Valutazione di sicurezza per attrezzature di monitoraggio della temperatura in raffineria

Giovanni Picciolo, Andrea Tonti

È descritto un sistema per il monitoraggio a lungo termine di componenti invecchiati che operano ad alte temperature (creep) in una raffineria. Le caratteristiche di base del sistema si riferiscono a dati di processo tempo-storia e caratterizzazione in termini di precisione, di sicurezza e di integrità funzionale (SIL). I dati di esercizio sono normalmente acquisiti dal BPCS che controlla l'Unità di processo e sono disponibili per ulteriori elaborazioni. È introdotto il concetto di rischio connesso con il tempo operativo critico delle attrezzature a pressione dell'Unità rispetto alle ore di esercizio, come una variabile controllata rispetto al target di sicurezza nominale vita utile H*. È presentato un controllo delle misure delle temperature di convalida del sistema basato su una "funzione di sicurezza" e relativo SIL, connessa con il rischio specifico di superamento della vita utile e la sua riduzione, sulla base dei dati reali o presunti oppure in mancanza di essi.

Il contesto normativo in cui si inquadra la problematica trattata è quello relativo all'esercizio delle attrezzature a pressione. In genere si tratta di generatori di vapore o recipienti a pressione esercitati ad alta temperatura. In tali condizioni di funzionamento, le proprietà meccaniche dei materiali subiscono un degrado nel tempo. Per questo motivo tali attrezzature sono dimensionate a durata. La durata è generalmente fissata in sede di progetto e, per attrezzature verificate in sede di costruzione attraverso la normativa nazionale previgente alla direttiva PED, si tratta, quasi esclusivamente, di durate pari a 100000 ore di funzionamento. Tali limiti costituiscono la vita di progetto dell'attrezzatura. Le attrezzature possono essere esercite ulteriormente se sottoposte ad una serie di verifiche specifiche volte ad accertare l'assenza di fenomeni di danneggiamento da scorrimento viscoso a caldo. Non si può escludere la possibilità che attrezzature PED siano state certificate per durate inferiori a 100000 ore e che quindi siano prossime alla scadenza della vita di progetto, ma ad oggi, tali verifiche sono state eseguite soltanto su attrezzature a pressione conformi alla normativa nazionale previgente.

Il quadro normativo in cui si inseriscono le verifiche "di vita residua" è basato sostanzialmente sulla circolare ISPESL n.48/2003. L'applicazione della procedura di valutazione prevede una preliminare definizione delle ore di funzionamento e dei parametri di pressione e temperatura: l'esercizio subito è suddiviso in intervalli omogenei per pressione e temperatura, di durata accertata dall'utente.

Alcune attrezzature hanno funzionato per periodi di tempo molto brevi a condizioni di temperatura e pressione in cui possono essere presenti fenomeni di danneggiamento da scorrimento viscoso. In questi casi la procedura prevede la possibilità di verifiche ridotte o addirittura nessuna verifica se è possibile accertare che la temperatura non ha mai superato tali limiti. Tali accertamenti, previsti dalla sezione 6 della procedura tecnica, devono essere basati su dati *certi*. Analogamente, per gli intervalli di ricontrollo successivi al primo, la storia d'esercizio deve essere monitorata con sistemi in grado di fornire elementi *certi*, sia in termini di ore di funzionamento, sia in termini di pressione e temperatura. In alternativa, devono essere presi in considerazione soltanto i parametri di progetto e l'intervallo temporale completo fra un controllo ed il successivo (non è possibile considerare soltanto le ore di funzionamento). Questo può condurre, però, a risultati eccessivamente conservativi. Si sta studiando, quindi, la possibilità di procedere ad una "certificazione" dei sistemi di acquisizione dati, basata sulla normativa inerente la sicurezza funzionale (CEI EN 61508) e sulla normativa specifica derivata per i sistemi di misura e controllo *safety-related* degli impianti di processo (IEC 61511). Del resto, l'uso di tali strumenti è previsto già dalle norme armonizzate PED (EN13445 ed EN12952, EN 764-7) Atex 94/9/CE (EN 13463-6) e Progetto Pr EN 50495. Si cita anche la Cei EN 50156-1 (2006).

Oggetto di questo articolo è uno schema metodologico basato, tuttavia, non solo sull'applicazione dei criteri di base delle normative succitate, ma anche su criteri che assicurano che le misure acquisite nel tempo non solo siano nei limiti della necessaria precisione (accuracy) *ma anche* siano integri da manipolazioni intenzionali o da corruttibilità da eventi esterni (security); parametri che costituiscono requisiti di *sicurezza funzionale*. La metodologia è sviluppata per una unità di processo di un Impianto di raffineria.

G. Picciolo, Bureau Veritas Italia SpA - Presidente SC CEI 65A, MT IEC 61508/61511; A. Tonti, ISPESL

IEC/EN 61508/61511 e la "Integrity" delle misure di processo

Sicurezza funzionale e normativa

Il problema della sicurezza degli impianti industriali, in relazione al personale addetto, nonché più in generale, alla popolazione potenzialmente coinvolta, è sempre più sottoposto all'attenzione degli organismi legislativi e normatori.

In particolare in Europa sono state pubblicate alcune Direttive Comunitarie che contengono una serie di requisiti essenziali per la sicurezza di alcune importanti categorie di prodotti (apparecchiature e impianti di bassa tensione, macchinario, apparecchi elettromedicali ecc.).

In molti casi per realizzare i requisiti di sicurezza richiesti, vengono utilizzati sistemi elettrici ed elettronici che devono intervenire per evitare che i rischi per le persone e per le cose non si mantengano entro limiti predefiniti e ritenuti accettabili.

Affinché questi ultimi sistemi di controllo e di protezione risultino efficaci, essi devono essere in grado di svolgere le funzioni ad essi affidate (funzioni di sicurezza) con un livello di affidabilità adeguato alla criticità delle conseguenze che malfunzionamenti o guasti dell'apparecchiatura/impianto protetto possono causare.

Tale livello di affidabilità di funzionamento di questi ultimi sistemi, che contribuiscono in maniera determinante alla sicurezza globale dell'apparecchio o dell'impianto che controllano, viene denominata "sicurezza funzionale" (functional safety).

Con riferimento alla situazione europea, la serie IEC 61508 è stata recentemente sottoposta dal CenElec all'inchiesta dei Comitati nazionali per una possibile armonizzazione di tali norme per l'applicazione delle direttive europee contenenti requisiti di sicurezza totale.

Definizione di sicurezza funzionale

Alla 103ª riunione del Bureau Technique del CenElec è stata accettata la proposta contenuta nel rapporto finale del BTWG 99-2 per la definizione della sicurezza funzionale, ripresa dalla Parte 4 della IEC 61508. Tale definizione è la seguente: "La sicurezza funzionale è quella parte della sicurezza globale delle apparecchiature e dei sistemi di controllo ad esse associati che dipende dal corretto funzionamento dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza, di altri sistemi tecnologici per applicazioni di sicurezza, di dispositivi esterni per la riduzione del rischio".

È opportuno evidenziare che la sicurezza funzionale deve essere intesa, con riferimento alle *Safety Functions* che devono essere individuate nella fase di analisi del rischio anche in termini di Affidabilità (safety integrity di funzione di sicurezza) delle prestazioni in un contesto progettuale e gestionale (SIL, Safety Integrity Level).

Per chiarire tale definizione il suddetto rapporto del BTWG 99-2 fa alcune precisazioni sui sistemi per applicazioni di sicurezza (safety-related systems) e fornisce alcune esemplificazioni.

Viene precisato che i sistemi per applicazioni di sicurezza (limitati, nel contesto della normativa CenElec, ai sistemi elettrici, elettronici ed elettronici programmabili) sono quei sistemi (generalmente composti da sensori, circuiti relativi alla logica di controllo, sistemi di comunicazione, circuiti attuatori) cui è richiesto di svolgere una funzione (o più funzioni) di sicurezza per ridurre il rischio a livelli considerati accettabili.

Concetti salienti dello Standard IEC 61511

Particolarmente importante nel settore dell'Industria di Processo è lo standard IEC 61511: *Safety Instrumented Systems (SIS) of the process industry sector*.

Lo standard (parte 1) pone dei requisiti sulla specificazione, progettazione, installazione ed esercizio, di sistemi di strumentazione di sicurezza, tali che garantiscano, con un elevato livello di fiducia (SIL) un esercizio dell'impianto di processo sicuro contro i rischi, a partire dalla fase di progetto di base, fino alla dismissione: Lo standard è fondamentalmente orientato ai soli sistemi di sicurezza di tipo strumentale (sistemi di allarme, controllo, blocco) e si rivolge ai progettisti degli impianti e degli integratori di sottosistemi di strumentazione.

Gli obiettivi dello standard sono orientati sia alla sicurezza, sia a conseguire benefici economici.

L'approccio metodologico per la stima della "certezza" dei dati di processo

Un'unità di processo è un sistema complesso di componenti classificabili come attrezzature elettriche, strumentazione, strutture meccaniche, apparecchiature in pressione e attrezzature di sicurezza dell'impianto. Nelle unità di processo in cui sono presenti componenti soggetti a fenomeni di invecchiamento nel tempo per stress termici e meccanici, quali le attrezzature a pressione in regime di *creep*, il controllo e misura del processo assumono un peso significativo per una gestione in sicurezza dell'Unità. In particolare, i sistemi di regolazione automatica ed i sistemi di allarme e blocco assicurano che non siano superate determinate soglie di sicurezza.

Specifiche misure, quali temperature e pressioni di componenti di forni e caldaie, quali i tubi di processo, che sono normalmente acquisite dai sistemi di misura e controllo (BPCS) costituiscono la base informativa per una gestione *in sicurezza* dei suddetti componenti. È pertanto definibile il concetto di rischio, come *la combinazione* della possibilità (probabilità/frequenza in un periodo di tempo: Top Event) di verificarsi di un *evento di pericolo* (*collasso* del materiale o, equivalentemente, il *superamento* della massima durata di esercizio alle condizioni di temperatura e pressione di progetto dei materiali in regime di creep) e della severità delle conseguenze. Il collasso dei materiali può costituire una causa di pericolo per il personale e l'ambiente, oltre naturalmente comportare una perdita economica. I sistemi di protezione, pertanto, assicurano contro condizioni anomale, con livelli di probabilità normalmente valutati nell'ambito degli studi di rischio e/o Rapporti di Sicurezza dell'Impianto cui l'Unità fa parte.

La riduzione e gestione del rischio, costituisce un importante obiettivo dell'Esercizio dell'Unità di Produzione, concetto base della legislazione vigente in materia (per esempio DLGS 334, 626, 329).

L'applicazione delle Norme europee IEC/EN61508 & IEC/EN61511 insieme all'utilizzo di metodologie di valutazione dell'idoneità al servizio, quali analisi di rischio RBI (Risk Based

Inspection) consentono di ridurre il rischio di possibili incidenti ai necessari livelli di accettabilità.
Misure *affidabili* di determinate variabili di processo costituiscono, quindi, la base informativa primaria per valutare lo stato di integrità dei materiali nel tempo realizzando, di conseguenza, una funzione di controllo per la sicurezza definibile come una vera e propria Funzione di sicurezza (Safety Function).
È infatti evidente che l'acquisizione di dati storici è essenziale per la valutazione di questo rischio: tanto più siamo sicuri sulle informazioni relative a condizioni di esercizio pregresse al di sotto delle condizioni di progetto dei materiali, tanto più il rischio di superamento del target delle ore ammissibili è basso e viceversa.
La valutazione del livello di affidabilità (SIL) delle misure sarà, pertanto definito sulla base della riduzione (SIL = 1/RRF: Risk Reduction Factor) del rischio (figura 1) di superamento, in un determinato orizzonte temporale, di parametri critici di stabilità dei materiali in condizioni di esercizio specifiche: creep a caldo.
Lo schema sviluppato è basato sul concetto di *riduzione del rischio* mediante una *funzione di sicurezza strumentata* (Safety Instrumented Function: SIF) a cui è associato un Livello di integrità di sicurezza: SIL che coincide con la disponibilità di misure di processo affidabili (certe). La Norma di riferimento è, pertanto, la IEC 61511.
Obiettivo, quindi, dello studio, è quello di verificare che il sistema di misura e regolazione automatica (e sistemi di blocco, eventualmente presenti) installato sia conforme ai requisiti funzionali e di disponibilità (SIL) di misure in caso di guasti del sistema di controllo *non rivelati* od eventi incidentali esterni per evitare la possibilità di supermento dei limiti di vita utile (integrità dei materiali) a livelli di probabilità accettabile.
Il sistema di acquisizione dei dati di processo si inserisce in uno schema più generale di disponibilità di "informazioni" per la completa qualificazione dei suaccennati dati ai fini della conformità della Norma IEC 61511.
Con il termine "informazioni" si intende il complesso di dati numerici, di documentazione, procedure e quant'altro si ritiene necessario per consentire una valutazione dello stato di integrità dei materiali ad un determinato istante dalla messa in servizio dell'Unità di Processo sufficiente ad assicurare la "certezza" delle misure al necessario livello di affidabilità.
Le attività condotte vertono su tre tematiche principali con l'obiettivo di garantire uno strumento di gestione e monitoraggio di specifici dati di processo che rispettino i seguenti requisiti di sicurezza: la *security*, l'*accuracy*, la *integrity*.
La specificazione del SIL minimo è obiettivo della valutazione di conformità della "Safety Instrumented Function" ai requisiti di sicurezza funzionale (Safety Requirements).

La Security delle misure dal campo
Il primo requisito riguarda la "security" dei dati dal campo acquisiti dal sistema esistente di misura e regolazione.
Con il termine "security" si definisce la sicurezza del Database reso disponibile dall'Utente contro alterazioni potenziali dei dati ivi contenuti dalla fase di acquisizione dal campo a quella di supporto hardware per la successiva elaborazione da parte del Progettista dell'attrezzatura a pressione.
Tenuto conto di sistemi di acquisizione di dati esistenti, ci si riferisce, per quanto possibile, a Norme e standard del settore specifico (per esempio la IEC 62443-3).

L'Accuracy
Il secondo requisito è relativo alla "precisione" dei dati in funzione dei requisiti richiesti dal processo (errore tollerabile della misura di processo).
Ciò comporta una verifica relativamente ai criteri e procedure (per esempio la disponibilità di "Certificati" del Controllo Qualità, le procedure ecc.) utilizzate dall'Azienda per assicurare nel tempo la necessaria precisione dei dati acquisiti.

La Sicurezza Funzionale
Il terzo requisito è relativo al livello di "Sicurezza Funzionale" (Functional Safety) delle opportune misure di variabili di processo acquisite mediante i sistemi di misura e controllo automatico installati presso l'Utente l'attrezzatura a pressione. Le suaccennate misure sono definite come funzioni di sicurezza strumentate (SIF). Alla Funzione di Sicurezza è associato un SIL ed una opportuna metrica probabilistica (Probability of Failure per Hour: PFH, Average Probability of Failure on Demand: PFDavg) secondo quanto riportato nella IEC /EN 61508-1 [1] e IEC/EN 61511-1 [2]. Si vedano le tabelle 1 e 2.

FUNZIONAMENTO IN MODO CONTINUO	
Livello di integrità di sicurezza (SIL)	Obiettivo della frequenza di guasti pericolosi per realizzare la la funzione strumentata di sicurezza (per ora)
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Tabella 1 - CEI-EN 61511-1. Livelli di integrità di sicurezza: probabilità di guasto

FUNZIONAMENTO IN MODO SU DOMANDA		
Livello di integrità di sicurezza (SIL)	Obiettivo di probabilità media di guasto su domanda	Obiettivo di riduzione del rischio
4	$\geq 10^{-5}$ to $<10^{-4}$	>10 000 to ≤100 000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1 000 to ≤10 000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1 000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100

Tabella 2 - CEI-EN 61511-1. Livelli di integrità di sicurezza: probabilità di guasto su domanda

La valutazione del livello di Integrità dei dati (Affidabilità delle misure che realizzano la Funzione di sicurezza) costituisce oggetto della attività (Scopo del Lavoro).
La conformità ai requisiti della IEC/EN 61511, in particolare, richiede la verifica di conformità per quanto riguarda anche aspetti organizzativi e gestionali aziendali.

L'analisi del rischio
Il sistema di acquisizione delle misure e di regolazione automatica di processo (BPCS) fornisce le informazioni e consente il monitoraggio delle variabili significative per la conduzione dell'Unità dell'Impianto. La conoscenza di informazioni di pro-

►

cesso, sia relativamente alle misure dirette e/o indirette in un determinato intervallo di tempo devono assicurare - con uno specifico livello di certezza - che il Rischio residuo sia accettabile (figura 1).
Ai fini di assicurare i livelli di sicurezza dell'Unità, tuttavia sono normalmente installati anche sistemi di protezione (sistemi di blocco) tali da evitare sia con interventi manuali, sia automatici, l'insorgere di situazioni di pericolo sia per guasti e/o disservizi inerenti l'Unità e/o per cause esterne. Il Sistema di sicurezza, nel suo complesso, è costituito da barriere (Independent Protection Layers: IPL, figura 2) la cui azione è quella di evitare, ciascuna con diversi livelli di probabilità di fallimento[1], il verificasi dell'evento pericoloso ipotizzato. Top Event che può essere definito come la "perdita delle misure certe delle variabili di processo che caratterizzano lo stato di integrità dei materiali in regime di creep a caldo" in un determinato intervallo di tempo: superamento della vita utile. Il sistema di monitoraggio delle variabili di processo costituisce *una di queste barriere*, poiché consente una gestione della emergenza efficace in caso di anomalie o eventi incidentali. C'è da osservare, tuttavia che la mancanza dei soli dati certi di processo (misure) comporta una perdita della conoscenza dello stato di integrità (per quanto attiene il sistema di monitoraggio) ma non necessariamente una contemporanea mancanza del controllo delle variabili (set point). Solo nel caso di indisponibilità delle misure (a) delle regolazioni automatiche (b) e del mancato intervento dei sistemi di blocco[2] e/o di misure correlate, si potranno avere condizioni disservizio - interno e/o) esterno all'Unità di processo e riduzione della vita dei materiali non rivelata.

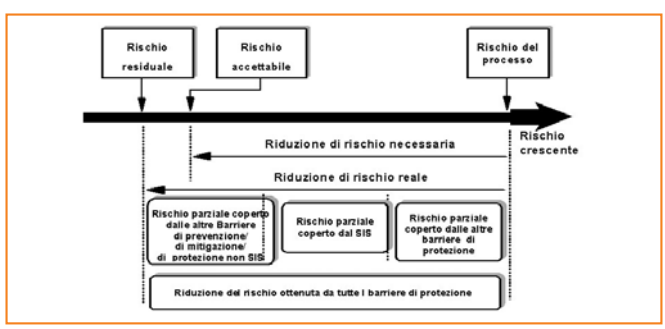


Figura 1 - Livelli di rischio e barriere di riduzione

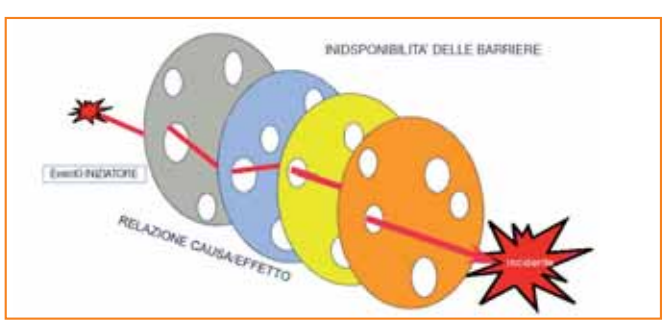


Figura 2 - Barriere indipendenti di sicurezza (IPL)

[1] Il livello di riduzione di rischio realizzato da una IPL deve non essere inferiore a 1:10

[2] Nel caso sia installato (analisi HAZOP)

Definizioni
Si premettono alcune definizioni:
- h*: variabili di esercizio a progetto (temperature).
- H*: periodo di tempo di esercizio (vita utile) in sicurezza del materiale alle condizioni di progetto.
- λ': soglia di frequenza di eventi di perdita delle misure e controlli con superamento delle condizioni di progetto per una durata Δτ'.
- λ'': soglia di frequenza di eventi di disservizio non rivelati con superamento delle condizioni di progetto per una durata Δτ''.
- λ*=λ'+λ'': soglia di frequenza di eventi di perdita delle misure e controlli o di eventi di disservizio non rivelati con superamento delle condizioni di progetto.
- λ_{target}: soglia di frequenza di eventi di perdita delle misure e controlli con superamento delle condizioni di progetto H*.
- k: numero di superamenti di h* delle variabili di processo in un determinato intervallo di tempo τ.
- R*(τ) = Pr(t>τ): probabilità cumulata al tempo τ, che siano superati i limiti di stabilità dei materiali in uno o più eventi di disservizio (k) non rivelati di durata Δτ'o Δτ''.
- Δτ': intervalli di tempo non rivelati di superamento delle condizioni di esercizio di progetto h* per disservizi di sistemi di misura e regolazione (e blocco) con frequenza λ'.
- Δτ'': intervalli di tempo non rivelati di superamento delle condizioni di esercizio di progetto h* per eventi esterni per disservizi di sistemi di misura e regolazione (e blocco) e frequenza λ''.
- Δτ*=Δτ', Δτ''.
- ρ' (k): riduzione di vita del materiale al k-mo evento di disservizio di durata Δτ'.
- Δρ'' (k): riduzione di vita del materiale al k-mo evento di disservizio di durata Δτ.
- ρ*(k) : riduzione di vita del materiale al k-mo evento di disservizio di durata Δτ' o Δτ'' per disservizi per cause interne (misure, regolazioni) o esterne, la cui frequenza è λ*.
- PFH : acronimo di Probability of Failure per hour.
- SIL : acronimo di Safety Integrity Level.
- SIF: acronimo di Safety Instrumented Function.
- MTTR: acronimo di Tempo Medio di Riparazione (Mean Time To Repair) = 1/μ.
- BPCS: sistema di controllo di processo base.
- EUC: attrezzatura a pressione (apparecchiatura sotto controllo).

Si veda la figura 3. Dalla analisi del particolare processo in

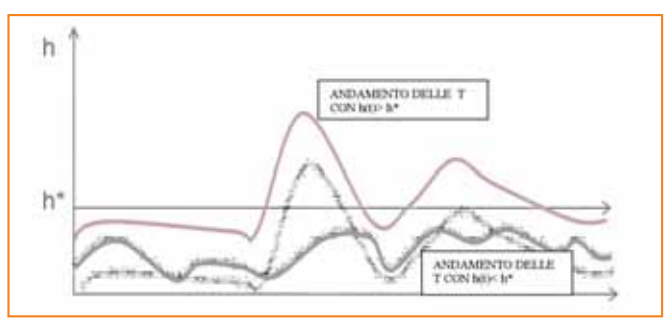


Figura 3 - Andamento nel tempo delle temperature del materiale in due tipologie di esercizio: inferiore e superiore alle condizioni di progetto h*

oggetto, la stima della vita residua dei materiali è, correlata alla temperatura di esercizio e/o ad altre variabili di processo funzionalmente equivalenti (pressioni, portate ecc.).
I valori delle misure di processo possono essere carenti in determinati periodi di tempo; quindi devono essere *ricondizionati*, tenuto conto anche della disponibilità, in quegli stessi intervalli di tempo, del controllo automatico e/o degli interventi dei sistemi di blocco. È inoltre necessario conoscere eventuali azioni di riparazione dei materiali o sostituzione in caso di eventi di danno accidentale (incidenti) dal Libretto.
La disponibilità, inoltre, di analisi di materiali in un determinato istante t su una replica del materiale fornisce lo stato effettivo di integrità e quindi la stima di vita residua [3].
Attraverso una replica metallografica sul materiale si può escludere - o meno - la presenza di difetti dovuti all'esercizio in regime di scorrimento viscoso. Se tale fenomeno si è verificato, si può stabilire lo stato di avanzamento del danno da creep.
La disponibilità delle misure dirette od indirette di temperatura così come quelle ricostruite sulla base della disponibilità eventuale del sistema di controllo automatico, consente di stimare lo stato di integrità ed il tempo di vita residua secondo le teorie dello scorrimento viscoso. In caso di guasto del sistema di misura e regolazione automatica si può perdere una quantità di informazione che può rivelarsi importante per la stima del rischio; in altre parole, la misura delle variabili di processo (temperatura e pressione: SIF) dovrà essere disponibile con un minimo livello di integrità (SIL).
Da quanto sopra ne consegue che la specificazione del livello di SIL della SIF è definibile sulla base di tre fattori:

- la frequenza $\lambda^*(\lambda du)$ del guasto non rivelato (dangerorus undetected) se non con test periodici o da altre variabili di processo direttamente correlate a quelle misurate e/o...
- la durata $\Delta\tau^*(\Delta\tau', \Delta\tau'')$ non rivelata dei disservizi dei sistemi di misura e regolazione (eventi esterni) a cui venga associato un superamento delle condizioni di progetto delle variabili di processo dell'attrezzatura a pressione;
- l'entità della riduzione di vita $\Delta\rho^*(k)$ per il superamento delle condizioni di progetto h* delle variabili di processo dell'attrezzatura a pressione al k-mo evento di guasto nell'intervallo $\Delta\tau^*$. Il $\Delta\rho^*(k)$ valore corrisponde alla riduzione della vita utile del materiale al k-mo evento di disservizio in un intervallo di tempo prefissato di esercizio τ dalla data di messa in servizio dell'attrezzatura. In generale i $\Delta\rho^*$ potrebbero non essere costanti in funzione di k, in quanto se il materiale ha memoria: $\Delta\rho^*(k+1) > \Delta\rho^*(k)$. La specificazione del $\Delta\rho^*(k)$ è oggetto della teoria del fenomeno del creep in condizioni di scorrimento viscoso a caldo.

Il primo fattore è relativo alla probabilità/frequenza (cumulata) dei guasti dei sistemi di misura e regolazione (e di protezione) con superamento h* (non rivelato per $\Delta\tau^*$) delle condizioni di progetto del materiale ad un determinato istante t; il secondo è valutabile sulla base frequenze di disservizio del BPCS e mancato intervento dei sistemi di blocco automatico ed il terzo delle conseguenze della perdita del controllo delle variabili critiche o di accadimento degli eventi esterni.
Risulterà:

$$H^* = \Sigma \Delta\rho^*_{1,N} \text{ per } k = 1, 2, .. N, \qquad (1)$$

dove k corrisponde al numero di eventi di disservizio in un intervallo di tempo definito τ (tempo di missione).
Se con $\Delta\rho'(k)$ e $\Delta\rho''(k)$ si indica la riduzione della vita utile del materiale per l'evento di durata $\Delta\tau'$ e $\Delta\tau''$ con frequenza λ'e λ'' rispettivamente ed assunti costanti, $\Delta\rho^*$ è distribuito con legge esponenziale, la probabilità di accadimento di numero di k disservizi in un determinato intervallo di tempo τ a cui sia associata una frequenza λ^*, è descrivibile con un processo di Poisson omogeneo: Poiss (k; $\lambda^*\tau$) che corrisponde alla probabilità in τ di avere un numero di eventi di guasto pari esattamente a k, ciascuno con frequenza λ^*.
Ne consegue che se H* è la vita utile del materiale quando si verificano almeno k = N eventi di disservizio di durata $\Delta\tau^*$, la probabilità Pr ($t > \tau$) di consumare la vita del materiale in τ sarà semplicemente:

$$\text{Poiss}\,(k = N;\ \lambda^*\tau) = (\lambda^*\tau)^N \times e^{-(\lambda^*\tau)}/N! \qquad (2)$$

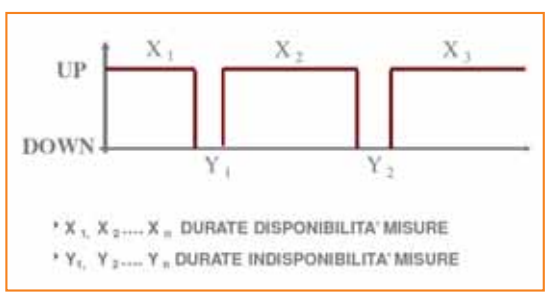


Figura 4 - Distribuzione frequenza/durate indisponibilità misure

Lo schema procedurale è basato sulla verifica del loop di misura (SIS) che realizza la SIF in accordo ai requisiti riportati nella IEC/EN 61511.
La perdita delle informazioni relative allo stato di integrità dei materiai dipende sia dalla perdita delle misure e contemporaneamente dalla perdita del controllo di processo o dalle informazioni relative a un evento di disservizio rilevante ed azioni conseguenti di ripristino.
Alla perdita di queste informazioni può essere associata una probabilità/frequenza cumulata (in un periodo di tempo di riferimento) ed una durata $\Delta\tau'$ (o $\Delta\tau''$) di superamento (non rivelato) delle specifiche di progetto h* della attrezzatura a pressione.
La soglia di rischio accettabile R* è quindi definibile come la probabilità di non superamento della H* ad un determinato intervallo temporale τ. La SIF, funzione strumentata di sicurezza, assicura che venga ridotto il rischio (definito come più sopra) di superamento di H* in un determinato intervallo di tempo τ nei limiti di accettabilità e con un livello minimo di integrità: SIL (PFH, PFDavg).
Da quanto sopra ne consegue che se indichiamo con PFH la probabilità (media annua) di perdita delle misure delle variabili di processo che caratterizzano lo stato di integrità dei materiali e PFDavg la probabilità contemporanea di mancato intervento dei sistemi di blocco automatico (se presenti), risulterà, se: dove si

assume che $\lambda^* = \lambda'$ e λ'' siano delle costanti, cosicchè il tempo t al disservizio è distribuito con legge esponenziale con distribuzione $f(t) = \lambda e^{-\lambda t}$ ed analogamente, le durate dei disservizi $\Delta\rho^*$ con superamento della soglia h*. Si assume, inoltre, che l'entità del superamento ed andamento della variabile di processo segua una legge deterministica, valutata sulla base dell'HAZOP (Analisi di rischio).
Quindi, se $R^*(\tau) = Pr[t>\tau]$ e definiamo $\lambda' = \lambda_{cont.} \times PFD_{avg\text{-}cont}$ la frequenza di guasto non rivelato di durata $\Delta\tau'$ sia del sistema di misura e della regolazione automatica ed anche del sistema di protezione e λ'' la frequenza di accadimento di un evento di superamento di h* per cause esterne non rivelato di durata $\Delta\tau''$ con riduzione del tempo di vita $\Delta\rho'(k)$ o $\Delta\rho''(k)$ al k-mo evento di guasto con $MTTR = 1/\mu_{cont}$, $MTTR = 1/\mu_{misure}$ è possibile determinare il valore del PFH del sistema di misura tale da assicurare che non si verifichi l'evento non rivelato di superamento del H* (Top Event) con il limite di accettabilità minimo di una frequenza λ^*, tale per cui risulterà:
$Pr[t>\tau] = Poiss(k=N, \lambda^*\tau) < Pr_{target}$ con $\lambda^* = (\lambda' + \lambda'') = \lambda_{Top\ event}$
È infatti evidente, che dalle (1) e (2) la stima della frequenza media annua di superamento di H*, la frequenza $\lambda^* = PFH$ può essere facilmente determinata sulla base del processo poissoniano associato alla distribuzione esponenziale del tempo al guasto per un determinato numero di accadimenti di disservizio.
Nella tabella 1 sono riportate (a titolo indicativo) stime relative a vari casi di frequenza di disservizio assunte dei sistemi di misura e regolazione (non si tiene conto del sistema di blocco automatico) basate su valore generali (IEC 61511-1, §8.2.2) delle frequenze di disservizio (non rivelati) e dei tempi di ripristino assunti per di sistemi di controllo distribuito (BPCS) per diversi periodi di esercizio e vita residua:

$$r(k, \tau) = H^* - \Sigma\Delta\rho^*(k, \tau) \qquad (3)$$

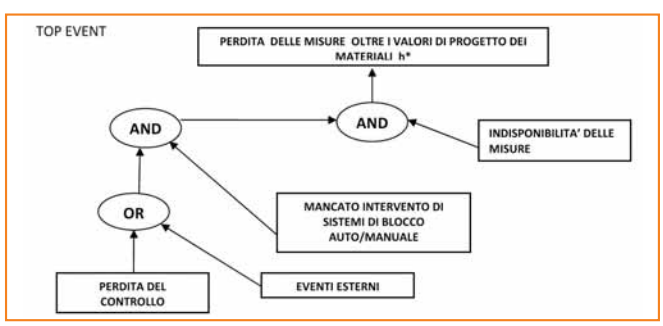


Figura 5 - Albero dei guasti relativo al Top Event: "Perdita delle misure oltre i valori di progetto dei materiali"

Acquisizione dei dati di processo e stima del SIL
Di seguito è la descrizione del sistema di acquisizione dei dati di processo e stima del SIL (PFH) della funzione di sicurezza realizzata (temperatura equivalente). Riferendoci all'EUC in oggetto (tubi in regime di scorrimento viscoso) è normalmente installato un sistema di misura e regolazione per fornire all'Operatore dell'Unità, cui l'EUC fa parte, le necessarie informazioni per l'operatività ed ad contempo, assicurare il mantenimento del *set point*.
In ogni caso è previsto un sistema di allarme e blocco automatico (e manuale) in caso di superamento di condizioni critiche per il processo e/o la sicurezza.

Figura 6 - Tipico schema funzionale di un sistema di acquisizione, elaborazione di variabili di processo

Il sistema di sensori misura le variabili di processo necessarie per la gestione dell'Unità. In genere i sensori sono ridondanti sia per canale di misura (con logiche maggioritarie) sia per funzione. Il sistema di misura è realizzato da interfacce (moduli di ingresso) che hanno la funzione di conversione del segnale dal campo da analogico in digitale per essere elaborato dal processore digitale e disponibile per l'acquisizione e memorizzazione.
Nella figura 5 è riportato l'albero dei guasti relativo al Top Event di indisponibilità delle misure oltre i valori di progetto h* dei materiali in esercizio alle condizioni di scorrimento viscoso.
Nella figura 6 è rappresentato lo schema a blocchi funzionale di principio del sistema di controllo e di acquisizione delle misure inerenti al funzione di sicurezza; nella figura 7 è, invece, riportato lo schema a blocchi di disponibilità (RBD) associato. Sulla base della struttura e configurazione del sistema di misura, partendo dai sensori in campo fino all'acquisizione e presentazione grafica e memorizzazione su opportuno supporto è valutabile la stima della metrica del PFH relativo al data base delle misure in un determinato periodo di tempo.

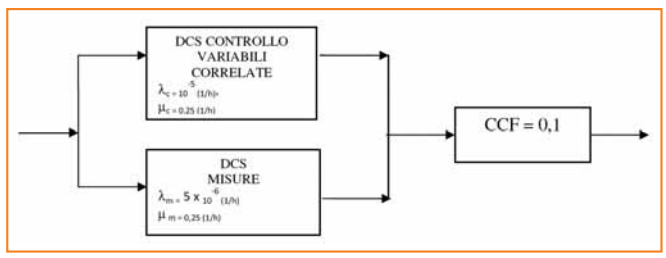


Figura 7 - Schema a blocchi di affidabilità (RBD) relativo alla SIF (misura e controllo)

Stima preliminare della indisponibilità delle informazioni di processo
Nel caso specifico, il SIS dovrà realizzare la SIF a cui è associato un SIL minimo e tale che la metrica sia conforme alle modalità richieste per la riduzione del rischio alla soglia di accettabilità. La stima del PFH (λ^*) della SIF è il primo parametro che concorre alla stima della indisponibilità media delle misure A. Il secondo riguarda la indisponibilità del controllo automatico relativo alle variabili dirette o correlate. Accanto a questa frequenza (PFH) di evento di perdita delle misure deve essere associato quella relativa al ripristino delle misure:
$\mu_{misure} = 1/MTTR_{misure}$. Analogamente per il controllo automatico: $\mu_{cont.} = 1/MTTR_{cont}$.

Una stima preliminare del PFH del sistema di misura costituito da sensori di temperatura, (per esempio termocoppie), trasmettitori di pressione, l'elettronica del BPCS (schede di acquisizione, CPU ecc.) può essere classificata nel campo del SIL 1 (in assenza di una verifica per livelli superiori, secondo della IEC 61511); quindi un PFH della SIF *non superiore* a 10^{-5} e *non inferiore* a 10^{-6} guasti per ora. Analogamente per quanto riguarda la Funzione di controllo automatico della variabili di processo.
Se si ipotizza una $\lambda_{du\text{-}misure} = 5.10^{-6}$ 1/h per il SIS di misura e $\lambda_{du\text{-}cont}$. (dangerous undetected: guasti non auto evidenziati dal sistema stesso[3]) di 1.10^{-5} 1/h per il SIS di controllo con verifica annuale (T1 = 8760 h) in occasione delle attività di manutenzione periodica nel sistema di controllo e di acquisizione delle misure con un tempo medio di ripristino (MTTR) del guasto di 4 ore e con un CCF del 10% (guasto comune BPCS e sistema di acquisizione delle misure) si otterrebbe, in prima approssimazione, un $PFH_{1\,O\,O\,2}$ del sistema pari a circa 2.10^{-6} (1/y) (cfr nota[4]). Questa stima, di massima, del PFH rientra nel campo del SIL 1 (tabella 1: 10^{-5} - 10^{-6} 1/h) della funzione di indisponibilità delle misure (SIF).
Il fatto che si verifichi questo evento con la frequenza sopracitata, comporta che nell'intervallo di tempo di indisponibilità delle misure e del controllo (assunto continuativo) di processo possa verificarsi il superamento delle condizioni di progetto dei materiali (o per la perdita del controllo automatico e delle misure, causa comune di guasto, e per mancato intervento dei sistemi di blocco[5]; o per altre cause non ad esso imputabili, esterne, per esempio: mancanza di vapore di emergenza, black out elettrico ecc.). Si determinerà, quindi, una riduzione del tempo di vita utile del materiale non rilevato (rischio) e non acquisito nel Database. Le cause del disservizio possono variare caso per caso e le conseguenze valutate in fase di analisi di rischio (figura 3).
Assumendo che si verifichi il superamento delle condizioni di progetto dei materiali (evento non escludibile, fondamentalmente per cause rilevanti esterne; ad esempio: mancanza di vapore di emergenza, black out elettrico, ecc. e non controllabili dal sistema di automazione) le informazioni saranno sicuramente riportate - da procedura aziendale - sul "libretto" della apparecchiatura a pressione, senza perdita, quindi della informazione necessaria per stima dello stato di integrità dei materiali. Diversamente se interviene il sistema di blocco automatico; in tal caso non verrebbero superate le condizioni di progetto dei materiali con una determinata probabilità (PFDavg[6]). La probabilità di mancato intervento del sistema di blocco automatico potrebbe comportare le stesse conseguenze dovuti ad eventi non controllabili esterni, quindi rivelati.
Nel caso di sistema di controllo automatico e di acquisizione delle misure realizzato nello stesso sistema (BPCS) è necessario verificare la indipendenza hw e sw per la stima del PFH. Non è escludibile infatti un Modo Comune di Guasto (CCF) che riduce la affidabilità (PFH) della SIF. In genere, tuttavia, il sistema di blocco sarà indipendente dal BPCS e costituirà, pertanto un IPL. La probabilità di mancato intervento di un blocco automatico (PFDavg) con test periodico almeno annuale infatti, è dell'ordine 10^{-2} (per SIS semplici: un solo sensore ed un solo attuatore e realizzato con sensori elettronici digitali e valvole pneumatiche di blocco o motori elettrici, [4]).
Questa analisi deve essere condotta, come previsto anche dalla IEC 61511-2, §11.5.2, per la verifica del SIL della SIF.
Quindi, il livello di rischio $R^*(\tau)=Pr(t>\tau)$ di superamento della vita utile della attrezzatura a pressione H*, dopo un intervallo di tempo τ è fortemente condizionato dal tipo di progetto del sistema di regolazione e di protezione (λ^*, SFF) dal numero k di eventi di superamento delle condizioni di progetto h* e della legge di accumulo del danno $\Delta\rho^*(\tau, k)$. Infatti come risulta dalle stime della probabilità di evento di superamento della vita H* ad un istante τ, in funzione della frequenza credibile media stimata di guasto λ' dell'ordine di $2x10^{-2}$. 10^{-2}1/y<5.10^{-4}1/y) del BPCS (e blocchi) riportate nella tabella 3, si otterrebbe una probabilità di superamento di H* pari a 10^{-6} nell'arco di tempo non inferiore a 20 anni dalla messa in servizio dell'attrezzatura a pressione, con un numero di eventi di guasto non rivelati superiore almeno a 2 (due guasti comporterebbero il superamento di H*).
Analoga considerazione vale nel caso di eventi di disservizio esterni all'Unità di processo, che tuttavia, potrà essere stimata per il caso specifico sulla base dei dati dell'analisi di rischio condotta.

λ [1/y]	λ [1/y] X T [y]	λ [1/y]	λ [1/y] X T [y]	λ [1/y]	λ [1/y] X T [y]	λ [1/y]	λ [1/y] X T [y]	
0,0005	0,005	0,01	0,1	0,02	0,2	0,04	0,4	K
T = 10 [y]								
	1,24377E-05		0,004524187		0,016374615		0,053625604	2
	2,07294E-08		0,000150806		0,001091641		0,00715008	3
	2,59118E-11		3,77016E-06		5,45821E-05		0,000715008	4
	2,59118E-14		7,54031E-08		2,18328E-06		5,72006E-05	5
T = 20 [y]	0,01		0,2		0,4		0,8	
	4,95025E-05		0,016374615		0,053625604		0,143785269	2
	1,65008E-07		0,001091641		0,00715008		0,038342738	3
	4,12521E-10		5,45821E-05		0,000715008		0,007668548	4
	8,25042E-13		2,18328E-06		5,72006E-05		0,001226968	5
T = 30 [y]	0,015		0,3		0,6		1,2	
	0,000110825		0,03333682		0,098786094		0,216859833	2
	5,54125E-07		0,003333682		0,019757219		0,086743933	3
	2,07797E-09		0,000250026		0,002963583		0,02602318	4
	6,23391E-12		1,50016E-05		0,00035563		0,006245563	5
T = 40 [y]	0,02		0,4		0,8		1,6	
	0,00019604		0,053625604		0,143785269		0,258427543	2
	1,30693E-06		0,00715008		0,038342738		0,137828023	3
	6,53466E-09		0,000715008		0,007668548		0,055131209	4
	2,61386E-11		5,72006E-05		0,001226968		0,017641987	5

Tabella 3 - Stima della probabilità di perdita di vita utile H* in funzione della frequenza di disservizio non rivelato (dangeorus undetected) ldu dei sistemi di misura e regolazione automatica in funzione del numero di disservizi k in un determinato scenario temporale T (y)

Conclusioni

È presentato uno schema di acquisizione delle misure di processo (temperature) relative ai materiali costitutivi delle attrezzature a pressione basato su una "funzione di sicurezza" connessa con il rischio specifico di collasso di materiali in esercizio

[3] Quindi, non riparabili.
[4] La stima del PFH è valutata con il modello matematico di cui all'Annesso D, §B3.2.2, della Norma IEC 61508, parte 6 con b= 10% e frequenza media ldu = 8.10-6 1/h (SIL 1) ed un intervallo di test periodico (T1) per i guasti non rilevati pari a 8760 ore e di riparazione di 4 ore (MTTR).
[5] Se presenti.
[6] Probability of failure on Demand

in condizioni di creep a caldo in un determinato scenario temporale. Si fa riferimento alla Norma IEC/CEI 61511, specifica per la valutazione della sicurezza funzionale dei sistemi strumentati di sicurezza per gli impianti di processo. Il sistema di acquisizione delle informazioni "certe", che tengono conto sia degli specifici requisiti di *accuracy*, *security* e di *sicurezza funzionale*, consente il monitoraggio delle variabili significative per la conduzione dell'Unità dell'Impianto in condizioni di sicurezza, a fronte di un obiettivo quantificato di rischio tollerabile. I dati di processo sono pertanto utilizzabili per una successiva valutazione, unitamente alle altre informazioni richieste dalla Circolare 48/2003, per la stima della vita residua. Lo schema è basato sulla ipotesi che l'andamento dei guasti dei sistemi di regolazione automatica e di acquisizione delle misure seguano una legge esponenziale; ipotesi che è normalmente verificata per questo tipo di sistemi. L'evoluzione del tempo medio al guasto è quindi descrivibile con un processo di Poisson omogeneo che fornisce la probabilità di riduzione r (3) della vita utile H* dell'attrezzatura a pressione in un determinato intervallo di esercizio τ in funzione del numero di eventi $\Delta\rho^*$ (k) necessari per il raggiungimento di H*. La metodologia è applicabile a tutte le attrezzature a pressione le cui condizioni di esercizio sono monitorate da sistemi di misura e controllo di processo. La frequenza $\lambda_{top\ event}$ soglia sarà quella che, in uno scenario temporale definito esclude credibilmente la possibilità del Top Event la cui frequenza è stabilita dall'Utente.
Lo schema è applicabile anche, quale strumento predittivo, per nuove Unità di processo.

Bibliografia

[1] IEC/CEI 61508, "Functional safety of Electric/Electronic/Programmable Electronic safety-related systems" - 1st Edition: 2000.
[2] IEC/CEI 61511, "Functional safety - Safety Instrumented Systems for the process industry sector" - 1st Edition: 2003.
[3] ISPESL, Circolare 48/2003, "Procedura tecnica per le verifiche di calcolo e controlli su componenti in pressione in regime di scorrimento viscose del materiale".
[4] G. Picciolo. A. Pievatolo, N. De Crecchio, "Safety Instrumented Systems (SIS) Proof test interval determination based on SIL validation in an petrochemical Facility", *CNIM*, Roma, 27-2-7-settembre 2007.

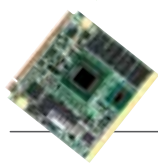
Si ringrazia Carmela Guarino di Bureau Veritas Italia per il prezioso supporto fornito.

SECO Italian Genie

SECOMExp-945
COM Express

SECOMX-945/M72
ETX/XTX


SECO104-CX700M
PC 104


QUADMO747
QSeven

Design & Manufacturing Made in Italy

SECO
Via Calamandrei, 91
52100 Arezzo - Italy
Tel. 0575 26979
info@seco.it
www.seco.it
readerservice.it n.23130