CITEL sicurezza centralizzata supervisione interoperabilità

Milano, Novembre 2014

Presentazione dell'e-Book: l'Ecosistema Centrax di Citel

Quello allegato è il secondo e-book di Citel (il primo è stato pubblicato da OSSIF (ABI) nel 2012 con il titolo "il Sistema Informativo della Sicurezza Fisica in Banca") ed è stato concepito per riempire di contenuti oggettivi i nuovi termini coniati per il mondo della sicurezza fisica professionale in corrispondenza di un cambio di passo dell'innovazione tecnica e funzionale del settore. Siamo infatti in un momento di evoluzione in cui conviene a tutti evitare che l'indeterminatezza iniziale della novità lasci spazio all'ambiguità strumentali degli operatori che si trovano a rincorrere il nuovo corso.

Il nuovo corso è quello che si riassume nel **PSIM** – Physical Security Information Management, una categoria sistemistica classificata da IMS Research-IHS e adottata da Frost & Sullivan alcuni anni fa, senza che per l'Italia questa fosse una novità perché Citel aveva già anticipato di alcuni anni questa innovazione con il sistema Centrax, decidendo di ufficializzarne proprio l'attributo di sistema informatico della sicurezza fisica (SISIF) nel 2009 al Convegno Annuale Banche e Sicurezza.

Per Citel e per la comunità dei suoi utenti è stata una buona notizia il riconoscimento internazionale del concetto PSIM e i requisiti distintivi rispetto ai normali sistemi di centralizzazione allarmi, soprattutto a conferma del fatto che adottando Centrax si erano avviati su una strada maestra in buona compagnia.

È significativo, peraltro, che mentre nessun concorrente si associava a Citel quando anni fa constatava l'avvento di un nuovo sistema informatico dipartimentale, oggi è iniziata la corsa all'annuncio del PSIM anche da parte di aziende che non sembrava avessero né la vocazione né la struttura R&D necessaria per sviluppare, mantenere, evolvere un sistema informatico. È normale che questo accada nel corso delle fasi di transizione, così come è normale che sia la selezione naturale a determinare l'assetto stabilizzato del settore.

In questa fase di fluidità è quindi utile per tutti una informazione basata sui fatti riguardanti i valori di fondo, e questa è l'impostazione di questo e-Book, che per la prima volta fa emergere in modo organico l'Ecosistema di Centrax, cioè quello che c'è dietro un sistema informatico maturo: un mondo di utenti e di fornitori complementari in simbiosi ormai da almeno un decennio per l'evoluzione dei processi gestionali e tecnici della sicurezza fisica, oltretutto con risultati perfettamente corrispondenti ai requisiti PSIM elaborati da IMS Research nei mercati internazionali.

Nils Fredrik Fazzini
Direzione Generale
Citel Spa

n.fazzini@citel.it
www.citel.it

L'ECOSISTEMA CENTRAX

una comunità di soluzioni interattive

Sommario

1. INTRODUZIONE E ASPETTI GENERALI

L'abbinamento dell'attributo "*ecosistema*" ad un sistema informatizzato è diventato un classico tra quei produttori di sistemistica per la sicurezza fisica che possono vantare una diffusione di rilievo nel mercato.

Rispetto al termine "PSIM", che chiunque può attribuire sulla carta al proprio software di supervisione, il termine *ecosistema* è quello più appropriato per far emergere e rendere immediatamente percepibili e dimostrabili i valori reali della soluzione e del suo produttore evitando così scelte influenzate dalle apparenze e dalle affermazioni puramente promozionali.

Quando una comunità di utenti è attiva e propositiva – ma anche numerosa – si possono sviluppare interazioni del produttore del PSIM con gli integratori e con i fornitori di prodotti complementari, con ricadute vantaggiose per tutti i componenti di quello che, una volta raggiunta la massa critica, potrà meritare l'attributo di *ecosistema*.

Un ecosistema è canonico solo se è aperto effettivamente a nuovi membri a tutti i livelli e se è capace di relazionarsi con altri ecosistemi; ecco quindi che l'attributo è meritato solo nei casi di architetture realmente aperte e di dimostrabili politiche di integrazione a fini di interoperabilità da parte del costruttore.

Passando dalle definizioni alla realtà del mercato, Centrax è innegabilmente un caso lampante di ecosistema, perché nei 15 anni di vita della piattaforma, oltre alla continua crescita numerica ha progressivamente innescato un circolo virtuoso alimentato da una comunità di utenti stimolante e proattiva, ma anche da integratori e produttori complementari, con i quali si è istituito un equilibrio stabile grazie a relazioni di convergenza naturale.

Ora che la comunità Centrax ha assunto nel mercato nazionale proporzioni importanti e una riconosciuta leadership per funzionalità e diffusione, è arrivato per Citel il momento di attivare accanto alle attività di laboratorio una specifica azione informativa e organizzativa per alimentare i valori dell'ecosistema con la propagazione organica delle nuove idee, l'incubazione delle innovazioni e la loro traduzione in prodotti e moduli funzionali, senza trascurare contributi alla diffusione di "*best practices*" e modelli procedurali.

Per cominciare, l'ecosistema Centrax è illustrato nel seguito, anche per immagini, con una suddivisione per categorie:

- utilizzatori di Centrax per settore o tipologia di applicazione
- i fornitori complementari integrati a fini di interoperabilità suddivisi per categoria applicativa.

L'ecosistema comprende anche le categorie delle terze parti di progettazione e implementazione di progetti, di installazione e di manutenzione che non trovano spazio in questa pubblicazione. Sono quegli operatori che mantengono il rapporto operativo con i clienti non diretti di Citel presidiando il territorio nazionale. Una categoria importante anche numericamente, in cui spiccano veri e propri partner rispetto ad una maggioranza di operatori indiretti in ruoli di installazione e manutenzione nel territorio.

2. LA COMUNITÀ DEGLI UTENTI CENTRAX

Citel si ritiene fortunata di poter esibire marchi come quelli inquadrati qui sotto e suddivisi per settore. Una comunità come questa ha un potenziale di sviluppo che in ottica PSIM permetterà di continuare a produrre per gli anni a venire innovazione allo stato dell'arte dietro la spinta dell'evoluzione tecnologica e della continua ricerca dell'efficienza dei processi sia nel privato che nel pubblico

2.1 L'ECOSISTEMA CENTRAX - IL RUOLO INNOVATIVO DEGLI UTENTI SUL PIANO STRUTTURALE

Innovazioni strutturali in ambito Centrax che hanno migliorato l'efficienza della sistemistica, delle piattaforme, delle applicazioni e delle comunicazioni; oppure che hanno contribuito al rafforzamento dei requisiti strutturali tipici di un PSIM *I casi riportati sono quelli valorizzati dall'adozione da parte degli utenti innovatori*	
innovazione strutturale (architettura e infrastruttura tecnica)	**Utenti innovatori** **i primi** a proporlo in seno all'ecosistema Centrax e/o a sperimentarlo e/o ad affinarlo e consolidarlo
CEI 79/5-6 (CEI-ABI) al massimo livello di sicurezza (liv. 2) utilizzato come base per l'intera infrastruttura centralizzata	(a valle dell'esperienza pionieristica del Consorzio CICAL-uno): **- BPL (Banco Popolare)** **- MPS** – Monte dei Paschi di Siena
adozione del protocollo aperto CEI-ABI fuori dall'ambito finanziario (per settore)	**COOP** (ambito GDO) **ENI Servizi** (ambito infrastrutture critiche) **Centro Residenziale Visconti** (ambito residenziale) **Milano-3 City** (comprensorio uffici)
primo caso di definizione di uno standard di gestione video unificato multi-marca / modello di DVR, NVR, IP-CAM, VMS correlato agli eventi in ambito Centrax	**- Poste Italiane** – primo tavolo comune (2008) con i principali produttori di DVR e accettazione di regole comuni di integrazione per pop-up unificato con funzioni di visualizzazione e operative indipendenti dal device
primi casi di condivisione di intranet aziendali su base TCP-IP per scopi di sicurezza fisica	**- BPL (Banco Popolare)** **- MPS** – Monte dei Paschi di Siena
innesto organico di applicazioni Android nell'architettura Centrax per soluzioni indossabili	**UBI Sistemi e Servizi (UBISS)**
Video Management System unico alimentato da 10 sistemi compartimentali Centrax con gestione dinamica del parco controllato e dei posti operatore	**Poste Italiane** – VMS unico (joint venture di Citel con la società specializzata Prassel di Roma)

NB.: gli utenti citati non sono tutti quelli che hanno implementato le applicazioni considerate, ma solo quelli che hanno svolto o stanno svolgendo un ruolo di "apripista" rispetto alla comunità di utilizzatori di Centrax o della platea complessiva dell'utenza italiana.

2.2 L'ECOSISTEMA CENTRAX - IL RUOLO INNOVATIVO DEGLI UTENTI SUL PIANO DEI PROCESSI

Innovazioni di processo in ambito Centrax che hanno introdotto nuove applicazioni o ne hanno migliorato l'efficienza; oppure che hanno contribuito al consolidamento delle prestazioni che oggi sono alla base di un PSIM	
innovazione di processo (evoluzione funzionale)	**Utenti evolutivi** **i primi** a proporre in seno all'ecosistema Centrax e/o a sperimentare e/o ad affinare e consolidare nuovi processi funzionali o impianti complessi allo stato dell'arte
Nuovi modelli standard di soluzioni di sicurezza integrata di Palazzi direzionali e Musei	**IntesaSanpaolo** - modello unificato per l'adeguamento della sicurezza dei grandi edifici con integrazione tra eventi e VMS e ricorso a supervisore nazionale in casi programmati **Poste Italiane** – gestione integrata di un complesso multi-edificio mediante Centrale di gestione eventi di Citel con prevalenza di connessioni LAN per la sensoristica remota; integrazione di nuova sistemistica Kaba per il controllo degli accessi, di centraline antincendio Notifier,
Nuovi modelli combinati di protezione di campi di produzione di energia verde con integrazione di allarmi e video	**ENEL Green Power** – protezione di perimetri chilometrici di campi fotovoltaici, eolici e idroelettrici con tecnologie diverse secondo dimensioni e morfologia. Gestione integrata allarmi-video e accessi con nuova centralizzazione bidirezionale su rete IP accentrata in Control Room nazionale
Nuovi modelli avanzati di telegestione di infrastrutture critiche	**SNAM Rete Gas** (in corso) – protezione al massimo livello per infrastrutture critiche (stazioni di compressione del gas nella rete nazionale) Telegestione integrale, comprese le funzioni di tele-accoglienza multimediale, integrazione del controllo accessi Honeywell
Nuove modalità di controllo dei consumi e dei malfunzionamenti di impianti elettrici in siti periferici	**Poste Italiane -** controllo di molte centinaia di uffici remoti con soluzione minimale in campo e utilizzo di un nuovo modulo software di Centrax con smistamento dei segnali e degli eventi su posti di lavoro separati dalla sicurezza. Trasmissione a costo zero
Protezione dei caveau con nuove soluzioni integrate immuni anche all'infedeltà interna o esterna	**- IntesaSanpaolo** – info non divulgabili **- Banco di Desio e della Brianza** – info non divulgabili
Integrazione tra sicurezza e safety con interazione tra allarmi malore / aggressione e attivazione sblocchi ingresso per soccorsi. Utilizzo bidirezionale di smartwatch per avvisi e allarmi	**- UBISS** – applicazione centralizzata per siti mono-operatore concepita per avere maggiori garanzie rispetto al radiocomando a collare riguardo al fatto che sia stato indossato; anche per la possibilità di rilevare posizione e vitalità della persona e l'invio di messaggi direttamente sull'orologio. Possibilità di espandere il raggio d'azione in sedi di maggiori dimensioni in cui il dipendente può rimanere solo oltre l'orario di lavoro.
Soluzione di Guardia Remota abbinata a più palinsesti promozionali multimediali	**- Cariparma** **- Barklays (maincontractor: Axitea)** **- UBI**
Guardia remota multimediale con video bidirezionale e voice over-IP	**- Cariparma** **- Deutsche Bank (maicontractor: Sicuritalia)**
Elaborazione e correlazione di input diversi per la rilevazione precoce di rapine e attacchi ad ATM	**Cariparma, Deutsche Bank, Poste, UBI** – integrazione di input e output diversificati, compresa l'analisi dell'immagine, la connessione a sistemi informatici per generare eventi e livelli di rischio tali da provocare l'attivazione automatica locale di misure dissuasive o di contenimento del danno

NB.: gli utenti citati non sono necessariamente gli unici ad utilizzare le innovazioni di processo riportate, ma sono quelli che hanno svolto o stanno svolgendo un ruolo di spinta alla realizzazione da parte di Citel di quelle innovazioni o miglioramenti funzionali nell'ambito di Centrax. Una casistica più completa verrà pubblicata a breve nella newsletter Securindex.

3. L'ECOSISTEMA CENTRAX – I FORNITORI COMPLEMENTARI E IL RUOLO NELL'INTEGRAZIONE

Il ruolo dei produttori complementari (talvolta concorrenti di Citel) è più importante per l'ecosistema Centrax di quanto non si possa pensare: con la loro collaborazione, dovuta a un interesse spontaneo o alla spinta della grande utenza, l'ecosistema è arrivato a integrare la maggioranza dei fornitori specializzati che abbiano un peso nel mercato italiano.

La spinta della grande utenza nazionale è stata in ogni caso decisiva, una volta scoperto che il sistema integrato non era necessariamente il sistema del fornitore unico e che esisteva una via che permetteva senza compromessi, di evolvere la propria impiantistica innestandola in una nuova sistemistica multifunzionale e aperta:

- salvaguardando l'impiantistica esistente evitandone la sostituzione e tutelando gli investimenti
- non sostenendo nell'immediato costi eventualmente rinviabili
- mantenendo stabilmente anche per il futuro la libertà di scelta di fornitori e prodotti senza costrizioni indotte dal sistema potendo mantenere i fornitori di fiducia di singoli prodotti e di servizi.

Il rapporto con i fornitori complementari in ambito Centrax può assumere varie forme e intensità che variano in funzione della dinamica evolutiva del settore specialistico di appartenenza e delle spinte dell'utenza motivata dai vantaggi della combinazione.

La classificazione che Citel ha adottato per una mappatura del fenomeno è la seguente:

Ambito dell'integrazione:

- **soluzioni di videosorveglianza**
- **dispositivi di trasmissione allarmi su reti tradizionali**
- **apparati di protezione / erogazione di denaro contante**
- **sistemi di gestione locali self-service e locali sicuri di carico/scarico valori**
- **dispositivi di controllo consumi e monitoraggio impianti**
- **soluzioni per la safety dei lavoratori**

e, per ogni ambito di integrazione, **l'intensità della richiesta e la qualità del risultato**, espressi dai seguenti fattori:

- **l'interesse del mercato e la richiesta**
- **la disponibilità e la collaborazione delle terze parti**
- **le innovazioni introdotte con l'integrazione.**
- **il livello raggiunto dalle applicazioni**

Nelle pagine successive i fornitori complementari coinvolti nei processi di integrazione in ambito Centrax sono raggruppati in categorie, e per ciascuna di esse sono riportate le risultanze riguardo alla frequenza relativa dei casi di integrazione, al livello di "intensità" tendenziale e, infine, alle eventuali innovazione di processo di gestione della sicurezza che esse hanno generato.

3.1 APPARATI E SISTEMI DI VIDEOSORVEGLIANZA

Integrazione con apparati di videosorveglianza			
via *SDK o protocollo* con apparati DVR / NVR / IP Camera			
AVIGILON THE BEST EVIDENCE™	aitek	alhua TECHNOLOGY	AXIS
BETTINI VIDEO & SECURITY TECHNOLOGY	BOSCH	CoMETA	ELMO Global Security Solutions
EUKLIS	EverFocus	GANZ	GeoVision
HIKVISION	HUNT ELECTRONIC	INSTEK DIGITAL	MARCH An Infinova Company
mesa	MOBOTIX	RTM	SAMSUNG
SONY make.believe	sightlogix	SYAC-TB	STANLEY Security Solutions
United Technologies	TELEDATA	Visimetrics	

integrazioni con VMS – Video Management Systems	
via *SDK o protocollo* con software e sistemi	
AVIGILON THE BEST EVIDENCE™	Genetec
milestone	PRASSEL Projects & Assets Leading

integrazioni con moduli di Video Analytics	
via *SDK* o *protocollo* a bordo telecamera o apparati e sistemi	
aimetis	COGNIMATICS
sightlogix	TechnoAware TECHNOLOGIES FOR AMBIENT INTELLIGENCE
funzioni comuni e inoltre: camouflage, face detection, face recognition, gate flow, heat map	

integrazioni con sistemi di video-citofonia	
via *SDK* e protocollo SIP	
2N ITALIA	COMMEND

L'interesse del mercato e la richiesta

Si tratta dell'integrazione più comune e più ovvia: quella tra la segnalazione dell'evento da sensoristica (intrusione, accessi) e l'attivazione di una video-ispezione istantanea con una o più telecamere correlate, in tempo reale o dal pregresso.

I vantaggi che questa funzionalità comporta sono facilmente intuibili:
- il minimo ricorso all'intervento umano sul posto, limitato ai soli casi di effettiva necessità
- la possibilità di decidere le modalità di intervento più mirate e appropriate in base all'osservazione della scena
- la possibilità di consegnare all'attenzione di un operatore responsabilizzato soltanto immagini pertinenti in una sorta di cruscotto, abbandonando così la dispersione dell'attenzione e l'inaccuratezza del video-controllo ciclato su maxi-schermi

La richiesta a Citel è iniziata dieci anni orsono, ha dato luogo alla prima standardizzazione di un cruscotto pop-up indipendente da costruttori e modelli di DVR (grazie al ruolo iniziale di Poste Italiane) ed è una costante delle forniture Centrax.

La disponibilità e la collaborazione delle terze parti

La disponibilità dei costruttori di soluzioni video a fornire specifiche e strumenti di integrazione (tipicamente SDK), alle origini data col contagocce, oggi è semplicemente la regola. L'utenza professionale avveduta non accetta infatti di acquistare prodotti senza avere preventivamente verificato – anche con il supporto di Citel – che siano integrabili nell'ambito di un sistema più articolato.

Quanto al grado di collaborazione dell'eventuale importatore italiano di prodotti esteri, esso dipende essenzialmente dalla sua struttura tecnica e dalla sua capacità di fornire eventuale assistenza all'attività di integrazione – se necessario – o di fare almeno da tramite rispetto al fabbricante e al suo laboratorio, spesso in estremo Oriente.

Le innovazioni introdotte con l'integrazione

Sono numerose e non si fermano al software di supervisione Centrax ma interessano i diversi livelli dell'architettura di sistema; di seguito ci si limita a riportare i titoli delle innovazioni di prodotto e di processo realizzate e in corso:
- le telecamere come sensori nell'ambito di una centralina di gestione eventi all-in-one e multimediale, sia su base motion detection che video analytics
- il video bidirezionale multimediale per soluzioni avanzate antirapina
- l'integrazione stretta tra Sistema di Gestione eventi e VMS – Video Management System
- l'utilizzo combinato della video analisi e del video bidirezionale sia per la sicurezza fisica sia che per funzioni di safety e di marketing
- nuove applicazioni centralizzate per nuove forme di servizi di vigilanza.

Il livello raggiunto dalle applicazioni

Praticamente tutti i Centrax forniti negli ultimi anni vengono richiesti con le funzioni complementari di integrazione con le piattaforme video. Il livello di integrazione tende ad essere sfruttato in modo che tutte le funzioni utili siano disponibili sui posti di lavoro Centrax per ottenere la massima efficacia con operazioni in tempo reale, proceduralizzate e tracciate

Citel quindi non si è fermata all'integrazione di DVR/NVR e IP-CAM in Centrax, ma ha sviluppato anche l'interazione Server – Server per i VMS più diffusi nel mercato e per i software di video-analisi sia in versione generalista che specializzata per determinati tipi di eventi.

Il livello delle applicazioni di sicurezza combinate con il video ha avuto un ulteriore impulso nelle varianti multimediali in abbinamento con il modulo Contax di telefonia over-IP e con il modulo Videoduplex di video bi-direzionale integrato con la fonia mono o bidirezionale.

L'integrazione della video-citofonia over-IP è un caso di multifunzionalità del sistema Centrax, per servizi che si aggiungono a quelli di sicurezza fisica, estendendosi alla tele-accoglienza di visitatori e lavoratori esterni in combinazione con il controllo accessi centralizzato.

3.2 SISTEMI DI ALLARME

Nel trattarne l'integrazione in ambito Centrax, i sistemi di allarme sono stati suddivisi in tre aree:

- **dispositivi e sistemi di teleallarmi**
- **controllo perimetrale**
- **centrali di allarme – intrusione e incendio**

3.2.1 DISPOSITIVI E SISTEMI DI TELEALLARMI

l'interesse del mercato e la richiesta

Il mercato è storicamente quello dei sistemi di teleallarme utilizzati dalla generalità degli Istituti di Vigilanza per i servizi tradizionali erogati all'utenza domestica, agli esercizi commerciali e alle micro-imprese, cioè ad utenti finali di servizi con esigenze non particolarmente sofisticate.

In questo settore di mercato, la sistemistica tipica prevede un centro di gestione progettato per applicazioni di vigilanza che riceve allarmi:

- codificati con protocollo proprietario e chiuso, eventualmente cifrato, a bordo di dispositivi periferici *obbligati* (solitamente trasmettitori abbinati a una centrale di allarme) tipicamente su reti GSM/GPRS o Radio
- oppure usando al centro apparati ricevitori *multiprotocollo* di mercato, tipicamente per reti telefoniche PSTN, in grado di ricevere protocolli pubblici o comunque aperti immessi in rete da trasmettitori accoppiati a una centrale di allarme oppure direttamente da quest'ultima.

La richiesta di integrazione nell'ambito di un sistema unico di gestione centralizzata, in grado di gestire una pluralità di protocolli e funzionalità che andassero oltre quelle tipiche della vigilanza, limitata a pochi casi nel passato, ha avuto un'accelerazione in anni recenti, quando il settore della vigilanza si è ristrutturato con l'accorpamento delle control room e con la concentrazione societaria di istituti dotati di tecnologie incompatibili tra loro, ma anche con la necessità di ogni impresa di vigilanza di competere nel mercato anche sul piano dell'innovazione dei servizi.

la disponibilità e la collaborazione delle terze parti

In generale si può affermare che la disponibilità è minima quando il produttore dispone di un proprio sistema di centralizzazione con protocollo proprietario che considera strategico a fini di fatturato e strumentale alla fidelizzazione dell'utente Vigilanza, indotto ad utilizzare un parco periferiche monomarca. Le eccezioni a questi meccanismi sono legate alla forza della pressione commerciale che il cliente può esercitare sul fornitore per ottenere un trattamento diverso.

Un caso significativo in positivo si è verificato con l'integrazione Server-Server tra Centrax e uno dei sistemi leader tra quelli centralizzati di tipo proprietario, permettendo all'istituto di vigilanza di avere posti operatore omogenei a fronte di una pluralità di vettori, protocolli, dispositivi, legati alla storia e alla varietà delle esigenze utenti.

Sempre in generale, la disponibilità è massima nel caso opposto, quando per il costruttore le periferiche sono un business in sé e la strategia scelta per renderle concorrenziali è quella dell'apertura architetturale mediante un protocollo pubblico o proprietario ma comunque disponibile per l'integrazione libera.

Le integrazioni effettuate nell'ambito dell'ecosistema Centrax (i loghi nei riquadri in figura) sono avvenute interfacciando i protocolli messi a disposizione di Citel dai costruttori dei singoli trasmettitori, oppure i protocolli di integrazione degli apparati ricevitori multiprotocollo che operano come Front-End in grado di riconoscere e transcodificare gli allarmi di un network eterogeneo di trasmettitori o centrali di allarme.

Le innovazioni introdotte con l'integrazione.

Le integrazioni di teleallarmi in Centrax non hanno portato innovazioni tecniche degne di nota: i protocolli pubblici sono un valore in sé in quanto disponibili, ma se sono monodirezionali, non protetti e basati su reti PSTN facili da sabotare, lasciano spazio alle reti radio e alla telefonia cellulare anche se con protocolli e crittografia proprietari.

Un caso interessante di innovazione funzionale – il primo in assoluto – è quello citato più sopra di interazione con Centrax Server-Server da parte di un fornitore leader di mercato di sistemi su base GPRS . Questo caso potrebbe aprire la strada a nuovi modelli di servizi all'utente

Il livello raggiunto dalle applicazioni

Nella misura in cui i Teleallarmi sono monodirezionali, non protetti e associati a reti di comunicazione commutate, è possibile che le applicazioni non possono evolvere oltre un certo limite. Livelli funzionali superiori sono necessariamente condizionati all'utilizzo delle moderne reti digitali.

Peraltro, va ricordato che la ricezione dei teleallarmi si aggiunge a tutte le altre possibili nell'ambito di una installazione Centrax, con una varietà di vettori e protocolli che rispetto ai quali quelli dei teleallarmi monodirezionali sono solo il primo gradino.

3.2.2 SISTEMI DI CONTROLLO PERIMETRALE

l'interesse del mercato e la richiesta

Si tratta dell'integrazione più comune e più ovvia: quella tra la segnalazione dell'evento da sensoristica in campo e l'attivazione di una video-ispezione istantanea con una o più telecamere correlate, in tempo reale o dal pregresso, che nella maggior parte dei casi evita un intervento a vuoto, oltretutto in siti remoti, per scoprire che si tratta di falsi allarmi.

I vantaggi che questa funzionalità comporta – in abbinamento con le funzioni di classe PSIM di Centrax sono facilmente intuibili:
- il ricorso all'intervento umano sul posto limitato ai soli casi di effettiva necessità
- la possibilità di tracciare e documentare l'intervento o le ragioni del non-intervento

la disponibilità e la collaborazione delle terze parti

La collaborazione non è mai mancata, e si è tradotta in integrazioni basate quasi sempre su protocollo o SDK.

Le innovazioni introdotte con l'integrazione.

Sono stati raggiunti i vertici dello stato dell'arte in applicazioni civili grazie all'integrazione con la centrale Novax di gestione eventi da correlazioni multiple (protocolli e segnali), integrata via LAN:
- l'acquisizione via protocollo da parte della centrale di gestione eventi dei singoli allarmi generati e filtrati dalla video-analisi
- la correlazione tra segnalazioni via protocollo e input tradizionali ai fini della generazione di eventi
- la grafica di visualizzazione su posto operatore degli spostamenti dell'intruso in condizioni di totale oscurità anche con l'utilizzo delle coordinate geografiche dei singoli pixel su sfondi grafici geo-referenziati
- l'impiantistica semplificata interamente over-IP con moduli intelligenti monitorabili e riconfigurabili da centro
- la possibilità di autorizzare da control room (o da dispositivi mobili) l'accesso autorizzato al sito di lavoratori e manutentori per l'esecuzione di operazioni senza accompagnamento.

Il livello raggiunto dalle applicazioni

Il livello raggiunto grazie alle suddette innovazioni ha toccato i massimi consentiti dallo stato dell'arte nei limiti di costi sostenibili in applicazioni civili. E a beneficiarne, nei casi di integrazione stretta con Centrax ai fini della telegestione è stata soprattutto l'efficienza dell'operatività:
- riduzione o annullamento degli interventi inutili sul posto per falsi allarmi
- invio tempestivo delle risorse di intervento appropriate sul punto esatto dell'evento
- interventi di manutenzione gestiti secondo scelte di efficienza con:
  - tele-diagnosi ai fini dell'organizzazione razionale degli interventi
  - tele-interventi di manutenzione, ove possibile mediante riconfigurazione da control room
  - tele-azionamenti di disattivazione temporanea per interventi differiti o cumulati

3.2.3 CENTRALI DI ALLARME INTRUSIONE E INCENDIO

l'interesse del mercato e la richiesta

Premessa: le centrali antintrusione considerate sono quelle tipicamente connesse su reti LAN/WAN con protocolli bidirezionali che permettono una telegestione da Control Room orientata agli "eventi", non ai semplici "allarmi" per i quali si utilizzano invece i dispositivi trattati in precedenza come "teleallarmi".

L'interesse dell'utenza per la centralizzazione di impianti con centrali di allarme di produttori qualsiasi è quasi sempre il motivo dell'adozione di Centrax, soprattutto se si sente la necessità:
1. di gestire in maniera normalizzata e unificata un certo numero di propri siti dotati di centrali anti-intrusione e antincendio, indipendentemente da marca, modello, epoca del loro acquisto; è il caso tipico delle banche, del retail, ma anche di grandi imprese multi-sito;
2. di passare alla gestione integrata e supervisionata di un impianto, singolo ma complesso e articolato, con necessità di interazione tra apparati e sistemi di produttori diversi.

Nel caso 1 l'esigenza è decisamente sentita da tempo ed è tipica di chi utilizza una Control Room interna di telegestione della sicurezza; meno sentita per chi è portato ad affidarsi su basi locali alle control room di società di security che forniscono anche il servizio di pronto intervento.

Nel caso 2, l'esigenza si è consolidata solo di recente; in passato il caso del supervisore unificato nel singolo edificio o non si poneva, lasciando separati i diversi sistemi, oppure l'integrazione avveniva nell'ambito della cosiddetta Building Automation in ambito rigorosamente chiuso mono-fornitore e ovviamente sbilanciato verso i tecnologici. Nell'ultimo decennio, però, quella chiusura protettiva, palesemente antistorica, ha portato – proprio nei grandi edifici e infrastrutture – alla crescita della domanda di una gestione separata della sicurezza fisica, con la richiesta di un PSIM basato sull'interoperabilità con accessi, video, safety ed emergenze a partire dalla centrale di allarme del sito, quasi sempre da preservare per non dover affrontare costosi rifacimenti dell'impiantistica antintrusione.

In entrambi i casi emerge comunque l'interesse dell'utenza ad ottenere l'integrazione con le centrali di allarme preesistenti per non rimettere mano agli impianti o per mantenere i fornitori abituali di prodotti e servizi: e questo spiega il numero elevato delle centrali di allarme, intrusione e incendio in fascia media e alta, che sono state integrate in Centrax.

la disponibilità e la collaborazione delle terze parti

Le centrali con protocollo proprietario integrate in Centrax sono tra le più diffuse nella fascia media e alta del mercato italiano. La disponibilità a fornire il protocollo è nettamente migliorata nel tempo grazie alla *moral suasion* esercitata dai grandi utenti di Centrax la cui massa critica ha dimostrato tutto il suo peso anche in questo settore, da sempre il più chiuso e protetto.

Le innovazioni introdotte con l'integrazione.

In una infrastruttura aziendale di sicurezza fisica la centrale di allarme è un elemento di condizionamento rilevante per il numero e l'importanza delle segnalazioni che gestisce, per i comandi che esegue e per i costi che implicherebbe una sua sostituzione. Pertanto l'alto numero di casi di integrazione multifornitore in ambito Centrax rappresenta – di per sé – l'origine di tutte le innovazioni di sistema o funzionali, essendo quella che ha fatto saltare l'assuefazione alle architetture chiuse a protezione dei *prodotti della casa* e la rassegnazione alle *non* scelte dei singoli moduli all'interno del sistema. È stato quello il passaggio chiave che ha portato al ripristino della competizione e della regola aurea dei sistemi aperti: la valorizzazione del pregi dei singoli moduli indipendentemente dal costruttore del sistema di supervisione, quindi la meritocrazia e l'innovazione nel suo corollario.

L'innovazione è consistita nella possibilità di trattare i segnali di singoli sensori in ingresso e di singoli attuatori in uscita senza essere costretti ad avere un unico costruttore sia per il centro che per la periferia. Una innovazione determinante per rendere accessibile il livello applicativo della gestione del singolo sensore riservato ai sistemi chiusi monomarca.

Il livello raggiunto dalle applicazioni

L'innovazione appena trattata porta alla possibilità di ottenere in un ambito aperto e multifornitore prestazioni avanzate di gestione da supervisore di solito riservate ai sistemi chiusi monomarca che prevedono la gestione per eventi trattando i segnali di ogni singolo sensore e l'azionamento di ogni singolo attuatore. Tale possibilità si può tradurre – tramite configurazione per eventi – in interventi appropriati, tempestivi, efficienti, documentati, grazie alla possibilità di configurare processi di gestione con, ad esempio:

- la precisa rilevazione spaziale dell'evento e la possibilità di puntare strumenti di verifica associati, come la telecamera abbinata allo spazio di interesse
- la possibilità di correlare altri segnali per determinare con precisione il tipo di evento, la sua attendibilità, il suo decorso a fini di *situation management*, l'abbinamento alle procedure di intervento, la generazione automatico di un reporting accurato

ottenendo quindi – su un piano più generale – di passare dalla semplice centralizzazione allarmi alla telegestione degli eventi senza rinunciare ai benefici dell'architettura aperta.

3.3 I SISTEMI DI CONTROLLO ACCESSI E VARCHI

l'interesse del mercato e la richiesta

Nell'esperienza di Citel l'integrazione del Controllo Accessi in una sistemistica di supervisione multifunzionale è stata sporadica nel passato e semplicistica nella realizzazione, del tipo: un allarme di varco = un contatto per un ingresso su una centrale di allarme. Oppure due centralizzazioni distinte e separate con posti operatore specializzati nella control room del grande utente.

Negli anni recenti, però, la richiesta di integrazione è cresciuta sia per numero di casi che per livello di interoperabilità, e lo dimostrano il numero e il peso dei marchi nella figura, in larga parte integrati di recente in ambito Centrax.

E con l'integrazione cresce il livello qualitativo delle applicazioni, che vanno ormai ben oltre il consenso all'apertura di un varco, allargandosi a un ambito più generale della rilevazione del passaggio e della presenza. Grazie alle nuove tecniche di rilevazione di prossimità nelle sue varie forme, oggi si possono infatti rilevare, correlare e gestire anche il transito in genere e il tracciamento del passaggio lungo percorsi monitorati, aprendo alla telegestione nuovi campi di applicazione.

la disponibilità e la collaborazione delle terze parti

La collaborazione dei costruttori alla fine non è mai mancata, avendo tutti interesse a partecipare a progetti di integrazione, e si è tradotta in interoperabilità basata sempre su protocollo o SDK.

Le innovazioni introdotte con l'integrazione.

L'innovazione tecnico/impiantistica in ambiente multifornitore si è tradotta nel passaggio dalle connessioni con contatti on/off dei *controller* di varco del passato (e delle informazioni elementari che essi fornivano) all'interazione con la centrale di gestione eventi Novax o direttamente con il Centrax via LAN o bus seriale:

- con una struttura dell'impianto più compatta, protetta e tele-monitorabile
- con la disponibilità di un protocollo applicativo bidirezionale basato su un set completo di informazioni in entrata e di comandi in uscita oltre alla diagnostica centralizzata di funzionamento.

Le innovazioni funzionali hanno origine dalla possibilità di poter utilizzare tutto il set di segnali e comandi del protocollo del costruttore per poter effettuare una telegestione basata sulla percezione completa e tempestiva dell'evento e sull'attivazione delle misure congruenti.

In particolare sono stati raggiunti i massimi livelli funzionali nella gestione da supervisore anche grazie all'integrazione con la centrale di gestione eventi (Novax o altre marche con protocollo CEI 79/5-6):

- l'acquisizione via protocollo da parte della centrale di gestione eventi dei singoli allarmi di varco
- la correlazione tra segnalazioni via protocollo e input tradizionali ai fini della generazione di eventi corredati da una informativa completa
- la grafica di visualizzazione su posto operatore della posizione del varco e del contesto pertinente
- la possibilità di autorizzare da control room (o da dispositivi mobili) l'accesso al sito di lavoratori, manutentori e visitatori con profili di accesso personalizzati anche senza accompagnamento su percorsi obbligati

- la possibilità di una gestione centralizzata e unitaria anche in un contesto multi-sito con dotazioni eterogenee.

Il livello raggiunto dalle applicazioni – controllo accessi

Il livello applicativo raggiunto grazie alle suddette innovazioni ha toccato i massimi consentiti dallo stato dell'arte in applicazioni civili. A beneficiarne, nei casi di integrazione stretta con Centrax ai fini della tele-gestione sono state soprattutto l'efficienza dell'operatività, sia nel controllo accessi e varchi che nelle applicazioni di monitoraggio:

- riduzione dei costi di gestione dei servizi di accoglienza e presidio tramite automatismi locali e servizi centralizzati
- riduzione degli interventi inutili sul posto per false emergenze
- tele-interventi di manutenzione, ove possibile mediante riconfigurazione da remoto

3.4 PROTEZIONE DEL CONTANTE E DEI VALORI IN GENERE.

l'interesse del mercato e la richiesta

Nel settore bancario l'integrazione di dispositivi direttamente o indirettamente riferibili alla protezione del contante è cresciuta costantemente negli anni recenti, in funzione dell'alto rischio rapina (sia in termini economici che di rischio safety per i dipendenti) e di attacco agli ATM, e per la contestuale necessità di individuare nuove soluzioni per abbattere i rilevanti costi ricorrenti del piantonamento armato delle filiali.

La richiesta a Citel è stata pertanto quella di studiare soluzioni efficienti, aperte a varianti banca per banca, compatibili con le dotazioni preesistenti, rassicuranti per i dipendenti, non invasive per i clienti e ad alto effetto dissuasivo per i malintenzionati.

Richieste che potevano essere soddisfatte solo mettendo in campo un elevato grado di integrazione di sistema tra vari dispositivi nella filiale – sia di protezione del contante che di accesso alla filiale o alle aree di self–banking – oltre a soluzioni di telegestione da Control Room, nella fattispecie interattiva e multimediale.

la disponibilità e la collaborazione delle terze parti

Negli anni recenti la collaborazione dei costruttori ai fini dell'integrazione non è mancata, avendo ormai tutti interesse a partecipare a progetti di integrazione importanti presso la grande utenza bancaria, e si è tradotta attualmente nell'interoperabilità diffusa, basata sempre su protocollo o SDK.

Va peraltro ricordato che in passato la disponibilità è stata spesso negata per questioni di certificazione di settore o a difesa dei contratti di servizio post-vendita.

le innovazioni introdotte con l'integrazione

L'innovazione più evidente ottenuta con l'integrazione è stata proprio un livello di interazione mai ottenuto prima in filiali bancarie tra apparati locali (erogatori, serrature, bussole, ecc.) fino al punto di poter inserire – per fare un esempio – nella configurazione dei pesi in un evento anche la somma in contanti contenuta nell'erogatore in un certo istante. Con questo permettendo di gestire come evento anche il superamento di soglie di rischio in base a criteri oggettivi e poter "dosare" la videosorveglianza da centro in funzione del grado di rischio del momento.

È stato quindi nel corso dei progetti ad alta integrazione che si è manifestata in modo evidente la differenza tra una normale centrale di allarme e una centrale di gestione eventi, dove quest'ultima (la Novax di Citel in particolare) ha permesso le integrazioni locali interamente su base over-IP con interoperabilità ottenuta via protocollo rispetto ad apparati funzionalmente diversi, valutando l'evento (o il livello di rischio) in base alla programmazione sulla centrale di ingressi, con pesi relativi e tempi di integrazione, per poi generare situazioni da gestire:

- modulando le richieste di monitoraggio e dissuasione al sistema centrale, anche interattive e multimediali
- intervenendo con comandi ai moduli locali

Modalità ottenibili solo con un elevato grado di integrazione di sistema tra vari dispositivi nella filiale – sia di protezione del contante che di accesso alla filiale o alle aree di self–banking – oltre a soluzioni di telegestione da Control Room, nella fattispecie interattiva e multimediale.

Altro aspetto decisamente innovativo è il fatto che le integrazioni, anche tecnicamente complesse, sono state rese modulari, normalizzate, allocate in un catalogo di oggetti software, e quindi facilmente implementabili, manutenibili e in definitiva scalabili e sostenibili per utenti di ogni dimensione.

La normalizzazione di *soluzioni* integrate ha avuto un effetto importante sulla concezione stessa della videosorveglianza da Control Room, con la possibilità di superare finalmente il cliché della parete occupata da un video-wall e operatori apparentemente intenti a osservarlo, per passare a forme più razionali, mirate, efficienti, tracciabili, in funzione dell'interazione con gli apparati remoti, ottenendo:

- l'abbinamento contestualizzabile al livello di rischio, all'evento, alla situazione
- la possibilità di fornire servizi di video-ispezione on-demand dal sito remoto
- di arrivare a combinare messaggistica di marketing a quella di sicurezza in condizioni di assenza di rischio

Il livello raggiunto dalle applicazioni – EROGAZIONE E GESTIONE DEL CONTANTE + MECCATRONICA

Le applicazioni di cosiddetta "Guardia Virtuale" o (più propriamente) "Guardia Remota" non sono una novità: risalgono a più di 10 anni fa e venivano gestite dalla vigilanza su linee ISDN sulla base di un video-rolling in control room e la visibilità della guardia su un monitor in filiale.

Questo tipo di applicazioni primordiali ha fatto un notevole salto di qualità grazie al livello di integrazione che è stato possibile raggiungere nel rapporto con gli apparati di erogazione del contante e con i dispositivi di meccatronica, consentendo:

- di ottenere informazioni sullo stato dei mezzi forti, sul denaro presente negli erogatori e metterle a disposizione dello scenario e contribuire a generare il livello di rischio in un certo istante
- di attivare in automatico o da consenso comandi su serrature ed erogatori per limitare il danno o anche per autorizzare un'operazione

Ma anche – e soprattutto – di inserire gli apparati e dispositivi in questione in un contesto di governo locale senza passare da costosi progetti ad-hoc come accaduto in passato né implementando cablaggi complessi, funzioni e interazioni personalizzate, manutenibili solo da chi li aveva realizzati. Al livello qualitativo delle applicazioni hanno quindi contribuito la normalizzazione delle soluzioni, la riproducibilità e quindi la sostenibilità dell'investimento e del TCO.

Il livello raggiunto dalle applicazioni – ATM E AREE SELF-BANKING

Lo scopo di questo tipo di applicazioni è di ottenere dei risultati essenziali: minimizzare sia il tempo di rilevazione che la possibilità di creare un disagio alla clientela. E anche in questo ambito l'interazione correlata tra tecniche diverse è il metodo classico per arrivare allo scopo.

Allo stato attuale l'integrazione è arrivata a coinvolgere ai fini della determinazione dell'evento, oltre alla sensoristica tradizionale antintrusione e antiskimming :

- varie funzioni specifiche di video-analisi, con la novità dei moduli software a bordo delle telecamere IP di Axis piuttosto che su piattaforme server
- gli Agent software dei produttori di ATM, in grado di rilevare anomalie di funzionamento dell'ATM (normalmente ricollegabili allo skimming) comandando blocchi operativi o generando una segnalazione associabile alla videosorveglianza e/o alla video-analisi
- il modulo di correlazione e trasmissione a bordo della centrale di gestione eventi della filiale o dedicato allo scopo, comunque in grado di:
  - ricevere direttamente da protocollo i segnali o gli eventi dei moduli di video-analisi e/o dell'Agent o della sensoristica comune
  - attivare automaticamente la reazione prevista oppure presentare immediatamente e contemporaneamente all'operatore tutti gli strumenti a video per dare o meno il consenso tempestivo ad attivazioni di inibizione dell'attacco come nebbiogeni, sirene
  - permettere all'operatore di gestire casi dubbi e casi umani con interazione di tipo video-citofonico

Anche in questo caso l'integrazione è stata gestita da Citel con la disponibilità di una biblioteca di moduli di integrazione e di modelli applicativi facilmente adottabili per sperimentazione preliminare e per impianti pilota di affinamento applicativo.

Il livello raggiunto dalle applicazioni – BUSSOLE e PORTE INTERBLOCCATE

Le applicazioni in questa area hanno coperto fondamentalmente la diagnostica con la segnalazione di malfunzionamenti da protocollo o da uscite digitali oppure comandi generali di blocco/sblocco per situazioni di pericolo o di emergenza.

3.5 SISTEMI GESTIONALI

integrazioni con sistemi centralizzati di sicurezza / safety / ticketing		
via *SDK* o *protocollo* con applicazioni software e sistemi		
SELEX Sistemi Integrati	Telespazio	Posteitaliane
BINKA	**EXPLOR**	**GUP**
NTT DATA	bmcsoftware	Bassilichi
data mining / analysis	**REMEDY ticketing**	**ticketing**

l'interesse del mercato e la richiesta

Soprattutto nelle installazioni di dimensioni consistenti o in organizzazioni complesse emerge la richiesta di interagire con altri sistemi informatici per uno scambio dati in ingresso e/o in uscita rispetto alle applicazioni di Centrax, dando luogo quasi sempre ad applicazioni interattive Server-Server come nei casi seguenti, alcuni occasionali altri di tipo organico e ripetitivo:
- trasmissione automatica al sistema di ticketing del manutentore di richieste di intervento contenenti la diagnostica di guasti in campo trattati da Centrax
- raccordo con sistemi informatici gestionali dell'utente o di suoi fornitori, come nel caso di GUP di Poste e Binka di Selex, utilizzati per ottenere, caricare e aggiornare dati anagrafici di referenti o impianti negli uffici periferici
- di sistemi specializzati di comunicazione satellitare come nel caso di Explor di Telespazio
- di moduli, su progetto, di analisi dei dati storici a fini predittivi

la disponibilità e la collaborazione delle terze parti

Nessun problema di disponibilità a fronte delle richieste di grandi utenti.

le innovazioni introdotte con l'integrazione

L'innovazione di tipo generale risiede nel fatto che si tratta di casi sempre più comuni di interazione tra sistemi informatici dove la gestione della sicurezza fisica si pone nell'ambito dell'organizzazione come un sistema informatico gestionale dipartimentale.

Nel particolare – soprattutto nel caso dell'interazione con sistemi di ticketing – si tratta di innovazioni che finalmente convergono con la tendenza generale dei processi gestionali di produrre informazioni che passano dall'uomo solo per eccezione mentre di norma diventano dati che alimentano direttamente altri processi informatici a valle.

il livello raggiunto dalle applicazioni

Nei casi citati si trovano esempi di come le applicazioni di sicurezza arrivano talvolta ad essere riprogettate, anche con bilanci costi / benefici controversi, quando la periferia da gestire è numerosa, eterogenea e indisciplinata. Il data mining & analysis può rivelarsi utile per isolare ricorrenze anomale o indesiderate e procedere di conseguenza a interventi correttivi o migliorativi di tipo impiantistico o comportamentale in determinate categorie di impianti nell'ambito della massa gestita. Oppure – teoricamente – per gestire in maniera selettiva – su basi predittive – determinati eventi decidendo in definitiva di risparmiare risorse correndo un (maggior) rischio calcolato.

3.6 MONITORAGGIO IMPIANTI E RISPARMIO ENERGETICO

l'interesse del mercato e la richiesta

Citel riceve una spinta crescente dall'utenza ad allargare le funzionalità di telegestione anche in direzione degli eventi di natura tecnica e strumentistica, e per verificarlo basterebbe il prospetto soprastante, comprendente sia marchi con protocollo proprio che protocolli pubblici del settore industriale.

La spinta primaria è attualmente quella di chi ha adottato Centrax per applicazioni di sicurezza e vede la possibilità di estenderne l'utilizzo ottenendo progressivamente funzioni di building automation partendo dal controllo dei consumi di energia. Si tratta di una progressione agli inizi, ma destinata ad estendersi al pari del settore della sicurezza fisica, in passato dominato dai sistemi chiusi mono-fornitore e oggi in fase di progressiva conversione all'apertura multifornitore.

Il Centrax è un sistema di tele-gestione proceduralizzata di eventi e situazioni. E gli eventi e le situazioni vanno gestiti secondo criteri di efficienza e di conformità alle norme e alle buone pratiche. Che gli eventi siano generati da impianti tecnici per la sicurezza fisica piuttosto che da impianti tecnici per la vivibilità dell'edificio non fa differenza sul piano concettuale mentre viene messa a fattor comune la sistemistica informatica che permette la gestione delle relazioni tra apparati e o sottosistemi, anche indipendentemente dal fatto che siano di produttori differenti.

L'utilizzo di Centrax in senso multifunzionale, in alternativa a più sistemi specializzati e separati, porta vantaggi gestionali ed economici per l'utente facilmente intuibili, ma la sua credibilità in settori esterni alla sicurezza ha origine nelle competenze specialistiche del laboratorio di progettazione di Citel che comprende anche specialisti di controllo di processi industriali. Non a caso tra le prime applicazioni di Centrax c'è stata la gestione dell'allarmistica tecnica in caselli e gallerie di una concessionaria autostradale.

la disponibilità e la collaborazione delle terze parti

Il settore del building automation, quindi quello della climatizzazione e degli impianti tecnici, ha fornitori in prevalenza multinazionali con una notevole propensione per i sistemi multifunzionali – sicurezza fisica compresa – ma di tipo protetto. Questa politica, basata su protocolli chiusi e di solito non disponibili, è però sempre meno accettata dal mercato e si suppone che sarà sempre meno praticata dai fornitori, e lo dimostrano casi già verificatisi di forzatura dell'apertura ad opera di grandi clienti.

Quando non si tratta di sistemi di Building Automation ma di singoli sottosistemi, da interfacciare a fini di telecontrollo, è possibile che non vi siano preclusioni purché a chiederlo siano grandi utenti.

le innovazioni introdotte con l'integrazione

Le innovazioni che hanno sollevato già interesse tra gli utilizzatori Centrax sono quelle per il telecontrollo di apparati o sottosistemi di controllo dei consumi di energia. L'innovazione emergente va a toccare invece il settore del Building Automation per affermare progressivamente l'interoperabilità e il governo complessivo dei sottosistemi specializzati di gestione, climatizzazione inclusa, ad opera di un supervisore in regola con i requisiti PSIM.

L'integrazione in ambito Centrax del monitoraggio impianti permette appunto l'interazione in architettura aperta e condivisa con le applicazioni della sicurezza e della safety passando da una rete dati e ottenendo:

- l'immediatezza della segnalazione, il monitoraggio della rete, l'affidabilità della trasmissione dei dati, grazie alle prestazioni e alle garanzie delle connessioni basate sulle norme CEI 79/5-6
- il trattamento corretto, proceduralizzato, tracciato, auditabile dell'allarme tecnico e dell'intervento, la possibilità di aprire ticket in automatico, ecc.

Più in generale, il committente e il progettista possono già pensare in termini di "automazione e controllo di edifici in *Open Architecture",* dove convivono sotto-sistemi di sicurezza, safety, automazione scelti singolarmente in base a valutazioni di prestazioni/prezzo ma interoperanti tra di loro e controllati da un supervisore unico. Senza considerare che la sistemistica aperta di Centrax permette di gestire non solo un grande edificio o comprensorio, ma anche – sotto una regia unica – un insieme di edifici dell'organizzazione in un ambito corporate o dei clienti di una società di servizi.

il livello raggiunto dalle applicazioni

Il caso di più immediata applicazione è stato lo sfruttamento delle prestazioni e dell'affidabilità delle connessioni CEI 79/5-6 over-IP per la connessione di apparati tecnici per la segnalazione di anomalie, superamenti di soglia ecc. Si pensi, solo per fare un esempio, al monitoraggio della catena del freddo nella GDO con la segnalazione garantita degli allarmi (o delle misure) provenienti dai dispositivi di monitoraggio dei surgelatori, ottenuta a costo zero o quasi se innestata nella sistemistica per la sicurezza, e con una qualità tecnica e gestionale di un altro ordine di grandezza rispetto alle formule correnti nel settore dei teleallarmi.

In fase di propagazione è il controllo dei consumi di energia come applicazione aggiuntiva al Centrax esistente; in questo caso non conta tanto la sicurezza della trasmissione quanto il fatto che sia gratuita e comunque assicurata. Il catalogo dei moduli Centrax prevede ora una famiglia di moduli di integrazione ma anche di misurazione, di interazione via protocollo con sistemi di condizionamento, di generazione, di continuità, ecc.

4. L'ECOSISTEMA ALLA BASE DI CENTRAX PSIM

Centrax non è stato il primo sistema di gestione centralizzata degli allarmi in Italia, ma è stato il primo in architettura realmente aperta multifornitore, il primo integralmente conforme alla normativa CEI 79/5-6 fino al massimo livello di integrità dei dati e di affidabilità delle comunicazioni; è stato anche il primo in tutta una serie di funzionalità innovative e quello che ha fatto dell'integrazione dei prodotti di terzi e concorrenti una chiave per aprire delle porte, favorire le nuove soluzioni, attivare il miglioramento dei processi a fini di efficienza.

È da questo approccio che è si sviluppata la comunità degli utenti, quella dei fornitori complementari e alternativi e quella di fornitura di servizi di installazione e manutenzione, molti dei quali spinti all'ottimizzazione dell'esistente, all'aggiunta di nuove funzionalità o addirittura di nuovi servizi nell'ambito della stessa infrastruttura.

Il PSIM, con i suoi requisiti indipendenti e autorevoli, rispetto ai quali Centrax era perfettamente aderente, è arrivato a rafforzare la propensione degli utenti a investire sulla piattaforma Centrax come sistema corporate per ogni esigenza di telecontrollo e di gestione degli asset immobiliari.

Per contro, visto l'improvviso proliferare dell'attributo PSIM nel mercato italiano, è l'ecosistema di Centrax visto nelle pagine precedenti e senza confronti nel mercato a fornire la misura della distanza in esperienza e funzionalità che corre tra il PSIM di Citel e quelli del tutto privi di un ecosistema.

APPENDICE – IL PSIM

Nelle prossime pagine il concetto di PSIM viene messo a fuoco e aggiornato anche per evidenziarne la versatilità e la potenza applicativa che solo un lungo rapporto interattivo con il proprio ecosistema può permettere nel corso degli anni. È da considerare quindi un'anomalia sulla quale riflettere l'improvvisa proliferazione di nuovi prodotti PSIM: un indicatore dell'interesse che questo paradigma ha suscitato ma anche della singolarità del fatto che in tempi apparentemente brevi possano arrivare nel mercato sistemi che richiede un impegno di molti anni/uomo per rispettare requisiti come quelli PSIM e maturare la necessaria affidabilità.

5. UN SISTEMA INFORMATICO PER LA SICUREZZA FISICA

5.1 DAL SISTEMA DI SUPERVISIONE AL SISTEMA INFORMATICO

Perché il responsabile della sicurezza fisica dovrebbe dotarsi di un sistema informatico? Semplificando, perché in ogni organizzazione moderna la gestione aziendale è affidata a sistemi informatici dipartimentali specializzati e specificamente impostati secondo le peculiarità dei processi da automatizzare.

E non vi sono ragioni perché la sicurezza fisica debba rinunciare all'uso delle stesse tecniche informatiche dei sistemi informatici dipartimentali specializzati in ambito ERP e amministrativo. Ma nel passato le resistenze di parte dell'industria di settore e la scarsa circolazione dell'informazione sui casi innovativi e virtuosi, hanno di fatto frenato l'allineamento della sicurezza fisica agli sviluppi in termini di sistema di gestione di processi.

Citel però non si è mai risparmiata negli anni nel pubblicare rapporti e White Papers sulla questione, e la posizione odierna di leader nel settore è stata raggiunta anche per gli sforzi fatti in termini di informazione tecnica non propagandistica, centrata tutta sull'apertura architetturale e poi sul SISIF, il sistema informatico della sicurezza fisica.

L'annuncio da parte di IMS Research dell'avvento del PSIM – Physical Security Information Management (l'esatta traduzione di SISIF, non a caso) ha dato finalmente una scossa a quella parte di utenti ancora incerta su dove sarebbe andato il mercato, e ha ridotto il consenso per chi ha deciso di perseguire la strada delle architetture chiuse mono-fornitore.

Il PSIM di IMS Research (USA) è stato annunciato il 12 gennaio 2010 con un comunicato stampa che riguardava l'esito di una ricerca condotta sulle opinioni e le aspettative della grande utenza e di grandi costruttori sugli indirizzi del mercato. Il risultato dell'indagine si traduceva in sintesi in 7 requisiti che permettevano di distinguere un PSIM da una comune piattaforma software di supervisione.

I 7 requisiti erano già stati tutti integralmente introdotti da Citel con il sistema Centrax nel 2004 e probabilmente anche da altri fornitori nei mercati internazionali; ma quello che era mancato fino a quel momento a tutti gli innovatori era proprio l'elencazione neutrale, sintetica e pubblica da parte di un organo indipendente che rendesse antistorici sistemi chiusi e tradizionali che rallentavano la modernizzazione del settore.

5.2 IL PSIM E I SETTE REQUISITI

I 7 requisiti vengono riportati nel prospetto successivo secondo una traduzione di Citel, concettualmente fedele del comunicato IMS Research, ma con adattamenti nella descrizione apportati per risultare comprensibile a chiunque.

La particolare sinteticità con cui i requisiti sono stati annunciati, è stata decisiva secondo analisti di mercato per fare presa con incisività su un mercato tendente alla conservazione a causa della scarsa possibilità di misurare merito ed efficienza dei processi in base a risultati quantitativi.

Ma se è vero che il mercato sta mostrando (anche per il concorso di altri fattori evolutivi) una propensione decisamente favorevole all'informatizzazione della sicurezza fisica, Citel ritiene che il ruolo svolto da quei requisiti vada supportato da istruzioni per l'uso e raccomandazioni ispirate dagli almeno 10 anni di esperienza PSIM, e quindi il prospetto dei 7 requisiti è stato completato con le azioni che l'utente dovrebbe mettere in campo per il buon fine del progetto PSIM.

5.2.1 PSIM – I 7 REQUISITI DI IMS RESEARCH (OGGI IHS) E I VINCOLI PER IL SUCCESSO DEL PROGETTO

requisito PSIM - da condividere	*vincoli per il buon fine del progetto PSIM*
1 - Connettività e integrazione: ricezione di dati da un numero qualsiasi di apparati o sistemi di sicurezza; capacità di integrazione sia nell'ambito della sicurezza fisica che rispetto ad altri sistemi di gestione dell'azienda (sia nei siti periferici che nell'interazione tra essi e il sistema centrale)	Nessuna limitazione a priori degli apparati gestibili vuol dire scalabilità, modularità, multifunzionalità. Ai fini della capacità di integrazione di altri sistemi non è sufficiente che il produttore sia disponibile a integrare: deve anche essere in grado di realizzare direttamente interfacce hardware e software con apparati, sottosistemi e sistemi diversi per tecnologie, funzionalità, tipologie di connessione, costruttore. Solo in tal caso tempi, costi, qualità della integrazione, saranno contenuti e prevedibili. La coerenza con il requisito comporta che il protocollo di trasmissione centro–periferia sia pubblico, bidirezionale, in grado di garantire la massima protezione dei dati, il monitoraggio continuo del funzionamento degli apparati periferici, della connessione in rete; e in grado di gestire la commutazione automatica della connessione su un vettore alternativo.
2 - Gestione Real Time e configurazione controllata: possibilità di configurare e modificare da centro procedure e parametri a bordo dei vari sistemi e dispositivi in ogni livello della infrastruttura (antintrusione, controllo accessi, videosorveglianza, ecc.)	
3 - Correlazioni e Verifiche: connessione automatica centro-periferia e correlazioni multiple tra diversi apparati per la sicurezza; verifiche real-time e gestione flessibile delle interazioni correlate.	Funzioni configurabili di correlazione in grado di trattare segnali elementari dagli apparati e dal campo per generare eventi (allarmi certi, inattendibili, falsi positivi, ecc.) corredati dalla precisa descrizione e localizzazione: - per rendere immediata per un operatore qualsiasi la consapevolezza più attendibile di ciò che ha generato l'evento (event awareness) - per tenere aggiornato in tempo reale l'operatore sull'evoluzione della situazione (situation management). Con la possibilità di generare correlazioni sia a bordo di un dispositivo/nodo locale presso il sistema centrale e anche presso il software centrale di supervisione
4 - Visualizzazione: in caso di evento il PSIM deve essere in grado di visualizzare graficamente informazioni sulla situazione in modo da dare a chi deve gestire l'evento un'idea anche complessiva della natura dell'evento, del contesto locale e dell'ampiezza della minaccia.	Cruscotti per operatori unificati rispetto agli apparati che originano gli eventi. Suite di cruscotti per la libertà di scegliere tra diversi tipi di gestione operatore: con la grafica animata, con la video-ispezione correlata, con la video-sorveglianza interattiva e multimediale

segue

requisito PSIM - da condividere	*vincoli per il buon fine del progetto PSIM*
5 - Processi di gestione eventi basati su procedure guidate: avvio immediato dell'operatore su un percorso guidato passo-passo, basato su procedure mirate al contenimento o al contrasto della minaccia, monitorizzando progressivamente l'esito delle attività svolte sul posto	Funzioni da cruscotto operatore per la gestione guidata per fasi successive lungo un percorso guidato e obbligato, con la presentazione contestualizzata delle informazioni necessarie all'accertamento degli eventi, alla gestione degli interventi e all'acquisizione dei feed-back
6 - Affidabilità e Resilienza: caratteristiche di robustezza e ripristino della piattaforma di sistema per ogni modulo ed a tutti i livelli, per assicurare la continuità del servizio e il ritorno alla normalità della gestione sia in caso di guasto parziale che di disastro totale.	Struttura di sistema e componentistica progettati e configurati con il requisito prioritario di una continuità di servizio superiore al 99,5%. Pertanto: - processi distribuiti ai vari livelli della sistemistica, - moduli di riserva in stand-by e servizio di teleassistenza specializzata H24 del fornitore per ripristini guidati - possibilità di disaster recovery center
7 - Reportistica e Riesame post-evento: tracciabilità e verbalizzazione documentata della gestione dell'evento anche ai fini della ricostruzione criminologica dell'accaduto e della sua gestione	Tracciamento di ogni singola attività operativa. Funzioni di generazione guidata e facilitata di report nel corso della gestione dell'evento, con possibilità di allegare al report snap-shot, video-clip e book-mark. Riesame di video pertinenti a partire dallo storico eventi e non dall'archivio video.

5.2.2 LA CONFORMITÀ PROCEDURALE DELLA SEQUENZA DEL TRATTAMENTO DI UN EVENTO

La figura schematizza i passaggi eseguiti dall'operatore Centrax, quasi soltanto con l'uso del mouse, per ottenere la gestione completa dell'evento secondo i criteri canonici del PSIM del prospetto precedente:

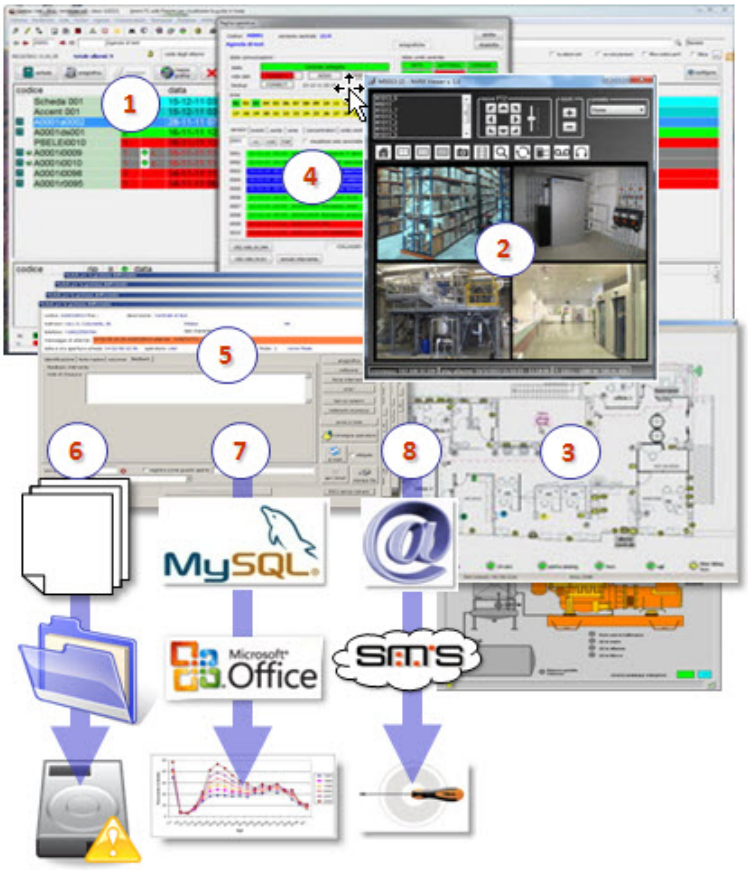
informazione immediata → verifica efficiente → telegestione dell'evento e dei suoi sviluppi situazionali con un procedimento guidato passo-passo → coinvolgimento operativo di altre funzioni per interventi e per escalation → conclusione, verbalizzazione e storicizzazione

1 - informazione immediata = coda allarmi dei nuovi eventi e di quelli in fase di gestione; verifica efficiente = pulsanti contestualizzati per attivare i controlli in tempo reale della situazione

2 - cruscotto video

- visualizzazione live di una o più telecamere associate all'evento (cosa sta accadendo)
- visualizzazione di video pre-evento (cosa è successo prima della segnalazione)
- commutazione a una videoronda mirata con le telecamere e Dome appropriate per quell'evento (se e come l'evento sta evolvendo in una situazione)

3 - oggetti dinamici, posti su mappe, planimetrie, sinottici e qualsiasi altro sfondo grafico, permettono di localizzare il punto dell'evento nell'ambito di un comprensorio, di un edificio, di un piano, oppure di un macchinario, apparato, quadro elettrico; gli oggetti dinamici sono configurati per evidenziare uno stato mediante colorazione e animazione; allo stesso tempo consentono di eseguire attivazioni, reset, pop-up informativi di stato (azionamenti intuitivi, mirati) ovviamente nei limiti del profilo autorizzativo



4 - cruscotto pop-up di verifica di stati / attivazione di comandi per singolo punto/sensore della Centrale di Gestione Eventi se questa lo consente; realizza la telegestione dell'elemento chiave del sito

5 - la gestione di eventi e situazioni guida l'operatore lungo un percorso procedurale passo – passo, presentando automaticamente le informazioni correlate: persone, servizi, e risorse necessarie a verifiche e interventi; il verbale non si chiude se l'operatore non ha rispettato la procedura e una segnalazione ne informa un livello responsabile, anche in una diversa Control Room

6/7/8 - archiviazione del log che traccia tutto il processo di gestione fino alla verbalizzazione in una base dati / possibilità di interagire con altri sistemi informatici interni ed esterni come quelli del ticketing e della vigilanza; si saltano le operazioni manuali nei rapporti con i fornitori di servizi

5.2.3 LA CONFORMITÀ ARCHITETTURALE DI SISTEMA DI CENTRAX-PSIM

Premesso che un PSIM è un sistema con un'architettura basata su
- una rete LAN e/o WAN di comunicazione bidirezionale aperta
- da una a numerose piattaforme in campo per i processi locali di generazione degli eventi
- da apparati e dispositivi preesistenti e nuovi che svolgono funzioni in campo: devices di controllo, sensoristica, attuazioni, moduli di interazione multimediale

il prospetto riporta, per ogni tipologia di modulo, la conformità specifica ai 7 requisiti

Modulo PSIM	*Composizione / descrizione*	*requisiti 1-7 di IMS cui il modulo risponde in conformità*
Server	• hardware di mercato (PC o server) • software Centrax-PSIM server	• hardware di qualità e assistito, per il rispetto del **requisito 6** • funzioni software Server per **tutti i 7 requisiti**
Posti di Lavoro	• software Centrax Client per cruscotti operativi e funzioni di controllo e manageriali	• funzioni software Client per i **requisiti 2, 4, 5, 7**
Rete dati	• intranet aziendale o VPN conforme alla normativa CEI 79/5-6 fino al massimo livello	• **requisito 1** per le funzionalità • **requisito 6** per affidabilità e resilienza
Correlatore PSIM	• hardware specializzato per integrazione fisica di dispositivi vari in campo • software specializzato di raccolta e interazione tra input differenziati mediante correlazioni configurabili per generare *eventi* (e non semplici allarmi) e *situazioni* (eventi in divenire) • possibilità di tunneling per far passare scambi dati proprietari per configurazioni e diagnostica	• **requisiti 2 e 3**
Devices vari	• funzioni antintrusione, controllo accessi, incendio, anomalie tecniche, connettibili al correlatore PSIM	• **requisito 1**
Servizi del costruttore	• servizi complementari per assicurare:	
	○ la continuità di funzionamento con assistenza H24	• **requisito 7**
	○ la specializzazione per supportare l'utente nella transizione dai sistemi tradizionali al PSIM e allo sfruttamento delle nuove possibilità	• garanzia di implementazione effettiva di **tutti i 7 requisiti**
	○ la missione di integrare incessantemente in ambito contrattuale o su richiesta nuovi dispositivi e sottosistemi	• **requisiti 1 e 2** mantenuti nel medio-lungo periodo
	○ la manutenzione evolutiva del sistema per ottenere una continua evoluzione delle funzionalità con il mutare del contesto	• **tutti i 7 requisiti** tutelati e aggiornati non solo nel breve ma anche nel medio-lungo periodo
Altri requisiti non codificati	• scalabilità della struttura, delle funzioni e dei relativi costi in modo da far crescere le dimensioni e le funzionalità del PSIM con la progressività e la sostenibilità adeguate al contesto aziendale	• possibilità di mantenere lo stesso PSIM, senza sostituzioni e disinvestimenti, mediante aggiunte e aggiornamenti successivi