La tecnologia Wireless nella protezione dei Musei

***Gianfranco Bonfante**, Direttore Generale e Presidente Onorario del Centro Studi ItaSForum*

***Luigi Brambilla**, Consiglio Direttivo del Centro Studi ItaSForum*

Premessa

Il termine ***wireless*** (dall'inglese senza fili) definisce i sistemi di comunicazione tra dispositivi elettronici che non fanno uso di cavi, mentre i sistemi tradizionali, basati su connessioni cablate, sono denominati ***wired.***

Il wireless utilizza onde radio a bassa potenza ma anche dispositivi, meno diffusi, che sfruttano la radiazione infrarossa o il laser.

La sua espansione è iniziata allorquando le esigenze di effettuare trasmissioni di informazioni si sono moltiplicate ed è subentrata l'esigenza di trasmissioni in movimento. I servizi radiotelefonici sono stati i primi a sfruttare questa opportunità.

Successivamente ne hanno beneficiato i servizi telefonici mobili, quindi la trasmissione dati e, con il proliferare delle applicazioni trasmissive, è sorto il problema di creare regole per lo sfruttamento e la condivisione dell'etere.

Sono così nati gli Standard, emessi, fondamentalmente, da tre Enti Internazionali denominati:

- ISO la cui etimologia è greca: "isos" cioè "uguale" perché le sue norme sono "uguali" per tutti gli Stati, circa 150 a livello mondiale, per consentire e facilitare lo scambio dei beni e dei servizi;
- IEC, acronimo di "International Electrotechnical Commission", organizzazione internazionale per la definizione di standard in materia di elettricità, elettronica e tecnologie correlate. Molti dei suoi standard sono definiti in collaborazione con l'ISO.
- IEEE, acronimo di "Institute of Electrical and Electronics Engineers" le cui finalità primarie sono il miglioramento della qualità della vita dell'uomo, favorendo conoscenza, applicazione delle nuove tecnologie, oltre che nobilitare l'attività tecnica. Le pubblicazioni IEEE costituiscono il 30% della letteratura ingegneristica e coprono quasi tutti gli aspetti dell'Elettronica e dell'Informatica moderna, senza contare gli oltre 900 standard industriali.

Wireless e security

Considerazioni preliminari

I sottosistemi di security, mediante centrali di gestione locali e remote, sono in grado d'interpretare fenomeni fisici per rivelare specifici eventi di allarmi, di stato, avarie ecc. utilizzando sensoristica di diverse tipologie:

puntuali: es. contatto magnetico;

lineari: es. barriera all'infrarosso a tratte di lunghezza differenziata;

volumetrici: es. barriera a microonde bistatica; microonda Doppler; ultrasuoni; tecnologie multiple, etc

sfruttando caratteristiche specifiche delle onde elettromagnetiche.

In tempi recenti, la sicurezza, intesa come security, safety, healt, environment, ecc. ha potuto trarre potenziamento e trasformazione di criteri impiantistici, grazie, non solo alla fase di rivelazione di eventi, ma soprattutto, alla trasmissione a distanza delle informazioni di varia natura.

Se si prende in considerazione uno schema classico di sottosistema antintrusione, sappiamo che i rivelatori possono essere connessi alla centrale di gestione in modalità stellare (ogni rivelatore fa capo alla centrale con un cablaggio dedicato), oppure in modalità seriale (i rivelatori, a gruppi, fanno capo a concentratori satelliti che, a loro volta, sono collegati alla centrale).

L'avvento di tecnologie Wireless, nel particolare Wi-Fi (Wireless Fidelity) con tecnica di modulazione FHSS, (Frequency Hopping Spread Spectrum - dispersione di spettro a salto di frequenza), offrono la possibilità di surrogare adeguatamente i cablaggi mediante collegamenti herthziani per brevi distanze (vedere Glossario alla voce Wi-Fi), mentre la trasmissione a distanza dei dati stessi avviene con tecnica WiMAX (Worldwide Interoperability for Microwave Access), tecnologia di trasmissione wireless che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili (BWA - Broadband Wireless Access) ed a distanze di decine di chilometri. La tecnologia può operare su varie bande di frequenza che sono in fase di armonizzazione in ambito europeo e mondiale, ma non ancora definite in Italia (vedere Glossario alla voce WiMAX).

Tra le tecnologie Wireless emerge lo standard IEEE 802.15.4 denominato ZigBee con campo di applicazione vastissimo, connotato, con eccitanti potenziali prospettive, "la vera rivoluzione nel wireless". Caratteristiche principali: la stabilità dei network creati, determinata

dal fatto che la velocità di trasmissione è piuttosto bassa (250 kbit al secondo) e il consumo quasi irrisorio (vedere Glossario alla voce ZigBee).

In questa fase euforica del Wireless, *occorre tener sempre presente che la sicurezza offerta da un cablaggio fisico,* è certamente più affidabile di un collegamento Wireless.

Il ricorso ad uno oppure all'altro tipo di vettore di trasmissione dati può derivare unicamente da attenta ed esaustiva analisi dei rischi esperita in rapporto al pregio dei beni da proteggere ed alle possibilità installative condizionate dalla natura architettonica dei locali espositivi o, estensivamente, degli edifici da tutelare il cui archetipo è costituito dai musei, sovente costruzioni irripetibili, che sono per l'Italia una ricchezza unica al mondo.

Secondo la definizione contenuta nello statuto dell'International Council of Museums "Il museo è un'istituzione permanente, senza scopo di lucro, al servizio della società e del suo sviluppo. È aperto al pubblico e compie ricerche che riguardano le testimonianze materiali e immateriali dell'umanità e del suo ambiente; le acquisisce, le conserva, le comunica e, soprattutto, le espone a fini di studio, educazione e diletto".

Pertanto, finalità del Museo è la conservazione e l'esposizione per prolungati archi temporali delle opere d'arte all'attenzione dei visitatori ed allo studio degli appassionati d'arte.

Ma la passione può nascondere finalità poco nobili che alimentano il furto delle opere d'arte e, in presenza di squilibri mentali, anche danneggiamenti e sfregi.

"Mille cause riunite hanno concorso a fare dell'Italia una specie di museo generale, un deposito completo di tutti gli oggetti che servono allo studio delle arti. "Questo paese è il solo che possa godere di questo specifico privilegio" scrisse Quatremère de Quincy famoso architetto illuminista, autore di noto Dizionario Storico di Architettura.

Aprire il capitolo delle opere d'arte rubate in Italia significa non riuscire a chiuderlo. Il saccheggio dura da secoli. Le prospettive non sono favorevoli e la tutela dei siti museali è argomento molto complesso, anche se non solo italiano.

Pierre Rosenberg, direttore del Louvre ed accademico di Francia, in un'intervista rilasciata dopo clamorosi furti di tele preziose, ha espresso tutta la determinazione ed il realismo pragmatico di chi ha compreso che la politica di tutela da perseguire nelle opere d'arte debba essere scevra da sterili e dannosi compromessi.

Senza ricorrere ad eufemismi, punta il dito alle forme di attacco delle opere d'arte in tutte le loro espressioni: furti, rapine, estorsioni danneggiamenti fortuiti e volontari.

Uomo di vasta esperienza, dopo i furti ha proceduto al rinnovamento completo del sistema di sicurezza, perfettamente consapevole dei disagi dei visitatori nel varcare la soglia del museo. Afferma: “I controlli devono essere più severi ed implacabili che negli aeroporti quando si passano le "forche caudine” dei metal detector e si può essere anche perquisiti.... I tempi obbligano l'arte a difendersi come se le avessero dichiarato guerra....Un'infinità di pericoli incombe sui musei: vandalismi, incendi, inondazioni. Sono istituti molto fragili..... Siamo attaccati da un esercito fantomatico di professionisti, matti, provocatori, lanzichenecchi che cercano la pubblicità "mediatica", giovani sbandati....Non escludo, poi, il terrorismo....Ci si deve aspettare anche i ricatti”.

Rosemberg descrive uno scenario quanto mai realistico, anche se, per ironia della sorte, dimentica che l’Louvre, di cui è direttore, venne aperto nel 1791 nel vecchio Palazzo Reale per ospitare opere d’arte confiscate nel corso della Rivoluzione Francese e per custodire moltissimi capolavori fiamminghi e, soprattutto, italiani, frutto del saccheggio metodico e scientifico posto in atto nel corso delle guerre napoleoniche. Di 506 dipinti di provenienza italiana, circa la metà, per la precisione 248, non tornarono in patria, senza contare sculture et similia.

I nazisti, dopo l’8 settembre 1943, diedero corso ad altra razzia con difficilissimo e parziale recupero. In sintesi, il patrimonio artistico dell’Italia ha subito, nel tempo, ripetuti, pesanti ladrocini che, con persistente stillicidio, purtroppo continuano in quanto tutti sanno che l’Italia possiede poco meno della metà del patrimonio artistico mondiale.

Impiego della tecnologia Wireless in ambito museale

Dopo l’inciso storico e prima di procedere all’esame tecnico del possibile impiego della tecnologia Wireless nella protezione dei Musei, si ritiene indispensabile una **premessa di carattere sistemico,** già anticipata in precedenza: *l’esigenza di attenta ed esaustiva analisi dei rischi esperita in rapporto alle esigenze dell’ambiente e dal pregio dei beni da proteggere.*

La Sicurezza di qualsivoglia bene dipende da adeguato Risk Management presieduto dal Security Manager.

Di conseguenza occorre instaurare un *Risk Management System* in grado di esaminare tutte le fasi di una Disk Analisi, per ottenere:

- Un quadro completo delle *Vulnerabilità* e dei *Rischi* presenti,
- *L’individuazione di Indicatori di Rischio e Parametri di Priorità***,** nelle decisioni relative alla *salvaguardia da introdurre,* basandosi sui loro costi e sulla loro efficacia.

E’ quindi di estrema importanza individuare una metodologia “standard” di acquisizione e valutazione delle informazioni per validare il ***profilo di rischio*** *del Bene* da tutelare, secondo le seguenti *fasi fondamentali di approccio metodologico:*

- identificazione dei Beni principali del Museo, classificandole in base al loro valore effettivo;
- raccolta di tutti i possibili flussi di informazione per i Beni selezionate;
- indicazione degli obiettivi della protezione da applicare agli elementi classificati al primo punto;
- individuazione di tutte le possibili minacce;
- attuazione dell'analisi dei rischi per ciascuna risorsa;
- definizione di regole e meccanismi necessari a proteggere le risorse dai rischi individuati;
- formulazione delle Procedure di Sicurezza sulla base del punto precedente.

In successione, il Security Manager potrà dar corso ad esaustive e congruenti politiche di sicurezza.

Tecnologia e salvaguardia delle infrastrutture museali

Sotto l'aspetto tecnico, la salvaguardia dei siti museali mediante la realizzazione di impianti tecnologici e sistemi di sicurezza complessi e correttamente funzionali, si è quasi sempre scontrata con le esigenze di salvaguardare le particolari caratteristiche e vetustà delle infrastrutture ed edifici.

Spesso tali strutture espositive sono vecchi castelli, palazzi ed edifici sacri storici, chiese di pregio storico-artistico, non progettati originariamente per questa tipologia d'impiego e, quasi sempre, sottoposti a vincoli, controlli e rilascio di autorizzazioni da parte delle Sovrintendenza alle Belle Arti e del Ministero dei Beni e le Attività Culturali (MIBAC).

All'estero, con esclusione di alcuni stati europei, la problematica non sussiste in quanto le infrastrutture che ospitano Musei e Gallerie d'Arte sono state progettate ad hoc con adeguate predisposizioni infrastrutturali, impiantistiche e tecnologiche.

Completamente differente la situazione nel nostro Paese, ove, secondo i dati del Ministero dei Beni e delle Attività Culturali, lo sterminato patrimonio culturale dell'Italia si articola, in base al censimento del 2003 su:

- 7.282 Chiese ed Abbazie,
- 4.109 Palazzi e Residenze,
- 2.054 Castelli e Fortificazioni,

- 1.034 Monumenti dell'Antichità,
- 491 Giardini Storici,
- 3.232 Musei pubblici e privati,
- 2.000 siti archeologici,
- un numero assai importante tra biblioteche ed archivi.

A fronte di simili valori numerici, che concretizzano un autentico Museo a cielo aperto, solo interventi mirati ed una programmazione efficiente possono garantire la corretta e funzionale custodia e valorizzazione del patrimonio.

Il problema è garantire sicurezza, monitoraggio e gestione degli ambienti che custodiscono i Beni (dipinti, affreschi, statue, etc,) e, contestualmente fruibilità e visibilità dei beni stessi da parte del pubblico. Come bilanciare le due esigenze contrapposte, senza penalizzare una o l'altra?

Un ambiente che ospita opere d'arte o di valore storico riveste, spesso, valore artistico ed architettonico ed è pressoché impossibile intervenire con opere di muratura, stesura di cavi elettrici, reti di collegamento, tubazioni sottotraccia, ecc…. mentre le esigenze di sicurezza sono molteplici, diversificate ed indispensabili.

In qualsiasi Sito Museale occorre, infatti, porre in essere un Sistema di Sicurezza articolato su sottosistemi di:

- rivelazione, anti-effrazione, anti-intrusione ecc.. durante l'orario di chiusura al pubblico dei locali;
- rivelazione furto, danneggiamento, sfregio durante l'orario di apertura al pubblico dei locali;
- allarme rapina;
- rivelazione incendio, allagamento, fughe di gas, ecc….
- misurazioni ambientali termoigrometriche e di illuminazione, significative ai fini della conservazione dei beni di natura organica, inorganica, mista;
- illuminazione di emergenza in caso di avaria o interruzione dell'erogazione dell'energia elettrica primaria;
- monitoraggio del numero di persone presenti in ciascun ambiente;
- analisi comportamentale delle persone presenti nella sala espositiva (ai fini della security, ma anche del marketing, statistici e di organizzazione logistica delle mostre);

- comunicazione audio mono o bidirezionale verso il pubblico presente.

La soddisfazione delle esigenze sopra elencate può essere ottenuta da un punto di vista tecnologico ed operativo mediante:

- l'installazione di sottosistemi di tipo cablato ad architettura tradizionale spesso non realizzabile per l'elevato impatto ambientale;
- l'installazione di sottosistemi di tipo integrato, dotato di architettura di filosofia innovativa ad " intelligenza distribuita " ed interconnessione senza fili, ossia Wireless.

Ed è di quest'ultima che intendiamo descrivere lo stato dell'arte il cui apice può essere identificato nei

Sistemi Integrati ad Intelligenza Distribuita

Le tecnologie elettroniche e della comunicazione nel corso degli ultimi anni sono progredite in modo esponenziale. Se un decennio fa un computer, tipo mainframe, doveva essere collocato in ambiente di 100 mq, oggi un elaboratore, migliaia di volte più potente, può stare nel palmo di una mano (es. Black Berry, Hi Phone, Smart Phone, e gli stessi telefoni cellulari ecc).

Analogo progresso tecnologico lo ritroviamo nei sensori o rivelatori. Se un sensore, solo dieci anni fà non riusciva a stare nel palmo di una mano, oggi si presenta con le dimensioni di un piccolo seme.

E' l'avvento dell'innovatività, della miniaturizzazione, dei consumi irrisori, delle multifunzionalità, della versatilità, della comunicazione, adattabili alle reali necessità dell'uomo.

In altri termini, il computer tenderà ad "incarnarsi" negli oggetti più impensati (dai vestiti, alle automobili, ai tavolini delle nostre case, in nuovi artefatti non ancora sviluppati, in piccoli animali).

Valgano un paio di esempi.

Lo Starlab (un laboratorio di ricerca Belga) ha recentemente lanciato un consorzio per lo sviluppo di vestiti "intelligenti" in grado di monitorare l'inquinamento ambientale ed i parametri vitali personali.

I ricercatori di un laboratorio israelo-americano hanno scoperto che le ferite delle larve cicatrizzano molto velocemente e possono essere utilizzate per inserire nelle future farfalle o

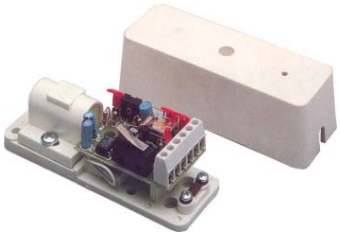
nelle mosche o nelle zanzare dei «mems», sofisticati microchip telecomandabili, in grado di registrare conversazioni dettagliate e intercettare materiale esplosivo.

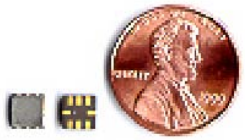
Il computer sta perdendo la sua caratteristica di macchina universale (general-purpose) per acquisire un corpo (o per meglio dire una serie di corpi, a seconda dei casi) con capacità diretta di interazione con l'ambiente esterno (mediata da sensori e da attuatori esattamente come nel caso degli organismi naturali o dei robot).

In sintesi: l'intelligenza dei sistemi si è spostata dal centro (centrale intelligente) verso il campo (sensori intelligenti). In unico elemento si integrano molteplici funzioni/servizi; sono possibili soluzioni HW e SW ad hoc, per ogni specifica applicazione/esigenza.

Per comprendere meglio, esaminiamo due tipi di tecnologia.

Il primo attiene alla tecnologia analogica di recente passato: sensore inerziale rilevatore d'impatto (anni 90) dimensioni mm 60x30



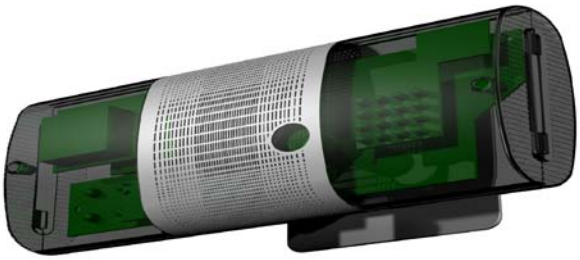


Il secondo si riferisce alla tecnologia di "accelerometro digitale" (sensore di misura dell'accelerazione lungo un asse generata dal movimento di un oggetto di ultima generazione. Per comprendere le dimensioni è stata posta a fianco una moneta): dimensioni mm 2x2.

Nelle nostre ricerche, abbiamo avuto la fortuna di esaminare, in anteprima, un dispositivo, che denomineremo con termine di fantasia "Defender".

E' in corso di produzione da parte di un'importante azienda italiana del nordest che opera a livello internazionale, specializzata in sensori e telecamere intelligenti per impieghi di sicurezza e controlli industriali.

Secondo il nostro parere, la tecnologia impiegata è quanto di meglio si possa offrire per la tutela dei Musei, senza provocare impatti negativi ai particolari ambienti.



Quello che all'apparenza, può sembrare una normale lampada di emergenza, presenta le seguenti dimensioni 29,5 x 6 x 14 cm (larghezza x profondità x altezza).

è dotato di:

- illuminatore agli infrarossi, in spettro non visibile;
- modulo multisensoristica ambientale;
- al centro, in un cerchietto, una mini telecamera fino a 3 Megapixel, ad altissima sensibilità, con ottica intercambiabile;
- al centro, nella maschera retinata, un altoparlante per comunicazioni ed un microfono per ascolto;
- led ad alta potenza illuminante (equivalente ad una lampada ad incandescenza di circa 60 Watt).

Si tratta di un sistema Integrato di Sicurezza dotato di tecnologie multisensore integrate a bordo di un'unica apparecchiatura digitale e rappresenta una nuova generazione di sistemi di sicurezza dotati di intelligenza a bordo e capacità di analisi su base algoritmica. Il dispositivo nasce dall'esigenza che in siti come quelli museali si rende necessario garantire un efficace misurazione e controllo dei fenomeni fisici che avvengono nell'ambiente da proteggere e quindi adottare soluzioni tecnologiche ed impiantistiche complementari difficilmente integrabili tra di loro, costose se adottate tutte insieme e di elevato impatto visivo se presentate singolarmente. Per realizzarlo sono state impiegate tutte le più innovative tecnologie di rilevazione oggi disponibili sul mercato della microelettronica. Tecnologia DSP BlackFin, video CMOS, Tecnologia micro-machining CMOSens, Tecnologia PIR, Tecnologia led SuperNova, POE (PowerOverEthernet), ZigBee, in grado di assicurare a questa nuova generazione di dispositivi di sicurezza:

- Ingombro ridotto.
- Alta efficienza, accuratezza delle misurazioni ed affidabilità del sistema elettronico.

- Bassissimi consumi energetici.
- Elevato grado di integrazione, soprattutto con reti di trasmissione digitali Ethernet e ZigBee mediante standard TCP/IP e UDP.

Il "Defender" è in grado di svolgere funzioni, fino a qualche anno fa inimmaginabili sia sotto l'aspetto numerico che applicativo, in unico contenitore:

- Telecamera digitale ad alta risoluzione (megapixels) con algoritmi di analisi scene per identificazione automatica di situazioni cosiddette critiche, esempio:

- *Motion detection* (rilevamento tradizionale di movimento).
- *Blob motion* (rilevamento di "soggetti/sagome in movimento").
- *Analisi stato ingressi digitali correlati in AND or con gli algoritmi video.*
- *Stato degli ingressi video* (assenza di segnale, oscuramento telecamera, accecamento telecamera, abbagliamento con laser, sfocamento, appannamento, vapore).
- *Conteggio di sagome e persone.*
- *Rilevamento generico di code di persone.*
- *Fault e avaria di sistema* (controlli di funzionalità del sistema di visione intelligente)
- *Lost and Found* (rilevamento di variazione nella immagine, abbandono di oggetti, atti vandalici, asportazione di oggetti).
- *Rilevamento di fumo e fiamme*.
- *Temporizzatore* (calendarizzazione di eventi automatici).
- *Rilevamento di disorientamento della telecamera* rispetto alla posizione originale.
- *Tracking*: inseguimento automatico di oggetti/soggetti in movimento con utilizzo delle coordinate spaziali dei soggetti analizzati.
- *Behaviour*: analisi comportamentale dei soggetti/oggetti ripresi.
- *Counting People*: algoritmo di conteggio delle persone in aree aperte (es. per esterni),

  ed altre specifiche a richiesta.

- Microfoni ambientali stereoscopici integrati da algoritmi di analisi dei suoni ambientali per identificare intensità, direzione, frequenza, caratteristiche dei rumori percepiti.
- Sistema di diffusione vocale completo di altoparlante amplificato per poter riprodurre messaggi preregistrati o fungere da sistema "viva-voce" in collegamento con un centro di

controllo locale o remoto. L'altoparlante funge anche da avvisatore acustico con suono a sirena.

- Rilevatore di temperatura.
- Rilevatore di umidità.
- Rilevatore di movimento a tecnologia PIR infrarosso.
- Rilevatore di movimento a tecnologia Microonde ad effetto doppler.
- Illuminatori a tecnologia LED in vari spettri di emissione (visibile ed invisibile).
- Memoria digitale SD integrata fino a 16 GB per archiviazione eventi con criptografia dei dati.
- Porta Seriale RS 232/485 per collegamento con sottosistemi di sicurezza locali dotati di microprocessore.
- Porta Fast Ethernet 10/100 Mbps per centralizzazione locale e geografica su rete TCP/IP (anche mediante onde convogliate).
- Ingressi ed Uscite digitali a relè per teleattivazioni e collegamento con sensori ausiliari esterni.
- Funzioni di Access Point per sensori ZigBee (IEEE 802.15.4) al fine di comunicare con sensori ambientali ausiliari: il sensore principale può fungere da concentratore di segnali di stato (temperatura, pressione, movimento, velocità, accelerazione, ecc….) di ulteriori sensori installati nell'ambiente circostante e collegati via radio di tipo autoalimentato.
- Il modulo multisensoristica ambientale è predisposto per l'alloggiamento di:
- Modulo cellulare GPRS/EDGE/UMTS;
- Modulo Wi-Fi per centralizzazione a mezzo infrastruttura di rete Wireless;
- Modulo Bluetooth per centralizzazione a mezzo infrastruttura di rete Wireless;
- Modulo antenna RFID per lettura di tag in radiofrequenza per applicazioni di controllo accessi e rilevazione di presenze.

Alimentazione: 12 – 48 Vdc + compatibilità POE (Power Over Ethernet).

Consumo: circa 3 W

Considerati i bassi consumi, è prevista un'alimentazione secondaria di soccorso, mediante batterie

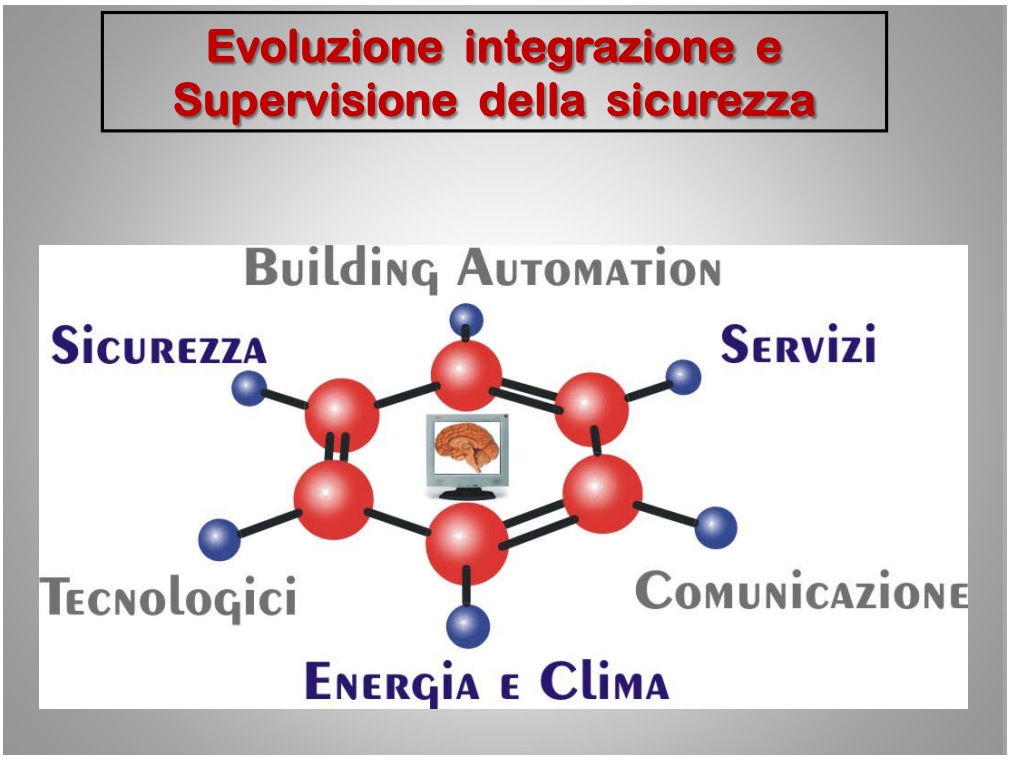
al Litio ricaricabili per garantire il corretto funzionamento del dispositivo. La finestra temporale di

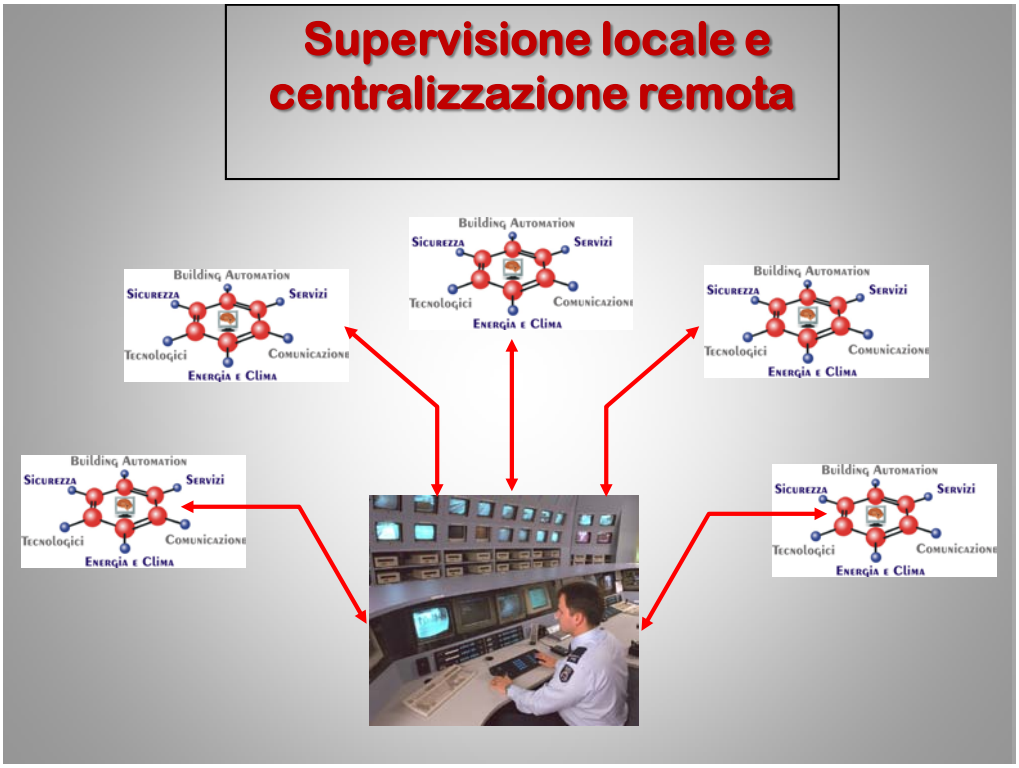
black out dell'alimentazione di rete, è prossima alle 24 ore, mentre l'autonomia

Il dispositivo può essere programmato per funzionare in modalità autonoma (stand-alone) (es. Ethernet, Wi-Fi) oppure centralizzata, gestita da Centrale di Supervisione remota (ADSL, GSM, GPRS, EDGE, UMTS).

Una modalità non esclude l'altra. Anzi, la comunicazione remota delle informazioni deve avvenire, secondo criterio di sicurezza, secondo logica di trasmissione multi-vettore, per disporre di sistema scalabile e ridondato dei mezzi di comunicazione.

Nella schematizzazione che segue, si è cercato di evidenziare la radicale evoluzione concettuale ed applicativa della security, in ambienti interni, che solo pochi produttori stanno perseguendo.





Ogni dispositivo può:

- fungere da stazione Master Ripetitrice per altri sensori presenti nell'edificio, creando architetture a logica ridondata. Ciascun dispositivo può dialogare con altri dispositivi collegati direttamente all'architettura di rete di edificio, costituendo uno o più gruppi logici;
- essere programmato secondo logica a matrice, in modo tale da garantire il massimo grado di personalizzazione delle funzioni mediante algoritmi di analisi per applicazioni di Sicurezza attiva.

Quelli illustrati**,** sono, solo alcuni dei percorsi evolutivi che caratterizzano il settore della sicurezza messo a punto dalle aziende più avanzate operanti a livello mondiale, contrassegnati dalla:

- miniaturizzazione delle tecnologie;
- trasferimento della intelligenza dei sistemi dal centro (centrale locale di gestione) verso il campo (rivelatori intelligenti);
- impiego della comunicazione interfunzionale in campo (logica bus);
- integrazione di più funzioni/servizi all'interno di un unico elemento;

- soluzioni HW e SW ad hoc, per ogni specifica applicazione/esigenza;
- nuovi servizi / applicazioni a supporto dei nuovi prodotti.

Ma, mentre queste caratteristiche sono normalmente riscontrabili nello sviluppo di nuovi apparati nel mondo della telefonia, dell'electronic consumer, dell'entertainment, dell'informatica, nel settore della sicurezza informatica, etc, nel settore della security trovano, purtroppo, scarsa applicazione.

Breve considerazione esemplificativa sull'evoluzione dei telefoni cellulari nel corso degli ultimi 5 anni che può essere sfuggita.

Il cellulare, oggi dispositivo miniaturizzato del costo di 100/150 Euro, si è trasformato in vero e proprio sistema integrato che dispone :

- di un microprocessore di gran lunga molto più potente di una centrale di gestione allarmi;
- è miniaturizzato e può essere inserito ovunque;
- consuma molto meno in termini energetici;
- dispone di capacità video superiori ad una normale telecamera analogica;
- dispone di capacità audio superiori ad un normale sistema citofonico;
- dispone di elevata capacità di memorizzazione di video, audio, eventi;
- dispone di capacità di comunicazione: vocale, SMS, MMS, Email, Push-to-Talk, Dati,Internet, Streaming video/audio, Videochiamate etc;
- dispone di una tastiera di comando multifunzione;
- dispone di un display a colori retroilluminato.

Se esaminiamo il rapporto Costo/Prestazioni con quello di una moderna centrale di gestione locale allarme con tastiera di media grandezza, tale rapporto non regge minimamente, tanto lo sbilanciamento risultante è a favore del telefono cellulare.

Ciò significa che le tecnologie che ci vengono costantemente proposte da molti operatori/costruttori del settore della sicurezza, nazionali e multinazionali sono <u>obsolete ed inadeguate</u> sia sotto il profilo tecnico e sia di quello dei costi.

E, sempre astraendo, dallo specifico settore della protezione museale, occorre, analogicamente rilevare che la tecnologia Wireless propone innovazioni che potrebbero avere una portata inarrestabile rispetto alle modalità di realizzazione attuale delle reti,.

La flessibilità e la mobilità, spesso associate a profili di costo contenuti, hanno un valore che rende l'applicazione delle tecnologie radio particolarmente appetibile rispetto alle alternative in cavo.

Siamo di fronte a prospettive rivoluzionare ed avveniristiche.

Partono dalla sostituzione della cavetteria per il collegamento delle periferiche di un computer ed evolvono verso reti ad-hoc e magliate di sensori. Proseguono con la disponibilità di tecnologie WiMax, Wi-Fi, MobileFi etc. che si basano su reti di accesso a pacchetti studiate per la massima efficienza spettrale.

Sono fronti portatori di radicale mutazione tecnica ed economica degli attuali assetti, prospetticamente incontenibili.

Tecnologie che, se a rischio di sovrapposizione tra loro, rimetteranno anche in discussione le linee di sviluppo e gli equilibri di business dell'ultimo miglio e dell'accesso a larga banda, tradizionalmente basato su tecniche xDSL e di accesso in fibra.