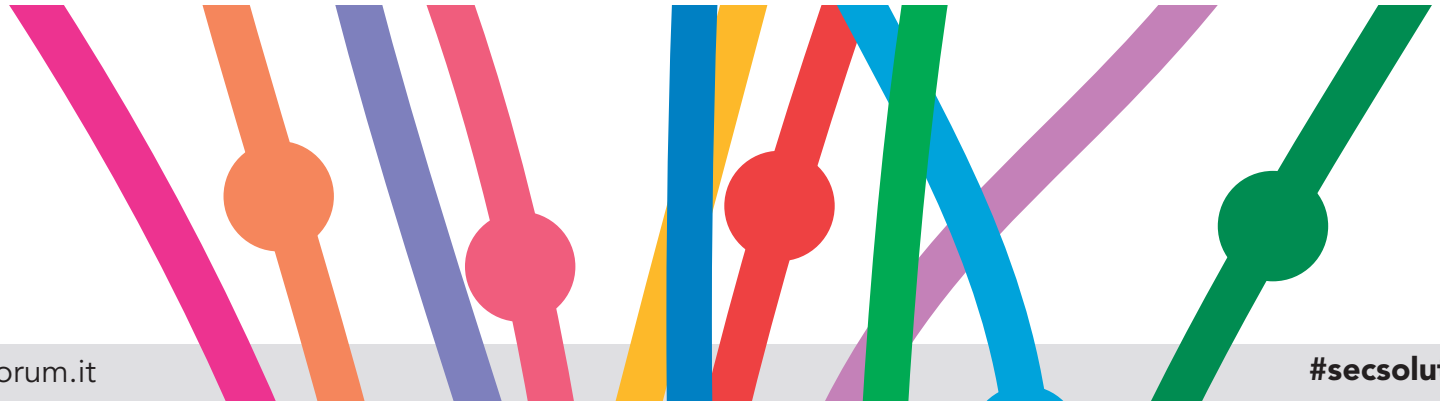
La convergenza digitale: opportunità VS criticità

Giulio Iucci

Presidente ANIE Sicurezza



La Convergenza Digitale - Opportunità vs Criticità

Giulio Iucci

Presidente ANIE SICUREZZA

ANIESICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI
ANIE FEDERAZIONE
CONFINDUSTRIA

LA TECNOLOGIA E' AL CENTRO DEL PROCESSO

SVILUPPO TECNOLOGICO	CONVERGENZA TECNOLOGICA	COPERTURA TERRITORIO	SENSIBILIZZAZIONE SOCIALE	CONTENIMENTO COSTI
• Significativa evoluzione nel campo tecnologico: Hardware e Software	• Grazie anche al digitale, tra Security, Safety, Automation e Sicurezza Informatica.	• Proliferarsi di sistemi di sicurezza e controllo (miriade di "sensori" sul territorio).	• Forte attenzione da parte delle istituzioni, delle aziende e dei singoli.	• Riduzione dei costi ed agevolazioni per l'acquisto di impianti di sicurezza.

L'UOMO?

Qual è il suo ruolo all'interno del nuovo processo? Il fattore umano è abilitante o disabilitante?

Gli uomini si trovano **all'inizio** – effettuano la **risk analysis** ed il **risk assessment**: ingegnerizzano, implementano e indirizzano – e **alla fine** del processo – **decidono**, ma con un'elevata velocità.

Oggi si riescono a governare tantissimi stati, funzioni, allarmi e informazioni, perché è la tecnologia a farlo, mettendo il tutto a disposizione dell'operatore, assistendolo nelle procedure da attivare.

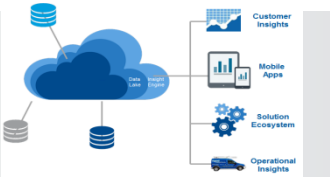
ANIESICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI
ANIE FEDERAZIONE
CONFINDUSTRIA

IL TREND DELL'INTEGRAZIONE

PASSATO: STAND-ALONE	ATTUALE: INTEGRAZIONE	FUTURO: CONVERGENZA
✓ Sistemi stand-alone con interconnessioni individuali. ✓ Incapacità di scambiare informazioni tra i sistemi. ✓ Processo decisionale dipendente dall'operatore.	✓ Una soluzione di gestione centrale che integra tutti i sistemi. ✓ Eventi e incidenti unificati in un unico processo standard. ✓ Maggiore abilità nel gestire il rischio e assicurare la conformità. ✓ Investimenti in soluzioni integrate guidate dal ROI.	✓ Convergenza della sicurezza IT, fisica e logica in piattaforme unificate. ✓ Processi decisionali supportati da scenari automatici e dinamici. ✓ Trasmissione dei dati più veloce ed elaborazione tramite architettura distribuita.

Integrazione

Convergenza



Le soluzioni integrate richiedono **dati unificati** tra i sistemi, per distribuire **informazioni utili e utilizzabili**, garantendo così una maggiore visibilità degli eventi e il controllo situazionale.

ANIESICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI
ANIE FEDERAZIONE
CONFINDUSTRIA

ALCUNE DOMANDE

I singoli sistemi sono realizzati seguendo un'architettura ed una visione strategica globale?

Come vengono interpretati informazioni ed allarmi diversi e con quali azioni correlate si attivano le procedure di intervento?

Abbiamo la mappatura (numerica, geografica e funzionale) ed il controllo di tutti i sensori in campo?

Come deve essere strutturata una Centrale Operativa per supportare tale attività?

Che tipo di collegamento hanno i singoli sistemi e dove arrivano i segnali generati dai sensori?

Quanti devono essere gli operatori in Centrale Operativa, con quali coperture e competenze?

I singoli sistemi si "parlano" tra loro e sono predisposti per parlare tutti con la stessa centrale?

Le procedure di ricezione allarme, presa in carico ed intervento, sono uniformate e coerenti le une con le altre (Safety, Security, Automation)?

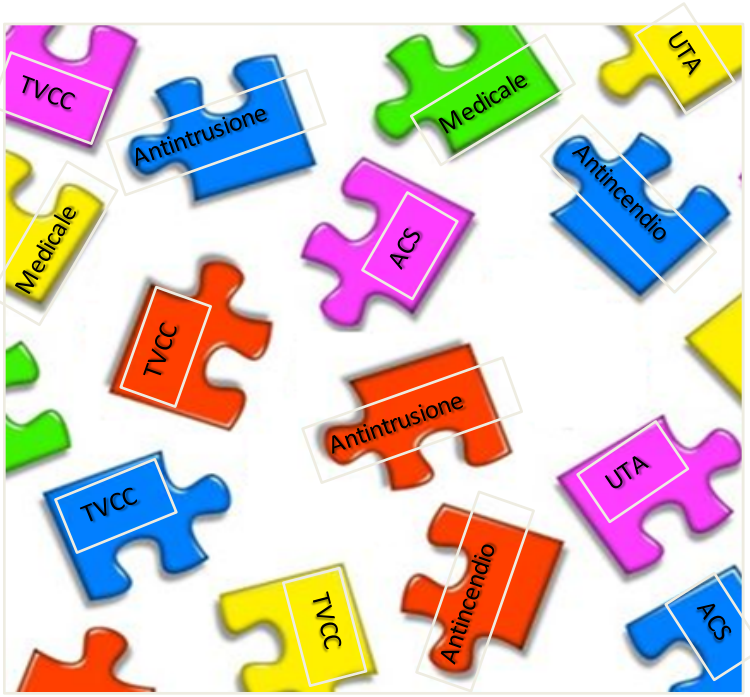
Chi legge la mole di dati che verrebbe generata da tutti questi sensori?

Quali sono i costi diretti, indiretti di tale operazione?

LA GESTIONE TRADIZIONALE DELL'INFRASTRUTTURA TECNOLOGICA

Gestire in modo unificato e correlato impianti complessi ed eterogenei di sicurezza fisica e automazione.

- ✓Polverizzazione dei dati e delle informazioni.
- ✓Gestione eventi difficoltosa e intempestiva.
- ✓Eccessiva manualità operativa.
- ✓Impossibilità di correlare allarmi eterogenei.
- ✓Frammentazione delle tecnologie in campo.
- ✓Applicativi software non best-in-class.
- ✓Scarsa adattabilità alle infrastrutture di rete.
- ✓Gestione difficoltosa delle evoluzioni tecnologiche.
- ✓Operatività preventiva inapplicabile.
- ✓Gestione obsolescenze e inventario impossibili.



ANIE SICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI

LO SCENARIO OPERATIVO TRADIZIONALE

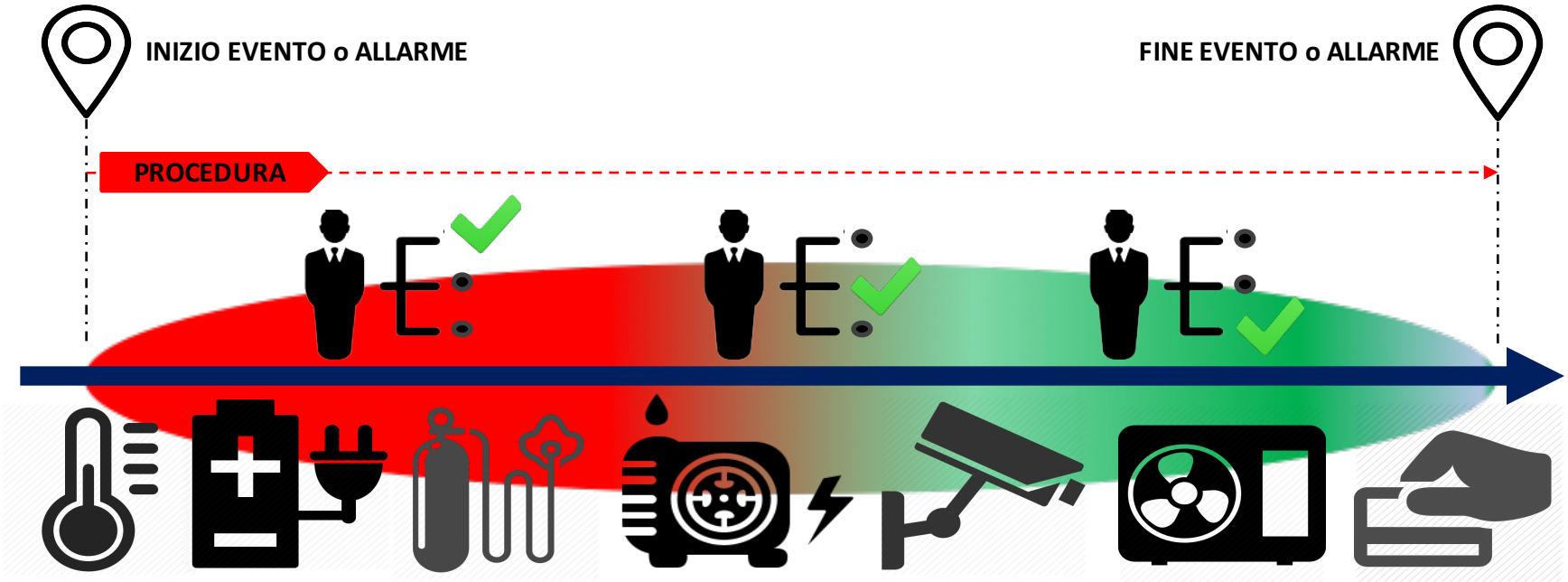
Frammentazione di impianti, sistemi e applicazioni eterogenei.

Nessuna correlazione ed automatizzazione degli eventi.

ANIE SICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI

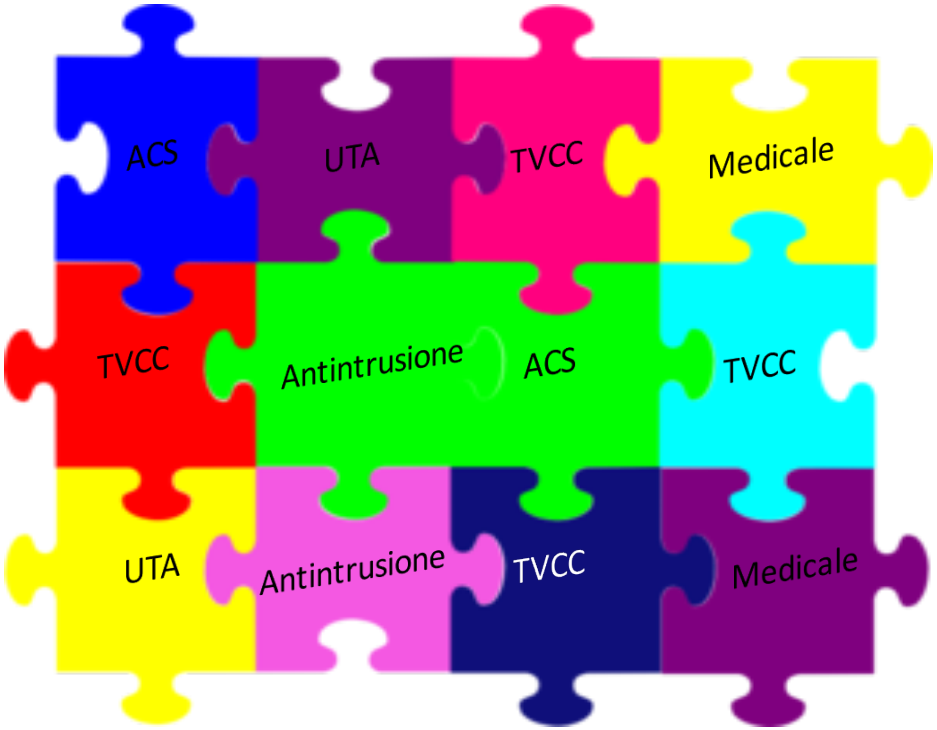
IL SUPPORTO ALLE DECISIONI

Manca una **gestione unificata delle tecnologie in campo**, che metta a disposizione dell'operatore **un unico strumento di supporto alle decisioni operative ed emergenziali**, trasversale all'infrastruttura, basato su procedure e meccanismi avanzati di notifica e riscontro, che sia semplice, dinamico e realmente efficace.



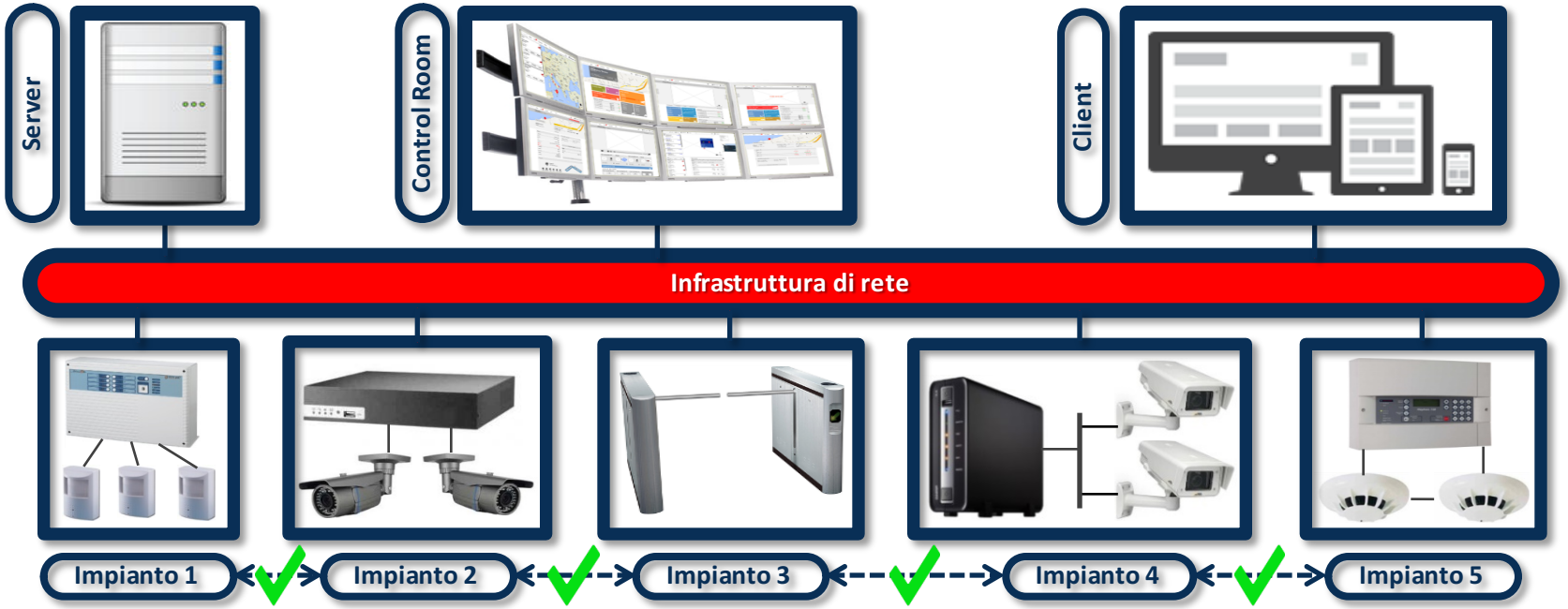
IL SUPPORTO ALLE DECISIONI

- ✓ Semplificazione ed automatizzazione delle procedure operative e di manutenzione.
- ✓ Dispiego contenuto di risorse umane, bassi costi di esercizio.
- ✓ Possibilità di aggiungere valore all'infrastruttura, ROI applicabile.
- ✓ Gestione semplificata di grandi volumi di dati e informazioni.
- ✓ Incremento dell'efficienza negli scenari complessi.
- ✓ Innalzamento globale della qualità dei servizi erogati.



IL NUOVO SCENARIO OPERATIVO

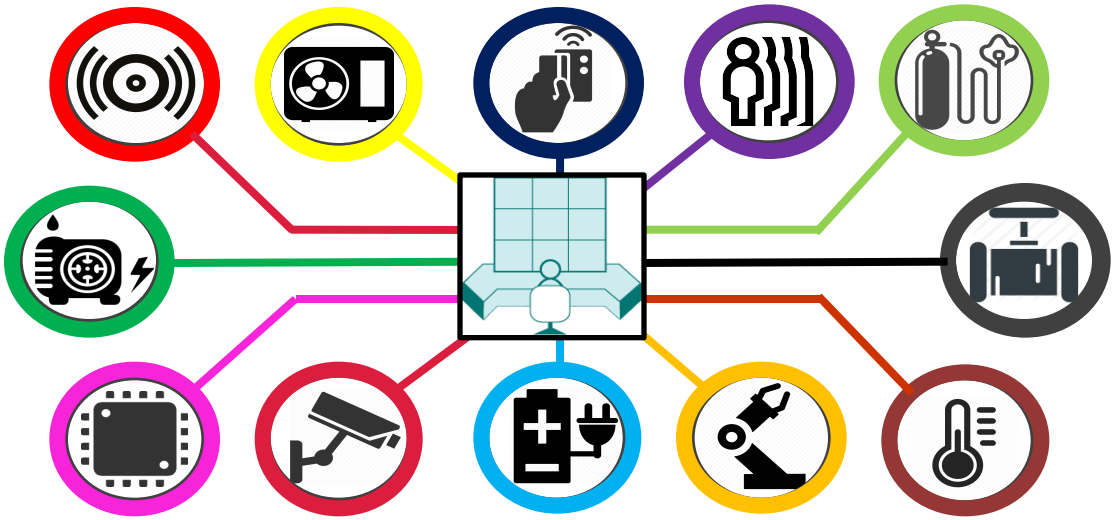
Una soluzione informatica unica per qualunque esigenza applicativa: razionalizzazione, correlazione, automatizzazione.



ANIE SICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI

UNA SOLUZIONE UNICA

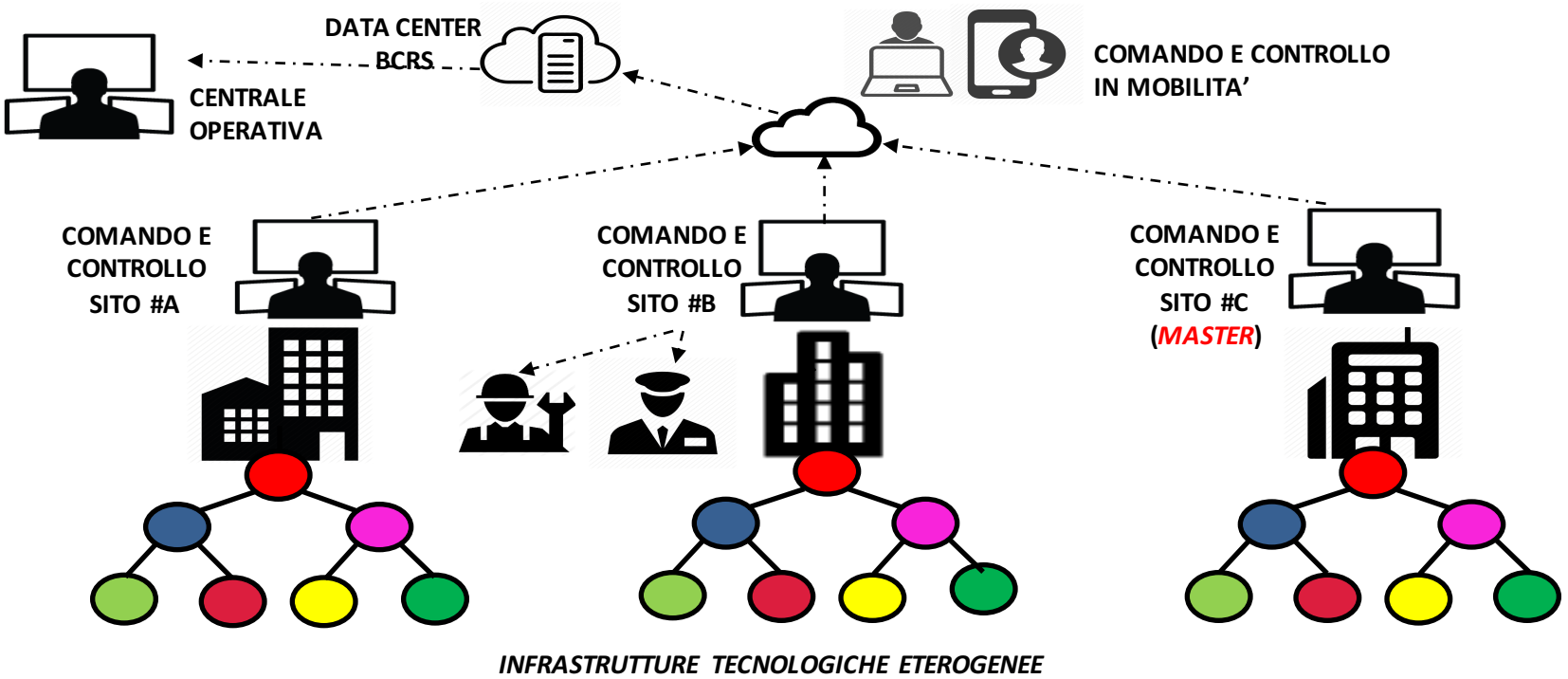
Un'unica soluzione. Una piattaforma con un front-end unificato e un back-end capace di dialogare con qualunque tecnologia in campo.



Sistemi, Soluzioni e Servizi integrati che consentono di monitorare gli Asset, velocizzare le informazioni dei sistemi di sicurezza, metterli in matrice automatica di confronto, valutare le contromisure ed operare di conseguenza, applicando un modello di intervento unificato che razionalizzi tutti i flussi operativi di sicurezza fisica ed automazione.

ANIE SICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI
ANIE FEDERAZIONE
CONFINDUSTRIA

UN ESEMPIO DI ARCHITETTURA



IL FLUSSO OPERATIVO DI COMANDO E CONTROLLO

La parola d'ordine è diventata **EARLY WARNING**, ma la filiera è più articolata.

- Monitorare	Sistemi, sensori, data base, informazioni on line, ecc. (manutenere)
- Intercettare	Allarmi, informazioni, anomalie, ecc.
- Correlare	Geograficamente, nel tempo e tra sistemi diversi.
- Interpretare	Le informazioni ricevute per darne un significato univoco, leggibile.
- Intervenire	Attivare le procedure pianificate d'intervento.
- Contenere	Minimizzare i danni potenziali o già verificatisi.
- Ripristinare	Riattivare e rendere operativo tutto ciò che è stato interrotto e/o danneggiato.
- Apprendere	Fare esperienza di quanto accaduto, comprendendone le cause e le dinamiche.
- Implementare	Attivare tutte le azioni correttive (operative e tecnologiche) e trasferirle.

Il problema è: PRENDERE DECISIONI **Corrette e nel più breve tempo possibile**

LA MATRICE COMPLETA DELLE ATTIVITA'

MAPPARE	MONITORARE	INTERCETTARE	INTERPRETARE	INTERVENIRE	ANALIZZARE	RE-INSERIRE
CODIFICARE CERTIFICARE	CONNETTERE	INFORMAZIONE PUSH	CORRELARE	PROCEDURE E REGOLE CERTE	ANOMALIE	CAPITALIZZARE
UNIFORMARE	INTERFACCIARE	INFORMAZIONE PULL	SIGNIFICATO ALLE INFORMAZIONI	MITIGARE	NOVITA'	CATEGORIZZARE
INDICIZZARE SEGMENTARE	PROTOCOLLI E TECNOLOGIE DIVERSI	SELEZIONARE E FILTRARE	ESPERIENZA E STATISTICA	RESILIENZA	SIGNIFICATO	CORREGGERE INSERIRE
GEO LOCALIZZARE	LOGICA DEI PROCESSI	DATA BASE	CONTESTO	VIRTUALIZZARE BACK-UP	IMPARARE PER PREVENIRE	METTERE A SISTEMA
COLLAUDARE	CONTROLLARE	SCENARIO GLOBALE	MATRICE DI CONFRONTO	RIPRISTINARE	DATA BASE	SISTEMA ESPERTO
SIMULAZIONI	PENETRATION TEST	MANUTENZIONE	PREDITTIVA	CONSERVATIVA	CORRETTIVA	EVOLUTIVA

IL NUOVO SCENARIO

La **Convergenza Digitale** non è più rimasta solo concettuale e/o di competenza specifica, ma è divenuta "sistemica" ed è questa la vera svolta e visione del futuro.

Gli **Impianti Speciali** di **automazione**, **sicurezza** di cose e persone, **gestione** dei **dati** e delle **informazioni**, a servizio di una infrastruttura tecnologica complessa di qualunque genere, non possono più essere considerati come entità separate, bensì **elementi appartenenti ad un unico Sistema**.

Inoltre i cittadini sono ormai degli utenti sempre connessi.

La sicurezza non può più essere percepita per settori e con un approccio azione-reazione, ma come un **unico "ambiente"** che consenta la supervisione del tutto, nell'ottica di quello che oggi viene chiamato **Early Warning.**

IL NUOVO SCENARIO

La sicurezza Fisica è anche sicurezza Cyber.

Tutti gli apparati ed i singoli sottosistemi sono, costantemente ed in tempo reale, connessi tra loro ed in alcuni casi, a loro volta, **connessi con gli utenti**, come parte di un unico grande **"organismo"** che può essere "attaccato", non come in passato, solo direttamente nelle sue "infrastrutture critiche", ma violando qualsiasi suo componente anche apparentemente residuale che faccia poi da "bridge" per entrare nel cuore dell'obiettivo principale.

E' necessario quindi conoscere e comprendere quali siano le criticità portate dalla convergenza tecnologica con relativa connessione globale, utilizzarne tutti i vantaggi, minimizzando i rischi che, in ogni caso, non potranno essere azzerati, ma mitigati adottando le **misure tecnologiche, architetturali e procedurali coerenti e proporzionate al contesto ed al bene da proteggere**, sia esso materiale, immateriale o umano.

LE CRITICITA'

Tutto è centrale e primario, non esiste la periferia ed il residuale.

Il concetto di sicurezza fisica che prevede sistemi più critici e sensibili, deve essere rivisto in un nuovo paradigma: **tutti i sistemi connessi**, anche residuali, devono essere considerati **potenzialmente critici e sensibili.**

Occorre innanzitutto determinare le nuove vulnerabilità introdotte e poi proteggere ciascun elemento che fa parte del sistema e i canali di comunicazione tra essi.

E', in ogni caso, evidente che le regole base per misurare **il rischio**, rimangono invariate ed utilizzano gli stessi parametri macro di riferimento per definire **la probabilità** e **l'entità** di ciò che può accadere.

E' quindi sempre importante effettuare con chiarezza **un'analisi di contesto** e definire in dettaglio quali siano **i beni da proteggere** e gli eventuali **offender**.

Tutto ciò anche per dare **equilibrio** e **sostenibilità** ad un'azione di **protezione** e **prevenzione** che sia **coerente** con i reali rischi e conseguenze di un'azione criminosa.

LE OPPORTUNITA'

- ✓ Maggiore **comprensione** e **valutazione tempestiva** delle situazioni emergenziali.
- ✓ **Semplificazione** ed **automatizzazione** delle procedure operative e di manutenzione.
- ✓ Dispiego contenuto di **risorse umane**, **bassi costi di esercizio** e maggiore **accuratezza**.
- ✓ Possibilità di **aggiungere valore** all'infrastruttura. Contenimento costi.
- ✓ Gestione **semplificata** di **grandi volumi di dati** e informazioni.
- ✓ Incremento di **efficienza ed efficacia negli scenari** complessi e nel **processo decisionale**.
- ✓ Innalzamento globale della **qualità dei servizi** erogati e della **sicurezza**.

I PUNTI DI ATTENZIONE

IN GENERALE

- ✓ Cultura
- ✓ Informazione
- ✓ Formazione
- ✓ Norme e Procedure
- ✓ Certificazioni
- ✓ Test e Controlli
- ✓ Incentivazioni
- ✓ Politiche Europee
- ✓ Investimenti Nazionali

DI DETTAGLIO

- ✓ Supervisione e Monitoraggio
  PSIM – Data Analytics – Artificial Intelligence
- ✓ Protezione e Segmentazione
- ✓ Prerogative di Accesso / Validazione
- ✓ Protezione e richiesta accesso rete da remoto
- ✓ Sicurezza porte di accesso ai singoli sistemi
- ✓ Suddivisione in zone isolate tra loro
- ✓ Trasmissioni sicure / Algoritmi di Crittografia / Autenticazione dati
- ✓ Aggiornamenti e Penetration Test periodici
- ✓ Virtualizzazione / Backup
- ✓ Resilienza / BCRS

RIASSUMENDO

- ✓ LA DIGITALIZZAZIONE PORTA ALLA **CONVERGENZA**: SECURITY / SAFETY / AUTOMATION.
- ✓ **SISTEMI DIVERSI** INTERAMENTE **INTEROPERABILI**, CONESSI TRA LORO E CON L'ESTERNO.
- ✓ LE INFRASTRUTTURE E GLI **IMPIANTI SENSIBILI** SONO CONNESSI CON IMPIANTI **PERIFERICI E SECONDARI**.
- ✓ L'IMPORTANZA DI FISSARE DELLE **BEST PRACTICE** E SEGUIRE DELLE LINEE GUIDA NAZIONALI ED EUROPEE.
- ✓ LA NECESSITA' DI UNA **PROGETTAZIONE SISTEMICA** GLOBALE CHE SEGUA FERREE REGOLE ARCHITETTURALI, PROCEDURALI, NORMATIVE E TECNOLOGICHE.
- ✓ DARE VALORE E QUALITA', **CERTIFICARE E CONTROLLARE** TUTTA LA FILIERA: DALLA RISK ANALYSIS, ALLA PROGETTAZIONE, DALLA SCELTA DEI PRODOTTI (HW / SW), ALLA LORO INSTALLAZIONE, COLLAUDO E MANUTENZIONE, DAI TEST PERIODICI DEGLI IMPIANTI, ALLE PROCEDURE OPERATIVE DI INTERVENTO.
- ✓ ATTIVAZIONE DI TUTTI I **PIANI E PROCEDURE** CHE CONSENTANO UN ELEVATO LIVELLO DI PROTEZIONE, PREVENZIONE E MITIGAZIONE DAI RISCHI DI ATTACCO: ES. PENETRATION TEST, BACK-UP, VIRTUALIZZAZIONE , RESILIENZA, ECC.
- ✓ UTILIZZO DI **NUOVE TECNOLOGIE DI CENTRALIZZAZIONE**, COMANDO E CONTROLLO.


LA TECNOLOGIA E' AL CENTRO
GRAZIE

Grazie
per l'attenzione!

Continua a seguirci su
www.secsolutionforum.it