

## «SISTEMA DI TELESORVEGLIANZA E VIDEOMONITORAGGIO DELLE CABINE PRIMARIE» - NOTA TECNICA

Enel Distribuzione S.p.a., a fini di esercizio e manutenzione degli impianti della rete elettrica e per la protezione degli stessi, si è dotata di un «Sistema di Telesorveglianza e Videomonitoraggio (TLSV)» degli apparati e dei locali delle Cabine Primarie (d'ora in avanti "siti") con l'obiettivo di:

*finalità del sistema*

- monitorare e/o gestire da remoto parti dell'impianto normalmente non coperte dal sistema di telecontrollo o per le quali, anche a fini manutentivi, sia richiesta la disponibilità di immagini in tempo reale;
- proteggere i siti maggiormente rilevanti dal punto di vista dell'esercizio elettrico e/o in cui sono presenti materiali di notevole valore (pannelli fotovoltaici, depositi temporanei di cavi elettrici, ecc.) rispetto al rischio di eventi dolosi, tenuto conto anche delle caratteristiche delle aree in cui i siti sono localizzati.

Il Sistema TLSV è costituito da un server centrale per ciascun Dipartimento Territoriale Rete (DTR) che, attraverso la rete IP realizzata per il telecontrollo della Rete AT, dialoga con i terminali periferici installati nelle Cabine Primarie interessate e da un web server che, attraverso la rete Intranet, rende disponibile agli utilizzatori finali una interfaccia web per l'accesso alle funzionalità proprie del sistema. Tali server sono allocati presso la sede di STUX (Sistema di Telecontrollo AT).

*caratteristiche tecniche*

I terminali periferici raccolgono ed elaborano le informazioni provenienti dagli apparati installati in Cabina Primaria e inviano i dati verso il server centrale. La gestione degli eventi generati dal sistema è affidata al Centro Operativo (CO) competente per la conduzione della rete AT.

In tale contesto i siti verranno classificati e dotato di sistemi e apparati in funzione delle specifiche esigenze di monitoraggio e/o di protezione.

*classificazione dei siti*

I "siti videomonitorati" verranno dotati di videocamere installate in modo da visualizzare esclusivamente la parte di impianto oggetto di monitoraggio. I "siti protetti" verranno dotati di videocamere e sistemi di protezione anti-intrusione.

La presenza di videocamere verrà segnalata all'esterno dell'impianto con idonea cartellonistica.

Nei siti dotati di videocamere verrà contestualmente installato un sistema di

*controllo accessi*

controllo accessi con tesserino elettronico di riconoscimento (un normale badge aziendale per i dipendenti) che ha lo scopo e la funzione di disattivare le funzionalità del sistema al momento dell'accesso e riattivarle all'uscita.

Nell'eventualità del protrarsi della presenza sull'impianto per più di quattro ore, la disattivazione del sistema di allarme dovrà essere riconfermata con le modalità più avanti specificate.

La disattivazione del sistema di allarme inibisce ogni funzionalità delle videocamere installate e quindi la ripresa delle attività effettuate in loco dal personale.

E' altresì tecnicamente preclusa la visualizzazione in tempo reale da remoto di immagini degli impianti in presenza di personale autorizzato in Cabina cioè "ad impianto escluso". Il funzionamento dell'impianto viene "escluso" dal personale che accede in Cabina utilizzando il badge aziendale.

Si precisa che la rilevazione, registrazione e salvataggio delle immagini è possibile solo quando il sistema di allarme è attivo; le citate operazioni sono tecnicamente precluse in presenza di personale autorizzato in Cabina Primaria.

*allarme  
protezione*

In caso di intrusione in una Cabina Primaria dotata di sistemi di protezione, ovvero in caso di "allarme protezione", le immagini registrate in impianto vengono estratte e inviate al server centrale. In tal caso l'Operatore incaricato - nel rispetto delle istruzioni ricevute dal Responsabile del trattamento dei dati - provvederà a estrarre e trasmettere le stesse alle unità preposte alla sicurezza (Unità Security) per le azioni di competenza.

Si precisa che in assenza di allarme le immagini rilevate in impianto "in continuo" vengono automaticamente sovrascritte e cancellate; ciò ne preclude tecnicamente l'archiviazione e la successiva estrazione.

Ai fini della protezione della riservatezza dei dati personali, il responsabile del trattamento dei dati personali è il Responsabile "pro tempore" del Dipartimento Territoriale Rete per il Centro Operativo e Cabine Primarie di competenza, nonché il Responsabile "pro tempore" della Funzione Tecnica Centrale Ingegneria.

*riservatezza  
dati personali*

La gestione dell'applicazione TLSV è affidata ad un ristretto numero di persone della Unità Esercizio Rete/TLV allo scopo autorizzate e incaricate; solo ad esse sarà consentito l'accesso, a mezzo login e password, al server su cui risiede l'applicazione TLSV. Alle stesse sarà affidata anche la gestione dei lettori di badge utilizzati per il controllo degli accessi agli impianti.

Ferme restando le procedure che regolamentano l'accesso negli impianti **Aspetti relativi**

primari di Enel Distribuzione, il personale che deve accedere ad un impianto dotato di controllo accessi dovrà procedere come segue:

*al personale*

- a) personale autorizzato ad accedere all'impianto ed in possesso di badge aziendale abilitato: una volta entrato in impianto, il personale dovrà immediatamente recarsi presso il punto ove è installato il lettore di badge - tipicamente l'ingresso dell'edificio quadri - ed escludere l'impianto di allarme, in modo da evitare che al Centro Operativo giungano falsi allarmi. Si osservi che l'invio dell'allarme al Centro Operativo è ritardato rispetto alla sua generazione in sito proprio per consentire al personale autorizzato di raggiungere in tranquillità il lettore di badge;
- b) personale autorizzato ad accedere all'impianto non in possesso di badge aziendale abilitato: prima di entrare in impianto il personale richiederà al Centro Operativo competente AT o MT la esclusione del sistema di allarme.

*accesso in C.P.*

L'esclusione dell'impianto di allarme comporta il contestuale spegnimento del sistema e degli apparati di protezione installati sul sito.

*attivazione e  
disattivazione  
allarmi*

La mancata esclusione dell'impianto genera un evento di allarme e avvia l'esecuzione delle azioni predefinite (es. attivazione sirena, invio segnalazione al Centro Operativo, ecc.)

All'uscita dall'impianto, il personale dovrà reinserire l'impianto di allarme nel caso a) utilizzando il proprio badge aziendale o, nel caso b) chiamando il Centro Operativo.

Tra il passaggio del badge e l'effettivo reinserimento dell'impianto di allarme è lasciato un intervallo di tempo sufficiente a consentire l'uscita dall'impianto del personale, senza che ciò determini falsi allarmi.

*condizione di  
pre-allarme*

Il reinserimento dell'impianto di allarme, così come la eventuale mancata disattivazione in tempo utile per evitare l'invio al Centro Operativo dell'allarme, sono evidenziati in sito a mezzo di segnali visivi e/o sonori. Si segnala che in condizioni di pre-allarme, può essere comandata l'accensione dell'impianto di illuminazione.

Nel caso in cui il mancato rispetto delle procedure generi un allarme, il personale è tenuto a contattare immediatamente il Centro Operativo competente per segnalare l'accaduto. In tal caso, l'Operatore classificherà l'evento come "falso allarme". Le immagini eventualmente registrate verranno cancellate decorse 24 ore,

fatte salve le festività, le giornate di sabato e domenica, nonché il caso in cui si debba aderire a specifica richiesta dell'Autorità Giudiziaria.

Le modalità di gestione dei principali eventi rilevati dal sistema, distinti tra eventi connessi alla protezione del sito e altri eventi, nonché i comportamenti da tenersi da parte del personale autorizzato presente in sito sono descritte nella Guida di Esercizio n. 19 del 2010 «Esercizio e manutenzione del sistema di telesorveglianza e videomonitoraggio delle Cabine Primarie».

*Guida di  
esercizio*

Le modalità di accesso e i comportamenti da tenersi da parte del personale autorizzato saranno portate a conoscenza del personale nelle dovute forme.

*Informativa al  
personale*

Roma, 22 marzo 2010