Il connubio tra control room, applicativi informatici e sistemi di spegnimento incendio nelle infrastrutture critiche e negli ospedali (di Bellardini Danilo)

Negli ultimi anni l'evoluzione tecnologica ha trasformato profondamente il modo in cui progettiamo, gestiamo e difendiamo le infrastrutture critiche: dalle centrali energetiche ai data center, fino agli ospedali. L'integrazione tra control room (sale di controllo), sistemi di supervisione SCADA/BMS e le soluzioni di spegnimento incendio gestite da applicativi informatici offre opportunità importanti di prevenzione e risposta rapida, ma introduce anche nuovi rischi — tecnici, umani e cyber — che richiedono un approccio multidisciplinare, rigoroso e proattivo.

Perché integrare control room e sistemi di spegnimento?

La centralizzazione delle informazioni in una control room permette di correlare eventi provenienti da rilevatori incendio, sistemi HVAC, sensori di fumo/termici, metri di flusso gas e telecamere termiche, e di attivare in modo mirato agenti estinguenti (schiume, gas inerti o sistemi ad acqua a zone). Questa integrazione riduce i tempi di identificazione e intervento, minimizza danni collaterali (es. spegnimento localizzato in una sala server) e migliora la governance degli scenari di emergenza. Studi recenti e linee guida tecniche indicano l'efficacia di soluzioni che combinano detection avanzata (es. VESDA, imaging termico) con soppressione selettiva e logiche decisionali automatizzate.

I rischi rilevanti — esempi concreti e lezioni apprese

Gli ospedali sono ambienti particolarmente critici: la presenza di alimentazione elettrica continua, apparecchiature medicali, bombole/linee di ossigeno e pazienti non evacuabili rapidamente rende le conseguenze di un incendio potenzialmente catastrofiche. La letteratura e le cronache mostrano che le cause ricorrenti includono guasti elettrici e problemi legati all'ossigeno medicale; le analisi raccomandano gestione della strumentazione, layout dei reparti e sistemi di spegnimento adeguati.

Un caso emblematico che ha richiamato l'attenzione internazionale è l'incendio del reparto COVID-19 dell'ospedale di Piatra Neamț (Romania, 14 novembre 2020), dove un rapido sviluppo dell'incendio in reparto con pazienti ventilati ha causato vittime e ha evidenziato carenze gestionali e infrastrutturali; la vicenda ha sottolineato quanto siano cruciali manutenzione, procedure e monitoraggio continuo per le strutture sanitarie.

Anche le infrastrutture energetiche e i centri dati mostrano che l'evoluzione tecnologica porta nuove fragilità: incendi legati a sistemi di accumulo energetico (BESS) o a UPS non correttamente gestiti possono propagarsi rapidamente e impattare reti critiche e capacità operative. Rapporti del settore sottolineano l'importanza di sistemi di rilevazione avanzata e di agenti soppressori che minimizzino danni a infrastrutture IT sensibili.

Infine, in scenari di conflitto o attacco mirato, la compromissione di sale di controllo o centri di crisi può degradare la capacità di comando e controllo. Notizie recenti su danni a centri di crisi esterni di impianti nucleari e altre infrastrutture mostrano la necessità di resilienza fisica e digitale alle control room stesse.

I principali punti di attenzione tecnico-operativi

1. Ridondanza e separazione dei percorsi di attivazione: le logiche di attivazione automatica della soppressione devono avere percorsi ridondanti — sia per i segnali sia per l'alimentazione — e modalità manuali di intervento locale e remoto.

2. Fail-safe e prevenzione degli attivatori accidentali: l'uso di logiche a più livelli (es. conferma da sensori multipli, validazione operatori in control room) riduce attivazioni ingiustificate che possono provocare danni (es. gas inerti in presenza di persone).

3. Manutenzione e testing certificato: i sistemi di rilevazione e di spegnimento devono essere oggetto di test periodici, reportabili e tracciati in CMMS; in ospedale, i test devono prevedere protocolli che tutelino i pazienti.

4. Cybersecurity: applicativi che comandano sistemi di spegnimento e BMS rappresentano un vettore d'attacco potenziale — hardening, segmentazione di rete OT/IT, autenticazione forte, logging immutabile e monitoraggio in real time sono obbligatori.

5. Simulazione e addestramento congiunto: esercitazioni tra manutentori, personale clinico, squadra antincendio e operatori control room migliorano tempi decisionali e coordinamento operativo.

6. Approccio human-centered: la tecnologia non sostituisce il giudizio umano; interfacce chiare, allarmi priorizzati e procedure di escalation ben rodate sono essenziali.

Proposte pratiche e governance

Audit integrato: verifiche congiunte tra safety (antincendio), security (protezione fisica e cyber) e continuità operativa per mappare rischi e dipendenze critiche.

Policy di change management per applicativi di spegnimento: ogni modifica software/hardware che impatta logiche di spegnimento deve passare per assessment di rischio, test in ambiente controllato e approvazione formale.

Investimenti mirati: non è sufficiente installare “più tecnologia”; servono soluzioni adeguate al contesto (es. gas inerti per sale server, sprinkler zonali per aree mediche, sistemi a rilevazione precoce VESDA nei corridoi tecnici).

In conclusione — integrazione responsabile per infrastrutture resilienti

Il vero valore dell’integrazione tra control room e sistemi di spegnimento informatizzati non sta solo nella tecnologia, ma nella capacità dell’organizzazione di governarla: progettazione attenta, manutenzione rigorosa, sicurezza informatica, formazione continua e legislazione applicabile. Le cronache (dai reparti ospedalieri ai data center) ci ricordano che l’inerzia o la superficialità nelle pratiche di gestione possono avere conseguenze drammatiche; al contrario, una strategia olistica e basata su evidenze tecniche aumenta significativamente la resilienza delle infrastrutture critiche.

BELLARDINI DANILO

Safety & Security manager