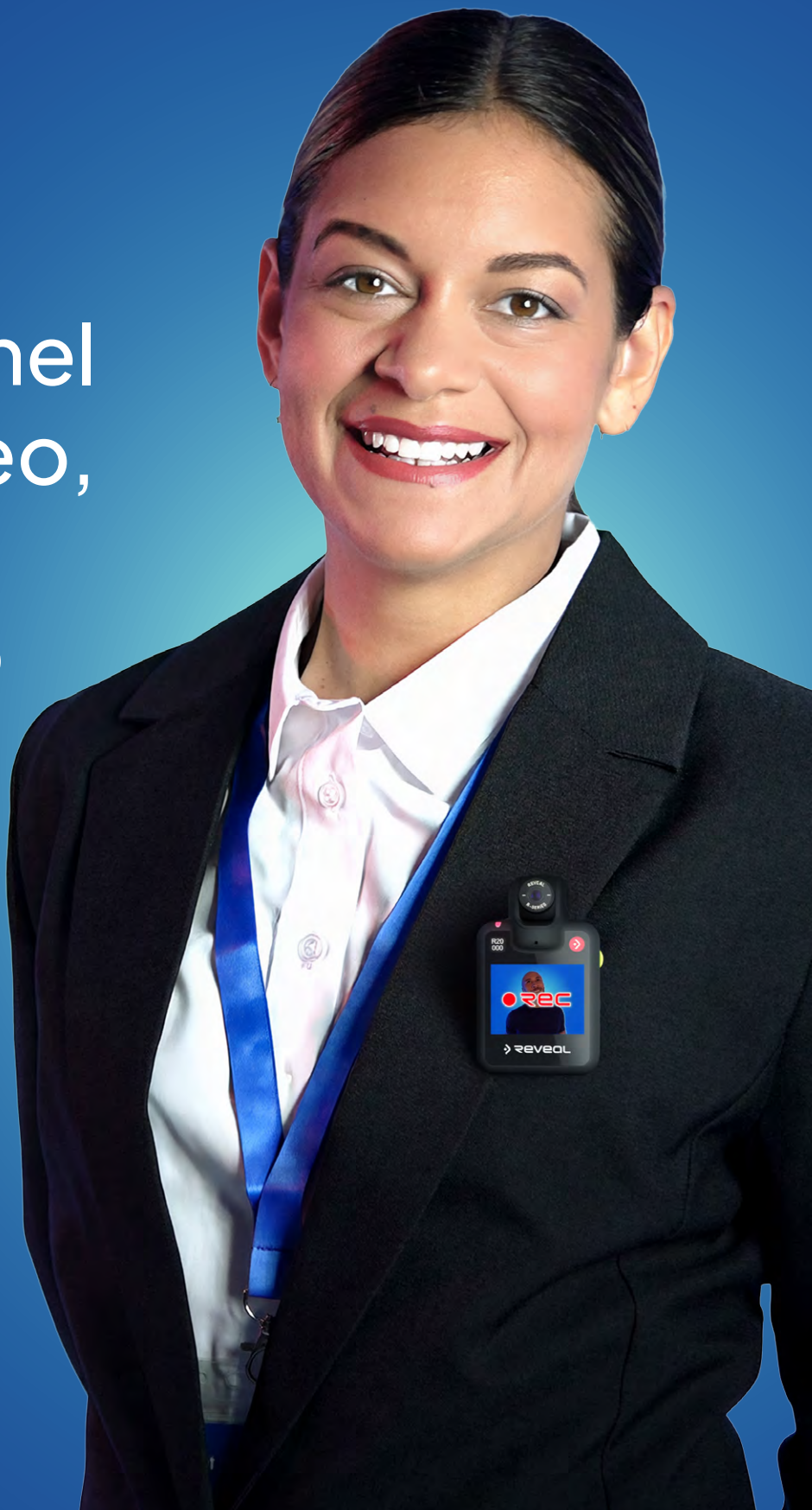
essecome ONLINE 05/26

Periodico digitale di informazione di security & safety

2026 · ANNO XLVI

REVEAL

Sicurezza e protezione nel settore aereo, portuale e ferroviario



www.revealmedia.it



Leader nella sensoristica.

Scelti in tutto il mondo.

Installati in migliaia di infrastrutture critiche in tutto il mondo, i sensori di sicurezza OPTEX sono scelti per la loro precisione e affidabilità nel tempo. Una qualità riconosciuta a livello internazionale che rende OPTEX un punto di riferimento nel settore della sicurezza.

optex-europe.com

OPTEX
Sensing Innovation



Proteggere il porto. Connettere le informazioni.

Soluzioni Axis per la sicurezza e le operazioni portuali.

Dai varchi al waterfront, le soluzioni Axis aiutano a monitorare aree estese, integrare sistemi e fornire agli operatori informazioni utili per verificare gli eventi e intervenire.

Punti chiave

- Monitoraggio di varchi, perimetri, banchine e aree operative
- Telecamere di rete selezionate in base alle condizioni ambientali e alle esigenze del sito
- Analisi video su dispositivi compatibili, a supporto dell'attenzione degli operatori
- Integrazione con sistemi di gestione video e altre tecnologie compatibili
- Attenzione a manutenzione, cybersecurity e continuità operativa

Scopri le soluzioni Axis per il settore marittimo
www.axis.com/it-it/solutions/maritime

AXIS COMMUNICATIONS



CoreSync

Il livello di integrazione che aspettavi.

La nuova funzione CoreSync introduce un livello di integrazione tra videosorveglianza InVista e sicurezza ancora più evoluto: le centrali **Prime** e **PrimeX** dialogano direttamente con gli **NVR InVista**, trasformando gli eventi di videoanalisi in azioni concrete. **Fino a 200 zone AI**, senza utilizzare le zone della centrale. Rilevamento intrusioni, attraversamento linea, analisi termica e riconoscimento targhe, possono attivare uscite e notifiche con immagini e video su Inim Home. Con InimTech Security, l'installatore mantiene il pieno controllo dell'impianto.

Un unico ecosistema, una sicurezza più intelligente.

www.inim.it

inim®
Evolving Protection



Frigoriferi e minacce combinate, come cambia l'arte della guerra nel XXI secolo



Il gruppo di hacker russi Z-Pentest Alliance, rivendicando i recenti attacchi ai sistemi refrigeranti di centinaia di supermercati francesi e di ospedali di mezza Europa, avrebbe precisato che: *"Il problema non sono gli hacker cattivi ma l'incredibile negligenza degli operatori europei e americani che hanno ignorato per anni le regole basilari di cybersecurity"*. Come dargli torto, quando si viene a sapere che gli hacker avrebbero utilizzato le falle di vecchi software non più aggiornati per la gestione da remoto degli impianti frigoriferi dei maggiori gruppi francesi della grande distribuzione? E che il fornitore di quei software, per facilitare la ricerca dei propri tecnici, avrebbe pubblicato su internet le interfacce di gestione relative allo stesso modello di sistema di refrigerazione preso di mira in questa ondata di attacchi cyber, come hanno scoperto i ricercatori di Check Point Research?

La prima considerazione che sorge spontanea è che, se noi europei siamo entrati a nostra insaputa in una guerra ibrida dove gli attacchi agli obiettivi materiali non vengono sferrati con le armi tradizionali ma con le armi informatiche, siamo impreparati a difenderci e, tanto meno, a ribattere gli attacchi avversari. Sono almeno dieci anni che gli esperti lanciano l'allarme sulle minacce combinate ma è stato finora inutile anche in settori per definizione molto esposti come la catena alimentare e la sanità.
Ora è indispensabile organizzare le difese nel minor tempo possibile, sperando che gli attacchi cyber ai frigoriferi che provocano milioni di danni e compromettono la continuità operativa dei servizi essenziali siano serviti almeno a far capire la portata del pericolo.

Ma l'ibridazione delle minacce produce, a nostro modo di vedere, anche altri effetti da prendere seriamente in considerazione pensando alla sicurezza pubblica di un paese ma anche a quella privata dei suoi cittadini.
Se, come sembra di capire, gli attacchi ai frigoriferi europei provengono realmente da hacker controllati o ispirati dai governi dei propri Paesi ostili all'Europa, avremmo davanti uno "schieramento ibrido" di forze attaccanti dove soggetti privati con determinate competenze svolgono funzioni sussidiarie a quelle dello Stato di appartenenza per operazioni rientranti in strategie di attacco decise dai vertici politici e militari ma non dichiarabili.
Questi privati potrebbero anche essere dei nerd che mai indosserebbero una divisa ma sono perfettamente in grado di colpire qualsiasi obiettivo partendo dai "soft target" come i frigoriferi che provocano più danni di uno sciame di missili lanciati dai reparti militari statali, per di più a costi marginali.
Considerando che il passo tra un obiettivo soft e un'infrastruttura critica è molto breve, sarebbe il caso di non offendersi per le frecciate di Z-Pentest Alliance ma di considerarle delle utili provocazioni a rimboccarsi le maniche e verificare le condizioni di sicurezza dei nostri obiettivi sensibili per implementare adeguate forme di difesa.

Sommario

08 APR 2026, l’evoluzione della sicurezza delle infrastrutture critiche

10 Verso APR 2026, le ragioni della diversità della Puglia

12 Direttiva CER e APR 2026: “in viaggio” verso la resilienza delle infrastrutture critiche

14 L’IA nelle infrastrutture del trasporto: governare prima di automatizzare

16 Telecamere di rete AXIS per la protezione integrata di porti e aeroporti

18 Sicurezza di porti e aeroporti: integrazione, resilienza e intelligenza artificiale

20 OPTEX, qualità e innovazione per contrastare le minacce combinate alle Infrastrutture critiche

22 Bodycam, il valore delle prove oggettive

24 Bodycam e vigilanza privata: bilanciamento tra sicurezza e privacy

26 Cube Protection Central integra mappe CAD e AI nella gestione della sicurezza

28 Oltre la conformità: perché le norme EN 54-21 ed EN 50136 sono importanti nella trasmissione degli allarmi antincendio

30 Riqualificare gli accessi: efficienza energetica, sicurezza e integrazione

32 Cube Service per la gestione digitale delle manutenzioni

34 Urmet ATE a MIBA, Smart Building Levante con la sua offerta completa

36 Allarme incendio, ogni secondo conta

ATE
urmet

instantTONE

VIGILANZA



La **tecnologia** che guarda
al **futuro** della **sicurezza**

Urmet ATE sviluppa soluzioni per la vigilanza professionale, integrando tecnologia, sistemi e competenze per supportare in modo concreto l’attività degli operatori. Piattaforme progettate per semplificare la gestione, coordinare le operazioni e migliorare il controllo in tempo reale, ottimizzando i processi e riducendo la complessità. Dall’evoluzione delle centrali operative, come **Ate Argo Next,** all’introduzione di strumenti avanzati come l’operatore virtuale **NEXTY**, ogni soluzione è pensata per rendere la vigilanza più efficiente e affidabile. Da oltre 20 anni, Urmet ATE è un punto di riferimento per una protezione che guarda al futuro.

**Siamo presenti a MIBA Levante,
18-19 novembre
Nuovo Padiglione. Stand 100,
ingresso Agricoltura.**

MIBA
MILAN INTERNATIONAL BUILDING ALLIANCE
GEE GLOBAL ELEVATOR EXHIBITION · MADE EXPO · SMART BUILDING EXPO · SiCUREZZA

Via Pola, 30 | 36040 Torri di Quartesolo VI (ITALY) T +39 0444 26 82 11 | info@urmet-ate.it | **urmet-ate.it** |

securindex.com

APR 2026
dalla SECURITY alla RESILIENZA

I NUOVI SCENARI DELLA SICUREZZA DELLE INFRASTRUTTURE CRITICHE DELLA PUGLIA

18 novembre 2026 Bari - MIBA LEVANTE

La XXI edizione di APR - Air, Port, Rail security & safety, l'appuntamento annuale organizzato da securindex per approfondire i problemi della sicurezza delle infrastrutture dei trasporti, è dedicata all'analisi del cambiamento delle minacce che si manifestano – come descrive la più recente Relazione sulla politica dell'informazione per la sicurezza italiana - attraverso dinamiche "pervasive, elusive, multidimensionali e multidominio", con la tecnologia protagonista assoluta della trasformazione. Un nuovo paradigma che impone un approccio diverso al concetto di sicurezza, ora da interpretare come resilienza delle infrastrutture alle nuove minacce ibride.

Anche la NATO, nel proprio attuale quadro strategico, considera le minacce ibride come fenomeni che possono combinare strumenti e modalità differenti e sottolinea la necessità di proteggere le infrastrutture critiche attraverso una cooperazione che coinvolga dimensione militare, civile e privata.

Considerazioni di assoluta rilevanza per la Puglia che, disponendo di circa 865 chilometri di costa, di un sistema portuale articolato, di quattro aeroporti, di una rete stradale e ferroviaria estesa e di un sistema logistico integrato è essa stessa un sistema infrastrutturale interconnesso, la cui importanza strategica viene moltiplicata nei momenti di alta tensione delle relazioni internazionali come l'attuale, data la sua posizione nel Mediterraneo Orientale.

Non a caso, nell'ambito del programma FESR-FSE+ 2021-2027, la Regione Puglia ha destinato 12,5 milioni di euro al miglioramento della sicurezza degli aeroporti esistenti e dei sistemi di gestione del traffico aereo, con una sempre maggiore attenzione degli operatori per le applicazioni di IA per la sicurezza e il miglioramento dei processi.

APR 2026 affronterà questi temi con i rappresentanti delle istituzioni militari e civili, i gestori aeroportuali e portuali, gli operatori logistici, i security manager, gli operatori della vigilanza privata e i responsabili della cybersecurity per creare un confronto tra domanda e offerta di sicurezza nel prestigioso contesto di MIBA Levante (Bari, 18-19 novembre), la più importante manifestazione fieristica della sicurezza in Meridione organizzata negli anni pari da Fiera Milano con la collaborazione di Pentastudio.

Programma

APR 2026
dalla SECURITY alla RESILIENZA

10:30 **Saluti istituzionali**
invitati: Rossana Riflesso (Prefetto di Bari), Elisabetta Vaccarella (VP Consiglio Regionale Puglia), sen. Filippo Melchiorre (videomessaggio), on. Marco Lacarra (videomessaggio)

10:50 **Relazione introduttiva**
Generale C.A. (ris) Leonardo di Marco

11:00 **Sicurezza ed efficienza operativa delle IC del trasporto in Puglia**
tavola rotonda
invitati: Michele Conte (Propeller Club), Pierluigi Di Palma (Osservatorio Antonio Catricalà), Francesco Hemmeler (AISEC), Gaetano Mesto (IFOA), Sergio Prete (direttore Servport), Antonio Vasile (presidente Aeroporti di Puglia)

12:10 **Le risposte della filiera e il ruolo della IA**
panel con vendor e service provider
presentazioni di: AISMA – AXIS – EL.MO – LIFE3 – OPTEX – REVEAL – UNIV

13:30 **Conclusioni**

Ai partecipanti verrà rilasciato su richiesta l'Attestato di Partecipazione.
Evento solo in presenza, per informazioni scrivere a **segreteria@securindex.com**

APR 2026, l’evoluzione della sicurezza delle infrastrutture critiche

intervista a Leonardo di Marco, Generale di Corpo d’Armata (Ris.) dell’Esercito Italiano

I criteri di valutazione dei rischi delle infrastrutture critiche e delle misure di difesa sono molto cambiati per molteplici motivi. Può descrivere in cosa consiste il cambiamento?

È cambiata soprattutto la natura della minaccia. Oggi un’infrastruttura critica non è più esposta soltanto a un attacco diretto al proprio perimetro fisico. Una minaccia può arrivare contemporaneamente dal dominio fisico, da quello cyber, da quello virtuale così come dalla conseguente percezione cognitiva, producendo effetti anche molto lontani dal punto in cui ha avuto origine.

Per questo dobbiamo cambiare anche il modo di concepire la difesa. Non basta più proteggere un aeroporto, un porto o un’infrastruttura: occorre proteggere le loro interdipendenze e la capacità del sistema di continuare a funzionare anche quando una delle sue componenti viene colpita.

La domanda che vorrei porre ad APR 2026 è quindi molto semplice: siamo ancora organizzati per difendere singoli perimetri, quando la minaccia si muove ben oltre le connessioni tra quei perimetri?

È dunque necessario evolvere anche la nozione di sicurezza?

Sì, perché sicurezza e resilienza non sono più concetti separabili. La sicurezza tradizionale tende a concentrarsi sulla prevenzione dell’evento e sulla protezione dell’asset. Oggi dobbiamo aggiungere la capacità di rilevare rapidamente una minaccia, comprenderne gli effetti, reagire, mantenere l’operatività e ripristinare le funzioni essenziali.

In altre parole, il vero obiettivo non è soltanto impedire che qualcosa accada, ma fare in modo che, anche quando accade, il sistema non smetta di funzionare. È un cambiamento culturale prima ancora che tecnologico: dalla protezione del singolo asset alla resilienza del sistema.



Perché è stata scelta la Puglia per parlare di un argomento che ha una valenza globale?

Perché la Puglia rappresenta particolarmente bene la complessità del problema. È una regione nella quale porti, aeroporti, rete stradale e ferroviaria, logistica e collegamenti con il Mediterraneo costituiscono un sistema fortemente interconnesso. Ciò che accade in un punto può produrre conseguenze anche molto lontano.

Ma c’è un’altra ragione. La Puglia consente di osservare concretamente il rapporto tra dimensione territoriale e dimensione globale della sicurezza.

Non parleremo quindi della Puglia come di un’area più esposta di altre, ma come di un laboratorio particolarmente significativo per capire come una minaccia globale debba essere affrontata sul territorio, attraverso la cooperazione tra istituzioni, gestori, operatori e filiera tecnologica.

Quale può essere l’apporto della filiera privata della sicurezza in un quadro che riguarda aspetti strategici per la sicurezza del Sistema Paese di competenza delle Forze Armate?

La sicurezza delle infrastrutture critiche è una responsabilità pubblica, ma la capacità di proteggerle non può essere esclusivamente pubblica.

Le Forze Armate e le Forze di Polizia hanno responsabilità e capacità che nessun soggetto privato può sostituire. Allo stesso tempo, chi gestisce quotidianamente un aeroporto, un porto, una rete logistica o un’infrastruttura digitale possiede conoscenze, tecnologie e capacità operative indispensabili.

La filiera privata può quindi contribuire soprattutto a rafforzare la capacità di prevenire, rilevare e reagire, mettendo a disposizione tecnologia, competenze e servizi.

Il punto, però, non è semplicemente acquistare tecnologie. È capire come integrare ciò che il pubblico e il privato già possiedono in un’unica capacità di sicurezza e resilienza.

Ed è proprio su questo rapporto che vorremmo aprire il confronto ad APR 2026.

Quale sarà il messaggio finale di APR 2026?

Credo che il messaggio possa essere molto semplice: nessuno può garantire da solo la sicurezza di un sistema così complesso. La minaccia attraversa i confini organizzativi; la risposta deve essere capace di attraversarli altrettanto rapidamente.

Per questo APR 2026 non vuole soltanto mettere intorno allo stesso tavolo istituzioni, gestori e imprese tecnologiche. Vuole capire come trasformare competenze diverse in una capacità comune di prevenire, proteggere, reagire e continuare a operare.

E forse la domanda con cui concluderemo sarà proprio questa: se la prossima minaccia sarà multidominio, siamo già capaci di rispondere come un unico sistema?

È una domanda alla quale difficilmente può rispondere una sola organizzazione. Ed è probabilmente per questo che vale la pena discuterne insieme il 18 novembre a Bari.



Verso APR 2026, le ragioni della diversità della Puglia

intervista a Gabriele Zito, dottore commercialista, esperto di governance e resilienza d'impresa, partner di KFD Studio

Ho studiato geopolitica al SIOI, ma sono anzitutto un tarantino che lavora a Bari da trent'anni, e credo che l'unicità della Puglia si legga meglio nei flussi che nella posizione. La geografia è rimasta la stessa; ciò che è cambiato è la densità di ciò che passa di qui. Pochissime regioni europee concentrano su uno spazio così compatto porti commerciali e militari, quattro aeroporti, l'approdo del gasdotto TAP, le interconnessioni elettriche e digitali con i Balcani e la Grecia ed il medioriente, e al tempo stesso una delle quote più alte di produzione da fonti rinnovabili del Paese. Energia, dati, merci e persone transitano dagli stessi pochi chilometri di costa.

La seconda unicità è culturale, e la considero la più preziosa. La Puglia ha una lunga tradizione di scambio: la Fiera del Levante nasce esattamente con questa vocazione. Questa abitudine a lavorare con l'altra sponda del Mediterraneo è un capitale relazionale che la tecnologia non sostituisce, anzi rende più necessario. Nell'era dell'intelligenza artificiale un territorio si distingue per la qualità della fiducia tra chi lo abita e chi ci lavora, non solo per l'infrastruttura. La Puglia ha questo capitale. La sfida è trasformarlo in capacità organizzata.



Unicità come fattore di rischio: come la percepiscono istituzioni e classe dirigente?

Direi che la percezione è a due velocità. I grandi gestori (aeroporti, autorità portuali, operatori dell'energia e delle telecomunicazioni) sono ormai strutturati: hanno security manager, piani di continuità operativa, rapporti consolidati con le Forze Armate e le Forze di Polizia. Il punto debole non sta lì, ma nella filiera che gira intorno a loro: logistica, manutenzione, fornitori di servizi, piccole e medie imprese che hanno accesso fisico o digitale a quelle infrastrutture e che spesso non si percepiscono come parte di un sistema critico. Le minacce ibride entrano proprio dalla porta più debole.

Su questo il legislatore europeo ha già cambiato le regole. Le norme di recepimento della direttiva NIS2 e della direttiva sulla resilienza dei soggetti critici spostano la sicurezza dentro la governance: sono gli organi di amministrazione a dover approvare le misure di gestione del rischio, e ne rispondono. Per un'impresa la sicurezza non è più un costo tecnico delegato a un ufficio, ma una componente degli adeguati assetti organizzativi che il codice civile richiede agli amministratori.

Da professionista che siede nei consigli di amministrazione, nei collegi sindacali e negli organismi di vigilanza, vedo che questa consapevolezza sta crescendo, ma non ancora con la velocità che servirebbe. Ho guidato per anni un'impresa della vigilanza privata e so quanto il presidio fisico sia importante. Oggi però la vera domanda per un consiglio di amministrazione è: «Se domani un nostro fornitore viene compromesso, che cosa succede a noi e all'infrastruttura che serviamo?». Le imprese pugliesi che sapranno rispondere saranno anche le più credibili come partner dei grandi operatori.

Quanto pesano le difficoltà sull'ex ILVA rispetto a progetti evoluti di sviluppo industriale?

Sono nato a Taranto, quindi non posso parlarne con distacco. Pesano molto, e su tre piani. Il primo è la fiducia degli investitori: un grande gruppo industriale valuta anzitutto la certezza delle regole, e la vicenda dell'ex ILVA, con autorizzazioni, decisioni giudiziarie e trattative di vendita che si sovrappongono da oltre dieci anni, comunica un'incertezza che va ben oltre lo stabilimento. Il secondo è l'assorbimento di risorse pubbliche, di attenzione politica e di capacità amministrativa, che vengono sottratte ad altri progetti. Il terzo, più silenzioso, riguarda l'indotto: centinaia di piccole imprese sane che rischiano di fallire non per colpa propria, ma per effetto di una crisi altrui.

Dalla mia esperienza nelle procedure concorsuali traggo però una lezione meno pessimista. Una crisi industriale, anche grave, si può gestire senza distruggere valore se si separano per tempo le questioni: la tutela della salute e dell'ambiente, la continuità produttiva possibile, la protezione dei creditori e dei fornitori, la ricerca di un acquirente con un piano credibile. Quando questi piani si confondono, ognuno blocca l'altro. Oggi i giudici, il Governo e le parti sociali stanno ancora cercando una soluzione, ma qualunque esito dovrà partire da qui: la sostenibilità ambientale non può essere un vincolo aggiunto a valle, deve essere parte del piano industriale fin dall'inizio.

Infine Taranto non è solo l'ex ILVA. Ha un porto con grandi potenzialità, la presenza della NATO e della Marina, l'aeroporto di Grottaglie con la sua vocazione aerospaziale, e competenze tecniche che pochi territori possiedono. Il rischio vero è che la crisi dell'acciaio continui a monopolizzare lo sguardo su una città che ha anche altro da offrire. Per chi investe in sicurezza, logistica e tecnologia, Taranto può essere un laboratorio, non solo un problema.



Direttiva CER e APR 2026: “in viaggio” verso la resilienza delle infrastrutture critiche

di Miryam Cattaneo, Senior Risk Security Consultant di AISEC, Security Advisory Company

Negli ultimi anni il contesto di sicurezza delle infrastrutture strategiche, in grado cioè di erogare servizi essenziali per il funzionamento dello Stato e dell’economia, ha subito una profonda trasformazione.
La crescente instabilità geopolitica, l’evoluzione delle minacce fisiche e cyber, la digitalizzazione dei processi operativi e l’aumento delle interconnessioni tra organizzazioni e filiere hanno reso sempre più evidente quanto la continuità dei servizi essenziali dipenda da ecosistemi complessi e fortemente integrati.
In questo scenario, la protezione di infrastrutture, definite come critiche, non può più essere affrontata esclusivamente attraverso misure di difesa fisica o tecnologica.
La capacità di garantire l’erogazione dei servizi essenziali erogati dalle stesse richiede infatti un approccio multidisciplinare che integri prevenzione, gestione del rischio, continuità operativa e risposta agli incidenti. Questa visione, in particolare, rappresenta il fondamento della direttiva CER (“Critical Entities Resilience”), il provvedimento europeo volto a rafforzare la resilienza dei soggetti critici, che nasce dalla consapevolezza che eventi apparentemente circoscritti possono generare conseguenze rilevanti su scala nazionale o internazionale, introducendo una prospettiva più ampia, orientata alla capacità delle organizzazioni di assorbire gli effetti di una crisi, adattarsi e ripristinare rapidamente le proprie funzioni vitali.

Il settore dei trasporti: rischi e vulnerabilità

Tra i settori coinvolti, quello dei trasporti rappresenta uno degli ambiti più significativi e strategici. Aeroporti, porti, ferrovie, infrastrutture metropolitane e reti logistiche costituiscono elementi fondamentali per il funzionamento dell’economia e della società. Oltre a garantire la mobilità di persone e merci, assicurano di fatto il collegamento con altri servizi essenziali, contribuendo alla continuità delle attività produttive e istituzionali.



Queste infrastrutture, in particolar modo negli ultimi anni, hanno accelerato i propri percorsi di trasformazione digitale, introducendo sistemi di automazione, piattaforme di monitoraggio, tecnologie operative interconnesse, sensoristica avanzata e strumenti di gestione intelligente delle operazioni. Un’evoluzione che ha prodotto importanti benefici in termini di efficienza e controllo, ma ha anche ampliato la superficie di esposizione verso minacce sempre più articolate.
Di fatto, le organizzazioni del settore oggi si trovano spesso a confrontarsi con minacce di natura fisica ed atti intenzionali quali sabotaggi, furti, intrusioni, danneggiamenti alle infrastrutture e altre azioni in grado di comprometterne l’operatività, a cui si affiancano guasti infrastrutturali, interruzioni energetiche ed eventi naturali estremi.
Unitamente ad essi, la crescente digitalizzazione ha introdotto ulteriori rischi legati ad attacchi informatici e alla compromissione di sistemi e servizi digitali. Il risultato? Sempre più frequentemente tali minacce si manifestano in maniera combinata, rendendo necessario un approccio integrato che superi la tradizionale separazione tra security fisica e cybersecurity.

La direttiva CER si inserisce proprio in questa prospettiva, richiedendo ai soggetti critici di eseguire una valutazione complessiva dei rischi e delle vulnerabilità che tenga conto delle interdipendenze esistenti tra infrastrutture, fornitori, tecnologie e processi organizzativi.

Un cambio di paradigma

Uno degli elementi più innovativi introdotti dalla direttiva riguarda il cambiamento di paradigma nella gestione della sicurezza. Infatti, se per lungo tempo l’obiettivo principale delle organizzazioni è stato identificato nella protezione di infrastrutture, impianti e sistemi da specifiche minacce, oggi, invece, l’attenzione si sposta verso la continuità delle funzioni essenziali che tali organizzazioni sono chiamate a garantire.
In quest’ottica assumono crescente importanza strumenti quali il risk management, il business continuity management, il crisis management e la pianificazione delle emergenze.
La capacità di individuare tempestivamente gli scenari di crisi, coordinare le decisioni, mantenere operative le attività prioritarie e ripristinare rapidamente i servizi sta diventando sempre più un fattore determinante per limitare impatti economici, sociali e reputazionali.
La resilienza non viene più quindi intesa come semplice capacità di resistere a un evento avverso, assume bensì un concetto più ampio che richiede una crescente collaborazione tra operatori infrastrutturali, istituzioni, fornitori e autorità competenti, riconoscendo che la sicurezza delle infrastrutture critiche costituisce una responsabilità condivisa.

APR 2026: il confronto sui nuovi scenari della sicurezza

Queste tematiche saranno al centro di APR 2026, l’evento dedicato ai temi della security, safety e resilienza nei comparti aeroportuale, portuale e ferroviario.
L’appuntamento rappresenterà un’importante occasione di confronto tra istituzioni, operatori del settore, gestori infrastrutturali ed esperti di sicurezza per approfondire l’evoluzione delle minacce che interessano le infrastrutture di trasporto e analizzare le implicazioni operative derivanti dall’attuazione della Direttiva CER. Particolare attenzione sarà dedicata alle strategie di gestione integrata del rischio, alle minacce ibride, alla protezione delle infrastrutture operative, alla sicurezza delle tecnologie digitali e al ruolo delle nuove soluzioni di monitoraggio e analisi avanzata nel supportare le attività di prevenzione e risposta agli incidenti.
Il dibattito consentirà inoltre di esaminare le modalità attraverso cui i soggetti critici possono sviluppare capacità organizzative sempre più mature in materia di resilienza, rafforzando la cooperazione tra le diverse componenti dell’ecosistema dei trasporti.

Una sfida strategica per il futuro

Infine, per tutti quei soggetti che verranno identificati come critici, la direttiva CER rappresenterà molto più di un adempimento normativo. Essa offre infatti l’opportunità di ripensare la sicurezza attraverso una prospettiva più ampia, capace di integrare protezione, continuità operativa e capacità di adattamento.
In un contesto caratterizzato da rischi sempre più interconnessi, la resilienza diventerà un elemento ancor più essenziale per garantire l’affidabilità dei servizi e la continuità operativa delle infrastrutture da cui dipendono cittadini, imprese e istituzioni: la capacità di preservare le funzioni critiche anche durante situazioni di crisi costituirà sempre più uno dei principali fattori distintivi per la sicurezza e la competitività del sistema Paese.



L’IA nelle infrastrutture del trasporto: governare prima di automatizzare

intervista ad Amir Topalovic, CEO di AISMA

Quali applicazioni di IA avete sviluppato o potreste sviluppare per i sistemi portuali e aeroportuali?
Porti e aeroporti producono ogni giorno una grande quantità di informazioni: eventi dei sistemi di sicurezza, flussi video, procedure operative, piani di security, documentazione tecnica, comunicazioni tra enti diversi. Il problema raramente è la mancanza di dati; è la difficoltà di metterli in relazione nel momento in cui occorre decidere. Per il mondo della sicurezza abbiamo sviluppato, sulla nostra piattaforma Cogniss, uno strato cognitivo che si affianca alle piattaforme PSIM esistenti senza sostituirle: ricerca in linguaggio naturale sullo storico degli eventi, classificazione automatica degli allarmi, assistenza all’operatore con il richiamo della procedura pertinente, analisi delle immagini video associate agli eventi. In porti e aeroporti gli stessi moduli possono aiutare la control room a distinguere gli allarmi rilevanti dai falsi positivi, a ricostruire in pochi secondi la cronologia di un incidente, a rendere interrogabili i piani di sicurezza e la documentazione delle infrastrutture. Lo stesso approccio vale per i processi che circondano la security: la gestione degli accessi di fornitori e operatori, il coordinamento con le autorità, la manutenzione degli impianti. Il mondo marittimo lo conosciamo da vicino. Come soci di ONTM lavoriamo con aziende del settore e, con il progetto di ricerca SEASMA, abbiamo sviluppato un sistema di monitoraggio marino e costiero che integra sensori IoT, immagini satellitari radar e droni di superficie e subacquei, con funzioni di allerta precoce validate sul campo in aree marine protette italiane. Le stesse tecniche di fusione dei dati si prestano alla sorveglianza degli specchi d’acqua portuali.

Si parla sempre più spesso di minacce combinate, multidimensionali, multidominio. In che modo l’IA risponde a esigenze sempre più articolate e complesse?



Una minaccia ibrida si riconosce dalle correlazioni: un’anomalia sulla rete informatica, un varco forzato, un drone segnalato, un’informazione che circola fuori contesto. Presi singolarmente sono eventi minori; insieme possono descrivere un attacco. L’IA è utile quando collega domini che di solito restano separati: fisico, cyber, operativo, informativo. Per farlo serve però una base di conoscenza strutturata, un’ontologia che descriva asset, aree, ruoli, procedure e relazioni, sulla quale i modelli possano ragionare. In un terminal portuale, ad esempio, significa sapere che un determinato varco serve una specifica banchina, chi è autorizzato a transitarvi e quale procedura si applica se l’evento coincide con un’anomalia di rete. Senza questa struttura un modello linguistico produce risposte plausibili, non affidabili. Con essa l’operatore riceve un quadro coerente e verificabile: ogni indicazione riporta le fonti da cui deriva. Quando la fonte manca, il sistema lo dichiara invece di colmare il vuoto con un’ipotesi. In un contesto di sicurezza, sapere di non sapere è un’informazione operativa. La complessità, in altre parole, non si affronta con modelli sempre più grandi, ma con una conoscenza meglio organizzata.

Esistono realmente dei rischi che l’IA possa sfuggire al controllo degli umani?
I rischi esistono, ma raramente hanno la forma degli scenari cinematografici. Nella pratica delle organizzazioni li vedo in tre forme molto concrete. La prima è l’opacità: sistemi che producono risposte senza che sia possibile ricostruire come vi siano arrivati. La seconda è la delega silenziosa: l’operatore che, sotto pressione, accetta il suggerimento della macchina senza verificarlo, perché nella maggior parte dei casi il suggerimento è corretto. La terza è la dipendenza: dati, conoscenza e processi critici affidati a un unico fornitore o a un’infrastruttura che l’organizzazione non controlla. In tutti e tre i casi il controllo non viene sottratto da un’IA autonoma; viene ceduto, spesso inconsapevolmente, da chi la adotta senza un’architettura di governo. Per le infrastrutture critiche è un rischio che non si può accettare, perché le conseguenze di una decisione sbagliata non restano confinate all’organizzazione che l’ha presa.

Si può fare ancora qualcosa per evitare che accada il peggio?
Si può fare molto, a partire dalla fase di progetto. Il controllo dell’IA non si aggiunge a posteriori: si progetta nell’architettura. Per questo abbiamo costruito Cogniss come un Cognitive Control Plane, un livello di governo tra dati, modelli e persone. Struttura la conoscenza in ontologie, applica regole, limiti operativi e permessi di accesso a ogni passaggio, registra ogni elaborazione in un audit trail immutabile. Il modello di IA si può sostituire senza ricostruire il sistema e la piattaforma può essere installata on-premises o in ambienti isolati dalla rete, così che i dati sensibili non escano dal perimetro dell’infrastruttura. Il principio è semplice: il sistema propone, la persona decide, e ogni decisione resta ricostruibile. Il quadro europeo va nella stessa direzione: come sottolinea l’Avv. Francesca Niola, Legal Chief di AISMA, l’AI Act pone supervisione umana e tracciabilità al centro dei sistemi ad alto rischio. Resta un elemento spesso sottovalutato, la formazione: un’organizzazione governa l’IA quando le sue persone sanno leggerne i risultati e riconoscerne i limiti.

Dalla security alla resilienza: come può un gestore portuale o aeroportuale avviare un progetto di IA in modo sostenibile?
Seguiamo un ordine preciso: prima le regole, poi le risorse, infine la soluzione. Si verifica anzitutto la conformità del progetto rispetto ad AI Act, GDPR e NIS2. Si individuano poi le leve di finanziamento disponibili, oggi significative anche per la sicurezza delle infrastrutture del trasporto. Infine si sviluppa la soluzione: un assessment iniziale dei processi, un progetto pilota su un perimetro controllato e misurabile, l’estensione alla produzione solo dopo averne validato il valore in condizioni reali. È un percorso che riduce il rischio a ogni passaggio e rende visibili fin dall’inizio costi e benefici. Resilienza, per noi, significa questo: tecnologie che rafforzano la capacità di decidere delle persone, senza creare nuove dipendenze, tecnologiche o di fornitore.

aisma

Contatti:
AISMA Srl
info@aisma.it
https://aismasrl.it/

Telecamere di rete AXIS per la protezione integrata di porti e aeroporti

intervista a Massimo Serpietri, Key Account Manager AXIS Communications

Porti e aeroporti sono infrastrutture critiche per definizione e richiedono livelli di sicurezza particolarmente elevati. Quali sono le vostre proposte?

Porti e aeroporti sono nodi essenziali per la mobilità delle persone e delle merci, ma anche sistemi complessi e in costante attività. Al loro interno convivono aree pubbliche e riservate, operatori diversi e flussi continui. Per questo la sicurezza non può basarsi su una singola tecnologia: va progettata considerando l'intero contesto e l'impatto che un'interruzione potrebbe avere sull'operatività.

La prima proposta è partire da un'analisi dei rischi e delle vulnerabilità del singolo sito. Ogni infrastruttura ha caratteristiche proprie: dimensioni, configurazione degli spazi, flussi, sistemi installati e livelli di esposizione. L'analisi consente di definire le priorità e scegliere misure proporzionate alle esigenze effettive.

Da qui si può costruire una protezione integrata. Le telecamere di rete Axis, selezionate in base alle condizioni ambientali e alle necessità operative, possono contribuire al monitoraggio di accessi, perimetri, aree estese e punti sensibili. Le esigenze variano: in ambito portuale possono essere determinanti le grandi distanze e le condizioni ambientali; in aeroporto, la densità dei flussi e la necessità di garantire continuità operativa.

La videosorveglianza può essere integrata con sistemi di gestione video, controllo degli accessi e altre tecnologie compatibili, così da presentare agli operatori informazioni utili in un quadro coerente. Le soluzioni Axis sono progettate per integrarsi con piattaforme e dispositivi di terze parti, secondo le caratteristiche dell'architettura adottata. L'obiettivo è valorizzare gli impianti esistenti e ridurre i sistemi isolati.

Anche l'analisi video può supportare il lavoro degli operatori. AXIS Object Analytics, disponibile su telecamere compatibili, può rilevare e classificare determinati oggetti o situazioni e generare eventi configurabili. In questo modo può richiamare l'attenzione su un'area o un evento, in base al caso d'uso e alle condizioni del sito. Non sostituisce la verifica dell'operatore: contribuisce a indirizzarne l'attenzione.



In un'infrastruttura critica contano anche affidabilità, manutenzione e protezione dei dispositivi connessi. La cybersecurity deve essere considerata lungo tutto il ciclo di vita: dalla configurazione iniziale alla gestione degli accessi e degli aggiornamenti.

Infine, la tecnologia deve inserirsi in procedure chiare: chi riceve un allarme, chi lo verifica e chi interviene. Servono personale formato, esercitazioni e collaborazione tra gestori, autorità, forze dell'ordine e operatori. L'obiettivo non è semplicemente "vedere di più", ma comprendere meglio gli eventi e rispondere in modo tempestivo e proporzionato, sostenendo la continuità dei servizi e la resilienza dell'infrastruttura.

Si parla sempre più spesso di minacce combinate, multidimensionali e multidominio. Come rispondete a esigenze sempre più articolate e complesse?

Le minacce attuali possono coinvolgere contemporaneamente più ambiti. Un problema fisico può incidere sull'operatività di un sistema; un attacco informatico può compromettere strumenti di monitoraggio; un evento isolato può aggravarsi se non viene riconosciuto e condiviso in tempo. Per questo la risposta deve superare la logica dei sistemi separati e collegare informazioni, persone e procedure.

L'integrazione aiuta a ridurre la frammentazione. Le telecamere Axis possono essere collegate a piattaforme di gestione video, sistemi di controllo degli accessi e altre applicazioni compatibili. In base all'architettura adottata, un allarme può essere associato alle immagini dell'area interessata o alle procedure operative pertinenti. Gli operatori possono così disporre di un quadro più coerente e verificare gli eventi con maggiore rapidità.

Anche l'analisi direttamente a bordo delle telecamere compatibili può essere utile. Applicazioni come AXIS Object Analytics possono generare eventi quando rilevano condizioni configurate, ad esempio la presenza o il movimento di determinati oggetti in aree definite. Questi strumenti aiutano a indirizzare l'attenzione, ma non interpretano da soli l'intero scenario: l'evento va valutato nel contesto e secondo le procedure del sito.

La resilienza dipende anche dalla capacità di far evolvere sistemi spesso installati in periodi diversi e forniti da produttori differenti. Un approccio basato su integrazioni e standard consente di valorizzare gli investimenti esistenti e introdurre miglioramenti gradualmente. È inoltre necessario pianificare manutenzione, aggiornamenti, gestione delle credenziali e protezione dei dispositivi di rete. Sicurezza fisica e informatica sono sempre più interdipendenti.

La tecnologia, tuttavia, non sostituisce la cooperazione. Occorrono ruoli definiti, canali di comunicazione adeguati e procedure condivise tra chi gestisce l'infrastruttura e gli altri soggetti coinvolti. Le esercitazioni permettono di verificare non solo gli strumenti, ma anche la capacità delle persone di collaborare sotto pressione.

In un contesto multidominio, il valore delle soluzioni non si misura dal numero di dispositivi installati, ma dalla loro capacità di integrarsi in processi affidabili. L'obiettivo è ridurre i punti ciechi e migliorare il coordinamento, mantenendo chiare le responsabilità e la supervisione umana.

Dal vostro punto di osservazione, quali sono i vantaggi e i rischi delle applicazioni di IA per migliorare la sicurezza di porti e aeroporti?

L'intelligenza artificiale può aiutare gli operatori a gestire grandi quantità di informazioni e a individuare situazioni che meritano attenzione. In porti e aeroporti, dove i flussi sono continui e le aree da monitorare possono essere estese, l'analisi automatizzata può contribuire a evidenziare eventi o a rendere più rapida la ricerca di una specifica situazione. Nel portfolio Axis, AXIS Object Analytics è un esempio di analisi video disponibile su telecamere compatibili. A seconda del modello e della configurazione, può rilevare e classificare determinati oggetti e generare eventi secondo regole definite. Può, per esempio, segnalare presenze o movimenti in aree configurate, quando il caso d'uso e le condizioni ambientali lo consentono. Le prestazioni dipendono dal dispositivo, dalla scena e dalla corretta configurazione.

Il vantaggio principale dell'IA non è eliminare il ruolo umano, ma rendere più efficace il lavoro delle persone. Un operatore che riceve informazioni pertinenti può verificare prima un allarme e dedicare più tempo alle decisioni che richiedono esperienza e conoscenza del contesto. L'analisi automatizzata deve quindi supportare il giudizio umano, non sostituirlo.

È importante considerare anche i limiti. Un sistema può generare falsi allarmi o non rilevare una situazione. Illuminazione, angolazione, occlusioni, densità dei flussi e condizioni ambientali possono influire sui risultati. Per questo le applicazioni vanno testate nelle condizioni reali del sito, verificate e monitorate nel tempo.

Ci sono inoltre aspetti di governance: bisogna chiarire quali dati vengono trattati, per quali finalità, per quanto tempo e da chi possono essere consultati. La progettazione deve rispettare la normativa applicabile e tutelare la privacy. Anche la cybersecurity è centrale: telecamere, applicazioni e sistemi di gestione devono essere protetti e mantenuti aggiornati.

Una segnalazione automatica va interpretata nel contesto e verificata da personale qualificato, soprattutto quando può avere conseguenze rilevanti per le persone o per l'operatività. Gli operatori devono conoscere le capacità e i limiti dello strumento e sapere come comportarsi quando il risultato non è attendibile.

L'approccio corretto è partire da un'esigenza precisa, definire criteri di efficacia e responsabilità, effettuare test e mantenere la supervisione umana. L'IA può contribuire alla sicurezza di porti e aeroporti quando è affidabile, governata con attenzione e integrata nei processi: non è una soluzione autonoma alla complessità, ma uno strumento a supporto di decisioni migliori e di infrastrutture più resilienti.

AXIS COMMUNICATIONS

Contatti:
Axis Communications
Tel. +39 02 8424 5762
www.axis.com

Sicurezza di porti e aeroporti: integrazione, resilienza e intelligenza artificiale

intervista a Massimo Broetto, Sales Director Italia EL.MO. S.p.a

Porti e aeroporti sono infrastrutture critiche per definizione, che richiedono livelli di sicurezza particolarmente elevati. Quali sono le vostre proposte?

Porti e aeroporti sono ecosistemi complessi, nei quali convivono flussi elevati di persone e merci, aree ad accesso controllato, infrastrutture tecnologiche e servizi essenziali. La loro protezione richiede quindi un approccio che superi la logica del singolo impianto e consideri la sicurezza come un sistema integrato, in grado di prevenire le minacce, gestire tempestivamente gli eventi e garantire la continuità operativa.

In EL.MO. riteniamo fondamentale partire da un'analisi puntuale del rischio e delle caratteristiche dell'infrastruttura, per individuare le vulnerabilità e definire soluzioni proporzionate alle effettive esigenze. Videosorveglianza, antintrusione, controllo degli accessi e supervisione devono poter operare in modo coordinato, offrendo agli operatori una visione chiara e tempestiva di ciò che accade.

L'integrazione è un fattore decisivo: correlare le informazioni provenienti da sistemi diversi consente di ridurre la frammentazione degli allarmi, migliorare la verifica degli eventi e rendere più efficaci le procedure di intervento. È altrettanto importante progettare architetture affidabili, con adeguate misure di protezione informatica e piani di continuità operativa.

La tecnologia, tuttavia, da sola non basta. Servono procedure condivise, personale formato, manutenzione costante e collaborazione tra gestori, autorità e operatori della sicurezza.

La nostra visione è quella di una sicurezza scalabile e integrata, progettata sulle specificità del sito e capace di evolvere nel tempo. Perché proteggere un'infrastruttura critica significa non soltanto impedire un accesso non autorizzato, ma anche preservare la disponibilità dei servizi e la capacità di reagire a situazioni impreviste.



Si parla sempre più spesso di minacce combinate, multidimensionali e multidominio. In che modo rispondete a esigenze sempre più articolate e complesse?

La complessità attuale nasce dall'interconnessione delle minacce. Un attacco informatico, un tentativo di intrusione fisica, un'interferenza nelle comunicazioni o un'interruzione di un servizio essenziale possono verificarsi contemporaneamente oppure rappresentare fasi successive di uno stesso scenario. Il rischio, quindi, non riguarda più soltanto il singolo dispositivo o la singola area, ma le relazioni tra sistemi e le conseguenze che un evento può produrre sull'intera infrastruttura.

Per affrontare questa evoluzione occorre superare la separazione tradizionale tra sicurezza fisica e sicurezza digitale. In EL.MO. consideriamo centrali l'integrazione dei sistemi, la gestione coordinata degli eventi e la possibilità di fornire agli operatori informazioni comprensibili e immediatamente utilizzabili. Un allarme assume infatti un valore maggiore quando può essere contestualizzato e verificato attraverso le informazioni disponibili, consentendo di stabilire priorità e modalità di intervento.

Questo approccio richiede anche attenzione alla resilienza: occorre prevedere come mantenere le funzioni essenziali in caso di guasto, compromissione di un sistema o indisponibilità temporanea di alcuni servizi. Ridondanza, segmentazione delle reti, aggiornamenti, controllo degli accessi informatici e procedure di ripristino sono elementi da considerare fin dalla progettazione.

Un altro aspetto fondamentale è la collaborazione. Nessun singolo operatore dispone, da solo, di tutte le informazioni necessarie per affrontare una minaccia multidominio. La condivisione strutturata dei dati, nel rispetto delle responsabilità e delle normative applicabili, e l'adozione di procedure comuni possono migliorare sensibilmente la capacità di risposta.

La sfida per un'azienda tecnologica come EL.MO. è contribuire a costruire sistemi affidabili, integrabili e adattabili, evitando che l'aumento delle tecnologie si traduca in una maggiore complessità gestionale. L'obiettivo finale è consentire a chi opera sul campo di avere una visione più completa degli eventi e strumenti efficaci per intervenire, mantenendo sempre chiare le responsabilità decisionali.

Dal vostro punto di osservazione, quali sono i vantaggi e i rischi delle applicazioni di IA per migliorare la sicurezza di porti e aeroporti?

L'intelligenza artificiale offre opportunità significative per migliorare la capacità di analisi e di gestione degli eventi, soprattutto in contesti caratterizzati da grandi spazi, flussi continui e volumi elevati di informazioni. Il suo principale vantaggio è la possibilità di trasformare i dati raccolti dai sistemi di sicurezza in segnalazioni più pertinenti, aiutando gli operatori a individuare situazioni che meritano attenzione e a intervenire con maggiore tempestività.

Nella videosorveglianza, ad esempio, la videoanalisi intelligente può contribuire a rilevare anomalie, attraversamenti di aree interdette o oggetti abbandonati, secondo le funzionalità effettivamente disponibili e configurate. Se integrati con gli altri sistemi di sicurezza, questi strumenti possono facilitare la verifica degli allarmi, ridurre le attività ripetitive e migliorare la gestione delle priorità. L'obiettivo non è generare più segnalazioni, ma fornire informazioni realmente utili.

I vantaggi, però, dipendono dalla qualità dell'implementazione. Gli algoritmi possono produrre falsi positivi o non rilevare un evento, anche in funzione delle condizioni ambientali, della qualità delle immagini e delle caratteristiche dello scenario. È quindi indispensabile effettuare test adeguati, verificare le prestazioni nelle condizioni operative reali e aggiornare periodicamente configurazioni e procedure.

Esistono inoltre rischi legati alla protezione dei dati personali, alla cybersecurity e all'eccessiva fiducia nell'automazione. Le applicazioni devono essere progettate nel rispetto della normativa, con misure di sicurezza adeguate e responsabilità chiaramente definite. In un'infrastruttura critica è essenziale che gli operatori possano comprendere e verificare le segnalazioni e che le decisioni più rilevanti non vengano affidate acriticamente a un algoritmo.

Dal nostro punto di vista, l'intelligenza artificiale deve essere considerata uno strumento a supporto delle competenze umane, non un sostituto del presidio professionale. La tecnologia può accelerare l'analisi e migliorare la capacità di individuare anomalie, ma il contesto, la valutazione del rischio e la decisione operativa restano elementi fondamentali.

Per EL.MO. la direzione da seguire è dunque un'innovazione concreta, misurabile e responsabile, nella quale l'IA sia inserita in un'architettura di sicurezza affidabile, integrata e resiliente. Non si tratta di adottare la tecnologia più avanzata in assoluto, ma di scegliere quella più adatta a risolvere un problema reale, garantendo efficacia, sostenibilità e tutela delle persone.

Contatti:
EL.MO. Spa
Tel. +39 049 9203333
info@elmospa.com

OPTEX, qualità e innovazione per contrastare le minacce combinate alle Infrastrutture critiche

intervista a Andrea Tiberti, Technical Manager OPTEX

Porti e aeroporti sono infrastrutture critiche per definizione che richiedono livelli di sicurezza globale particolarmente elevati. Quali sono le vostre proposte?
Porti e aeroporti sono nodi essenziali per la mobilità delle persone, il commercio e il funzionamento delle catene di approvvigionamento. La loro protezione presenta sfide specifiche: perimetri estesi, aree operative molto diverse tra loro, condizioni ambientali variabili e un flusso continuo di veicoli, merci e persone. In questi contesti, un'intrusione o un'interruzione delle attività può avere conseguenze che vanno ben oltre il singolo sito.
OPTEX propone un approccio alla sicurezza basato sul rilevamento affidabile di tentativi di intrusione e sulla combinazione di tecnologie complementari, selezionate in funzione delle caratteristiche dell'infrastruttura e dei rischi da affrontare. L'obiettivo è individuare tempestivamente un evento potenzialmente pericoloso, fornire informazioni utili per verificarlo e consentire al personale di sicurezza di intervenire prima che la minaccia raggiunga un'area sensibile.
Per la protezione perimetrale, le soluzioni in fibra ottica permettono di rilevare tentativi di scavalcamento, taglio o manomissione di recinzioni e altre barriere fisiche. A seconda della tecnologia utilizzata, il cavo sensore può essere installato sulla recinzione, integrato in una struttura oppure interrato. Si tratta di una soluzione particolarmente interessante per i siti che richiedono la supervisione di tratti molto estesi.
La tecnologia LiDAR della serie REDSCAN consente invece di creare aree di rilevamento virtuali, configurabili in funzione della geometria e delle esigenze del sito. Può essere utilizzata, ad esempio, per proteggere accessi, facciate, coperture e zone in cui è necessario individuare un movimento non autorizzato.
Queste tecnologie possono essere integrate con i sistemi di videosorveglianza e con le piattaforme di gestione della sicurezza già presenti nell'infrastruttura. In questo modo



il rilevamento può attivare una verifica visiva dell'evento e fornire agli operatori informazioni più precise per valutare la situazione.
Non esiste, naturalmente, una configurazione valida per ogni porto o aeroporto. La scelta delle soluzioni deve partire dall'analisi delle vulnerabilità, delle condizioni ambientali e delle procedure operative. È questa combinazione tra valutazione del rischio, progettazione, tecnologie adeguate e integrazione a consentire una protezione efficace, senza compromettere la continuità operativa.

Si parla sempre più spesso di minacce combinate, multidimensionali, multidominio. In che modo rispondete a esigenze sempre più articolate e complesse?
La crescente complessità delle minacce richiede di superare una concezione della sicurezza basata su dispositivi isolati o singole tecnologie. Un'infrastruttura può essere esposta contemporaneamente a tentativi di intrusione fisica, sabotaggio, accessi non autorizzati e minacce informatiche che interessano i sistemi di controllo e le reti di comunicazione. È quindi fondamentale valutare non solo le singole vulnerabilità, ma anche le loro possibili interazioni e gli effetti che un evento in un ambito può produrre sugli altri.
Un approccio efficace richiede tecnologie affidabili, adatte alle specifiche condizioni operative e capaci di fornire allarmi tempestivi. È inoltre importante combinare sistemi con funzioni complementari, evitando di affidare la protezione a un unico principio di rilevamento.
OPTEX propone soluzioni integrabili in un sistema multilivello. I sistemi in fibra ottica proteggono perimetri estesi, rilevando tentativi di manomissione o attraversamento delle recinzioni. Il LiDAR della serie REDSCAN crea aree di rilevamento virtuali per proteggere accessi, facciate e zone sensibili, mentre le barriere a infrarossi consentono di controllare passaggi specifici. L'integrazione con la videosorveglianza e con i sistemi di gestione della sicurezza facilita la verifica degli allarmi e aiuta gli operatori a valutarne la natura.
Un altro aspetto fondamentale è la continuità operativa. Alcune soluzioni Fiber SenSys, come EchoPoint e Point Defender, integrano meccanismi di ridondanza e tolleranza ai guasti. Quando è installato in configurazione ad anello, EchoPoint può mantenere il rilevamento anche in caso di taglio del cavo; inoltre, può prevedere un secondo processore che subentra in caso di guasto. Point Defender è invece progettato per mantenere il rilevamento in presenza di un singolo taglio del cavo, grazie alla configurazione del sistema e alla collaborazione tra i processori.
Anche le reti di comunicazione devono essere protette da accessi non autorizzati e attacchi informatici. Misure come VPN, segmentazione della rete e controllo degli accessi devono essere definite in base all'architettura e ai rischi dell'infrastruttura, insieme a soluzioni di backup e procedure di ripristino.
Il contributo di OPTEX consiste nel fornire tecnologie di rilevamento che possano essere combinate e integrate in architetture di sicurezza più ampie. L'obiettivo è costruire un sistema coerente e resiliente, in cui protezione fisica, continuità operativa e sicurezza delle comunicazioni concorrano alla protezione dell'intera infrastruttura.

Dal vostro punto di osservazione, quali sono i vantaggi e i rischi delle applicazioni di IA per migliorare la sicurezza dei porti e degli aeroporti?
L'intelligenza artificiale è una tecnologia relativamente giovane nel settore della sicurezza, ma presenta potenzialità considerevoli, soprattutto nell'analisi delle informazioni e nel supporto agli operatori. Il suo sviluppo merita attenzione, mantenendo un approccio pragmatico e una valutazione concreta dei benefici che può offrire.
Per OPTEX, l'affidabilità del rilevamento rimane un principio fondamentale. Rilevamento e analisi svolgono infatti funzioni diverse: il primo individua un evento, come un tentativo di intrusione o un movimento in un'area protetta; la seconda elabora le informazioni disponibili per interpretarlo e supportare le decisioni degli operatori. L'IA può contribuire, ad esempio, all'analisi delle immagini e alla verifica degli allarmi, integrandosi con tecnologie di rilevamento dedicate. Le due funzioni sono complementari ma distinte, perché l'efficacia dell'analisi dipende anche dalla qualità delle informazioni ricevute.
Occorre tuttavia considerare i possibili limiti, come i falsi allarmi, gli eventi non riconosciuti e l'eccessiva dipendenza dall'automazione. Le prestazioni devono essere verificate nelle reali condizioni operative e il personale deve mantenere un ruolo centrale nella valutazione degli eventi e nelle decisioni.
In definitiva, l'IA può contribuire a rendere più efficiente la gestione della sicurezza, purché sia utilizzata in modo responsabile e integrata correttamente con le tecnologie esistenti. Per OPTEX, l'innovazione deve rispondere a un'esigenza concreta: migliorare la capacità di rilevare una minaccia e fornire informazioni utili, mantenendo affidabilità e attenzione alle responsabilità che accompagnano ogni sistema di sicurezza.

OPTEX Sensing Innovation

Contatti:
OPTEX
Tel. +39 351 9272789
enquiry-it@optex-europe.com
www.optex-europe.com/it

Bodycam,
il valore delle prove oggettive

intervista a Luigi Lagonigro, Head of Sales Europe & Latam Reveal Media

Porti e aeroporti sono infrastrutture critiche che richiedono livelli di sicurezza particolarmente elevati. Quali sono le vostre proposte?
La nostra proposta parte dalla protezione delle persone che lavorano ogni giorno sul campo: addetti alla sicurezza, personale operativo e operatori a contatto con il pubblico. In ambienti complessi come porti e aeroporti, le bodycam aggiungono un punto di vista mobile alla videosorveglianza fissa, documentando ciò che accade durante un controllo, un intervento o una situazione di tensione.
Per Reveal, il valore è nell'intero processo: dalla ripresa alla gestione delle evidenze video, fino alla possibilità, nelle configurazioni abilitate, di condividere immagini in diretta con la sala operativa. Questo permette a chi coordina l'intervento di comprendere meglio il contesto e supportare il personale. Proponiamo quindi un percorso che parte dalle esigenze del sito e comprende scelta dei dispositivi, gestione dei filmati, formazione e verifica sul campo.
L'obiettivo è offrire agli operatori uno strumento semplice da utilizzare e utile nelle condizioni reali di lavoro.



Si parla sempre più spesso di minacce combinate, multidimensionali e multidominio. In che modo rispondete a esigenze sempre più articolate e complesse?
La risposta deve essere coordinata, perché nessun singolo dispositivo può coprire tutte le dimensioni della sicurezza. Il nostro contributo consiste nel collegare meglio ciò che accade sul campo con le informazioni disponibili alla sala operativa. Pensiamo a un controllo a un accesso che si trasforma in una situazione critica: le telecamere fisse mostrano il contesto generale, mentre la bodycam può documentare l'interazione dalla prospettiva dell'operatore. Dove è previsto lo streaming, queste immagini possono aiutare la sala operativa a valutare la situazione e coordinare il supporto.
Per questo puntiamo sull'integrazione con i sistemi esistenti, verificando compatibilità, connettività e responsabilità operative. Prima di un'estensione su larga scala, riteniamo fondamentale una prova sul campo con criteri di successo condivisi. La complessità va gestita nella progettazione, affinché l'utilizzo resti semplice per chi deve intervenire.

Dal vostro punto di osservazione, quali sono i vantaggi e i rischi delle applicazioni di IA per migliorare la sicurezza dei porti e degli aeroporti?
Il vantaggio principale dell'IA è aiutare gli operatori a individuare informazioni rilevanti all'interno di grandi quantità di dati. Nelle applicazioni opportunamente validate, può velocizzare la ricerca nei filmati, supportare l'analisi degli eventi e richiamare l'attenzione su situazioni da verificare. Il beneficio concreto è rendere più tempestiva e informata la valutazione umana.
I rischi riguardano soprattutto falsi allarmi, eventi non rilevati, risultati distorti e un'eccessiva fiducia nell'automazione. In un porto o in un aeroporto, un'indicazione errata può assorbire risorse o condizionare una decisione operativa. A questo si aggiungono la protezione dei dati e la sicurezza dei sistemi di IA stessi.
La nostra posizione è che ogni applicazione debba partire da un'esigenza precisa ed essere verificata nell'ambiente in cui verrà utilizzata. Servono dati affidabili, accessi controllati, tracciabilità e supervisione umana. L'efficacia va misurata sul miglioramento del lavoro e della sicurezza, mantenendo chiara la responsabilità delle decisioni.

I vantaggi delle bodycam in porti, aeroporti e stazioni

Deterrenza e de-escalation:
Lo schermo frontale mostra la persona che viene ripresa, e spesso basta a calmare la situazione.

Più sicurezza per il personale:
Addetti ai controlli, steward, capitreno e guardie giurate si sentono più protetti nei punti di contatto con il pubblico.

Intervento più rapido:
Con SOS, GPS e video in diretta la sala operativa vede subito cosa accade e dove inviare i soccorsi.

Prove oggettive:
Registrazioni cifrate e tracciate aiutano denunce, indagini e la gestione di reclami e contestazioni. Copertura dove le telecamere fisse non arrivano: banchine, piazzali, treni, aree di imbarco e zone temporanee.

Formazione e miglioramento:
Gli episodi registrati aiutano a rivedere procedure e formazione sulla gestione dei conflitti.

Contatti:
Reveal
sales@revealmedia.com
www.revealmedia.it

Bodycam e vigilanza privata: bilanciamento tra sicurezza e privacy

di Diego Di Simone Perricone, Senior Security Manager Certificato UNI 10459 ed esperto ESRM. CISO e DPO



Il Garante della Privacy ha delineato le condizioni di liceità per l'uso di bodycam da parte delle Guardie Particolari Giurate (GPG). Gli istituti di vigilanza privata possono dotare il personale di videocamere indossabili, purché l'attivazione sia circoscritta a situazioni emergenziali, eventi reato o scenari in cui la ripresa sia strettamente necessaria quale ausilio alle indagini della polizia giudiziaria.
L'adozione delle bodycam nel settore della vigilanza privata richiede un rigido coordinamento normativo che intreccia la disciplina sulla protezione dei dati personali e il diritto del lavoro. La nota del Dipartimento Attività Economiche e Lavoro del Garante della Privacy (*) ha chiarito la necessità di non confondere i compiti delle Guardie Particolari Giurate (GPG) con le attività di law enforcement statale (regolate dal D.Lgs. 51/2018), riconducendo l'uso dei dispositivi sotto l'alveo del Regolamento (UE) 2016/679 (GDPR).
I dati raccolti tramite le bodycam sono utilizzabili a tutti i fini connessi al rapporto di lavoro (anche disciplinari) solo se il datore di lavoro ha fornito al dipendente una piena e adeguata informativa sulle modalità d'uso dei dispositivi e l'effettuazione dei controlli, nel rispetto di quanto previsto dal GDPR.
Le bodycam, pur essendo indossate dalle GPG per motivi di sicurezza, tutela dei beni e documentazione di illeciti, sono per loro natura strumenti tecnologici capaci di registrare immagini e audio relativi al lavoratore stesso, traducendosi in un potenziale controllo a distanza dell'attività lavorativa. Pertanto la legittimità dell'infrastruttura è rigidamente subordinata al rispetto dell'art. 4 della Legge n. 300/1970 (Statuto dei Lavoratori), come riformato dal Jobs Act (D.Lgs. 151/2015):
1. Divieto di controllo intenzionale e presupposti: È tassativamente vietato l'uso di apparecchiature con la sola finalità di monitorare la prestazione del dipendente. L'installazione e l'impiego sono consentiti esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Quindi, l'attività delle GPG (difesa di beni mobili e immobili) rientra pienamente in tali tutele.
2. La procedura codeterminata (Accordo o Autorizzazione): Prima di mettere in esercizio i dispositivi, l'Istituto di vigilanza (Titolare del trattamento) ha l'obbligo tassativo di sottoscrivere un accordo collettivo con le rappresentanze sindacali aziendali (RSU/RSA).
3. L'attivazione manuale da parte della GPG unicamente in presenza di un pericolo concreto o di un reato in corso, unita alla redazione di una relazione giustificativa dettagliata, rappresenta la misura organizzativa corretta per dimostrare che il sistema non effettua un monitoraggio massivo o ingiustificato da parte dell'operatore, rispettando i canoni di proporzionalità e necessità imposti sia dall'art. 4 dello Statuto sia dall'art. 35 del GDPR.
È consigliabile che la conservazione delle immagini non superi le 72 ore, termine oltre il quale si impone la cancellazione automatica. Sotto il profilo procedurale, la GPG è tenuta a redigere una relazione di servizio dettagliata che giustifichi l'impiego del dispositivo, esplicitando le ragioni e la necessità operativa della registrazione.
In un'ottica di privacy by design, la memorizzazione dei dati su server interni aziendali è preferibile rispetto a soluzioni cloud, poiché garantisce una maggiore robustezza e sicurezza della tenuta del sistema informatico contro le violazioni (data breach). Pilastro della conformità resta l'obbligo in capo al Titolare di redigere e custodire la DPIA (Valutazione di Impatto). Se l'indice di rischio rilevato è basso o medio, il documento va conservato ed esibito in caso di controlli da parte dell'Autorità. Qualora l'indice sia alto, sarà necessario adire, per ottenere la prescritta autorizzazione preventiva, l'Ufficio del Garante ai sensi dell'art. 36 GDPR.

(*) GPDP.Ufficio.Protocollo:U:0141218.05/10/2026 – DAEL/LG/522419-1/ istanza relativa all'adozione di dispositivi di videoregistrazione individuale ("bodycam"). Invio chiarimenti.

ERMES: L'EVOLUZIONE DELLA SICUREZZA FISICA E LOGICA IN AZIENDA

Controllo totale e sicuro per il tuo ecosistema aziendale



Dalla porta d'ingresso al login del PC. Abbandona le password vulnerabili e passa alla *Strong Authentication* con lettori e carte sicure di altissima qualità.

QUALITÀ TOP DI GAMMA
Integrazione dei migliori lettori professionali sul mercato, come la linea HID Omnikey, sinonimo di massima affidabilità nel tempo.

ACCESSO CENTRALIZZATO
Un'unica tessera tecnologica per gestire l'apertura dei varchi fisici, il login sicuro a PC/reti e l'uso delle stampanti condivise.

INTEGRAZIONE FLUIDA
Sistemi hardware studiati per dialogare perfettamente con la tua infrastruttura attuale, assicurando un'integrazione rapida e sicura.

info@ermes-online.it www.ermes-online.it 051 757040

ermes your business partner

Cube Protection Central integra mappe CAD e AI nella gestione della sicurezza

comunicato aziendale

La piattaforma Life3 affianca alla supervisione degli impianti le planimetrie DWG e DXF e nuove funzioni di analisi degli eventi, a supporto degli operatori e dei responsabili della sicurezza.

Localizzare un allarme, verificare quali dispositivi siano coinvolti e comprendere il contesto sono attività quotidiane per chi presidia una centrale operativa. Quando gli impianti appartengono a marchi diversi o sono distribuiti su più sedi, queste operazioni possono richiedere la consultazione di applicazioni e documenti separati, con un maggiore impegno per ricostruire ciò che sta accadendo.
Cube Protection Central, sviluppata da Life3, centralizza le informazioni provenienti dai sistemi di sicurezza integrati e le rende consultabili in un unico ambiente. La piattaforma si rivolge a centrali operative, security manager e organizzazioni multisede che devono supervisionare impianti antintrusione e antincendio, gestire le segnalazioni e disporre di riferimenti utili per gli interventi. Le evoluzioni dedicate alle mappe CAD e all'intelligenza artificiale intervengono su due esigenze: individuare gli eventi nello spazio e facilitarne l'analisi.

Supervisione di impianti e sedi differenti

La gestione centralizzata consente di consultare eventi e stati degli impianti collegati, associando le segnalazioni al sito e ai dispositivi da cui provengono. L'operatore può così inquadrare un'anomalia all'interno dell'ambiente presidiato e accedere alle informazioni disponibili senza ricomporre ogni volta il quadro attraverso strumenti distinti. Le possibilità di interazione dipendono dalle apparecchiature connesse e dai protocolli di integrazione disponibili. Ove supportato, il collegamento bidirezionale permette anche di operare sui sistemi dal software, secondo le autorizzazioni assegnate. La definizione delle integrazioni



e dei profili utente resta quindi un passaggio essenziale nella configurazione della soluzione.

Planimetrie CAD per localizzare gli eventi

Una delle evoluzioni di Cube Protection Central riguarda la gestione delle planimetrie CAD nei formati DWG e DXF. Il disegno dell'edificio entra nell'ambiente di supervisione e diventa un riferimento grafico per individuare aree e dispositivi. Le funzioni di zoom e navigazione permettono di passare dalla vista generale del sito al dettaglio di un locale o di un apparato.
La rappresentazione grafica affianca l'elenco degli eventi e ne facilita la lettura. La posizione di un dispositivo, il locale in cui si trova e la vicinanza ad altri elementi dell'impianto offrono indicazioni utili per comprendere una segnalazione e orientare le verifiche successive. Il beneficio è particolarmente rilevante negli edifici articolati o nei siti con un'elevata densità di dispositivi.
L'efficacia della mappa dipende dalla qualità delle planimetrie e dalla corretta associazione tra elementi grafici e dispositivi reali. Mantenere coerente questa rappresentazione con le modifiche apportate agli impianti permette agli operatori di utilizzare riferimenti attendibili durante la gestione degli eventi.

Un esempio nella gestione di un allarme

Si consideri, a titolo esemplificativo, una segnalazione proveniente da un sensore installato in un magazzino. Nell'elenco eventi l'operatore trova il riferimento tecnico del dispositivo; sulla planimetria ne individua la posizione rispetto al locale e alle aree circostanti. Può quindi consultare gli stati e le altre informazioni rese disponibili dall'integrazione, verificando se siano presenti ulteriori segnalazioni utili a inquadrare la situazione.
Questo percorso facilita il passaggio dalla ricezione dell'allarme alla valutazione del contesto e alla scelta delle azioni previste dalle procedure interne. La disponibilità di riferimenti grafici condivisi agevola anche il confronto tra la centrale operativa e il personale che deve effettuare una verifica sul posto.

AI per analizzare gli eventi e le ricorrenze

Alle funzioni di supervisione si affiancano nuove funzionalità di intelligenza artificiale (AI), dedicate all'analisi degli eventi raccolti dalla piattaforma. Il loro impiego supporta la consultazione delle informazioni e l'individuazione di anomalie e problematiche ricorrenti negli impianti di security e safety. La generazione di report sintetici facilita la comprensione di quanto accaduto e offre elementi utili per gli approfondimenti tecnici e organizzativi. In presenza di numerose segnalazioni, una sintesi aiuta il personale a orientarsi nei dati e a individuare gli aspetti da verificare sullo storico disponibile.

Un possibile ambito di utilizzo è l'esame delle segnalazioni ripetute relative a uno stesso dispositivo o a una determinata area. L'analisi può aiutare a riconoscere una ricorrenza da approfondire, mettendo a disposizione elementi per successive verifiche sul campo. La diagnosi della causa e la scelta dell'intervento richiedono la valutazione del personale competente.
I risultati prodotti dall'AI restano soggetti alla verifica degli operatori, cui competono le valutazioni finali e le decisioni operative. La qualità dell'analisi dipende anche dalla completezza delle informazioni raccolte e dalla corretta configurazione degli impianti integrati.

Strumenti per il lavoro della centrale operativa

Per una rete di punti vendita, un gruppo industriale o un'organizzazione con sedi distribuite, disporre di un ambiente comune facilita la consultazione delle informazioni dei diversi siti. Le mappe CAD aiutano a localizzare le segnalazioni, mentre le funzioni AI supportano la lettura degli eventi e la preparazione di sintesi utili agli approfondimenti.
Il valore operativo di Cube Protection Central si misura nella possibilità di accedere ai dati disponibili con riferimenti chiari, comprendere meglio le situazioni e coordinare le verifiche necessarie. La piattaforma offre strumenti a supporto delle procedure e delle competenze delle persone chiamate a presidiare gli impianti ogni giorno.

Life3

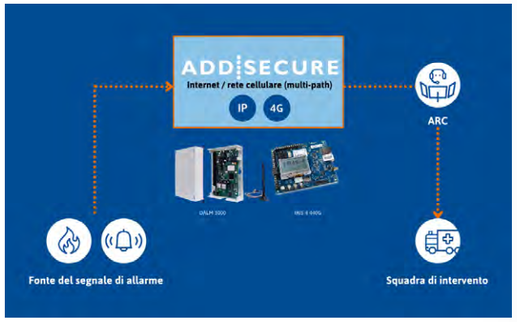
Contatto:
Life3 Srl
Tel. 045 485 25 29
info@life3.it

Oltre la conformità: perché le norme EN 54-21 ed EN 50136 sono importanti nella trasmissione degli allarmi antincendio

comunicato aziendale

Quando scatta un allarme antincendio, il segnale deve raggiungere la destinazione corretta affinché si possa intervenire tempestivamente. Una trasmissione affidabile degli allarmi è quindi un elemento fondamentale della sicurezza antincendio.
Ma come puoi verificare che le apparecchiature che scegli soddisfino i requisiti della tua applicazione? Norme come EN 54-21 ed EN 50136 ti aiutano a prendere decisioni consapevoli.
Per AddSecure, la certificazione non significa soltanto soddisfare requisiti tecnici. Dimostra che le apparecchiature sono state sottoposte a valutazioni specifiche e ti aiuta a scegliere le soluzioni con maggiore sicurezza.

Due norme con ruoli complementari
La norma EN 54-21 specifica i requisiti e i metodi di prova per le apparecchiature di trasmissione degli allarmi e di segnalazione dei guasti utilizzate con i sistemi di rilevazione e di allarme incendio.
La serie EN 50136 riguarda più in generale i sistemi e le apparecchiature di trasmissione degli allarmi. La EN 50136-1 definisce i requisiti a livello di sistema, comprese le prestazioni e l'affidabilità. La EN 50136-2 riguarda le apparecchiature di ricetrasmissione presso i locali protetti, sottoposte a supervisione.
Le due norme svolgono ruoli complementari. Insieme, contribuiscono infatti a definire i requisiti in base ai quali vengono valutate le apparecchiature e i sistemi interessati. Quando scegli le apparecchiature per un impianto antincendio, è importante conoscere l'ambito di applicazione di ciascuna norma. Questo ti aiuta a valutare se una soluzione è adatta all'utilizzo previsto e ai requisiti specifici dell'impianto.
La certificazione non elimina ogni possibile rischio di guasto. Non sostituisce neppure una corretta progettazione, installazione e manutenzione del sistema. Fornisce invece evidenza del fatto che i requisiti pertinenti sono stati valutati.



Perché la certificazione è importante
La connettività IP e le reti mobili offrono maggiore flessibilità nella trasmissione degli allarmi. Tuttavia, la sola connettività non garantisce che un'apparecchiatura soddisfi i requisiti di una determinata applicazione.
È importante considerare anche le prestazioni, la supervisione e le certificazioni pertinenti.
Le norme riconosciute ti offrono una base più chiara per valutare le apparecchiature. Ti aiutano a:
• **Scegliere le apparecchiature più adatte.** Individua i requisiti applicabili al tuo impianto e verifica le certificazioni pertinenti.
• **Prendere decisioni consapevoli.** Confronta le soluzioni sulla base di requisiti documentati, non soltanto delle caratteristiche tecniche o del prezzo.
• **Aumentare la fiducia.** Utilizza la documentazione relativa alle certificazioni per supportare le valutazioni tecniche con clienti, integratori di sistema e centrali di ricezione allarmi.
• **Prepararti all'evoluzione delle reti.** Verifica che le apparecchiature di trasmissione degli allarmi supportino le tecnologie di comunicazione richieste dal tuo impianto.
La certificazione è particolarmente importante nella sicurezza antincendio, dove una trasmissione affidabile degli allarmi rappresenta un collegamento essenziale tra il rilevamento di un incendio e l'intervento conseguente.

Soluzioni certificate per diverse esigenze di installazione
IRIS-4 440G e DALM3000 di AddSecure offrono soluzioni per diverse esigenze di installazione.
IRIS-4 440G fa parte della gamma IRIS-4 di dispositivi per la trasmissione degli allarmi. Quando lo scegli per un'applicazione antincendio, verifica le certificazioni applicabili, i requisiti del sistema e la compatibilità con l'impianto esistente.
DALM3000, rappresenta un'ulteriore opzione per le installazioni compatibili. Come per qualsiasi apparecchiatura di trasmissione degli allarmi, è importante verificare che la configurazione certificata e l'utilizzo previsto soddisfino i requisiti della tua applicazione.
Entrambi i prodotti permettono di valutare il ruolo della trasmissione certificata degli allarmi nella progettazione degli impianti e nell'adattamento alle nuove tecnologie di comunicazione.
Entrambi i comunicatori, IRIS-4 440G e DALM3000, sono inoltre certificati secondo la norma EN 50131, Grado 4, il massimo livello di sicurezza previsto per i sistemi antintrusione e antirapina. Questa caratteristica ne consente l'impiego sia in applicazioni antincendio sia antintrusione, anche in contesti con elevati requisiti di sicurezza.
Prima di scegliere una soluzione, consulta la documentazione tecnica del prodotto e verifica quali norme, configurazioni e applicazioni sono effettivamente coperte.

La certificazione nella transizione alle reti IP e mobili
Con l'evoluzione delle reti di comunicazione, potresti dover aggiornare gli impianti di trasmissione degli allarmi esistenti per adattarli alle nuove tecnologie.
Le reti IP e mobili offrono diverse possibilità per la trasmissione degli allarmi, ma le apparecchiature devono comunque soddisfare i requisiti dell'applicazione prevista. È importante valutare le prestazioni richieste, la supervisione e la resilienza del sistema, oltre alle norme e alle disposizioni locali applicabili.
La certificazione ti aiuta a valutare le apparecchiature rispetto a requisiti definiti. Tuttavia, la certificazione di un singolo prodotto non significa automaticamente che l'intero impianto sia conforme a tutti i requisiti applicabili.
Per questo motivo, è importante valutare l'apparecchiatura, la progettazione del sistema e l'installazione nel loro insieme.

Dalla certificazione alla fiducia
Quando scegli le apparecchiature per la trasmissione degli allarmi antincendio, non basta conoscere le caratteristiche tecniche. Devi sapere rispetto a quali requisiti sono state valutate e se sono adatte alla tua applicazione.
Le norme EN 54-21 ed EN 50136 forniscono un riferimento utile per questa valutazione. Conoscendo l'ambito di applicazione delle norme e verificando le certificazioni pertinenti, puoi prendere decisioni più consapevoli sui tuoi sistemi di trasmissione degli allarmi antincendio.
In AddSecure crediamo che l'affidabilità debba essere dimostrata con evidenze concrete, non soltanto promessa. Perché, quando un allarme antincendio deve essere trasmesso, ogni anello della catena è importante.

ADDSECURE®

Contatti:
AddSecure International AB
Tel. +39 347 9977 838
www.addsecure.it

Riqualificare gli accessi: efficienza energetica, sicurezza e integrazione

intervista a Fabio Irrera, Responsabile Sviluppo Business Italia di FAAC

La riqualificazione degli edifici riguarda sempre più anche gli ingressi. Quali opportunità offre intervenire sugli impianti esistenti?
Una porta automatica è spesso considerata solo una soluzione per l'accessibilità, ma incide anche sulla sicurezza, sul comfort ambientale e sui consumi energetici. FAAC è presente nel settore degli ingressi automatici pedonali da più di 30 anni: un percorso che è arrivato alla quinta generazione di prodotto, con soluzioni che integrano connettività, efficienza energetica e flessibilità progettuale, rispondendo anche a requisiti di sicurezza fisica. Riqualificare con FAAC significa valorizzare gli ingressi anche negli edifici esistenti, attraverso una verifica delle condizioni dell'impianto, della manutenzione, dei requisiti normativi applicabili, requisiti funzionali e di sostenibilità.



Quanto pesa l'efficienza energetica e come agire sull'ingresso automatico pedonale?
Quando una porta rimane aperta più del necessario, l'aria climatizzata si disperde. Il problema è evidente nei luoghi ad alto transito, come i punti vendita del retail, della GDO, degli aeroporti o di altri grandi infrastrutture, dove la temperatura interna incide su consumi e comfort.
Un ingresso automatico, correttamente configurato, gestisce apertura e chiusura in funzione del transito e della direzione di camminata. Inoltre, l'integrazione di lame d'aria può offrire ulteriori benefici concreti e tangibili. È il caso di Airslide, la prima barriera d'aria integrata che si attiva solo con l'apertura delle ante e assorbe 3 watt in stand-by. Prove condotte in alcuni punti vendita della GDO con il supporto di Ergon Research Srl (società di consulenza per analisi progettuali innovative con significative esperienze nelle analisi termofluidodinamiche) hanno evidenziato che la riduzione dei volumi di aria climatizzata può superare il 60%, anche in condizioni di ridotti gap termici tra l'interno e l'esterno dell'edificio.
A rendere il tema sempre più urgente contribuisce anche il quadro normativo: gli obiettivi ESG e le direttive europee sulle prestazioni energetiche degli edifici spingono verso la riduzione dei consumi, anche nel contesto non residenziale. Gli ingressi, pertanto, non rappresentano un dettaglio marginale ma possono diventare un'occasione concreta per migliorare l'efficienza energetica complessiva dell'edificio e, al contempo, aggiornare il parco installato in coerenza con le normative cogenti, tra cui la EN 16005, introdotta nell'aprile del 2013.

La sicurezza è l'altro grande tema della riqualificazione. Da dove occorre partire?
Dalla valutazione del rischio e del sito: una banca, un punto vendita del retail del lusso, un ingresso pedonale di un'azienda o di un centro direzionale hanno esigenze diverse. Occorre riconsiderare la protezione degli ingressi ed i livelli di resistenza antieffrazione delle porte di ingresso e di uscita oltre che delle uscite di emergenza. I sistemi di controllo accessi per la gestione delle credenziali non possono sostituire la protezione fisica dalle intrusioni.

Quali soluzioni consentono di proteggere gli accessi pedonali senza rinunciare alla funzionalità?
CoMETA, che nel 2026 celebra 40 anni di attività e fa parte del Gruppo FAAC Technologies, propone sistemi per la protezione degli accessi, comprese soluzioni certificate secondo la norma UNI EN 1627 nelle classi RC3 e RC4. La gamma comprende bussole di sicurezza, porte girevoli antintrusione, portali rototraslanti ma anche porte blindate manuali ed uscita di emergenza in versione RC4. La scelta deve conciliare resistenza, flussi pedonali, vie di fuga e caratteristiche architettoniche del sito.





Quando la protezione deve estendersi agli spazi esterni, quale ruolo assumono dissuasori e sistemi di controllo perimetrale?
La protezione perimetrale interessa infrastrutture e luoghi sensibili, ma anche aree industriali e commerciali, così come i punti vendita del retail particolarmente esposti al rischio di intrusioni e tentativi di sfondamento. I dissuasori FAAC regolano i transiti e, in alcune configurazioni specifiche, contrastano le intrusioni veicolari anche di mezzi pesanti.
Per i siti più esposti, i modelli JS48 e JS80 sono progettati per arrestare un veicolo da 7,5 tonnellate rispettivamente a 48 e 80 km/h, con penetrazione inferiore a un metro, rimanendo operativi dopo il tentativo di sfondamento.
Ai dissuasori FAAC, si affiancano i tornelli Magnetic®, che nel 2026 celebra 80 anni: i tornelli a tutta altezza MPT delimitano perimetri di industrie, strutture logistiche e centri direzionali, mentre i varchi motorizzati FlowMotion® regolano il passaggio negli accessi non perimetrali anche in ambienti esterni e in contesti caratterizzati da elevati flussi di persone. Sono livelli complementari di un'unica strategia di protezione del sito, finalizzata ad assicurare la continuità operativa.

Quanto conta l'integrazione tra dispositivi, sicurezza e sistemi IT?
L'integrazione è un aspetto sempre più centrale in quanto la sicurezza fisica deve dialogare con i sistemi di supervisione e gestione del building. Le tecnologie del Gruppo FAAC Technologies consentono di digitalizzare il controllo di porte automatiche, barriere e cancelli, anche in installazioni esistenti, con dispositivi di diversa provenienza.
Le informazioni che arrivano sullo stato dei varchi aiutano a individuare tempestivamente gli allarmi, a rilevare le cause dei guasti e le anomalie delle macchine e a programmare in modo efficace gli interventi di manutenzione ordinaria e preventiva, migliorando continuità operativa riducendo gli oneri di manutenzione.

In sintesi, la connettività delle macchine non serve soltanto a comandarle ma anche a raccogliere dati utili alla gestione e allo sviluppo di piani di manutenzione predittiva.

È possibile ottenere questi benefici senza sostituire integralmente gli impianti?
Sì, ed è uno dei temi chiave della riqualificazione. Il patrimonio installato non può essere sempre rinnovato da zero: laddove compatibile con le normative specifiche cogenti, il retrofit permette di collegare e valorizzare gli impianti esistenti. Un approccio modulare consente di procedere per fasi, contenendo l'impatto economico e operativo, nel rispetto dei requisiti di sicurezza delle macchine.
Esistono poi soluzioni salvaspazio, come gli ingressi con ante rototraslanti e pieghevoli, adatti anche alle vie di fuga e in grado di superare i vincoli di spazio presenti negli edifici esistenti. Sono inoltre disponibili soluzioni specifiche per ambienti a contaminazione batterica controllata. La scelta va calibrata sulle caratteristiche dell'edificio e sull'uso previsto.
Il tema della riqualificazione va affrontato anche considerano il panorama delle agevolazioni fiscali disponibili, compreso l'iperammortamento 2026 o il Conto Termico 3.0: l'accesso a questi benefici non è automatico e va adeguatamente verificato in base alla riqualificazione svolta nel suo complesso. È inoltre importante guardare alla sicurezza nel suo insieme: il Regolamento europeo sulle macchine 2023/1230 si applicherà dal 20 gennaio 2027 e introduce requisiti anche in materia di cybersecurity, rafforzando l'attenzione alla connettività e alla sicurezza dei sistemi.

FAAC

Contatti:
FAAC
www.faac.it

Cube Service per la gestione digitale delle manutenzioni

comunicato aziendale

Pianificazione, documentazione e nuove funzioni AI in un unico ambiente Life3, per coordinare le attività sul territorio e rendere consultabili gli esiti dei controlli.

Una visita programmata, un'anomalia rilevata dal tecnico, un rapporto da consegnare al cliente. Nella manutenzione degli impianti di sicurezza e dei presidi antincendio, ogni intervento richiede il coordinamento di attività e informazioni che devono restare collegate nel tempo. Quando documenti, scadenze ed esiti sono distribuiti tra archivi e strumenti diversi, ricostruire la storia di un impianto richiede lavoro aggiuntivo.

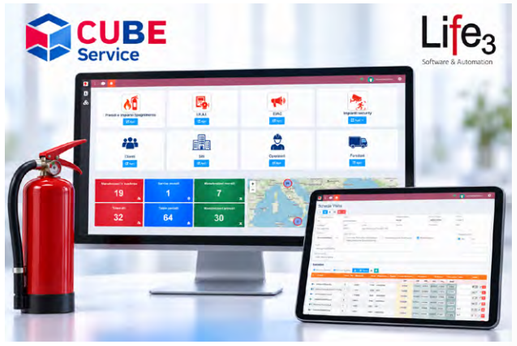
Cube Service, sviluppata da Life3, raccoglie questi elementi in una piattaforma dedicata alla gestione delle manutenzioni. Si rivolge alle aziende del settore, ai facility manager e alle organizzazioni multisede che devono pianificare i controlli, coordinare i tecnici e verificare le attività svolte.

Pianificazione e coordinamento sul territorio

Il calendario condiviso permette di programmare visite e interventi, assegnarli alle squadre e seguirne l'avanzamento. L'ufficio dispone così di un riferimento comune per organizzare il lavoro e controllare le scadenze, mentre le informazioni relative a clienti, siti e impianti rimangono associate alle attività da eseguire.
La mappa geografica interattiva mostra la distribuzione dei siti e delle manutenzioni sul territorio. La consultazione di questa vista aiuta a valutare la vicinanza tra le attività previste e a organizzare gli spostamenti delle squadre.

Documenti e verifiche collegati allo stesso impianto

Per ciascun sito o impianto, Cube Service consente di organizzare manuali, schede tecniche, certificazioni,



fotografie e rapporti di intervento. Gli utenti autorizzati possono consultare i documenti associati al riferimento corretto, riducendo la necessità di cercarli in archivi separati o di richiederli nuovamente all'ufficio.
Durante le attività sul campo, procedure e checklist guidano la registrazione dei controlli e dei relativi esiti. Le anomalie rilevate entrano nello storico dell'impianto e possono essere seguite attraverso la gestione dei ticket, dalla presa in carico alla chiusura. Il collegamento tra verifica, segnalazione e intervento successivo aiuta a mantenere visibile ciò che richiede ancora una soluzione. Si consideri, ad esempio, un controllo nel quale il tecnico riscontri un componente da sostituire. La registrazione dell'anomalia, la documentazione fotografica e il successivo aggiornamento dell'attività permettono all'ufficio e al cliente di ricostruire il percorso seguito, senza limitarsi al solo esito della visita iniziale.

AI per acquisire i dati e agevolare il censimento

Il caricamento iniziale delle informazioni rappresenta spesso una parte impegnativa dell'avvio di un sistema di gestione. Le funzioni AI di Cube Service analizzano la documentazione fornita, individuano i dati utili e supportano la compilazione delle schede cliente e impianto. Informazioni già presenti nei documenti possono così essere recuperate riducendo le trascrizioni manuali. A queste funzioni si affianca il riconoscimento delle matricole dei dispositivi tramite fotocamera, utile nelle attività di censimento sul campo. L'acquisizione assistita agevola la raccolta dei riferimenti identificativi e il loro inserimento nella gestione delle manutenzioni.
Gli utenti verificano i dati estratti prima di utilizzarli nelle attività operative. La leggibilità dei documenti e delle immagini e la qualità delle informazioni di partenza incidono sul risultato. L'AI facilita l'inserimento, mentre il personale controlla la correttezza dei contenuti acquisiti.

Rapporti digitali e integrità dei documenti

La produzione del rapporto conclude l'intervento e ne rende consultabili gli esiti. Cube Service supporta la compilazione e la sottoscrizione dei rapporti, la generazione dei PDF e la loro condivisione con il cliente. La documentazione rimane collegata al sito o all'impianto, a disposizione degli utenti autorizzati per successive verifiche.
La piattaforma utilizza inoltre impronte hash SHA-256 per la verifica dell'integrità documentale. Confrontando l'impronta del file con quella di riferimento, conservata in modo attendibile, è possibile rilevare eventuali modifiche successive. Questa funzione supporta il controllo della corrispondenza tra il documento consultato e la versione registrata.

Tracciabilità a supporto della conformità

Nel settore antincendio, il D.M. 1° settembre 2021, noto come Decreto Controlli, disciplina il controllo e la manutenzione degli impianti, delle attrezzature e degli altri sistemi di sicurezza antincendio. Il decreto richiede che controlli e interventi siano eseguiti e registrati secondo i criteri applicabili.
Cube Service aiuta a raccogliere le evidenze delle attività eseguite e a renderle consultabili in occasione di audit, verifiche o richieste del committente. La disponibilità di uno storico strutturato facilita il controllo delle manutenzioni e delle anomalie ancora aperte. La conformità resta legata alla corretta esecuzione delle attività, alle competenze del personale e all'applicazione dei requisiti pertinenti.

Protezione delle informazioni e accessi profilati

Documenti tecnici, dati dei clienti e rapporti di intervento richiedono regole di accesso coerenti con i ruoli degli utenti. Cube Service prevede accessi profilati e autorizzazioni differenziate, affiancati da strumenti di cifratura e verifica dell'integrità, per supportare la protezione delle informazioni gestite.
Life3 ha ottenuto la certificazione ISO/IEC 27001:2022 per il proprio sistema di gestione della sicurezza delle informazioni. La certificazione riguarda l'organizzazione e i processi di gestione della sicurezza e dei rischi.
Per il manutentore, un ambiente condiviso facilita il collegamento tra programmazione, lavoro sul campo e documentazione finale. Per il proprietario o il gestore dell'immobile, rende più semplice consultare gli esiti e seguire le richieste aperte. L'obiettivo è mantenere leggibile la storia manutentiva di ciascun impianto e disporre delle informazioni necessarie per decidere gli interventi successivi.

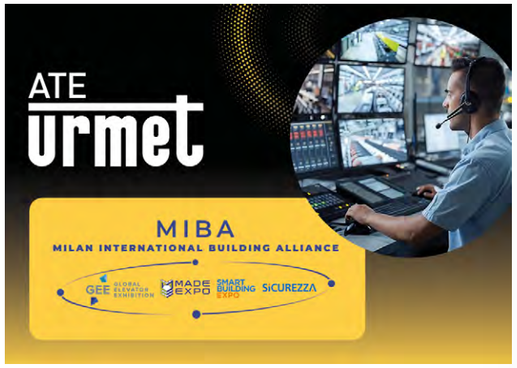
Life3

Contatto:
Life3 Srl
Tel. 045 485 25 29
info@life3.it

Urmet ATE a MIBA, Smart Building Levante con la sua offerta completa

comunicato aziendale

Il 18 e 19 novembre a Bari, con Nexty e l'intero ecosistema ATE ARGONEXT al fianco degli istituti di vigilanza.



Un'offerta in continua evoluzione, con un obiettivo costante: rispondere alle esigenze concrete degli operatori della sicurezza in un mercato che si trasforma. È la strada che **Urmet ATE**, società del Gruppo Urmet attiva dal 1991 nello sviluppo di software e soluzioni hardware per istituti di vigilanza e telesoccorso, percorre con un portafoglio di prodotti e servizi pensato per semplificare il lavoro quotidiano delle centrali operative. L'occasione per fare il punto è MIBA Levante, in programma il 18 e 19 novembre alla Nuova Fiera del Levante di Bari, dove l'azienda presenterà l'intera gamma, dalle novità più recenti all'ecosistema che le tiene insieme. Vediamo quali.

Nexty, la centrale operativa entra nell'era dell'AI

Protagonista dello stand è Nexty, il nuovo assistente virtuale basato su intelligenza artificiale che affianca gli operatori delle centrali. Dialoga al telefono con il cliente in modo naturale, lo riconosce e lo chiama per nome, effettua le verifiche necessarie e compila in autonomia il verbale dell'evento. Gestisce solo le chiamate che può risolvere da solo: se non riesce a chiudere l'evento, trasferisce la chiamata a un operatore umano nel giro di pochi secondi. Statisticamente Nexty può occuparsi fino al 65% delle chiamate di centrale: controlli orari, richieste di accensione e spegnimento impianto e allarmi tecnologici possono essere completamente automatizzati. Può restare attivo sempre, solo nelle fasce orarie di punta o su richiesta, ed è espandibile attivando il numero di operatori virtuali desiderato. Viene fornito chiavi in mano, non richiede formazione per gli operatori, mette a disposizione una dashboard con dati statistici e di sistema ed è integrato in Contact Evo e in Ateargo Next. Una risposta concreta alla difficoltà di reperire personale qualificato, Nexty nasce per rispondere alle esigenze di mercato di velocità e presenza.

L'ecosistema ATEARGO NEXT

Il filo conduttore dell'offerta è l'ecosistema ATEARGO NEXT, il gestionale eventi certificato EN 50518 per le centrali operative: componibile, integrato, flessibile e stabile. Ruota attorno al software PSIM e si articola in soluzioni di campo e servizi di centrale: Contact Evo per la telefonia, i moduli di reportistica e le API che permettono a software di terze parti di dialogare con la piattaforma. A completare il quadro, l'assistenza h24 e il servizio SaSS di assistenza sistemistica specializzata.

One Click, ricevere, vedere e decidere con un solo gesto

Tra le opportunità in evidenza c'è One Click, una funzionalità innovativa dei moduli multiprotocollo Unify Alarm e Unify Video Next. In un solo gesto l'operatore riceve il segnale di allarme, visualizza l'evento e prende una decisione, con più velocità, più precisione e più controllo. I due moduli gestiscono da un'unica interfaccia oltre cento protocolli antintrusione e oltre cento protocolli video.

Sul campo: Webu 4G, Fire 4G e Tracker 4G

Le periferiche portano l'ecosistema fuori dalla centrale. Webu 4G Next è il comunicatore per impianti antintrusione compatibile EN 50131 grado 3, con otto ingressi e quattro uscite a relè. Trasmette in protocollo bidirezionale Urmet ATE o in SIA IP (DC-09), quindi con qualsiasi sistema di centralizzazione, e grazie alle interfacce Ethernet e 4G LTE, con fallback su rete 2G, garantisce comunicazioni anche in condizioni critiche. Può inoltre inviare gli eventi a più centri di ricezione allarmi, assicurando la trasmissione verso un centro di backup in caso di blackout della stazione principale.

Per l'antincendio c'è Fire 4G PRO, che integra nel comunicatore alimentazione, batteria di backup e caricabatterie in conformità alla EN 54-4. Insieme al ricevitore software dedicato, rispetta i requisiti delle norme EN 54-21 ed EN 50518 e consente di presidiare h24 impianti già esistenti, centralizzandoli verso le sale degli istituti. Doppio vettore 4G ed Ethernet, compatibilità con tutti i centri di ricezione allarmi e prodotto made in Italy. Entrambi i comunicatori possono essere forniti con SIM già configurata e censita in centrale, per un'installazione plug and play.

Sul fronte della sicurezza personale e del telesoccorso, il nuovo Tracker 4G dà priorità alla comunicazione dati su rete IP e, se il canale non è disponibile, invia automaticamente un SMS di backup. Può essere fornito in modalità Ready to Use: configurazione iniziale automatica e censimento in ATEARGO NEXT senza operazioni manuali, con teleconfigurazione da parte dell'assistenza. In caso di allarme SOS invia la posizione ogni minuto per i successivi 30 minuti, se il segnale GPS è disponibile, e in ATEARGO NEXT la centrale visualizza sulla mappa il tracciato completo fino all'archiviazione dell'evento.

La "videoanalisi universale" a un livello superiore

Completa il panorama il nuovo modello per la videoanalisi, totalmente integrato nell'ecosistema ATEARGO NEXT e pensato per collegare impianto di videosorveglianza e istituto di vigilanza. La connessione 4G LTE, utilizzabile come backup o come vettore primario, ne consente l'uso anche in aree prive di connessione internet, come campi fotovoltaici, cantieri edili e strutture temporanee. Le uscite relè permettono automazioni avanzate, anche in base alle regole di videoanalisi, e non serve calibrare le telecamere: l'analisi complessa viene svolta in modo intuitivo e rapido. Si integra con il sistema esistente senza sostituire telecamere o registratori, mentre un processore avanzato elabora le immagini con grande velocità.

Ascoltare chi lavora sul campo

È questa la forza della proposta Urmet ATE: un insieme di soluzioni che cresce seguendo l'evoluzione tecnologica e le richieste del mercato. Perché innovare significa, prima di tutto, ascoltare chi lavora ogni giorno sul campo e trasformarne le esigenze in strumenti concreti.

MIBA Levante sarà l'occasione per vedere da vicino le novità, approfondire le soluzioni con il team e confrontarsi sulle esigenze di chi opera ogni giorno nelle centrali operative.

Urmet ATE vi aspetta a MIBA Levante il 18 e 19 novembre, Stand 100, ingresso Agricoltura.

ATE urmet

Contatto:
Urmet ATE
www.urmet-ate.it
info@urmet-ate.it
Tel. 0444 268211

Allarme incendio, ogni secondo conta

comunicato aziendale

Ogni secondo conta. Anche nella manutenzione. Ma oggi un sistema EVAC può fare molto più che gestire le emergenze.

Nel panorama delle moderne infrastrutture, la sicurezza rimane una priorità assoluta. Tuttavia, le esigenze odierne richiedono soluzioni sempre più evolute, capaci di integrare funzionalità differenti in un unico impianto.

È da questa visione che nascono le soluzioni EVAC Vivaldi, progettate non soltanto per garantire affidabilità e intelligibilità nelle comunicazioni ma anche per migliorare l'esperienza quotidiana degli ambienti attraverso una gestione ponderata dell'audio.



Un sistema EVAC che diventa anche una piattaforma audio evoluta

Grazie all'integrazione degli streamer audio Vivaldi, il sistema EVAC supera il tradizionale ruolo di impianto dedicato alle sole comunicazioni d'emergenza e si trasforma in una piattaforma audio capace di gestire e distribuire contenuti musicali differenti nelle diverse aree dell'edificio.

Lo **streamer audio** consente di accedere in modo semplice e immediato a contenuti provenienti dal web, dalle reti locali e dai principali servizi di streaming musicale, offrendo un'esperienza d'ascolto moderna, flessibile e sempre aggiornata.

Ogni zona può disporre della propria programmazione musicale, creando atmosfere personalizzate e perfettamente in linea con la destinazione d'uso degli ambienti. Grazie allo streamer audio integrato è possibile accedere a oltre 55.000 web radio, alle librerie musicali presenti su NAS e reti locali, alle emittenti DAB+ e FM, oltre a utilizzare connessioni Bluetooth, USB e AirPlay ed altri.

Una dotazione che permette di gestire musica di sottofondo, annunci e comunicazioni attraverso un unico sistema, mantenendo sempre adeguati standard qualitativi ed una resa sonora di livello Hi-Fi.

Manutenzione intelligente: ogni secondo conta

L'efficienza di un sistema si misura anche nella rapidità con cui è possibile mantenerlo operativo nel tempo.

Le soluzioni EVAC Vivaldi sono state progettate per semplificare e velocizzare gli interventi tecnici grazie al sistema di diagnostica e supervisione remota.

Grazie alle notifiche diagnostiche ricevibili su PC, tablet e smartphone, il sistema segnala tempestivamente eventuali anomalie, permettendo di localizzare immediatamente il problema e velocizzare gli interventi di manutenzione.

Questo significa eliminare gran parte del tempo normalmente dedicato alla ricerca del guasto, consentendo ai tecnici di intervenire in modo rapido e mirato, riducendo i tempi i inattività e consentendo la continuità del servizio.

Un sistema che cresce insieme alla struttura

Le esigenze di una struttura cambiano nel tempo. Per questo motivo i sistemi EVAC Vivaldi sono stati progettati secondo una logica scalabile e modulare.

Che si tratti di una soluzione compatta all-in-one o di una configurazione a rack per installazioni più articolate, il sistema può essere ampliato progressivamente grazie alla connessione in rete tra i dispositivi. Nuove zone, nuove funzionalità e nuove sorgenti audio possono essere integrate anche successivamente alla prima installazione, senza dover ripensare l'intera architettura dell'impianto.

La possibilità di collegare sorgenti audio multimediali esterne e di gestire in modo indipendente musica, comunicazioni e sicurezza nelle diverse aree dell'edificio consente inoltre di adattare il sistema alle necessità presenti e future della struttura, proteggendo l'investimento nel tempo.

Efficienza energetica e sostenibilità

L'innovazione passa anche attraverso una maggiore attenzione ai consumi energetici.

Per questo i dispositivi EVAC Vivaldi integrano la funzione Eco Mode, sviluppata per ridurre l'assorbimento energetico quando il sistema non si trova in stato di emergenza. Una tecnologia che ottimizza l'efficienza complessiva dell'impianto senza compromettere affidabilità, prestazioni e sicurezza.

Il risultato è un sistema capace di coniugare continuità operativa e attenzione ai consumi, contribuendo a una gestione più sostenibile delle infrastrutture e a una maggiore efficienza energetica complessiva.

Oltre l'EVAC: la competenza audio a 360 gradi.

VIVALDI

Contatti:
Vivaldi srl
Tel. +39 0421 307825
info@vivaldigroup.it

Partner

ADDSECURE INTERNATIONAL AB
www.addsecure.it
28-29

AISMA S.R.L.
www.aismasrl.it
14-15, IV copertina

AXIS COMMUNICATIONS
www.axis.com
I romana, 16-17

EL.MO. S.P.A.
www.elmospa.com
18-19, III copertina

ERMES S.R.L.
www.ermes-online.it
25

FAAC
www.faac.it
30-31

INIM ELECTRONICS S.R.L.
www.inim.biz
2

LIFE 3 S.R.L.
www.life3.it
26-27, 32-33

OPTEX
www.optex-europe.com
II copertina, 20-21

REVEAL
www.revealmedia.it
Copertina, 22-23

URMET-ATE S.R.L.
www.urmet-ate.it
5, 34-35

VIVALDI S.R.L.
www.vivaldigroup.it
36-37

essecome ONLINE

n. 05/2026
Anno XLVI
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

HA COLLABORATO A QUESTO NUMERO
Myriam Cattaneo e
Diego Di Simone Perricone

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
essecome editore srls
Piazza Gae Aulenti 1, torre B - 20154 Milano
Tel. +39 02 3675 7931

REGISTRAZIONE
- Tribunale di Milano n. 21 del 31 gennaio 2018
- Registro pubblico Operatori di Comunicazione (ROC) n. 34727

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it



Soluzioni di sicurezza Globali

La sicurezza è un aspetto sempre più importante nella nostra vita. Affidarsi a un partner competente è la chiave per garantirsi la serenità di una vita sicura.

Dal 1975 operiamo nel campo italiano e internazionale della sicurezza con la progettazione, la produzione e la fornitura di prodotti antintrusione, domotica, antincendio, videosorveglianza e controllo accessi, utilizzando tecnologie innovative e un know-how sempre in evoluzione.

Antintrusione
Antincendio
Videosorveglianza
Controllo Accessi

aisma

cognitive governance · knowledge · decisions

APR 2026

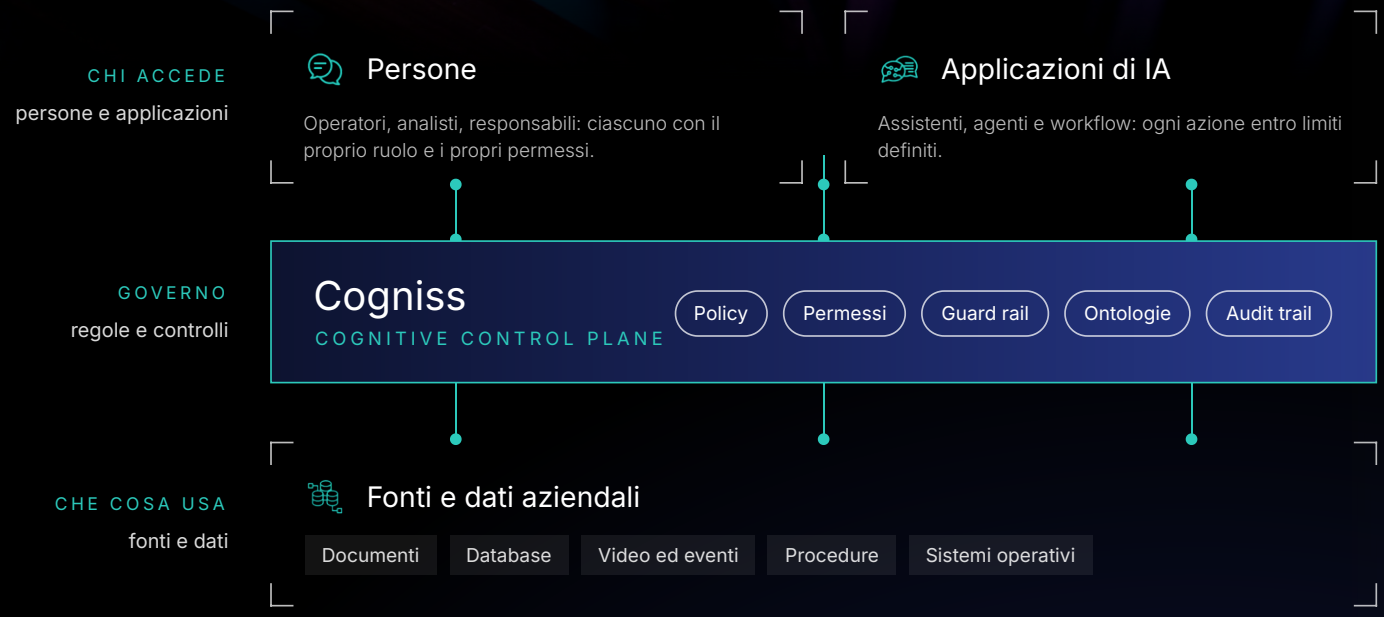
AIR · PORT · RAIL

SECURITY & SAFETY

dati · persone · applicazioni

Governare l'IA: dalle fonti a chi la *usa*.

Cogniss, il Cognitive Control Plane di AISMA, si colloca tra i dati aziendali e chi li interroga. Stabilisce che cosa può essere usato, da chi e secondo quali regole, e ne conserva traccia.



01 · FONTI

Ogni risposta ha una fonte. Se la fonte manca, il sistema lo dichiara.

02 · ACCESSI

Ognuno vede ciò che può vedere. Persone e applicazioni operano solo entro i permessi assegnati.

03 · TRACCIABILITÀ

Ogni passaggio resta registrato. Decisioni ricostruibili in un audit trail immutabile.

INCONTRIAMOCI A BARI

APR 2026 · 18 novembre · Fiera del Levante (MIBA Levante)
Ore 12:00, panel «Le risposte della filiera e il ruolo della IA»

Governing AI. Preserving Knowledge.
Enabling Decisions.

aisma.it

Centro di Ricerca e Trasferimento Tecnologico
accreditato Unioncamere / MIMIT · ISO 9001 · ISO/IEC 27001