Le comunicazioni in IP nei sistemi di sicurezza

di FIlippo Gambino, Ermes - www.ermes-cctv.com

Che una protezione “sicura” sia frutto dell'integrazione tra sistemi diversi è ormai generalmente acquisito: la sola recinzione di un'area, per quanto robusta, da sola non è sufficiente a garantire la sicurezza di un sito in quanto con abbastanza tempo a disposizione qualsiasi barriera fisica può essere violata.

Ecco quindi che si preferisce installare, oltre alla recinzione, un sistema di allarme perimetrale che dia l'immediata segnalazione del tentativo di intrusione al quale quasi sempre si aggiunge un sistema di telecamere che consenta l'immediata verifica visiva della causa che ha generato l'allarme.

Appare evidente come in quest'ottica di integrazione di sistemi diversi può essere molto utile installare un impianto audio che permetta all'operatore di un centro di controllo sia di effettuare l'ascolto remoto delle voci e dei suoni sia di interagire in maniera attiva con gli eventuali intrusi diffondendo avvertimenti atti a scoraggiare l'azione in atto su una serie di altoparlanti.

Una soluzione di questo tipo è stata fino ad oggi di difficile adozione in quanto i sistemi di comunicazione audio tradizionali utilizzano in massima parte tecniche di trasmissione dei segnali di tipo analogico che limitano le possibilità di integrazione degli impianti audio nei moderni sistemi di sicurezza; l'utilizzo della tecnologia IP rende possibili in modo semplice ed affidabile questo tipo di realizzazioni.

Altri esempi dove è evidente l'utilità di un sistema di comunicazione audio in IP integrato con i tradizionali sistemi di sicurezza sono l'installazione in unione ad un sistema di controllo accessi di interfoni che consentano all'utente di comunicare con il centro di controllo per la gestione delle eccezioni come anche l'utilizzo, in associazione ad un impianto di rilevazione incendi, di un sistema di chiamate di emergenza (colonnine SOS) installate in aree sicure che mettendo in comunicazione queste aree con un centro di controllo consenta di portare soccorso a persone che si dovessero trovare in difficoltà nell'evacuare l'area come, ad esempio, persone disabili.

I sistemi di comunicazione audio/video in IP, infine, possono di per se costituire una parte essenziale di un sistema di sicurezza come avviene con l'adozione di videocitofoni per l'identificazione delle persone che chiedano di accedere a siti protetti non presidiati.

Una tale applicazione è stata utilizzata da una società del settore della telefonia mobile per identificare da un centro di controllo remoto, unico in ambito nazionale, il personale che per effettuare degli interventi di manutenzione deve

accedere ai siti tecnici sparsi sul territorio.
Questi servizi, infatti, sono solitamente affidati in service a ditte esterne da qui la necessita di identificare in modo visivo il personale non dipendente che deve effettuare l'intervento ed i cui documenti sono inviati di volta in volta in copia al centro di controllo. L'identificazione sicura della persona grazie al supporto visivo e al dialogo con l'operatore consente di disabilitare da remoto con la massima tranquillità i sistemi di protezione.
Tuttavia perché l'integrazione di sistemi di comunicazione audio o audio/video nella sicurezza sia semplice ed efficace gli apparati devono possedere alcuni requisiti fondamentali.
- dovranno essere nativi IP in modo da collegarsi direttamente ad una rete standard come apparati stand-alone evitando la necessità di interfacce o altri elementi intermedi verso la rete che complicherebbero la progettazione, l'installazione e la manutenzione del sistema.
- dovranno adottare tecniche di comunicazione Peer-To-Peer che consentono di stabilire collegamenti audio e audio/video diretti senza la necessità di centralini, server o unità di gestione di alcun tipo in modo da elevare l'affidabilità complessiva del sistema

Impianti con queste caratteristiche costituiscono dei sistemi ad intelligenza distribuita dove ciascun apparato si relaziona direttamente con gli altri elementi con cui deve comunicare senza mediazioni di tipo hardware o software stabilendo quindi una comunicazione altamente affidabile in quanto non esistono elementi critici che possano pregiudicare il funzionamento dell'intero sistema: il guasto di un apparato provoca il fuori servizio di quella sola unità senza influire sulle rimanenti comunicazioni come avverrebbe se queste fossero gestite da una unità centrale. Inoltre un tale sistema è facilmente espandibile, anche successivamente alla prima installazione, in quanto la sola limitazione alla possibilità di aggiungere nuovi apparati è data solamente dalla disponibilità di indirizzi IP.