L'importanza della **certificazione Safety Integrity Level** per i sistemi a riduzione permanente di ossigeno

La certificazione SIL di un impianto ORS è un metodo efficace e internazionalmente accettato per garantire il suo livello di affidabilità

Stefano Chiti, *Fire Protection Commissioning Engineer*

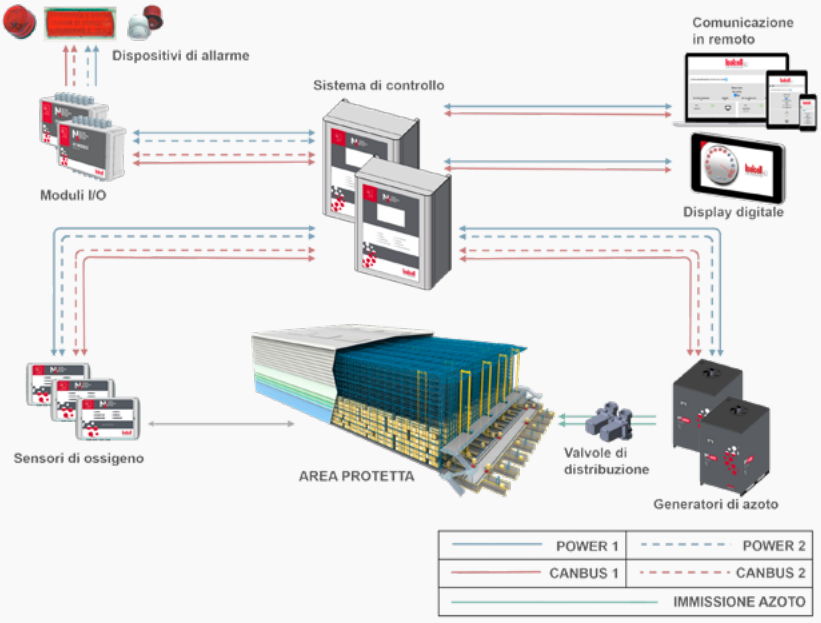
Si sente già parlare da tempo di certificazione Safety Integrity Level (SIL) per gli impianti di rilevamento incendio e gas pericolosi in ambito petrolchimico, ma la certificazione SIL sta prendendo sempre più piede anche per impianti di spegnimento incendi e loro componenti come valvole a diluvio, monitori, ed attuatori per bombole. Non fanno eccezione gli impianti a riduzione permanente di ossigeno (ORS).
Gli ORS sono una moderna tecnologia di prevenzione incendi basata su una riduzione permanente della concentrazione di ossigeno all'interno dell'ambiente protetto. Negli ambienti protetti dagli ORS viene creato un ambiente ipossico normobarico dove un incendio non può né nascere né diffondersi grazie alle molecole di azoto che, presenti in numero maggiore rispetto ad un ambiente normossico, riducono la disponibilità dell'ossigeno comburente.

Gli impianti ORS sono costituiti essenzialmente da:

- un impianto di generazione dell'azoto che, negli impianti fatti a regola d'arte, prevede un'adeguata ridondanza per sopperire ad eventi imprevisti come malfunzionamenti e/o improvvise perdite d'aria dal volume protetto maggiori di quelle considerate in fase di progetto;
- un sistema di distribuzione dell'azoto con numerosi punti di immissione (secondo la EN 16750 e ISO 20338 almeno uno ogni 150 m^2 e ogni 10 m di altezza del volume protetto) per assicurare una concentrazione di ossigeno omogenea in tutto il volume protetto;
- un sistema di rivelatori di ossigeno distribuiti omogeneamente nel volume protetto per monitorare la concentrazione di ossigeno al suo interno; proprio per aumentare la capillarità del sistema di monitoraggio, gli impianti progettati seguendo la stessa logica degli impianti rivelazioni incendi descritta nella UNI 9795 prevedono che ciascun rivelatore abbia un raggio massimo di copertura di 6.5 metri (per soffitti piani).

Stefano Chiti

Ingegnere meccanico, specialista in impianti di spegnimento con particolare attenzione ai sistemi a riduzione permanente di ossigeno ORS, è stato membro del gruppo di lavoro CEN sulla norma su questi sistemi (EN 16750). È autore di articoli su sistemi ORS pubblicati su riviste scientifiche internazionali e di diverse presentazioni a conferenze del settore. Ha maturato esperienza come progettista e consulente per numerosi impianti ORS in diversi paesi e per varie applicazioni.
Si occupa inoltre di diversi tipi di impianti di spegnimento in ambito navale nonché di sicurezza antincendio attiva e passiva in ambito nucleare.



Gli impianti ORS, a differenza di tutti gli altri impianti antincendio tradizionali, hanno il sistema di analisi e controllo dell'ossigeno costantemente in funzione: secondo la ISO 20338 infatti la concentrazione di ossigeno deve essere misurata costantemente da ogni sensore almeno una volta al minuto. Proprio per questo è molto importante che questi impianti abbiano un elevato livello di affidabilità, ossia un'elevata integrità della sicurezza che minimizzi la probabilità di guasti pericolosi che vadano a minare lo svolgimento della funzione di sicurezza prescritta in tutte le condizioni di esercizio dichiarate.
Si pensi ad esempio ad un sistema di monitoraggio dell'ossigeno di un impianto ORS che sia soggetto ad un guasto che non venga opportunamente identificato e corretto: questo guasto potrebbe comportare una concentrazione di ossigeno troppo alta nei volumi protetti e quindi un impianto ORS non capace di garantire la sua funzione di sicurezza principale, cioè prevenire un incendio, o, caso ancora peggiore, una concentrazione di ossigeno troppo bassa nei volumi protetti e quindi un pericolo per la sicurezza dei lavoratori che entrassero nel volume protetto.
Quello appena descritto è un caso estremo ed altamente improbabile grazie alle rigorose norme di progettazione dei sistemi ORS che, come descritto in precedenza, impongono una severa ridondanza ed indipendenza dei singoli rivelatori di ossigeno, ma rende tuttavia l'idea dell'importanza di avere un impianto ORS affidabile e sicuro.
I guasti pericolosi che minano lo svolgimento della funzione di sicurezza del sistema includono numerose cause che tengono conto di tutti i possibili scenari come specifiche errate, requisiti di sicurezza omessi, guasti casuali/sistematici del software, guasti comuni, errori umani, disturbi ambientali (sollecitazioni termiche, meccaniche, elettromagnetiche, sbalzi di umidità e pressione etc.) e problemi all'alimentazione elettrica.
Ed è appunto per minimizzare l'effetto di questi guasti che il livello d'integrità della sicurezza di un sistema di controllo viene misurato e certificato secondo lo IEC 61508, standard che viene appunto indicato nell'ultima norma internazionale sui sistemi ORS, la ISO 20338, come possibile metodo da seguire per garantire un'elevata integrità della sicurezza di questi sistemi.
Inoltre è importante ricordare che la IEC 61508 è recepita in Italia come CEI EN 61508, norma alla quale si riferisce anche la legge n.186 del 01/03/1968 che indica che tutte le apparecchiature, macchinari, installazioni ed impianti elettrici ed elettronici devono essere realizzati a regola d'arte e sono tali quando realizzati secondo le norme CEI, pertanto anche secondo la CEI EN 61508.
La norma IEC 61508 introduce il concetto di SIL (Safety Integrity Level), un'unità di misura quantitativa e certificata per stabilire il livello di integrità dei sistemi di sicurezza elettrici, elettronici ed elettronici programmabili per l'intero arco della loro vita, partendo dalla loro analisi fino all'esercizio passando per la realizzazione.
Vengono definiti quattro livelli SIL, da SIL1 a SIL4: maggiore è il SIL, minore è la probabilità che il sistema sia soggetto a guasti pericolosi che non permettano di eseguire la funzione di sicurezza richiesta. Il SIL è perciò una misura dell'affidabilità del sistema di sicurezza. I valori di probabilità utilizzati nell'analisi dipendono dal fatto che il componente funzionale sia chiamato a intervenire con alta o bassa frequenza: a differenza di tutti gli altri sistemi antincendio tradizionali che sono chiamati ad intervenire con bassa frequenza (low demand), i sistemi ORS hanno il sistema di monitoraggio

>

e controllo dell'ossigeno costantemente in funzione e quindi chiamati ad intervenire ad alta frequenza (high demand).
Per i sistemi high demand il livello SIL corrisponde a una frequenza ammissibile di guasto pericoloso all'ora secondo la seguente tabella:

Livello SIL	Frequenza ammissibile di guasto pericoloso all'ora [1 / h]
SIL 1	da 10^{-6} (incluso) a 10^{-5} (escluso)
SIL 2	da 10^{-7} (incluso) a 10^{-6} (escluso)
SIL 3	da 10^{-8} (incluso) a 10^{-7} (escluso)
SIL 4	da 10^{-9} (incluso) a 10^{-8} (escluso)

All'interno di un determinato impianto ci sono normalmente diverse funzioni di sicurezza ciascuna delle quali relativa a un determinato pericolo a cui va associato un appropriato SIL.
Affinchè un impianto raggiunga una determinata classe SIL, ciascuno dei suoi elementi collegato ad una determinata funzione di sicurezza deve rispettare i requisiti prescritti da quella classe SIL: se anche uno solo degli elementi collegati ad una funzione di sicurezza raggiungesse una classe SIL inferiore, l'impianto verrebbe classificato con la classe SIL raggiunta da quell'elemento.
Gli impianti ORS vengono normalmente scomposti nei seguenti elementi collegati ad una funzione di sicurezza a ciascuno dei quali viene assegnato un certo livello SIL:
sensore di ossigeno
sistema di controllo
modulo I/O
generatore di azoto
valvola di distribuzione dell'azoto

In base a quanto spiegato sopra, affinché un impianto ORS raggiunga una classe SIL-3, occorre che ciascun elemento (sensori ossigeno, sistema di controllo, moduli I/O, generatore di azoto e valvola di distribuzione dell'azoto) raggiunga la classe SIL-3.
La norma IEC 61508 prevede essenzialmente 3 tipologie diverse di certificazione:

a) Certificazione dell'hardware: generalmente una FMEDA (Failure Modes, Effects and Diagnostic Analysis) per determinare il comportamento del sistema in caso di guasto pericoloso.

b) Certificazione hardware con calcolo di SIL "proven in use": in aggiunta al FMEDA viene fornito un calcolo di SIL basato su dati storici relativi al funzionamento del prodotto sul campo.

c) Certificazione completa: in aggiunta alle certificazioni sopra descritte, prevede la certificazione FSMS (Functional Safety Management System), cioè la capacità aziendale di evitare e controllare i guasti durante la progettazione e lo sviluppo del prodotto.

Abbiamo visto che la certificazione SIL di un impianto di sicurezza quale è un impianto ORS è un metodo efficace e internazionalmente accettato per garantire e dimostrare il suo livello di affidabilità. Inoltre la certificazione SIL sta sempre più spesso diventando un requisito per forniture di prodotti/sistemi meccanici, elettrici ed elettronici ed avere un alto livello SIL è sicuramente un vantaggio per i sistemi di sicurezza ai quali è connesso un rischio più elevato. Gli impianti ORS rientrano sicuramente in quest'ultima categoria considerando che sono impianti di sicurezza spesso connessi a rischi elevati. Un esempio lampante sulle certificazioni SIL richieste per impianti ORS e i loro componenti sono le linee guida sul lavoro in atmosfera sotto-ossigenata redatte dell'ente svizzero SUVA, le quali richiedono un livello SIL-3 per il sistema di misurazione e regolazione dell'ossigeno nei volumi protetti dagli ORS. ◆

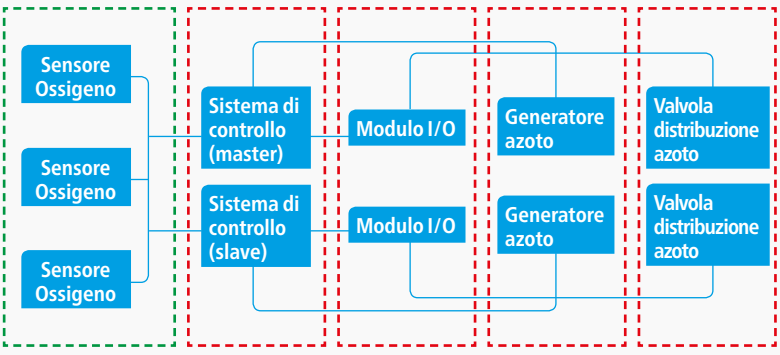


Figura 1 | Scomposizione in blocchi funzionali di un impianto ORS ai fini di ottenere la certificazione SIL