Sistema o impianto a disponibilità superiore

Luca Fiorentini
Direttore TECSA S.r.l.

Piergiacomo Cancelliere
Corpo Nazionale dei Vigili del Fuoco

Marco Di Felice
Ingegnere

Raffaele Sabatino
Tecnologo INAIL

Estratto da Antincendio n. 04/2020

Sistema o impianto
a disponibilità superiore

Piergiacomo Cancelliere, Marco di Felice, Raffaele Sabatino, Luca Fiorentini

L'abstract
La recente revisione della R.T.O. del Codice (D.M. 18/10/2019) introduce, relativamente alla protezione attiva, la definizione di *Sistema o impianto a disponibilità superiore*. A determinate condizioni, sarà possibile fornire un supporto alle analisi sul comportamento della protezione passiva tenendo conto del contributo favorevole della protezione attiva, grazie ad adeguate e peculiari misure gestionali per assicurare la piena disponibilità degli impianti e sistemi di protezione attiva. Il progettista potrà sviluppare e adattare al contesto specifico i principi generali che concorrono a classificare un sistema a disponibilità superiore, al fine di beneficiare del contributo positivo apportato dalla presenza dell'impianto automatico di protezione attiva. In particolare si potrà assicurare tale requisito dimostrando che i requisiti di *affidabilità, manutenibilità* e gestione siano garantiti, con specifico riguardo agli aspetti che concorrono a migliorare la probabilità di intervento ed efficacia in ogni tempo del sistema/impianto.

19. Sistema o impianto a disponibilità superiore: sistema o impianto dotato di un livello di disponibilità più elevato rispetto a quello minimo previsto dalle norme di riferimento del sistema o dell'impianto.

Si tratta di una novità non marginale nel panorama della progettazione antincendio in quanto, per la prima volta, si scardina la tradizionale demarcazione netta e "non collaborativa" tra protezione passiva e protezione attiva antincendio, con il supporto delle misure gestionali per la sicurezza antincendio. Sarà pertanto possibile, a determinate condizioni,

Premessa generale

La revisione del Codice (D.M. 18/10/2019) introduce, nell'aggiornamento delle definizioni del capitolo G.1.14 – protezione attiva, la definizione di Sistema o impianto a disponibilità superiore:

vello di integrità (mantenimento della capacità, dell'efficacia e dell'efficienza) del sistema rispetto agli aspetti di sicurezza. Rimandando agli approfondimenti necessari per un trattamento esaustivo dei SIL, si rappresenta in questa sede che la norma IEC EN 61508[4] individua 4 valori di SIL. Lo standard IEC 61508 associa i livelli di SIL ai valori di probabilità di guasto pericoloso alla richiesta di intervento (PFD) e di fattore di riduzione di rischio (RRF).
Per sistemi o dispositivi in operazione continua, ci si riferisce alla *Probabilità di guasto o mancato intervento all'ora* (*Probability of dangerous failure per hour* – PFH) anziché alla probabilità di guasto pericoloso alla richiesta di intervento (*probability of dangerous failure on demand – PFD*).
A titolo esemplificativo, nella tabella successiva si riporta la tabella tratta dalla IEC EN 61508 con le relazioni fra SIL, PFD e RRF per sistemi strumentati di sicurezza di tipo a "bassa domanda" (low demand) di cui fanno parte gli impianti o i sistemi di protezione antincendio: un freno di un tamburo per il controllo di velocità di un volano di un processo chimico pericoloso è una funziona di sicurezza "high demand" (il freno interviene con continuità per regolare la velocità del processo pericoloso), viceversa un impianto di spegnimento che si deve attivare in caso di incendio è definito come "low demand").

SIL	PFD	PFD (power)	RRF
1	0.1-0.01	10^{-1}-10^{-2}	10-100
2	0.01-0.001	10^{-2}-10^{-3}	100-1000
3	0.001-0.0001	10^{-3}-10^{-4}	1000-10.000
4	0.0001-0.00001	10^{-4}-10^{-5}	10.000-100.000

Tabella 1 | PFD and RRF of low demand operation for different SILs as defined in IEC EN 61508

L'affidabilità (in termini di probabilità di fallimento su domanda) di un sistema cosiddetto in attesa è quindi implicitamente connessa, oltre che alle caratteristiche tecniche dei componenti del sistema critico ed alla configurazione/architettura di questi a formare il sistema critico, anche agli aspetti di ispezione, controllo e manutenzione [5]. In generale è quindi possibile ottenere un miglioramento dell'affidabilità (ed in particolare della disponibilità su domanda del sistema in relazione allo scenario di riferimento) ed un mantenimento del RRF definito come necessario rispetto allo scenario di riferimento individuato nell'ambito della valutazione del rischio migliorando le politiche di controllo e di manutenzione. Pertanto il progettista del sistema tecnico critico deve essere in grado di determinare e fornire:

- Una stima della vita utile del sistema, al fine di assicurare una pronta sostituzione dello stesso al termine di tale intervallo temporale.
- Un piano di manutenzione (inclusivo delle ispezioni e dei controlli periodici) del sistema in esame, da applicare durante la vita utile dello stesso, il cui recepimento e la cui implementazione devono essere oggetto verifica periodica da parte del responsabile dell'attività nell'ambito delle attività connesse con l'attuazione della gestione della sicurezza antincendio.

Nei casi più complessi (sistemi tecnici critici di tipo complesso o combinazione di sistemi tecnici critici o ancora sistemi critici che condividono componenti, logiche, intere funzioni strumentate di sicurezza), il progettista dovrà effettuare una valutazione quantitativa della Probabilità di Fallimento su Domanda (PFD) o della Probabilità di Fallimento Orario (PFH) con calcolazioni effettuate secondo metodiche validate e sulla base di dati in ingresso riconosciuti ed applicabili per la dimostrazione dell'affidabilità. Rientrano tra queste tecniche le seguenti [6]:

- Albero dei guasti (Fault Tree Analysis).
- Albero degli eventi (Event Tree Analysis).
- Bow-Tie.
- LOPA (Level of Protection Analysis).
- Reliability Block Diagram (RBD).
- Studi RAM (Reliability Availability & Maintenability).