

## **Guardian: Descrizione tecnica**

***Release: 1.4 – 24 giugno 2010***

***Autore: Andrea Gualducci***

### ***Modifiche***

***1.0 → 1.1***

- Aggiunta capitolo Topologia

***1.1 → 1.2***

- Aggiunta descrizione popup-video sul client

***1.2 → 1.3***

- Aggiunti Report Parametrici
- Aggiunto backup ContactID

***1.3 → 1.4***

- Estensione Building automation

## SOMMARIO

Guardian: Descrizione tecnica.....	1
Introduzione.....	3
Portabilità.....	3
Modularità.....	3
Java.....	3
Grafica avanzata.....	3
Diagnostica interna.....	3
Integrazione video.....	3
Architettura del server.....	4
PSI – Sintesi dati e Distribuzione.....	4
CHI – Server di accesso.....	4
TAU – I driver.....	4
Lambda: il client.....	7
Le parti del layout.....	7
Il menu generale.....	11
Integrazione eventi-video: i popup.....	15
Integrazione regolazione meccanica: i gauge.....	16
Topologia.....	17
Installazione a macchina singola.....	17
Installazione in backup.....	17
Installazione asimmetrica (Guardian MS).....	18

## Introduzione

Il supervisore Guardian rappresenta l'ultima evoluzione dei supervisori per *building security* proposti e sviluppati da MetaRec s.r.l.

### Portabilità

Esso si basa sulla architettura JaMIX™, un insieme di moduli scritti in Java che possono essere eseguiti su qualunque sistema operativo (Windows, Linux, Unix, Macintosh) e possono essere configurati per svolgere qualunque compito di supervisione.

### Modularità

I moduli che compongono Guardian possono essere eseguiti tutti su una singola macchina, come su macchine differenti a seconda delle esigenze, permettendo così di calibrare e distribuire nel miglior modo possibile il carico computazionale che le macchine devono sopportare.

### Java

Questo supervisore trae vantaggio dal linguaggio Java in cui è interamente scritto il quale permette di ottenere codice molto più sicuro e pulito, con minore probabilità di errori di programmazione e maggiore facilità di gestione dei progetti.

### Grafica avanzata

Guardian permette di gestire anche una interfaccia grafica animata che visualizza le mappe degli ambienti controllati e da queste è possibile gestire integralmente tutti i sensori anti-intrusione, antincendio e antiallagamento dislocati.

Guardian permette l'utilizzo delle mappe come interfaccia di controllo fondamentale: navigando tra le mappe, è possibile tenere sotto monitoraggio visivo tutti i sensori presenti negli edifici controllati e agire su di essi per riconoscere gli allarmi, ripristinarli, o per compiere verifiche.

Guardian inoltre gestisce in modo più pulito le azioni da compiere sulle centrali: queste sono raggruppate in uno speciale sinottico grafico che mostra con simboli di facile ed intuitiva interpretazione problemi di disconnessione, particolari stati di verifica e controllo in cui esse possono trovarsi.

### Diagnostica interna

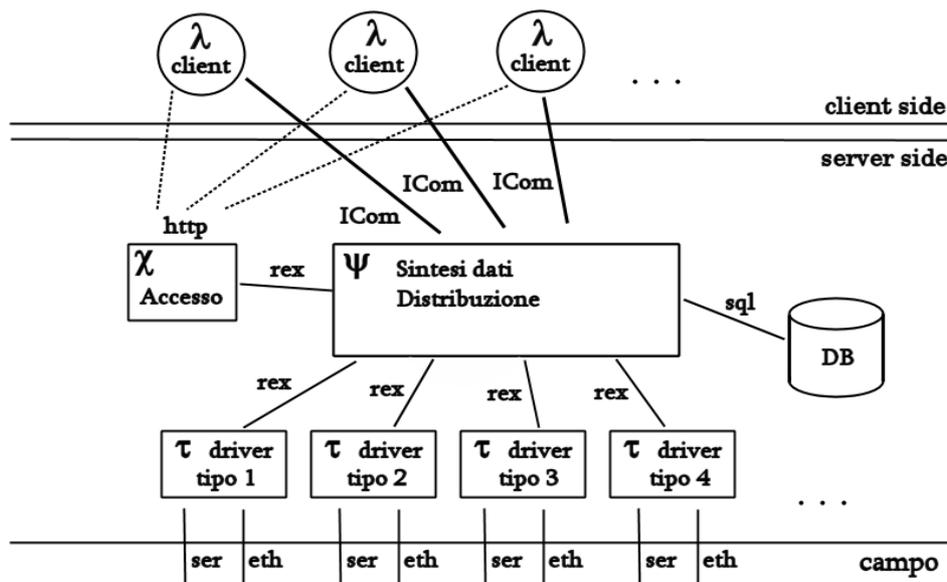
Guardian è inoltre dotato di un particolare sistema software che gli permette di tenere sotto controllo tutti i moduli di cui è composto: se uno di questi moduli per qualunque motivo smette di funzionare o si trova in uno stato non risolvibile, il sistema provvede a rimpiazzarlo e in pochi secondi viene ripristinata la funzionalità originale.

### Integrazione video

Associando i sensori alle telecamere dislocate sull'impianto, Guardian permette di corredare gli eventi di allarme con immagini contestuali, attraverso un sistema di popup. Il video dell'evento può essere visualizzato in modo automatico o richiamato dall'operatore su eventi presenti, eventi storici o dalle mappe.

## Architettura del server

Il server di Guardian si compone di diversi moduli, ciascuno dei quali costituisce un processo separato del sistema operativo. Poiché tutti i moduli sono applicativi java, tutti questi processi appaiono come macchine virtuali java (JVM). Nella seguente immagine viene rappresentato uno schema a blocchi dei moduli



### PSI – Sintesi dati e Distribuzione

Il modulo fondamentale che ospita tutti le unità di sintesi dei dati. Fondamentalmente si tratta di un RTDB (Real-Time Data Base), ma con una struttura di scambio dati basata sul push delle variazioni, caratteristica che lo rende notevolmente efficiente e capace di pesanti elaborazioni con minimo consumo di CPU.

Le unità di sintesi dei dati sono delle singole classi java che implementano sostanzialmente una tabella relazionale e possono essere programmate per svolgere qualunque compito ed interazione. Il linker dinamico di java fornisce l'ambiente ideale per questo tipo di approccio.

Questo modulo si connette a tutti gli altri moduli interni tramite il protocollo ReX (Record eXchange), ai moduli client tramite il protocollo InterCOM (abb. ICom) e ad un database relazionale tramite JDBC.

Per dettagli sui protocolli interni, si rimanda agli allegati.

### CHI – Server di accesso

Fondamentalmente si tratta di un WebServer ed ha il compito fondamentale di far partire e tenere sotto controllo tutti gli altri moduli del server e di fornire la diagnostica interna.

Verso i client si comporta come un server di accesso, validando le credenziali dell'utente e rimandando il collegamento dati al server di distribuzione più appropriato.

Tramite questo server viene gestita l'anagrafica utenti del sistema.

### TAU – I driver

Per ogni tipologia (protocollo) di dispositivo di campo configurato su Guardian, viene fatto partire un driver che gestirà tutti i dispositivi di quel tipo, fornendo una interfaccia fra la sintesi dei dati ed il campo.

Tutti i driver di Guardian possono aprire canali seriali (COM) o ethernet (TCP o UDP) di comunicazione verso i dispositivi controllati, che si possono quindi remotizzare compatibilmente con le impostazioni di routing della rete in uso.

Viene fornita di seguito una lista dei driver a corredo di Guardian, relativa alla data del presente documento.

#### **Notifier AM2020**

Vecchia centrale antincendio di Notifier, da tempo non più prodotta e anche la sua supervisione è in disuso (sostituita generalmente con AM6000). Questo è l'unico driver JNI di Guardian e ha una limitazione strutturale di una centrale per driver. La supervisione è comunque completa. La centrale può dare problemi su riconnessione che rendono necessario il riavvio della stessa.

#### **Notifier AM6000-AM2000**

Centrale antincendio estremamente pratica, con un ottimo protocollo di interfacciamento che è una semplificazione del CEI-ABI. Supervisione completa, ma priva di gestione anagrafiche, effettuata su SIB600 (richiesta). Non è prevista una gestione delle aree per centrali antincendio

#### **Boselli CP100**

Centrale antintrusione. Antica centrale, una delle prime con protocollo APLEX. E' l'antenato della Hesa-Metro. Funzionalità identiche al driver per Hesa-Metro. Nessuna gestione aree. Gestione anagrafica molto limitata: anagrafica codici solo in lettura.

#### **Hesa Metro**

Centrale antintrusione. Di fatti lo stesso driver della Boselli CP100. La centrale è fisicamente migliore e la supervisione è migliore, ma le funzionalità sono identiche.

#### **Hesa Primato e Primato30**

Centrale antintrusione. Sempre protocollo APLEX, ma con estensione a 200 punti invece che 100. Può essere utilizzata in modalità con o senza aree. Gestione anagrafica molto più avanzata rispetto al driver Hesa-Metro. Il driver inoltre accetta anche la versione Primato 30, ultima evoluzione del firmware da Hesa. La supervisione è ottimale per questa centrale.

#### **Hesa SigNET**

Centrale antintrusione. Dispositivo completamente rivisto e riprogettato rispetto alle Metro e Primato.

La supervisione di questa centrale viene fatta direttamente tramite ethernet sulla centrale, senza il bisogno di passare attraverso un serial-hub, caratteristica che rende enormemente più veloci tutte le operazioni. Tuttavia il protocollo di trasporto è UDP, non TCP, quindi particolare attenzione al routing.

Alla data del presente documento le carenze del protocollo obbligano ancora ad una definizione manuale delle associazioni area-sensore.

#### **Bosch BZ500**

Centrale antintrusione. Protocollo UAZ2000 di Bosch. Ha una gestione degli stati molto particolare, tanto che tutti i sensori vengono esposti sia come sensori di allarme che come tecnologici dal driver.

La gestione anagrafiche si limita alla lista punti.

#### **Bosch DIVAR**

Server video. Driver di diagnostica per video server DIVAR. Non riporta il video, ma tiene solo sotto controllo il videosever comunicando situazioni limite, come perdita telecamera, riempimento disco, ecc.

#### **GE-Interlogix CD150**

Centrale antintrusione. Supervisione effettuabile tramite modulo apposito di Aritech MPI232 (fuori produzione) oppure tramite modulo della SIDES CDP10. La supervisione tramite modulo SIDES è completa, fornisce tutte le anagrafiche ed è ottimale.

La gestione anagrafiche comprende la lista punti, la lista aree, la lista utenti.

Alto livello di affidabilità.

#### **GE-Interlogix Master**

Centrale antintrusione. Protocollo molto avanzato, gestione centrale molto semplice ed efficace. Il modulo di comunicazione permette una gestione in multidrop su RS485.

#### **GE-Interlogix FP2000**

Centrale antincendio. Protocollo molto avanzato, gestione centrale completa, con 8 tipi di anagrafica. La centrale può essere gestita direttamente o in relay collegandosi ai moduli concentratori, caso in cui può essere interfacciata l'intera rete ARCNET con una sola seriale.

#### **GE-Interlogix CSx75**

Centrale antintrusione di piccolo-medio taglio e dal costo contenuto.

#### **Honeywell Galaxy**

Centrale antintrusione. Per nuovo e vecchio firmware. Buona supervisione con gestione anagrafiche. Tutte le notifiche del protocollo SIA devono essere attivate sulla centrale e il livello deve essere posto a 3.

Le centrali gestite sono sia le classic (60, 504 et al.), sia le G2 e G3 che le nuove Dimension per le quali sono implementati anche la storicizzazione degli accessi e gli allarmi per accessi rifiutati.

#### **CIAS SA2ISI**

Centrale antintrusione con protocollo R3, tramite scheda SA3COM. La limitazione dell'allineamento fornita dalla centrale rende tale supervisione poco precisa e da evitare dove possibile. Attenzione sia alla scheda SA3COM (deve essere la versione giusta) e ad alcuni moduli interni prodotti da CIAS senza compatibilità.

#### **Raychem TTDM**

Centrale antiallagamento. Nelle versioni TTDM, TTDM Plus.

La gestione dell'evento associa un punto di allarme per ogni range (configurabile) sul cavo sensore. Nel caso della TTDM+ è necessario configurare la centrale in lingua inglese e lasciare il pannello nella schermata principale.

#### **Advantech Adam5000**

Modulo di IO di rete. Permette di associare la gestione degli IO (input e relé) a situazioni complesse di allarme/inserimento aree/sensori.

#### **Advantech PCI1762**

Modulo di IO scheda interna. Permette di associare la gestione degli IO (input e relé) a situazioni complesse di allarme/inserimento aree/sensori.

#### **Trend IQ3**

Modulo di regolazione meccanica (building automation) di Trend (gruppo Honeywell). Interfacciamento XML agli elementi sWitch, Knob, digital Input, Analog input, Sensor, Driver. Permette di scrivere valori su K e W.

#### **STS-Elettronica FD68**

Centrali di piccolo taglio, antintrusione e antincendio. Gestione completa. Possibilità di interfacciamento diretto, oppure off-line tramite modem con chiamate in uscita o in entrata da centrale.

#### **ContactID**

Per Ademco 685 o altri ricevitori ContactID, non è un driver autonomo: recupera informazioni che gli altri driver useranno come backup o come integrazione dati.

#### **MC55**

Driver di gestione modem con protocollo AT esteso (MC55) utilizzato per l'invio di SMS, collegabili agli allarmi, tramite apposito sottosistema di Guardian.

#### **Δ-VID**

Driver di ingresso video. Può acquisire direttamente telecamere BNC, USB oppure interfacciare video server o altri moduli Δ-VID. Il video viene riportato all'interno di Guardian permettendo una gestione combinata video-allarmi.

## Lambda: il client

Il client di Guardian viene distribuito senza licenze e per una installazione di Guardian può essere installato un numero di client senza limitazioni.

Si tratta di client non specializzati, che recuperano cioè dal server tutta l'interfaccia operativa e tutte le funzionalità che forniscono.

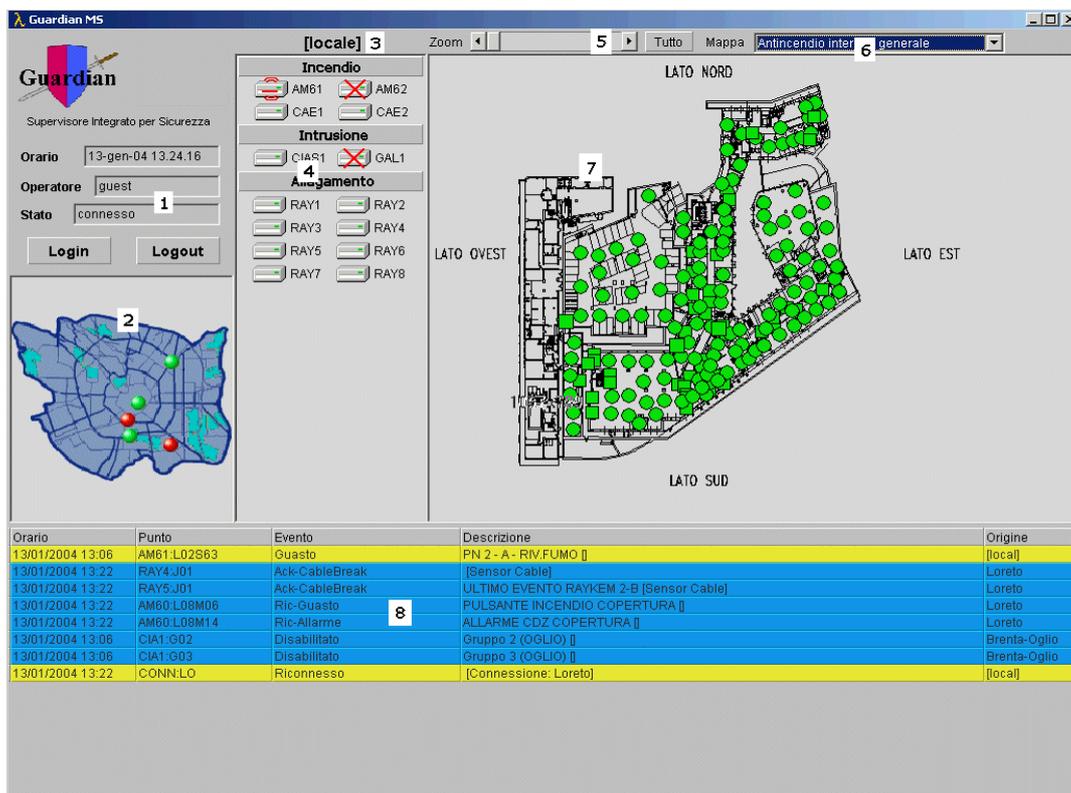
Una installazione di Guardian viene quindi configurata e programmata interamente sul server.

I client possono essere ospitati su pagine HTML oppure funzionare come applicazioni autonome. Nel primo caso si dovrà avere l'accortezza anche di preparare alcune pagine web ospitanti, possibilmente integrate in un contesto più ampio.

Il disegno della interfaccia si basa su speciali files, gli LNI, che rendono particolarmente rapido l'adattamento del client alle esigenze del cliente. Per questo motivo ogni installazione di Guardian ha un layout differente con funzionalità differenti.

Nella descrizione seguente verranno utilizzate immagini relative ad una installazione MS di Guardian, cioè della versione MultiSite in cui vari server autonomi e limitati a specifici siti (edifici) vengono raccolti da un server centrale con layout differente, in una architettura NON simmetrica.

## Le parti del layout



Orario	Punto	Evento	Descrizione	Origine
13/01/2004 13:06	AM61.L02S63	Guasto	PN 2 - A - RIV.FUMO [ ]	[local]
13/01/2004 13:22	RAY4.J01	Ack-CableBreak	[Sensor Cable]	Loreto
13/01/2004 13:22	RAY5.J01	Ack-CableBreak	ULTIMO EVENTO RAY/EM 2-B [Sensor Cable]	Loreto
13/01/2004 13:22	AM60.L09M06	Ric-Guasto	PULSANTE INCENDIO COPERTURA [ ]	Loreto
13/01/2004 13:22	AM60.L09M14	Ric-Allarme	ALLARME CDZ COPERTURA [ ]	Loreto
13/01/2004 13:06	CIA1.G02	Disabilitato	Gruppo 2 (OGLIO) [ ]	Birenta-Oglio
13/01/2004 13:06	CIA1.G03	Disabilitato	Gruppo 3 (OGLIO) [ ]	Birenta-Oglio
13/01/2004 13:22	CONNLO	Riconnesso	[Connessione: Loreto]	[local]

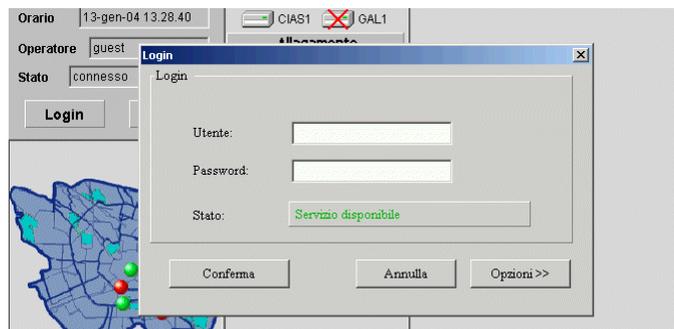
### 1 – Informativa sulla connessione

Una speciale area sempre presente, anche se con diversa disposizione e grafica delle parti, visualizza poche fondamentali informazioni sulla connessione attuale. Viene indicato l'orario del server (a cui tutti gli orari degli eventi fanno riferimento), l'utente attualmente connesso e lo stato di connessione.

Fanno parte dell'area anche due pulsanti.

Il pulsante di **Login**, apre una finestra di dialogo in cui l'operatore inserisce il proprio nome utente e password e tramite la quale può opzionalmente cambiare la propria password.

Il pulsante di **Logout**, tramite il quale un operatore può terminare la propria sessione.



Nello schema di autenticazione di Guardian esiste sempre un utente connesso, che di solito è l'utente anonimo 'guest'. Tale utente può vedere gli allarmi e le mappe, ma non può riconoscerli o effettuare alcun'altra operazione. Quando un utente si collega, in base alla sua identificazione gli vengono forniti dei permessi (sulle operazioni o sulla visibilità) e tutte le operazioni effettuate vengono registrate a suo nome. Per questo motivo se un operatore lascia la propria postazione, prima che un altro operatore effettui il login, è bene che effettui il logout, per tornare all'operatore di base 'guest' ed evitare di prendere la responsabilità di operazioni effettuate in sua assenza.

## 2 – Mappa cumulativa

Una mappa raramente presente nelle versioni non MS, che può visualizzare una città, regione o l'intero stato, fornisce informazioni cumulative di allarme in sistemi distribuiti su ampia area geografica.

Ha il solo scopo di fornire un colpo d'occhio sulla situazione globale indicando quali siti hanno bisogno di attenzione. Nella versione MS di Guardian questa mappa è sempre presente e permette il passaggio contestuale fra i server controllati.

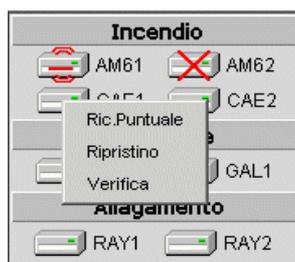
## 3 – Indicatore di contesto (solo MS)

Indicatore del sito correntemente visualizzato. Ha senso solo in una architettura asimmetrica come MS.

## 4 – Lista centrali

Questo elemento è fondamentale e sempre presente.

Raccoglie tutti i dispositivi di campo controllati (centrali), in una struttura gerarchica organizzandoli per gruppo. Nella configurazione di Guardian sono associabili vari livelli di gruppo ad una centrale che a seconda delle preferenze possono riguardare la tipologia della centrale, la zona nella quale si trovano o una organizzazione interna del cliente. Tramite questa lista possono essere gestite le centrali: cliccando su una di esse si aprirà infatti il menu di centrale



Questo menu varia fortemente da centrale a centrale e di solito contiene alcuni comandi globali, quelli da effettuare direttamente sulla centrale, più l'apertura di alcune tabelle di gestione che di solito riguardano la lista delle aree, la lista dei codici e la lista delle zone. In alcuni casi, per le centrali che lo consentono, sono presenti anche i pannelli di gestione delle uscite.

Come per tutte le altre operazioni in Guardian, anche per queste voci sono associabili dei livelli di accessibilità che inibiscono le funzionalità per operatori non autorizzati a quella specifica operazione.

La lista centrali inoltre riporta alcune fondamentali informazioni sullo stato della centrale, tramite semplici icone

- Centrale disconnessa (o non raggiungibile)
- Centrale in allarme
- Centrale in verifica (allineamento)
- Centrale in manutenzione
- Centrale occupata ((BUSY)
- Sospensione manuale della connessione

## 5 – Controllo ZOOM della mappa

Questo elemento è presente solo se si utilizzano mappe vettoriali, cioè convertite direttamente da disegni CAD, per le quali è sensato ingrandire o rimpicciolire l'immagine per identificare i dettagli con maggiore precisione. Nel caso di mappe bitmap, l'utilizzo di questo controllo è sconsigliato per l'antiestetica perdita di definizione che ne consegue.

## 6 – Selettore di mappa

Indica sempre la mappa attualmente visualizzata e permette di passare ad altre mappe.

E' uno strumento non indispensabile, poiché nelle mappe possono essere inseriti elementi grafici di navigazione.

## 7 – Mappe

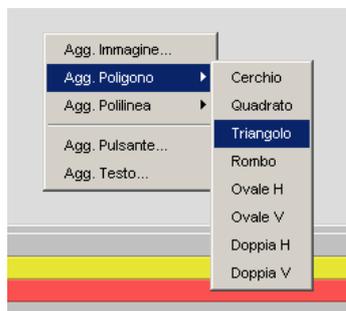
Le mappe di Guardian possono essere di due tipi, vettoriali o bitmap, utilizzabili anche in modo eterogeneo.

All'interno delle mappe vengono configurati alcuni elementi grafici di seguito elencati

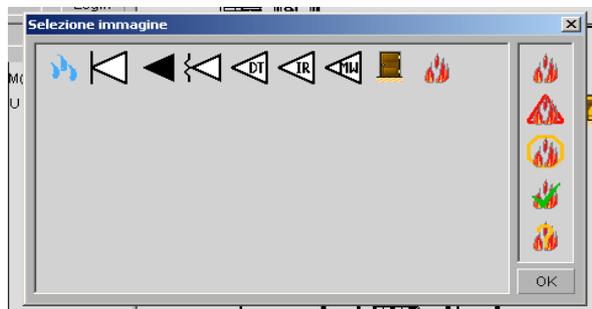
- Marcatori poligonali: rappresentano un sensore tramite un poligono, cerchio o altro il quale assumerà un colore specifico a seconda dello stato del sensore.
- Marcatori bitmap: rappresentano un sensore tramite un insieme di immagini, ciascuna delle quali associata ad uno stato del sensore
- Marcatori polilineari: simili ai marcatori poligonali, ma definibili come una linea spezzata, per rappresentare elementi come cavi o barriere
- Elementi di testo: semplici elementi didascalici
- Pulsanti di navigazione: permettono la navigazione fra le mappe

Per inserire o configurare uno di questi elementi nelle mappe è necessario autenticarsi su un qualunque client con un utente particolare che abilita le funzioni di editing di mappa. Nel caso Guardian sia installato con la 'configurazione protetta', questo non sarà sufficiente e sarà necessario anche inserire nel computer sul quale gira il client anche una chiavetta HW specifica.

Quando un utente ha i diritti di modifica delle mappe, oltre alle usuali operazioni sulle mappe, ottiene anche l'accesso al menu di modifica e di aggiunta elementi



Il menu di aggiunta permette di aggiungere uno degli elementi precedentemente elencati. Nel caso di un marcatore bitmap (Aggiunta Immagine) si aprirà un ulteriore pannello che permette di scegliere le icone sensore da un set predefinito

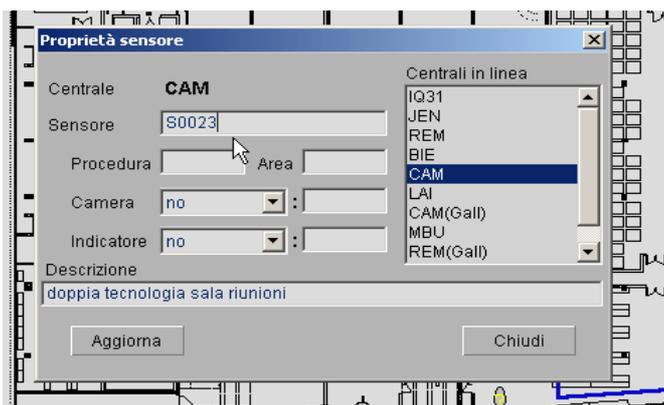


Tutti gli elementi aggiunti possono essere posizionati con precisione sulle mappe tramite semplice trascinamento (ovviamente solo per utente abilitato all'editing di mappa).

Il menu di modifica invece permette di cancellare o modificare le proprietà di un oggetto già inserito nelle mappe.

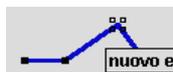


In particolare la voce proprietà apre il pannello di configurazione di un marcatore e ne permette l'associazione al sensore.



In questo pannello si seleziona una delle centrali configurate ed l'identificativo del sensore. Altri dati sono la descrizione del sensore e la sua eventuale associazione ad una telecamera. E' inoltre possibile associare una procedura ad un sensore. In questo caso su evento la procedura sarà richiamabile su richiesta dell'operatore.

Per i marcatori polilineari, oltre lo spostamento semplice sulla mappa è anche possibile il trascinamento dei singoli vertici, in modo da poter disporre la polilinea sulla mappa nel percorso più consono (molto comodo per i cavi anti allagamento e le barriere ad infrarossi)



Al di là delle operazioni di editing dei marcatori, sulle mappe possono essere effettuate una serie di operazioni da parte degli operatori autorizzati, come l'inclusione/esclusione dei sensori, l'inibizione/abilitazione degli stessi, il settaggio della uscita (se il marcatore viene associato ad una uscita) e il richiamo del video LIVE.



Per questa particolare funzionalità si possono predisporre anche marcatori con l'immagine di una telecamera, non associati ad alcun sensore, ma associati solo ad una telecamera nel caso l'unica funzione che si vuole ottenere sia appunto la richiesta del video LIVE.

## 8 – Sinottico eventi

La lista eventi contiene tutti gli eventi attivi (allarmi, guasti o segnalazioni) raccolti da Guardian. Guardian prevede per ogni evento una delle 2 possibili transizioni

1 – **Evento (ACK) Evento riconosciuto (END) Riposo**

## 2 – Evento (END) Evento terminato (ACK) Riposo

In entrambe le sequenze l'iter dell'evento è determinato da 2 condizioni, l'ACK cioè l'azione di riconoscimento e presa in carico da parte dell'operatore, e dall' END, cioè la condizione, proveniente dal campo, di evento non più sussistente.

Senza una delle due condizioni l'evento non può sparire dalla lista degli eventi (riposo).

I colori nella lista degli eventi aiutano a seguire l'evento nella sua evoluzione

- Rosso – è un evento o un evento terminato (ma non riconosciuto) di tipo allarme.
- Giallo – è un evento o un evento terminato (ma non riconosciuto) di tipo guasto.
- Azzurro – è un evento riconosciuto di tipo allarme o guasto.

I colori dei sensori sulle mappe corrispondono a quelli degli eventi relativi nella tabella eventi, con la sola eccezione che nelle mappe i sensori non riconosciuti in allarme o in guasto possono essere resi lampeggianti per una più facile localizzazione.



Oltre al comando di riconoscimento, l'altro fondamentale comando sulla lista eventi è la localizzazione.

Tramite questo comando Guardian cambierà la mappa posizionandosi su quella che contiene il sensore relativo all'evento selezionato.

In Guardian non sono previsti cambi di mappa automatici su arrivo di eventi: questa è una precisa scelta in quanto all'arrivo di un evento l'operatore potrebbe essere impegnato su una mappa e sarebbe poco funzionale toglierla dalla sua vista in modo arbitrario.

Se il sensore relativo all'evento è associato ad una telecamera, da questo menu possono essere richiamati anche i comandi Osserva LIVE e Osserva EVENTO. Il primo aprirà un popup del LIVE della telecamera associata, mentre il secondo un popup visualizzante la registrazione di quella telecamera a partire da 10 secondi (tempo configurabile, ma globalmente, non per singolo sensore) prima dell'orario dell'evento, in modo da avere una panoramica temporale attorno all'evento.

Guardian si occupa di effettuare tutte le conversioni di orario necessarie, rendendo superfluo l'allineamento dell'orario di tutti i videosever.

## Il menu generale

Selezionando lo scudo di Guardian, in alto a sinistra del client, si apre il menu generale che permette l'accesso a delle funzioni avanzate di configurazione, reportistica e altro.



## Sinottico generale

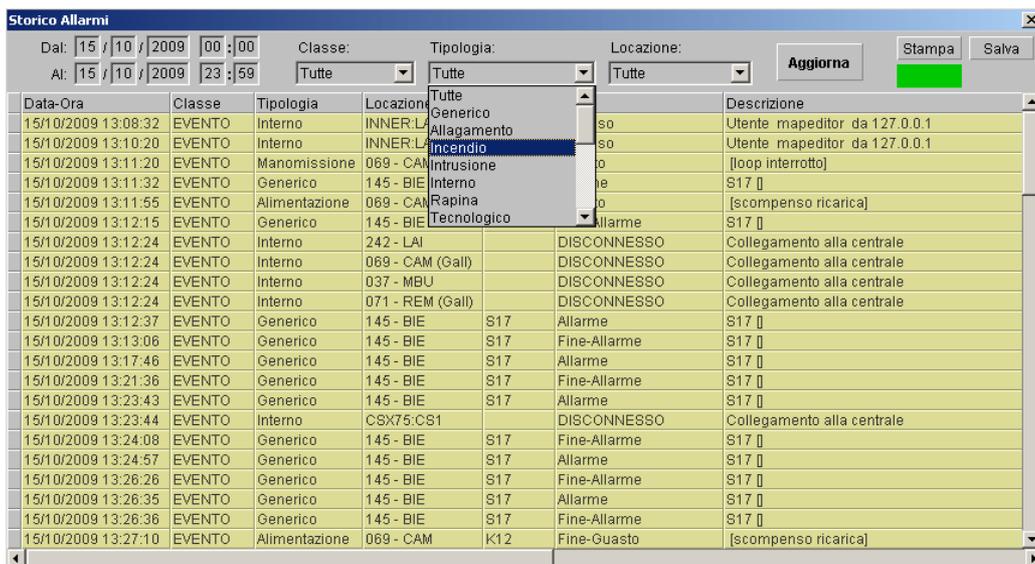
E' un pannello che riassume, in formato grafico, tutte le aree presenti nel sistema, e mostra se sono inserite (rosse) o disinserite (verdi).

Questo pannello viene spesso inserito come una sezione del layout di Lambda, direttamente senza doverlo aprire, nel qual caso questa opzione di menu diviene superflua e viene tolta.

### Storico allarmi

E' una pannello che permette il recupero degli eventi storicizzati tramite 4 filtri associati:

- selezione temporale
- classe evento (evento, azione operatore o stato)
- tipologia dell'evento (le tipologie sono associabili liberamente ai sensori)
- locazione (sfrutta i gruppi associati alla centrale a cui l'evento fa capo, ad esempio la sede)



Data-Ora	Classe	Tipologia	Locazione	Descrizione
15/10/2009 13:08:32	EVENTO	Interno	INNER-L	Utente mapeditor da 127.0.0.1
15/10/2009 13:10:20	EVENTO	Interno	INNER-L	Utente mapeditor da 127.0.0.1
15/10/2009 13:11:20	EVENTO	Manomissione	069 - CAM	[loop interrotto]
15/10/2009 13:11:32	EVENTO	Generico	145 - BIE	S17 []
15/10/2009 13:11:55	EVENTO	Alimentazione	069 - CAM	[scompenso ricarica]
15/10/2009 13:12:15	EVENTO	Generico	145 - BIE	S17 []
15/10/2009 13:12:24	EVENTO	Interno	242 - LAI	DISCONNESSO Collegamento alla centrale
15/10/2009 13:12:24	EVENTO	Interno	069 - CAM (Gall)	DISCONNESSO Collegamento alla centrale
15/10/2009 13:12:24	EVENTO	Interno	037 - MBU	DISCONNESSO Collegamento alla centrale
15/10/2009 13:12:24	EVENTO	Interno	071 - REM (Gall)	DISCONNESSO Collegamento alla centrale
15/10/2009 13:12:37	EVENTO	Generico	145 - BIE	S17 Allarme
15/10/2009 13:13:06	EVENTO	Generico	145 - BIE	S17 Fine-Allarme
15/10/2009 13:17:46	EVENTO	Generico	145 - BIE	S17 Allarme
15/10/2009 13:21:36	EVENTO	Generico	145 - BIE	S17 Fine-Allarme
15/10/2009 13:23:43	EVENTO	Generico	145 - BIE	S17 Allarme
15/10/2009 13:23:44	EVENTO	Interno	CSX75:CS1	DISCONNESSO Collegamento alla centrale
15/10/2009 13:24:08	EVENTO	Generico	145 - BIE	S17 Fine-Allarme
15/10/2009 13:24:57	EVENTO	Generico	145 - BIE	S17 Allarme
15/10/2009 13:26:26	EVENTO	Generico	145 - BIE	S17 Fine-Allarme
15/10/2009 13:26:35	EVENTO	Generico	145 - BIE	S17 Allarme
15/10/2009 13:26:36	EVENTO	Generico	145 - BIE	S17 Fine-Allarme
15/10/2009 13:27:10	EVENTO	Alimentazione	069 - CAM	K12 Fine-Guasto [scompenso ricarica]

La funzione di stampa, ampiamente configurabile, permette la generazione di report graficamente gradevoli su carta. Tramite questo strumento è possibile tracciare tutta la 'vita' di un evento, valutare se è stato preso in carico dall'operatore in tempi accettabili, ecc.

### Rapporto commenti

Ogni operatore può associare un commento ad un evento quando lo prende in carico.

Il pannello di rapporto commenti permette di visualizzare i commenti immessi dagli operatori, sostituendo brevi note cartacee (post-it)

### Elenco esclusi

Un pannello sinottico che riassume tutti i sensori attualmente esclusi o inibiti nel sistema, fornendo informazioni sull'orario di esclusione.

Il pannello, che fornisce filtri simili allo storico eventi (tranne quello temporale), è uno strumento utile per non dimenticare sensori esclusi.

### Fuori orario

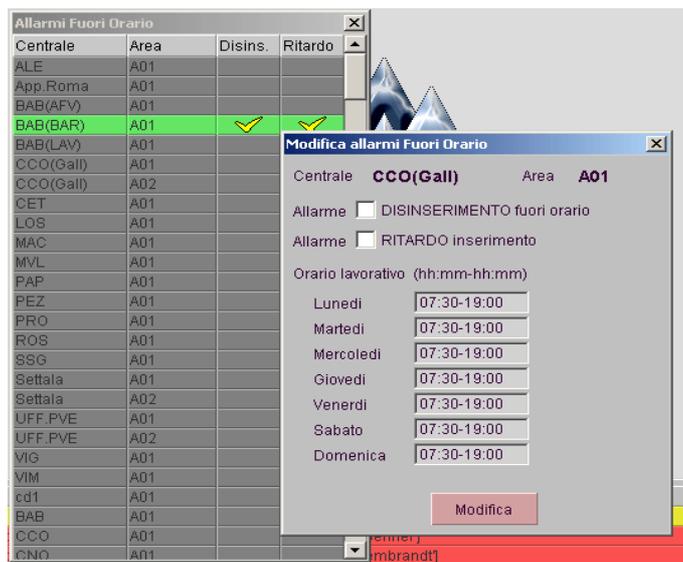
Per ogni singola area, Guardian permette di impostare delle segnalazioni di anomalie rispetto ad una schedulazione settimanale.

Tramite il pannello dei fuori orario si può configurare per ogni giorno della settimana un intervallo orario nel quale ci si aspetta che l'area sia inserita o disinserita e attivare gli allarmi di

- DISINSERIMENTO fuori orario – Se l'area viene disinserita da tastiera (non da Guardian) in un orario in cui ci si aspettava che l'area fosse inserita.
- RITARDO inserimento – Se arriva il momento di inserire le aree, ma l'operatore se ne dimentica, riceverà degli allarmi di ritardo inserimento, a promemoria.

Le fasce orarie all'interno di una giornata possono comprendere più intervalli.

Tutte le aree presenti nel sistema (appartenenti a tutte le centrali antintrusione), rientrano nella lista presentata dal pannello, anche se inizialmente per tutte i due tipi di allarme saranno disattivati, fino a differente programmazione esplicita.



### Lista centrali – Disconnesse

Un semplice sinottico che riassume tutte le centrali attualmente non raggiungibili. Utile solo nel caso di sistemi enormi.

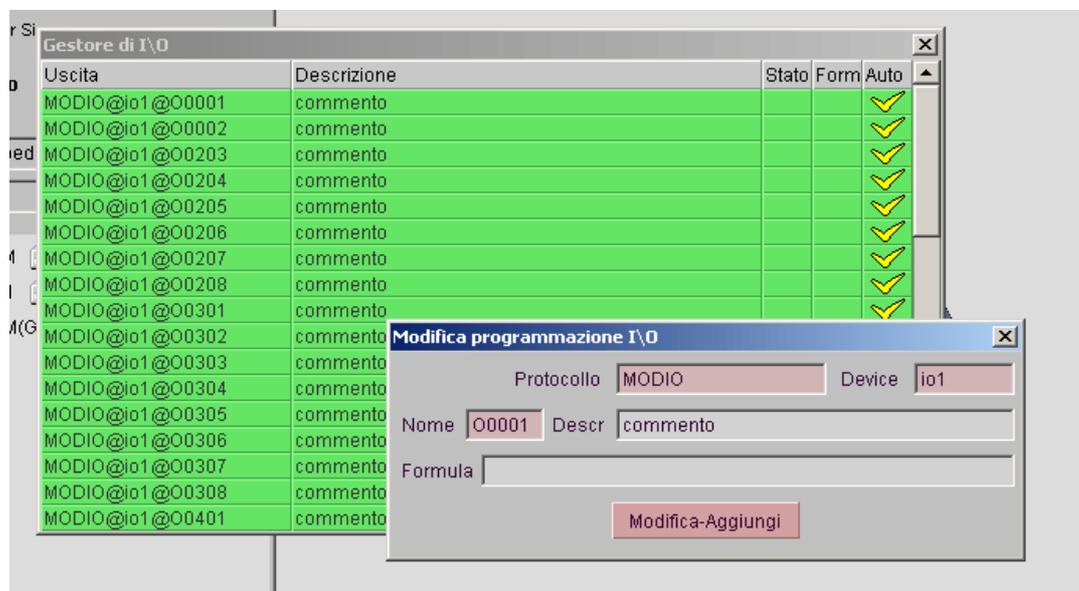
### Lista centrali – Manutenzione

Tramite apposito comando sulla centrale, una centrale può essere posta in stato di manutenzione, per cui Guardian ignorerà tutti gli eventi provenienti da essa, finché non verrà di nuovo rimessa in condizione normale.

Questo sinottico riassume le centrali attualmente poste in tale stato.

### Gestione – Input/Output

Il gestore di IO di Guardian permette di configurare formule booleane complesse per pilotare qualunque uscita collegata al sistema.



Le uscite pilotabili non sono solo quelle dei device di IO, ma anche quelle delle centrali di sicurezza collegate. Possono essere inseriti nelle formule booleane i seguenti elementi

- allarmi di sensori
- guasti di sensori o di sistema
- stato inserimento aree
- allarme di area

Il formalismo di tali formule esula dallo scopo del presente documento.

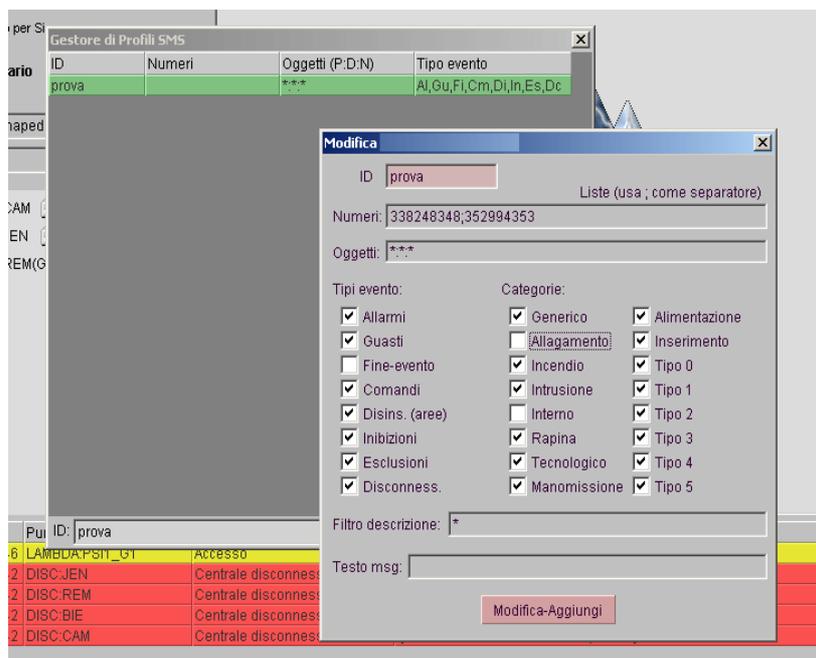
### Gestione – Sorgenti video

E' una sorta di anagrafica dei videosever di cui Guardian necessita per poi permettere l'associazione delle telecamere ai sensori.

In questa anagrafica vengono inserite anche le credenziali per l'accesso ai videosever, e le tipologie di popup da utilizzare.

### Gestione – Profili SMS

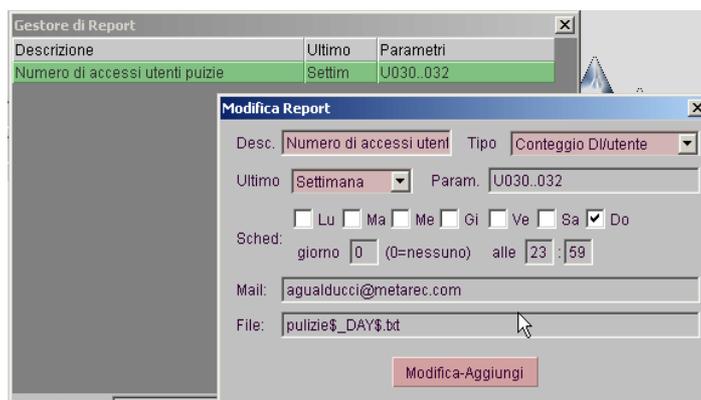
Permette di creare una lista di profili di notifica e per ciascun profilo configurare un insieme di numeri telefonici di destinazione, una serie di tipologie di allarmi da notificare e un formato di messaggio da inoltrare.



La notifica SMS per funzionare deve far capo ad un dispositivo MC55 (modem GSM) che deve essere collegato e raggiungibile dal server di Guardian.

### Gestione – Report

I Report Parametrici di Guardian possono essere definiti per produrre un'ampia gamma di reportistica attivabile con schedulatore (giornalieri, settimanali, mensili, annuali) o manualmente.



Questi report attingono alla stessa base dati dello storico allarmi, ma la sintesi di cui sono capaci permette di estrarre informazione comoda e con un valore aggiunto.

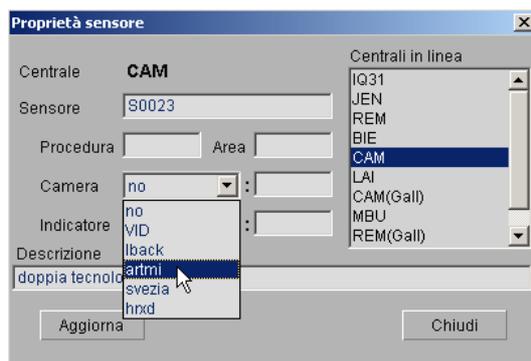
Possono essere salvati su file, inviati per posta o entrambi.

## Integrazione eventi-video: i popup

Guardian permette una efficace e duttile integrazione fra eventi di sicurezza (intrusione, incendio, allagamento) o tecnologici (stati e soglie) e le sorgenti video configurate.

Questo viene realizzato tramite dei popup, cioè finestre in primo piano che visualizzano sempre un solo flusso video e non hanno interazione con l'utente se non lo spostamento e la chiusura del popup stesso.

Qualunque marcatore grafico nelle mappe può essere associato ad una sorgente video, ma una sola, tramite il pannello di proprietà del marcatore.



Al marcatore si associa la sorgente video (videoserver) ed i parametri, come nella immagine sopra.

I parametri sono della forma: N\$Pxxx\$Pxxx\$Pxxx...

dove N è il numero di telecamera, relativamente al server video indicato, mentre i parametri sono tutti opzionali e sono divisi in 2 categorie:

### Parametri interni

Sono parametri utilizzati dal client Lambda e quindi validi per tutti i popup.

**\$A** – Attiva AUTOPOP, cioè all'arrivo di un allarme sul sensore associato al marcatore, viene aperto il popup video. A seconda della installazione, il popup può partire in LIVE (video corrente), oppure può partire in GET (video registrato) a partire da un certo numero di secondi precedenti l'allarme stesso.

**\$AL** – Variante di \$A da utilizzare nel caso di popup che partono in GET. Permette di stabilire, per un certo sensore-marcatore, che su allarme il suo video deve partire in LIVE, invece che in GET.

**\$AH** – Variante di \$A per far partire il popup video nascosto (non visibile). Un popup ovviamente non visualizza alcun video, ma può impostare dei preset sulla telecamera.

**\$LBsource** – Imposta Live BackDrop su quel marcatore. Ogni volta che questo popup viene fatto partire in LIVE, viene utilizzata la sorgente video (videoserver) indicato da source, al posto della sorgente video impostata nel pannello di preferenze del marcatore. Questo permette, nel caso di videoserver con telecamere IP, di bypassare il videoserver stesso per ottenere il flusso video in LIVE, accedendo direttamente alla telecamera.

### Parametri esterni

Sono parametri interpretati dal popup specifico e possono essere o non essere presenti, a seconda delle funzionalità implementate. Di norma questi parametri definiscono la qualità del video e funzioni PTZ.

Descritti di seguito solo alcuni disponibili in molti casi: per gli altri fare riferimento alla documentazione specifica dei popup.

**\$Pnn** – Imposta sulla telecamera il preset numero nn (due cifre, ad esempio '\$P02' per il preset numero 2).

**\$B** – Attiva la gestione del brandeggio sul popup.

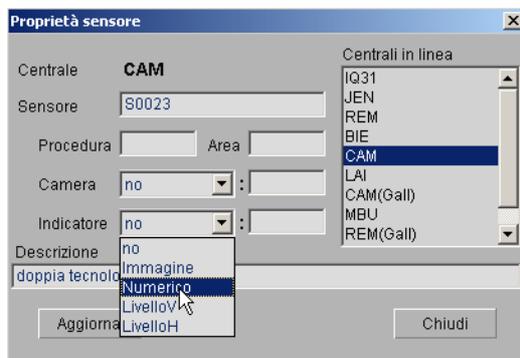
Per quanto riguarda l'autopop (attivazione automatica dei popup su allarme), ciascuna installazione di Guardian può definire una particolare politica di allocazione dei popup sullo schermo, ad esempio una allocazione a cascata, oppure tutti su un lato, su una riga, ecc. Sta comunque all'utente chiudere i popup quando non servono più.

Le altre modalità di accesso ai popup sono:

- Richiesta LIVE da mappa
- Richiesta LIVE dalla lista degli eventi correnti
- Richiesta GET (n secondi prima) dalla lista degli eventi correnti
- Richiesta GET (n secondi prima) dallo storico allarmi

## Integrazione regolazione meccanica: i gauge

Guardian integra le segnalazioni di allarme con la gestione dei valori di campo tipica della automazione industriale e della regolazione meccanica. Per fare questo si utilizzano degli elementi grafici in sovrapposizione ai classici marcatori chiamati 'gauge' (indicatori).

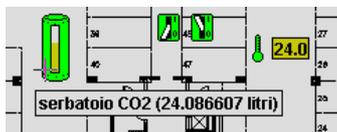


Ciascun elemento di campo può avere, in aggiunta al suo stato di allarme, anche i seguenti 3 elementi:

- valore di campo
- valori di range (min,max)

Esistono 4 tipi di gauge:

- **Immagine** – ottenuto sovrapponendo delle icone descrittive ai marcatori di mappa. Tale indicatore è adatto a valori 0,1 (digitali) o comunque a valori finiti e limitati – NON necessita del range
- **Numerico** – sovrappone al marcatore un riquadro che visualizza il valore di campo – NON necessita del range
- **LivelloV** e **LivelloH** – sovrappone al marcatore una barra di riempimento orizzontale o verticale ed è adatto a visualizzare un riempimento di un serbatoio, la carica di una batteria, o la percentuale di completamento di un processo. NECESSITA del range.



-esempi di gauge-

Tutti i driver di Guardian sono in grado di produrre i valori di campo per gli elementi che controllano: i gauge immagine possono essere quindi utilizzati in tutti i casi, anche solo per segnalare i sensori attivi sulla mappa o per evidenziare accessi (barriere, varchi) aperti, sia sui sensori, sia sugli I/O di centrale.

I gauge numerici e di livello sono invece utili solamente per i dispositivi specifici per l'automazione.

Ciascun gauge permette inoltre di alterare i valori di campo con delle scritture. A seconda delle situazioni questo può essere fatto anche con pulsanti specifici preimpostati, oppure con i comandi da menu.

## Topologia

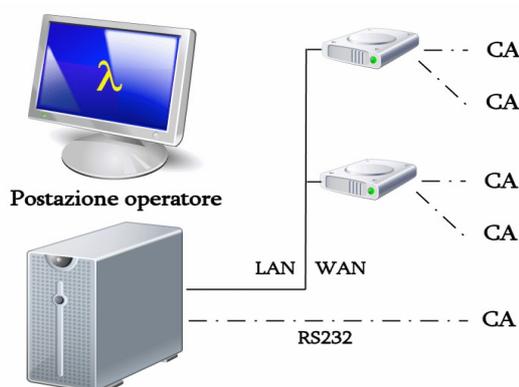
L'architettura del server di Guardian sfrutta una modularità che gli permette di essere installato in varie configurazioni che seguono al meglio le esigenze del cliente.

Il server infatti può risiedere interamente su una singola macchina fisica (PC server) oppure essere distribuito su diverse macchine.

Di seguito vengono illustrate alcune applicazioni tipiche, attive presso clienti.

### Installazione a macchina singola

Si tratta della installazione più naturale ed immediata in cui un unico server fisico gestisce in modo autonomo tutte le componenti del supervisore.



Il server di Guardian, compresi i driver per i vari protocolli, possono essere ospitati direttamente sulla postazione dell'operatore, su cui funziona anche il client Lambda. Le centrali d'allarme (CA) vengono raggiunte direttamente tramite seriale a bordo macchina, oppure tramite serial-hub dislocato in remoto e quindi via LAN o WAN (cioè con o senza routing).

Anche in questo caso non ci sono limitazioni al numero di client collegabili.

Le installazioni di questo tipo risultano poco costose, efficaci, facili da mantenere, facilmente estendibili.

Si consiglia comunque, per motivi di sicurezza e di stabilità, di non utilizzare il client sulla stessa macchina del server che in generale dovrebbe essere una macchina cieca (priva di monitor e tastiera) e di utilizzare come client sempre dei computer collegati in rete, di classe desktop.

### Installazione in backup

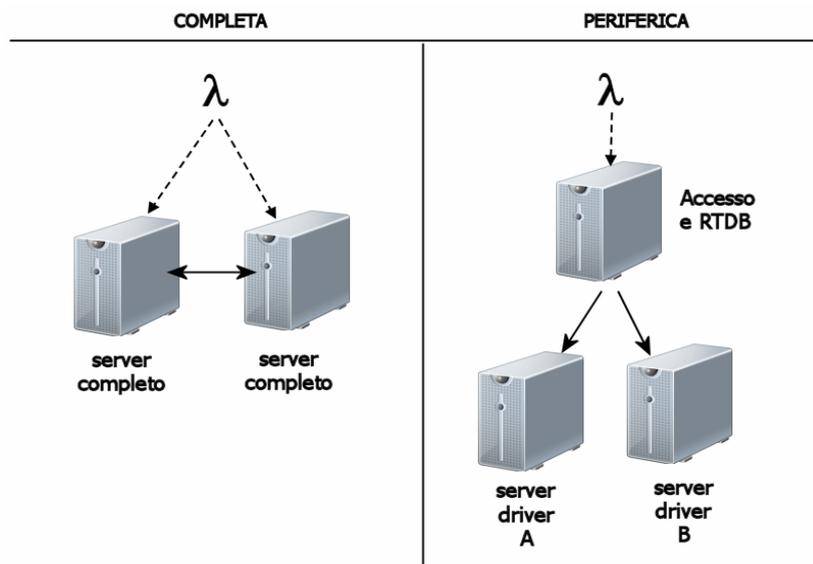
Per assicurare una maggiore continuità di servizio nel caso di cedimenti hardware è possibile configurare due server fisici di Guardian con gli stessi moduli e la stessa configurazione per funzionare in backup caldo fra di loro.

In questo caso ci sono diverse soluzioni di ridondanza possibili:

- ridondanza completa – l'intero server (driver compresi) è ridondato
- ridondanza periferica – solo le macchina adibite ai driver vengono ridondate
- ridondanza mista – comprende tutti gli schemi intermedi
- 

Nella **ridondanza completa** l'accesso al campo (centrali d'allarme) è di tipo concorrente e i due server competono per l'acquisizione delle risorse non condivisibili, tra cui tipicamente l'accesso alle seriali a bordo macchina ed alle porte server dei serial-hub. L'allineamento fra i due RTDB (parti centrali dei server di Guardian) viene assicurato dal 'double-feed' dei driver, cioè tutti i driver mandano gli stati del campo ad entrambe i server, e i comandi verso il campo parimente vengono spediti a tutti i driver. Si tratta quindi di un allineamento passivo.

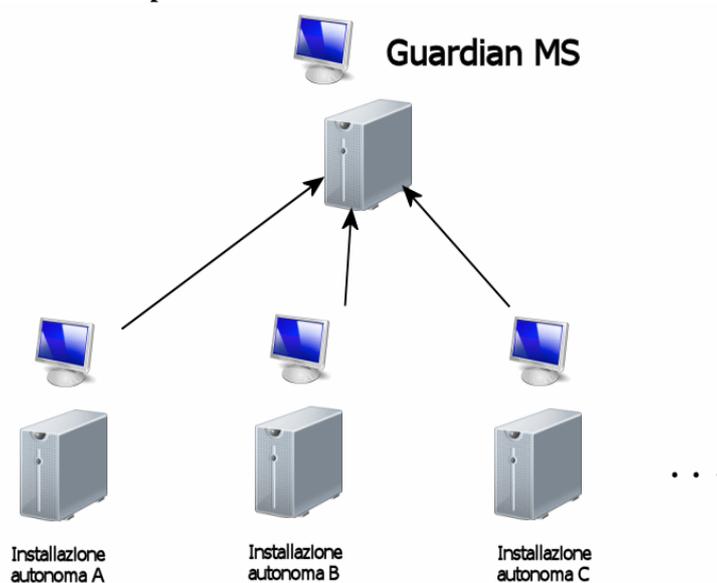
I client installati in rete devono essere configurati per accedere ad entrambi i server: utilizzeranno poi uno o l'altro server a seconda di quale è attivo.



Nella **ridondanza periferica** invece, utilizzata anche per estendere la capacità di supervisione di Guardian, il server centrale (RTDB) utilizza i driver situati su server periferici in modo selettivo e quindi l'allineamento è non necessario. Non c'è accesso concorrente al campo. Con queste due architetture di backup sono ad oggi gestiti diversi impianti su scala nazionale con oltre 200 centrali ciascuno e diverse peculiarità operative.

### Installazione asimmetrica (Guardian MS)

La sigla MS della versione di Guardian significa multi-site. Ma questo non ha nulla a che fare col numero di computer su cui Guardian è installato, né con l'ampiezza dell'installazione. In generale Guardian MS può essere visto come un ulteriore strato di supervisione posto sopra un certo numero di installazioni di Guardian **autonome e indipendenti**.



Le installazioni autonome possono mostrare fra di loro differenze notevoli, nel tipo e numero di mappe, nelle centrali configurate, negli operatori configurati, ecc., ma soprattutto nel layout del client, cioè nella disposizione degli oggetti di gestione dell'impianto.

Guardian MS si collega a tutti i siti periferici e ne ingloba la configurazione, predisponendo un sovra-strato di supervisione basato sul cambio di contesto, da cui il nome MultiSite.

Tutti i controlli tipici di Guardian, in Guardian MS tengono conto dei contesti: ad esempio nello Storico Allarmi la usuale griglia contiene una colonna in più (e quindi anche un filtro in più) che specifica il contesto dell'evento.

Nota: un server di tipo MS ingloba SEMPRE anche un server normale, che supervisiona le centrali locali e costituisce in Guardian MS un contesto sempre presente, chiamato appunto 'locale'.