SAFEBOOK 1 – PROCESSO

PlantPAx
Process Automation System

Sicurezza funzionale nell'industria di processo

Principi, standard ed implementazione

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Sommario

Premessa

La norma IEC 61508 tratta la gestione della sicurezza dei sistemi elettrici, elettronici ed elettronici programmabili per tutta la loro vita utile, dalla progettazione alla messa fuori servizio ed associa i principi di sicurezza alla gestione dei sistemi e l'ingegnerizzazione della sicurezza al loro sviluppo.

Alla base vi è il principio che gli obiettivi di sicurezza dovrebbero essere impostati in fase di pianificazione della sicurezza e in base alla valutazione dei rischi, in modo tale che l'esecuzione rigorosa delle attività di gestione e dei processi permetta di raggiungere gli obiettivi indicati. Questo rende la norma basata su obiettivi anziché prescrittiva e significa che, in caso di problemi di sicurezza, la conformità con la norma non esonera gli utenti dalle loro responsabilità.

La norma può essere utilizzata sia come base per la preparazione di norme più specifiche sia in modo indipendente. La prima ipotesi è quella preferibile perché, nel secondo caso, è necessario che la norma venga adattata, compresa a fondo da parte della direzione e pianificata accuratamente in termini di introduzione ed uso.

Per molti, la norma si è rivelata di difficile comprensione. Nonostante ciò, ha già prodotto molti risultati. È stata e continuerà ad essere la base delle moderne norme di sicurezza e degli attuali quadri legislativi di riferimento; quindi, è fondamentale che tutti coloro con responsabilità in qualunque fase della vita di un sistema di sicurezza si impegnino a capirla a fondo.

Questo documento vuole essere un'introduzione alla sicurezza funzionale e una guida nell'applicazione della norma IEC 61511, l'implementazione specifica per l'industria di processo della norma IEC 61508. Anche se basata sulla IEC 61511, la norma americana ANSI/ISA-84.00.01 è sostanzialmente identica e, di conseguenza, questa guida si applica ad entrambe.

Scopo di questo documento è quello di fornire le informazioni necessarie ad una migliore comprensione delle norme e dei loro requisiti. Per spiegare i principi di base, i requisiti e le tecniche utilizzabili per rispondere a tali requisiti, il documento utilizza volutamente un linguaggio semplice e fa riferimento a progetti reali.

Esclusione di responsabilità

Anche se le tecniche qui presentate sono state efficacemente utilizzate per la dimostrazione della conformità nell'ambito di progetti reali, va osservato che la conformità, le tecniche utilizzate per dimostrarla e la raccolta delle evidenze rimangono di competenza del responsabile.

Le parentesi quadre [ ] indicano un riferimento incrociato ad una sezione di questo documento.

1. Introduzione a IEC 61511

1.1. Che cosa sono le norme IEC 61508 e IEC 61511?

La norma IEC 61508 è una norma internazionale, pubblicata dalla International Electrotechnical Commission (IEC), il cui principale obiettivo è quello di identificare gli aspetti da considerare quando, per l'esecuzione delle funzioni di sicurezza, vengono utilizzati sistemi elettrici, elettronici o elettronici programmabili (E/E/PE).

La norma IEC 61508 [19.1] è una norma generica applicabile a tutti i sistemi di sicurezza E/E/PE, a prescindere dall'uso o dall'applicazione. Il titolo della norma è:

> **IEC 61508:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. (CEI EN 61508:2011: Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza (testo in inglese)).**

La norma si basa sul principio che, nel momento in cui qualcosa non funzionasse a livello di processo o di apparecchiature, un processo può rappresentare un rischio per la sicurezza o l'ambiente. Di conseguenza, la norma mira a distinguere i problemi di processo ed i guasti di sistema da altri tipi di pericoli, quali inciampi e cadute, e permette di gestire la sicurezza di processo in modo sistematico e basato sui rischi.

La norma presuppone che, per ridurre quei rischi, debbano essere previste funzioni di sicurezza. Le funzioni di sicurezza possono formare, nel loro insieme, un sistema strumentato di sicurezza (SIS) la cui progettazione e il cui funzionamento devono essere basati sulla valutazione e sulla comprensione dei rischi presentati.

Un obiettivo secondario della norma IEC 61508 è quello di permettere lo sviluppo dei sistemi di sicurezza E/E/PE nelle applicazioni in cui non esistono norme di settore. Nell'industria di processo, questo ulteriore obiettivo è coperto dalla norma internazionale IEC 61511 [19.2]. Il titolo di questa norma è:

> **IEC 61511:2004 Functional Safety – Safety Instrumented Systems for the Process Industry Sector (CEI 61511:2007 Sicurezza funzionale – Sistemi strumentati di sicurezza per l'industria di processo).**

La norma IEC 61511 non identifica una struttura standard, ma è una norma che tratta la gestione della sicurezza per l'intera vita di un sistema, dalla progettazione alla messa fuori servizio. Fondamentale, per questo approccio, è il ciclo di vita globale della sicurezza che

descrive le attività correlate alla specifica, allo sviluppo, al funzionamento ed alla manutenzione di un sistema SIS.

1.2. Che cos'è la sicurezza funzionale?

IEC 61511-1, 3.2.25 fornisce la seguente definizione.

"La sicurezza funzionale è la parte della sicurezza globale relativa al processo ed al BPCS (sistema base del controllo di processo) che dipende dal corretto funzionamento del sistema SIS e di altri livelli di protezione."

Più semplicemente, la sicurezza funzionale si identifica con la riduzione dei rischi fornita dalle funzioni implementate per garantire il funzionamento sicuro del processo.

1.3. IEC (International Electrotechnical Commission)

La Commissione elettrotecnica internazionale, fondata nel 1906 ed inizialmente presieduta dallo scienziato britannico Lord Kelvin, ha sede a Ginevra, in Svizzera. La Commissione IEC redige e pubblica standard internazionali per l'elettrotecnologia ovvero tecnologie elettriche, elettroniche e correlate.

La Commissione IEC supporta le prestazioni di sicurezza ed ambientali dell'elettrotecnologia, promuove l'efficienza energetica e le fonti di energia rinnovabili e gestisce la valutazione della conformità di apparecchiature, sistemi o componenti alle sue norme internazionali.

La norma e tutte le altre pubblicazioni IEC sono protette e soggette a determinate condizioni di copyright ma possono essere acquistate o scaricate dal sito web IEC [http://www.iec.ch].

1.4. La struttura della norma

La norma è suddivisa in tre parti, come illustrato nella Figura 1.

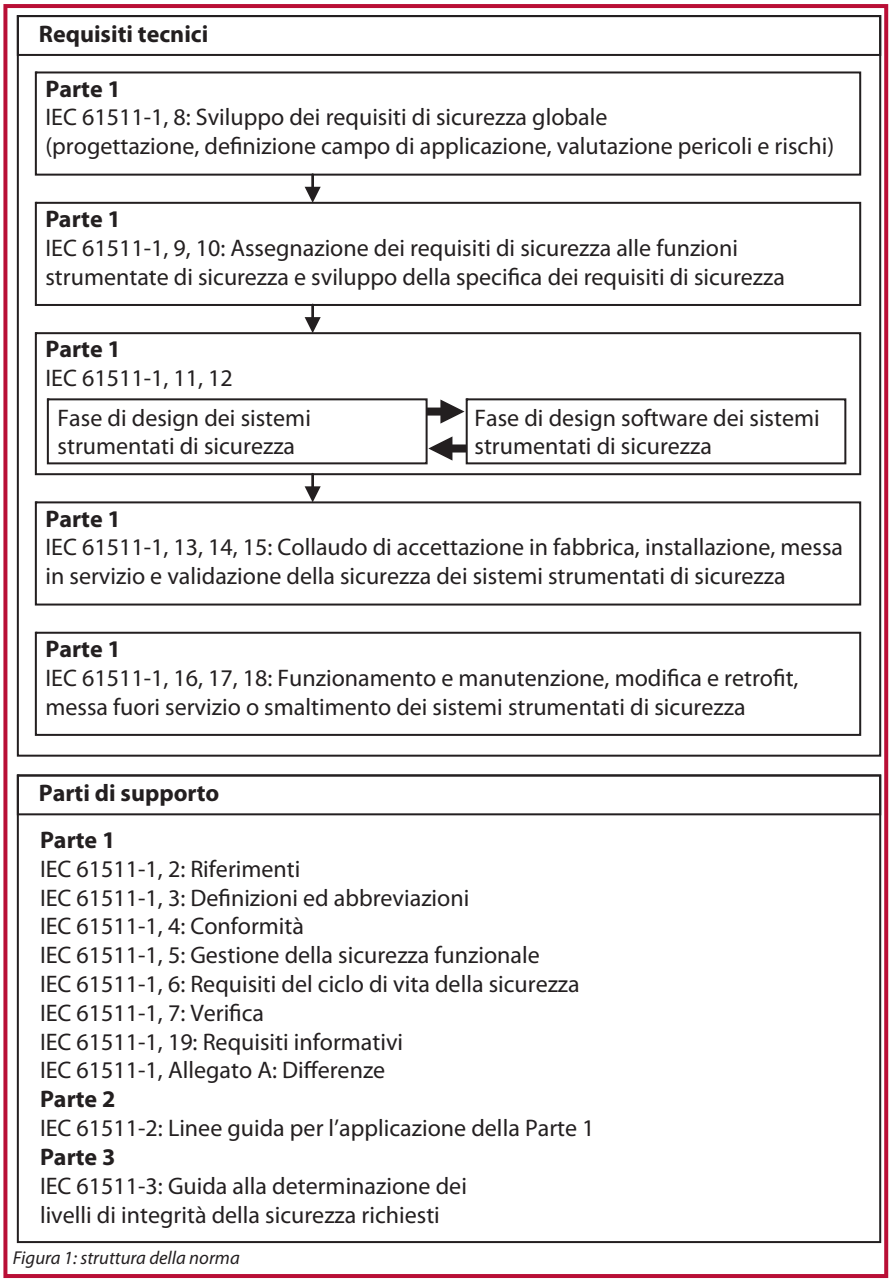


Figura 1: struttura della norma

La Parte 1 delinea i requisiti per la conformità. Pianificazione del progetto, gestione, documentazione e requisiti di competenza, oltre che definizione dei requisiti tecnici per ottenere la sicurezza per tutto il ciclo di vita della sicurezza.

In linea generale, la Parte 1 è "normativa" in quanto definisce specifici requisiti per la conformità ed è strutturata in modo coerente per consentire di dimostrare la conformità punto per punto.

La Parte 2 guida all'utilizzo della Parte 1.

La Parte 3 fornisce una serie di esempi pratici di valutazione dei rischi per l'assegnazione dei livelli di integrità della sicurezza [4].

Le Parti 2 e 3 sono "informative" e rappresentano una guida ai requisiti normativi.

1.5. Conformità con la norma IEC 61511

1.5.1. Requisiti dell'Health and Safety at Work Act etc. 1974

L'Health and Safety at Work Act etc. 1974 (HASAW o HSW) è la principale legislazione su salute e sicurezza sul lavoro nel Regno Unito. La Health and Safety Executive (HSE) è responsabile dell'applicazione di questa e di altre leggi e regolamentazioni riguardanti l'ambiente di lavoro.

Nota: in vari paesi del mondo sono in vigore leggi o norme analoghe allo Health and Safety at Work Act etc. 1974 del Regno Unito, citato nel testo come standard di riferimento. Le affermazioni relative alla norma suddetta presenti nel testo implicano sempre il rispetto anche delle eventuali norme e regolamenti vigenti nei singoli paesi presi in considerazione.

Il testo integrale della legge può essere richiesto all'Office of Public Sector Information (OPSI) o scaricato gratuitamente. Gli utenti devono comunque controllare la validità del testo. I documenti stampati e on-line potrebbero non essere aggiornati ed è quindi consigliabile richiedere una consulenza legale indipendente o consultare HSE Infoline, [http://www.hse.gov.uk/contact/index.htm].

In termini semplici, l'Health and Safety at Work Act stabilisce che, per quanto ragionevolmente fattibile, ogni datore di lavoro è tenuto a garantire la salute, la sicurezza ed il benessere sul lavoro di tutti i suoi dipendenti. Ciò implica la fornitura e la manutenzione di impianti e sistemi di lavoro che siano, per quanto ragionevolmente fattibile, sicuri e senza rischi per la salute.

Ogni datore di lavoro, inoltre, è tenuto a gestire la sua impresa in modo da garantire che, per quanto ragionevolmente fattibile, anche le persone non direttamente dipendenti non siano esposte a rischi per la loro salute o sicurezza.

1.5.2. Requisiti per la conformità

La norma IEC 61511 stabilisce che, per attestare la conformità, occorre dimostrare che i requisiti della norma sono stati soddisfatti in base ai criteri richiesti e che, per ogni punto o sottopunto, sono stati raggiunti tutti gli obiettivi.

In pratica, è generalmente difficile dimostrare la piena conformità ad ogni punto e clausola subordinata della norma ed è necessaria un'attenta valutazione per determinare il grado di rigore da applicare per soddisfare i requisiti. Generalmente, il grado di rigore richiesto dipende da una serie di fattori:

- la natura dei pericoli;
- la gravità delle conseguenze;
- la riduzione dei rischi necessaria;
- la fase del ciclo di vita applicabile;
- la tecnologia interessata;
- la novità del progetto.

In altre parole, è necessario prendere una decisione basata sui rischi. In mancanza di esperienza, il coinvolgimento di soggetti esterni può conferire maggiore credibilità all'attestazione di conformità.

1.5.3. Conseguenze della non conformità

La norma non è legge e quindi, che ci si conformi o meno ai suoi requisiti, bisogna essere consapevoli delle conseguenze della non conformità. Datori di lavoro, responsabili o titolari del rischio hanno l'obbligo, in base all'Health and Safety at Work Act, di gestire il rischio sul proprio posto di lavoro.

La norma fornisce un approccio sistematico alla gestione di tutte le attività del ciclo di vita della sicurezza relativamente ai sistemi utilizzati per eseguire le funzioni di sicurezza e, di conseguenza, è una buona fonte di informazioni e tecniche. In caso di problemi che comportino lesioni o malattia, il mancato utilizzo delle migliori informazioni disponibili per la gestione di un certo rischio espone i responsabili ad indagine ed azione penale, come previsto dall'Health and Safety at Work Act.

In caso di problemi, le informazioni raccolte e l'analisi fornita per la conformità ai requisiti della norma IEC 61511 diventano, di fatto, un importante strumento di difesa in giudizio.

1.5.4. Requisiti per la conformità in un impianto nuovo

Qualunque sia la parte del ciclo di vita della sicurezza in cui siete coinvolti, è ragionevole aspettarsi che utilizziate le migliori informazioni disponibili per assicurare che i rischi associati al vostro impianto siano gestiti ad un livello tollerabile. Potendosi sostenere che le migliori informazioni disponibili derivano dalla IEC 61511, in caso di problemi, il mancato rispetto di questa norma potrebbe essere interpretato come negligenza.

1.5.5. Requisiti per la conformità in un impianto esistente

Diversi impianti sono stati progettati e costruiti prima della pubblicazione formale della norma IEC 61511. Questo fatto non modifica però le vostre responsabilità e, se siete coinvolti in una qualunque parte del ciclo di vita della sicurezza di un vecchio impianto (funzionamento, manutenzione ecc.), i vostri obblighi nell'ambito dell'Health and Safety at Work Act permangono ed i rischi dovrebbero essere gestiti di conseguenza. La norma quindi si applica anche ai vecchi impianti.

La norma ANSI/ISA-84 tratta specificamente i sistemi precedenti, stabilendo che per un sistema SIS esistente, progettato e costruito secondo i codici, le norme e le pratiche applicabili prima dell'emissione della norma, il proprietario/operatore deve determinare se le apparecchiature sono progettate, manutenute, ispezionate, collaudate ed utilizzate in modo sicuro. In pratica, è necessario verificare che i sistemi esistenti siano sicuri facendo ricorso ai migliori metodi disponibili.

È possibile che riteniate di dover risalire alle prime fasi del ciclo di vita della sicurezza dell'impianto esistente e riesaminare lo studio HAZOP o condurne uno nuovo partendo da zero. Analizzando il processo fino la sua conclusione, potete identificare i rischi non protetti dalle funzioni di sicurezza esistenti e la gestione di quei rischi sarà vostra responsabilità.

Molto probabilmente, non sarà economicamente conveniente sviluppare nuove funzioni strumentate di sicurezza (SIF) per un impianto che ha già 20 anni di vita. Tuttavia, se l'impianto ha funzionato in sicurezza per un ragionevole periodo di tempo, i rischi che identificate e la loro frequenza, considerando le protezioni esistenti, possono già essere considerati tollerabili.

Il vostro obbligo è almeno quello di documentare il processo, per assicurare che tutti i pericoli siano stati identificati, i rischi valutati e che l'efficacia delle funzioni di protezione o delle protezioni attualmente esistenti sia stata dimostrata. In una situazione di questo genere, è possibile valutare a posteriori e utilizzare i dati storici per quantificare la frequenza dei pericoli con maggiore precisione, diversamente da quanto accadrebbe se si trattasse di una installazione nuova. Attraverso l'analisi, dovreste quindi essere in grado di dimostrare che i rischi che avete identificato sono tollerabili.

Invece, nel caso peggiore in cui sussistano pericoli non protetti o fosse necessario adottare qualche misura aggiuntiva di riduzione dei rischi, è necessario esserne consapevoli ed agire di conseguenza.

1.5.6. Motivi della conformità alla norma IEC 61511

A parte l'obbligo legale implicito nell'Health and Safety at Work Act, possono esserci altre ragioni per conformarsi alla norma:

- requisiti contrattuali;
- ottimizzazione dell'architettura;
- possibili vantaggi commerciali.

Si potrebbe sostenere che il primo dovere di un'impresa è quello di sopravvivere ed il suo obiettivo non dovrebbe essere massimizzare il profitto ma evitare le perdite. Su questa base, dovete chiedere a voi stessi se volete imparare dagli errori degli altri o sbagliare da soli.

1.6. Applicazione della norma IEC 61511

La sicurezza funzionale può essere applicata solo a funzioni complete che, generalmente, consistono in un sensore, un computer o PLC ed un dispositivo azionato. Non ha senso applicare questo concetto a parti di apparecchiatura quali sensori o computer.

Quindi, quando un costruttore attesta che il proprio prodotto è un sensore di pressione SIL2 o un PLC SIL3, ciò significa in realtà che il sensore di pressione può essere utilizzato in una funzione di sicurezza SIL2 o che il PLC può essere usato in una funzione di sicurezza SIL3.

Il costruttore dovrebbe qualificare l'attestazione con avvertenze e restrizioni sull'utilizzo (ad es. i requisiti per la tolleranza ai guasti [13.3.1] o le prove funzionali [12.8]) per ottenere il SIL dichiarato.

Le attestazioni del costruttore possono anche essere supportate da un Certificato SIL rilasciato da un organismo di valutazione indipendente, ma ciò non significa che la funzione di sicurezza predefinita sarà conforme SIL. Il certificato SIL non sostituisce la dimostrazione della conformità ed il responsabile non può usare tali attestazioni per scaricare le responsabilità a lui assegnate dall'Health and Safety at Work Act.

1.7. Devo conformarmi alla norma?

1.7.1. Nuova costruzione

Come già detto, esiste un obbligo legale implicito di conformità alla norma. Ciò significa che la norma non è legge, ma che la legge richiede al responsabile o al detentore del rischio di gestire il rischio ad un livello accettabile. La norma fornisce un approccio sistematico per raggiungere questo obiettivo e, se qualcosa non funziona e qualcuno si ferisce, il mancato uso delle migliori informazioni disponibili potrebbe essere considerato segno di negligenza e tradursi in un'azione giudiziaria.

1.7.2. Impianto esistente

L'Health and Safety at Work Act si applica anche agli impianti esistenti i cui rischi, quindi, dovrebbero essere identificati e gestiti adeguatamente [1.5.5]. La norma IEC 61511 fornisce anche un modello applicabile alla gestione dei rischi negli impianti progettati ed utilizzati prima della pubblicazione della norma.

2. Ciclo di vita globale della sicurezza

2.1. Ciclo di vita della sicurezza

Il ciclo di vita della sicurezza integra tutte le attività necessarie, dalla specifica allo sviluppo e dal funzionamento alla manutenzione del sistema SIS. A seconda del campo di applicazione delle attività, è possibile che siate coinvolti solo in alcune delle fasi (ad es. funzionamento e manutenzione) ma dovreste essere consapevoli dell'approccio all'intero ciclo di vita.

Il ciclo di vita della sicurezza è presentato nella Figura 2.

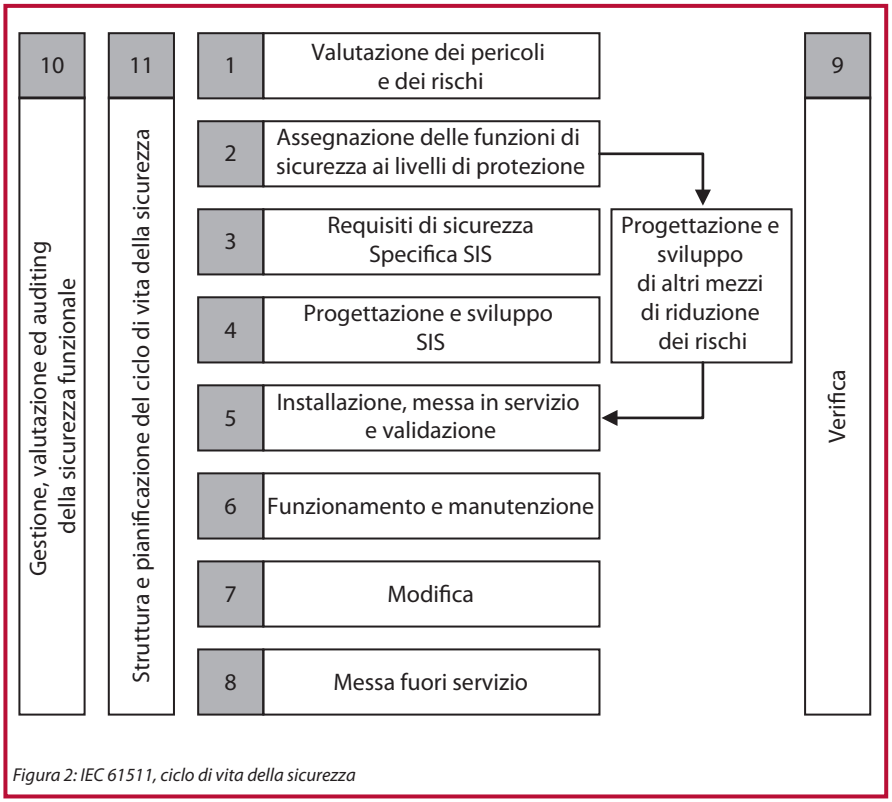


Figura 2: IEC 61511, ciclo di vita della sicurezza

2.2. Fasi del ciclo di vita

La Fase 1 definisce il campo di applicazione tenendo conto dell'ambito fisico, sociale e politico ed affronta le implicazioni di sicurezza in termini di pericoli e di percezione del rischio. Ciò è fondamentale per capire i pericoli ed i rischi presentati dal processo.

Una volta determinata la necessaria riduzione dei rischi, i mezzi per ottenerla vengono specificati durante la Fase 2 (assegnazione) e la Fase 3 (requisiti di sicurezza globale).

Nella Fase 4, i requisiti di sicurezza globale si traducono in funzioni di sicurezza. A questo punto, vengono esaminate l'ottimizzazione delle funzioni, la separazione ed altre questioni di progetto quali le procedure di collaudo, mentre la pianificazione di queste attività viene affrontata nell'ambito della Fase 11.

Le Fasi da 5 a 10 dimostrano che la norma non si limita allo sviluppo dei sistemi ma che tratta la gestione della sicurezza funzionale per tutta la vita di servizio di un sistema.

Molti dei requisiti nella norma sono di natura tecnica ma l'approccio in termini di ciclo di vita conferisce uguale importanza all'efficacia delle attività di gestione (ad es. pianificazione, documentazione, funzionamento, manutenzione e modifica) che devono quindi essere considerate in tutte le fasi. Le attività di documentazione, gestione e valutazione sono parallele ed applicabili a tutte le fasi del ciclo di vita ed alle attività illustrate nella Figura 2.

2.3. Requisiti di conformità

Dato che la norma non è prescrittiva, il percorso per il raggiungimento della conformità non è mai diretto ed univoco. Quanto fate per ottenere la conformità è una scelta personale, ma dovreste arrivare alla conclusione di aver agito in modo corretto. Per essere sicuri di aver considerato tutto ciò che sarebbe ragionevole aspettarsi da voi, è consigliabile adottare un approccio che consideri la norma punto per punto. In altre parole, un approccio rigoroso.

La conformità alla norma richiede che voi dimostriate con evidenze di aver adottato un approccio sistematico per gestire il rischio e che quell'approccio sia stato applicato alle pertinenti parti del ciclo di vita. Tale approccio sistematico è fornito dalla norma e basato sul ciclo di vita della sicurezza.

La conformità alla norma richiede la comprensione del ciclo di vita, oltre che la realizzazione e la documentazione delle attività specificate. Seguire il ciclo di vita non è una semplice pratica che può limitarsi alla generazione di rapporti, documenti e caselle da vistare. La conformità richiede che le attività vengano realizzate in modo efficace e che le informazioni raccolte in ogni fase permettano di realizzare le fasi successive.

Raramente è applicabile una valutazione parziale delle attività e si raccomanda di considerare tutte le fasi del ciclo di vita. Per un operatore, ad esempio, una modifica nella fase di funzionamento e manutenzione può richiedere la riconsiderazione di decisioni e valutazioni (ad es. HAZOP ed analisi dei rischi) effettuate in fasi precedenti del ciclo di vita.

2.4. Ciclo di vita della sicurezza – Fasi 1 e 2

Ogni fase del ciclo di vita descrive un'attività ed ogni attività richiede delle informazioni come input. Ogni fase consiste in un'attività, che dovrebbe avere procedure documentate, che genera informazioni come output per le fasi successive.

La Figura 3 mostra le attività ed i requisiti informativi per la Fase 1 (Valutazione dei pericoli e dei rischi) e per la Fase 2 (Assegnazione dei requisiti di sicurezza). Lo schema elenca le informazioni richieste come input (I/P) all'attività e quelle generate dall'attività come output per la fase successiva.

Va osservato che, sebbene la norma descriva le fasi del ciclo di vita ed i requisiti informativi di ogni fase, in pratica alcune delle fasi ed i relativi documenti possono essere combinati, se opportuno. Chiarezza e semplicità sono importanti, le attività dovrebbero essere eseguite nel modo più efficace e le informazioni presentate nel modo più chiaro.

L'output della Fase 3 consiste generalmente in uno studio HAZOP e nell'analisi dei rischi, per identificare i requisiti delle funzioni di sicurezza ed i target di riduzione dei rischi.

La Fase 4 tratta l'assegnazione delle funzioni di sicurezza in base ai requisiti di sicurezza identificati nella fase precedente. L'assegnazione dei requisiti di sicurezza consiste nel considerare ogni requisito di sicurezza e nello stabilire le funzioni strumentate di sicurezza. Si tratta di un processo iterativo che prende in considerazione il processo ed altre eventuali misure di riduzione dei rischi per rispondere ai requisiti di integrità della sicurezza globale.

Quando inizia l'assegnazione delle funzioni di sicurezza, è importante che siano pianificate anche le fasi successive, tra cui installazione, messa in servizio e validazione, funzionamento e manutenzione (vedere anche la Figura 5).

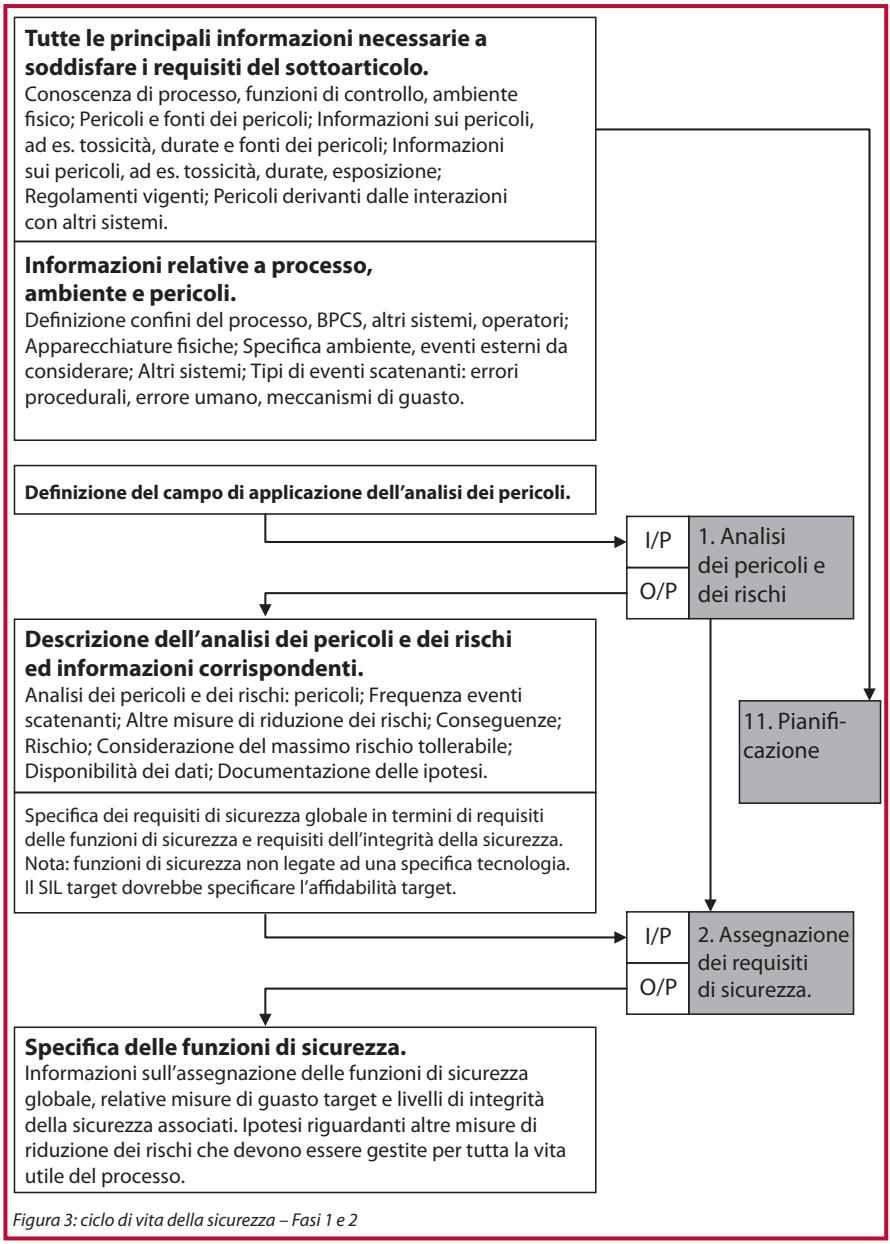


Figura 3: ciclo di vita della sicurezza – Fasi 1 e 2

Ciclo di vita della sicurezza globale

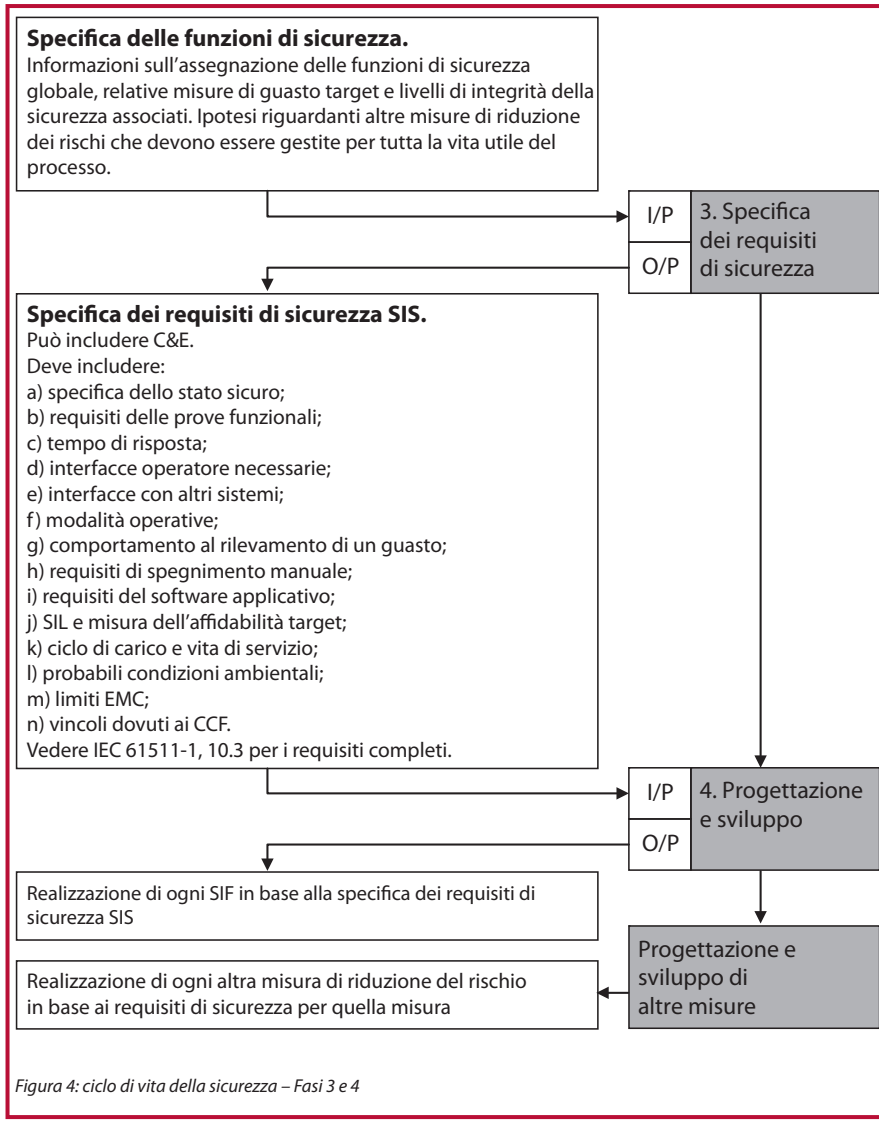


Figura 4: ciclo di vita della sicurezza – Fasi 3 e 4

2.5. Ciclo di vita della sicurezza – Fasi 3 e 4

La Fase 3 si occupa della specifica dei requisiti di sicurezza (SRS) che permette di avviare la fase di progettazione e sviluppo (Fase 4), Figura 4.

È possibile che la vostra organizzazione abbia già un elenco delle voci da includere nella specifica di progettazione. Ciò garantirà la generazione di una specifica completa e comprensiva per ogni progetto e contribuirà a minimizzare i problemi della funzione di sicurezza dovuti ad errori di specifica.

La Fase 4 può essere adeguatamente espletata con una specifica funzionale (FDS) o un simile documento che stabilisca lo scenario, definisca il processo e le considerazioni ambientali ed operative e stabilisca il campo di applicazione delle fasi successive.

2.6. Ciclo di vita della sicurezza – Fasi 5 e 6

Le Fasi 5 e 6 identificano i requisiti per l'installazione, la messa in servizio, la validazione, il funzionamento e la manutenzione del sistema SIS, Figura 5.

2.7. Ciclo di vita della sicurezza – Fasi 7 e 8

Input, output ed attività associate alla Fase 7 – Modifica sono essenzialmente uguali a quelle per la Fase 8 – Messa fuori servizio. In effetti, la messa fuori servizio è una modifica che avviene alla fine del ciclo di vita, iniziata con gli stessi controlli e gestita con le stesse protezioni, Figura 6.

Ciclo di vita della sicurezza globale

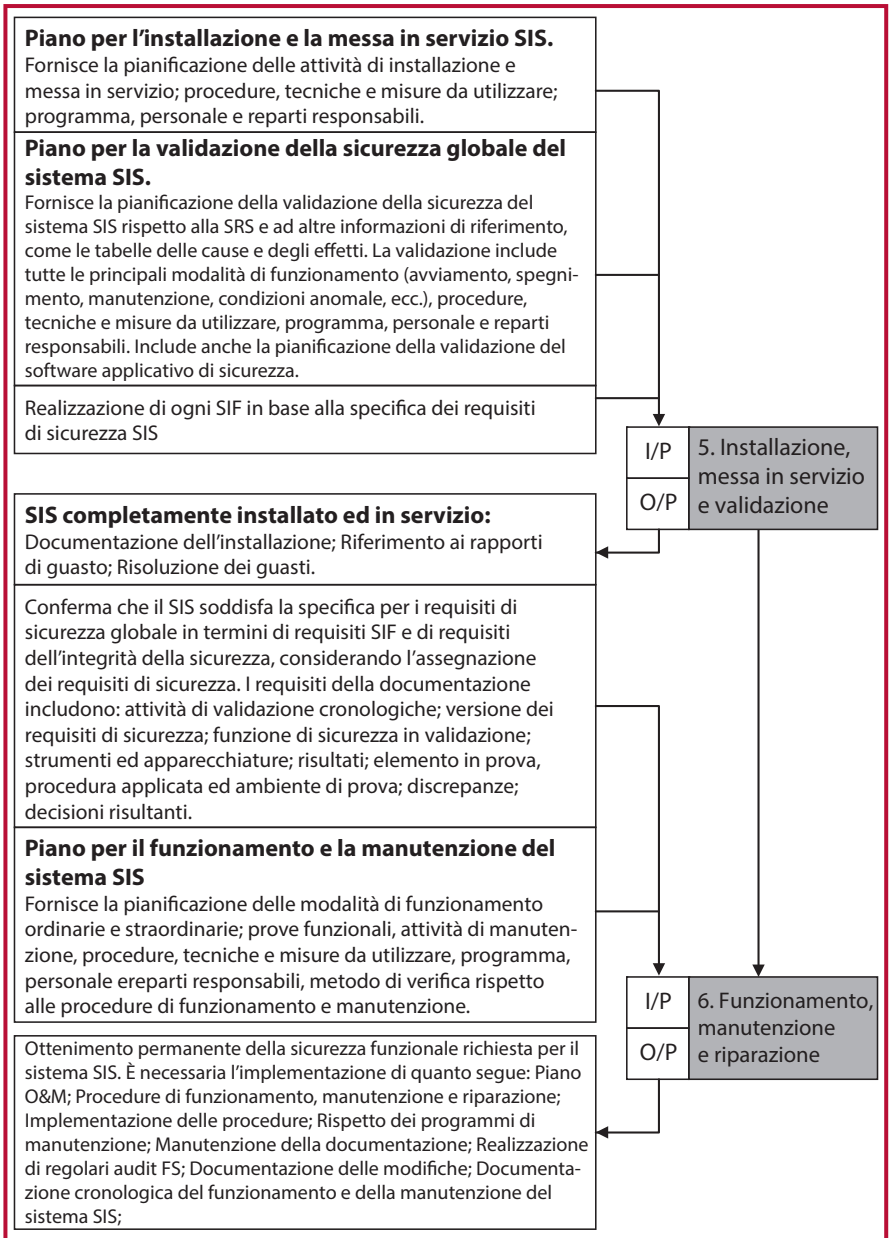


Figura 5: ciclo di vita della sicurezza – Fasi 5 e 6

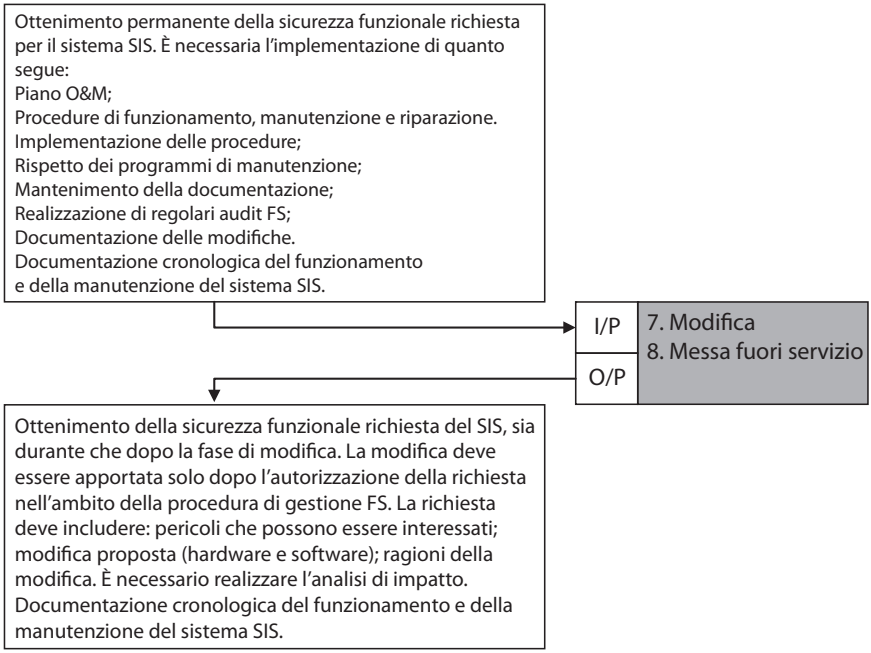


Figura 6: ciclo di vita della sicurezza – Fasi 7 e 8

3. Pericoli ed identificazione dei pericoli

3.1. Fasi del ciclo di vita

La Figura 7 mostra la fase del ciclo di vita in questione.

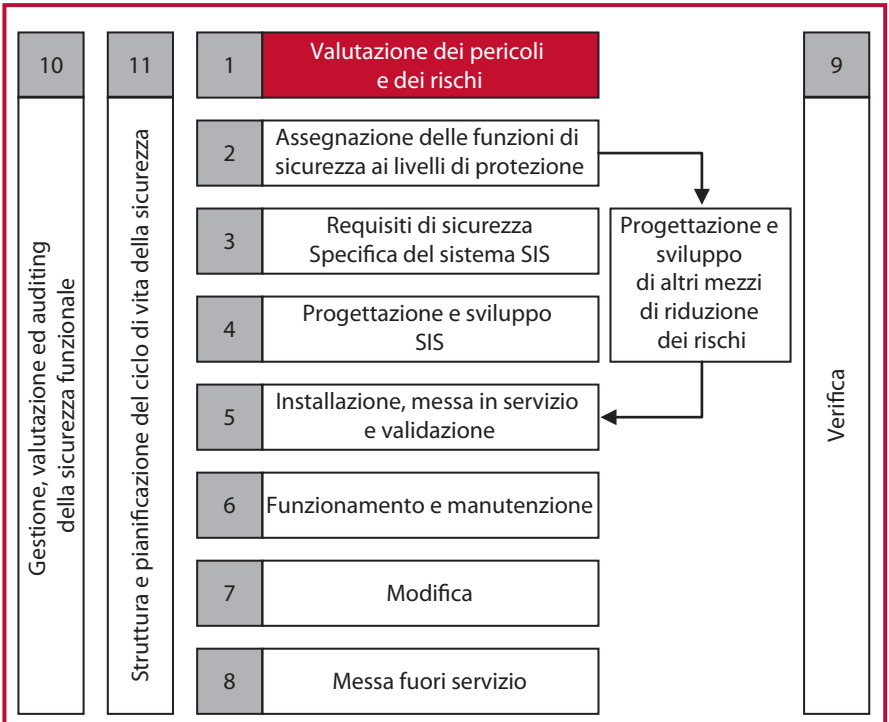


Figura 7: ciclo di vita – Fase 1

L'obiettivo di questa fase, come definito nella norma IEC 61511-1, 8.1, è quello di determinare:

- Pericoli/eventi pericolosi del processo e delle apparecchiature associate, la sequenza di eventi che conduce al pericolo ed i rischi del processo coinvolti [3.2 – 3.7];
- Requisiti per la riduzione dei rischi [5 e 6];
- Funzioni di sicurezza necessarie alla riduzione dei rischi [7 e 8].

3.2. Pericoli

Il significato della parola "pericolo" può non essere univocamente inteso. Spesso i dizionari non forniscono definizioni specifiche di questo termine oppure lo combinano con la parola "rischio" (ad esempio, "un pericolo o rischio") e ciò fa capire perché tante persone usino questi termini in modo intercambiabile.

Nel contesto della sicurezza funzionale, i pericoli sono eventi che possono procurare lesioni alle persone e danni all'ambiente o all'attività.

In casa, i possibili esempi di pericoli includono:

- vetri rotti perché potrebbero provocare tagli;
- pozze d'acqua perché potrebbero provocare scivolamenti e cadute;
- troppe spine in una presa elettrica perché potrebbero sovraccaricarla e provocare un incendio.

Sul lavoro, i possibili esempi di pericoli potrebbero includere:

- rumore eccessivo perché potrebbe provocare perdita dell'udito;
- inspirazione di polvere di amianto perché potrebbe provocare il cancro.

Nell'industria di processo, i pericoli potrebbero essere i seguenti.

- Il livello del liquido in un serbatoio: un livello elevato potrebbe comportare il riversamento di liquido nei flussi di gas o il traboccamento di un prodotto chimico pericoloso o di un liquido infiammabile; un livello basso può comportare il funzionamento a secco delle pompe o il trafilamento di gas nei serbatoi a valle.
- La pressione del liquido in un serbatoio: una pressione elevata può comportare perdita di contenimento, perdite o rottura del serbatoio.

Nella valutazione dei rischi, il primo passo è quello di identificare i pericoli. Per identificare i pericoli, vengono utilizzate diverse tecniche ma quella più comune è lo studio dei pericoli e dell'operabilità (HAZOP).

3.3. Uso degli studi HAZOP nell'industria

Gli studi HAZOP sono stati originariamente sviluppati nel Regno Unito dalla ICI, in seguito al disastro di Flixborough del 1974 e, successivamente, hanno cominciato ad essere ampiamente utilizzati nell'industria di processo.

Sabato 1 giugno 1974, lo stabilimento Nypro di Flixborough (Regno Unito) è stato gravemente danneggiato da una grande esplosione che ha ucciso 28 lavoratori e ne ha feriti altri 36. Tutti hanno ammesso che il numero di vittime sarebbe stato più alto se

l'incidente fosse avvenuto in un giorno feriale, quando sarebbe stato occupato anche il principale blocco di uffici. È stata coinvolta anche l'area attorno allo stabilimento, con 53 persone che hanno subito lesioni e danneggiamento delle proprietà circostanti.

I 18 decessi nella sala di controllo sono stati causati dalla rottura delle finestre e dal cedimento del tetto. Nessuno si è salvato. Gli incendi hanno continuato a divampare per diversi giorni ed ostacolato le operazioni di soccorso per i successivi dieci giorni.

Dall'industria chimica, attraverso lo scambio generale di idee e personale, gli studi HAZOP sono stati poi adottati anche dall'industria petrolifera che ha un potenziale molto simile di gravi disastri. Successivamente, sono diventati patrimonio del settore alimentare e idrico, dove il potenziale di pericolo è lo stesso ma più legato a problemi di contaminazione anziché ad esplosioni o al rilascio di prodotti chimici.

3.4. Ragioni per usare gli studi HAZOP

Anche se la progettazione dell'impianto si basa sull'applicazione di codici e norme, il processo HAZOP rappresenta un complemento attraverso cui è possibile immaginare in anticipo le deviazioni che possono verificarsi a causa, ad esempio, di condizioni o problemi del processo, malfunzionamento delle apparecchiature o errore degli operatori.

Anche le pressioni derivanti da tempi di progetto spesso molto stretti possono essere causa di errori e omissioni che l'analisi HAZOP permette di correggere prima che le modifiche diventino troppo costose. Essendo facili da capire e da adattare a qualunque processo o attività, gli studi HAZOP sono diventati la metodologia di identificazione dei pericoli più ampiamente utilizzata.

3.5. Deviazione dall'obiettivo progettuale

Tutti i processi, le apparecchiature sotto controllo o gli impianti industriali hanno un obiettivo progettuale. Questo potrebbe far riferimento ad una capacità di produzione target, in termini di tonnellaggio annuale di un particolare prodotto chimico o di un determinato numero di articoli fabbricati.

Tuttavia, un importante obiettivo progettuale secondario può essere quello di far funzionare il processo in modo sicuro ed efficiente e, per farlo, ogni apparecchiatura deve funzionare efficacemente. È questo aspetto che potrebbe essere considerato l'obiettivo progettuale di ogni particolare componente dell'apparecchiatura.

Ad esempio, nell'ambito dei requisiti di produzione del nostro impianto, potremmo aver bisogno di un impianto per l'acqua di raffreddamento costituito da un circuito dell'acqua di raffreddamento con pompa di circolazione e scambiatore di calore, come illustrato nella Figura 8.

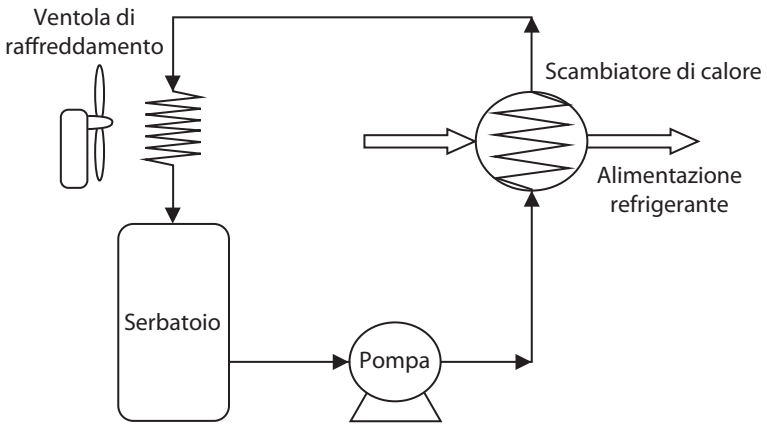


Figura 8: obiettivo progettuale

L'obiettivo progettuale di questa piccola sezione dell'impianto potrebbe essere quello di far circolare costantemente l'acqua di raffreddamento ad una temperatura di x ºC e ad una portata di xxx litri all'ora. È generalmente a questo livello secondario di obiettivo progettuale che si rivolge uno studio HAZOP. L'uso della parola "deviazione" ora diventa più facile da capire. Una deviazione (scostamento) dall'obiettivo progettuale, nel caso della nostra struttura di raffreddamento, sarebbe rappresentata da una riduzione del flusso circolante o da un aumento della temperatura dell'acqua.

La differenza tra una deviazione e la sua causa è un concetto da chiarire. Nel caso che precede, la rottura della pompa sarebbe una causa, non una deviazione.

In questo esempio, un aumento della temperatura dell'acqua sarebbe il pericolo perché potrebbe provocare lesioni alle persone e danni all'ambiente o all'attività.

3.6. Tecnica HAZOP

Gli studi HAZOP vengono utilizzati per identificare i pericoli potenziali ed i problemi di operabilità causati dalle deviazioni dall'obiettivo progettuale negli impianti di processo nuovi o già esistenti e vengono generalmente realizzati periodicamente per tutta la vita dell'impianto. Naturalmente, già in fase di progettazione, dovrebbe essere realizzata un'analisi HAZOP iniziale o preliminare. Il processo dovrebbe poi essere esaminato man mano che lo sviluppo avanza ed ogni volta che vengono proposte modifiche importanti, oltre che alla fine della fase di sviluppo, per garantire che non sussistano rischi residui prima della fase di costruzione.

L'analisi HAZOP viene condotta, in un incontro tra le parti interessate, da persone in possesso dei livelli adeguati di conoscenza ed esperienza del funzionamento e della manutenzione dell'impianto. L'incontro è una sessione di brainstorming strutturata in cui viene utilizzata una serie di parole chiave per stimolare idee sui possibili pericoli. Le discussioni e le informazioni su pericoli potenziali, cause e conseguenze vengono registrate su appositi verbali.

3.6.1. Team dello studio HAZOP

È importante che il team HAZOP sia costituito da persone in grado di apportare allo studio il massimo contributo in termini di conoscenza ed esperienza del tipo di impianto da considerare. Un tipico team HAZOP è costituito come segue:

Nome	**Ruolo**
Presidente	Persona che ha la responsabilità di spiegare il processo HAZOP, dirigere le discussioni e facilitare l'analisi HAZOP. Qualcuno con esperienza nel processo HAZOP ma non direttamente coinvolto nel progetto, per assicurare che il metodo venga seguito attentamente.
Segretario	Persona che ha la responsabilità di registrare la discussione dell'incontro HAZOP in modo tangibile. Responsabile della registrazione di raccomandazioni o azioni.
Ingegnere di processo	Generalmente l'ingegnere responsabile del diagramma di flusso del processo e dello sviluppo degli schemi dell'impianto e della strumentazione (P&ID).
Utente/Operatore	Persona esperta sull'uso e l'operabilità del processo, oltre che sull'effetto delle deviazioni.
Specialista C&I	Persona in possesso delle corrispondenti conoscenze tecniche di controllo e strumentazione.
Manutentore	Persona coinvolta nella manutenzione del processo.
Rappresentante del team di progettazione	Persona esperta sulla progettazione in grado di fornire informazioni specifiche.

3.6.2. Informazioni utilizzate nello studio HAZOP

Il team HAZOP dovrebbe disporre dei seguenti elementi:

- Schemi dell'impianto e della strumentazione (P&ID);
- Documenti di descrizione o concezione del processo;
- Procedure operative e di manutenzione;
- Diagrammi cause ed effetti (C&E);
- Layout dell'impianto.

3.6.3. La procedura HAZOP

La procedura HAZOP implica una completa descrizione del processo ed una sistematica analisi di ogni sua parte, per stabilire in che modo le deviazioni dall'obiettivo progettuale possono incidere negativamente sul funzionamento sicuro ed efficiente dell'impianto.

La procedura deve essere applicata dal team HAZOP in modo strutturato e basarsi su un'identificazione preventiva dei pericoli plausibili.

Molti dei pericoli saranno ovvi (ad es. un aumento della temperatura), ma il merito di questa tecnica risiede nella capacità di scoprire pericoli meno ovvi, per quanto improbabili possano sembrare ad una prima analisi.

3.6.4. Parole chiave

Per focalizzare l'attenzione del team sulle deviazioni dall'obiettivo progettuale e sulle cause e conseguenze possibili, il processo HAZOP ricorre all'utilizzo di parole chiave. Queste parole chiave sono divise in due sottogruppi:

- Parole chiave primarie che richiamano l'attenzione su un particolare aspetto dell'obiettivo progettuale o su parametri o condizioni di processo associati (flusso, temperatura, pressione, livello, ecc.);
- Parole chiave secondarie che, quando combinate ad una parola chiave primaria, suggeriscono possibili deviazioni (maggiore temperatura, livello inferiore, nessuna pressione, inversione di flusso, ecc.).

L'intera tecnica dipende dall'uso efficace di queste parole chiave che, di conseguenza, devono essere perfettamente comprese dal team, sia in termini di significato sia di modalità di utilizzo.

Va osservato che l'uso delle parole chiave serve semplicemente a stimolare l'immaginazione su ciò che potrebbe accadere. Non tutte le parole chiave saranno pertinenti e non tutti i pericoli saranno credibili. Se identifica eventi senza significato o incredibili, il team dovrebbe registrarli come tali e non perdere altro tempo ad approfondirli.

3.6.5. Modalità operative

Dato che una procedura HAZOP è uno studio dei pericoli e dell'operabilità, è importante considerare non solo il normale funzionamento del processo ma anche le anomalie di altre modalità, quali avviamento, spegnimento, riempimento, svuotamento, bypass e prova funzionale.

Ciò può avvenire considerando separatamente ogni modalità operativa specificata nell'oggetto ed eseguendo un'analisi HAZOP per ognuna di loro. In alternativa, per sistemi relativamente semplici, è possibile aggiungere una colonna nei fogli di lavoro per identificare la modalità. Con una singola analisi HAZOP, è quindi possibile considerare tutte le modalità operative.

3.6.6. Registrazione dello studio HAZOP

È disponibile una serie di strumenti software in grado di guidare attraverso il processo HAZOP. In alternativa, per registrare le discussioni ed i risultati, può essere utilizzato un semplice foglio di calcolo elettronico. I fogli di calcolo elettronico permettono facili operazioni di ordinamento e categorizzazione e forniscono la visibilità e la tracciabilità dei dati necessarie al riferimento incrociato con altre analisi.

Ogni evento ed ogni combinazione di parole chiave dovrebbero essere registrati. Dove applicabile, può essere aggiunto il commento: Nessuna causa plausibile, Nessuna conseguenza o Nessun pericolo. Questa è considerata una registrazione completa e porta alla generazione di un rapporto HAZOP che dimostra l'esecuzione di uno studio completo e rigoroso. Ciò sarà utilissimo nella valutazione della sicurezza e dell'operabilità delle successive modifiche dell'impianto.

Oltre a quanto sopra, vengono spesso utilizzate le parole secondarie "Tutto" e "Rimanente". Ad esempio, alcune combinazioni di parole chiave primarie possono essere identificate come aventi cause plausibili (ad es. Flusso/Nessuno, Flusso/Inversione). Per altre combinazioni (Flusso/Inferiore, Flusso/Superiore, Flusso/Altro) per cui non possono essere identificate cause plausibili, può essere utilizzata la combinazione "Flusso/Rimanente".

3.6.7. Identificazione dei pericoli – Intestazione dei fogli di lavoro HAZOP

La tabella che segue presenta un esempio di foglio di lavoro HAZOP per una camera di decompressione. Va sottolineato che si tratta di un esempio puramente rappresentativo e non destinato ad illustrare un sistema effettivo.

Riferimento

È sempre opportuno includere una colonna di riferimento in modo da poter fare riferimenti incrociati con altre analisi e mantenere la tracciabilità per analisi successive, ad es. LOPA [8].

Parole chiave

È opportuno utilizzare parole chiave primarie e secondarie. Su Internet, è possibile reperire vari elenchi di parole chiave applicabili ad attività e settori industriali differenti.

Deviazione

La deviazione è lo scostamento dall'obiettivo progettuale determinato attraverso le parole chiave primarie e secondarie e rappresenta il pericolo identificato.

Causa

Si tratta delle cause potenziali alla base della deviazione. Sulla causa, è importante includere informazioni specifiche. Ad esempio, se consideriamo un aumento della concentrazione di ossigeno dovuta alla rottura di un sensore di O_2, bisogna tener presente che il sensore può rompersi in diversi modi ma che solo una falsa lettura di bassa concentrazione di O_2 comporta una condizione pericolosa.

Conseguenza

Le conseguenze derivanti dall'effetto della deviazione e, all'occorrenza, dalla causa stessa. Essere sempre espliciti nella registrazione delle conseguenze. Non presumere che il futuro lettore capirà comunque qual è il pericolo o come si sviluppano le conseguenze.

Quando si documentano le conseguenze, è importante ricordare che lo studio HAZOP può essere usato per determinare i rischi ed è quindi fondamentale una piena e completa descrizione delle modalità di sviluppo del pericolo e delle conseguenze risultanti. Le conseguenze, ad esempio, possono essere descritte come segue:

"Potenziale sovrappressione che porta a rottura delle tubazioni di scarico del gas e perdita di contenimento. Il rilascio di grandi volumi di gas è infiammabile a contatto con lo scarico caldo di una macchina comportando esplosioni o incendi istantanei, con potenziale incidente mortale per un numero massimo di due addeti alla manutenzione. Danni al compressore per un importo massimo di 2 milioni di sterline e perdita di produzione per un periodo massimo di 1 anno"

Quando si valutano le conseguenze, è importante non considerare l'azione di sistemi o strumenti di protezione già inclusi nella struttura.

Protezioni

Tutti i dispositivi di protezione esistenti che prevengono la causa o proteggono dalle conseguenze dovrebbero essere registrati in questa colonna. Come protezioni, non si intendono soltanto quelle fisiche ma anche gli aspetti procedurali quali, ad esempio, le regolari ispezioni dell'impianto (se si è certi che saranno effettivamente eseguite E che sono in grado di prevenire o proteggere).

3.7. Esempio di HAZOP

3.7.1. Serbatoio separatore

L'esempio che segue mostra uno schema semplificato di un serbatoio separatore di processo. Il serbatoio contiene il liquido di processo che viene riscaldato da un bruciatore a gas. Il vapore viene separato dal liquido di processo ed indirizzato verso la linea di estrazione. Al termine della reazione, il liquido concentrato rimanente viene prelevato dal fondo del serbatoio, Figura 9.

Il serbatoio è dotato di un sistema di controllo distribuito (DCS) che monitora il livello del liquido all'interno del serbatoio, la pressione e la temperatura del gas.

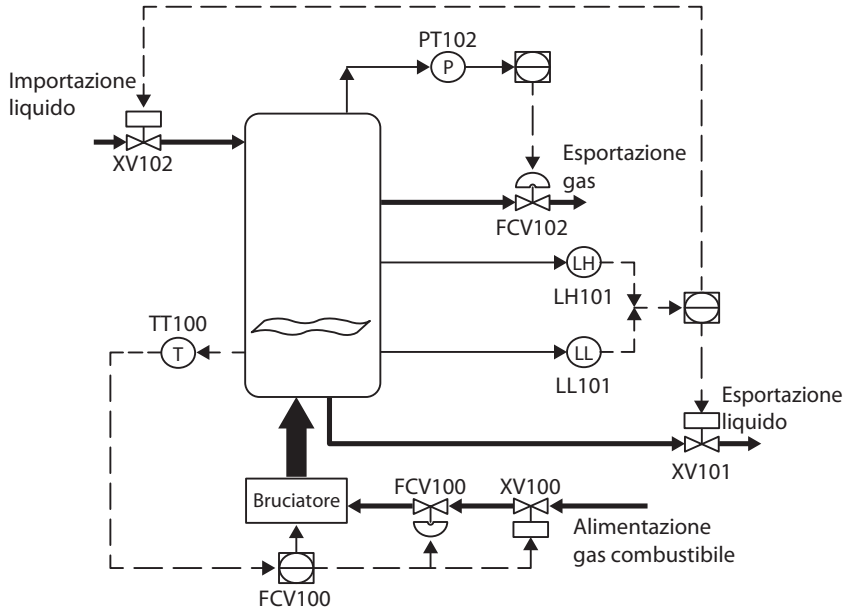


Figura 9: serbatoio separatore

Nello schema che segue, è riportato un esempio di HAZOP per questo serbatoio separatore.

Rif.	Parola chiave primaria	Parola chiave secondaria	Deviazione	Pericolo	Conseguenza
01.01	Flusso	Più	Elevato flusso di liquido di processo nel serbatoio.	Flusso elevato nel serbatoio che potrebbe comportare eccessivo aumento del livello e riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.
01.02			Elevato flusso di liquido di processo dal serbatoio nel liquido di esportazione.	Flusso elevato dal serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.
01.03			Elevato flusso di gas dal serbatoio del gas di esportazione.	Nessun pericolo credibile	Nessuno.
01.04		Meno	Basso flusso di liquido di processo nel serbatoio.	Basso flusso dal serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.
01.05			Basso flusso di liquido di processo dal serbatoio del liquido di esportazione.	Basso flusso dal serbatoio che potrebbe comportare un eccessivo aumento del livello e riversamento del liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.
01.06			Basso flusso di gas dal serbatoio del gas di esportazione.	Nessun pericolo credibile	Nessuno.
01.07		Inversione	Non credibile.	Nessun pericolo credibile	Nessuno.
01.08		Anche	Non credibile.	Nessun pericolo credibile	Nessuno.
01.09		Altro	Non credibile.	Nessun pericolo credibile	Nessuno.
01.10	Pressione	Più	Alta pressione nel serbatoio.	Rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
01.11		Meno	Bassa pressione nel serbatoio.	Rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
01.12		Inversione	Non credibile.	Nessun pericolo credibile	Nessuno.
01.13		Anche	Non credibile.	Nessun pericolo credibile	Nessuno.
01.14		Altro	Non credibile.	Nessun pericolo credibile	Nessuno.
01.15	Temperatura	Più	Alta temperatura nel serbatoio.	La temperatura elevata porta ad alta pressione, rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
01.16		Meno	Bassa temperatura nel serbatoio.	Possibile congelamento del liquido (solidificazione), rottura del serbatoio e perdita di contenimento.	Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi. Rilascio nell'ambiente con ordine di notifica.
01.17		Inversione	Non credibile.	Nessun pericolo credibile	Nessuno.
01.18		Anche	Non credibile.	Nessun pericolo credibile	Nessuno.
01.19		Altro	Non credibile.	Nessun pericolo credibile	Nessuno.
01.20	Livello	Più	Alto livello nel serbatoio.	Livello elevato nel serbatoio che potrebbe comportare il riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.
01.21		Meno	Basso livello nel serbatoio.	Basso livello nel serbatoio che potrebbe comportare il trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.
01.22		Inversione	Non credibile.	Nessun pericolo credibile	Nessuno.
01.23		Anche	Non credibile.	Nessun pericolo credibile	Nessuno.
01.24		Altro	Non credibile.	Nessun pericolo credibile	Nessuno.

3.7.3. Risultati dello studio HAZOP

Riepilogando, i pericoli identificati sono:

Pericolo	**Conseguenza**
Livello elevato nel serbatoio che potrebbe comportare il riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.
Alta pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
Alta temperatura che porta ad alta pressione, rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
Basso livello nel serbatoio che potrebbe comportare il trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.
Bassa pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.
Bassa temperatura, potenziale congelamento del liquido (solidificazione), rottura del serbatoio e perdita di contenimento.	Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi. Rilascio nell'ambiente con ordine di notifica.

L'elenco dei pericoli identificati forma il registro dei pericoli del sistema. Il registro dei pericoli dovrebbe rimanere un documento "vivo" per tutto il ciclo di vita del sistema, da integrare o revisionare quando vengono effettuati altri studi.

Ognuno dei pericoli identificati potrebbe avere possibili conseguenze di sicurezza, ambientali o commerciali ma, per adempiere ai nostri obblighi nell'ambito dell'Health and Safety at Work Act [1.5.1], dobbiamo determinare il livello di rischio associato ad ognuno dei pericoli [4].

4. Rischi e riduzione dei rischi

4.1. Concetto di rischio

Un rischio è la probabilità che un pericolo provochi un effetto avverso misurabile.

Si tratta di un concetto in due parti che, perché abbia senso, vanno considerate entrambe. Le probabilità possono essere espresse in diversi modi; come probabilità nel senso stretto della parola (una su mille), come frequenza o tasso (1000 casi all'anno) o in modo qualitativo (trascurabile o significativo).

L'effetto può essere descritto in molti modi diversi. Ad esempio:

- Lesioni gravi o fatali di un singolo dipendente;
- Lesioni di più soggetti terzi;
- Personale esterno esposto a gas tossici.

Per un dipendente, il rischio annuale di essere vittima di un incidente fatale [effetto] sul lavoro dovuto al contatto con macchine in movimento [pericolo] è inferiore ad uno su 100.000 [frequenza].

Il rischio quindi deve essere quantificato in due dimensioni. È necessario valutare l'impatto, ovvero le conseguenze del pericolo, e la probabilità di occorrenza. Per semplicità, è opportuno procedere ad una classificazione su una scala da 1 a 4, come mostrato nella Figura 10, dove più grande è il numero, maggiore è l'impatto o la probabilità di occorrenza. In linea generale, utilizzando una matrice di rischio come questa, è possibile stabilire le priorità e valutare i rischi.

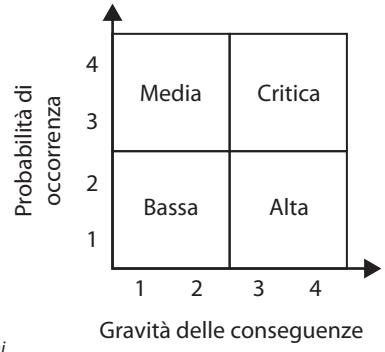


Figura 10: matrice dei rischi

Se la probabilità di occorrenza è alta e la gravità delle conseguenze è bassa, il rischio può essere considerato "medio". D'altra parte, se la gravità delle conseguenze è alta e la

probabilità di occorrenza è bassa, il rischio può essere considerato "alto". Generalmente, la possibilità remota di un evento catastrofico dovrebbe essere valutata con maggiore attenzione rispetto ad un problema minore che si verifica frequentemente.

Fin qui, i rischi considerati fanno riferimento solo alla sicurezza del personale ma non c'è ragione per cui lo stesso approccio non possa essere adottato per i rischi legati all'ambiente, all'azienda ed alle sue risorse, alla capacità di generare ricavi, alla reputazione della società o ai processi di approvvigionamento riguardanti le aziende di generazione di energia.

4.2. Analisi dei pericoli (HAZAN)

Una prima valutazione dei rischi può essere realizzata nell'ambito dello studio HAZOP e si tratta di un'analisi dei pericoli (HAZAN). Come illustrato nella Figura 10, ogni pericolo può essere categorizzato in termini di gravità (da 1 a 4, dove 4 è il più grave) e di probabilità di occorrenza o frequenza (da 1 a 4, dove 4 è la più probabile).

L'esempio HAZOP [3.7.2] può essere sviluppato e, moltiplicando tra loro le categorie di gravità e frequenza, è possibile ottenere una misura preliminare del rischio – ovvero l'indice di priorità del rischio (RPN) – che può essere usata per mettere in ordine di priorità le azioni di riduzione dei rischi [4.3].

4.3. HAZAN del serbatoio separatore

La colonna "Azione" consente di formulare raccomandazioni per azioni correttive quali, ad esempio, l'identificazione di quali altre protezioni possono essere implementate.

Le possibili azioni rientrano in due gruppi:

- azioni che eliminano la causa;
- azioni che mitigano le conseguenze.

Eliminare la causa del pericolo è sempre la soluzione da preferire. Solo quando ciò non è fattibile, si dovrebbe considerare la mitigazione delle conseguenze.

4.3.1. Azioni dello studio HAZOP

I fogli di lavoro HAZOP identificano anche le azioni su cui indagare ulteriormente. In questo esempio, sono state identificate le azioni che seguono.

Rif.	Deviazione	Pericolo	Conseguenza	Cat. grav.	Cat. freq.	RPN	Protezioni	Azione
01.01	Elevato flusso di liquido di processo nel serbatoio.	Flusso elevato nel serbatoio che potrebbe comportare eccessivo aumento del livello e riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.	3	2	6	Controllo del livello.	Considerare l'installazione di un allarme di alto livello.
01.02	Elevato flusso di liquido di processo dal serbatoio del liquido di esportazione.	Flusso elevato dal serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.	2	1	2	Controllo del livello.	Considerare l'installazione di un allarme di basso livello.
01.03	Elevato flusso di gas dal serbatoio del gas di esportazione.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.04	Basso flusso di liquido di processo nel serbatoio.	Basso flusso dal serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.	2	2	4	Controllo del livello.	Considerare l'installazione di un allarme di basso livello.
01.05	Basso flusso di liquido di processo dal serbatoio del liquido di esportazione.	Basso flusso dal serbatoio che potrebbe comportare un eccessivo aumento del livello e riversamento del liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.	3	1	3	Controllo del livello.	Considerare l'installazione di un allarme di alto livello.
01.06	Basso flusso di gas dal serbatoio del gas di esportazione.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.07	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.08	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.09	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.10	Alta pressione nel serbatoio.	Rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	4	2	8	Controllo della pressione.	Considerare l'installazione di un allarme di alto livello.
01.11	Bassa pressione nel serbatoio.	Rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	4	1	4	Controllo della pressione.	Considerare l'installazione di un allarme di basso livello.
01.12	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.13	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.14	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.15	Alta temperatura nel serbatoio.	La temperatura elevata porta ad alta pressione, rottura del serbatoio e rilascio di gas	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	4	1	4	Controllo della temperatura.	Considerare l'installazione di un allarme di alta temperature.
01.16	Bassa temperatura nel serbatoio.	Possibile congelamento del liquido (solidificazione), rottura del serbatoio e perdita di contenimento.	Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi. Rilascio nell'ambiente con ordine di notifica.	3	1	3	Controllo della temperatura.	Considerare l'installazione di un allarme di bassa temperatura.
01.17	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.18	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.19	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.20	Alto livello nel serbatoio.	Livello elevato nel serbatoio che potrebbe comportare il riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.	3	2	6	Controllo del livello.	Considerare l'installazione di un allarme di alto livello.
01.21	Basso livello nel serbatoio.	Basso livello nel serbatoio che potrebbe comportare il trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.	2	1	2	Controllo del livello.	Considerare l'installazione di un allarme di basso livello.
01.22	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.23	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	
01.24	Non credibile.	Nessun pericolo credibile	Nessuno.				Nessuno.	

Rif.	Pericolo	Conseguenza	Azione	Azione assegnata	Data di completamento
01.01	Flusso elevato nel serbatoio che potrebbe comportare eccessivo aumento del livello e riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di alto livello.	S Smith C&I_Dept	14 Apr 12
01.02	Flusso elevato dal serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di basso livello.	S Smith C&I_Dept	14 Apr 12
01.04	Basso flusso nel serbatoio che potrebbe comportare eccessivo abbassamento del livello e trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di basso livello.	S Smith C&I_Dept	14 Apr 12
01.05	Basso flusso dal serbatoio che potrebbe comportare un eccessivo aumento del livello e riversamento del liquido nel gas di esportazione.	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di alto livello.	S Smith C&I_Dept	14 Apr 12
01.10	Rottura del serbatoio e rilascio di gas.	Possibile incidente mortale per i manutentori. Danni alle apparecchiature. Rilascio nell'ambiente.	Considerare l'installazione di un allarme di alta pressione.	J Jones Process Dept	21 Apr 12
01.11	Rottura del serbatoio e rilascio di gas.	Possibile incidente mortale per i manutentori. Danni alle apparecchiature. Rilascio nell'ambiente.	Considerare l'installazione di un allarme di bassa pressione.	J Jones Process Dept	21 Apr 12
01.15	Alta temperatura che porta ad alta pressione, rottura del serbatoio e rilascio di gas.	Possibile incidente mortale per i manutentori. Danni alle apparecchiature. Rilascio nell'ambiente.	Considerare l'installazione di un allarme di alta temperatura.	V White C&I_Dept	21 Apr 12
01.16	Potenziale congelamento del liquido, rottura del serbatoio e perdita di contenimento.	Danni alle apparecchiature. Rilascio nell'ambiente.	Considerare l'installazione di un allarme di bassa temperatura.	V White C&I_Dept	21 Apr 12
01.20	Livello eccessivo nel serbatoio che potrebbe comportare il riversamento del liquido nel gas di esportazione	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di alto livello.	S Smith C&I_Dept	14 Apr 12
01.21	Basso livello nel serbatoio che potrebbe comportare il trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle.	Considerare l'installazione di un allarme di basso livello.	S Smith C&I_Dept	14 Apr 12

4.4. Esempi di categorizzazione nella matrice dei rischi

La Figura 11 presenta informazioni simili a quelle della semplice matrice dei rischi utilizzata prima. La gravità delle conseguenze è stata classificata con semplici descrizioni generiche (incidentali, minori, gravi, catastrofiche ecc.). Se è stato condotto uno studio HAZOP, le probabili conseguenze dei pericoli identificati saranno note e possono quindi essere raggruppate e categorizzate.

La quantificazione della frequenza di occorrenza è più difficile. La Figura 11 mostra un approccio attraverso cui la frequenza viene categorizzata in modo descrittivo da molto frequente (il pericolo si verifica diverse volte all'anno) a molto raro (mai sperimentato nel settore o in altri settori). Con una tale descrizione qualitativa della frequenza di occorrenza, è possibile assegnare intervalli di frequenza ad ogni categoria.

La tabella che ne risulta, quindi, consente una categorizzazione dei rischi che va da molto basso (VL) a basso (L), medio (M), alto (H) e molto alto (VH), a seconda della categoria di gravità e della frequenza.

Gravità		Frequenza							
		Mai sperimentato in altri settori/ tipi di lavoro	Mai sperimentato nel settore/ tipo di lavoro	Sperimentato nel settore/ tipo di lavoro	Sperimentato nell'attività	Sperimentato diverse volte nell'attività	Sperimentato nello stabilimento	Sperimentato diverse volte nello stabilimento	Sperimentato diverse volte all'anno nello stabilimento
		A	B	C	D	E	F	G	H
Catastrofica 10^{-6}/anno	6	VL	L	M	H	VH	VH	VH	VH
Grave 10^{-5}/anno	5		VL	L	M	H	VH	VH	VH
Rilevante 10^{-4}/anno	4			VL	L	M	H	VH	VH
Moderata 10^{-3}/anno	3				VL	L	M	H	VH
Minore 10^{-2}/anno	2					VL	L	M	H
Incidentale 10^{-1}/anno	1						VL	L	M
		$<10^{-6}$/anno	$10^{-6} – 10^{-5}$/anno	$10^{-5} – 10^{-4}$/anno	$10^{-4} – 10^{-3}$/anno	$10^{-3} – 10^{-2}$/anno	$10^{-2} – 10^{-1}$/anno	$10^{-1} – 1$/anno	>1/anno

Figura 11: matrice dei rischi

4.5. Quantificazione dei rischi

La tollerabilità del rischio è stata considerata, fino ad ora, a livello qualitativo. La quantificazione della tollerabilità dei rischi per la sicurezza del personale dipende da come i rischi vengono percepiti e su questo possono influire diversi fattori, tra cui i seguenti:

- esperienza personale degli effetti avversi;
- background ed elementi sociali o culturali;
- grado di controllo su un particolare rischio;
- modo in cui vengono ottenute le informazioni dalle diverse fonti (ad es. i media).

Naturalmente, esistono dei rischi così alti da essere ovviamente inaccettabili, come fumare durante u na gravidanza, ed altri così bassi da essere trascurabili, come far bollire il latte in un pentolino. L'area di discussione più interessante è quella che sta nel mezzo ovvero quella dei rischi tollerabili, evidenziati in grigio. Il compito è quindi definire i due limiti:

- quello tra i rischi inaccettabili e tollerabili;
- quello tra i rischi tollerabili ed accettabili.

Il documento di guida HSE "Reducing Risks, Protecting People (Riduzione dei rischi, protezione delle persone)" (R2P2) [19.3] prospetta che un **rischio di morte di uno su un milione all'anno, sia per i dipendenti sia per il personale esterno**, corrisponde ad un livello di rischio molto basso che può essere usato come un limite di rischio ampiamente accettabile (trascurabile).

L'R2P2 prosegue suggerendo che un **rischio di morte di 1 su 1000 all'anno** dovrebbe rappresentare la condizione limite tra ciò che è appena tollerabile per una numerosa categoria di lavoratori per gran parte delle loro vite lavorative e ciò che è inaccettabile per chiunque tranne che gruppi piuttosto eccezionali. Nel Regno Unito, il target di salute e sicurezza sul lavoro è quello di ottenere un livello a cui quasi tutta la popolazione potrebbe essere esposta, tutti i giorni, senza effetti avversi.

Per le persone soggette a rischio, questo limite dovrebbe avere un ordine di grandezza inferiore a **1 su 10.000 all'anno**.

I criteri adottati dalla guida HSE possono essere dimostrati in un quadro di riferimento noto come "Tollerabilità del rischio" (TOR), Figura 12, dove sono stati indicati il massimo rischio individuale tollerabile ed il rischio ampiamente accettabile.

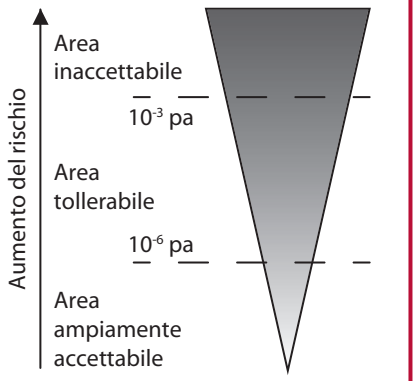


Figura 12: tollerabilità del rischio

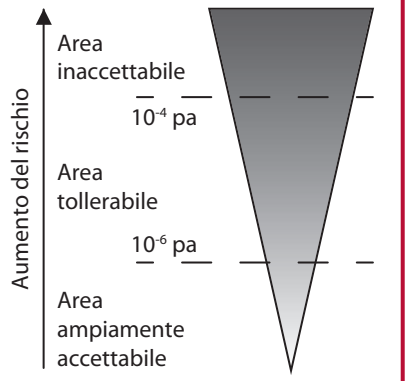


Figura 13: criteri di rischio individuali

4.6. Tollerabilità ed accettabilità del rischio

Nel determinare il rischio quantitativo presentato dai pericoli identificati, ad esempio, in uno studio HAZOP, è necessario stabilire criteri di rischio quantitativi e considerare gli altri pericoli sul lavoro a cui può essere esposto un individuo durante la giornata. È ragionevole presumere che un individuo sia esposto a circa 10 di tali pericoli. La tollerabilità dei criteri di rischio, Figura 12, può quindi essere ripartita tra questi 10 pericoli, assegnando un massimo rischio tollerabile di morte di 1 su 10.000 all'anno, Figura 13.

Il limite di rischio ampiamente accettabile per il rischio di morte, sia per i dipendenti che per i soggetti terzi, rimane di uno su un milione all'anno, già considerato trascurabile. La tollerabilità del rischio può essere riepilogata come illustrato nella Figura 14.

RISCHIO INDIVIDUALE per anno

Conseguenza	Minore/Grave	Grave/Mortale	Mortale (+ persone)
Dipendenti	10^{-3}	10^{-4}	10^{-5}
Soggetti terzi	10^{-4}	10^{-5}	10^{-6}

RISCHIO AMPIAMENTE ACCETTABILE (trascurabile)

Conseguenza	Minore/Grave	Grave/Mortale	Mortale (+ persone)
Dipendenti	10^{-5}	10^{-6}	10^{-6}

Figura 14: sommario della tollerabilità del rischio

A partire dal massimo rischio tollerabile di morte di 1 su 10.000 all'anno, è possibile determinare altri valori di massimo rischio tollerabile, a seconda della gravità e del coinvolgimento o meno di terze parti, Figura 15.

RISCHIO INDIVIDUALE per anno

Conseguenza	Minore/Grave	Grave/Mortale	Mortale (+ persone)
Dipendenti	10^{-3}	10^{-4}	10^{-5}
Soggetti terzi	10^{-4}	10^{-5}	10^{-6}

RISCHIO AMPIAMENTE ACCETTABILE (trascurabile)

Conseguenza	Minore/Grave	Grave/Mortale	Mortale (+ persone)
Dipendenti	10^{-5}	10^{-6}	10^{-6}

Figura 15: sommario della tollerabilità del rischio

4.7. Tollerabilità del rischio

Il sommario della tollerabilità del rischio [Figura 15] può essere rappresentato graficamente come mostrato nella Figura 16.

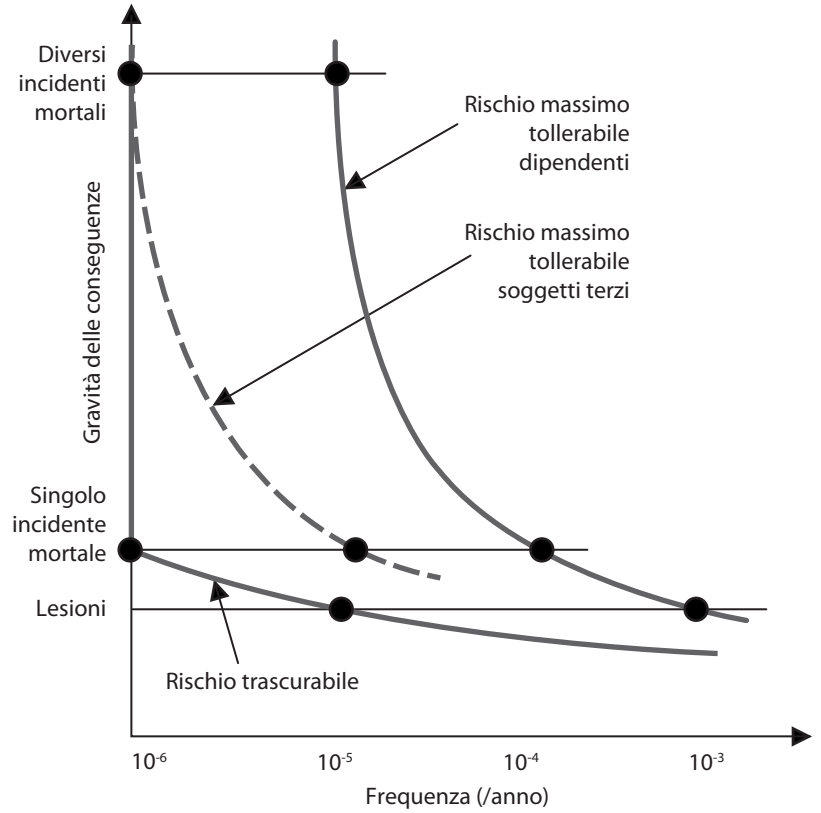


Figura 16: sommario della tollerabilità del rischio

4.8. Requisiti per la conformità

I requisiti per i livelli di integrità della sicurezza derivano dalle probabili frequenze degli eventi pericolosi. A seconda delle conseguenze di un pericolo, viene determinata la massima frequenza tollerabile e sviluppata una funzione di sicurezza in grado di ridurre la frequenza ad un livello tollerabile.

La riduzione del rischio richiesta della funzione di sicurezza rappresenta il primo requisito per la conformità con la norma: si tratta della misura di affidabilità numerica.

La misura di affidabilità numerica viene categorizzata per valore, in fasce o in livelli di integrità della sicurezza (SIL). Sono quattro i SIL basati sulla misura dell'affidabilità target richiesta. SIL4 rappresenta il massimo livello di integrità, la massima riduzione dei rischi ed il target di affidabilità più oneroso. SIL1 rappresenta il minimo livello di integrità ed il target di affidabilità meno oneroso.

4.9. Il principio ALARP

La presentazione di cui sopra dell'analisi dei pericoli e dei rischi spiega come possono essere determinati i rischi di processo ed illustra il massimo rischio tollerabile ottenuto. Tuttavia, in base alla legge HSAWA, è necessario uno sforzo continuo per ridurre ulteriormente il rischio, con altri mezzi, fino a quando possa essere dimostrato che il rischio è **"il minimo per quanto ragionevolmente praticabile"** (ALARP) ovvero che un'ulteriore riduzione del rischio non è economicamente efficiente [5].

5. Il principio ALARP

5.1. Benefici e costi

L'utilizzo dell'espressione "ragionevolmente praticabile" stabilisce obiettivi per i responsabili, anziché essere prescrittiva. Questa flessibilità è un grande vantaggio in quanto permette ai responsabili di scegliere il metodo più adatto a loro e supporta l'innovazione, ma presenta tuttavia alcuni inconvenienti. Decidere se un rischio è ALARP può essere complicato perché richiede una valutazione da parte dei responsabili e dei valutatori.

I principali criteri applicati nella valutazione dei rischi industriali prevedono di determinare se:

a) il rischio è così grande da dover essere rifiutato del tutto;
b) il rischio è, o è stato reso, così piccolo da essere trascurabile;
c) il rischio ricade tra i due stati di cui ai punti a) e b) ed è stato ridotto ad un livello in cui è "il minimo per quanto ragionevolmente praticabile".

Il concetto di "ragionevolmente praticabile" è difficile da quantificare. Implica l'esecuzione di un calcolo per verificare che la possibile ulteriore riduzione del rischio sia bilanciata rispetto al costo che implica (in termini di denaro, tempo o lavoro). Se tra questi elementi c'è grande sproporzione ed il beneficio risulta insignificante rispetto al costo, il rischio è considerato ALARP.

Quindi, la dimostrazione che i rischi sono stati ridotti a livello ALARP implica la valutazione di quanto segue:

- il rischio da evitare;
- il costo (in termini di denaro, tempo e lavoro) necessario ad adottare le misure per evitare quel rischio;
- il confronto di questi due elementi.

Questo processo può prevedere vari gradi di rigore che dipendendo da:

- la natura del pericolo;
- l'importanza del rischio;
- le misure di controllo da adottare.

I responsabili, tuttavia, non dovrebbero essere eccessivamente responsabilizzati se tale rigore non è garantito. Maggiore è il livello iniziale del rischio considerato, maggiore sarà il grado di rigore richiesto.

5.2. Sproporzionalità

Un'analisi del rapporto costi/benefici (CBA) può aiutare un responsabile a stabilire se sono giustificate ulteriori misure di riduzione dei rischi. Le ulteriori misure di riduzione dei rischi possono essere considerate ragionevolmente praticabili se i costi di implementazione non sono manifestamente sproporzionati rispetto ai vantaggi. In altre parole, se il rapporto costi/benefici è > DF, dove DF è il "fattore di sproporzione", la misura può essere considerata eccessiva rispetto alla riduzione del rischio ottenuta.

I DF che possono essere considerati manifesti vanno da 1 in su in base ad una serie di fattori, tra cui la gravità delle conseguenze e la frequenza di tali conseguenze, ovvero maggiore è il rischio, maggiore è il DF.

5.3. Che cos'è la manifesta sproporzione?

La guida HSE non ha formulato un algoritmo che possa essere utilizzato per determinare quando il grado di sproporzione può essere giudicato "manifesto". Non esistono direttive ufficiali da parte dei tribunali su quali fattori dovrebbero essere considerati per determinare se il costo è manifestamente sproporzionato. È quindi necessario giudicare caso per caso e, dalle inchieste sugli incidenti gravi, è possibile trarre alcuni indizi ed una serie di linee guida.

Dall'inchiesta Sizewell B del 1987, sono stati usati i seguenti DF:

- un fattore di 2 per i bassi livelli di rischio applicabili a soggetti terzi;
- fino a 3 (ovvero costi tre volte superiori ai benefici) per i rischi applicabili ai lavoratori;
- un fattore di 10 per gli alti livelli di rischio.

5.4. Analisi del rapporto costi/benefici (CBA)

Per diverse decisioni ALARP, la guida HSE non prevede che i responsabili intraprendano un'analisi dettagliata del rapporto costi/benefici (CBA), ma che effettuino un semplice confronto dei costi e dei benefici.

L'analisi CBA dovrebbe essere usata solo a supporto delle decisioni ALARP. Non dovrebbe rappresentare l'unico argomento alla base di una decisione ALARP né essere utilizzata per ignorare le norme e le buone prassi esistenti. Di per sé, un'analisi CBA non costituisce un caso ALARP e non può essere usata come argomentazione contro doveri obbligatori o per giustificare rischi intollerabili o gli evidenti problemi di scarsa ingegnerizzazione.

I costi giustificabili che possono essere considerati in un'analisi CBA includono:

- installazione;
- funzionamento;
- formazione;
- eventuali interventi di manutenzione aggiuntivi;
- le perdite commerciali che deriverebbero da uno spegnimento effettuato esclusivamente per l'attuazione della misura;
- interessi sulla produzione differita come, ad esempio, il petrolio/gas non estratto da un giacimento mentre sulla piattaforma vengono realizzati i lavori;
- i costi rivendicati devono essere quelli sostenuti dal responsabile (i costi sostenuti da altri soggetti quali, ad esempio, i soggetti terzi non dovrebbero essere calcolati);
- i costi considerati dovrebbero essere solo quelli necessari all'implementazione delle misure di riduzione dei rischi (non eccessive rispetto al rischio).

I benefici giustificabili che possono essere rivendicati in un'analisi CBA possono includere tutti i benefici di implementazione di una misura di miglioramento della sicurezza nel suo complesso, non sottostimati in alcun modo. I benefici dovrebbero includere la riduzione del rischio per i soggetti terzi, i lavoratori e la comunità nel suo complesso e possono includere:

- decessi prevenuti;
- lesioni prevenute (gravi o lievi);
- malattie prevenute;
- danni ambientali prevenuti, se pertinente (ad es. COMAH).

I benefici rivendicati possono anche includere la possibilità di evitare il dispiegamento dei servizi di emergenza ed eventuali contromisure quali l'evacuazione e la decontaminazione post-incidente. Tuttavia, per confrontare i benefici dell'implementazione di un miglioramento della sicurezza con i costi associati, la comparazione deve essere condotta su una base comune. Un metodo semplice per un primo screening delle misure consiste nell'esprimere costi e benefici in un formato comune di "€ all'anno" per la vita di un impianto.

La Tabella 1 riporta alcuni valori monetari rappresentativi, che potrebbero essere utilizzati.

Incidente mortale		€1.336.800 (il doppio per cancro)
Lesioni	Lesioni permanenti invalidanti. Una serie di restrizioni permanenti alle attività di svago ed eventualmente di lavoro.	€207.200
	Gravi. Una serie di restrizioni alle attività di lavoro e/o di svago per diverse settimane/mesi.	€20.500
	Lesioni lievi tra cui tagli ed ecchimosi di lieve entità con un rapido e completo recupero.	€300
Malattia	Malattia permanentemente invalidante. Come per le lesioni.	€193.100
	Altri casi di malattia. Oltre una settimana di assenza. Nessuna conseguenza permanente per la salute.	€2300 + €180 per giorno di assenza
Problemi minori	Fino ad una settimana di assenza. Nessuna conseguenza permanente per la salute.	€530

Tabella 1: Somme accordate dai tribunali (2003)

5.5. Esempio

Domanda: considerare un impianto chimico con un processo che, se dovesse esplodere, comporterebbe:

- 20 decessi;
- 40 lesioni permanenti;
- 100 lesioni gravi;
- 200 lesioni lievi.

La frequenza di questo evento di esplosione è di circa 10^{-5} all'anno, equivalente a 1 su 100.000 all'anno. L'impianto ha una vita stimata di 25 anni. Quanto potrebbe ragionevolmente spendere l'organizzazione per eliminare i rischi legati all'esplosione?

Risposte: se il rischio di esplosione venisse eliminato, i benefici potrebbero essere valutati come segue:

Decessi:	20 x €1.336.800 x 10^{-5} x 25 anni	=	€6684
Lesioni permanenti:	40 x €207.200 x 10^{-5} x 25 anni	=	€2072
Lesioni gravi:	100 x €20.500 x 10^{-5} x 25 anni	=	€512
Lesioni lievi:	200 x €300 x 10^{-5} x 25 anni	=	€15
Benefici totali		=	€9283

La somma di €9283 è il beneficio stimato derivante dall'eliminazione del rischio di esplosione sulla base delle vittime evitate (questo metodo non include l'attualizzazione o la considerazione dell'inflazione).

Perché una misura sia ritenuta non ragionevolmente praticabile, il costo deve essere manifestamente sproporzionato rispetto ai benefici. In questo caso, il DF rifletterà che le conseguenze di tali esplosioni sono alte. Un DF superiore a 10 è improbabile e quindi, per eliminare il rischio di esplosione, potrebbe essere ragionevolmente praticabile spendere fino a €93.000 circa (€9300 x 10). L'utilizzo di un DF più piccolo dovrebbe essere debitamente giustificato del responsabile.

Questa semplice analisi può essere utilizzata per eliminare o includere alcune misure calcolando i costi dei vari metodi alternativi per eliminare o ridurre i rischi.

Approccio alternativo

Una misura di miglioramento della sicurezza, probabilmente, non eliminerà il rischio ma lo ridurrà parzialmente e tale riduzione deve essere valutata, come il beneficio, rispetto al costo di implementazione.

Generalmente, le organizzazioni fanno riferimento ad un costo per vita salvata target (valore di prevenzione di un incidente mortale: VPF).

Il costo di prevenzione degli incidenti mortali per l'intera vita dell'impianto viene confrontato con il VPF target.

I miglioramenti vengono implementati a meno che i costi siano manifestamente sproporzionati.

5.6. Esempio

Domanda: applicazione del criterio ALARP

In una particolare industria, viene utilizzato un costo per vita salvata target di 2 milioni di sterline. Il rischio massimo tollerabile target per un particolare pericolo che potrebbe provocare 2 decessi è stato stabilito in 10^{-5} pa.

Il sistema di sicurezza proposto è stato valutato ed è stato previsto un rischio di 8,0 x 10^{-6} pa. Poiché il rischio ampiamente accettabile (trascurabile) è di 10^{-6} pa, è necessaria l'applicazione del criterio ALARP.

In questo esempio, per un costo di €10.000, strumentazione aggiuntiva e ridondanza saranno in grado di ridurre il rischio a 2,0 x 10^{-6} pa (immediatamente sopra l'area di rischio trascurabile) per tutta la durata dell'impianto, pari a 30 anni.

La proposta dovrebbe essere adottata?

Risposta: il numero di vite salvate per tutta la durata dell'impianto è dato da:

N = (riduzione della frequenza di decessi) x numero di decessi per incidente x durata dell'impianto
= (8,0 x 10^{-6} – 2,0 x 10^{-6}) x 2 x 30
= 3,6 x 10^{-4}

Quindi il costo per vita salvata è:

VPF = €10000/3,6 x 10^{-4}
= €27,8M

Il VPF calcolato è superiore di 10 volte al costo target per vita salvata di 2 milioni di sterline e la proposta, quindi, dovrebbe essere rifiutata.

6. Determinazione dei target SIL

6.1. Funzioni di sicurezza in modalità su domanda ed in modalità continua

Quando si valuta un sistema di sicurezza in termini di mancato funzionamento, esistono due principali opzioni, a seconda della modalità di funzionamento. Se la frequenza di domanda a cui è soggetto un sistema di sicurezza è bassa (generalmente, meno di una all'anno), si parla di modalità su domanda. Un esempio di tale sistema di sicurezza sono gli airbag di un'auto.

I freni di un'auto, invece, sono un esempio di sistema di sicurezza in modalità continua perché vengono utilizzati (quasi) continuamente. Per i sistemi di sicurezza in modalità su domanda si calcola, in genere, la probabilità di guasto media su domanda (PFD) mentre, per sistemi di sicurezza che funzionano in modalità continua, si utilizza la probabilità di guasto pericoloso all'ora (PFH).

6.2. Funzione di sicurezza in modalità su domanda

Presumiamo, ad esempio, che una fabbrica sia soggetta ad una media di 1 incendio ogni 2 anni e che, se non adottassimo altre misure, questo incendio si tradurrebbe in un incidente mortale. Potremmo tracciare un grafico della frequenza di incidenti mortali (Figura 17) in cui la frequenza è di 0,5/anno.

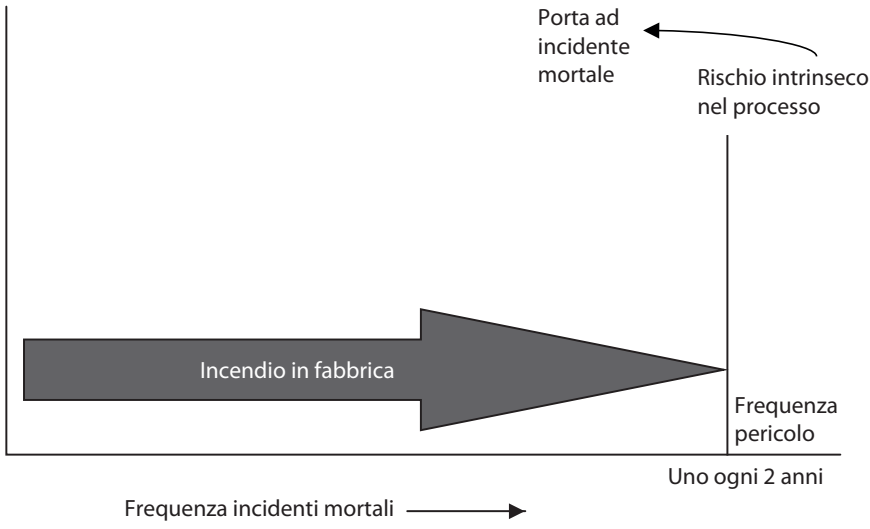


Figura 17: frequenza degli incidenti mortali

In casi come questo, quando si determinano le conseguenze dell'incendio, è fondamentale non considerare alcuna misura di sicurezza già in atto. Ciò che cerchiamo sono le conseguenze del caso peggiore.

Se abbiamo installato un allarme antifumo che, ad esempio, ha funzionato 9 volte su 10, dovremmo aspettarci un incidente mortale in quell'unica occasione, su 10 incendi, in cui l'allarme antifumo non funziona su domanda. In questo caso, la frequenza di incidenti mortali scenderebbe da 1 decesso ogni 2 anni a 1 decesso ogni 20 anni.

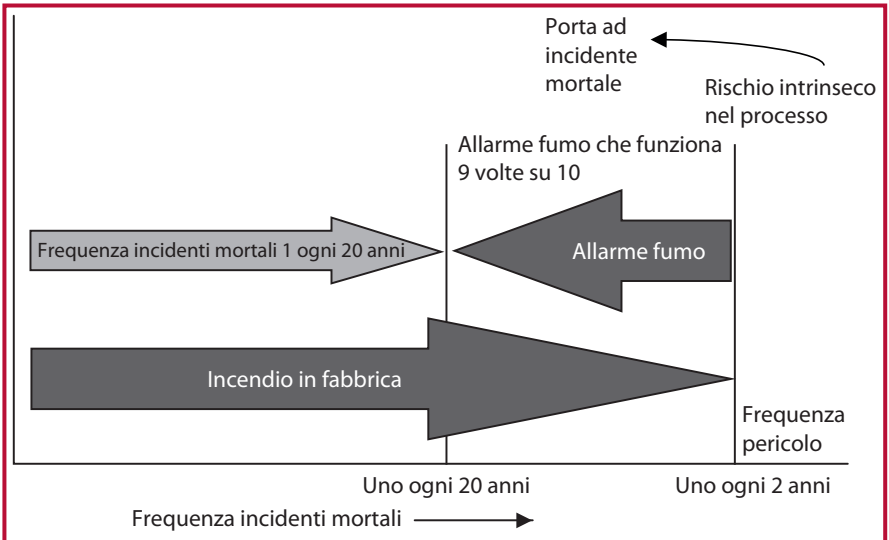


Figura 18: riduzione della frequenza degli incidenti mortali

Se l'allarme antifumo funziona per 9 incendi su 10, la probabilità di guasto su domanda (PFD) è di 1 su 10 ovvero del 10%. In questo caso, PFD = 0,1. L'allarme antifumo con una PFD di 0,1 ridurrebbe la frequenza di incidenti mortali di un fattore di 10, permettendo di ottenere un fattore di riduzione del rischio (RRF) di 10.

Riepilogando, PFD = 1/RRF.

È utile ricordare che, matematicamente, la PFD è una probabilità e quindi una quantità adimensionale, con un valore compreso tra zero e 1.

6.3. Esempio di livello di integrità della sicurezza target

L'approccio per determinare un SIL target consiste nel calcolare la riduzione del rischio necessaria ad abbassare ad un livello tollerabile la frequenza delle conseguenze di un pericolo.

Determinazione dei target SIL

L'approccio raccomandato per determinare i livelli di integrità della sicurezza è quello di valutare i rischi presentati da ogni pericolo nell'impianto. Se conduciamo un'analisi HAZOP sul nostro impianto e, nel processo, identifichiamo un pericolo in grado di nuocere se non adottiamo alcuna contromisura, dobbiamo valutare le potenziali conseguenze. Saranno le conseguenze del caso peggiore a determinare la massima frequenza tollerabile per questo pericolo.

Se il pericolo considerato può comportare il decesso di un dipendente, in base alla tollerabilità ed all'accettabilità dei criteri di rischio [4.6], possiamo assegnare al pericolo una frequenza massima tollerabile. In altre parole, per il pericolo identificato, possiamo specificare un rischio massimo tollerabile di 10^{-4} all'anno.

Analizzando le cause scatenanti del pericolo, possiamo stimarne la frequenza, ipotizzando di non fare altro, e confrontarla alla massima frequenza tollerabile specificata. Ad esempio, possiamo fare qualche analisi e determinare che il nostro pericolo, se non controllato, potrebbe verificarsi una volta all'anno. Esiste quindi un gap di rischio che deve essere affrontato, Figura 19.

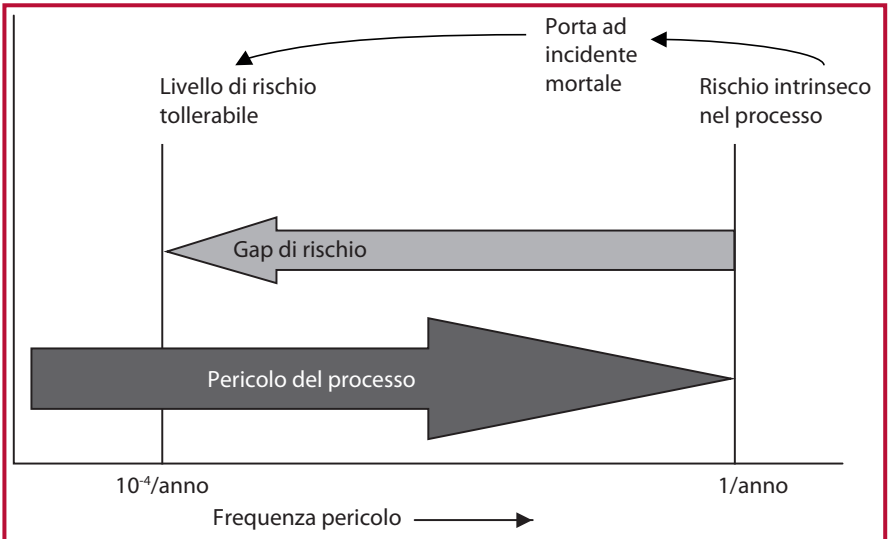


Figura 19: gap di rischio

Possiamo allora considerare le eventuali protezioni già esistenti per ridurre la frequenza del pericolo, come un allarme, Figura 20. In questo caso, l'allarme riduce la frequenza delle conseguenze del pericolo della sua PFD. Il gap di rischio è ridotto ma il rischio residuo globale, sebbene inferiore, è ancora superiore al massimo rischio tollerabile.

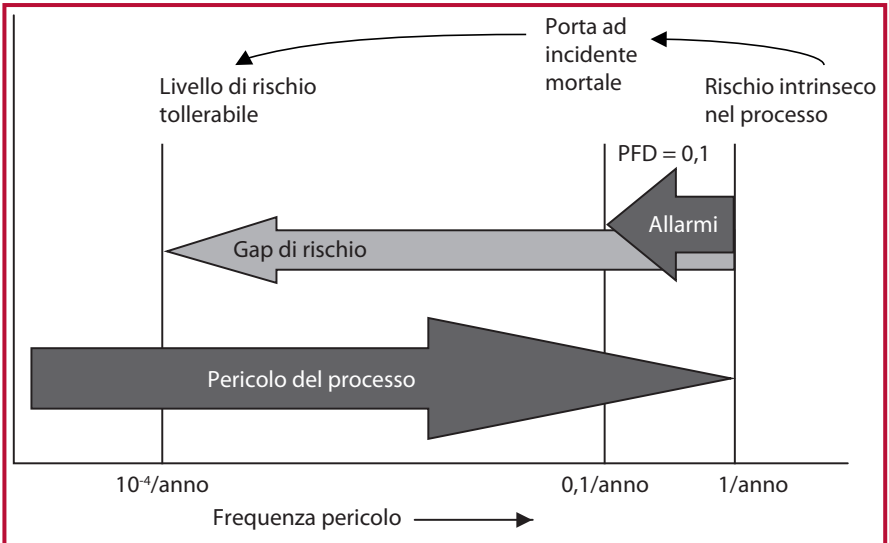


Figura 20: considerazione degli allarmi

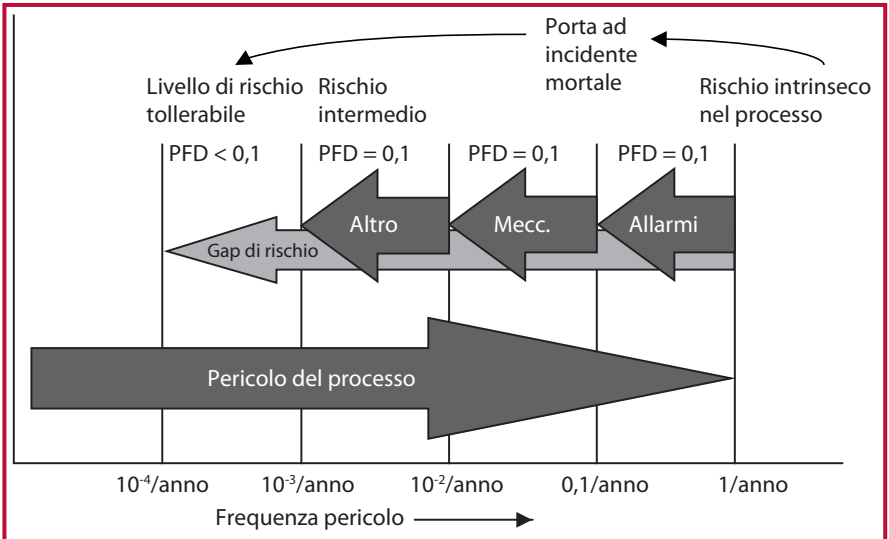


Figura 21: considerazione di altri livelli di protezione

Determinazione dei target SIL

Prendere in considerazione altri livelli di protezione può ridurre ulteriormente il rischio residuo. Ad esempio, possono essere installati dei dispositivi meccanici quali una valvola di scarico della pressione, un muro o un bacino di contenimento. Altre misure di riduzione del rischio possono coinvolgere il controllo di processo, la strumentazione o le procedure ed ognuna di loro può ridurre il rischio residuo (Figura 21) delle rispettive PFD. In questo esempio, abbiamo considerato tutte le varie protezioni già esistenti nell'impianto ma rimane comunque un gap di rischio residuo. Come si può vedere, per ridurre la frequenza del pericolo ad un livello inferiore alla massima frequenza tollerabile, abbiamo bisogno di un altro livello, con una probabilità PFD inferiore a 0,1. Questo è il compito del sistema SIS, Figura 22. Questo calcolo, sebbene rappresentato graficamente, fornisce la probabilità PFD target del nostro sistema SIS e permette di determinare il livello SIL target. Questo è un esempio di funzione di sicurezza in modalità su domanda.

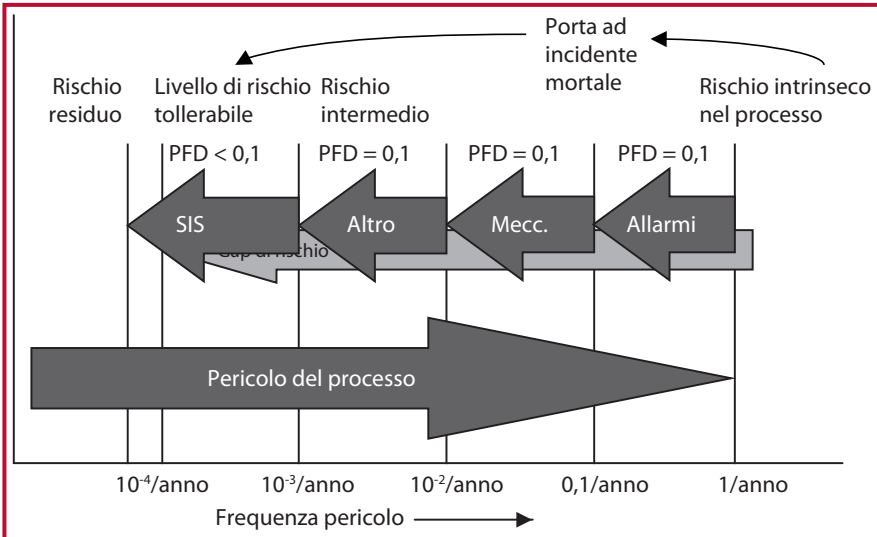


Figura 22: target PFD

6.4. Funzioni di sicurezza

Generalmente, la struttura di un sistema SIS e del suo processo è quella mostrata nella Figura 23.

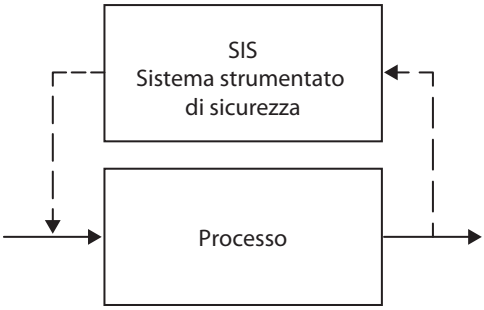


Figura 23: sistema strumentato di sicurezza

La funzione strumentata di sicurezza monitora una serie di parametri di processo e, se vengono superati certi limiti, interviene per rendere il processo sicuro. Un semplice esempio relativo all'industria di processo è illustrato nella Figura 24.

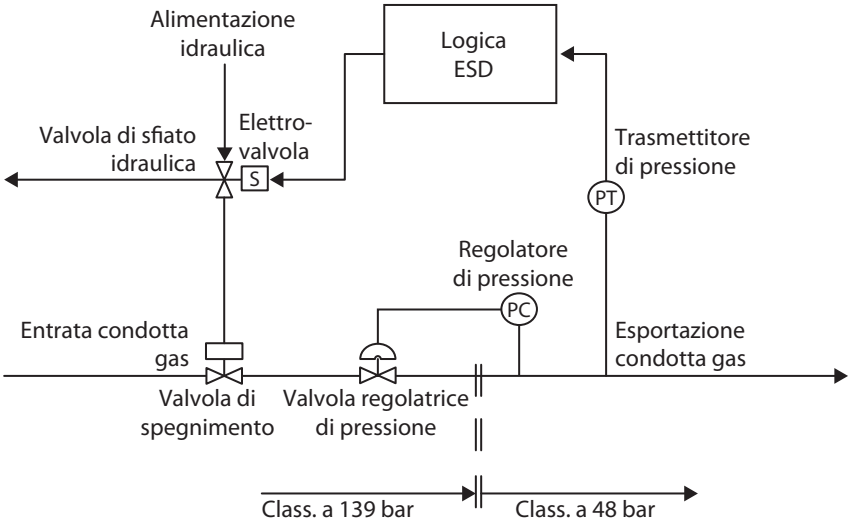


Figura 24: esempio di funzione strumentata di sicurezza

Lo schema mostra una condotta di gas che alimenta una centrale elettrica. Il gas passa da sinistra a destra, attraverso una valvola di arresto, fino a raggiungere la valvola regolatrice di pressione (Pressure Control Valve, PCV). La valvola PCV è controllata da un regolatore di pressione (PC) che mantiene la pressione del gas a meno di 48 bar, il valore nominale di sicurezza della condotta di esportazione. Il mancato funzionamento di questa funzione di controllo della pressione potrebbe comportare sovrapressurizzazione della condotta a valle, rottura, generazione di incendi ed incidenti mortali; quindi, è stata sviluppata una funzione di sicurezza per evitare questo scenario. La funzione di sicurezza, costituita da un trasmettitore di pressione (PT) separato, una logica di spegnimento di emergenza (ESD) ed una valvola di arresto (Shutdown Valve, SDV) azionata da un'elettrovalvola idraulica (SOV), serve ad arrestare l'alimentazione di gas nel caso in cui la pressione a valle superi una determinata soglia di intervento.

6.5. Esempio di una funzione di sicurezza in modalità su domanda

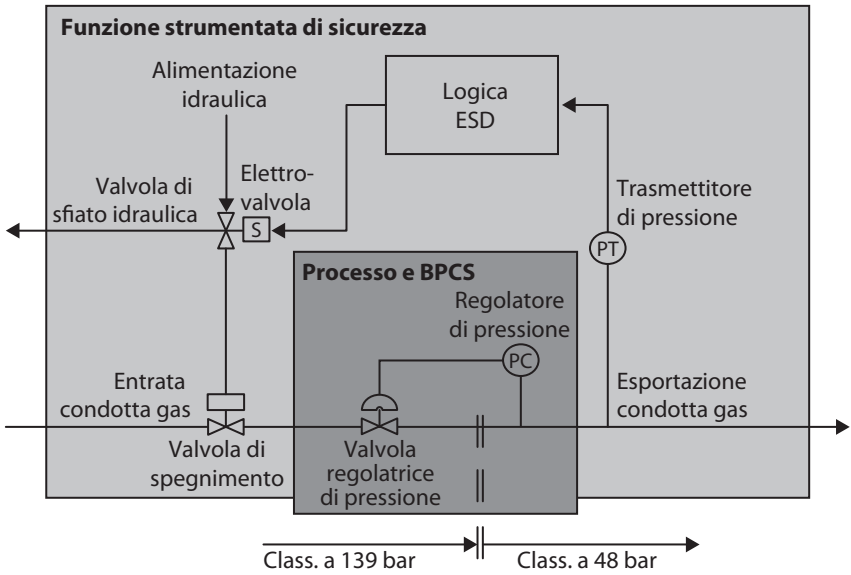


Figura 25: funzione di sicurezza in modalità su domanda

Quello che segue è un esempio di funzione di sicurezza in modalità su domanda. Le principali caratteristiche di una funzione di sicurezza in modalità su domanda sono le seguenti:

- è generalmente separata dal processo;
- il mancato funzionamento della funzione di sicurezza comporta la perdita della protezione ma non è pericoloso in se stesso;

- la frequenza delle domande di intervento è bassa, meno di una all'anno.

Le funzioni di sicurezza in modalità su domanda includono sistemi di spegnimento del processo (PSD), sistemi di spegnimento di emergenza (ESD) e sistemi di protezione dalla pressione ad alta integrità (HIPPS).

Il fatto che il trasmettitore di pressione PT che fa parte della funzione di sicurezza, pur monitorando costantemente la pressione di processo, rimanga comunque in modalità su domanda è spesso motivo di confusione. Il termine "modalità su domanda" si riferisce alla frequenza delle domande di intervento (ad es. alla frequenza delle escursioni di alta pressione).

6.6. Esempio di una funzione di sicurezza in modalità continua

La Figura 26 mostra un esempio di una funzione di sicurezza in modalità continua.

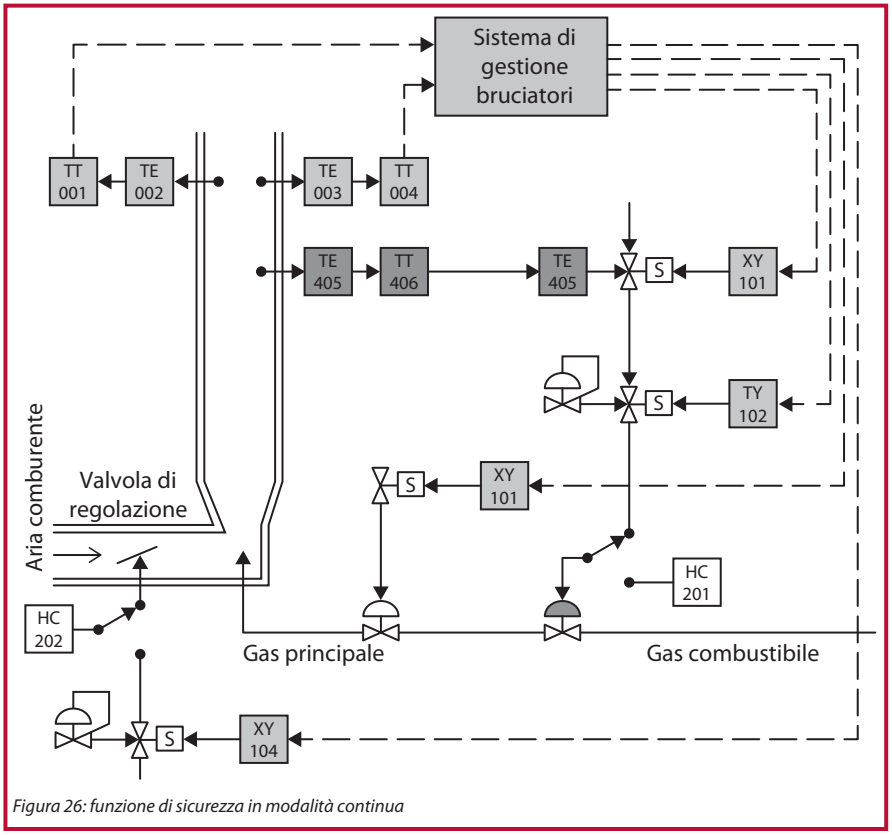


Figura 26: funzione di sicurezza in modalità continua

La figura mostra un tipico sistema di gestione bruciatori (BMS) utilizzato per il controllo di una camera di combustione. Il sistema controlla il gas combustibile e l'aria comburente nella camera di combustione e monitora la fiamma dei bruciatori con rilevatori di fiamma.

In mancanza di fiamma, il sistema BMS deve arrestare il gas combustibile per prevenirne l'accumulo e la possibile esplosione. Prima dell'accensione, inoltre, il bruciatore deve essere spurgato per assicurare che il gas non si sia accumulato nella camera di combustione per infiltrazioni a valle delle valvole o problemi di controllo.

Il sistema BMS, quindi, deve controllare la sequenza di avviamento, provvedere allo spurgo necessario e monitorare il funzionamento dopo l'accensione. In questo esempio, il sistema BMS e tutti i sensori e le valvole corrispondenti costituiscono una funzione di sicurezza in modalità continua.

Le principali caratteristiche di una funzione di sicurezza in modalità continua sono le seguenti:

- generalmente, fornisce qualche funzione di controllo;
- il mancato intervento della funzione di sicurezza generalmente comporta una situazione pericolosa;
- la frequenza delle domande di intervento è alta – più di una all'anno – o addirittura continua.

Le funzioni di sicurezza in modalità continua generalmente includono sistemi di gestione dei bruciatori e di controllo delle turbine.

6.7. SIL target della modalità su domanda

La norma IEC 61511-1, 9.2.4 raggruppa le probabilità PFD target in fasce ovvero in livelli di integrità della sicurezza (SIL). Nell'esempio che precede [6.3], per la nostra funzione di sicurezza abbiamo una PFD target di $<10^{-1}$ che corrisponde a un livello SIL1, come mostrato nella Tabella 2.

Modalità di funzionamento su domanda (probabilità di guasto media nell'eseguire la funzione su domanda)	**Livello di integrità della sicurezza**
$\geq 10^{-5} \ldots < 10^{-4}$	4
$\geq 10^{-4} \ldots < 10^{-3}$	3
$\geq 10^{-3} \ldots < 10^{-2}$	2
$\geq 10^{-2} \ldots < 10^{-1}$	1

Tabella 2: SIL target della modalità su domanda

Nota: la probabilità PFD target è raggruppata in fasce SIL perché la norma richiede un adeguato grado di rigore delle tecniche e delle misure applicate nel controllo e nell'esclusione dei guasti sistematici. Questi requisiti sono trattati in modo più approfondito nella Sezione [12.15].

6.8. SIL target della modalità continua

La norma IEC 61511-1, 9.2.4 fornisce SIL target anche per i sistemi in modalità continua, Tab. 3.

Modalità di funzionamento continua (probabilità di guasti pericolosi all'ora, PFH)	**Livello di integrità della sicurezza**
$\geq 10^{-9} \ldots < 10^{-8}$	4
$\geq 10^{-8} \ldots < 10^{-7}$	3
$\geq 10^{-7} \ldots < 10^{-6}$	2
$\geq 10^{-6} \ldots < 10^{-5}$	1

Tabella 3: SIL target della modalità continua

Nota: la misura dei guasti target della modalità continua è la probabilità PFH ovvero il tasso di guasto.

Nota a piè di pagina.

Ad una prima occhiata, questi tassi di guasto target possono sembrare più onerosi dei target per i sistemi modalità su domanda; ad esempio, il livello SIL1 (modalità su domanda) dovrebbe avere una probabilità PFD di $<10^{-1}$ mentre il livello SIL1 (modalità continua) ha una probabilità PFH di $<10^{-5}$ guasti/ora.

Tuttavia, se convertiamo i target della modalità continua da guasti/ora a guasti/anno, le tabelle diventano sovrapponibili. In un anno, ci sono circa 10^{-4} ore (effettivamente 8760) e la tabella della modalità continua può quindi essere modificata come illustrato nella Tabella 4.

Modalità di funzionamento continua (probabilità di guasti pericolosi all'anno)	**Livello di integrità della sicurezza**
$\geq 10^{-5} \ldots < 10^{-4}$	4
$\geq 10^{-4} \ldots < 10^{-3}$	3
$\geq 10^{-3} \ldots < 10^{-2}$	2
$\geq 10^{-2} \ldots < 10^{-1}$	1

Tabella 4: SIL target della modalità continua (PA)

6.9. Modalità di funzionamento (sistemi in modalità su domanda e continua)

Nel determinare il modo in cui funziona un sistema SIS, la norma IEC 61511-1, 3.2.43 propone le seguenti definizioni.

Modalità su domanda

- quando, in risposta alle condizioni di processo o ad altre domande, viene intrapresa una specifica azione. In caso di guasto pericoloso della funzione SIF, il potenziale pericolo si verifica solo in presenza di un guasto del processo del sistema BPCS;

Modalità continua

- quando, in caso di guasto pericoloso della funzione SIF, il potenziale pericolo si verifica senza un ulteriore guasto, a meno che siano state adottate misure di prevenzione.

Una buona regola generale per decidere se la funzione di sicurezza è in modalità continua o su domanda, è quella di identificare la metrica significativa ovvero la misura dell'affidabilità.

Gli airbag di un'auto forniscono una funzione di sicurezza molto utile e come automobilista, sarei interessato alla loro probabilità di guasto su domanda e questo è una buona indicazione del fatto che si tratta di una funzione in modalità su domanda. Facendo riferimento alla Sezione [6.5], le principali caratteristiche di una funzione di sicurezza in modalità su domanda sono le seguenti:

- è generalmente separata dal processo;
- il mancato funzionamento della funzione di sicurezza comporta la perdita della protezione ma non è pericoloso in se stesso.

La Tabella 2, quindi, conferma che i target per le funzioni in modalità su domanda sono la probabilità di guasto su domanda.

Per i freni di un'auto, invece, la metrica significativa sarebbe il tasso di guasto ovvero la probabilità di guasto all'ora. Come automobilista, sarei molto interessato al tasso di guasto della funzione di sicurezza e questo è una buona indicazione del fatto che si tratta di una funzione in modalità continua.

A supporto di quanto detto, le principali caratteristiche di una funzione di sicurezza in modalità continua sono le seguenti:

- generalmente, fornisce qualche funzione di controllo e, in questo caso, la frenatura;

- il mancato intervento della funzione di sicurezza generalmente comporta una situazione pericolosa (perdita del controllo della velocità).

La Tabella 3 conferma che i target della modalità continua sono le probabilità di guasti pericolosi all'ora.

6.10. Funzioni di sicurezza della modalità su domanda

6.10.1. Esempio

Domanda: un'area di processo è presidiata per 2 ore al giorno. La sovrappressione del processo comporterebbe una fuga di gas e si stima che 1 su 10 di tali fughe di gas provocherebbe un'esplosione e la conseguente morte dell'operatore.

L'analisi indica che la condizione di sovrappressione può verificarsi ogni 5 anni (una frequenza di 0,2 pa).

Supponiamo che la massima frequenza tollerabile per il pericolo (operatore ucciso dall'esplosione) sia di 10^{-4} pa.

Qual è la probabilità PFD richiesta del sistema SIS?

Risposta: il tasso di incidenti mortali è:

$= 0{,}2 \text{ pa} \times 2/24 \times 1/10$
$= 1{,}67 \times 10^{-3} \text{ pa}$

Quindi, il sistema di sicurezza deve avere una probabilità di guasto su domanda di:

$= 10^{-4} \text{ pa}/1{,}67 \times 10^{-3} \text{ pa}$
$= 6{,}0 \times 10^{-2}$, equivalente a SIL1.

Questo è un esempio di un sistema SIS in modalità su domanda, in quanto il suo intervento viene richiesto solo alla frequenza determinata dal tasso di guasto dell'apparecchiatura sotto controllo.

Noi possiamo confermare che il risultato sia effettivamente una probabilità PFD perché abbiamo diviso un tasso per un tasso per ottenere un valore adimensionale, ovvero una probabilità.

6.11. Funzioni di sicurezza in modalità continua

La Figura 27 presenta un semplice esempio di funzione di sicurezza in modalità continua. Il prodotto chimico nella caldaia viene riscaldato da un elemento elettrico controllato da un trasmettitore di temperatura che misura l'uscita.

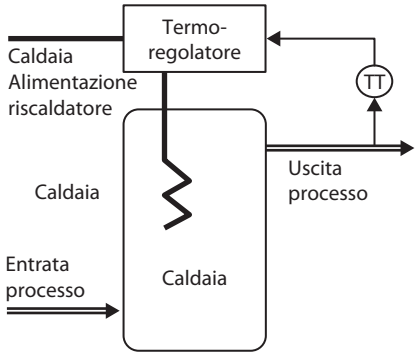


Figura 27: funzione di sicurezza in modalità continua

Ipotizziamo che il surriscaldamento della caldaia comporti rottura, rilascio del prodotto chimico e conseguente incendio con potenziale incidente mortale. Esiste chiaramente un rischio che dovrebbe essere gestito. In questo esempio, il tasso di guasto dell'intero processo non dovrebbe superare il rischio massimo tollerabile per il pericolo.

6.11.1. Esempio

Domanda: Supponiamo che il guasto della caldaia porti a surriscaldamento ed incendio e che 1 su 400 guasti comporti un incidente mortale. Supponiamo anche che il massimo tasso tollerabile di incidenti mortali sia di 10^{-5} pa (incidenti mortali di soggetti terzi).

Qual è il massimo tasso di guasto tollerabile della caldaia?

Risposta: dato che 1 su 400 guasti deve essere inferiore o uguale al massimo rischio tollerabile, possiamo dire che:

$$10^{-5} \text{ pa} \geq \lambda_B \times 1/400$$

Dove λ_B è il tasso di guasto della caldaia.

Quindi:

$$\lambda_B = 400 \times 10^{-5} \text{ pa}$$
$$= 4{,}0 \times 10^{-3} \text{ pa, equivalente a SIL2.}$$

Questo è un esempio di un sistema SIS in modalità continua costantemente a rischio ovvero in uso continuo. È ammissibile che la caldaia si guasti 400 volte più frequentemente del massimo tasso di guasto tollerabile perché solo 1 su 400 guasti comporta un incidente mortale.

In questo esempio, dovremmo progettare e costruire il processo – ovvero la caldaia, l'elemento riscaldante ed il sensore di temperatura – conformemente a SIL2 ed il tasso di guasto dovrebbe essere inferiore a 4,0 x 10^{-3} pa. Si tratterebbe di un progetto complesso, ma c'è un'alternativa.

6.11.2. Esempio

Ipotizziamo di aver costruito il nostro processo della caldaia e calcolato che il suo tasso di guasto è di 5,0 x 10^{-2} pa, di molto superiore al target di 4,0 x 10^{-3} pa.

In tal caso, se 1 su 400 guasti comporta un incidente mortale, la frequenza degli incidenti mortali sarebbe:

= 5,0 x 10^{-2} pa x 1/400
= 1,25 x 10^{-4} pa

ovvero superiore al massimo tasso tollerabile di 10^{-5} pa (incidenti mortali di soggetti terzi).

Un approccio alternativo potrebbe essere quello di permettere alla caldaia di guastarsi a questa frequenza altamente insoddisfacente e sviluppare una funzione di sicurezza in modalità su domanda per abbassare la frequenza degli incidenti mortali al massimo tasso tollerabile, Figura 28.

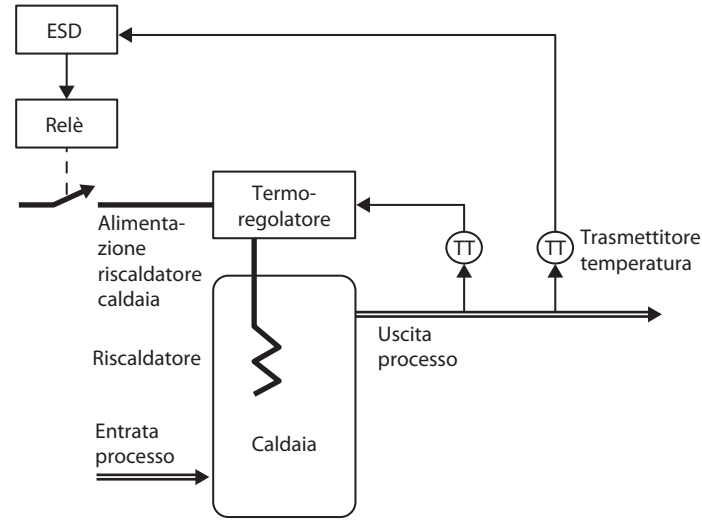


Figura 28: funzione di sicurezza in modalità su domanda

In questa configurazione, abbiamo un secondo trasmettitore di temperatura indipendente che misura la temperatura di uscita e che, in caso di guasto del processo, interrompe l'alimentazione al riscaldatore elettrico attraverso un sistema ESD.

Possiamo dire che:

$$10^{-5} \text{ pa} \geq \lambda_B \times PFD_T$$

dove λ_B è il tasso di guasto della caldaia, $1{,}25 \times 10^{-4}$ pa e PFD_T è la probabilità di guasto su domanda dell'intervento indipendente.

Quindi:

$$PFD_T \leq 10^{-5} \text{ pa} / 1{,}25 \times 10^{-4} \text{ pa}$$
$$PFD_T \leq 0{,}08$$

che è equivalente ad una funzione di sicurezza in modalità su domanda SIL1.

Nota: questi due esempi ci permettono di scegliere se progettare l'intero sistema caldaia e le apparecchiature sotto controllo come SIL2 oppure se permettere al sistema caldaia di guastarsi e proteggerlo con una funzione di sicurezza in modalità su domanda SIL1. Entrambe le opzioni rispondono al massimo rischio tollerabile target ma lo sviluppo di un piccolo sistema SIL1 in modalità su domanda è, in termini di costo, un'opzione più efficiente rispetto ad un sistema di controllo caldaie SIL2.

7. Grafici di rischio

7.1. Introduzione

Le Sezioni [6.10] e [6.11] illustrano il metodo di determinazione dei SIL target mediante calcolo ma i grafici di rischio rappresentano un'utile alternativa, soprattutto se i pericoli da analizzare sono diversi. Il metodo del grafico dei rischi è una tecnica utile e veloce da applicare quando i pericoli da valutare sono diversi.

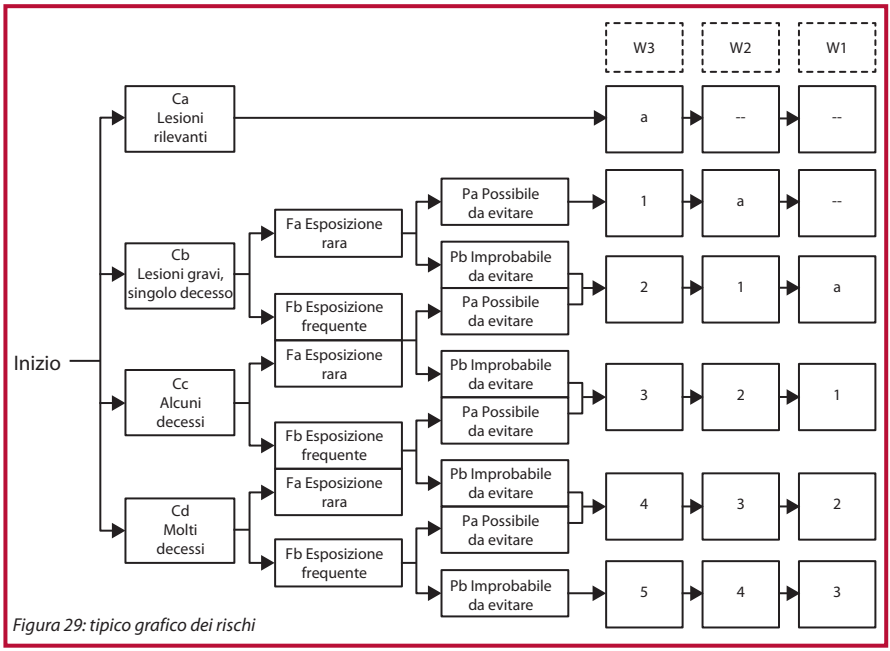


Figura 29: tipico grafico dei rischi

Prima di tutto si determinano le conseguenze del pericolo, Ca, Cb, Cc o Cd.

Quindi, si stima la frequenza o l'esposizione della persona più a rischio, scegliendo tra Fa (esposizione rara) e Fb (esposizione frequente). In genere, se la persona più a rischio ha una probabilità del 10% o meno di ricadere nella portata degli effetti pericolosi, l'esposizione può essere considerata rara. In caso contrario, l'esposizione può essere considerata frequente.

Proseguendo sul grafico dei rischi, se è probabile che la persona a rischio sia in grado di evitare il pericolo (ad es. con la fuga, venendo avvisata o protetta da qualche funzione), possiamo dire che è possibile evitare il pericolo e scegliere quell'opzione sul grafico dei rischi. In caso contrario, dobbiamo presumere che sia improbabile evitare il pericolo ed arriveremo ad una delle righe nelle colonne a destra del grafico dei rischi.

Infine, dobbiamo selezionare la probabilità che il pericolo si verifichi scegliendo la colonna W3 (probabilità di occorrenza relativamente alta), W2 (probabilità di occorrenza bassa) o W1 (probabilità di occorrenza minima). Nel punto in cui si incontrano la riga e la colonna selezionate, possiamo leggere il SIL richiesto.

7.2. Esempio

Ipotizziamo, ad esempio, la possibile tracimazione di un serbatoio di stoccaggio del petrolio ed il rilascio di vapori che potrebbero infiammarsi e provocare diversi decessi sul posto. Abbiamo valutato la frequenza delle operazioni di riempimento e deciso che la probabilità che il pericolo si verifichi potrebbe essere W1 (probabilità minima). Non ci sono mezzi con cui i dipendenti dell'impianto potrebbero evitare il pericolo, nel caso in cui si verificasse. Il personale dell'impianto è sul posto raramente, solo per attività di manutenzione e, generalmente, per meno di 1 ora al giorno. La Figura 30 mostra come utilizzare il grafico dei rischi per ottenere un target SIL1.

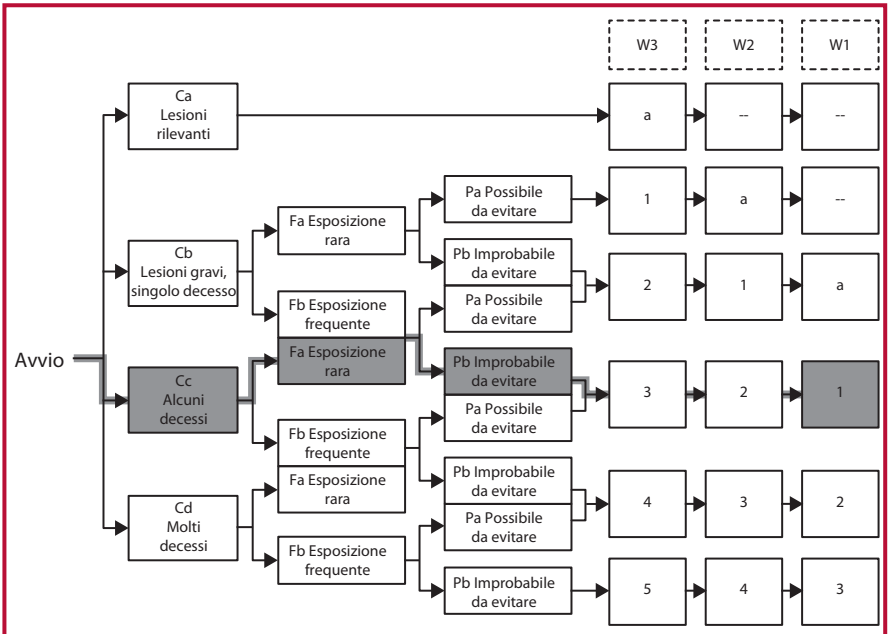


Figura 30: esempio di uso del grafico dei rischi

In questo esempio, la funzione di sicurezza potrebbe essere un dispositivo di intervento che, in caso di livello eccessivo, chiude la valvola di entrata del serbatoio. Corrisponde a un target SIL1.

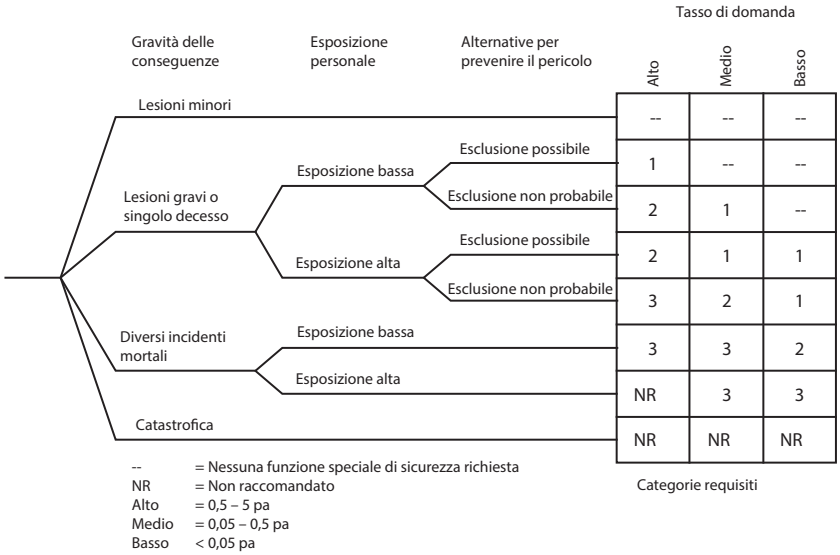
Tuttavia, il convenzionale grafico dei rischi può essere soggettivo e porre problemi di interpretazione dei parametri di rischio. In tal caso, può portare a risultati incoerenti che possono risultare in SIL target pessimistici.

Nel grafico dei rischi illustrato, alcune delle caselle SIL target sono etichettate "a" e "b". I termini SILa e SILb vengono talvolta usati nell'industria, anche se non citati nella norma. SILa, generalmente, significa che dovrebbe essere prevista una qualche riduzione del rischio, ma che non è necessario che il fattore di riduzione del rischio arrivi a SIL1. In altre parole, è necessaria una probabilità PFD compresa tra 1 (nessuna riduzione del rischio) e 0,1 (SIL1). Qualche organizzazione si riferisce a "SILa" come a "(SIL1)".

SILb è in una posizione più alta rispetto a SIL4. Generalmente, con un requisito SIL4, è consigliabile che il processo venga riesaminato perché è semplicemente troppo pericoloso. Un requisito SILb è ancora più pericoloso.

7.3. Esempio

La Figura 31 mostra un esempio di grafico dei rischi simile a quelli utilizzati nell'industria di processo, in cui sono illustrati alcuni dei potenziali problemi associati all'interpretazione dei parametri di rischio.



Alto	Medio	Basso
--	--	--
1	--	--
2	1	--
2	1	1
3	2	1
3	3	2
NR	3	3
NR	NR	NR

Figura 31: grafico dei rischi nell'industria di processo

Il principio d'uso è identico a quello del grafico dei rischi illustrato nella Figura 29 ma, in questo caso, la stima del tasso di domanda è maggiormente guidata.

Se un pericolo può comportare diversi incidenti mortali, con un'esposizione rara ed un tasso di domanda di 0,05/anno, il tasso di domanda ricadrà tra le categorie "Basso" e "Medio" e bisognerà decidere quale colonna scegliere. Adottando un approccio conservativo, si otterrebbe un target SIL3, Figura 32.

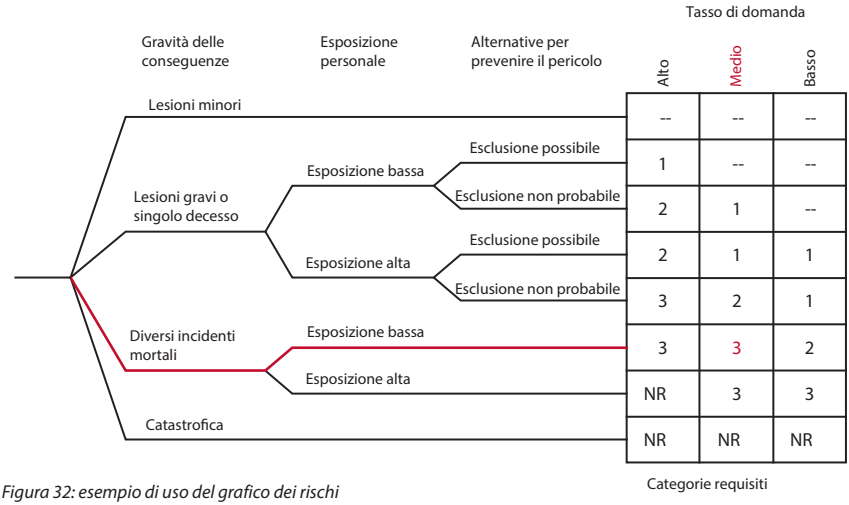


Figura 32: esempio di uso del grafico dei rischi

Un'interpretazione meno cautelativa avrebbe comportato un target SIL2.

7.4. Esempio

La Figura 33 mostra un esempio di una tipica matrice di rischio. Le colonne P, A, E ed R forniscono descrizioni delle possibili conseguenze del pericolo, le frequenze di occorrenza sono descritte in termini qualitativi ed i SIL target si trovano all'incrocio tra le righe e le colonne.

P Persone	A Risorse	E Ambiente	R Reputazione	<0,01/anno	<0,05/anno	<0,25/anno	>2/anno	>2/anno
				A	B	C	D	E
				Mai sperimentato nel settore	Sperimentato nel settore	Sperimentato nella società	Sperimentato diverse volte/anno nella società	Sperimentato diverse volte/anno nello stabilimento
Nessuna lesione	Nessun danno	Nessun effetto	Nessun effetto					(SIL1)
Lesioni lievi (<1/anno)	Danni lievi (<$10K)	Effetti lievi	Impatto lieve				(SIL1)	SIL1
Lesioni minori (<1E-01/anno)	Danni minori (<$100K)	Effetti minori	Impatto minore			(SIL1)	SIL1	SIL2
Lesioni rilevanti (<1E-02/anno)	Danni rilevanti (<$500K)	Effetti localizzati	Impatto considere-vole		(SIL1)	SIL1	SIL2	SIL3
Singolo decesso (<1E-03/anno)	Danni rilevanti (<$10M)	Effetti rilevanti	Impatto nazionale	(SIL1)	SIL1	SIL2	SIL3	N/A
Diversi decessi (<1E-04/anno)	Danni estesi (>$10M)	Effetti rilevanti	Impatto internazio-nale	SIL1	SIL2	SIL3	N/A	N/A

Figura 33: esempio di uso della matrice dei rischi

Sembra essere un approccio diretto ed utile ma, se non si presta attenzione, potrebbero sorgere dei problemi.

A: Le frequenze di occorrenza devono essere quantificate in modo che, oltre ad essere coerenti con la descrizione, risultino anche nel corretto SIL target.

B: "Mai sperimentato nel settore" può essere stimato presumendo, ad esempio, 5000 impianti in funzione per 20 anni che darebbero una frequenza di circa $<10^{-5}$/anno e non di $<10^{-2}$/anno come illustrato. Con un massimo rischio tollerabile di $<10^{-4}$/anno, a cui non corrisponderebbe alcun SIL target.

C: Le massime frequenze di rischio tollerabili devono essere appropriate. Un valore di $<10^{-3}$/anno per un singolo incidente mortale è troppo alto e risulterà in SIL target ottimistici ed in un'inadeguata riduzione del rischio.

D: Per incrementare i SIL target per riga e per colonna come mostrato nella Figura 33, anche le frequenze di occorrenza dovrebbero aumentare di un ordine di grandezza tra ogni colonna.

E: Il SIL target di (SIL1) significa che sono necessarie delle misure di riduzione del rischio ma che non c'è effetto consequenziale. In mancanza di evento pericoloso, non è necessaria alcuna protezione.

F: Infine, per le categorie commerciali, la frequenza di occorrenza dei danni alle risorse dell'impianto deve essere realistica e coerente con il costo di implementazione della SIF richiesta.

La matrice di rischio deve quindi essere calibrata e si suggerisce quanto segue, Figura 34.

P Persone	A Risorse	E Ambiente	R Reputazione	<1E-04/anno	<1E-03/anno	<1E-02/anno	<0,1/anno	>0,1/anno
				A	B	C	D	E
				Mai sperimentato nel settore	Sperimentato nel settore	Sperimentato nella società	Sperimentato diverse volte/anno nella società	Sperimentato diverse volte/anno nello stabilimento
Nessuna lesione	Nessun danno	Nessun effetto	Nessun effetto					
Lesioni lievi (<0,1/anno)	Danni lievi (<$10K)	Effetti lievi	Impatto lieve				(SIL1)	SIL1
Lesioni minori (<1E-02/anno)	Danni minori (<$100K)	Effetti minori	Impatto minore			(SIL1)	SIL1	SIL2
Lesioni rilevanti (<1E-03/anno)	Danni rilevanti (<$500K)	Effetti localizzati	Impatto considere-vole		(SIL1)	SIL1	SIL2	SIL3
Singolo decesso (<1E-04/anno)	Danni rilevanti (<$10M)	Effetti rilevanti	Impatto nazionale	(SIL1)	SIL1	SIL2	SIL3	N/A
Diversi decessi (<1E-05/anno)	Danni estesi (>$10M)	Effetti rilevanti	Impatto internazio-nale	SIL1	SIL2	SIL3	N/A	N/A

Figura 34: calibrazione della matrice dei rischi

7.5. Sommario

Grafici dei rischi e matrici di rischio possono essere molto utili, soprattutto quando utilizzati come tecnica preliminare e veloce per filtrare tutto tranne i SIL più alti, ovvero SIL2 e superiori. Tuttavia, un'attenta calibrazione delle tecniche utilizzate dovrebbe evitare risultati errati dovuti alle insidie qui mostrate.

8. Analisi del livello di protezione (LOPA)

8.1. Introduzione

L'analisi del livello di protezione (LOPA) è un modo strutturato di calcolare i target di riduzione del rischio (ed i SIL). L'analisi LOPA viene realizzata in un incontro simile a quello dello studio HAZOP.

I potenziali pericoli vengono generalmente identificati tramite l'approccio HAZOP [3] ed importati nei fogli di lavoro LOPA, mantenendo così un link tracciabile tra le due analisi, dall'identificazione del pericolo al requisito di riduzione del rischio ed al SIL target. L'analisi LOPA può essere la naturale estensione di un incontro HAZOP.

8.2. Team di studio LOPA

È importante che il team LOPA sia costituito da persone in grado di apportare allo studio il miglior contributo in termini di conoscenza ed esperienza del tipo di impianto da considerare. Un tipico team LOPA è costituito come segue:

Nome	**Ruolo**
Presidente	Persona responsabile di spiegare il processo LOPA, dirigere le discussioni e facilitare l'analisi LOPA. Qualcuno con esperienza nel processo LOPA ma non direttamente coinvolto nel progetto, per assicurare che il metodo venga seguito attentamente.
Segretario	Persona responsabile di registrare la discussione dell'incontro LOPA e fornire l'analisi on-line dei target SIL. Qualcuno che registri raccomandazioni o azioni.
Ingegnere di processo	Generalmente l'ingegnere responsabile del diagramma di flusso del processo e dello sviluppo degli schemi dell'impianto e della strumentazione (P&ID).
Utente/Operatore	Persona responsabile di consigliare sull'uso e l'operabilità del processo, oltre che sull'effetto delle deviazioni.
Specialista C&I	Persona in possesso delle corrispondenti conoscenze tecniche di controllo e strumentazione.
Manutentore	Persona coinvolta nella manutenzione del processo.
Rappresentante del team di progetto	Persona esperta sulla progettazione in grado di fornire informazioni specifiche.

8.3. Informazioni utilizzate nello studio LOPA

A disposizione del team LOPA, dovrebbero esserci i seguenti elementi:

- P&ID della struttura;
- Documenti di descrizione o concezione del processo;
- Procedure operative e di manutenzione;
- Layout dell'impianto.

8.4. Determinazione dei SIL target

La tecnica LOPA, come descritta nel documento AIChE Centre for Chemical Process Safety, Layer of Protection Analysis, 2001 [19.4] può essere utilizzata per stabilire i SIL target.

L'analisi LOPA considera i pericoli identificati con altri strumenti (ad es. HAZOP) ma può essere condotta nell'ambito di un incontro HAZOP, per valutare ogni pericolo nel momento in cui viene identificato.

Il team LOPA considera ogni pericolo identificato e documenta le cause innescanti ed i livelli di protezione che prevengono o limitano il pericolo. Successivamente, viene determinata l'entità totale di riduzione del rischio ed analizzato il bisogno di un'ulteriore riduzione. Se occorre fornire protezione aggiuntiva sotto forma di un sistema SIS, la metodologia consente la determinazione del SIL appropriato e della PFD richiesta.

Il processo LOPA viene registrato nei fogli di lavoro LOPA che permettono di quantificare gli eventi scatenanti e le loro frequenze, oltre che di attestare la riduzione del rischio fornita dai livelli di protezione indipendenti. Le intestazioni del foglio di lavoro sono descritte nelle seguenti sezioni, insieme ad un esempio di analisi LOPA [8.5].

8.5. Esempio di analisi LOPA

Considerando l'esempio del serbatoio di pressione [3.7], è possibile importare i pericoli identificati nel foglio di lavoro LOPA ed analizzare i rischi.

8.6. Fogli di lavoro LOPA

8.6.1. Introduzione

Le sezioni che seguono descrivono le intestazioni del foglio di lavoro e forniscono istruzioni sulla quantificazione.

In questo capitolo, è riportato un esempio di foglio di lavoro LOPA.

8.6.2. ID/rif. pericolo

Fornisce un identificativo per ogni pericolo. Nell'esempio, il pericolo considerato per l'analisi è il rif. **1.10: Alta pressione nel serbatoio.** Questo riferimento fornisce la tracciabilità all'indietro con altri studi (in questo caso, HAZOP) e, con l'avanzamento del progetto, fornisce tracciabilità in avanti con l'assegnazione della funzione SIF e la verifica del SIL.

8.6.3. Descrizione evento (pericolo)

Fornisce una descrizione del pericolo potenziale identificato.

8.6.4. Conseguenza

Descrive la conseguenza del pericolo. Nell'analisi LOPA di esempio, abbiamo analizzato le conseguenze del pericolo in termini di sicurezza del personale, rischi per l'ambiente e rischi per le risorse dell'impianto ovvero rischi commerciali.

8.6.5. Categoria di gravità (Cat. grav.)

La gravità delle conseguenze documentate può essere categorizzata e derivata da una tabella di classificazione dei rischi, ad esempio la Tabella 5.

8.6.6. Massimo rischio tollerabile (MTR)

La massima frequenza tollerabile della conseguenza del pericolo, come applicata alla sicurezza del personale ma generalmente applicata anche all'ambiente, alla reputazione dell'organizzazione ed al danno potenziale all'ambiente, alla reputazione della società ed ai costi commerciali derivanti dal danneggiamento delle risorse dell'impianto, dalla perdita di profitto o dalla sicurezza di approvvigionamento. Le massime frequenze tollerabili utilizzate dovrebbero essere in linea con la guida HSE, ad es. R2P2 [19.3] per lasicurezza.

Le massime frequenze tollerabili per i rischi ambientali, di reputazione e commerciali, tuttavia, dovrebbero essere decise dalla società. I valori tipici che potrebbero essere utilizzati sono illustrati nella Tabella 5.

Conseguenza	Cat. grav.	Frequenza target dei rischi (/anno)	Descrizione delle conseguenze	
			Nello stabilimento	**Fuori dallo stabilimento**
Persone (sicurezza)	P1	1,0E-01	Trattamento medico dei dipendenti o lesioni che limitano la capacità di lavoro	Trattamento medico o lesioni che limitano la capacità di lavoro (terze parti)
	P2	1,0E-02	Tempo perduto per incidente (LTA) dei dipendenti senza effetto permanente	LTA (terze parti) senza effetto permanente
	P3	1,0E-03	Effetto permanente dipendenti	Senza effetti permanenti
	P4	1,0E-04	1 incidente mortale dipendenti e/o diverse disabilità permanenti	Effetti permanenti (terze parti)
	P5	1,0E-05	Diversi incidenti mortali dipendenti (2 – 10)	Singolo incidente mortale terze parti e/o diverse disabilità permanenti
	P6	1,0E-06	Diversi incidenti mortali dipendenti (oltre 10)	Diversi incidenti mortali terze parti
Ambiente	E1	1,0E-01	Nessuna dichiarazione alle autorità ma necessità di bonifica	Nessuna dichiarazione alle autorità ma necessità di bonifica di lieve entità (ad es. versamento di 1 – 100 litri con kit implementato)
	E2	1,0E-02	Dichiarazione alle autorità, ma senza conseguenze ambientali	Dichiarazione alle autorità, ma senza conseguenze ambientali (ad es. versamento di > 100 litri in locali del cliente confinati/intercettati)
	E3	1,0E-03	Moderato inquinamento nei limiti dello stabilimento	Moderato inquinamento che richiede lavori di bonifica (ad es. con fumo in uscita dal sito che rimane comunque operativo)
	E4	1,0E-04	Significativo inquinamento nei limiti dello stabilimento. Evacuazione di persone/temporanea chiusura dello stabilimento O significativo inquinamento esterno allo stabilimento. Evacuazione di persone. (ad es. versamento fuori dallo stabilimento alla stazione di servizio)	Significativo inquinamento esterno allo stabilimento. Evacuazione di persone. (ad es. versamento fuori dallo stabilimento alla stazione di servizio)
	E5	1,0E-05	Vedere le conseguenze "Fuori dallo stabilimento"	Importante inquinamento con conseguenze ambientali reversibili esterne allo stabilimento. (ad es. incidente di grave entità per l'ambiente)
	E6	1,0E-06	Vedere le conseguenze "Fuori dallo stabilimento"	Grave e sostenuto inquinamento esterno allo stabilimento e/o estensiva perdita di vita acquatica (ad es. perdita del carico di una nave)
Costo	C1	1,0E-01	Perdita <€10K	N/A
	C2	1,0E-02	Perdita €10K < €100K	N/A
	C3	1,0E-03	Perdita €100K < €1,0M	N/A
	C4	1,0E-04	Perdita €1,0M < €10M	N/A
	C5	1,0E-05	Perdita €10M < €100M	N/A
	C6	1,0E-06	Perdita ≥ €100M	N/A
Reputazione	R1	1,0E-01	Senza pubblicità. Comunità locale interessata.	N/A
	R2	1,0E-02	Stampa locale	N/A
	R3	1,0E-03	Stampa nazionale	N/A
	R4	1,0E-04	Televisione nazionale	N/A
	R5	1,0E-05	Stampa internazionale	N/A
	R6	1,0E-06	Televisione internazionale	N/A

Tabella 5: criteri di rischio

Va sottolineato che, quando applicata alla sicurezza personale, questa rappresenta la frequenza a cui l'individuo più a rischio è esposto al pericolo.

8.6.7. Causa scatenante

Elenca le cause identificate del pericolo. Queste cause vengono determinate durante l'incontro LOPA in base all'esperienza dei partecipanti. Per il pericolo di esempio (sovrappressione), nella Tabella 6 sono riportate le potenziali cause scatenanti, le loro frequenze di occorrenza e la fonte dei dati. L'analisi LOPA dovrebbe fornire visibilità a tutti i dati, presentando tutti gli eventi scatenanti e le frequenze, con riferimento alle fonti dei dati, in questo modo.

Causa scatenante	**Frequenza della causa scatenante (pa)**	**Fonte dati**
Il sistema DCS non controlla la pressione.	1,65E-02	Exida 2007, articolo x.x.x
Il sensore di livello del liquido LL101 è guasto e legge un basso livello.	1,10E-02	Exida 2007, articolo x.x.x
Il trasmettitore TT100 è guasto e legge una bassa temperatura.	2,68E-03	Exida 2007, articolo x.x.x
Il trasmettitore PT102 è guasto e legge una bassa pressione.	8,58E-04	Exida 2007, articolo x.x.x
Guasto in chiusura della valvola di esportazione gas FCV102.	1,01E-02	Oreda 2002, articolo x.x.x
Guasto in apertura della valvola del gas combustibile FCV100.	1,01E-02	Oreda 2002, articolo x.x.x
Guasto in chiusura della valvola di esportazione del liquido XV102.	2,89E-03	Oreda 2002, articolo x.x.x
Guasto in apertura della valvola di importazione del liquido XV102.	2,89E-03	Oreda 2002, articolo x.x.x

Tabella 6: eventi scatenanti e frequenze

8.6.8. Frequenza della causa scatenante (/anno), colonna [a]

Quantifica il tasso di occorrenza previsto della causa scatenante. Questo tasso può essere stimato in base all'esperienza dei partecipanti ed a qualunque dato storico disponibile o può essere acquisito da adeguate fonti sui tassi di guasto [14.6].

Gli eventi scatenanti e le loro frequenze di occorrenza sono presentati nella Tabella 6.

Quando basate su fattori umani quali l'errore di un operatore, le frequenze della cause scatenanti possono essere difficile da stimare. Una tecnica è quella di basare la stima sulla frequenza delle opportunità che ha un operatore di compiere un errore, per poi moltiplicarla per la probabilità che ha di compiere un errore pericoloso.

Ipotizziamo che, chiudendo una valvola, un operatore possa innescare una condizione di sovrappressione in una condotta. Generalmente, prima di chiudere la valvola principale,

l'operatore apre una valvola di bypass ed esegue questa operazione ogni mese. La frequenza di base λ_B per questa attività è quindi di 12 all'anno (una volta al mese).

Presumendo che l'operatore sia ben formato, che il compito sia di routine e che egli non sia soggetto a stress, possiamo stimare che la probabilità che ha di compiere un errore P_E (ad es. non aprire prima la valvola di bypass) sia dell'1%. La frequenza dell'evento innescante λ_{INIT} può essere stimata come:

$$\lambda_{INIT} = \lambda_B \times P_E$$
$$\lambda_{INIT} = 12 \times 1\%/\text{anno}$$
$$\lambda_{INIT} = 0{,}12/\text{anno}$$

In genere, su questi dati è possibile realizzare una verifica basata sulla sensibilità chiedendo ai partecipanti all'analisi LOPA se hanno qualche esperienza del verificarsi di un tale evento o se ritengono che la frequenza sia ragionevole. Una frequenza di 0,12/anno è equivalente ad un errore ogni 8 anni.

8.6.9. Modificatori condizionali

Distribuzione della grandezza delle perdite, colonna [b]

Nell'esempio, le conseguenze postulate del pericolo di sovrappressione si verificano solo in caso di rottura di un serbatoio. Si potrebbe sostenere che la maggior parte delle condizioni di sovrappressione non comporterebbe la perdita di contenimento o una fuga di lieve entità da una flangia, ad esempio. In questo caso, il team LOPA ha stimato che solo il 10% degli eventi innescanti avrebbe delle conseguenze.

Probabilità di innesco, colonna [c]

Per le conseguenze di sicurezza e commerciali postulate, il gas rilasciato dovrebbe infiammarsi. In questo esempio, abbiamo fatto riferimento ad uno studio di sicurezza antincendio che ha previsto il 75% di probabilità di innesco, in caso di rottura importante. Per le conseguenze di sicurezza, quindi, possiamo attestare come modificatore condizionale 0,75 e la frequenza dell'evento scatenante verrà ridotta di questo fattore.

Per le conseguenze ambientali, non può essere attestata alcuna riduzione del rischio dato che, per le conseguenze, l'accensione non è necessaria.

Soluzione generica, colonna [d]

Un esempio di soluzione generica potrebbe essere un tubo rivestito atto a proteggere dalla perdita di contenimento. Nell'esempio, la soluzione generica non è stata considerata perché non prevedeva specifiche caratteristiche in grado di fornire una qualunque riduzione del rischio.

8.6.10. Livelli di protezione indipendenti (IPL)

Ogni livello di protezione è costituito da un insieme di apparecchiature e/o di controlli amministrativi che funzionano in sinergia con gli altri livelli.

Il livello di protezione fornito da ogni livello IPL è quantificato dalla probabilità che non riuscirà ad eseguire la funzione specificata su domanda, la probabilità PFD, un valore adimensionale compreso tra 0 e 1. Al diminuire del valore della probabilità PFD, aumenta il fattore di riduzione del rischio che viene applicato come fattore modificante, alla frequenza della causa scatenante calcolata [8.6.8]; quindi, dove non viene attestato alcun livello IPL, nel foglio di lavoro LOPA viene inserito "1".

Nell'esempio, i livelli IPL attestati nelle colonne da [e] a [h] possono essere personalizzati in base all'applicazione. Quelli presentati sono i livelli IPL tipici.

Sistema di controllo di processo di base (BPCS), colonna [e].

Può essere preso in considerazione se un anello di controllo nel sistema BPCS (DCS) previene il verificarsi di un pericolo derivante da una potenziale causa scatenante. Nell'esempio, il sistema BPCS (DCS) può compensare alcune delle cause scatenanti (ad es. la mancata apertura valvola di importazione del liquido XV102) aprendo la valvola di esportazione del liquido e prevenendo una condizione di livello eccessivo. È stata attestata una probabilità PFD di 0,1 e ciò significa che il sistema DCS sarà in grado di prevenire le conseguenze in 9 eventi su 10.

Una probabilità PFD di 0,1 è generalmente la massima riduzione del rischio attestabile per un sistema non classificato SIL. Questo perché il sistema DCS può essere regolato manualmente, il controllo sulle impostazioni del punto di intervento non è così rigido ed il regime di collaudo non è così rigoroso come per un sistema SIS.

Allarmi indipendenti, colonna [f].

È possibile considerare allarmi, indipendenti dal sistema BPCS, che avvisino l'operatore e ne richiedano l'azione. L'allarme può essere considerato solo se realmente indipendente dal sistema BPCS e dalla funzione SIF e solo se l'operatore può rispondere all'allarme e intervenire rendendo il processo sicuro entro il tempo di processo sicuro.

Generalmente, per gli allarmi indipendenti, può essere rivendicata una probabilità PFD di 0,1. In questo esempio, non sono stati considerati.

8.6.11. Mitigazione aggiuntiva

Presenza, colonna [g].

Accesso – I livelli di mitigazione possono includere la presenza ovvero l'intervallo di tempo durante cui un operatore è esposto ad un pericolo ed ha accesso limitato alle zone pericolose. In questo esempio, è stata attestata una presenza basata su un turno di 8 ore.

Altra mitigazione: colonna [h].

Un'ulteriore mitigazione è possibile nelle seguenti forme:

- Fisica – Livelli di mitigazione possono essere barriere fisiche che proteggano dal pericolo una volta innescato. Ad esempio, dispositivi di sfiato della pressione e muri di protezione.
- Azione dell'operatore – Possono essere considerati il rilevamento e l'ispezione ad intervalli regolari, a condizione che l'operatore possa agire in maniera efficace.

In questo esempio, non sono stati considerati.

8.6.12. Frequenza degli eventi di livello intermedio

La frequenza di eventi intermedi viene calcolata moltiplicando la frequenza della causa scatenante per le probabilità PFD dei livelli di protezione. Il numero calcolato è in unità di eventi all'anno. La frequenza totale di eventi di livello intermedio indica il tasso di domanda su qualunque funzione SIF proposta.

8.6.13. PFD richiesta dal sistema SIS

Calcolata confrontando il massimo rischio tollerabile (λMTR) con la frequenza di eventi di livello intermedio o la frequenza del pericolo (λ_{HAZ}).

$$PFD = \lambda_{MTR}/\lambda_{HAZ}$$

8.6.14. SIL richiesto dal sistema SIS

Ottenuto dalla Tabella 7 e corrispondente alla probabilità PFD richiesta dal sistema SIS.

Livello SIL	**Modalità su domanda** Probabilità di guasto su domanda	**Modalità continua** Tasso di guasto all'ora
SIL4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
SIL3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
SIL2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
SIL1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Tabella 7: PFD specificata dal livello SIL e tassi di guasto

Va osservato che la probabilità PFD ed il tasso di guasto di ogni livello SIL dipendono dalla modalità di funzionamento in cui si prevede che venga utilizzato il sistema SIS rispetto alla frequenza delle domande di intervento [8.6.12].

Di seguito, sono riportati i fogli di lavoro LOPA.

Analisi del livello di protezione (LOPA)

ID/Rif.	Descrizione zona	Descrizione evento (pericolo)	Conseguenza	Categoria di gravità	Massimo rischio tollerabile (pa)	Causa scatenante	Frequenza della causa scatenante (pa)	Distribuzione della grandezza delle perdite	Probabilità di accensione	Design generale (design nominale)	Livelli di protezione indipendenti				Frequenza eventi di livello intermedio (pa)	SRS PFD richiesta	SRS SIL richiesto	Commenti/ipotesi
											BPCS [DCS]	Allarmi indipendenti	Mitigazione ad opera dell'Occupazione (livelli di presidio)	Mitigazione ad opera di ES, ad es. pareti tagliafuoco, in atto Procedure/ valvole di sfiato				
							[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]				
1.10	Serbatoio	Alta pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Sicurezza: Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due dei manutentori.	P5	1,00E-05	Il DCS non controlla la pressione.	1,65E-02	0,10	0,75				0,33		4,13E-04	1,87E-02	SIL1	[a] Vedere i dati degli eventi scatenanti. [b] Il team LOPA stima la probabilità di grandi perdite (rottura) al 10%. [c] Lo studio sul rischio di incendio stima la probabilità di accensione al 75%. [d] Nessuna considerazione delle caratteristiche di progetto. [e] Il DCS è la causa scatenante, quindi nessuna considerazione del DCS. [f] Nessun allarme indipendente disponibile. Nessuna considerazione. [g] Area del serbatoio occupata 8 ore al giorno. [h] Nessuna valvola di sfiato della pressione. Nessuna considerazione.
						Il trasmettitore PT102 è guasto a legge bassa pressione	8,58E-04	0,10	0,75				0,33		2,15E-05			Come sopra.
						Guasto in apertura della valvola di importazione del liquido XV102.	2,89E-03	0,10	0,75		0,10		0,33		7,23E-06			Come sopra tranne che: [e] Il DCS può compensare i guasti della valvola di importazione. Stima PFD = 0,1.
						Guasto in chiusura della valvola di esportazione gas FCV102.	1,01E-02	0,10	0,75		0,10		0,33		2,52E-05			Come sopra.
						Guasto in chiusura della valvola di esportazione del liquido XV102.	2,89E-03	0,10	0,75		0,10		0,33		7,23E-06			Come sopra.
						Il trasmettitore TT100 è guasto a legge bassa temperatura	2,68E-03	0,10	0,75		0,10		0,33		6,70E-06			Come sopra.
						Guasto in apertura della valvola del gas combustibile FCV100.	1,01E-02	0,10	0,75		0,10		0,33		2,52E-05			Come sopra.
						Il sensore LL101 è guasto e legge basso livello del liquido.	1,10E-02	0,10	0,75		0,10		0,33		2,74E-05			Come sopra.
															5,34E-04			

ID/Rif.	Descrizione zona	Descrizione evento (pericolo)	Conseguenza	Categoria di gravità	Massimo rischio tollerabile (pa)	Causa scatenante	Frequenza della causa scatenante (pa)	Distribuzione della grandezza delle perdite	Probabilità di accensione	Design generale (design nominale)	Livelli di protezione indipendenti				Frequenza eventi di livello intermedio (pa)	SRS PFD richiesta	SRS SIL richiesto	Commenti/Ipotesi
											BPCS [DCS]	Allarmi indipendenti	Mitigazione aggiuntiva: Occupazione (livelli di presidio)	Mitigazione aggiuntiva, ad es. pareti tagliafuoco, in atto Procedure/ valvole di sfiato				
							[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]				
1.10	Serbatoio	Alta pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Ambientale: Rottura serbatoio, fuga di gas, senza accensione. Rilascio nello stabilimento. Bonifica e dichiarazione alle autorità ma senza conseguenze ambientali.	E2	1,00E-02	Il DCS non controlla la pressione.	1,65E-02	0,10							1,65E-03	Nessuna	Nessuna	[a] Vedere i dati degli eventi scatenanti. [b] Il team LOPA stima la probabilità di grandi perdite (rottura) al 10%. [c] Accensione non richiesta Nessuna attestazione di riduzione del rischio [d] Nessuna considerazione delle caratteristiche di progetto. [e] Il DCS è la causa scatenante, quindi nessuna considerazione del DCS. [f] Nessun allarme indipendente disponibile. Nessuna considerazione. [g] Ambiente a rischio 24 ore/giorno. Nessuna attestazione di riduzione del rischio. 8 ore al giorno. [h] Nessuna valvola di sfiato della pressione. Nessuna considerazione.
						Il trasmettitore PT102 è guasto e legge bassa pressione	8,58E-04	0,10							8,58E-05			Come sopra.
						Guasto in apertura della valvola di importazione del liquido XV102.	2,89E-03	0,10			0,10				2,89E-05			Come sopra tranne che: [e] Il DCS può compensare I guasti della valvola di importazione. Stima PFD = 0,1.
						Guasto in chiusura della valvola di esportazione gas FCV102.	1,01E-02	0,10			0,10				1,01E-04			Come sopra.
						Guasto in chiusura della valvola di esportazione del liquido XV102.	2,89E-03	0,10			0,10				2,89E-05			Come sopra.
						Il trasmettitore TT100 è guasto e legge bassa temperatura	2,68E-03	0,10			0,10				2,68E-05			Come sopra.
						Guasto in apertura della valvola del gas combustibile FCV100.	1,01E-02	0,10			0,10				1,01E-04			Come sopra.
						Il sensore LL101 è guasto e legge basso livello del liquido.	1,10E-02	0,10			0,10				1,10E-04			Come sopra.
															2,14E-03			

ID/Rif.	Descrizione zona	Descrizione evento (pericolo)	Conseguenza	Categoria di gravità	Massimo rischio tollerabile (pa)	Causa scatenante	Frequenza della causa scatenante (pa)	Distribuzione della grandezza delle perdite	Probabilità di accensione	Design generale (design nominale)	Livelli di protezione indipendenti				Frequenza eventi di livello intermedio (pa)	SRS PFD richiesta	SRS SIL richiesto	Commenti/Ipotesi
											BPCS [DCS]	Allarmi indipendenti	Mitigazione aggiuntiva: Occupazione (livelli di presidio)	Mitigazione aggiuntiva, ad es. pareti tagliafuoco, in atto Procedure/ valvole di sfiato				
							[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]				
1.10	Serbatoio	Alta pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Commerciale: Rottura serbatoio, fuga di gas, accensione e danni alle risorse dell'impianto. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e perdita di produzione per 1 anno	C5	1,00E-05	Il DCS non controlla la pressione.	1,65E-02	0,10	0,75						1,24E-03	6,24E-03	SIL2	[a] Vedere i dati degli eventi scatenanti. [b] Il team LOPA stima la probabilità di grandi perdite (rottura) al 10%. [c] Lo studio sul rischio di incendio stima la probabilità di accensione al 75%. [d] Nessuna considerazione delle caratteristiche di progetto. [e] Il DCS è la causa scatenante, quindi nessuna considerazione del DCS. [f] Nessun allarme indipendente disponibile. Nessuna considerazione. [g] Area del serbatoio occupata 8 ore al giorno. [h] Nessuna valvola di sfiato della pressione. Nessuna considerazione.
						Il trasmettitore PT102 è guasto e legge bassa pressione	8,58E-04	0,10	0,75						6,44E-05			Come sopra.
						Guasto in apertura della valvola di importazione del liquido XV102.	2,89E-03	0,10	0,75		0,10				2,17E-05			Come sopra tranne che: [e] Il DCS può compensare i guasti della valvola di importazione. Stima PFD = 0,1.
						Guasto in chiusura della valvola di esportazione gas FCV102.	1,01E-02	0,10	0,75		0,10				7,56E-05			Come sopra.
						Guasto in chiusura della valvola di esportazione del liquido XV102.	2,89E-03	0,10	0,75		0,10				2,17E-05			Come sopra.
						TT100 è guasto e legge bassa temperatura	2,68E-03	0,10	0,75		0,10				2,01E-05			Come sopra.
						Guasto in apertura della valvola del gas combustibile FCV100.	1,01E-02	0,10	0,75		0,10				7,56E-05			Come sopra.
						Il sensore LL101 è guasto e legge basso livello del liquido.	1,10E-02	0,10	0,75		0,10				8,21E-05			Come sopra.
															1,60E-03			

8.6.15. Risultati LOPA

I risultati (Tabella 8) mostrano che il pericolo di sovrappressione ha conseguenze di sicurezza che possono essere protette con una funzione SIF SIL1 con PFD ≤ 1,87E-02, escludendo il rischio commerciale che richiede una funzione SIF SIL2 con PFD ≤ 8,24E-03.

Pericolo	**Conseguenza**	**Target SIL**	**Target PFD**
Sicurezza	Sicurezza: Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori.	SIL1	1,87E-02
Ambientale	Ambientale: Rottura serbatoio, fuga di gas, senza innesco. Rilascio nello stabilimento. Bonifica e dichiarazione alle autorità ma senza conseguenze ambientali.	Nessuno	Nessuna
Commerciale	Commerciale: Rottura serbatoio, fuga di gas, innesco e danni alle risorse dell'impianto. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e perdita di produzione per 1 anno.	SIL2	6,24E-03

Tabella 8: risultati LOPA

Non è inusuale che siano i pericoli non legati alla sicurezza a prevalere. In questo esempio, le risorse dell'impianto sono costantemente a rischio mentre, in termini di sicurezza, il personale è a rischio solo per parte del tempo.

La funzione SIF che deve essere sviluppata per proteggere dalla sovrappressione dovrebbe quindi rispondere ai target commerciali e, in tal modo, proteggerà adeguatamente anche il personale.

9. Assegnazione delle funzioni di sicurezza

9.1. Fasi del ciclo di vita

La Figura 35 mostra la fase del ciclo di vita in questione.

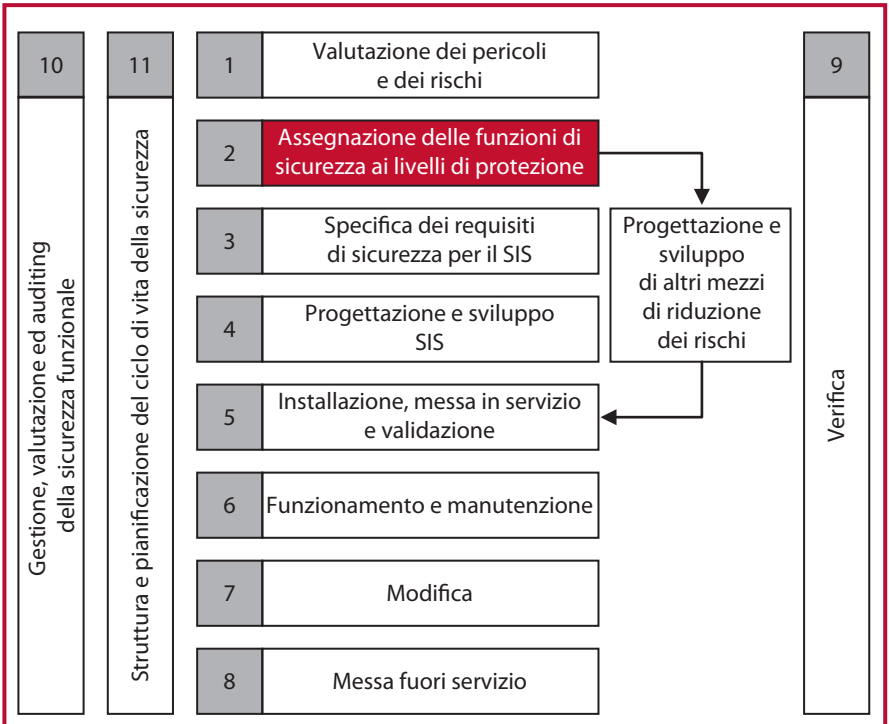


Figura 35: ciclo di vita – Fase 2

L'obiettivo di questa fase come definito nella norma IEC 61511-1, 9.1 è quello di assegnare le funzioni di sicurezza ai livelli di protezione.

Come input, la fase richiede una descrizione dei requisiti della funzione di sicurezza e dei requisiti dell'integrità della sicurezza.

Come output, la fase deve fornire informazioni sull'assegnazione delle funzioni di sicurezza globali, le loro misure di guasto target ed i livelli associati di integrità della sicurezza. Inoltre, devono essere definite le ipotesi elaborate su altre misure di riduzione del rischio che devono essere gestite per tutta la vita del processo/impianto.

9.2. Assegnazione delle funzioni di sicurezza

Facendo riferimento all'esempio del serbatoio separatore (3.7.1), sono stati identificati i seguenti requisiti SIF e SIL (Tabella 9). L'analisi del riferimento 1.10 è stata illustrata nell'ambito dell'esempio fatto per l'analisi LOPA [8.5]. Attraverso l'analisi LOPA, sono stati determinati i livelli SIL e le probabilità PFD target per gli altri pericoli identificati.

Rif. HAZOP	Pericolo	Conseguenza	Target SIL	Target PFD
1.01	Alta pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	SIL2	6,24E-03
1.11	Bassa pressione che provoca la rottura del serbatoio ed il rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	Nessuno	Nessuna
1.15	Alta temperatura che porta ad alta pressione, rottura del serbatoio e rilascio di gas.	Il gas rilasciato si infiamma a contatto del bruciatore e delle superfici calde. Possibile incidente mortale per due manutentori. Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 1 anno. Rilascio nell'ambiente di lieve entità.	Nessuno	Nessuna
1.16	Bassa temperatura, potenziale congelamento del liquido (solidificazione), rottura del serbatoio e perdita di contenimento.	Danni alle apparecchiature che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi. Rilascio nell'ambiente con ordine di notifica.	Nessuno	Nessuna
1.20	Livello elevato nel serbatoio che potrebbe comportare il riversamento di liquido nel gas di esportazione.	Danni alle apparecchiature a valle che richiedono la sostituzione del serbatoio stimata a €10M e lo spegnimento del processo per 6 mesi.	SIL1	8,10E-02
1.21	Basso livello nel serbatoio che potrebbe comportare il trafilamento di gas nel liquido di esportazione.	Danni alle apparecchiature a valle che richiedono la pulizia del serbatoio stimata a €2M e lo spegnimento del processo per 6 settimane.	SIL1	6,22E-02

Tabella 9: requisiti SIF

Assegnazione delle funzioni di sicurezza

La frequenza di eventi intermedi indicata dall'analisi LOPA ha determinato che tutte le funzioni SIF proposte sono in modalità su domanda. Per le condizioni di alto e basso livello, sono stati stabiliti target SIL1 e proposte le seguenti funzioni SIF. Per mitigare le condizioni di alta pressione, è stata implementata una valvola di scarico della pressione e determinata una funzione SIF come illustrato di seguito.

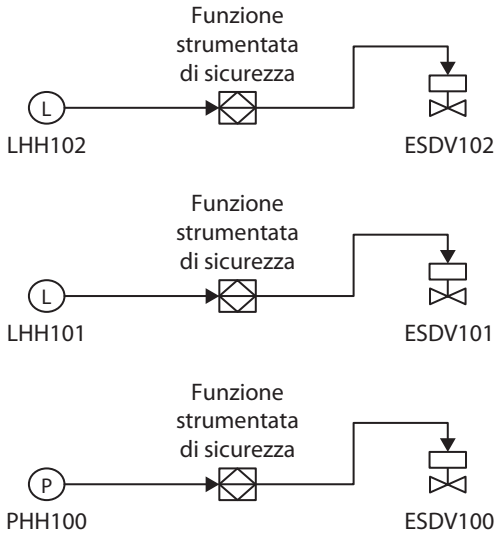


Figura 35a: ciclo di vita – Fase 2

Le singole funzioni SIF formano, nel loro insieme, il sistema SIS globale:

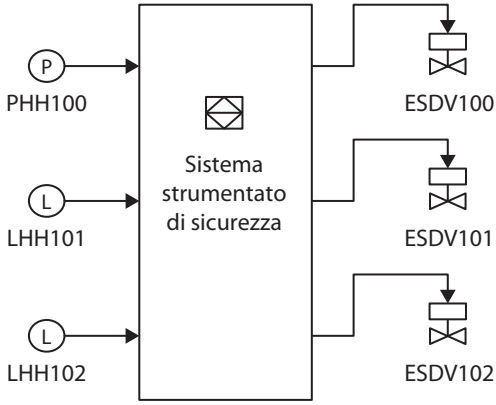


Figura 35b: ciclo di vita – Fase 2

Lo schema che segue evidenzia le funzioni SIF assegnate:

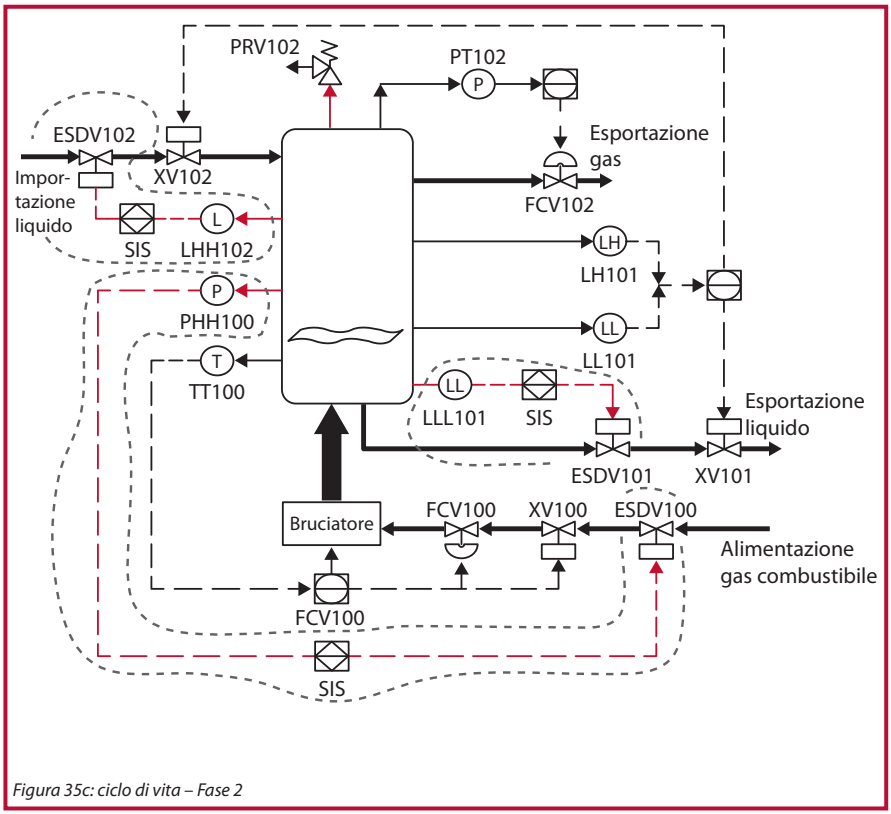


Figura 35c: ciclo di vita – Fase 2

10. Specifica dei requisiti di sicurezza per il sistema SIS

10.1. Fasi del ciclo di vita

La Figura 36 mostra la fase del ciclo di vita in questione.

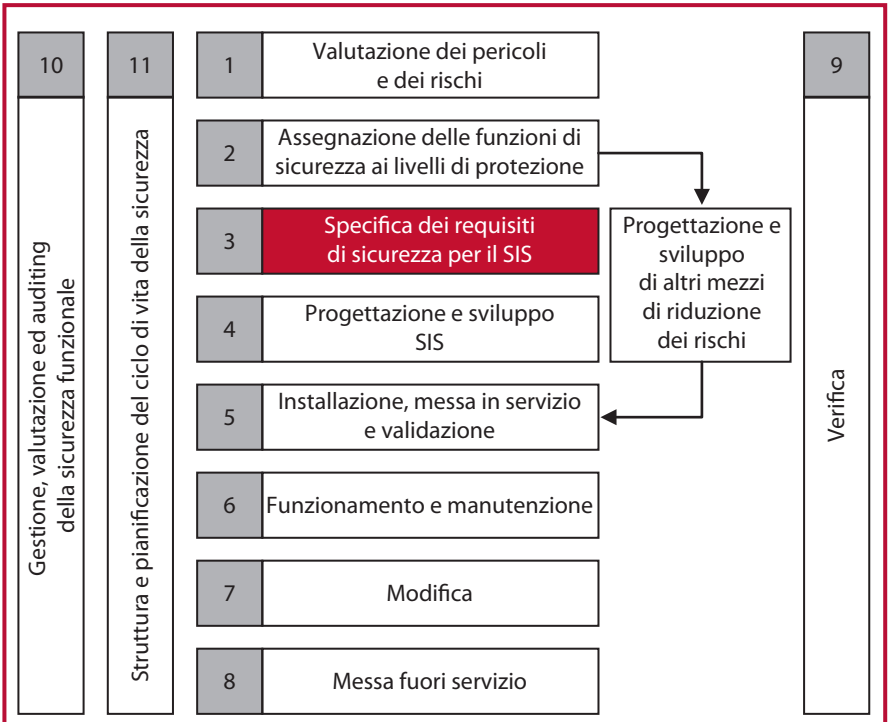


Figura 36: ciclo di vita – Fase 3

L'obiettivo di questa fase come definito nella norma IEC 61511-1, 10.1 è quello di specificare i requisiti delle funzioni SIF.

10.2. Requisiti di integrità della sicurezza di una funzione SIF

Il livello SIL di ogni funzione SIF è stato selezionato durante lo studio di determinazione del livello SIL mediante il grafico dei rischi, l'analisi LOPA o la matrice dei rischi.

Ora, queste informazioni devono essere comunicate al team di progetto mediante la specifica dei requisiti di sicurezza (SRS) per garantire che, durante l'implementazione, il progetto soddisfi i requisiti di integrità della sicurezza SIF. La specifica SRS è la base della validazione delle funzioni SIF.

10.3. Quadro di riferimento per la specifica SRS

Prima di iniziare qualunque attività di progetto, è necessario preparare la specifica SRS in base alle istruzioni fornite nella norma IEC 61511-1/2, articoli 10 e 12. La specifica SRS contiene i requisiti funzionali e di integrità di ogni funzione SIF e dovrebbe fornire informazioni sufficienti a progettare e sviluppare il sistema SIS. La specifica dovrebbe essere espressa e strutturata in modo da essere chiara, precisa, verificabile, mantenibile e fattibile, favorendone la comprensione da parte di chi dovrà usare tali informazioni in una qualunque fase del ciclo di vita.

La specifica SRS dovrebbe includere, per ogni funzione SIF, le seguenti informazioni:

- Descrizione della funzione SIF;
- Guasti per causa comune;
- Definizione dello stato sicuro della funzione SIF;
- Tasso di domanda;
- Intervalli di prova funzionale;
- Tempi di risposta per portare il processo ad uno stato sicuro;
- SIL e modalità di funzionamento (su domanda o continua);
- Misure di processo e relativi punti di intervento;
- Azioni di output del processo e criteri di funzionamento di successo;
- Relazioni funzionali tra input ed output;
- Requisiti di spegnimento manuale;
- Eccitazione o diseccitazione all'intervento;
- Ripristino dopo uno spegnimento;
- Massimo tasso ammesso di interventi di protezione indesiderati;
- Modalità di guasto e risposta SIS ai guasti;
- Avviamento e riavviamento del sistema SIS;
- Interfacce tra il sistema SIS e gli altri sistemi;
- Software applicativo;
- Override/inibizioni/bypass e relative modalità di azzeramento;
- Azioni che seguono il rilevamento di un guasto del sistema SIS.

Il sistema SIS può eseguire funzioni strumentate non relative alla sicurezza per garantire procedure di spegnimento gestite o procedure di avviamento più rapide.

11. Progettazione e sviluppo del sistema SIS

11.1. Fasi del ciclo di vita

La Figura 37 mostra la fase del ciclo di vita in questione.

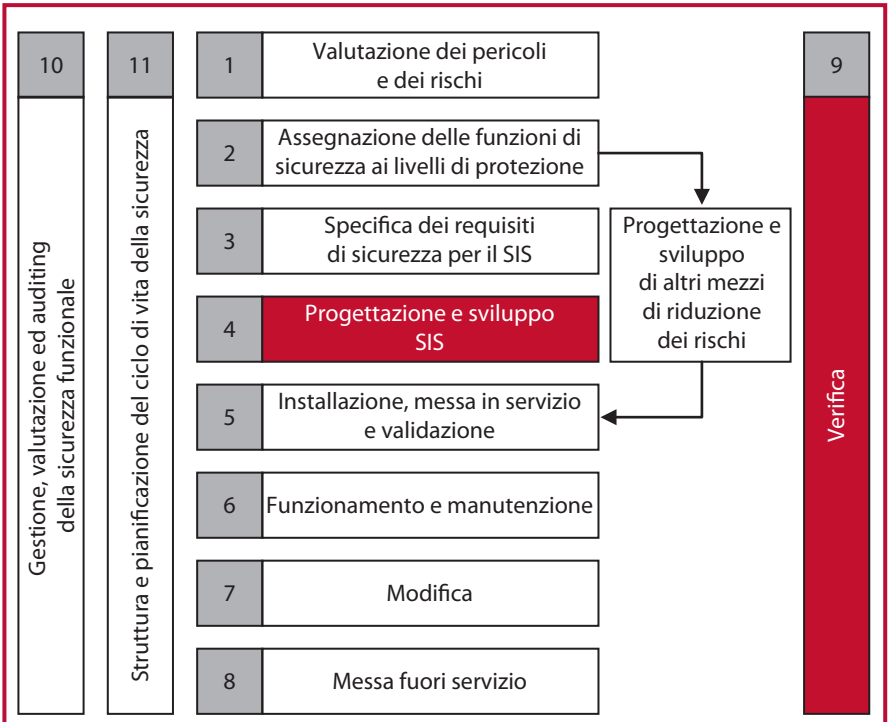


Figura 37: ciclo di vita – Fase 4

L'obiettivo di questa fase come definito nella norma IEC 61511-1, 11.1 è quello di:

- Progettare il sistema SIS in modo da fornire le funzioni SIF necessarie [11.2];
- Verificare che la struttura delle funzioni SIF soddisfi il livello SIL specificato, definito durante la determinazione del livello SIL [13].

11.2. Definizione delle funzioni SIF

La specifica SRS costituirà la base della definizione delle funzioni SIF e permetterà al team di progettazione di tradurre la funzionalità in documenti di progetto, come una specifica FDS. La specifica FDS, quindi, dovrebbe contenere tutti i requisiti funzionali e di integrità necessari a progettare e sviluppare il sistema SIS.

È importante che la documentazione di progetto includa i seguenti requisiti:

- Requisiti di comportamento del sistema al rilevamento di un guasto [13.2];
- Tolleranza ai guasti hardware [13.3];
- Selezione di componenti e sottosistemi [13.4];
- Dispositivi di campo [13.5];
- Interfacce operatore, manutentore e di comunicazione con il sistema SIS [13.6];
- Requisiti di progetto per manutenzione o collaudo [13.7];
- Probabilità di guasto SIF [13.8];
- Software applicativo [13.9].

12. Tecniche di affidabilità

12.1. Introduzione

Questa sezione fornisce una breve introduzione alle tecniche di affidabilità. Non si tratta in alcun modo di uno studio completo dei metodi di ingegneria dell'affidabilità e non fornisce informazioni nuove o non convenzionali ma i metodi normalmente utilizzati dagli ingegneri di competenza.

12.2. Definizioni

Per praticità, viene fornita una breve lista dei termini e delle definizioni chiave. Definizioni più complete dei termini e della nomenclatura sono riportate nei numerosi testi standard sull'argomento.

Affidabilità – (1) Durata o probabilità delle prestazioni senza guasto in determinate condizioni. (2) Probabilità che un elemento possa eseguire la funzione prevista per un intervallo specificato in determinate condizioni. Per gli elementi non ridondanti, questa è equivalente alla definizione (1). Per gli elementi ridondanti, questa è la definizione di affidabilità della missione.

Attendibilità – Misura del grado in cui un elemento è utilizzabile e in grado di realizzare la funzione richiesta in qualunque momento (casuale) durante uno specifico profilo di missione, data la disponibilità all'inizio della missione.

Capacità – Misura della capacità di un elemento di raggiungere gli obiettivi della missione nelle condizioni stabilite durante la missione.

Disponibilità – Una misura del grado in cui un elemento è in stato utilizzabile all'inizio della missione, quando la missione viene richiamata in uno stato sconosciuto.

Durata media fino ad avaria (MTTF) – Misura di base dell'affidabilità di elementi non riparabili: il numero medio di unità di tempo durante cui tutte le parti dell'elemento funzionano nei limiti specificati, durante un particolare intervallo di misura in determinate condizioni.

Durata media fra due guasti (MTBF) – Misura di base dell'affidabilità degli elementi riparabili: il numero medio di unità di tempo durante cui tutte le parti dell'elemento funzionano nei limiti specificati, durante un particolare intervallo di misura in determinate condizioni.

Guasto – Evento o stato inoperabile in cui un elemento o una sua parte non funziona o non funzionerebbe come previamente specificato.

Guasto, casuale – Guasto la cui occorrenza è prevedibile solo in termini probabilistici o statistici. Si applica a tutte le distribuzioni.

Guasto, dipendente – Guasto provocato dal guasto di un elemento associato. Non indipendente.

Guasto, indipendente – Guasto che si verifica senza essere provocato dal guasto di un altro elemento. Non dipendente.

Manutenibilità – Misura della capacità di un elemento di essere manutenuto o riportato alla condizione specificata quando le operazioni di manutenzione vengono realizzate da personale avente i livelli di competenza specificati, utilizzando le procedure e le risorse prescritte, ad ogni livello prescritto di manutenzione e riparazione.

Manutenzione, correttiva – Tutte le azioni eseguite, in conseguenza di un guasto, per riportare un elemento ad una condizione specificata. La manutenzione correttiva può includere alcune o tutte le seguenti fasi: localizzazione, isolamento, smontaggio, interscambio, rimontaggio, allineamento e controllo.

Manutenzione, preventiva – Tutte le azioni eseguite nel tentativo di mantenere un elemento nelle condizioni specificate, realizzando sistematiche operazioni di ispezione, rilevamento e prevenzione dei possibili guasti.

Meccanismo di guasto – Processo fisico, chimico, elettrico, termico o di altro tipo che genera un guasto.

Modalità di guasto – Conseguenza del meccanismo attraverso cui il guasto si verifica ovvero cortocircuito, interruzione, rottura, eccessiva usura.

Tasso di guasto – Numero totale di guasti in una popolazione di elementi, diviso per il numero totale di unità di tempo utilizzate da quella popolazione, durante un particolare intervallo di misura in determinate condizioni.

Tempo medio di riparazione (MTTR) – Misura di base della manutenibilità: la somma dei tempi di manutenzione correttiva, a qualunque livello specificato di riparazione, diviso per il numero totale di guasti in un elemento riparato a quel livello, durante un particolare intervallo in determinate condizioni.

12.3. Concetti matematici di base nell'ingegneria dell'affidabilità

Sono diversi i concetti matematici applicabili all'ingegneria dell'affidabilità, in particolare dai campi delle probabilità e della statistica. Diverse sono anche le distribuzioni matematiche che possono essere usate per vari scopi, tra cui la distribuzione Gaussiana (normale), la distribuzione log-normale, la distribuzione Rayleigh, la distribuzione esponenziale, la distribuzione Weibull e molte altre. Per questa breve introduzione, limiteremo la discussione alla distribuzione esponenziale.

Tasso di guasto e durata media fra due guasti o fino ad avaria (MTBF/MTTF).

Lo scopo delle misure di affidabilità quantitative è quello di definire il tasso di guasto relativamente al tempo per poi modellarlo in una distribuzione matematica al fine di comprendere gli aspetti quantitativi del guasto. Il blocco di base fondamentale è il tasso di guasto, che viene stimato mediante la seguente equazione:

$$\lambda = F/T$$

Dove: λ = tasso di guasto (talvolta chiamato tasso di pericolo);

T = numero totale di ore dispositivo (tempo di funzionamento/cicli/miglia/ecc.) durante un periodo di indagine per elementi che si sono guastati e che non si sono guastati;

F = numero totale di guasti che si verifica durante il periodo di indagine.

Ad esempio, se cinque motori elettrici funzionano per un tempo totale collettivo di 50 anni, con cinque guasti funzionali durante il periodo, il tasso di guasto è di 0,1 guasti all'anno.

Un altro concetto basilare è la durata media fra due guasti o fino ad avaria (MTBF/MTTF). L'unica differenza tra MTBF e MTTF è che il termine MTBF viene utilizzato quando si parla di elementi che, quando si rompono, vengono riparati. Per gli elementi che vengono semplicemente smaltiti e sostituiti, si usa il termine MTTF. I calcoli sono gli stessi. Il calcolo di base per stimare la durata media fra due guasti (MTBF) e la durata media fino ad avaria (MTTF), è il reciproco della funzione del tasso di guasto. L'equazione di calcolo è la seguente.

$$\theta = T/F$$

Dove: θ = Durata media fra due guasti/fino ad avaria;

T = Tempo di funzionamento totale/cicli/miglia/ecc. durante un periodo di indagine per elementi che si sono guastati e che non si sono guastati;

F = numero totale di guasti che si verifica durante il periodo di indagine.

L'MTBF per i motori elettrici industriali di cui sopra è di 10 anni, che è il reciproco del tasso di guasto per i motori. Per i motori elettrici che vengono ricostruiti dopo un guasto, calcoleremmo l'MTBF mentre, per quelli più piccoli che possono essere considerati "monouso", stabiliremmo l'MTTF.

Il tasso di guasto è un elemento di base di diversi calcoli di affidabilità più complessi. A seconda della struttura meccanica/elettrica, del contesto di funzionamento, dell'ambiente e/o dell'efficacia della manutenzione, il tasso di guasto di una macchina in funzione del tempo può decrescere, rimanere costante, aumentare in modo lineare o geometricamente. Tuttavia, per la maggior parte dei calcoli di affidabilità, si ipotizza un tasso di guasto costante.

12.4. La curva bathtub (a vasca da bagno)

In teoria, la curva bathtub illustra le tre caratteristiche di base del tasso di guasto di una macchina: decrescente, costante e crescente. In pratica, la maggior parte delle macchine trascorre gran parte della vita nella fase iniziale, o nelle regioni a tasso di guasto costante della curva bathtub. Raramente è possibile osservare meccanismi di guasto dipendenti dal tempo, dato che le tipiche macchine industriali tendono ad essere sostituite, in tutto o in parte, prima che si usurino. Tuttavia, nonostante i limiti di modellazione, la curva bathtub è un utile strumento per spiegare i concetti di base dell'ingegneria dell'affidabilità.

Il corpo umano è un eccellente esempio di un sistema che segue la curva bathtub. Le persone (macchine) tendono ad avere un elevato tasso di mortalità (guasto) durante i loro primi anni di vita ma il tasso scende quando il bambino (prodotto) cresce. Presumendo che una persona sopravviva agli anni dell'adolescenza, il tasso di mortalità diventa abbastanza costante e così rimane fino a quando malattie dipendenti dall'età (tempo) iniziano ad aumentare il tasso di mortalità (usura).

La curva bathtub è un insieme di diverse distribuzioni di guasto, Figura 38.

Il tasso di guasto decrescente dei primi anni di vita è dovuto a ragioni sistematiche, quali i difetti di fabbricazione presenti in un prodotto. Durante la produzione di un lotto, una parte della popolazione conterrà punti deboli che, in servizio, genereranno guasti. Quando gli elementi guasti vengono mandati in riparazione, la popolazione di prodotti difettosi si riduce ed il tasso di guasto, di conseguenza, scende.

Anche i tassi di guasto crescenti dovuti all'usura possono dipendere da simili ragioni sistematiche. I meccanismi di guasto possono essere dovuti ad una minore resistenza derivante dall'accumulo di danni per fatica. In elettronica, i meccanismi di guasto dipendenti dal tempo tendono ad essere di tipo meccanico ed includono il guasto da fatica dei giunti saldati.

Il periodo del tasso di guasto costante rappresenta la maggior parte della vita di un prodotto ed è una misura della qualità. È proprio la regione del tasso di guasto costante quella in cui vengono eseguiti i semplici calcoli di affidabilità.

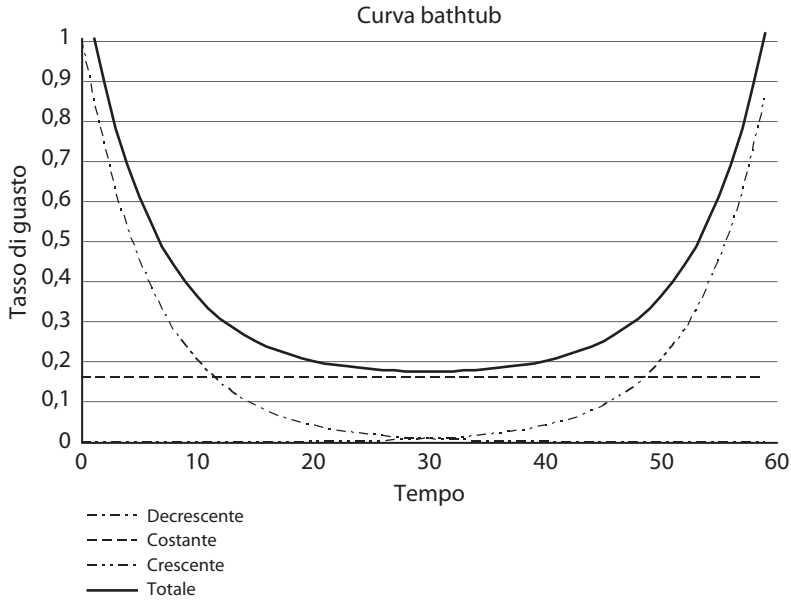


Figura 38: curva bathtub

12.5. La distribuzione esponenziale

La distribuzione esponenziale, la formula più basilare e comunemente utilizzata di previsione dell'affidabilità, modella le macchine con il tasso di guasto costante, la sezione piatta della curva bathtub. La maggior parte delle macchine industriali trascorre gran parte della vita nell'area a tasso di guasto costante che, quindi, è ampiamente applicabile.

Di seguito, è riportata l'equazione di base per stimare l'affidabilità di una macchina che segue la distribuzione esponenziale, in cui il tasso di guasto in funzione del tempo è costante.

$$R(t) = \text{esp} \{ -\lambda . t \}$$

Dove: R(t) = Stima dell'affidabilità per un periodo di tempo, cicli, miglia, ecc. (t);

λ = Tasso di guasto (1/MTBF o 1/MTTF) e t = Tempo a rischio.

Nell'esempio dei motori elettrici, ipotizzando un tasso di guasto costante, la probabilità di far funzionare un motore per sei anni senza un guasto – ovvero l'affidabilità prevista – è del 55 percento. Questo viene calcolato come segue:

$$R(t) = \text{esp}\{-0,1 \times 6\}$$
$$= \text{esp}\{-0,6\}$$
$$= 0,5488 \approx 55\%$$

In termini probabilistici, si può prevedere che, dopo sei anni, il 45% circa di una popolazione di motori identici che funzionano in un'identica applicazione si guasti. A questo punto, è opportuno ribadire che questi calcoli proiettano la probabilità per una popolazione di elementi. Per quanto riguarda i singoli elementi della popolazione, uno potrebbe guastarsi il primo giorno di funzionamento mentre un altro potrebbe durare 30 anni. Questa è la natura delle proiezioni di affidabilità probabilistiche.

Una caratteristica della distribuzione esponenziale è che la durata MTBF si verifica nel punto in cui l'affidabilità calcolata è del 36,78%, punto in corrispondenza del quale il 63,22% delle macchine si è già guastata. Nell'esempio dei motori, si può prevedere che, dopo 10 anni, il 63,22% di una popolazione di motori identici che funzionano in applicazioni identiche si guasti. In altre parole, il tasso di sopravvivenza della popolazione è del 36,78%.

12.6. Stima dell'affidabilità del sistema

Una volta stabilita l'affidabilità dei componenti o delle macchine in relazione al contesto di funzionamento ed al ciclo di vita richiesto, gli ingegneri di processo devono valutare l'affidabilità di un sistema o processo. Anche in questo caso, per motivi di brevità e semplicità, tratteremo le stime dell'affidabilità dei sistemi in serie, in parallelo e ridondanti a carico condiviso (M su N) (sistemi MooN).

12.6.1. Sistemi in serie

Prima di discutere i sistemi in serie, dovremmo chiarire che cosa sono gli schemi a blocchi dell'affidabilità (RBD). Gli schemi RBD semplicemente mappano un processo dall'inizio alla fine. Per un sistema in serie, il sottosistema 1 è seguito dal sottosistema 2 e così via. Nei sistemi in serie, la capacità di utilizzare il sottosistema 2 dipende dallo stato operativo del sottosistema 1. Se il sottosistema 1 non funziona, il sistema rimane inattivo a prescindere dalle condizioni del sottosistema 2 [Figura 39].

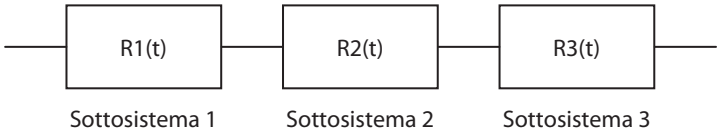


Figura 39: sistema in serie

Per calcolare l'affidabilità del sistema per un processo seriale, è sufficiente moltiplicare l'affidabilità stimata del sottosistema 1 al tempo (t) per l'affidabilità stimata del sottosistema 2 al tempo (t). L'equazione di base per calcolare l'affidabilità del sistema di un semplice sistema in serie è:

$$Rs(t) = R1(t) \cdot R2(t) \cdot R3(t)$$

Dove: Rs(t) – Affidabilità del sistema per un determinato tempo (t);

Rn(t) – Affidabilità del sottosistema o della sottofunzione per un determinato tempo (t)

Quindi, per un semplice sistema costituito da tre sottosistemi (sottofunzioni), ognuno con un'affidabilità stimata di 0,90 (90%) al tempo (t), l'affidabilità del sistema viene calcolata come 0,90 X 0,90 X 0,90 = 0,729 ovvero circa il 73%.

12.6.2. Sistemi in parallelo

Spesso, nelle macchine critiche, i progettisti incorporano la ridondanza. Questi sistemi vengono definiti dagli ingegneri che si occupano dell'affidabilità "sistemi in parallelo". Tali sistemi possono essere progettati come sistemi in parallelo attivi o in standby. Nella Figura 40, è riportato lo schema a blocchi di un semplice sistema in parallelo a due componenti.

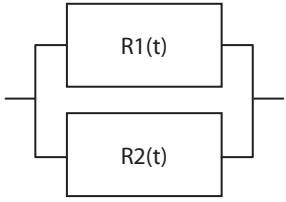


Figura 40: sistema in parallelo

Per calcolare l'affidabilità di un sistema in parallelo attivo, in cui entrambe le macchine sono in funzione, si usa la semplice equazione che segue:

$$Rs(t) = 1 - [\{1-R1(t)\} . \{1-R2(t)\}]$$

Dove: Rs(t) – Affidabilità del sistema per un determinato tempo (t);

Rn(t) – Affidabilità del sottosistema o della sottofunzione per un determinato tempo (t)

Il semplice sistema in parallelo di questo esempio, con due componenti in parallelo ognuno dei quali con un'affidabilità di 0,90, ha un'affidabilità totale del sistema di 1 – (0,1 X 0,1) = 0,99. L'affidabilità del sistema, quindi, è stata notevolmente migliorata.

12.6.3. Sistemi M su N (MooN)

Per gli ingegneri responsabili dell'affidabilità dell'impianto, un concetto importante è quello dei sistemi MooN. Questi sistemi richiedono che le unità M di una popolazione totale N siano disponibili per l'uso. Un buon esempio industriale sono i polverizzatori di carbone all'interno di una centrale elettrica. Spesso, gli ingegneri progettano questa funzione dell'impianto ricorrendo ad un approccio MooN. Se ci sono quattro polverizzatori, ad esempio, per funzionare a pieno carico l'unità deve poterne utilizzare almeno tre [Figura 41].

12.7. Guasti pericolosi e guasti non pericolosi

Perché i calcoli sull'affidabilità siano significativi, non è sufficiente conoscere il tasso di guasto del sistema, ma dobbiamo anche sapere in che modo un sistema può guastarsi ovvero conoscere le modalità di guasto.

Le modalità di guasto possono essere classificate come non pericolose o pericolose. La Figura 42 mostra una condotta di gas. Se la condotta fornisce combustibile ad una centrale elettrica e la valvola di spegnimento si guasta chiudendosi intempestivamente, l'alimentazione di combustibile si arresta e, nonostante qualche perdita di profitto, la modalità di guasto in chiusura è un guasto non pericoloso.

Se la stessa valvola si guasta in posizione di apertura, l'alimentazione di combustibile continua ma, in condizioni di sovrappressione, non saremmo in grado di isolare il combustibile e mettere in sicurezza la condotta. Questa modalità di guasto in apertura è quindi considerata un guasto pericoloso.

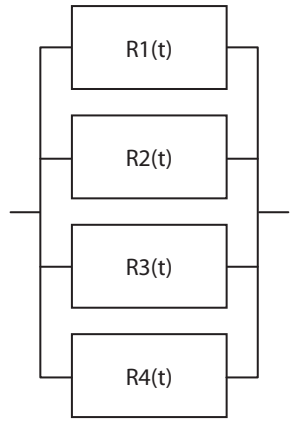


Figura 41: sistema 3oo4

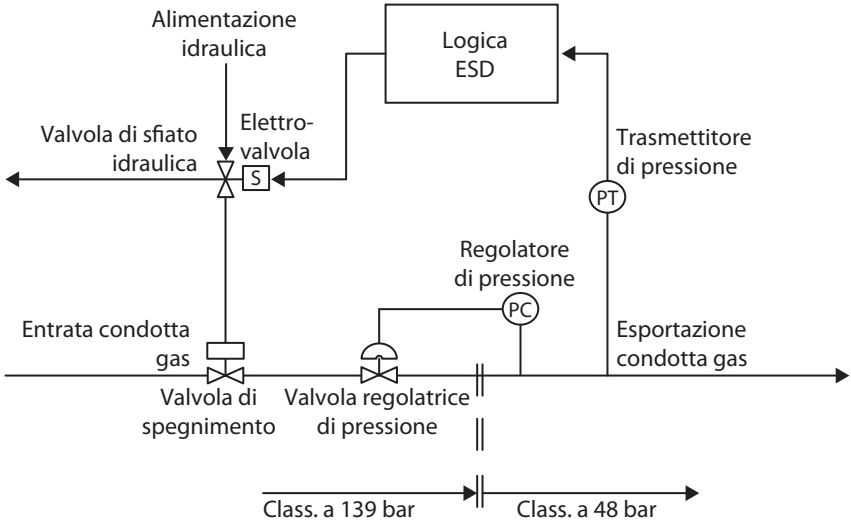


Figura 42: esempio di funzione strumentata di sicurezza

In questo esempio, la modalità di guasto pericoloso in apertura non verrebbe rivelata fino alla successiva domanda di intervento ovvero fino ad un comando di chiusura della valvola. Questo è considerato un guasto non rilevato pericoloso.

Se invece la condotta fornisce alla centrale elettrica il refrigerante e la valvola SSV969A si guasta chiudendosi intempestivamente, l'alimentazione di refrigerante si arresta e la centrale elettrica può surriscaldarsi. In questa applicazione, la stessa valvola e la stessa modalità di guasto in chiusura rappresentano un guasto pericoloso. Se la valvola si guasta in posizione di apertura, invece, il flusso di refrigerante continua e la modalità di guasto in apertura può essere considerata un guasto non pericoloso.

Il guasto pericoloso di un componente in una funzione strumentata di sicurezza impedisce a quella funzione di raggiungere uno stato sicuro quando ciò viene richiesto. Il tasso di guasto pericoloso è identificato dal simbolo: λ_D.

Un guasto non pericoloso non può portare il sistema strumentato di sicurezza in uno stato pericoloso o di mancato funzionamento ma avviene in modo tale da richiedere lo spegnimento del sistema o l'attivazione della funzione strumentata di sicurezza in assenza di pericolo. Il tasso dei guasti non pericolosi è identificato dal simbolo: λ_S.

Alcune modalità di guasto non incidono del tutto sulla funzione di sicurezza come, ad esempio, quelle riguardanti le funzioni di manutenzione, gli indicatori, la registrazione dei dati ed altre funzioni non legate alla sicurezza (non SR). Il tasso di guasto non SR è identificato dal simbolo: $\lambda_{non\text{-}SR}$.

Il tasso di guasto totale di un elemento λ è uguale alla somma dei tassi di guasto legati alla sicurezza e non SR. Generalmente, nei calcoli di affidabilità sono inclusi solo λ_D e λ_S.

$$\lambda = \lambda_D + \lambda_S + \lambda_{non\text{-}SR}$$

12.8. Guasti rilevati e non rilevati

La probabilità PFD fa riferimento ai guasti pericolosi che impediscono il funzionamento del sistema SIS quando richiesto. Queste modalità di guasto sono classificate come guasti rilevati se vengono rilevate dalla diagnostica o come guasti non rilevati se possono essere rilevate solo da prove funzionali manuali che vengono solitamente eseguite una volta all'anno. Le modalità di guasto classificate dall'analisi FMECA come guasti rilevati pericolosi dovrebbero essere rilevate attraverso la diagnostica e verificate nella validazione software. Inoltre, per essere efficaci, le procedure delle prove funzionali dovrebbero garantire il rilevamento dei guasti non rilevati pericolosi.

Conformemente alla norma IEC 61508-6, Allegato B.3.1, l'analisi può considerare che per ogni funzione di sicurezza è prevista la prova funzionale e la riparazione più idonea, ovvero che tutti i guasti non rilevati verranno rivelati dalla prova funzionale.

12.9. Periodo di prova funzionale (T_P) e tempo medio di indisponibilità (MDT)

Se si verifica un guasto, si presume che in media esso si presenterà in corrispondenza del punto centrale dell'intervallo di prova. In altre parole, il guasto rimarrà non rilevato per il 50% del periodo di prova.

Sia per i guasti rilevati sia per quelli non rilevati, il tempo medio di indisponibilità (MDT) dipende dall'intervallo di prova oltre che dal tempo di riparazione (MTTR).

Il tempo MDT viene quindi calcolato come segue:

$$MDT = \frac{\text{intervallo di prova}}{2} + MTTR$$

Il tempo MDT per i guasti rilevati si approssima quindi al tempo di riparazione, poiché l'intervallo di prova (autodiagnostica) è generalmente breve rispetto al tempo MTTR. Per i guasti non rilevati, il tempo di riparazione è breve rispetto all'intervallo di prova (periodo di prova funzionale, Tp) e quindi il tempo MDT per i guasti non rilevati si approssima a Tp/2.

12.10. Modellazione del tasso di guasto del sistema (λsys)

Il tasso di guasto di un sistema ridondante λsys può essere calcolato considerando il numero di modi in cui il guasto del sistema può verificarsi. In un sistema 3oo4, è richiesto il funzionamento di 3 canali su 4 perché il sistema funzioni; due guasti, quindi, si tradurranno in un guasto del sistema.

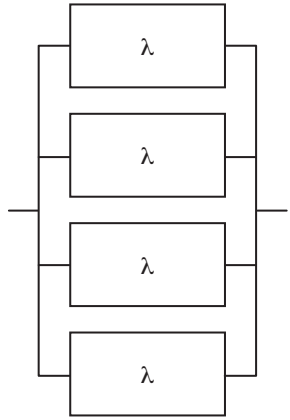


Figura 43: sistema 3oo4

Il tasso a cui possono verificarsi due guasti (λ_2) è dato dal tasso di guasto di un elemento (λ) moltiplicato per la probabilità di un secondo guasto durante il tempo di indisponibilità (MDT) del primo guasto (λ.MDT).

Quindi:

$$\lambda_2 = \lambda.(\lambda.MDT)$$

Tuttavia, in un sistema 3oo4 sono 12 le permutazioni di due guasti (l'ordine è importante): A.B, A.C, A.D, B.C, B.D, C.D, B.A, C.A, D.A, C.B, D.B e D.C, e tutte devono essere considerate. Il tasso di guasto del sistema diventa approssimativamente:

$$\lambda_{SYS} = 12.\lambda^2.MDT$$

Per essere esatti, dovremmo includere tutte le permutazioni di 3 e 4 guasti concorrenti oltre che i guasti per causa comune, poiché anche questi comporteranno il guasto del sistema ma, per una prima approssimazione, questi altri termini possono essere trascurati. Il tasso di guasto dei sistemi 3oo4 e di altre configurazioni è riportato nella Tabella 10. Anche queste sono approssimazioni che trascurano i termini di ordine superiore.

Configurazione	**λsys**
1oo1	λ
1oo2	$2.\lambda^2.MDT$
2oo2	$2.\lambda$
1oo3	$3.\lambda^3.MDT^2$
2oo3	$6.\lambda^2.MDT$
3oo3	$3.\lambda$
1oo4	$\lambda^4.MDT^3$
2oo4	$12.\lambda^3.MDT^2$
3oo4	$12.\lambda^2.MDT$
4oo4	$4.\lambda$

Tabella 10: tasso di guasto del sistema

Il contributo dei guasti per causa comune viene trattato più avanti [12.17].

12.11. Modellazione dei tassi di guasto rilevati e non rilevati pericolosi (λ_{DD}) e (λ_{DU})

Sostituendo λ_{DD} e λ_{DU} a λ nella Tabella 10 ed usando il tempo MDT o Tp/2 come più opportuno, è possibile ricavare il tasso di guasto del sistema dovuto a guasti pericolosi rilevati o non rilevati, Tabella 11.

Configurazione	Rilevato	Non rilevato
	λsys	**λsys**
1oo1	λ_{DD}	λ_{DU}
1oo2	$2.\lambda_{DD}^2.MDT$	$\lambda_{DU}^2.T_P$
2oo2	$2.\lambda_{DD}$	$2.\lambda_{DU}$
1oo3	$3.\lambda_{DD}^3.MDT^2$	$\lambda_{DU}^3.T_P^2$
2oo3	$6.\lambda_{DD}^2.MDT$	$3.\lambda_{DU}^2.T_P$
3oo3	$3.\lambda_{DD}$	$3.\lambda_{DU}$
1oo4	$\lambda_{DD}^4.MDT^3$	$\lambda_{DU}^4.T_P^3$
2oo4	$12.\lambda_{DD}^3.MDT^2$	$4.\lambda_{DU}^3.T_P^2$
3oo4	$12.\lambda_{DD}^2.MDT$	$6.\lambda_{DU}^2.T_P$
4oo4	$4.\lambda_{DD}$	$4.\lambda_{DU}$

Tabella 11: tasso di guasto pericoloso del sistema

12.12. Modellazione del tasso di interventi intempestivi del sistema (λ_{STR})

Dato che si presume che i tassi di guasto non pericoloso, in una configurazione ridondante, vengano tutti rilevati, i canali in guasto saranno riparati a condizione che il sistema non intervenga. Quindi si applica l'approccio adottato per i guasti rilevati pericolosi, con la differenza che il numero di guasti richiesto per un intervento intempestivo può differire da quello richiesto per un guasto pericoloso.

Generalmente, gli interventi intempestivi includono solo i tassi di guasto non pericoloso ma, a seconda del comportamento del sistema al rilevamento di un guasto, possono essere inclusi anche i guasti rilevati pericolosi ed il tasso di interventi intempestivi sarà la somma dei due.

La Tabella 12 riepiloga i tassi di intervento intempestivo del sistema per i guasti non pericolosi.

Configurazione	Intempestivo
	λstr
1oo1	λ_S
1oo2	$2.\lambda_S$
2oo2	$2.\lambda_S^2.MDT$
1oo3	$3.\lambda_S$
2oo3	$6.\lambda_S^2.MDT$
3oo3	$3.\lambda_S^3.MDT^2$
1oo4	$4.\lambda_S$
2oo4	$12.\lambda_S^2.MDT$
3oo4	$12.\lambda_S^3.MDT^2$
4oo4	$\lambda_S^4.MDT^3$

Tabella 12: tasso di interventi intempestivi del sistema

12.13. Modellazione della disponibilità del sistema di sicurezza in modalità su domanda

Per un sistema di sicurezza, la disponibilità dovuta a guasti rilevati pericolosi (A_{DD}) è data da:

$$A_{DD} = 1/(1 + .\lambda_{DD(SYS)}.MDT)$$

dove $\lambda_{DD(SYS)}$ è il tasso di guasto del sistema risultante dai guasti rilevati pericolosi [12.11].

Per i guasti non rilevati pericolosi (ADU) è dato da:

$$A_{DU} = 1/(1 + .\lambda_{DU(SYS)}.T_P/2)$$

dove $\lambda_{DU(SYS)}$ è il tasso di guasto del sistema risultante dai guasti non rilevati pericolosi [12.11].

Per i guasti non pericolosi A_S è dato da:

$$A_S = 1/(1 + .\lambda_{S(SYS)}.MDT)$$

dove $\lambda_{S(SYS)}$ è il tasso di guasto del sistema risultante da guasti (non pericolosi) intempestivi [12.12].

La disponibilità del sistema è quindi il prodotto delle disponibilità dovute a guasti rilevati pericolosi, guasti non rilevati pericolosi e guasti non pericolosi:

$$A_{SYS} = A_{DD} \cdot A_{DU} \cdot A_S$$

Questo metodo può essere utilizzato per la modellazione di sistemi in serie (simplex) e di sistemi ridondanti.

12.14. Modellazione della disponibilità del sistema di sicurezza in modalità continua

Quando il metodo viene applicato ai sistemi di sicurezza in modalità continua, l'analista deve capire la natura delle domande di intervento della funzione di sicurezza. Alcune funzioni di sicurezza in modalità continua funzionano su domanda (proprio come una funzione di sicurezza in modalità su domanda) ma sono considerate in modalità continua data la frequenza della domanda, superiore ad una volta all'anno. In questo caso, la disponibilità può essere calcolata come per una funzione di sicurezza in modalità su domanda, con la differenza che l'intervallo di prova funzionale (T_P) dovrebbe essere sostituito con l'intervallo di domanda (T_D). I guasti pericolosi non rilevati rimarrebbero non rivelati fino alla successiva domanda di intervento della funzione di sicurezza.

Quando la funzione di sicurezza in modalità continua assicura il controllo continuo, la disponibilità può essere calcolata come per un sistema di controllo [12.15].

12.15. Modellazione della disponibilità del sistema di controllo

Nel modellare la disponibilità dei sistemi di controllo, consideriamo i guasti che interessano il processo e dobbiamo decidere se un guasto interessa il processo in modo tale da rendere il sistema di controllo effettivamente non disponibile.

Se il rilevamento di un guasto avviene tramite la diagnostica e gli allarmi, viene richiesta una riparazione ed il sistema non sarà disponibile fino a quando ripristinato; se il rilevamento di un guasto è basato sui sintomi, il processo sotto controllo continua a funzionare fuori dai limiti di setpoint.

I guasti non rilevati non si traducono immediatamente nell'indisponibilità del sistema di controllo. A volte, il guasto non rilevato può comportare la deviazione di un parametro di processo dai limiti specificati e, in tal caso, verrà rivelato rendendo il sistema indisponibile.

La disponibilità del sistema di controllo può quindi essere modellata considerando il tasso di guasto totale del sistema A_{SYS} dato da:

$$A_{SYS} = 1/(1 + \lambda_{SYS}.MDT)$$

dove λ_{SYS} è il tasso di guasto totale del sistema risultante da tutti i guasti [Tabella 10].

12.16. Probabilità di guasto pericoloso/ora (PFH) e probabilità di guasto su domanda (PFD)

Le formule semplificate PFH e PFD per configurazioni comuni sono presentate nella Tabella 13 per i guasti rilevati e nella Tabella 14 per i guasti non rilevati.

Configurazione	PFH	PFD
1oo1	λ_{DD}	$\lambda_{DD}.MDT$
1oo2	$2.\lambda_{DD}^2.MDT$	$2.\lambda_{DD}^2.MDT^2$
2oo2	$2.\lambda_{DD}$	$2.\lambda_{DD}.MDT$
1oo3	$3.\lambda_{DD}^3.MDT^2$	$3.\lambda_{DD}^3.MDT^3$
2oo3	$6.\lambda_{DD}^2.MDT$	$3.\lambda_{DD}^2.MDT^2$
3oo3	$3.\lambda_{DD}$	$3.\lambda_{DD}.MDT$
1oo4	$4.\lambda_{DD}^4.MDT^3$	$\lambda_{DD}^4.MDT^4$
2oo4	$12.\lambda_{DD}^3.MDT^2$	$4.\lambda_{DD}^3.MDT^3$
3oo4	$12.\lambda_{DD}^2.MDT$	$6.\lambda_{DD}^2.MDT^2$
4oo4	$4.\lambda_{DD}$	$4.\lambda_{DD}.MDT$

Tabella 13: calcolo PFH/PFD (guasti rilevati)

Configurazione	PFH	PFD
1oo1	λ_{DU}	$\lambda_{DD}.T_P/2$
1oo2	$\lambda_{DU}^2.T_P$	$\lambda_{DD}^2.T_P^2/3$
2oo2	$2.\lambda_{DU}$	$\lambda_{DD}.T_P$
1oo3	$\lambda_{DU}^3.T_P^2$	$\lambda_{DD}^3.T_P^3/4$
2oo3	$3.\lambda_{DU}^2.T_P$	$\lambda_{DD}^2.T_P^2$
3oo3	$3.\lambda_{DU}$	$3.\lambda_{DD}.T_P/2$
1oo4	$\lambda_{DU}^4.T_P^3$	$\lambda_{DD}^4.T_P^4/5$
2oo4	$4.\lambda_{DU}^3.T_P^2$	$\lambda_{DD}^3.T_P^3$
3oo4	$6.\lambda_{DU}^2.T_P$	$2.\lambda_{DD}^2.T_P^2$
4oo4	$4.\lambda_{DU}$	$2.\lambda_{DD}.T_P$

Tabella 14: calcolo PFH/PFD (guasti non rilevati)

12.17. Considerazione dei guasti per causa comune

I guasti per causa comune (CCF) sono guasti che possono derivare da una singola causa ma che interessano simultaneamente più di un canale. Possono essere dovuti, ad esempio, ad un guasto sistematico, ad un errore di specifica del progetto o a sollecitazioni esterne come la sovratemperatura e comportare il guasto del componente in entrambi i canali ridondanti. È responsabilità del progettista del sistema adottare le misure necessarie a minimizzare la frequenza dei guasti per causa comune utilizzando adeguate tecniche di progettazione.

Il contributo dei CCF nei percorsi ridondanti in parallelo viene considerato con l'inclusione di un fattore β. Il tasso di guasto CCF incluso nel calcolo è uguale a β x il tasso di guasto totale di uno dei percorsi ridondanti.

Il modello del fattore β [IEC 61508-6, Allegato D] è la tecnica preferenziale, perché oggettiva e perché consente di tracciare la stima di β. Il modello è stato compilato per porre una serie di domande specifiche a cui viene poi assegnato un punteggio obiettivo. Nel modello, il punteggio massimo per ogni domanda è stato ponderato calibrando i risultati di varie valutazioni, in base a dati di guasto reali noti.

Due sono le colonne usate per i punteggi. La colonna A contiene i punteggi per quelle caratteristiche della protezione CCF percepite come migliorate da un aumento della frequenza di diagnostica (autodiagnostica o prova funzionale). La colonna B contiene i punteggi per quelle caratteristiche che non si ritengono migliorate da un aumento della frequenza di diagnostica.

Il modello consente di modificare il punteggio in base alla frequenza ed alla copertura del test diagnostico. I punteggi della colonna A vengono moltiplicati per un fattore C, derivato dalle considerazioni legate alla diagnostica. Il fattore β finale viene poi stimato dal punteggio totale non elaborato:

Punteggio non elaborato = (A * C) + B

La relazione tra β e il punteggio non elaborato è sostanzialmente una funzione esponenziale negativa, non essendoci dati per respingere l'ipotesi che quando β diminuisce (migliora), i miglioramenti successivi diventino sempre più difficili da ottenere.

Se una particolare domanda non è applicabile al sistema in valutazione, si inserisce un punteggio del 100% o dello 0%, a seconda di quale risulta più pertinente.

Quelli che seguono sono alcuni tipici fattori che possono essere considerati per stimare il contributo dei CCF:

- canali ridondanti fisicamente separati;
- tecnologie diverse (ad es. un canale elettronico ed un altro basato su relè);
- sistema documentato di lavoro sul posto che dovrebbe assicurare l'analisi dei guasti;
- procedure di manutenzione scritte che dovrebbero prevenire il reinstradamento dei cavi;
- accesso limitato del personale;
- ambiente operativo controllato ed apparecchiature classificate per valori superiori al range ambientale previsto.

Le effettive prestazioni in servizio dipenderanno dall'installazione e dalle procedure di progettazione, funzionamento e manutenzione adottate, ma solo se sono state adottate tutte le buone prassi di progettazione il modello fornirà una stima tracciabile del contributo dei CCF.

Quando si considerano i CCF nelle formule per PFD e PFH [Tabella 13 e Tabella 14], è possibile utilizzare il seguente approccio. Le equazioni utilizzate sono semplificate rispetto alle equazioni standard e sono derivate al punto [19.6].

Per i guasti rilevati:

$PFD1oo1 = \lambda_{DD}.MDT$	Rif. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DD}^2.MDT^2 + \beta.\lambda_{DD}.MDT$	Rif. IEC 61508-6, B.3.2.2.2

Per i guasti non rilevati:

$PFD1oo1 = \lambda_{DU}.T_P/2$	Rif. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DU}^2.T_P^2/3 + \beta.\lambda_{DU}.T_P/2$	Rif. IEC 61508-6, B.3.2.2.2

Dove λ_{DD} è il tasso di guasto rilevato pericoloso, λ_{DU} è il tasso di guasto non rilevato pericoloso e β è il contributo dai guasti per causa comune. T_P è l'intervallo di prova funzionale e MDT è il tempo medio di indisponibilità.

Le forme generiche di queste equazioni per varie configurazioni, sia per i sistemi in modalità continua sia per quelli in modalità su domanda, sono esaminate al punto [19.7].

12.18. Tassi di guasto

Nel calcolo di PFD e SFF, l'analisi usa l'ipotesi di base della norma IEC 61508-6, Allegato B.3 per cui i tassi di guasto dei componenti sono costanti per tutta la vita del sistema.

I tassi di guasto utilizzati nei calcoli possono essere ottenuti mediante analisi dei modi, degli effetti e della criticità dei guasti (FMECA) e quantificati mediante i dati reali disponibili o facendo riferimento a dati pubblicati dalle fonti di settore. I tassi di guasto utilizzati dovrebbero essere confrontati ai dati disponibili per moduli simili a livello di complessità e tecnologia. Questo approccio può ritenersi conservativo in termini di modellazione dell'affidabilità ed offre buone garanzie di poter ottenere in servizio le prestazioni di affidabilità calcolate.

I tassi di guasto e le loro fonti sono discussi al punto 14.8.

12.19. Modellazione 1oo2, 1oo2D e hot-standby

I seguenti esempi mostrano la modellazione degli schemi RBD di alcune comuni configurazioni di sistema.

1oo2

Un sistema 1oo2 è un'architettura 1 su 2, in cui uno qualsiasi dei due canali può eseguire la funzione di sicurezza. Si tratta di una configurazione tollerante ai guasti in cui il guasto di un canale può essere tollerato.

Se si tratta di un guasto non rivelato pericoloso, il guasto del canale non verrà rilevato dalla diagnostica e non ci sarà alcuna indicazione di guasto. La funzione di sicurezza continuerà comunque a funzionare poiché il canale rimanente può comandare l'intervento. Se il guasto del canale è un guasto rilevato pericoloso, viene generalmente segnalato in un'indicazione di guasto.

Al punto 12.20, è riportato uno schema RBD di esempio.

1oo2D

Un'architettura di sistema 1oo2D ha due canali collegati in parallelo ed ogni canale ha circuiti di diagnostica per rilevare i guasti ad alta copertura diagnostica. Durante il normale funzionamento del sistema, i due canali devono concordare l'esecuzione di un'azione di spegnimento. Se il circuito di diagnostica di un canale rileva un guasto, l'altro canale controlla il sistema.

In termini di modellazione dell'affidabilità, per i guasti rilevati pericolosi il sistema 1oo2D funziona come una configurazione 1oo2; tasso di guasto e PFD del sistema possono essere modellati come 1oo2 per i guasti rilevati.

Un singolo guasto non rilevato pericoloso di un canale in un sistema 1oo2D impedirà al sistema di funzionare e quindi tasso di guasto e la probabilità PFD del sistema devono essere modellati come 2oo2 per i guasti non rilevati. In altre parole, devono funzionare entrambi i canali.

Uno schema RBD di esempio è mostrato in 12.21.

Hot-standby

Un'architettura di sistema hot-standby ha due canali collegati in parallelo, uno dei quali è designato come master e controlla la funzione di sicurezza. L'altro canale funge da riserva nel caso in cui nel canale master venga rilevato un guasto pericoloso; in tal caso, sarà il canale in standby ad assumere il controllo della funzione di sicurezza.

In termini di modellazione dell'affidabilità, per i guasti rilevati pericolosi il sistema hot-standby funziona come una configurazione 1oo2; tasso di guasto e probabilità PFD del sistema possono essere modellati come 1oo2 per i guasti rilevati.

Un singolo guasto non rilevato pericoloso del canale impedirà al sistema di funzionare e quindi il tasso di guasto e la probabilità PFD del sistema devono essere modellati come 1oo1 per guasti non rilevati. In altre parole, la funzione di sicurezza non può tollerare un guasto non rilevato del canale master e non c'è ridondanza per i guasti non rilevati. Al punto 12.22, è riportato uno schema RBD di esempio.

Tasso di guasto del sistema per un sistema 1oo2

CCF											5%
Q.tà	1	1	1	1	1	2	1	1			
Configurazione	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2	1oo2			
λDD (diagnostica)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08			
λ.DD*Q.tà	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08			
λ.DD per ramo			1,16E-06				1,01E-06	5,25E-08			
MDT			24				24	24			
Totaleλ.DD			1,16E-06				4,93E-11	5,25E-08			
λDU (prova funzionale)	3,66E-07	2,00E-07	2,00E-07	9,10E-09	3,28E-08	2,26E-08	1,54E-08	5,84E-09			
λ.DU*Q.tà	3,66E-07	2,00E-07	2,00E-07	9,10E-09	6,56E-08	2,26E-08	1,54E-08	5,84E-09			
λ.DU per ramo			7,66E-07				1,13E-07	5,84E-09			
Periodo di prova funzionale, T			8760				8760	8760			
TotaleλDU			7,66E-07				1,11E-10	5,84E-09			
λ.S (diagnostica)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08			
λ.S*Q.tà	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08			
λ.S per ramo			2,63E-03				1,13E-06	5,84E-08			
MDT			24				24	24			
TotaleλS			2,63E-03				2,25E-06	5,84E-08			
TotaleλDD	1,21E-06										
TotaleλDU	7,72E-07										
TotaleλS	2,63E-03										
TotaleλSYS	**2,63E-03**	**/h**									

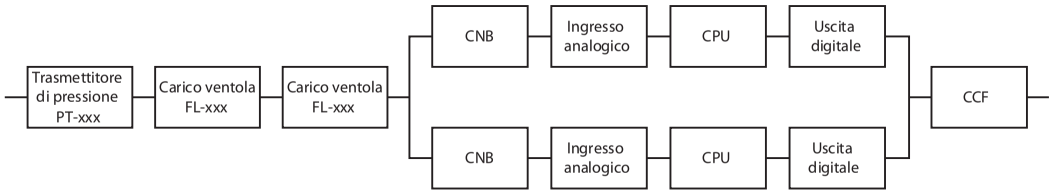
Tasso di guasto del sistema per un sistema 1oo2D

CCF								5%						
Q.tà	1	1	1	1	2	1	1		2	4	2	2		
Configurazione	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2		2oo2	2oo2	2oo2	2oo2		
λDD (diagnostica)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08						
λDD*Q.tà	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08						
λDD per ramo			1,16E-06				1,01E-06	5,25E-08						
MDT			24				24	24						
Totale λ.DD			1,16E-06				4,93E-11	5,25E-08						
λDU (prova funzionale)	3,66E-07	2,00E-07	2,00E-07						9,10E-09	3,28E-08	2,26E-08		1,54E-08	
λDU*Q.tà	3,66E-07	2,00E-07	2,00E-07						1,82E-08	1,31E-07	4,52E-08		3,07E-08	
λDU per ramo			7,66E-07										2,23E-07	
Periodo di prova funzionale, T			8760										8760	
Totale λ.DU			7,66E-07										9,87E-04	
λS (diagnostica)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08						
λS*Q.tà	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08						
λS per ramo			2,63E-03				1,13E-06	5,84E-08						
MDT			24				24	24						
Totale λ.S			2,63E-03				2,25E-06	5,84E-08						
Totale λ.DD	1,21E-06													
Totale λ.DU	9,88E-04													
Totale λ.S	2,63E-03													
Totale λ.SYS	**3,62E-03**	**/h**												

Tasso di guasto del sistema per un sistema hot-standby

Q.tà	1	1	1	1	2	1	1		1	2	1	1		
Configurazione	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2		1oo1	1oo1	1oo1	1oo1		
λDD (diagnostica)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08						
λDD*Q.tà	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08						
λDD per ramo			1,16E-06				1,01E-06	5,25E-08						
MDT			24				24	24						
TotaleλDD			1,16E-06				4,93E-11	5,25E-08						
λDU (prova funzionale)	3,66E-07	2,00E-07	2,00E-07						9,10E-09	3,28E-08	2,26E-08	1,54E-08		
λDU*Q.tà	3,66E-07	2,00E-07	2,00E-07						9,10E-09	6,56E-08	2,26E-08	1,54E-08		
λDU per ramo			7,66E-07									1,13E-07		
Periodo di prova funzionale, T			8760									8760		
TotaleλDU			7,66E-07									4,93E-04		
λS (diagnostica)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08						
λS*Q.tà	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08						
λS per ramo			2,63E-03				1,13E-06	5,84E-08						
MDT			24				24	24						
TotaleλS			2,63E-03				2,25E-06	5,84E-08						
TotaleλDD	1,21E-06													
TotaleλDU	4,94E-04													
TotaleλS	2,63E-03													
Totale λSYS	**3,13E-03**	**/h**												

Disponibilità di un sistema complesso



CCF								5%
Q.tà	1	1	1	1	2	1	1	
Configurazione	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2	
λDD (diagnostica)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08
λDD*Q.tà	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08
λDD per ramo			1,16E-06				1,01E-06	5,25E-08
MDT			24				24	24
TotaleλDD			1,16E-06				4,93E-11	5,25E-08
λDU (prova funzionale)	3,66E-07	2,00E-07	2,00E-07	9,10E-09	3,28E-08	2,26E-08	1,54E-08	5,84E-09
λDU*Q.tà	3,66E-07	2,00E-07	2,00E-07	9,10E-09	6,56E-08	2,26E-08	1,54E-08	5,84E-09
λDU per ramo			7,66E-07				1,13E-07	5,84E-09
Periodo di prova funzionale, T			8760				8760	8760
TotaleλDU			7,66E-07				1,11E-10	5,84E-09
λS (diagnostica)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08
λS*Q.tà	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08
λS per ramo			2,63E-03				1,13E-06	5,84E-08
MDT			24				24	24
TotaleλS			2,63E-03				2,25E-06	5,84E-08

TotaleλDD	=	1,21E-06	Media (DD)	=	0,99997
TotaleλDU	=	7,72E-07	Media (DU)	=	0,99328
TotaleλS	=	2,63E-03	Media (S)	=	0,94062

TotaleλSYS = 2,63E-03 /h
Disponibilità = 0,9343

12.24. Esempio di foglio dati

I dati del tasso di guasto utilizzati nei precedenti schemi RBD dovrebbero essere visibili nel rapporto e fornire tracciabilità della fonte. La fonte, quando si tratta di dati pubblicati, dovrebbe fornire dettagli sufficienti a permettere a terzi di verificare indipendentemente i dati utilizzati. Ciò potrebbe includere l'identificazione dei documenti, il numero ISBN (se applicabile), il numero di pagina ed il codice.

La Tabella 15 è una tipica tabella dati per i precedenti schemi RBD di esempio.

Descrizione	Codice prodotto	λtotale	λD	λDD	λDU	λS	Commenti/Fonte
Trasmettitore di pressione PT-xxx	PT-xxx	3,68E-06	1,53E-06	1,16E-06	3,66E-07	2,15E-06	Produttori PT-xxx Manuale di sicurezza funzionale, M-xxx-xxx, Mese-20xx
Trasformatore di corrente carico ventola FL-xxx	FL-xxx	5,00E-07	2,00E-07	0,00E+00	2,00E-07	3,00E-07	FARADIP-THREE V6.4, Reliability Data Base. Technis, 26 Orchard Drive, Tonbridge, Kent TN10 4LG, ISBN 0-951-65623-6.
Modulo di comunicazione ControlNet CNB	1756-CNB	1,82E-07	9,10E-08	8,19E-08	9,10E-09	9,10E-08	Documento Allen-Bradley "Using ControlLogix in SIL2 Applications"
Modulo di ingresso analogico	1756-AI16	6,56E-07	3,28E-07	2,95E-07	3,28E-08	3,28E-07	Documento Allen-Bradley "Using ControlLogix in SIL2 Applications"
CPU ControlLogix	1756-L63	4,52E-07	2,26E-07	2,03E-07	2,26E-08	2,26E-07	Documento Allen-Bradley "Using ControlLogix in SIL2 Applications"
Modulo di uscita digitale	1756-OB32	3,07E-07	1,54E-07	1,38E-07	1,54E-08	1,54E-07	Documento Allen-Bradley "Using ControlLogix in SIL2 Applications"

Tabella 14: calcolo PFH/PFD (guasti non rilevati)

12.25. Modellazione dei sistemi di rilevamento incendi e gas (F&G)

Nella modellazione dei sistemi F&G, è importante fornire qualche informazione sulla tolleranza ai guasti. Generalmente, la modellazione della logica ESD o sistemi simili segue la stessa configurazione usata dalla logica di voting del logic solver. Ad esempio, l'affidabilità dei trasmettitori di pressione con logica di voto uno su due (1oo2), su alta pressione da un sistema ESD, sarà modellata come 1oo2. Lo stesso non è sempre vero per i sistemi F&G.

In generale, un'analisi conservativa può essere intrapresa senza basarsi su ipotesi di copertura dei rilevatori e ridondanza nel layout di allarme ma, in pratica, ciò può risultare in un'analisi pessimistica e nel mancato raggiungimento dei target. Dove sorgono tali difficoltà, una conoscenza dettagliata dei pericoli permette di sviluppare un modello più mirato e di eseguire un'analisi più realistica dell'affidabilità.

I sistemi F&G, oltre a proteggere le persone, possono essere usati per proteggere le risorse dell'impianto dai rischi commerciali o per proteggere un sito da un rischio ambientale e sarà l'azione esecutiva richiesta dalla funzione SIF, nel fornire questa protezione, a determinare il modello di affidabilità da usare.

Quando si modella una funzione SIF F&G, per determinare la conformità rispetto ai target di affidabilità hardware (ad es. PFD), è necessario decidere esattamente quale configurazione hardware modellare.

In genere, i dati C&E per una funzione SIF F&G specificano:

a) un qualunque rilevatore di gas su sei (1oo6) in stato di allarme viene indicato come "Single Gas" (allarme singolo) ed attiverà l'allarme nella sala di controllo;
b) due qualunque rilevatori di gas su sei (2oo6) in stato di allarme vengono indicati come "Confirmed Gas" (allarme confermato) ed attiveranno allarmi e segnalatori luminosi sul posto, generando un ESD dell'impianto.

Tuttavia, per una corretta modellazione, dobbiamo capire la funzione SIF ed il pericolo da cui protegge. Sarà l'azione esecutiva richiesta dalla funzione SIF a determinare il modello appropriato da usare.

12.26. Modellazione delle configurazioni di rilevatori dei sistemi F&G

In pratica, in caso di allarme singolo, l'operatore cercherà di capire se è reale, intempestivo o dovuto ad un guasto del rilevatore. L'azione esecutiva viene intrapresa solo in caso di allarme confermato, garantendo l'evacuazione in sicurezza del personale dall'impianto. Questa è la funzione di sicurezza che ha richiamato il SIL target e quindi il caso di cui al precedente punto b) dovrebbe essere il punto di partenza per la modellazione dell'affidabilità: un allarme confermato garantirà l'evacuazione in sicurezza del personale.

Il layout nella Figura 44 mostra sei rilevatori di gas posizionati in una zona e la logica di voting 2oo6 del logic solver è configurata in modo da attivare l'azione esecutiva se 2 dei 6 rilevatori rilevano la presenza di gas.

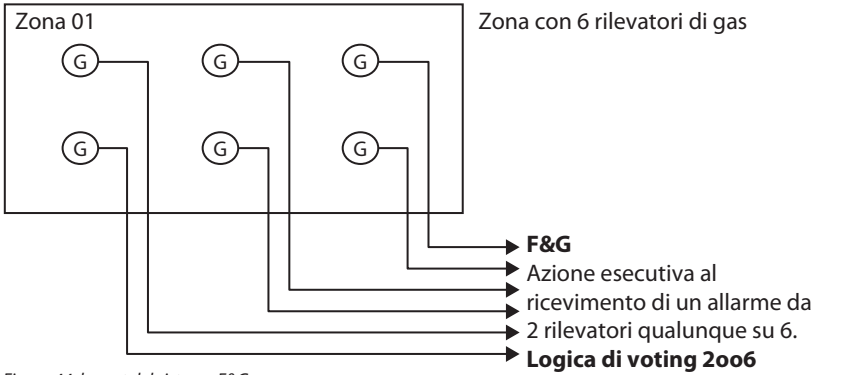


Figura 44: layout del sistema F&G

Tuttavia, la modellazione delle funzioni SIF rispetto alle probabilità PFD target richiede di calcolare la probabilità di mancato intervento per gas quando richiesto. Una fuga di gas sufficientemente estesa da essere pericolosa può trovarsi nell'area di copertura della metà, ad esempio, dei 6 rilevatori (Figura 45).

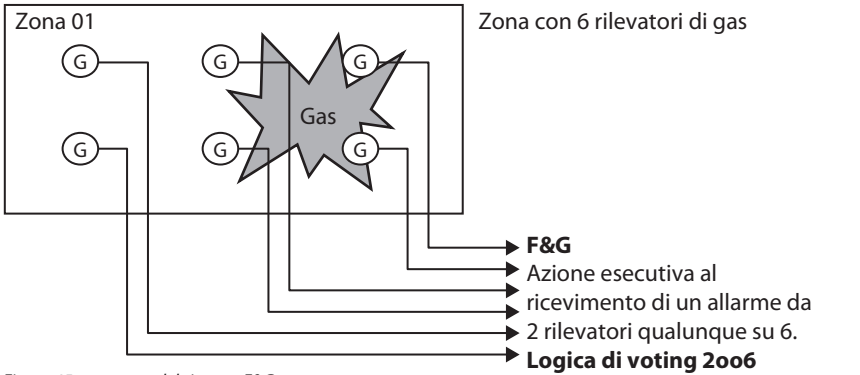


Figura 45: copertura del sistema F&G

In pratica, possiamo richiedere che l'azione esecutiva venga intrapresa non appena possibile ovvero quando solo due sensori si trovano nella nuvola di gas. In questo caso, dovremmo modellare i sensori come 2oo2, senza ridondanza, e conseguentemente nessun guasto dei sensori potrebbe essere tollerato. Se i target vengono ottenuti con una

configurazione non ridondante, questo rappresenterebbe un approccio conservativo perché non basato sulla considerazione della copertura dei rilevatori.

In realtà, è probabile che la PFD del sottosistema dei sensori sia migliore di quella calcolata per una configurazione non ridondante perché, dato il loro posizionamento, esisterà un certo grado di sovrapposizione nella loro copertura ed il guasto di un singolo sensore potrebbe anche essere tollerato.

In termini di modellazione dell'affidabilità, l'analista deve quindi giudicare le massime dimensioni della fuga di gas (dimensioni della nuvola) che potrebbero essere tollerate prima che venga richiesta l'azione esecutiva e stimare quanti sensori rientrano nella nuvola in quel momento.

In questo esempio, se possiamo permettere che la nuvola di gas sia grande abbastanza da interessare 3 sensori prima di innescare l'azione esecutiva, con una logica di voting di 2 su 6, possiamo tollerare il guasto di un sensore. In altre parole, l'affidabilità del rilevamento di gas potrebbe essere modellata come 2 su 3.

12.27. Effetto della scorretta modellazione sulla PFD

Nell'esempio che precede, dato che la logica di voting dei rilevatori di gas è 2oo6, alcuni analisti cedono alla tentazione di modellare l'affidabilità del sistema come 2oo6 anziché come 2oo3 o 2oo2. Ovviamente, la discrepanza risultante nella probabilità PFD globale della funzione di sicurezza e delle sue prestazioni rispetto ai SIL target tra configurazioni ridondanti e non ridondanti può essere significativa.

Ammesso che una certa tolleranza ai guasti possa essere ragionevolmente attestata (ad es. modellando 2oo3 o 2oo4), le differenze risultanti nella probabilità PFD globale della funzione di sicurezza e delle sue prestazioni rispetto ai SIL target saranno piccole. La probabilità PFD per le configurazioni ridondanti è limitata dai guasti per causa comune ed i miglioramenti in termini di probabilità PFD, quindi, non sono significativi quando la tolleranza ai guasti hardware (HFT) aumenta oltre 1.

Tuttavia, se la tolleranza ai guasti non può essere garantita a causa della posizione dei rilevatori o delle dimensioni tollerabili della nuvola di gas nel momento in cui viene richiesta l'azione esecutiva, la discrepanza risultante tra configurazioni ridondanti e non ridondanti può essere significativa, Figura 46.

Nota: la probabilità PFD viene calcolata per tassi di guasto dei sensori e tempi di riparazione tipici e presume un contributo dalle cause comuni per le configurazioni ridondanti. In questo esempio, una tolleranza ai guasti di zero rappresenta una configurazione 2oo2, una tolleranza ai guasti di 1 rappresenta 2oo3, 2 rappresenta 2oo4 e così via.

I risultati mostrano che, a seconda dell'architettura o della tolleranza HFT selezionata per la modellazione, la probabilità PFD calcolata potrebbe rientrare nella fascia SIL1, SIL2 o SIL3.

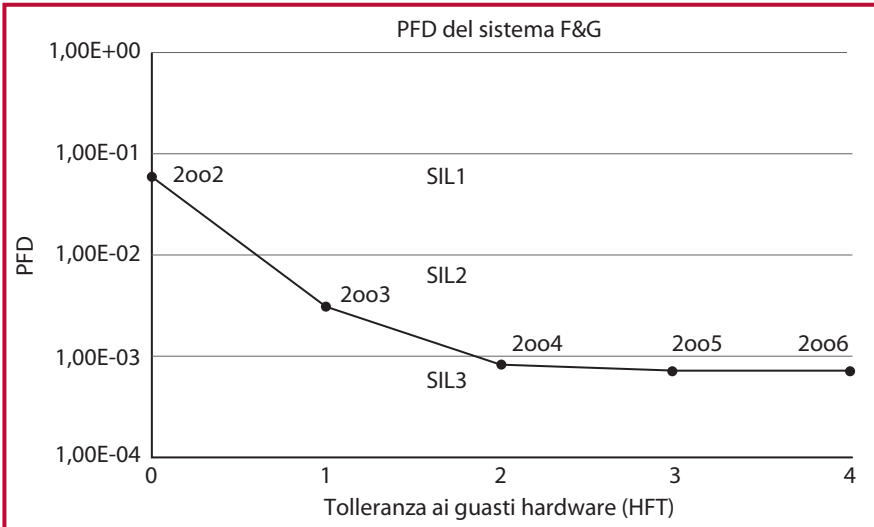


Figura 46: calcolo PFD del sistema F&G

12.28. Effetto della scorretta modellazione sull'architettura

Sulle prestazioni dell'architettura della funzione di sicurezza, una scorretta modellazione avrà un effetto più significativo. Per una determinata percentuale di guasti non pericolosi (SFF), le prestazioni SIL del sottosistema di rilevatori dipendono dalla tolleranza HFT.

Ad esempio, per un rilevatore Tipo B con una percentuale SFF compresa tra il 60% ed il 90%, potrebbero essere attestate le seguenti capacità SIL dell'architettura:

HFT	Configurazione	SIL (architettura)
0	2oo2	SIL1
1	2oo3	SIL2
2	4oo4	SIL3

Anche in questo caso, se l'analista ipotizza una configurazione 2oo6 per la logica di voting, un'architettura ottimistica risulterà nell'attestazione di un livello SIL3 quando, effettivamente, il livello SIL applicabile è inferiore.

12.29. Modellazione delle configurazioni di allarme dei sistemi F&G

Il personale è protetto dai pericoli di incendio e gas da un allarme confermato. Gli allarmi visivi ed acustici sono tutto ciò che serve per garantire l'evacuazione in sicurezza del personale. Quindi, per i pericoli di sicurezza, la configurazione di uscita deve considerare solo la disponibilità di segnalatori visivi ed acustici.

Per i sistemi F&G, l'azione esecutiva può essere generalmente specificata con l'attivazione di 6oo6 allarmi visivi E 4oo4 allarmi acustici. Generalmente, la modellazione di tali configurazioni rende difficile ottenere una probabilità PFD target superiore a SIL1 e questo a causa del numero di dispositivi da includere. Inoltre, dato che gli allarmi ed i segnalatori luminosi hanno una percentuale SFF molto bassa, le loro prestazioni in termini di architettura non possono generalmente superare il livello SIL1 nelle configurazioni simplex.

Tenendo presente che una zona può contenere apparecchiature che possono oscurare un segnalatore luminoso o impedire che un allarme acustico venga udito, una buona prassi dovrebbe mirare a posizionare gli allarmi in modo tale che il personale all'interno della zona pericolosa possa sempre vedere o ascoltare più di un segnalatore alla volta. Se questa ipotesi può essere verificata, l'analista può sfruttare tale tolleranza ai guasti nella modellazione dell'affidabilità della configurazione degli allarmi.

Una configurazione 6oo6 dei segnalatori può coprire 2 o 3 zone separate, magari con 2 o 3 segnalatori per zona. L'analista deve quindi decidere, in base agli schemi di layout dell'impianto, quale tolleranza ai guasti è attestabile per ogni zona e poi modellare di conseguenza, Figura 47.

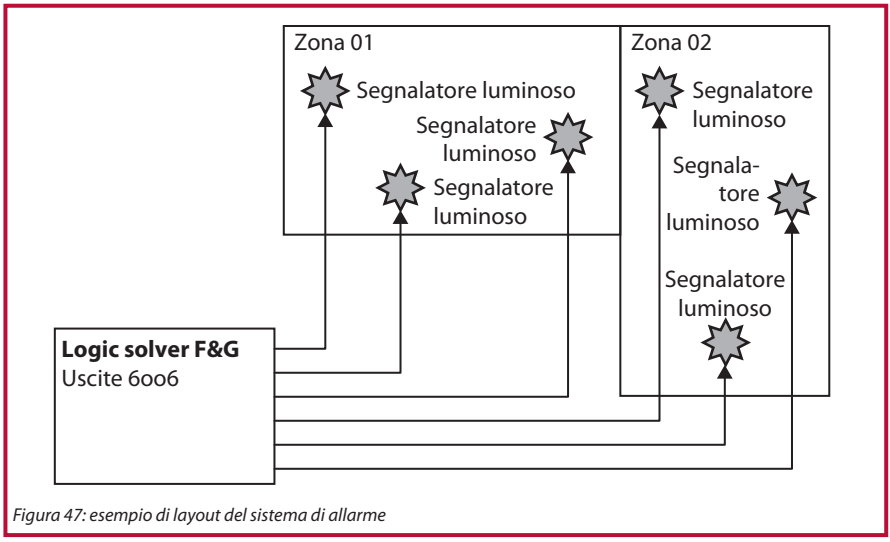


Figura 47: esempio di layout del sistema di allarme

Il fattore chiave è decidere quanti segnalatori luminosi possono essere visti e quanti di questi possono guastarsi senza provocare la perdita della funzione di sicurezza. Nel layout di esempio, è stato deciso che in ogni zona saranno sempre visibili due dei 3 segnalatori luminosi presenti.

In un tale layout, un approccio ragionevole sarebbe quello di modellare ogni zona 1 come 1oo2, essendo sufficiente vedere un solo segnalatore luminoso. Tuttavia, dato che entrambe le zone devono essere protette, entrambe dovrebbero essere incluse nel modello, ovvero 1oo2 + 1oo2.

Per un ulteriore esempio, si possono considerare 6 segnalatori luminosi in una singola zona in cui era stato deciso di poter vedere sempre 4 dei 6 segnalatori luminosi presenti, Figura 48. Poiché è necessario che funzioni almeno uno dei 4 segnalatori luminosi visibili, possiamo modellare gli allarmi come 1oo4.

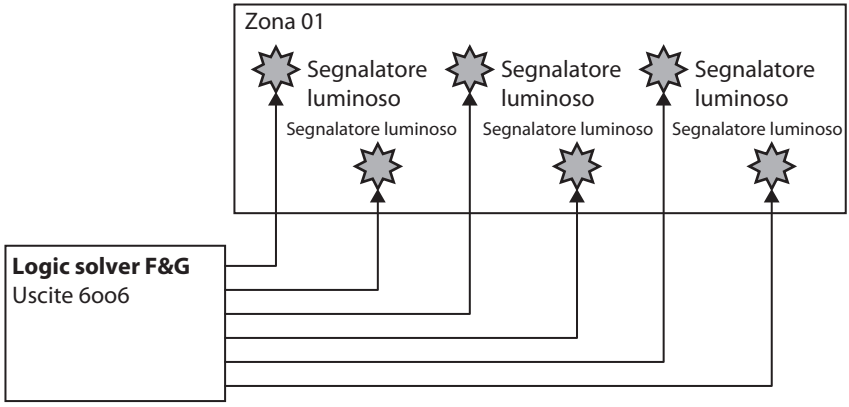


Figura 48: esempio di layout del sistema di allarme (1 zona)

12.30. Attivazione dello spegnimento di emergenza (ESD) da parte dei sistemi F&G

Fino ad ora, non abbiamo menzionato la necessità di generare uno spegnimento ESD dell'impianto in caso di allarme per incendio o gas. L'inclusione dell'intervento ESD nella funzione SIF F&G dipenderà dalle conseguenze del pericolo e dalla protezione richiesta.

Dove il pericolo rappresenta un rischio per la sicurezza delle persone, si può sostenere che gli allarmi sono sufficienti ad assicurare protezione. Generalmente, l'intervento dei sistemi F&G è legato anche all'attivazione di un ESD ma, in diversi casi, ciò serve solo prevenire un aumento del pericolo e a proteggere le risorse dell'impianto. L'intervento ESD può essere richiesto anche come buona prassi per consentire un avviamento più controllato dopo la

risoluzione del pericolo. Il sistema F&G serve a proteggere contro incendi o fughe di gas; il sistema ESD serve a proteggere contro altri pericoli. Ammesso che il sistema F&G soddisfi i target in termini di riduzione del rischio, non dovrebbe esserci ragione, a parte quella di cui sopra, per l'intervento ESD. Il sistema ESD, quindi, non sarebbe normalmente incluso nella funzione SIF F&G.

Esistono tuttavia delle eccezioni. Quando il pericolo comporta danni all'ambiente o alle risorse dell'impianto, gli allarmi non bastano a fornire protezione e quindi, al rilevamento di incendio o gas, può essere necessario isolare l'impianto. In tali casi, nella modellazione dell'affidabilità delle funzioni SIF F&G, è necessario includere lo spegnimento e l'isolamento.

12.31. Sommario

Come si può vedere, la modellazione del sottosistema di ingresso può dare risultati ottimistici se viene modellata la configurazione della logica di voting anziché la tolleranza ai guasti dei rilevatori. Lo stesso approccio, quando si modella il sottosistema di uscita, darà risultati molto pessimistici. Tra i due sottosistemi, l'approccio alla modellazione adottato può comportare una grande variazione nelle prestazioni calcolate della PFD e dell'architettura e, di conseguenza, una grande variazione del SIL rivendicato.

È quindi importante adottare un approccio ponderato alla modellazione dei sistemi F&G ed avere una chiara comprensione delle tecniche di modellazione, dei pericoli e dei sistemi analizzati. Ciò garantirà di ottenere un'accurata valutazione della riduzione del rischio fornita da un sistema F&G e gli utilizzatori finali non sono fuorviati da rivendicazioni ottimistiche.

13. Verifica SIL

13.1. Conformità ai target dei livelli di integrità della sicurezza

Diverse persone chiedono che cosa devono fare per dimostrare la conformità. Non è sufficiente acquistare componenti "certificati SIL" e presumere che questo basti ad ottenere la conformità; inoltre, poiché la norma non è prescrittiva, non è neanche possibile avere una checklist di ciò che bisogna fare. In realtà, quanto fate per ottenere la conformità dipenderà da diverse cose. L'approccio dipenderà da quante informazioni o dati sono disponibili; il grado di approfondimento dell'analisi o il rigore applicato devono soddisfare il vostro cliente o il regolatore ma soprattutto dovreste arrivare alla conclusione di aver fatto abbastanza.

Se qualcosa andasse storto e qualcuno rimanesse ucciso, potreste affrontare le famiglie e dimostrare che avete fatto tutto ciò che era ragionevole aspettarsi da voi?

Un piano suggerito per la conformità sarebbe quello di soddisfare i requisiti della norma IEC 61511-1, 10 e 12. Questi includono i seguenti sottoarticoli, come illustrato nella Figura 49:

- Requisiti di comportamento del sistema al rilevamento di un guasto [13.2];
- Tolleranza ai guasti hardware [13.3];
- Selezione di componenti e sottosistemi [13.4];
- Dispositivi di campo [13.5];
- Interfacce operatore, manutentore e di comunicazione con il sistema SIS [13.6];
- Requisiti di progettazione della manutenzione o del collaudo [13.7];
- Probabilità di guasto SIF [13.8];
- Software applicativo [13.9].

Sono illustrati anche gli eventuali requisiti più dettagliati di questi punti.

Conformità con la norma IEC 61511-1, 5: la gestione della sicurezza funzionale è trattata anche nella Sezione [18].

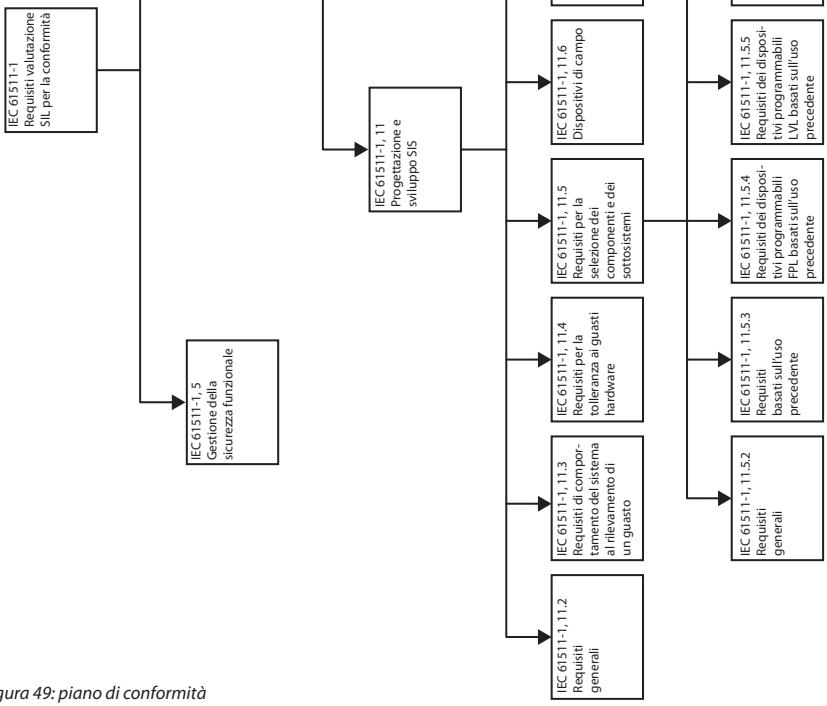


Figura 49: piano di conformità

13.2. Requisiti di comportamento del sistema al rilevamento di un guasto, IEC 61511-1, 11.3

Il comportamento del sistema al rilevamento di un guasto dovrebbe essere specificato. Ad esempio, può essere dettagliato nella specifica SRS o nella specifica di progetto.

Di seguito, sono riportati tipici esempi del tipo di parametri che potrebbero essere inclusi:

1. Tutti i blocchi di uscita hanno una logica di voting 1oo2 alla domanda del PLC e tornano a 1oo1 al rilevamento della perdita di comunicazione da un PLC.
2. La specifica di progetto stabilisce che si applica un principio a prova di guasto. Tutti gli elementi di spegnimento del sistema SIS sono basati sul principio di guasto in sicurezza.
3. Nel caso di un sistema ESD, è stata implementata una funzione di intervento per diseccitazione.
4. Nel caso del sistema F&G, è stato implementato il rilascio di estinguente con intervento per eccitazione. Il rilevamento di un singolo guasto pericoloso in una configurazione ridondante è indicato da una condizione di allarme. Il sistema F&G continua a funzionare in modo sicuro per la durata ammessa del tempo di riparazione e sono state implementate altre misure di riduzione del rischio quali la fornitura di estinguente tramite un dispositivo manuale cablato.

13.3. Requisiti per la tolleranza ai guasti hardware, IEC 61511-1, 11.4

13.3.1. Approccio

Per soddisfare i requisiti della tolleranza ai guasti hardware (HFT), è necessario procedere ad una valutazione quantitativa rispetto alla percentuale di guasti non pericolosi (SFF) ed ai vincoli hardware.

13.3.2. Percentuale di guasti non pericolosi

Nel contesto dell'integrità della sicurezza hardware, il livello SIL più alto raggiungibile da una funzione di sicurezza è limitato dalla tolleranza HFT e dalla percentuale SFF dei sottosistemi che eseguono quella funzione di sicurezza.

Una tolleranza ai guasti hardware di 1 indica che l'architettura del sottosistema è tale che un guasto pericoloso di uno dei sottosistemi non impedisce l'azione di sicurezza; in altre parole, una configurazione 1oo2 o 2oo3 avrebbe una tolleranza HFT di 1 ed una configurazione 1oo3 o 2oo4 avrebbe una tolleranza di 2.

Rispetto a questi requisiti, la norma IEC 61508 [19.1] fornisce le seguenti istruzioni aggiuntive:

- una tolleranza ai guasti hardware di N significa che N+1 guasti potrebbero provocare la perdita della funzione di sicurezza. Nel determinare la tolleranza ai guasti hardware, non bisognerebbe considerare altre misure, quali la diagnostica, che possono controllare gli effetti dei guasti;
- quando un guasto provoca direttamente il verificarsi di uno o più guasti conseguenti, questi sono considerati come un guasto singolo;
- nel determinare la tolleranza ai guasti hardware, alcuni guasti possono essere esclusi, a condizione che la loro frequenza sia molto bassa in relazione ai requisiti di integrità della sicurezza del sottosistema. Qualunque esclusione di guasti deve essere debitamente giustificata e documentata.

Si utilizzano le seguenti relazioni generali:

$$SFF = \Sigma (\Sigma \lambda_S + \Sigma \lambda_{DD})/(\Sigma \lambda_S + \Sigma \lambda_D)$$ Rif. IEC 61508-2.C.1

Dove:

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

Per ogni elemento della funzione di sicurezza, dovrebbe essere calcolata la percentuale SFF. Il valore dovrebbe poi essere utilizzato nella Tabella 16 per determinare la conformità SIL per il livello di tolleranza ai guasti hardware.

13.3.3. Vincoli hardware

La norma IEC 61511-1, 11.4.5 permette la valutazione della tolleranza ai guasti hardware mediante i requisiti di IEC 61508-2, Tabelle 2 e 3.

Nella norma IEC 61508 [19.1], i sottosistemi sono categorizzati come Tipo A o Tipo B. Generalmente, se le modalità di guasto sono ben definite, il comportamento in condizioni di guasto può essere determinato esaurientemente ed esistono sufficienti ed adeguati dati storici, il sottosistema può essere considerato di Tipo A. Se una qualunque di questa condizioni non sussiste, il sottosistema deve essere considerato di Tipo B.

I semplici dispositivi meccanici, come le valvole, sono solitamente considerati di Tipo A. I logic solver sono generalmente di Tipo B in quanto, avendo alcune capacità di elaborazione, il loro comportamento in condizioni di guasto non può essere determinato con precisione. I sensori possono essere di Tipo A o di Tipo B, a seconda della tecnologia e della complessità del dispositivo.

I vincoli hardware di una funzione di sicurezza sono riepilogati nella Tabella 16.

Definizione dei sottosistemi di Tipo A: Completa definizione delle modalità di guasto di tutte le parti costituenti, completa determinazione del comportamento del sottosistema in condizioni di guasto e disponibilità sufficiente di dati storici affidabili a supporto dei tassi di guasto attestati per guasti pericolosi rilevati e non rilevati			
Percentuale di guasti non pericolosi	Tolleranza ai guasti hardware (N)		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% – <90%	SIL2	SIL3	SIL4
90% – <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4
Definizione dei sottosistemi di Tipo B: Incompleta definizione della modalità di guasto di almeno una parte costituente, incompleta determinazione del comportamento del sottosistema in condizioni di guasto e disponibilità insufficiente di dati storici affidabili a supporto dei tassi di guasto attestati per guasti pericolosi rilevati e non rilevati			
Percentuale di guasti non pericolosi	Tolleranza ai guasti hardware (N)		
	0	1	2
<60%	Non ammessa	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Tabella 16: vincoli hardware

Nota: una tolleranza ai guasti hardware di N significa che N+1 guasti potrebbero provocare la perdita della funzione di sicurezza.

13.3.4. Esempio

In questo esempio, Figura 50, la funzione di sicurezza è costituita da due trasmettitori di livello che funzionano in una configurazione 1oo2. Se un trasmettitore rileva un livello alto, il PLC Allen Bradley diseccita l'elettrovalvola che consentirà alla valvola ESD di chiudersi.

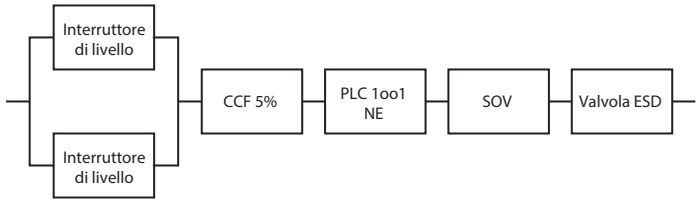
La valutazione delle prestazioni hardware richiede che prima si identifichi di che tipo è ogni elemento (A o B). In genere, ciò può essere determinato usando le definizioni fornite nella Tabella 16. Come regola generale, per poter considerare un elemento di Tipo A, bisogna essere sicuri delle modalità di guasto e del comportamento di guasto, oltre ad avere dati di guasto affidabili. In caso contrario, l'elemento deve essere considerato di Tipo B.

I dati di guasto che abbiamo per ogni elemento ci consentono di calcolare la percentuale

SFF. Nella Figura 50, sotto ogni elemento, sono riportati il tipo di elemento e la percentuale SFF.

La tolleranza HFT si riferisce al livello di tolleranza ai guasti di ogni elemento. I trasmettitori di livello che funzionano in configurazione 1oo2 hanno una tolleranza HFT di 1. Tutti gli altri elementi non hanno tolleranza ai guasti e quindi hanno una tolleranza HFT di 0.

Infine, usando queste informazioni nella Tabella 16, può essere determinato il livello SIL per le prestazioni hardware di ogni elemento.



Tipo	A	B	A	A
SFF	0,40	0,95	0,72	0,25
HFT	1	0	0	0
SIL dell'architettura	2	2	2	1
SIL ammesso (arch.)	1			
SIL ammesso globale	**SIL1**			

Figura 50: esempio di funzione strumentata di sicurezza

I livellostati sono di Tipo A; quindi, si applicano i criteri del Tipo A. Con una percentuale SFF di 0,40 ed una tolleranza ai guasti di 1, i trasmettitori di livello si conformano ai vincoli hardware del livello SIL2.

Anche l'elettrovalvola e la valvola ESD possono essere valutati in modo simile. L'elettrovalvola, sempre di Tipo A, ha una tolleranza ai guasti di 0 ed una percentuale SFF di 0,72; quindi è SIL2. La valvola ESD, di Tipo A, ha una tolleranza ai guasti di 0 ed un SFF di 0,25; quindi è SIL1.

Definizione dei sottosistemi di Tipo A: Completa definizione delle modalità di guasto di tutte le parti costituenti, completa determinazione del comportamento del sottosistema in condizioni di guasto e disponibilità sufficiente di dati storici affidabili a supporto dei tassi di guasto attestati per guasti pericolosi rilevati e non rilevati			
Percentuale di guasti non pericolosi (SSF)	Tolleranza ai guasti hardware (N)		
	0	1	2
<60%	**SIL1 (valore ESD)**	**SIL2 (LT)**	SIL3
60% – <90%	**SIL2 (SOV)**	SIL3	SIL4
90% – <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

Figura 51: vincoli hardware del trasmettitore di livello

Il PLC è stato considerato un dispositivo di Tipo B. Ciò vale per la maggior parte dei PLC perché, essendo controllati da software, sussiste un elemento di incertezza sul loro comportamento di guasto e, di conseguenza, non soddisfano tutte le condizioni richieste per il Tipo A.

La valutazione del PLC deve quindi essere effettuata rispetto ai requisiti del Tipo B, Figura 52.

Definizione dei sottosistemi di Tipo B: Incompleta definizione della modalità di guasto di almeno una parte costituente, incompleta determinazione del comportamento del sottosistema in condizioni di guasto e disponibilità insufficiente di dati storici affidabili a supporto dei tassi di guasto rivendicati per guasti pericolosi rilevati e non rilevati			
Percentuale di guasti non pericolosi (SSF)	Tolleranza ai guasti hardware (N)		
	0	1	2
<60%	Non ammessa	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	**SIL2 (PLC)**	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Figura 52: vincoli hardware del PLC

Nella Figura 50 sono riepilogate le prestazioni SIL dell'hardware di ogni elemento ed il livello SIL attestabile per l'intera funzione di sicurezza è SIL1. Le prestazioni SIL dell'hardware dell'intera funzione di sicurezza sono limitate dal più basso SIL rivendicato.

13.4. Requisiti per la selezione di componenti e sottosistemi, IEC 61511-1, 11.5

13.4.1. Approccio

Per le applicazioni del settore di processo, la selezione di componenti e sottosistemi può essere basata sulla valutazione dell'adeguatezza. L'obiettivo è quello di specificare i requisiti:

- per la selezione dei componenti e dei sottosistemi;
- per integrare un componente o sottosistema nell'architettura di una funzione SIF;
- per specificare i criteri di accettazione dei componenti e dei sottosistemi.

13.4.2. Requisiti generali, IEC 61511-1, 11.5.2

Questa procedura non dovrebbe essere usata per applicazioni SIL4 ma per tutti gli altri componenti e sottosistemi.

La dimostrazione di adeguatezza deve includere una valutazione del livello SIL che consiste nel calcolo della probabilità PFD e dei vincoli hardware rispetto ai target.

La dimostrazione di adeguatezza deve includere anche la considerazione della documentazione dell'hardware e del software integrato del costruttore. La documentazione che accompagna i componenti ed i sottosistemi selezionati sarà costituita da specifiche tecniche che illustrano funzionalità e prestazioni ambientali. La specifica FDS deve quindi includere una dichiarazione che giustifichi l'adeguatezza dei componenti e dei sottosistemi selezionati ai requisiti funzionali in base alla documentazione del costruttore.

Componenti e sottosistemi devono essere coerenti con la specifica dei requisiti di sicurezza SRS. In pratica, componenti e sottosistemi vengono selezionati in base alla loro capacità di soddisfare i requisiti di sicurezza. La dimostrazione di conformità avviene mediante valutazione e valgono sempre i requisiti per vincoli hardware e PFD.

13.4.3. Uso precedente, IEC 61511-1, 11.5.3

Prima di tutto, la selezione dei componenti dovrebbe avvenire mediante specifica di approvvigionamento da fornitori approvati.

La considerazione del sistema QMS del costruttore e dei sistemi di gestione della configurazione dovrebbe far parte della valutazione del fornitore e della prova di adeguatezza presentata nella specifica FDS.

Per tutti i componenti ed i sottosistemi selezionati, la specifica FDS dovrebbe anche giustificare l'uso accumulato. La giustificazione può essere basata su:

- ore dispositivo accumulate per SIL1 e dispositivi di campo;
- ore dispositivo accumulate con identificazione dei guasti pericolosi per SIL2 ed elementi complessi.

Per le applicazioni con logic solver SIL3, è richiesta la certificazione.

L'uso accumulato richiesto per un componente o un sottosistema dipenderà dal tasso di guasto target e dalla segnalazione di eventuali guasti. La Figura 53 è solo di riferimento e mostra il numero richiesto di anni dispositivo accumulati (numero di dispositivi x anni in uso) per vari valori di tasso di guasto target.

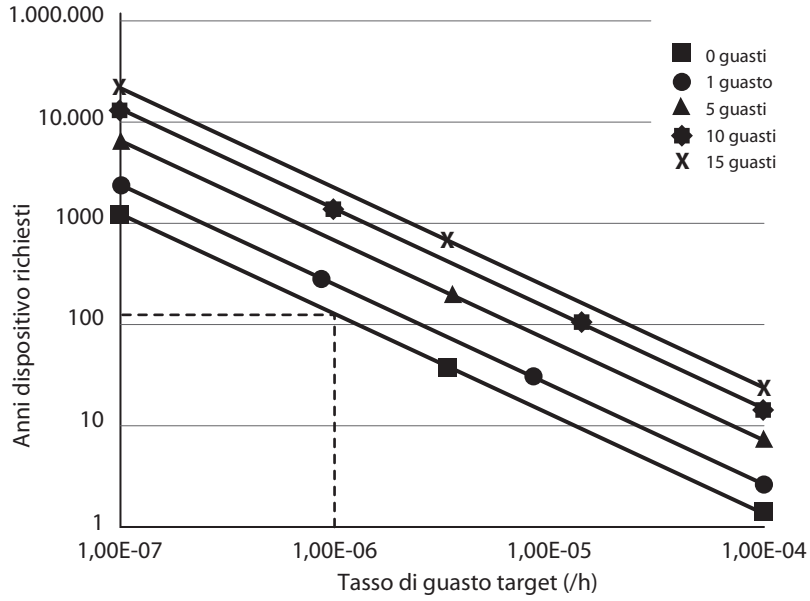


Figura 53: guida sull'uso richiesto

Ad esempio, se il tasso di guasto target è 1,00E-06/ora e sono stati segnalati zero guasti, sulla Figura 53 ciò corrisponde a circa 137 anni dispositivo che possono essere ottenuti con 14 dispositivi che funzionano senza guasti per 10 anni. Se sono stati segnalati guasti nella popolazione di dispositivi, l'effettivo tasso di guasto dei dispositivi sarà più alto e, di conseguenza, saranno necessarie più ore operative senza guasti per giustificare lo stesso tasso di guasto target.

La figura è basata su una distribuzione X^2 con un limite di affidabilità del 70% e dovrebbe essere usata solo per avere un'indicazione di quando è stato accumulato un sufficiente numero di anni dispositivo.

La norma IEC 61511 richiede anche il monitoraggio documentato dei dati dei resi ed un processo di modifica, da parte del costruttore, che valuti l'impatto dei guasti segnalati.

In pratica, le informazioni di guasto sono raramente disponibili e la selezione può quindi includere una valutazione dei componenti e dei sottosistemi per assicurare che funzioneranno come richiesto. Questa valutazione può richiedere discussioni con altri utenti o con i costruttori o utenti di dispositivi o applicazioni simili. Tale giustificazione di supporto dovrebbe essere documentata nella specifica FDS nell'ambito delle considerazioni sull'adeguatezza di componenti e sottosistemi.

13.4.4. Dispositivi programmabili FPL (linguaggi di programmazione fissi), IEC 61511-1, 11.5.4

Quando devono essere usati componenti e sottosistemi programmabili FPL (ad es. dispositivi di campo), per le applicazioni SIL1 e SIL2 dovrebbero essere soddisfatti i requisiti generali [13.4.2], i requisiti relativi all'uso precedente [13.4.3] ed i requisiti che seguono per i componenti ed i sottosistemi programmabili FPL.

Inoltre, per ogni componente selezionato, la specifica FDS deve giustificare la selezione dei componenti FPL dichiarando che il componente risponde, in termini di funzionalità, ai requisiti specificati tra cui:

a) caratteristiche dei segnali di ingresso e di uscita;
b) modalità d'uso;
c) funzioni e configurazioni utilizzate;
d) scarsa probabilità che le funzioni inutilizzate influiscano sulle funzioni di sicurezza.

Per le applicazioni SIL3, è richiesta la realizzazione di una valutazione formale.

Un approccio alternativo adottato da alcuni integratori di sistemi è quello di procurare un dispositivo FPL conforme SIL3. Questi dispositivi dovrebbero essere già stati sottoposti ad una valutazione formale da un'organizzazione a ciò preposta e, insieme alle giustificazioni documentali di supporto, dovrebbe essere fornita la certificazione SIL3.

L'evidenza dovrebbe dimostrare che il dispositivo è in grado di eseguire la funzione richiesta e che la probabilità di guasti pericolosi, dovuti a guasti hardware casuali o a guasti hardware o software sistematici, è sufficientemente bassa. Per il dispositivo,

dovrebbe essere disponibile anche un manuale di sicurezza che indichi con precisione i vincoli di funzionamento e manutenzione.

13.4.5. Dispositivi programmabili LVL (linguaggi a variabilità limitata), IEC 61511-1, 11.5.5

Quando devono essere usati componenti e sottosistemi programmabili LVL (ad es. logic solver), per le applicazioni SIL1 e SIL2 dovrebbero essere soddisfatti i requisiti generali [13.4.2], i requisiti relativi all'uso precedente [13.4.3], i requisiti per i dispositivi programmabili FPL [13.4.4] ed i requisiti che seguono per i componenti ed i sottosistemi programmabili LVL.

La documentazione dovrebbe giustificare che dove sussiste una differenza già sperimentata tra il profilo operativo e l'ambiente fisico, ed il profilo operativo e l'ambiente fisico utilizzati nella funzione di sicurezza, la specifica FDS deve identificare queste differenze e dimostrare che la probabilità PFD non sarà pregiudicata.

Per applicazioni SIL 1 o 2, è possibile usare un logic solver PE elettronico programmabile (un logic solver PE per uso industriale generale specificamente configurato per l'utilizzo in applicazioni di sicurezza) a condizione che sia giustificato nella documentazione.

La documentazione della specifica messa a disposizione dal costruttore deve dimostrare che, su hardware e software, sono disponibili informazioni adeguate a garantire la comprensione del comportamento di guasto. Ciò dovrebbe essere confermato nella specifica FDS elencando tutte le modalità di guasto pericoloso ed identificando, dove pertinente, le misure diagnostiche e le azioni di protezione. La specifica FDS dovrebbe identificare anche i mezzi di protezione dalle modifiche non autorizzate o involontarie.

Per le applicazioni con logic solver SIL2, la specifica FDS dovrebbe confermare la tecnica di protezione prevista contro i guasti durante l'esecuzione del programma:

a) monitoraggio della sequenza del programma;
b) protezione del codice da modifiche o rilevamento dei guasti mediante monitoraggio on-line;
c) asserzione dei guasti o programmazione diverse;
d) controllo del campo delle variabili o controllo della plausibilità dei valori;
e) approccio modulare;
f) utilizzo di standard di codifica appropriati per il software integrato.

Inoltre, deve essere dimostrato che:

g) il collaudo è stato effettuato in configurazioni tipiche, con casi di test rappresentativi dei profili operativi previsti;
h) sono stati utilizzati componenti e moduli software affidabili;
i) il sistema è stato sottoposto ad analisi dinamica e collaudo;
j) il sistema non si avvale di intelligenza artificiale o di riconfigurazione dinamica;
k) è stata realizzata una prova documentata di generazione dei guasti.

Per le applicazioni SIL2, la specifica FDS dovrebbe identificare i vincoli di funzionamento, manutenzione e rilevamento guasti riguardanti le configurazioni del logic solver PE ed i profili operativi previsti.

Per le applicazioni SIL3, la documentazione dovrebbe presentare la certificazione SIL per qualunque logic solver LVL.

13.4.6. Dispositivi programmabili FVL (linguaggi a variabilità completa), IEC 61511-1, 11.5.6

La documentazione dovrebbe presentare la certificazione SIL di ogni logic solver FVL.

13.5. Dispositivi di campo, IEC 61511-1, 11.6

Per la selezione dei dispositivi di campo, dovrebbero essere soddisfatti i requisiti generali [13.4.2], i requisiti relativi all'uso precedente [13.4.3] ed i requisiti che seguono per i dispositivi di campo. Se pertinente, dovrebbero essere soddisfatti anche i requisiti per i dispositivi programmabili FPL.

I dispositivi di campo devono essere selezionati ed installati in modo da minimizzare i guasti che potrebbero comportare informazioni imprecise a causa delle condizioni di processo ed ambientali. Le condizioni che dovrebbero essere considerate includono corrosione, congelamento dei materiali nei tubi, solidi in sospensione, polimerizzazione, cottura, temperature e pressioni estreme, condensazione nelle linee di impulso a secco e condensazione insufficiente nelle linee di impulso ad umido.

Per i dispositivi di campo, la documentazione della specifica dovrebbe dimostrare che il componente risponde, in termini di funzionalità, ai requisiti specificati per tutte le condizioni di processo ed ambientali e la probabilità FDS dovrebbe confermarlo. La specifica FDS dovrebbe anche confermare che tutti i circuiti discreti di ingresso/uscita con eccitazione all'intervento applichino un metodo che garantisce l'integrità dei circuiti e dell'alimentazione, ad es. monitoraggio di linea.

I sensori intelligenti devono essere protetti da scrittura per prevenirne la modifica involontaria da una postazione remota, a meno che un'adeguata analisi della sicurezza ne permetta l'uso in lettura/scrittura.

13.6. Interfacce operatore, manutentore e di comunicazione, IEC 61511-1, 11.7

Per tutte le interfacce di comunicazione, dovrebbero essere soddisfatti i seguenti requisiti.

L'interfaccia di comunicazione del sistema SIS deve garantire che eventuali guasti dell'interfaccia di comunicazione non pregiudichino la capacità del sistema SIS di portare il processo ad uno stato sicuro. Ciò dovrebbe essere confermato nella documentazione di progetto.

La documentazione dovrebbe anche confermare:

a) il tasso di errore previsto della rete di comunicazione;
b) che la comunicazione con il sistema BPCS e le periferiche non inciderà sulla funzione SIF;
c) che l'interfaccia di comunicazione è sufficientemente robusta da sopportare i disturbi elettromagnetici – tra cui le sovratensioni momentanee – senza provocare un guasto pericoloso della funzione SIF;
d) che l'interfaccia di comunicazione è adatta alla comunicazione tra dispositivi che fanno riferimento a potenziali di massa differenti. NOTA: può essere necessario un supporto alternativo (ad es. fibre ottiche).

13.7. Requisiti di progetto relativi a manutenzione o collaudo, IEC 61511-1, 11.8

Il sistema SIS dovrebbe essere tale che il collaudo possa essere realizzato end-to-end o in parti. Ciò, come opportuno, prende in considerazione quanto segue:

- Prova funzionale on-line – il tipo di prova deve garantire che i guasti non rilevati possano essere adeguatamente rivelati;
- Strutture di prova e bypass – se una qualunque parte del sistema SIS viene bypassata a fini di manutenzione o collaudo, l'operatore dovrebbe essere avvisato;
- La forzatura degli ingressi e delle uscite non dovrebbe essere ammessa senza la messa offline del sistema SIS, a meno che non siano in atto procedure e misure di protezione adeguate. Come per la funzione di bypass, l'operatore deve essere avvisato della forzatura di qualunque ingresso/uscita.

13.8. Probabilità di guasto SIF, IEC 61511-1, 11.9

Fare riferimento alla Sezione [14].

13.9. Requisiti per il software applicativo, IEC 61511-1, 12

La norma IEC 61511-1, 12 elenca i requisiti applicabili a qualunque software integrato in un sistema SIS o utilizzato per sviluppare un sistema SIS. Il requisito definisce i requisiti del ciclo di vita della sicurezza del software applicativo per garantire che:

- tutte le attività richieste per sviluppare il software applicativo siano state definite;
- gli strumenti software utilizzati per sviluppare e verificare il software applicativo (software di utilità) siano completamente definiti;
- sia in atto un piano per rispondere agli obiettivi di sicurezza funzionale.

Il requisito generale è quello di definire le fasi applicabili del ciclo di vita della sicurezza del software da considerare e documentare tutte le corrispondenti informazioni. Tra le possibili informazioni ci sono le seguenti:

- specifica dei requisiti di sicurezza del software – in modo simile a quanto previsto per i requisiti hardware, è necessario definire una specifica che elenca tutti i requisiti di sicurezza software in modo chiaro e strutturato e che permetta al team di progetto di sviluppare il software applicativo di conseguenza;
- pianificazione della validazione della sicurezza del software – dovrebbe essere realizzata nell'ambito della pianificazione della validazione SIS globale;
- progettazione e sviluppo – il software applicativo deve essere sviluppato per rispondere ai requisiti di progetto del sistema, delineati nella specifica SRS del software, in termini di funzioni di sicurezza e di livelli di integrità della sicurezza. Per la verifica, la validazione, la valutazione e la modifica, dovrebbero essere utilizzati linguaggi e strumenti di programmazione e supporto di livello adeguato. Il design dovrebbe essere modulare e strutturato, in modo da facilitare le prove e consentire modifiche sicure. Per verificarne la corretta funzionalità, dovrebbe essere realizzato un adeguato collaudo dei moduli software. Va sottolineato che la verifica dovrebbe essere realizzata per ogni fase del ciclo di vita della sicurezza del software;
- Integrazione – una volta testato e verificato, il software deve essere integrato nel sottosistema SIS e testato per dimostrare che, quando in esecuzione sull'hardware, risponda ai requisiti riportati nella specifica SRS;
- validazione della sicurezza del software – dovrebbe essere realizzata nell'ambito della validazione SIS globale (fase 5);
- modifica – qualunque modifica del software validato dovrebbe essere realizzata in modo controllato per garantire il mantenimento dell'integrità del software.

14. Probabilità di guasto SIF, IEC 61511-1, 11.9

14.1. Conformità con la norma

Fino ad ora, abbiamo identificato di dover stabilire le misure di affidabilità target per garantire che il rischio globale non superi il massimo rischio tollerabile.

Abbiamo anche visto che la misura di affidabilità target può essere espressa in SIL e che, per la conformità con la norma, dobbiamo dimostrare non solo che la funzione di sicurezza risponde ai target quantitativi ma che noi applichiamo adeguati controlli.

Conformarsi alla norma richiede che le misure di affidabilità target siano adeguate al livello SIL applicato.

14.2. Requisiti di affidabilità dei target SIL

La probabilità PFD di ogni livello SIL dipende dalla modalità di funzionamento in cui si prevede di usare il sistema SIS rispetto alla frequenza delle domande di intervento. Queste sono definite nella Sezione [6.9] e possono essere:

Modalità su domanda – quando, in risposta alle condizioni di processo o ad altre domande, viene intrapresa una specifica azione. In caso di guasto pericoloso della funzione SIF, il potenziale pericolo si verifica solo in presenza di un guasto del processo del sistema BPCS;

Modalità continua – quando, in caso di guasto pericoloso della funzione SIF, il potenziale pericolo si verifica senza un ulteriore guasto, a meno che siano state adottate misure di prevenzione.

In base a questi criteri, è possibile applicare i target adeguati, presentati nella Tabella 17.

Livello SIL	**Modalità su domanda** Probabilità di guasto su domanda	**Modalità continua** Tasso di guasto all'ora
SIL4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
SIL3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
SIL2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
SIL1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Tabella 17: PFD e tassi di guasto specificati in base al SIL

14.3. Calcolo della probabilità PFD di una funzione di sicurezza in modalità su domanda

Quando si eseguono i calcoli di affidabilità, si presume che i guasti si verifichino casualmente nel tempo ad un tasso costante e che, quando si verifica un guasto,

l'elemento in guasto non sarà disponibile fino al rilevamento ed alla riparazione del guasto.

Nel calcolo della probabilità PFD, essenzialmente calcoliamo la probabilità che il sistema SIS non sia disponibile nel momento in cui ne viene richiesto l'intervento. Per un sistema ridondante 1oo2, considerato il guasto di un canale, la probabilità PFD è la probabilità che, durante il tempo di fermo del primo, si guasti anche il secondo canale.

Nel calcolo della probabilità PFD, è possibile usare le seguenti relazioni generali. Le equazioni utilizzate sono semplificate rispetto alle equazioni standard e sono derivate al punto [19.6].

Per i guasti rilevati:

$PFD1oo1 = \lambda_{DD}.MDT$	Rif. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DD}^2.MDT^2 + \beta.\lambda_{DD}.MDT$	Rif. IEC 61508-6, B.3.2.2.2

Per i guasti non rilevati:

$PFD1oo1 = \lambda_{DU}.T_P/2$	Rif. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DU}^2.Tp2/3 + \beta.\lambda_{DU}.T_P/2$	Rif. IEC 61508-6, B.3.2.2.2

Dove λ_{DD} è il tasso di guasto rilevato pericoloso, λ_{DU} è il tasso di guasto non rilevato pericoloso e β è il contributo dai guasti per causa comune, sezione [12.17]. T_P è l'intervallo di prova funzionale e MDT è il tempo medio di indisponibilità.

Le forme generiche di queste equazioni per varie configurazioni, sia per i sistemi in modalità continua che per quelli in modalità su domanda, sono esaminate al punto [12.9].

14.4. Tassi di guasto

Nel calcolo di PFD e SFF, l'analisi usa l'ipotesi di base della norma IEC 61508-6, Allegato B.3 per cui i tassi di guasto dei componenti sono costanti per tutta la vita del sistema.

I tassi di guasto utilizzati nei calcoli possono essere ottenuti dall'analisi FMECA, quantificati mediante i dati storici o facendo riferimento a dati pubblicati dalle fonti di settore. I tassi di guasto utilizzati dovrebbero essere confrontati ai dati disponibili per moduli simili a livello di complessità e tecnologia. Questo approccio può ritenersi conservativo in termini di modellazione dell'affidabilità ed offre buone garanzie di poter ottenere in servizio le prestazioni di affidabilità calcolate.

I tassi di guasto e le loro fonti sono discussi al punto 14.8.

14.5. Modellazione dell'affidabilità

Nell'esempio di cui al punto [6.5], il processo e la funzione SIF sono evidenziati, Figura 54.

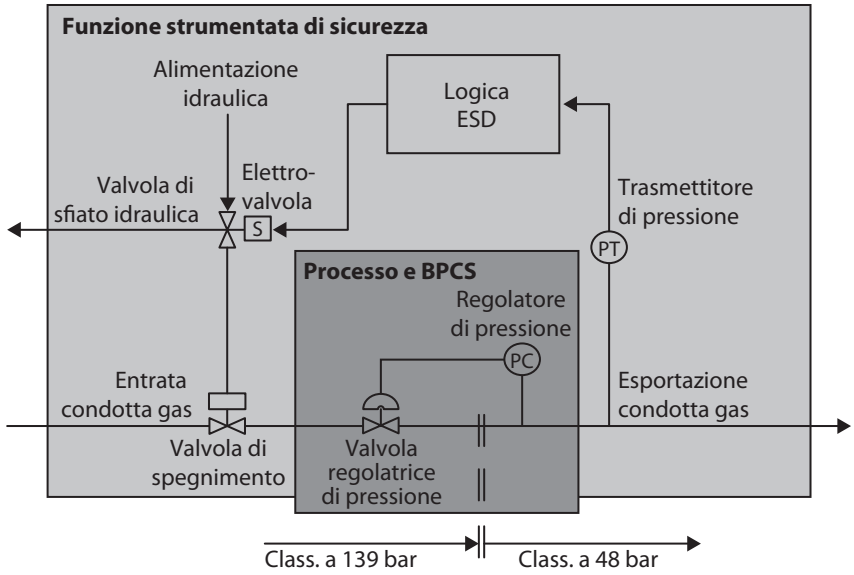


Figura 54: funzione strumentata di sicurezza in modalità su domanda

Il calcolo della probabilità PFD può essere eseguito più facilmente utilizzando la tecnica degli schemi a blocchi dell'affidabilità (RBD). Gli schemi RBD mostrano gli elementi o i componenti necessari per un sistema affidabile e non rappresentano necessariamente il layout o le connessioni fisiche. La modellazione RBD è descritta nella norma IEC 61508-6, Allegato B, 4.2.

La Figura 55 illustra lo schema RBD per il sistema SIS descritto.

λDD	2,64E-07	3,42E-06	0,00E+00	0,00E+00
MTD	48	48	48	48
PFD configurazione	1,27E-05	1,64E-04	0,00E+00	0,00E+00
λDU	4,00E-08	1,63E-07	6,00E-07	4,64E-06
Periodo di prova funzionale	8760	8760	8760	8760
PFD configurazione	1,75E-04	7,14E-04	2,63E-03	2,03E-02
PFD (rivelati)	1,77E-04			
PFD (non rivelati)	2,38E-02			
PFD	2,40E-02			
SIL ammesso (PFD)	SIL1			

Figura 55: funzione di sicurezza in modalità su domanda

Lo schema RBD mostra il calcolo della probabilità PFD. Sotto ogni elemento ci sono i valori per il tasso di guasto rilevato pericoloso (λ_{DD}), il tasso di guasto non rilevato pericoloso (λ_{DU}), il tempo medio di indisponibilità (MDT) ed il periodo di prova funzionale (T).

14.6. Esempio di valutazione del livello di integrità della sicurezza della modifica del processo di prepolimerizzazione in modalità su domanda

Di seguito, è riportato un esempio di valutazione SIL della probabilità PFD e delle prestazioni hardware di una funzione SIF.

Campo di applicazione

La funzione ESD S-005 previene una reazione non controllata in 39-R-050 e, di conseguenza, protegge dalla perdita di contenimento dal reattore che potrebbe comportare lesioni alle persone e danni ambientali. Attualmente, la funzione di sicurezza S-005 viene attivata dal rilevamento di alta temperatura o alta pressione nel reattore e la valvola di sfiato ROV0503 viene aperta per scaricare la pressione.

Essendoci dubbi sul fatto che la valvola ROV0503 avesse sufficiente capacità di scarico, l'azione ESD della funzione S-005 è stata modificata in modo da includere l'attivazione di una valvola di sfiato aggiuntiva ROV0501.

Inoltre, durante il programma di aggiornamento, sono stati inclusi due interruttori manuali (HS0900 di consenso e HS2004 di override) a fini di manutenzione.

Obiettivi

Il cliente ha un grande numero di sensori nel sistema SIS e vuole minimizzare questo onere. L'obiettivo di questa analisi è quindi di:

1. determinare quali elementi debbano essere inclusi nell'analisi della funzione di sicurezza ESD modificata S-005;
2. realizzare uno schema RBD per determinare la probabilità PFD e l'architettura della funzione S-005;
3. suggerire il principio di prova funzionale (intervalli di prova di sensori, interruttori manuali, logica e valvole di sfiato) che permetta di soddisfare i target (Tabella 18) minimizzando, nel contempo, la frequenza di prova dei sensori.

Nota: il cliente ha stabilito che gli intervalli di prova funzionale di qualunque elemento non dovrebbero superare i 36 mesi. Dal punto di vista dell'engineering, il cliente non è sicuro riguardo alle parti del sistema SIS che non vengono attivate per lunghi periodi di tempo.

Consensi e override

Al sistema ESD S-005, sono associati due interruttori manuali, HS2004 e HS0900.

L'interruttore HS0900 viene utilizzato per indirizzare il catalizzatore al reattore e, di conseguenza, se l'interruttore è nella posizione sbagliata o si guasta nello stato sbagliato, il pericolo non può verificarsi. L'interruttore HS2004 viene utilizzato come override d'intervento su S-005. Se dopo l'intervento di manutenzione, HS2004 viene inavvertitamente lasciato o si guasta in posizione di override, la funzione di sicurezza S-005 sarà disabilitata.

Configurazione hardware

Il logic solver è basato su una configurazione TMR (ridondante modulare tripla) con logica di voting 2 su 3 (2oo3). La Figura 56 presenta uno schema della configurazione hardware.

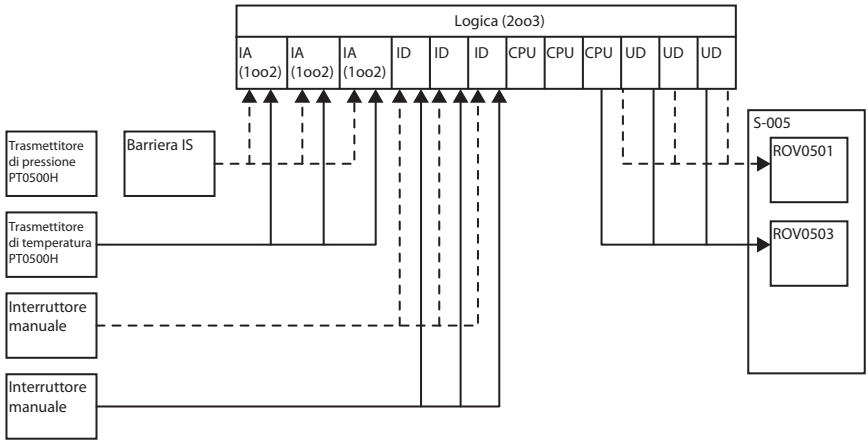


Figura 56: schema hardware

Funzioni di sicurezza analizzate

La Tabella 18 presenta i target SIL e PFD stabiliti.

Loop	Causa scatenante	Azione ESD	Condizioni richieste per mitigare il pericolo	Target PFD	Target SIL
1	Alta pressione [PT0500H] o alta temperatura [TT0504HH]	Attiva S-005	ROV0503 e ROV0501 aperte	5,56E-03	SIL2

Tabella 18: funzioni di sicurezza per analisi

Copertura diagnostica

Si presume che tutte le modalità di guasto non rilevate verranno riscontrate dalla prova funzionale ovvero dalla completa esecuzione della funzione SIS.

Tempo medio di indisponibilità

In questa analisi, dovrebbe essere usato un tempo MDT di 72 ore.

Periodo di prova funzionale

Gli intervalli di prova funzionale dovrebbero essere selezionati per raggiungere i target massimizzando, nel contempo, l'intervallo di prova dei sensori.

Considerazione dei guasti per causa comune

I CCF sono guasti che possono derivare da una singola causa ma che interessano più di un canale simultaneamente. Possono essere dovuti, ad esempio, ad un guasto sistematico, ad un errore di specifica del progetto o a sollecitazioni esterne come la sovratemperatura e comportare il guasto del componente in entrambi i canali ridondanti.

Il contributo dei guasti CCF nei percorsi ridondanti in parallelo dovrebbe essere considerato nel modello con l'inclusione di un fattore β. Il tasso di guasto CCF incluso nel calcolo è uguale a β x il tasso di guasto totale di uno dei percorsi paralleli. I fattori β da utilizzare nell'analisi sono riepilogati nella Tabella 19.

Configurazione ridondante	Fattore *β*	Motivazione
Sensori PT0500, TT0504	3%	Dato che i sensori sono di tecnologia differente e misurano variabili di processo differenti, il potenziale dei guasti per causa comune è limitato al processo stesso, al meccanismo di collegamento dei sensori ed all'instradamento ed alla separazione delle connessioni dei sensori. Il valore del 3% è quindi ritenuto ragionevolmente conservativo.
Logica TMR del PLC	5%	I guasti per causa comune in una configurazione TMR ridondante sono ridotti ma è stato adottato un valore del 5% per mantenere un approccio conservativo.

Tabella 19: Fattori β

Componenti Tipo A

I seguenti elementi possono essere considerati di Tipo A:

- Barriera IS (sezionatore dell'alimentatore del trasmettitore; PB0500);
- Trasmettitore di temperatura (TT0504);
- Interruttore manuale (HS0900, HS2004);
- Valvole di sfiato del processo di prepolimerizzazione.

Componenti Tipo B

I seguenti elementi sono stati considerati di Tipo B:

- Moduli logici PLC;
- Trasmettitori di pressione (PT0500).

Tassi di guasto dei componenti

L'analisi dovrebbe ipotizzare tassi di guasto costanti, essendo prevista l'eliminazione degli effetti delle avarie premature mediante processi adeguati. Questi processi includono l'uso di prodotti collaudati da fonti approvate, collaudo interno prima della consegna, prove funzionali e di funzionamento prolungato della funzione nell'ambito delle operazioni di installazione e messa in servizio. I dati dei resi dal campo per altri simili progetti indicano che i guasti prematuri non comportano un significativo numero di resi e quindi le tecniche impiegate sono giudicate sufficienti.

Si presume anche che i componenti non vengano utilizzati oltre la loro vita utile garantendo, in tal modo, che i guasti dovuti a meccanismi di usura non si verifichino. I tassi di guasto (in guasti/ora) che possono essere utilizzati nel modello per il calcolo della probabilità PFD, λ_{DD} e λ_{DU}, sono riepilogati nella Tabella 20. I tassi di guasto sono stati ottenuti da una combinazione di fonti.

Rif./Tag elemento	Descrizione	λ	λD	λDU	λDD	λS	SFF
Dispositivi di ingresso							
PT 0500	Trasmettitore di pressione (IS)	1,5E-06	1,4E-06	6,0E-07	7,5E-07	1,5E-07	0,60
PT 0501	Trasmettitore di pressione (IS)	1,5E-06	1,4E-06	6,0E-07	7,5E-07	1,5E-07	0,60
PB 0500	Barriera – per trasmettitori di pressione (PT) precedenti (non IS)	2,1E-07	6,3E-08	6,3E-08	0,0E+00	1,5E-07	0,70
PB 0501	Barriera – per trasmettitori di pressione (PT) precedenti (non IS)	2,1E-07	6,3E-08	6,3E-08	0,0E+00	1,5E-07	0,70
FT 0041	Flussometro Coriolis	2,6E-06	2,2E-06	9,0E-07	1,3E-06	4,0E-07	0,65
TT 0504	RTD a 3 fili con trasmettitore montato in testa	2,0E-06	1,4E-06	4,0E-07	1,0E-06	6,0E-07	0,80
HS 2004	Interruttore di override	2,00E-06	8,00E-07	8,00E-07	0,00E+00	1,20E-06	0,60
HS0900	Interruttore di consenso	2,00E-06	8,00E-07	8,00E-07	0,00E+00	1,20E-06	0,60
Dispositivi logici							
CPU	CPU	1,51E-06	5,16E-07	6,42E-09	5,09E-07	9,91E-07	1,00
Modulo ID 32pt	Modulo ID 32pt	2,19E-08	1,09E-08	9,91E-11	1,08E-08	1,09E-08	0,99
Modulo ingresso analogico IA 32pt	Modulo ingresso analogico IA 32pt	1,40E-08	7,00E-09	9,86E-11	6,90E-09	7,00E-09	0,99
Modulo uscita digitale UD 16pt	Modulo uscita digitale UD 16pt	2,95E-08	1,47E-08	9,93E-11	1,46E-08	1,47E-08	0,99
Dispositivi di uscita							
39-PM-050	Stato di funzionamento pompa da contattore e contatto relè NA	3,0E-07	2,0E-07	1,95E-07	0,00E+00	1,05E-07	0,35
ROV 0501	Valvola di scarico AOV (FO) con elettrovalvola SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0503	Valvola di scarico AOV (FO) con elettrovalvola SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0404	AOV (FC) con SOV	9,72E-06	3,03E-06	3,03E-06	0,00E+00	6,69E-06	0,688
ROV 0405	Valvola di scarico AOV (FO) con elettrovalvola SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0406	Valvola di scarico AOV (FO) con elettrovalvola SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734

Tabella 20: tassi di guasto (/ora) e calcolo della SFF

Una possibile soluzione

L'obiettivo di questa analisi è quello di:

1. determinare quali elementi debbano essere inclusi nell'analisi della funzione di sicurezza ESD modificata S-005;
2. realizzare uno schema RBD per determinare la probabilità PFD e l'architettura di S-005;
3. suggerire il principio di prova funzionale (intervalli di prova di sensori, interruttori manuali, logica e valvole di sfiato) che permetta di soddisfare i target (Tabella 18) minimizzando, nel contempo, la frequenza di prova dei sensori.

L'RBD mostrato nella Figura 57 illustra gli elementi necessari nell'ambito della funzione di sicurezza. Nella valutazione della funzione di sicurezza, non è necessario includere l'interruttore HS0900 perché il suo guasto non può impedire il funzionamento della funzione di sicurezza. Se l'interruttore HS0900 si guasta o viene lasciato nella posizione sbagliata, il pericolo non può verificarsi.

L'interruttore HS2004 invece deve essere incluso perché, se dopo l'intervento di manutenzione, viene inavvertitamente lasciato o si guasta in posizione di override, la funzione di sicurezza S-005 sarà disabilitata.

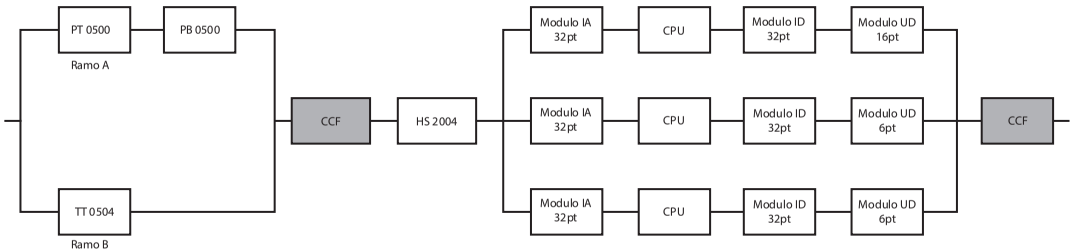
Il calcolo della probabilità PFD ha richiesto un'attenta considerazione per ciò che riguarda l'impostazione degli intervalli di prova funzionale, Tp. Il requisito era quello di massimizzare l'intervallo fino a 3 anni mantenendo, nel contempo, la PFD target. Le possibili soluzioni sono diverse ed andranno discusse con il cliente. Nella Tabella 21, è illustrato un possibile principio di prova funzionale.

Periodo di prova funzionale (sensori)	24	mesi	17.520	ore
Periodo di prova funzionale (interruttore manuale)	6	mesi	4380	ore
Periodo di prova funzionale (logica)	36	mesi	26.280	ore
Periodo di prova funzionale (valvole)	3	mesi	2190	ore

Tabella 21: possibili intervalli di prova funzionale

Questi intervalli di prova funzionale forniscono una probabilità PFD calcolata di 4,91E-03 rispetto ad un target di 5,56E-03 e sia la PFD sia le prestazioni dell'architettura soddisfano il livello SIL2 target.

Figura 57: soluzione RBD



Contributo CCF			3%						5%
Q.tà	1	1		1	1	1	1	1	1
Configurazione		1oo2						2oo3	
λDD [Ramo A]	7,50E-07	0,00E+00	2,25E-08	0,00E+00	6,90E-09	5,09E-07	1,08E-08	1,46E-08	2,71E-08
λDD [Ramo B]	1,00E-06	0,00E+00							
λDD per ramo			2,25E-08	0.00E+00				5,42E-07	2,71E-08
MDT		72	72	72				72	72
PFD configurazione		3,89E-09	1,62E-06	0,00E+00				4,56E-09	1,95E-06
λDU [Ramo A]	6,00E-07	6,30E-08	1,99E-08	8,00E-07	9,86E-11	6,42E-09	9,91E-11	9,93E-11	3,36E-10
λDU [Ramo B]	4,00E-07	0,00E+00							
λDU per ramo			1,99E-08	8,00E-07				6,72E-09	3,36E-10
Periodo di prova funzionale, T		17.520	17.520	4380				26.280	26.280
PFD configurazione		2,71E-05	1,74E-04	1,75E-03				3,11E-08	4,41E-06

PFD (rivelati)	3,58E-06
PFD (non rivelati)	4,91E-03
PFD	4,92E-03
SIL ammesso (PFD)	2

Tipo	B	A	A	B	B	B
SFF	0,60	0,70	0,60	>99	>99	>99
Ridondanza	1	0	0	1	1	1
SIL dell'architettura	2	2	2	3	3	3
SIL ammesso (arch.)	2					

14.7. Tracciabilità dei dati relativi ai tassi di guasto

Nell'eseguire i calcoli PFD, è vitale che tutti i calcoli siano visibili e che tutti i dati utilizzati siano tracciabili alla fonte. Microsoft Excel è uno strumento utile perché risponde ad entrambi questi requisiti e permette anche di sviluppare una rappresentazione grafica del modello di affidabilità, come nella Figura 57.

Il foglio di calcolo elettronico permette ad ogni cella di dati di puntare ad una tabella dati in cui possono essere presentati tutti i dati di tasso di guasto raccolti e tutte le fonti di tali dati. Un esempio di tabella dati è illustrato nella Tabella 22. È importante che il riferimento alla fonte dei dati sia abbastanza dettagliato da permettere a chiunque di controllare e confermare i valori utilizzati.

Se si usa un formato Excel, è opportuno elencare anche i tipi di componenti ed i valori MDT e Tp utilizzati nel calcolo. Ciò consente di modificare facilmente gli intervalli di prova funzionale e di calcolare automaticamente l'effetto sulla PFD.

Elemento/ codice	λ	λD	λDD	λDU	λS	Tipo	SFF	MDT	Tp	Fonte dati
PT0500	1,35E-06	8,18E-07	7,50E-07	6,80E-08	5,27E-07	B	0,95	4380	4380	exida [14.8.2]
Logic solver SIL3	5,57E-06	2,23E-06	2,21E-06	2,20E-08	3,34E-06	B	1,00	168	4380	Sintef [14.8.8]
Modulo di ingresso analogico	1,07E-06	5,34E-07	5,08E-07	2,60E-08	5,34E-07	B	0,98	168	4380	Sintef [14.8.8]
Modulo di uscita discreto	5,26E-07	2,63E-07	2,50E-07	1,30E-08	2,63E-07	B	0,98	168	4380	Sintef [14.8.8]
Valvola HIPPS 12"	5,29E-06	2,12E-06	0,00E+00	2,12E-06	3,17E-06	A	0,60	730	4380	Oreda 2002 [14.8.6]

Tabella 22: tipica tabella dati

14.8. Fonti dei dati relativi ai tassi di guasto

14.8.1. Approccio

I dati relativi ai tassi di guasto dovrebbero essere ricavati solo da fonti adeguate e ciò dipende dall'applicazione. Di seguito, è riportato un elenco delle fonti utilizzate per l'industria di processo.

14.8.2. Exida.com Safety Equipment Reliability Handbook, 2007, 3rd Edition Volume 1 – Sensors, ISBN 978-0-9727234-3-5/Volume 2 – Logic Solvers and Interface Modules, ISBN 978-0-9727234-4-2/Volume 3 – Final Elements, ISBN 978-0-9727234-5-9

14.8.3. Handbook of Reliability Data for Electronic Components used in Telecommunications Systems, HRD-5.

14.8.4. Hydrocarbon Leak and Ignition Database Report No. 11.4/180 May 1992

14.8.5. IEEE Standard 500-1984. Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data.

14.8.6. OREDA, The Offshore Reliability Data Handbook 4th Edition 2002 ISBN 82-14-02705-5

14.8.7. Parloc 2001: 5th Edition, The Institute of Petroleum, Energy Institute ISBN 0 85293 404 1.

14.8.8. Reliability Data for Control and Safety Systems, 2006 Edition, PDS Data Handbook, SINTEF, ISBN 82-14-03898-7.

14.8.9. Reliability Technology, AE Green and AJ Bourne, Wiley, ISBN 0-471-32480-9.

15. Installazione, messa in servizio e validazione, IEC 61511-1, 14, 15

15.1. Fasi del ciclo di vita

La Figura 58 mostra la fase del ciclo di vita in questione.

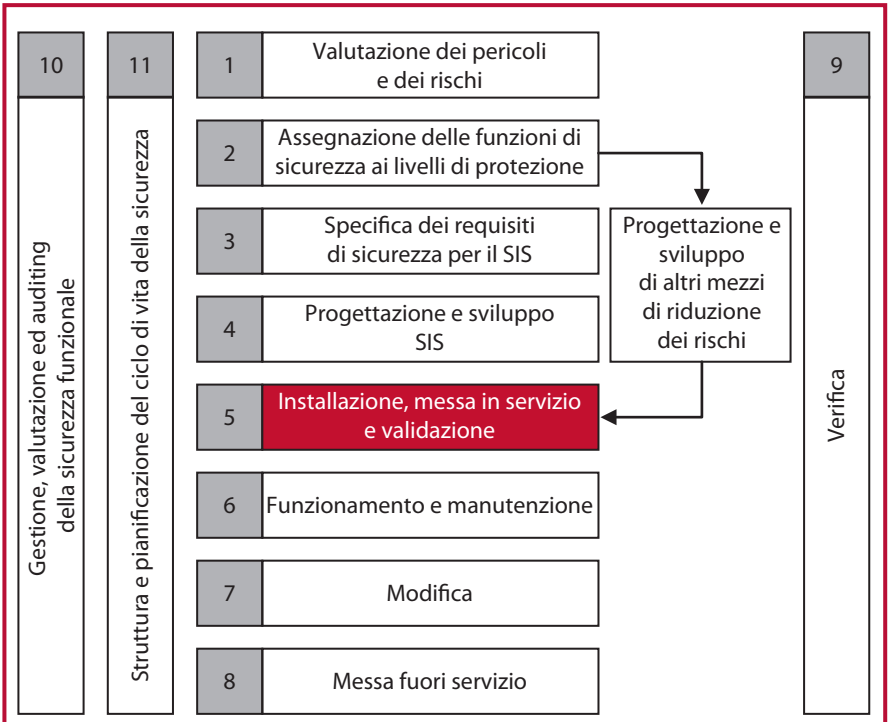


Figura 58: ciclo di vita – Fase 5

Gli obiettivi delle fasi definite nella norma IEC 61511-1, 14 e 15 sono quelli di:

- installare il sistema SIS in base alle specifiche ed alla documentazione [15.2];
- mettere in servizio il sistema SIS in modo che sia pronto alla validazione finale del sistema [15.3];
- validare che il sistema SIS installato e messo in servizio risponda ai requisiti definiti nella SRS [15.4].

15.2. Installazione SIF

I requisiti per l'installazione dovrebbero essere definiti nel piano di installazione e messa in servizio o integrati nel piano di progetto globale. Le procedure di installazione dovrebbero

definire le attività da realizzare, le tecniche e le misure da utilizzare, le persone, i dipartimenti o le organizzazioni responsabili ed il calendario delle attività di installazione.

15.3. Messa in servizio SIF

Il sistema SIS dovrebbe essere messo in servizio nel rispetto della pianificazione e delle procedure. Bisognerebbe registrare i risultati delle prove e dichiarare se i criteri di accettazione definiti durante la fase di design sono stati soddisfatti. I guasti dovrebbero essere esaminati e registrati. Per i punti in cui l'installazione effettiva non si conforma alle informazioni di progetto, è necessario esaminare le differenze e determinarne l'impatto sulla sicurezza.

15.4. Validazione SIF

Le procedure di validazione dovrebbero includere tutte le modalità di funzionamento del processo e delle apparecchiature associate e dovrebbero includere:

- avviamento, normale funzionamento, spegnimento;
- funzionamento manuale o automatico;
- modalità di manutenzione, vincoli di bypass;
- sequenza temporale;
- ruoli e responsabilità;
- procedure di calibrazione.

La validazione del software applicativo, inoltre, dovrebbe includere:

- identificazione del software per ogni modalità di funzionamento;
- procedura di validazione da utilizzare;
- strumenti ed apparecchiature da utilizzare;
- criteri di accettazione.

La validazione dovrebbe assicurare che il sistema SIS sia operativo in tutte le modalità di funzionamento e che non sia interessato dall'interazione del sistema BPCS e di altri sistemi collegati. La validazione delle prestazioni dovrebbe assicurare che tutti i canali ridondanti, le funzioni di bypass, gli override di avviamento ed i sistemi di spegnimento manuale funzionino.

In caso di perdita di energia (alimentazione elettrica, idraulica o aria strumentale), dovrebbe essere raggiunto lo stato definito (sicuro). Le funzioni di allarme della diagnostica definite nella specifica SRS dovrebbero funzionare ed agire come specificato sulle variabili di processo non valide (ad es. ingressi fuori campo). Dopo la validazione, bisognerebbe procedere alle debite registrazioni ed identificare gli elementi, le apparecchiature, i documenti ed i risultati di prova, oltre che le eventuali discrepanze, le analisi o le richieste di modifica risultanti.

16. Funzionamento e manutenzione, IEC 61511-1, 16

16.1. Fasi del ciclo di vita

La Figura 59 mostra la fase del ciclo di vita in questione.

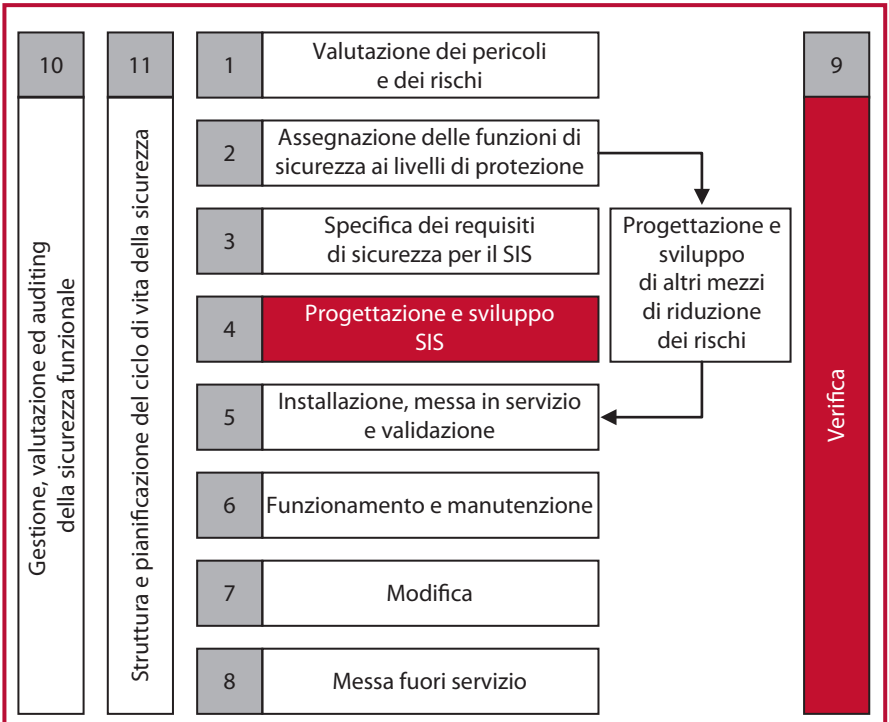


Figura 59: ciclo di vita – Fase 6

Gli obiettivi di questa fase come definito nella IEC 61511-1, 16.1 sono quelli di:

- assicurare che il livello SIL richiesto di ogni funzione SIF venga mantenuto durante il funzionamento e la manutenzione [16.2];
- utilizzare e manutenere il sistema SIS in modo da non perdere la sicurezza funzionale progettata [16.3].

16.2. Funzionamento e manutenzione (O&M) SIF

I requisiti O&M dovrebbero essere definiti nel piano O&M o integrati nel piano di progetto globale. Le procedure O&M dovrebbero definire le operazioni di routine da realizzare per

mantenere la sicurezza funzionale del sistema SIS. Queste operazioni dovrebbero includere i requisiti per:

- prova funzionale;
- bypass di una funzione SIF per test o riparazione;
- raccolta dei dati di routine (ad es. risultati di audit e prove sul sistema SIS, registrazione delle domande di intervento SIF, tempi di fermo per guasti, riparazione e prove funzionali.

Le procedure delle prove funzionali dovrebbero essere sviluppate in modo che ogni funzione SIF venga testata per rivelare i guasti pericolosi non coperti dalla diagnostica [16.4].

È necessario prevedere procedure di manutenzione per la diagnostica dei guasti, la riparazione, la rivalidazione del sistema in seguito a riparazione, le azioni da intraprendere in seguito a discrepanze tra il comportamento previsto e quello effettivo, la calibrazione e la manutenzione dell'apparecchiatura di prova ed i report di manutenzione.

Per i report dei guasti, l'analisi dei guasti sistematici e per causa comune e la tracciabilità delle prestazioni di manutenzione, è necessario prevedere procedure di reporting.

16.3. Formazione O&M

La formazione del personale O&M dovrebbe essere pianificata e realizzata a tempo debito, in modo che il sistema SIS possa essere usato e manutenuto come previsto nella SRS. La formazione dovrebbe includere:

- pericoli;
- punti di intervento;
- azioni esecutive;
- funzionamento di tutti i bypass ed eventuali vincoli d'uso;
- funzionamento manuale (ad es. avviamento e spegnimento) ed eventuali vincoli d'uso;
- funzionamento degli allarmi e diagnostica disponibile.

16.4. Prove funzionali

Le procedure per le prove funzionali dovrebbero testare la funzione SIF completa, dall'elemento di rilevamento al dispositivo azionato finale. L'intervallo di prova funzionale dovrebbe essere quello usato nella quantificazione della probabilità PFD [14].

È possibile testare differenti elementi della funzione SIF a differenti intervalli, a condizione che:

- la probabilità PFD calcolata sia ancora accettabile;
- la prova preveda qualche sovrapposizione in modo che nessuna parte della funzione SIF venga trascurata.

17. Modifica e messa fuori servizio, IEC 61511-1, 17, 18

17.1. Fasi del ciclo di vita

La Figura 60 mostra le fasi del ciclo di vita in questione.

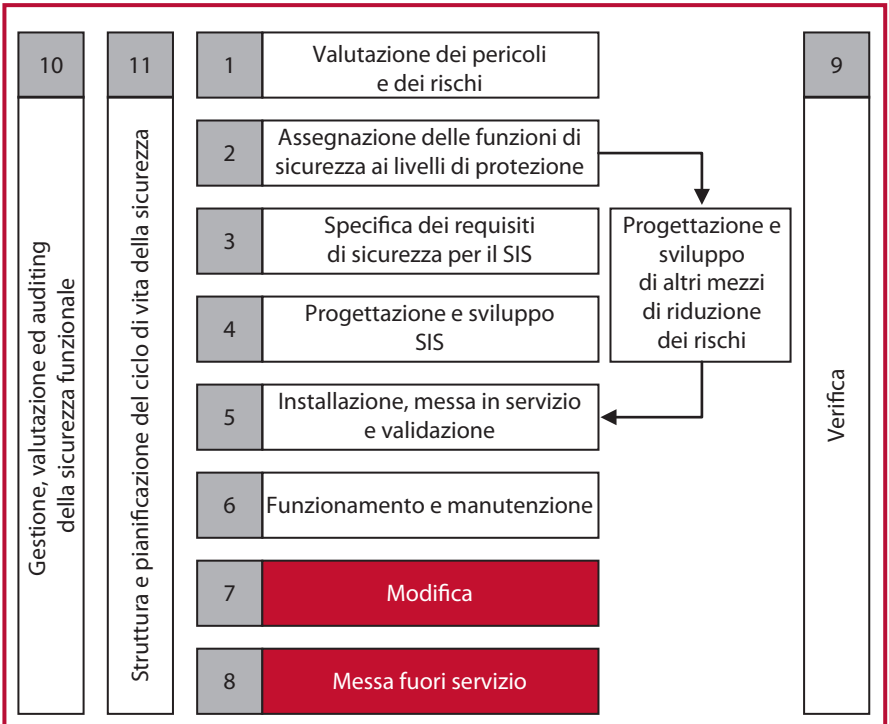


Figura 60: ciclo di vita – Fasi 7 e 8

Gli obiettivi di questa fase come definito nella norma IEC 61511-1, 17.1 e 18.1 sono quelli di assicurare che:

- tutte le modifiche a qualunque funzione SIF vengano correttamente pianificate, esaminate ed approvate prima di essere implementate [17.2];
- l'integrità della sicurezza richiesta venga mantenuta anche dopo eventuali modifiche [17.3];
- prima della messa fuori servizio, venga condotta un'adeguata analisi che assicuri il mantenimento dell'integrità della sicurezza durante la messa fuori servizio con debita autorizzazione [17.4].

17.2. Modifica SIF

Prima di qualunque modifica, è opportuno che siano in atto le procedure necessarie ad autorizzare e controllare le modifiche. Ciò viene generalmente gestito con una CRN (Notifica di richiesta di modifica) che di solito fa parte di un sistema QMS.

Le richieste di modifica dovrebbero descrivere la modifica richiesta e le ragioni della richiesta. Possono essere chieste dal personale O&M in seguito ad incidenti durante il funzionamento o la manutenzione. Il normale processo di approvazione delle richieste di modifica dovrebbe coinvolgere più dipartimenti all'interno di un'organizzazione, per determinare l'impatto delle modifica sul design, sulla base installata e sull'implementazione richiesta.

Quando un'organizzazione è coinvolta nella sicurezza funzionale, qualunque richiesta di modifica dovrebbe essere esaminata anche da una persona competente (ad es. l'autorità per la sicurezza – SA) per determinare se la modifica può incidere sulla sicurezza e, in tal caso, è necessaria un'adeguata analisi dell'impatto.

17.3. Analisi dell'impatto

I risultati dell'analisi possono richiedere il riesame delle prime parti del ciclo di vita e, ad esempio, può essere necessario riesaminare i pericoli identificati e le valutazioni di rischio. Le attività di modifica non possono iniziare fino al completamento di questo processo ed all'autorizzazione della modifica da parte della SA.

L'impatto delle modifiche sulla funzione SIF può avere effetti consequenziali sul personale O&M e può essere necessaria formazione aggiuntiva.

17.4. Messa fuori servizio SIF

La messa fuori servizio dovrebbe essere un'attività pianificata nell'ambito della fase 11 del ciclo di vita e può essere trattata come una modifica alla fine della vita del progetto.

L'inizio della fase di messa fuori servizio dovrebbe iniziare con un'analisi di impatto per determinare l'effetto della messa fuori servizio sulla sicurezza funzionale. L'analisi dovrebbe includere la revisione dell'identificazione dei pericoli e della valutazione dei rischi, con particolare considerazione dei pericoli che possono presentarsi per le attività di messa fuori servizio.

18. Gestione, valutazione ed auditing della sicurezza funzionale

18.1. Fasi del ciclo di vita

La Figura 61 mostra la fase del ciclo di vita in questione.

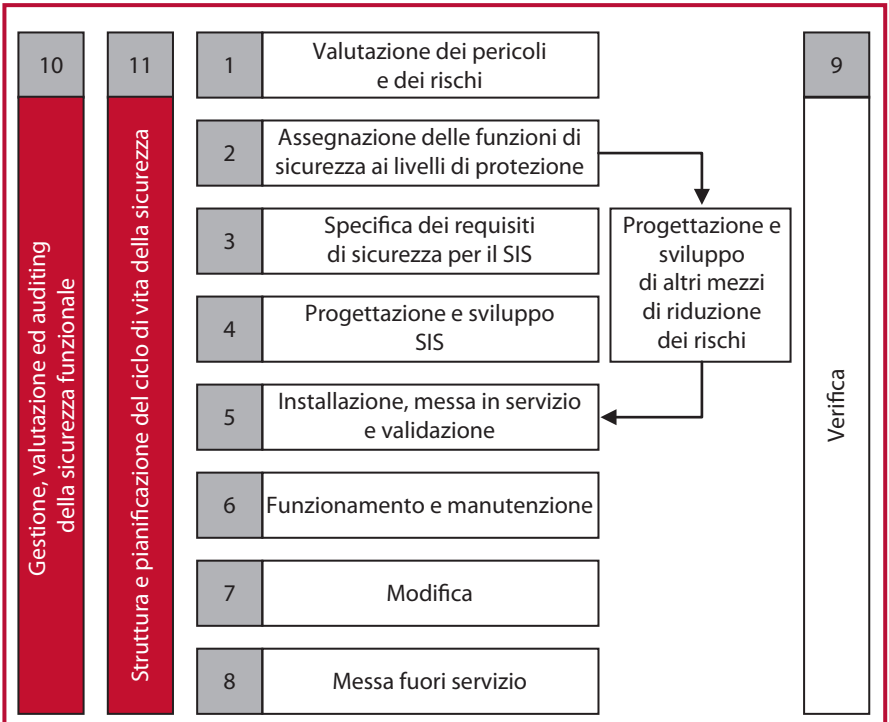


Figura 61: ciclo di vita – Fasi 10 e 11

L'obiettivo di questa fase – come definito nella norma IEC 61511-1, 5 – è quello di identificare le attività di gestione e la documentazione necessarie a permettere l'adeguata gestione delle fasi del ciclo di vita applicabili da parte delle persone responsabili.

La norma elenca i requisiti generali per la gestione e la documentazione necessari a permettere l'adeguata gestione delle fasi del ciclo di vita applicabili da parte delle persone responsabili.

Ciò significa che la documentazione di progetto deve contenere sufficienti informazioni per ogni fase del ciclo di vita che è stata completata e per l'efficace completamento delle fasi successive e delle attività di verifica.

La conformità con la norma richiede la specifica di:

- responsabilità nella gestione della sicurezza funzionale;
- attività che devono realizzare le persone responsabili.

La conformità rispetto ai requisiti può essere ricercata mettendo in atto procedure che trattano ogni requisito in oggetto, implementando quelle procedure ed assicurando che le informazioni disponibili siano adatte a permettere una gestione efficace della sicurezza funzionale.

18.2. Gestione della sicurezza funzionale

I requisiti per la gestione della sicurezza funzionale sono riepilogati nella Tabella 23.

È possibile che la maggior parte dei requisiti sia già soddisfatta da un sistema di gestione qualità (QMS) dell'organizzazione. Le sezioni che seguono evidenziano alcune aree che generalmente devono essere affrontate.

Gestione del requisito di sicurezza funzionale	**Descrizione**
Requisiti generali IEC 61511-1, 5.2.1 Dovrebbero essere specificate una politica ed una strategia, unitamente ai mezzi di comunicazione all'interno dell'organizzazione.	**Politica e comunicazioni** Dovrebbe essere in atto una politica di sicurezza funzionale da comunicare a tutta l'organizzazione. È consigliabile che il contenuto di tale politica includa specifici obiettivi di sicurezza funzionale, i mezzi di valutazione (se esistenti) ed il metodo di comunicazione all'interno dell'organizzazione.
Dovrebbe essere in atto un sistema di gestione della sicurezza funzionale per garantire che il sistema SIS sia in grado di portare e mantenere il processo in uno stato sicuro.	Dovrebbe essere disponibile un documento di gestione della sicurezza funzionale di alto livello che identifichi tutte le fasi del ciclo di vita in oggetto. Il documento di gestione dovrebbe far riferimento alle procedure necessarie per tutte le attività legate alla sicurezza. Devono essere in atto procedure che specifichino tutte le attività tecniche e di gestione da realizzare sul progetto. Le procedure dovrebbero identificare i documenti da produrre. I progetti dovrebbero essere controllati usando un piano di qualità e sicurezza che identifichi le attività da realizzare, i mezzi di controllo e permetta la firma al completamento.

Gestione del requisito di sicurezza funzionale	Descrizione
Organizzazione e risorse IEC 61511-1, 5.2.2 Persone, dipartimenti, organizzazioni ed altre unità responsabili della realizzazione e dell'analisi di ognuna delle fasi del ciclo di vita della sicurezza devono essere identificati ed informati delle responsabilità loro assegnate (inclusi, dove pertinente, autorità di rilascio delle licenze o organismi di regolamentazione della sicurezza).	**Ruoli e responsabilità** Tutte le persone, i dipartimenti e le organizzazioni responsabili di realizzare ed esaminare le attività legate alla sicurezza dovrebbero essere identificati e le loro responsabilità chiarite. In un'organizzazione, di solito ciò avviene mediante la pubblicazione di organigrammi che identificano gli individui ed i loro ruoli. La descrizione del lavoro identifica quindi le responsabilità di ogni ruolo.
Persone, dipartimenti ed organizzazioni coinvolti nelle attività del ciclo di vita della sicurezza devono avere le competenze necessarie a realizzare le attività di cui sono incaricati.	**Competenza** Le competenza di tutte le persone responsabili di cui sopra deve essere documentata. Dovrebbero essere in atto procedure in grado di garantire che le persone responsabili abbiano le competenze necessarie alle attività loro assegnate. La procedura dovrebbe includere un'analisi ed una valutazione delle competenze e delle esigenze di formazione. La documentazione delle competenze dovrebbe considerare: a) conoscenze di engineering (processo, tecnologia, novità e complessità dell'applicazione, sensori ed elementi finali); b) competenze di gestione e leadership adeguate al ruolo svolto nel ciclo di vita della sicurezza; c) comprensione delle conseguenze potenziali di un evento; integrità della sicurezza delle funzioni SIF; engineering della sicurezza e requisiti cogenti e normativi di sicurezza.
Valutazione e gestione dei rischi IEC 61511-1, 5.2.3 I pericoli dovrebbero essere identificati, i rischi valutati e la necessaria riduzione dei rischi determinata.	**Determinazione SIL** Fare riferimento alla Sezione [6].
Pianificazione IEC 61511-1, 5.2.4 La pianificazione della sicurezza dovrebbe essere effettuata per definire le attività da realizzare insieme alle persone, ai dipartimenti, alle organizzazioni o ad altre unità responsabili di realizzare tali attività. Questa pianificazione deve essere aggiornata come necessario per l'intero ciclo di vita della sicurezza.	**Pianificazione** La pianificazione dovrebbe garantire che le attività di gestione, verifica e valutazione della sicurezza funzionale vengano programmate ed applicate alle corrispondenti fasi del ciclo di vita. La pianificazione può essere inclusa nel piano di qualità del progetto e dovrebbe identificare tutte le attività legate alla sicurezza, il calendario e le persone o le organizzazioni responsabili. Ogni attività legata alla sicurezza può includere riferimenti a procedure o pratiche di lavoro, strumenti di sviluppo o produzione.
Implementazione e monitoraggio IEC 61511-1, 5.2.5 Dovrebbero essere implementate procedure atte a garantire un puntuale monitoraggio ed una soddisfacente attuazione delle raccomandazioni derivanti da: a) analisi dei pericoli e valutazione dei rischi; b) valutazione ed audit; c) verifica e validazione; d) attività post-incidente.	**Implementazione e monitoraggio** Le procedure dovrebbero permettere di formulare raccomandazioni in base alle attività di analisi e revisione e dovrebbe essere implementato un metodo per esaminare e tracciare l'attuazione delle raccomandazioni. Deve essere prevista una procedura che assicuri di poter dar seguito a qualunque raccomandazione derivante da incidenti o pericoli.

Gestione del requisito di sicurezza funzionale	Descrizione
Dovrebbero essere implementate procedure per valutare le prestazioni del sistema SIS rispetto ai requisiti di sicurezza tra cui: a) Raccolta ed analisi dei dati di guasto sul campo durante il funzionamento; b) Registrazione delle domande di intervento della funzione SIF per verificare che le ipotesi fatte durante la determinazione del livello SIL rimangano valide.	Quando l'organizzazione è responsabile delle fasi di funzionamento e manutenzione, devono essere implementate procedure atte a riconoscere le prestazioni di funzionamento e manutenzione tra cui: • guasti sistematici; • guasti ricorrenti; • valutazione della conformità dei tassi di domanda e dei tassi di guasto alle ipotesi formulate durante il progetto o la valutazione della sicurezza funzionale. I requisiti per gli audit di sicurezza funzionale dovrebbero includere: frequenza, autonomia, documentazione richiesta e monitoraggio.
I fornitori che forniscono prodotti o servizi ad un'organizzazione che abbia la responsabilità globale di una o più fasi del ciclo di vita di sicurezza devono fornire i prodotti o i servizi come specificato da tale organizzazione ed avere un adeguato sistema di gestione della qualità. Devono essere in atto procedure in grado di stabilire l'adeguatezza del sistema di gestione della qualità.	**Gestione dei fornitori** I fornitori devono fornire prodotti come specificato ed avere un adeguato sistema di gestione della qualità. Per l'approvvigionamento, in genere, si fa riferimento ad un elenco di fornitori approvati e controllati mediante una specifica di approvvigionamento. Dovrebbero essere in atto procedure di verifica dell'approvazione dei fornitori.
Valutazione, auditing e revisioni IEC 61511-1, 5.2.6 è necessario definire ed eseguire una procedura di valutazione della sicurezza funzionale in modo tale da poter giudicare la sicurezza funzionale e l'integrità della sicurezza ottenuta dal sistema strumentato di sicurezza. La procedura deve prevedere la nomina di un team di valutazione che abbia le competenze tecniche, applicative ed operative necessarie per la specifica applicazione. Il team di valutazione deve includere almeno una persona competente ed esperta non direttamente coinvolta nel team di progetto. Le fasi nel ciclo di vita della sicurezza in cui devono essere realizzate le attività di valutazione della sicurezza funzionale devono essere identificate durante la pianificazione della sicurezza.	**Valutazione della sicurezza funzionale** Attività di valutazione della sicurezza funzionale – Fare riferimento alla Sezione [13]. Dovrebbe essere implementata una procedura atta a permettere la realizzazione di una valutazione della sicurezza funzionale. I requisiti per dimostrare la conformità ai target SIL e PFD (o PFH) stabiliti durante la determinazione del livello SIL [6] sono riportati al punto [11.1]. Il team può essere nominato all'interno dell'organizzazione, a condizione che abbia i requisiti di competenza ed indipendenza richiesti. Se ci si rivolge ad un'organizzazione esterna, i requisiti di competenza dovrebbero far parte della procedura di gestione dei fornitori. I requisiti per il rischio MTR dovrebbero essere inclusi nell'oggetto [8.6.6].

Gestione del requisito di sicurezza funzionale	Descrizione
Almeno una valutazione della sicurezza funzionale dovrebbe essere realizzata prima che siano presenti i pericoli identificati e dovrebbe confermare che: • la valutazione dei rischi e dei pericoli sia stata realizzata; • le raccomandazioni formulate in base alla valutazione dei pericoli e dei rischi siano state attuate; • il sistema SIS sia stato progettato, costruito ed installato conformemente alla specifica SRS; • le procedure di sicurezza, funzionamento e manutenzione siano in atto; • le attività di validazione siano state completate; • la formazione O&M sia stata completata e che siano state fornite adeguate informazioni sul sistema SIS; • le strategie per ulteriori valutazioni siano in atto.	La valutazione della sicurezza funzionale dovrebbe seguire un piano per la conformità. I momenti in cui dovrebbe essere effettuata, nell'ambito del programma del progetto o del ciclo di vita della sicurezza, dovrebbero essere specificati nel piano di qualità e sicurezza del progetto. È importante che almeno una valutazione di sicurezza funzionale venga realizzata prima che i pericoli identificati siano presenti sull'impianto o processo.
Devono essere definite ed eseguite procedure atte a verificare la conformità con i requisiti tra cui: a) la frequenza delle attività di auditing; b) il grado di indipendenza tra i soggetti, i dipartimenti, le organizzazioni o altre unità che eseguono il lavoro e quelle che si occupano delle attività di auditing; c) le attività di registrazione e monitoraggio.	Gli audit della sicurezza funzionale dovrebbero essere realizzati per verificare che il progetto preveda procedure adeguate e che tali procedure siano state implementate. Generalmente, un audit della sicurezza funzionale dovrebbe essere realizzato in una fase molto precoce del ciclo di vita del progetto, per verificare che esistano procedure per tutte le attività legate alla sicurezza. Gli audit successivi dovrebbero avvenire periodicamente nel corso del progetto, per garantire che le procedure vengano seguite e che vengano attuate tutte le raccomandazioni o le attività successive.
Gestione della configurazione del sistema SIS IEC 61511-1, 5.2.7 Dovrebbero essere disponibili procedure per la gestione della configurazione del sistema SIS durante il ciclo di vita. Dovrebbe essere specificato quanto segue: a) la fase in cui è implementato il controllo formale della configurazione; b) il metodo di identificazione delle parti (hardware e software); c) le procedure atte a prevenire che entrino in servizio parti non autorizzate.	Gestione della configurazione Le procedure per la gestione della configurazione, l'attuazione delle modifiche, le approvazioni e la gestione delle richieste di modifica sono generalmente già previste da un tipico sistema di gestione della qualità aziendale. Tuttavia, quando si considerano modifiche ad una funzione di sicurezza, deve essere previsto qualche tipo di analisi d'impatto per determinare se la sicurezza può essere compromessa ed a quale punto del ciclo di vita tornare per iniziare il processo di rivalutazione. Può essere necessaria una procedura per condurre l'analisi di impatto e gestire la rivalutazione.

Tabella 23: requisiti per la gestione della sicurezza funzionale

18.3. Requisiti generali

L'organizzazione deve prevedere una politica ed una strategia per ottenere la sicurezza funzionale ed identificare i mezzi attraverso cui comunicarle al suo interno.

È importante che l'organizzazione sviluppi la propria politica di sicurezza funzionale perché ciò richiederà alle parti interessate all'interno dell'organizzazione di considerare attentamente che cosa significa la sicurezza funzionale ed in che modo ciò può essere comunicata per creare una cultura di sicurezza che abbracci tutte le attività dell'organizzazione.

18.4. Organizzazione e risorse

Tutto il personale di progetto deve essere identificato sulla base delle competenze e delle responsabilità definite. Le competenze del personale devono essere annotate in un apposito registro e deve essere prevista una procedura che le esamini in modo da poter aggiornare periodicamente il registro in base all'esperienza acquisita ed alle esigenze di formazione. I requisiti di competenza devono essere definiti per ogni ruolo di progetto.

Le organizzazioni che non sono pratiche di sicurezza funzionale possono considerare la nomina un'autorità per la sicurezza (SA) che si assuma la responsabilità della sicurezza funzionale, della politica aziendale e delle comunicazioni, delle fasi del ciclo di vita e della pianificazione delle attività. Questa autorità sarà indipendente dai progetti.

Molto probabilmente, dovrà stabilire e gestire un registro delle competenze o sviluppare un sistema esistente per includere le attività e le responsabilità riguardanti la sicurezza funzionale.

18.5. Implementazione e monitoraggio del progetto

Se ci sono alcune attività nuove rispetto all'oggetto (ad es. HAZOP), è necessario creare una procedura per condurre l'analisi HAZOP. Se, ad esempio, lo sviluppo prevede l'inclusione di un software applicativo di sicurezza, devono essere in atto procedure atte ad assicurare che il software venga sviluppato come previsto nella fase 4 del ciclo di vita [11].

18.6. Gestione e modifica della configurazione

Le procedure per la gestione della configurazione, l'attuazione delle modifiche, le approvazioni e la gestione delle richieste di modifica sono generalmente già previste da un tipico QMS aziendale.

Tuttavia, quando si considerano modifiche ad una funzione di sicurezza, deve essere previsto qualche tipo di analisi d'impatto per determinare se la sicurezza può essere compromessa ed a quale punto del ciclo di vita tornare per iniziare il processo di rivalutazione. Può essere necessaria una procedura per condurre l'analisi di impatto e gestire la rivalutazione.

18.7. Prestazioni O&M

A seconda delle fasi del ciclo di vita in oggetto, può essere necessario implementare delle procedure per gestire, raccogliere e mantenere le informazioni acquisite su pericoli, incidenti e modifiche. Le procedure possono anche descrivere quanto segue:

- gestione di incidenti pericolosi;
- analisi dei pericoli rilevati;
- attività di verifica.

Può essere necessario prevedere la raccolta dei dati e il mantenimento delle registrazioni dato che, durante la valutazione della sicurezza, può essere stata ipotizzata una funzione di sicurezza, ad esempio, per un sistema in modalità su domanda. Il monitoraggio del tasso di domanda sulla funzione di sicurezza assicura quindi che i target e le misure prestazionali appropriati siano stati impostati in modo corretto e rimangano validi.

19. Riferimento

19.1. IEC 61508:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems (CEI EN 61508:2011: Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza (in inglese)).

19.2. IEC 61511:2004 (CEI EN 61511:2007): Sicurezza funzionale: Sistemi strumentali di sicurezza per il settore dell'industria di processo.

19.3. Reducing Risks, Protecting People, HSE 2001, ISBN 0 7176 2151 0.

19.4. AIChE Centre for Chemical Process Safety, Layer of Protection Analysis (LOPA), 2001

19.5. IEC 61784-3:2010 Industrial Communications Networks (CEI EN 61784-3:2012, Reti di comunicazione industriale (in inglese)). Profili Parte-3: Bus di campo per sicurezza funzionale – Regole generali e definizioni del profilo.

19.6. Derivation of the Simplified PFDavg Equations, D Chauhan, Rockwell Automation (FSC).

19.7. General Reliability Calculations for MooN Configurations, KJ Kirkcaldy, Rockwell Automation (FSC).

19.8. Functional Safety: Safety Instrumented Systems for the Process Industry Sector. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

20. Definizioni

2oo3	Circuito logico due su tre (circuito logico 2/3) – Un circuito logico con tre ingressi indipendenti. L'uscita del circuito logico ha lo stesso stato di una qualunque combinazione di due ingressi corrispondenti. Ad esempio, un circuito di sicurezza in cui sono presenti tre sensori ed in cui, per attivare uno spegnimento, è necessario un segnale di due qualunque di questi sensori. Il sistema 2oo3 è detto tollerante al singolo guasto (HFT = 1) in quanto, anche se uno dei sensori si guasta, il sistema può ancora procedere in sicurezza allo spegnimento. Altre logiche di voting sono 1oo1, 1oo2, 2oo2, 1oo3 e 2oo4.
A prova di guasto (o preferibilmente diseccitazione all'intervento)	Una caratteristica di un particolare dispositivo che fa sì che il dispositivo entri in uno stato sicuro in mancanza dell'energia elettrica o pneumatica.
Affidabilità	1. La probabilità che un dispositivo esegua il suo obiettivo adeguatamente, per il periodo di tempo specificato e nelle condizioni operative specificate. 2. La probabilità che un componente, parte di apparecchiatura o sistema eseguirà la sua funzione prevista per un periodo di tempo specificato, generalmente ore di funzionamento, senza richiedere manutenzione correttiva.
ALARP	As Low As Reasonably Practicable (il minimo per quanto ragionevolmente praticabile). Il principio di trattamento dei rischi che rientrano tra un estremo superiore ed un estremo inferiore. L'estremo superiore è il punto in cui il rischio è così grande che viene rifiutato completamente, mentre l'estremo inferiore è in punto in cui il rischio è (è stato reso) insignificante. Questo principio considera sia i costi che i benefici della riduzione del rischio per rendere il rischio "il minimo per quanto ragionevolmente praticabile".
Analisi dell'albero degli eventi	Un metodo di modellazione della propagazione dei guasti. L'analisi costruisce una struttura ad albero delle catene di eventi che portano da un evento scatenante a vari risultati potenziali. L'albero si espande dall'evento scatenante in rami di eventi di propagazione intermedi. Ogni ramo rappresenta una situazione in cui è possibile un diverso risultato. Dopo aver incluso tutti i rami appropriati, l'albero di eventi termina con molteplici possibili risultati.
Architettura	La logica di voting dei vari elementi di una funzione strumentata di sicurezza. Vedere "Vincoli hardware", "Tolleranza ai guasti" e "2oo3".
Avaria casuale	Un guasto che si verifica in un momento casuale e che è dovuto ad uno o più meccanismi di degradazione. Le avarie casuali possono essere efficacemente previste con metodi statistici e sono la base per i requisiti di calcolo basati sulla probabilità di guasto su domanda per il livello di integrità della sicurezza. Vedere "Guasto sistematico".
BPCS	Vedere "Sistema di controllo di processo di base".
Conseguenza	L'entità del danno o la misura del risultato di un evento dannoso. Una delle due componenti utilizzate per definire un rischio.
Copertura della prova funzionale	La percentuale di guasti che viene rilevata durante la manutenzione dell'apparecchiatura. In generale si presume che, alla realizzazione di una prova funzionale, vengano rilevati e corretti tutti gli errori del sistema (100% di copertura della prova funzionale).
Copertura diagnostica	Una misura della capacità di un sistema di rilevare i guasti. Si tratta del rapporto tra il tasso di guasto per i guasti rilevati ed il tasso di guasto per tutti i guasti nel sistema.

Diagnostica D	Alcuni logic solver di sicurezza sono designati come aventi una diagnostica con la D maiuscola. Si tratta di una diagnostica differente da quella normale in quanto, dopo il rilevamento di un guasto, l'unità è in grado di riconfigurare la propria architettura. L'effetto più importante è quello sui sistemi 1oo2D che, dopo il rilevamento di un guasto non pericoloso, possono riconfigurare il funzionamento 1oo1. In tal modo, il tasso di interventi intempestivi di questo sistema viene drasticamente ridotto.
Diagramma ad albero dei guasti	Metodo di combinazione delle probabilità per stimare probabilità complesse. Dato che generalmente offre una visuale completa dei guasti di un sistema, è utile nella modellazione di modalità di guasto multiple. Prestare attenzione quando lo si usa per calcolare le probabilità medie integrate.
Diagramma cause ed effetti	Un metodo comunemente utilizzato per dimostrare la relazione tra gli ingressi dei sensori ad una funzione di sicurezza e le uscite richieste. Spesso utilizzato come parte di una specifica dei requisiti di sicurezza. I punti di forza di questo metodo sono il limitato livello di impegno ed una chiara rappresentazione visiva mentre i suoi punti deboli sono la rigidità del formato (alcune funzioni non possono essere rappresentate) e l'eccessiva semplificazione della funzione.
Disponibilità	La probabilità che un dispositivo funzioni correttamente in un determinato momento. Si tratta di una misura del "tempo di disponibilità" ed è espressa in unità percentuali. Per la maggior parte dei componenti dei sistema di sicurezza testati e riparati, la disponibilità nel tempo varia "a dente di sega", in base ai cicli di prova funzionale e riparazione. Quindi, per calcolare la probabilità di guasto media su domanda, si utilizza la disponibilità media integrata. Vedere "PFDavg".
E/E/PE – Elettrico/ elettronico/elettronico programmabile	Vedere 61508 e 61511.
FMECA	Analisi delle modalità di guasto, degli effetti e delle criticità – Si tratta di un'analisi dettagliata delle differenti modalità di guasto e delle criticità di una parte di apparecchiatura.
Frequenza	La frequenza di un evento dannoso spesso espressa in eventi all'anno o eventi per milione di ore. Una delle due componenti utilizzate per definire un rischio. Va osservato che l'accezione, in questo caso, è diversa da quella della tradizionale definizione inglese che significa "probabilità".
Guasto di modo comune	Un problema casuale che fa sì che due o più componenti si guastino contemporaneamente e per la stessa ragione. È diverso da un guasto sistematico in quanto è casuale e probabilistico e non segue un percorso causa/effetto fisso e prevedibile. Vedere "Guasto sistematico".
Guasto in apertura	Una condizione in cui il componente che chiude la valvola si muove in posizione di apertura in mancanza della sorgente di energia.
Guasto in chiusura	Una condizione in cui il componente che chiude la valvola si muove in posizione di chiusura in mancanza della sorgente di energia.
Guasto non pericoloso	Guasto che non può mettere il sistema strumento di sicurezza in uno stato pericoloso o di mancato funzionamento. Situazione in cui un sistema o componente di sicurezza non funziona correttamente e provoca lo spegnimento del sistema o l'attivazione della funzione strumentata di sicurezza in assenza di pericolo.
Guasto pericoloso	Un guasto di un componente in una funzione strumentata di sicurezza che impedisce a quella funzione di raggiungere uno stato sicuro quando ciò viene richiesto. Vedere "Modalità di guasto".

Guasto sistematico	Un guasto che si verifica in modo deterministico (non casuale) e prevedibile per una causa che può essere eliminata solo con una modifica del progetto o del processo di fabbricazione, delle procedure operative, della documentazione o di altri fattori rilevanti. Non essendo matematicamente prevedibili, il ciclo di vita della sicurezza include un gran numero di procedure per prevenire che si verifichino. Le procedure sono più rigorose per i sistemi ed i componenti con un più alto livello di integrità della sicurezza. Tali guasti non possono essere prevenuti con la semplice ridondanza.
HAZOP	Studio dei pericoli e dell'operabilità. Una procedura di analisi dei pericoli del processo originariamente sviluppata da ICI negli anni 1970. Il metodo è altamente strutturato, divide il processo in differenti nodi operativi ed esamina il comportamento delle differenti parti di ogni nodo in base ad una matrice di possibili condizioni di deviazione o a parole chiave.
HFT	Tolleranza ai guasti hardware (v. tolleranza ai guasti)
HSE (Regno Unito)	Responsabile salute e sicurezza
IEC	Commissione elettrotecnica internazionale. Un'organizzazione internazionale per la standardizzazione. Lo scopo della IEC è quello di promuovere la cooperazione internazionale su tutte le questioni riguardanti la standardizzazione in campo elettrico ed elettronico. A tal fine ed in aggiunta ad altre attività, la IEC pubblica norme internazionali. Vedere 61508 e 61511. Analisi dell'impatto per determinare l'effetto che avrà la modifica di una funzione o di un componente sulle altre funzioni o gli altri componenti di un sistema, oltre che su altri sistemi.
IEC 61508	La norma IEC che tratta la sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili – Il principale obiettivo della norma IEC 61508 è quello di usare sistemi strumentati di sicurezza per ridurre il rischio ad un livello tollerabile seguendo le procedure globali del ciclo di vita della sicurezza hardware e software ed aggiornando la documentazione associata. Pubblicata nel 1998 e nel 2000, fino ad ora è stata usata soprattutto dai fornitori di dispositivi di sicurezza per dimostrare che le loro apparecchiature sono adatte all'uso nei sistemi classificati SIL (safety integrity level).
IEC 61511	La norma IEC per i sistemi elettrici/elettronici/elettronici programmabili legati alla sicurezza nell'industria di processo. Come la norma IEC 61508, si concentra su una serie di processi del ciclo di vita della sicurezza per gestire il rischio di processo. Originariamente pubblicata dalla IEC nel 2003, è stata ripresa dagli USA nel 2004 come ISA 84.00.01-2004. Diversamente dalla IEC 61508, questa norma si rivolge agli utenti dei sistemi strumentati di sicurezza dell'industria di processo.
Incidente	Il risultato di un evento scatenante a cui non viene impedito di propagarsi. L'incidente è la descrizione più basica di un evento indesiderato e ne fornisce le informazioni minime. Il termine incidente viene semplicemente usato per esprimere il fatto che in un processo si è verificata, ad esempio, la perdita di contenimento di un prodotto chimico o la perdita di altre potenziali sorgenti di energia. In pratica, il potenziale di danno esiste ma il risultato nocivo non ha assunto forma specifica.
Intervallo di prova funzionale	Intervallo di tempo tra gli interventi di manutenzione delle apparecchiature.
Intervento intempestivo	Vedere Guasto non pericoloso

IPL	Livello o livelli di protezione indipendente. Si riferisce a vari altri metodi possibili di riduzione dei rischi in un processo. I possibili esempi includono elementi quali dischi di rottura e valvole di sfiato che riducono indipendentemente la probabilità che il pericolo conduca ad un incidente vero e proprio con risultati dannosi. Per essere efficace, ogni livello deve impedire specificamente che il pericolo in questione provochi danni, agire indipendentemente dagli altri livelli, avere una ragionevole probabilità di funzionare e poter essere verificato, una volta che l'impianto è in funzione, per controllare che le sue prestazioni siano quelle previste.
Lambda	Tasso di guasto di un sistema. Vedere "Tasso di guasto".
Livello di protezione	Vedere IPL.
LOPA	Analisi del livello di protezione. Un metodo di analizzare la frequenza di un evento dannoso in base alla frequenza dell'evento scatenante ed alla probabilità di guasto di una serie di livelli di protezione indipendenti in grado di prevenire l'evento dannoso.
Modalità (a bassa domanda)	(Anche modalità su domanda per IEC 61511) – Quando le domande di intervento della funzione strumentata di sicurezza (SIF) sono poco frequenti rispetto all'intervallo di prova della funzione SIF. L'industria di processo definisce questa modalità quando le domande di intervento della funzione SIF sono meno di una volta ogni due intervalli di prova funzionale. La modalità di funzionamento a bassa domanda è quella più comune nelle industrie di processo. Quando si definisce il livello di integrità della sicurezza per la modalità a bassa domanda, le prestazioni di una funzione SIF vengono misurate in termini di probabilità di guasto media su domanda (PFDavg). In questa modalità di domanda, sono la frequenza dell'evento scatenante, modificata dalla probabilità di guasto su domanda della funzione SIF per il tasso di domanda e tutti gli altri livelli di protezione a valle a determinare la frequenza degli incidenti indesiderati.
Modalità (a domanda elevata)	(Anche modalità continua per IEC 61511) – Simile alla modalità continua ma con specifica considerazione della diagnostica automatica. La differenza tra modalità a domanda elevata e modalità continua risiede nella velocità di ripetizione più elevata della diagnostica automatica rispetto al tasso di domanda sulla funzione di sicurezza. Se la diagnostica è più lenta, non viene considerata e si applica la modalità continua.
Modalità (continua)	Quando le domande di intervento di una funzione di sicurezza (SIF) sono frequenti rispetto all'intervallo di prova della funzione SIF. Va osservato che altri settori definiscono una separata modalità di domanda elevata, a seconda che la diagnostica possa ridurre il tasso di incidenti. In ogni caso, la modalità continua si applica dove la frequenza di un incidente indesiderato è essenzialmente determinata dalla frequenza di un guasto SIF pericoloso. Nel caso di guasto SIF, la domanda di intervento avverrà in un intervallo di tempo molto più breve rispetto a quello della prova funzionale; quindi, parlare della sua probabilità di guasto non ha senso. Fondamentalmente, tutti i guasti pericolosi in una funzione SIF in modalità continua vengono rivelati da una domanda del processo anziché da una prova funzionale. Vedere "Modalità a bassa domanda", "Modalità a domanda elevata" e SIL.
Modalità di guasto	Il modo in cui un dispositivo si guasta. Questi modi sono generalmente raggruppati in una delle quattro modalità di guasto: non pericoloso rilevato (SD), pericoloso rilevato (DD), non pericoloso non rilevato (SU) e pericoloso non rilevato (DU) secondo ISA TR84.0.02.
MTTR	Tempo medio di riparazione – Il tempo medio tra il verificarsi di un guasto ed il completamento della riparazione di quel guasto. Include il tempo necessario a rilevare il guasto, iniziare la riparazione e completarla.

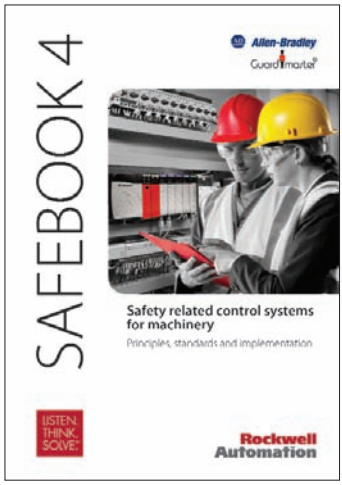
Occupazione	Una misura della probabilità che, nella zona di effetto di un incidente, siano presenti una o più persone soggette all'effetto. Questa probabilità dovrebbe essere determinata facendo riferimento ai principi ed alle pratiche di gestione del personale specifiche dell'impianto.
P&ID	Schema dell'impianto e della strumentazione. Mostra l'interconnessione delle apparecchiature di processo e della strumentazione utilizzata per controllare il processo. Nell'industria di processo, per preparare gli schemi dei processi, viene utilizzato un set di simboli standard. I simboli degli strumenti utilizzati in questi schemi sono generalmente basati sulla norma S5. 1. 2 della Instrument Society of America (ISA). Il principale schema utilizzato per il layout di un'installazione di controllo di processo.
Percentuale di guasti non pericolosi	Vedere SFF.
Pericolo	Il potenziale di danno.
PFDavg	Probabilità media di guasto su domanda – Questa è la probabilità che un sistema si guasti in modo pericoloso e non sia in grado di eseguire la sua funzione di sicurezza quando richiesto. La probabilità PFD può essere determinata come un probabilità media o massima su un determinato periodo di tempo. IEC 61508/61511 e ISA 84.01 usano la probabilità PFDavg come la metrica del sistema su cui viene definito il livello SIL.
Prova funzionale	Prova dei componenti del sistema di sicurezza atta a rilevare eventuali guasti non rilevati dalla diagnostica automatica on-line (guasti pericolosi, guasti della diagnostica e guasti parametrici) seguita dalla riparazione di quei guasti che riporta i componenti ad uno stato equivalente a quello nuovo. La prova funzionale è una parte vitale del ciclo di vita della sicurezza ed è critica per garantire che un sistema ottenga il livello di integrità della sicurezza richiesto per tutto il ciclo di vita della sicurezza.
Ridondanza	Uso di molteplici elementi o sistemi per eseguire la stessa funzione. La ridondanza può essere implementata con elementi identici (ridondanza identica) o elementi diversi (ridondanza diversa). La ridondanza viene utilizzata principalmente per migliorare affidabilità o disponibilità.
RRF	Fattore di riduzione del rischio – L'inverso di PFDavg
Schema a blocchi dell'affidabilità	Metodo di combinazione delle probabilità per stimare probabilità complesse. Dato che generalmente offre una visuale "positiva" di un sistema, può confondere quando utilizzato nella modellazione di modalità di guasto multiple.
SFF	Percentuale di guasti non pericolosi – La percentuale del tasso di guasto globale di un dispositivo che comporta un guasto non pericoloso o un guasto pericoloso diagnosticato (rilevato). La percentuale di guasti non pericolosi include i guasti pericolosi rilevabili quando tali guasti vengono segnalati e sono in atto procedure di riparazione o spegnimento.
Sicurezza funzionale	Affrancamento dal rischio inaccettabile ottenuto attraverso il ciclo di vita della sicurezza. Vedere IEC 61508, IEC 65111, ciclo di vita della sicurezza e rischio tollerabile.
SIF	Funzione strumentata di sicurezza – Un gruppo di apparecchiature destinate a ridurre il rischio dovuto ad uno specifico pericolo (loop di sicurezza). Il suo scopo è quello di 1. Portare automaticamente un processo industriale ad uno stato sicuro quando vengono violate determinate condizioni; 2. Permettere ad un processo di proseguire in modo sicuro quando determinate condizioni lo consentono (funzioni di autorizzazione); 3. Intraprendere azioni per mitigare le conseguenze di un pericolo industriale. Include elementi che rilevano l'imminenza di un incidente, decidono di intervenire ed eseguono l'azione necessaria a portare il processo in uno stato sicuro. La sua capacità di rilevare, decidere ed agire è designata dal livello di integrità della sicurezza (SIL) della funzione. Vedere SIL.

SIL	Livello di integrità della sicurezza – Un target quantitativo per misurare il livello di prestazioni della funzione di sicurezza necessario ad ottenere un rischio tollerabile per un pericolo di processo. La definizione del livello SIL target del processo dovrebbe essere basata sulla valutazione della frequenza di occorrenza di un incidente e delle conseguenze dell'incidente. La tabella che segue descrive i livelli SIL per differenti modalità di funzionamento.
SIS	Sistema strumentato di sicurezza – Implementazione di una o più funzioni strumentate di sicurezza. Un sistema SIS è composto da una qualunque combinazione di sensori, logic solver ed elementi finali. Un sistema SIS ha generalmente una serie di funzioni di sicurezza con differenti livelli di integrità della sicurezza (SIL); quindi, è meglio evitare di descriverlo con un unico livello SIL. Vedere SIF.
Sistema di controllo di processo di base	Sistema che risponde a segnali di ingresso provenienti dal processo, dalle apparecchiature associate e/o da un operatore e che genera segnali di uscita che permettono che il processo e le apparecchiature associate funzionino nel modo desiderato. Il sistema BPCS non può eseguire alcuna funzione strumentata di sicurezza classificata SIL1 o superiore a meno che non risponda ai requisiti di uso comprovato. Vedere "Uso comprovato".
Stato di sicurezza	Stato del processo dopo l'eliminazione del pericolo senza danni significativi.
Tasso di guasto	Il numero di guasti per unità di tempo di una parte di apparecchiatura. Generalmente presunto come valore costante. Può essere suddiviso in diverse categorie quali sicuro e pericoloso, rilevato e non rilevato, indipendente/normale e di causa comune. Perché il valore del tasso di guasto sia effettivamente costante, è necessario trattare correttamente i casi di mortalità infantile e usura.
Tolleranza ai guasti	Capacità di un'unità funzionale di continuare a realizzare la funzione richiesta in presenza di guasti o errori casuali. Un sistema con logica di voting 1oo2, ad esempio, può tollerare un guasto casuale dei componenti e continuare a svolgere la sua funzione. La tolleranza ai guasti è uno degli specifici requisiti per il livello di integrità della sicurezza (SIL) ed è spiegata in modo più approfondito nelle norme IEC 61508 Parte 2, Tabelle 2 e 3 e IEC 61511 (ISA 84.01 2004), articolo 11.4
Uso comprovato	Base per l'uso di un componente o sistema nell'ambito di un sistema strumentato di sicurezza (SIS) classificato SIL che non è stato progettato conformemente alla norma IEC 61508. Per determinare se un prodotto presenta problemi sistematici di design, è necessario disporre di sufficienti ore di funzionamento del prodotto, storico delle revisioni, sistemi di reporting dei guasti e dati di guasto storici. IEC 61508 fornisce i livelli dello storico di funzionamento richiesti per ogni SIL.
Verifica SIL	Processo di calcolo della probabilità di guasto media su domanda (o la probabilità di guasto all'ora) e dei vincoli hardware per il design della funzione di sicurezza, per vedere se soddisfa il livello SIL richiesto.
Vincoli hardware	Le limitazioni imposte all'hardware selezionato per implementare una funzione strumentata di sicurezza, a prescindere dalle prestazioni calcolate per un sottosistema. I vincoli hardware sono specificati (in IEC 61508-2-Tabella 2 e IEC 61511-Tabella 5) in base al livello SIL richiesto del sottosistema, al tipo di componenti utilizzati ed alla percentuale SFF dei componenti del sottosistema. I componenti di Tipo A sono semplici dispositivi che non incorporano microprocessori mentre i dispositivi di Tipo B sono dispositivi complessi come quelli che incorporano microprocessori. Vedere "Tolleranza ai guasti".

Abbreviazioni

λ	Tasso di guasto, rapporto del numero totale di guasti che si verificano in un determinato periodo di tempo
λD	Tasso di guasti pericolosi
λDD	Tasso di guasti pericolosi rilevati dalla diagnostica
λDU	Tasso di guasti pericolosi non rilevati dalla diagnostica
λS	Tasso di guasti non pericolosi
1oo1	Logica di voting 1 su 1 (simplex)
1oo2	1 su 2
AI Analog Input	(Ingresso analogico)
ALARP	As Low As Reasonably Practicable (il minimo per quanto ragionevolmente praticabile)
ANSI	American National Standards Institute
BMS	Burner Management System (sistema di gestione bruciatori)
BPCS	Basic Process Control System (sistema di controllo di processo di base)
C&E	Cause and Effect (causa ed effetto)
CBA	Cost Benefit Analysis (analisi costi/benefici)
CCF	Common Cause Failure (guasti per causa comune)
COMAH	Control Of Major Accident Hazards (controllo dei pericoli di incidenti rilevanti)
DCS	Distributed Control System (sistema di controllo distribuito)
DD	Dangerous Detected (pericoloso rilevato)
DI	Digital Input (ingresso digitale)
DO	Digital Output (uscita digitale)
DU	Dangerous Undetected (pericoloso non rilevato)
E/E/PES	Electrical/Electronic/Programmable Electronic System (sistema elettrico/elettronico/ elettronico programmabile)
ESD	Emergency Shutdown (spegnimento di emergenza)
ESDV	Emergency Shutdown Valve (valvola di spegnimento di emergenza)
F&G	Fire and Gas (incendio e gas)
f/hr	Failures per hour (guasti all'ora)
FC	Fail Closed (guasto in chiusura)
FDS	Functional Design Specification (specifica design funzionale)
FMECA	Failure Modes, Effects and Criticality Analysis (Analisi dei modi, degli effetti e della criticità dei guasti)
FO	Fail Open (guasto in apertura)
FPL	Fixed Programmable Language (linguaggi di programmazione fissi)
FSC	Functional Safety Capability (capacità sicurezza funzionale)
FVL	Full Variability Language (linguaggio a variabilità completa)
Guasto non pericoloso	Modalità di guasto che non può mettere il sistema di sicurezza in stato pericoloso o di mancato funzionamento.
Guasto pericoloso	Modalità di guasto che può mettere il sistema di sicurezza in stato pericoloso o di mancato funzionamento
HASAW	Health and Safety at Work Act (HSW) (legge sulla salute e la sicurezza sul lavoro)
HAZAN	Hazard Analysis (analisi dei pericoli)
HAZOP	Hazard and Operability Study (studio dei pericoli e dell'operabilità)
HFT	Hardware Fault Tolerance (tolleranza ai guasti hardware)
HIPPS	High Integrity Pressure Protection System (sistema di protezione dalla pressione ad alta integrità)
HSE	Health and Safety Executive (responsabile salute e sicurezza)
I/O	Input/Output (ingresso/uscita)
IEC	International Electrotechnical Commission (commissione elettrotecnica internazionale)
IPL	Independent Protection Layer (livello di protezione indipendente)
ISA	International Society of Automation (società internazionale di automazione)
LOPA	Layer of Protection Analysis (analisi del livello di protezione)
LVL	Limited Variability Language (linguaggio a variabilità limitata)
MDT	Mean Down Time (tempo medio di indisponibilità)
MooN	M out of N (caso generale) (M su N)

MTBF	Mean Time Between Failures (durata media fra due guasti)
MTR	Maximum Tolerable Risk (rischio massimo tollerabile)
MTTF	Mean Time To Failure (durata media fino ad avaria)
MTTR	Mean Time To Repair (tempo medio di riparazione)
Non-SR	Non-Safety Related (non legato alla sicurezza)
O&M	Operation and Maintenance (funzionamento e manutenzione)
OPSI	Office of Public Sector Information (ufficio informazioni del settore pubblico)
P&ID	Piping and Instrumentation Diagram (schemi dell'impianto e della strumentazione)
PA	Per Annum (all'anno)
PE	Programmable Electronic (elettronica programmabile)
PFD	Probability of Failure on Demand (probabilità di guasto su domanda)
PFH	Probability of Failure per Hour (probabilità di guasto all'ora)
PSD	Process Shutdown (spegnimento del processo)
PT	Pressure Transmitter (trasmettitore di pressione)
PTI	Proof Test Interval (intervallo di prova funzionale)
QMS	Quality Management System (sistema di gestione qualità)
R2P2	Reducing Risk Protecting People (riduzione del rischio, protezione delle persone)
RBD	Reliability Block Diagram (schema a blocchi di affidabilità)
RRF	Risk Reduction Factor (fattore di riduzione del rischio)
S	Safe (sicuro)
SA	Safety Authority (autorità di sicurezza)
SFF	Safe Failure Fraction (percentuale di guasti non pericolosi).
SIF	Safety Instrumented Function (funzione strumentata di sicurezza)
SIL	Safety Integrity Level (livello di integrità della sicurezza).
SIS	Safety Instrumented System (sistema strumentato di sicurezza)
SOV	Solenoid Operated Valve (elettrovalvola)
SRS	Safety Requirements Specification (specifica dei requisiti di sicurezza)
STR	Spurious Trip Rate (tasso di interventi indesiderato)
TMR	Triple Modular Redundant (ridondanza modulare tripla)
Tp	Proof Test Interval (intervallo di prova funzionale)



È disponibile anche:
Safebook 4 – Sistemi di controllo legati alla sicurezza delle macchine.
Questa guida in formato tascabile tratta i principi di sicurezza delle macchine, la legislazione ed una serie di elementi di teoria e pratica.
Numero di pubblicazione: SAFEBK-RM002B

Per avere una copia di questa guida, contattare il rappresentante Rockwell Automation o visitare il sito www.rockwellautomation.com

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, www.rockwellautomation.it
Svizzera: Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279

Pubblicazione: SAFEBK-RM003A-IT-P – Marzo 2013