificati approvati ed autorizzati da SICEP.
- In ogni caso non sono coperti dalla garanzia i danni ed i difetti che risultino dall'utilizzo, non preventivamente ed espressamente autorizzato da SICEP, di ricambi ed accessori non compatibili, non originali, non conformi, non certificati ed approvati dal produttore medesimo, nonché tutti quei danni imputabili a qualsiasi modifica del prodotto o di parti di essi e/o del software, che non sia stata, in alcun modo, assentita dal produttore; o, comunque, dovuti a cause di forza maggiore e/o caso fortuito.
- Il materiale da riparare deve essere fatto pervenire in porto franco a SICEP accompagnato dal "Modulo di richiesta riparazione" compilato in ogni sua parte.
- SICEP si riserva il diritto di apportare modifiche alle condizioni di garanzia sopra elencate, senza alcun obbligo di preavviso. Saranno, in ogni caso, valide le condizioni vigenti al momento dell'acquisto del prodotto elettrico e/o elettronico di produzione SICEP.



<http://www.sicep.it>
e-mail: sicep@sicep.it

SICEP S.r.l.
Via Calabria, 14
50052 Certaldo (FI) - ITALY
Tel. 0571 664 166 r.a.
Fax 0571 652 285

