N O R M A I T A L I A N A C E I

Progetto

C. 1225

Data Scadenza Inchiesta

07-01-2019

Data Pubblicazione

2018-11

Classificazione

65-186

Titolo

Linea guida per l'applicazione della Norma della serie CEI EN 61511
Sicurezza funzionale – Sistemi strumentati di sicurezza per il settore dell'industria di processo

Title

CEI COMITATO ELETTROTECNICO ITALIANO

AEIT FEDERAZIONE ITALIANA DI ELETTROTECNICA, ELETTRONICA, AUTOMAZIONE, INFORMATICA E TELECOMUNICAZIONI

CNR CONSIGLIO NAZIONALE DELLE RICERCHE

INDICE

1 Scopo e campo di applicazione 9
1.1 Scopo della guida 9
1.2 Campo di applicazione 10
1.3 Struttura ed utilizzo della Guida 11
2 Normativa di riferimento 14
3 Abbreviazioni e definizioni 15
3.1 Abbreviazioni 15
3.2 Definizioni 16
4 Conformità alla norma 17
5 Gestione della sicurezza funzionale 17
5.1 Obiettivi 17
5.2 Requisiti 20
6 Requisiti del ciclo di vita in sicurezza 25
6.1 Obiettivi 25
6.2 Requisiti 25
7 Modalità di verifica 27
7.1 Obiettivi 27
8 Analisi dei pericoli potenziali e dei rischi del processo 27
8.1 Obiettivi 27
8.2 Requisiti 28
9 Allocazione delle funzioni di sicurezza alle barriere di protezione 32
9.1 Obiettivi 32
9.2 Requisiti relativi al processo di allocazione 32
9.3 Requisiti del sistema di controllo di processo base come livello di protezione 36
9.4 Requisiti per prevenire guasti di causa e di modo comune e guasti dipendenti 36
10 Specificazione dei requisiti dei sistemi strumentati di sicurezza (SIS) 37
10.1 Obiettivi 37
10.2 Requisiti generali 37
10.3 Requisiti relativi alla sicurezza del SIS 37
10.4 Linea guida per la definizione dei requisiti dei SIS 37
11 Progettazione ed ingegnerizzazione del SIS 39
11.1 Obiettivi 39
11.2 Requisiti generali 39
11.3 Requisiti relativi al comportamento del sistema nella rilevazione di una anomalia 39
11.4 Requisiti relativi alla tolleranza alle anomalie dell'hardware 39
11.5 Requisiti relativi alla scelta dei componenti dei sottosistemi 42
11.6 Dispositivi da campo 47
11.7 Interfacce 48
11.8 Requisiti manutentivi 48

11.9 Quantificazione dei guasti casuali 48
12 Requisiti del software 48
13 Prove di accettazione in fabbrica (FAT) 49
13.1 Obiettivi 49
13.2 Raccomandazioni 49
14 Installazione e messa in servizio del SIS 50
14.1 Obiettivi 50
14.2 Requisiti 50
15 Validazione della sicurezza del SIS 51
15.1 Obiettivi 51
15.2 Requisiti 51
16 Esercizio e manutenzione del SIS 53
16.1 Obiettivi 53
16.2 Requisiti 54
16.3 Prove periodiche ed ispezioni 56
17 Modifica del SIS 56
17.1 Obiettivi 56
17.2 Requisiti 57
18 Dismissione del SIS 57
18.1 Obiettivi 57
18.2 Requisiti 57
19 Requisiti relativi alle informazioni ed alla documentazione 58
19.1 Obiettivi 58
19.2 Requisiti 58
19.3 Esempio di strutturazione della documentazione 58
Allegato A Sviluppo delle fasi del ciclo di vita in sicurezza per un piccolo impianto (dalla individuazione dei rischi alla definizione del sistema strumentato di sicurezza) 60
Allegato B Sviluppo del progetto dei sistemi di sicurezza di un impianto di processo industriale 82
Allegato C Criteri di individuazione delle SIF nella fase di sviluppo del progetto 95
Allegato D Criteri di valutazione dei SIL delle funzioni strumentate di sicurezza (SIF) 98
Allegato E Architetture di sottosistemi per tipici livelli di SIL di determinate SIF 102
Allegato F Linea guida per le prove di accettazione 107
Allegato G Analisi quantitativa e qualitativa dei rischi 114
Allegato H Calcolo analitico della probabilità di guasto su domanda (PFD) 123
Allegato I Determinazione della probabilità di guasto su domanda (PFD) secondo le tabelle della CEI EN 61508-6 132
Allegato L Verifica pratica del SIL in funzione dell'architettura del SIS 142
Allegato M Prove periodiche parziali dell'architettura del SIS 145
BIBLIOGRAFIA 146

PREMESSA

La presente Guida riguarda l'applicazione della normativa tecnica relativa alla sicurezza funzionale dei sistemi strumentati per gli impianti di processo industriale. Conseguentemente, essa si applica essenzialmente alla Norma di Settore CEI EN 61511:2017, che è specifica per questi sistemi. Poiché questa norma di settore è fortemente basata, per l'impostazione generale, sulla Norma Generica CEI EN 61508:2011 e ad essa rimanda per alcuni aspetti, la Guida considera spesso le due norme congiuntamente.

Sebbene la CEI EN 61511 sia composta da tre parti:

Parte 1: che specifica i requisiti del sistema di sicurezza e del relativo hardware e software;

Parte 2: che illustra le modalità per l'applicazione della CEI EN 61511-1;

Parte 3: che riporta le indicazioni per la determinazione dei necessari livelli di integrità della sicurezza,

e nonostante la Parte 2 fornisca già elementi di guida all'applicazione della Norma, è stato ritenuto opportuno sviluppare in ambito CEI questa Guida di applicazione per le seguenti ragioni principali:

- gli argomenti trattati sono piuttosto innovativi e complessi e spesso richiedono competenze multidisciplinari;
- l'intero corpo normativo presenta ancora aspetti interpretativi non del tutto chiari e spesso introduce metodologie non univoche;
- le attività che la normativa prescrive sono spesso presentate in maniera astratta e generale, senza un sufficiente numero di esemplificazioni.

La Guida si propone di aiutare i progettisti dell'impianto (processo, strumentazione & controllo, HSE), i costruttori e gli installatori dei sistemi strumentati di sicurezza, gli utilizzatori dell'impianto nelle diverse fasi (esercizio e manutenzione fino alla dismissione dei sistemi strumentati di sicurezza), gli ispettori delle autorità di controllo di sicurezza ed ambiente a superare le suddette difficoltà, cercando di fornire utili elementi per l'esatta interpretazione della Norma, per la scelta adeguata delle metodologie più consone alle diverse applicazioni e nel contempo una serie di esempi che facilitano la comprensione della Norma e le danno maggiore concretezza.

INTRODUZIONE

Ormai da decenni, le funzioni vitali per la gestione degli impianti sono affidate a sistemi automatici di misura, protezione, controllo, monitoraggio e supervisione, realizzati con tecnologie elettroniche programmabili. Questi sistemi sono in genere distribuiti all'interno degli impianti e sono interconnessi da reti di comunicazione locale e da collegamenti remoti, che per alcuni tipi di impianti, come, per esempio, quelli del sistema elettrico, sono caratterizzati da grandi estensioni territoriali.

In questo quadro, gli impianti vengono a dipendere sempre più, oltre che dalle funzionalità dei suddetti sistemi e sottosistemi di automazione, dalla loro affidabilità e di quella dell'infrastruttura di comunicazione. In particolare, se alcune delle funzioni da loro svolte coinvolgono problemi di sicurezza, l'affidabilità dei sistemi che realizzano tali funzioni deve essere particolarmente vagliata e proporzionata ai livelli di sicurezza richiesti alle diverse funzioni: si richiede, in altri termini, di considerare la cosiddetta sicurezza funzionale del sistema o sottosistema.

Nella sua accezione iniziale la sicurezza funzionale era intesa come quella parte della sicurezza globale degli impianti che dipende dal corretto funzionamento dei sistemi elettrici ed elettronici di misura, protezione e controllo preposti ad applicazioni che comportano problemi di sicurezza. I sistemi per applicazioni di sicurezza sono quei sistemi (generalmente composti da sensori, circuiti relativi alla logica di controllo, sistemi di comunicazione, attuatori finali) cui è richiesto di svolgere funzioni di sicurezza, cioè funzioni volte a ridurre il rischio di danno all'impianto, alle persone e all'ambiente, e quindi di ridurre le conseguenze economiche a livelli considerati accettabili. Le funzioni di sicurezza sono definite sia in termini di funzionalità (definizione della funzione), sia in termini di integrità della sicurezza (la probabilità che una funzione di sicurezza sia eseguita soddisfacentemente).

Le metodologie di analisi e le applicazioni delle prescrizioni di sicurezza funzionale ai suddetti sistemi strumentati si sono negli ultimi anni particolarmente evolute, portando a notevoli sviluppi e miglioramenti nelle valutazioni affidabilistiche e, con riferimento ad impianti particolarmente pericolosi, ad una più razionale gestione della sicurezza. Esse si sono quindi estese, in modo naturale, anche ad altri sistemi e componenti elettrici ed elettronici (ad esempio motori, apparecchiature di manovra, sistemi di riduzione del rischio di malfunzionamento) che, pur non essendo strumentazione di misura, protezione e controllo vera e propria, possono essere responsabili, per una loro avaria, di problemi di sicurezza.

Il concetto di sicurezza funzionale ha assunto quindi nel tempo maggiore generalità e la normativa tecnica internazionale, che si sta ora assestando in linea con lo sviluppo della tecnologia, ha recentemente aggiornato la definizione di sicurezza funzionale nel modo seguente.

"La sicurezza funzionale è quella parte della sicurezza globale delle apparecchiature e dei sistemi di controllo ad esse associati che dipende dal corretto funzionamento dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza, di altri sistemi tecnologici per applicazioni di sicurezza, di dispositivi esterni per la riduzione del rischio".

Sin da quando si cominciarono a realizzare i primi impianti tenendo conto dei requisiti di sicurezza funzionale, ci si accorse della necessità di disporre di una regolamentazione tecnica in questo importante settore dell'ingegneria. Furono prima preparate linee guida e specifiche di carattere generale da parte dei principali costruttori di sistemi di automazione e progettisti e gestori di impianti di diversa natura. Successivamente nell'ambito dell'ente di normazione internazionale (IEC) fu avviata un'intensa attività che ha già portato alla predisposizione di un consistente corpo normativo sulla sicurezza funzionale, sia di carattere generale trasversale, sia di carattere specifico per i settori particolarmente critici (centrali nucleari, stabilimenti chimici, apparecchi elettromedicali, macchinario e azionamenti).

Le prime norme tecniche sulla sicurezza funzionale sviluppate in ambito internazionale (IEC) e/o europeo (CENELEC) hanno riguardato principalmente:

- i sistemi di controllo delle centrali nucleari (Norma IEC 61513 [1]);
- i sistemi di segnalamento dei sistemi ferroviari (Norme EN 50126 [2], EN 50128 [3], EN 50129 [4]);
- le apparecchiature elettromedicali (Norma CEI EN 60601-1-4 [5]);
- i sistemi di misura e controllo dei processi industriali.

L'organo tecnico della IEC incaricato dello sviluppo della normativa tecnica per questi ultimi sistemi (il SC 65 A "Industrial-Process Measurement and Control – System Aspects") ha affrontato il problema in modo più sistematico e generale, sviluppando una norma (la serie IEC 61508 [6], composta di sette parti, successivamente recepita dal CENELEC come serie EN 61508 e dal CEI come serie CEI EN 61508), che, pur coprendo soprattutto il settore della strumentazione di controllo dei processi industriali, può essere considerata un riferimento comune anche per altre applicazioni.

Si ritiene inoltre segnalare una linea guida (la Technical Specification IEC 61000-1-2 [7]), preparata dal TC 77 "Electromagnetic Compatibility" della IEC, che fornisce indicazioni generali per la scelta dei livelli di immunità elettromagnetica dei componenti in funzione del livello di sicurezza funzionale richiesto al sistema cui essi sono destinati.

Negli anni più recenti altri importanti settori hanno ritenuto opportuno predisporre norme tecniche specifiche di prescrizioni di sicurezza funzionale, prendendo generalmente come riferimento di base i criteri generali della CEI EN 61508.

In primo luogo si vuole ricordare il settore dell'industria di processo, che pur disponendo della norma generica CEI EN 61508 nata in quell'ambito, ha predisposto (attraverso il suddetto SC 65A della IEC) una nuova norma più specifica, composta di tre parti: la IEC 61511 [8] recepita dal CENELEC come EN 61511 e dal CEI come CEI EN 61511. Si ritiene anche opportuno segnalare che il SC 65A ha elaborato, sempre per il settore dell'industria di processo, secondo i criteri generali indicati nella suddetta IEC/TS 61000-1-2, alcune parti della norma di prodotto sulla compatibilità elettromagnetica, la IEC 61326, relative alla definizione dei livelli di immunità elettromagnetica per i componenti dei sistemi di sicurezza nei processi industriali [9].

Altre norme di settore già pubblicate o in fase di elaborazione riguardano:

- il macchinario (Norme IEC 62061 [10] e ISO 13849 [11]);
- gli azionamenti (Progetto IEC 61800-5-2 [12]);
- la domotica (Norma EN 50090-2-3 [13]).

La presente Guida riguarda l'applicazione della normativa tecnica relativa ai sistemi strumentati per gli impianti di processo industriale. Conseguentemente, essa si applica essenzialmente alla Norma CEI EN 61511 Edizione 2 del 2017, che è specifica per questi sistemi; poiché però questa norma di settore è fortemente basata, per l'impostazione generale, sulla Norma generale CEI EN 61508 Edizione 2 del 2011 e ad essa rimanda per alcuni aspetti, la Guida considera spesso le due norme congiuntamente.

Nella preparazione della Guida, si è tenuto conto di una serie di documenti disponibili nella letteratura tecnica sull'argomento, sviluppati da diverse organizzazioni [14-15].

Si ritiene opportuno, per una migliore comprensione della Guida, riassumere qui di seguito i punti salienti delle due norme.

La Norma CEI EN 61508

Come già accennato, si tratta di una norma generica che, anche se è stata sviluppata precipuamente per applicazioni riguardanti i sistemi di misura e controllo dei processi industriali, contiene metodologie generali che possono essere applicate nello sviluppo dei sistemi per la sicurezza di altri tipi di impianto che non dispongono di altre norme di riferimento specifiche.

La norma definisce i criteri di progettazione e gestione dei sistemi di sicurezza Elettrici/Elettronici/Elettronici Programmabili (E/E/PE) degli impianti per garantire un adeguato livello di sicurezza funzionale.

In particolare, a livello progettuale, la Norma considera:

- l'analisi dell'ambiente, dell'impianto in esame e la determinazione dei suoi confini;
- l'analisi dei rischi in tutte le possibili situazioni;
- la specifica dei requisiti delle funzioni di sicurezza e del loro necessario livello di integrità;
- l'allocazione delle funzioni di sicurezza nei sistemi strumentali per la sicurezza;
- la pianificazione dell'esercizio e della manutenzione dei sistemi di sicurezza per garantirne la funzionalità e l'affidabilità nel tempo.

Elemento essenziale del processo è il controllo del ciclo di vita in sicurezza (Safety-Life-cycle) dell'impianto, dalla sua concezione alla sua dismissione, sulla base dell'analisi quantificata dell'affidabilità dell'hardware e del software che realizzano le funzioni di sicurezza e sulla validazione della sicurezza funzionale (Functional Safety Assessment).

Il concetto fondamentale introdotto dalla CEI EN 61508 è quello di livello di integrità della sicurezza delle funzioni di sicurezza (SIL - Safety Integrity Level), sul quale è basato il ciclo di vita per la sicurezza dei sistemi e, in particolare, la progettazione delle funzioni che devono garantire la sicurezza dell'apparecchio sotto controllo (EUC) e delle catene di strumentazione che le realizzano.

La Norma definisce valori discreti di SIL da 1 a 4, in ordine crescente di integrità (si veda la Tabella sottostante), a cui corrispondono gamme di valori di probabilità di fallimento decrescente della funzione di sicurezza considerata, per due condizioni di funzionamento:

- funzionamento a bassa richiesta di intervento della funzione (meno di una volta all'anno), per il quale si specifica la probabilità per ogni singolo evento;
- funzionamento ad alta richiesta di intervento della funzione (o continua), per il quale si specifica la densità di probabilità (probabilità per ora di funzionamento).

Livelli di Integrità della Sicurezza definiti nella Norma CEI EN 61508

SIL	**FUNZIONAMENTO A BASSA RICHIESTA O SU DOMANDA** Probabilità di fallimento a fronte di una richiesta	**FUNZIONAMENTO AD ALTA RICHIESTA O CONTINUA** Probabilità di fallimento per ora
1	da $\geq 10^{-2}$ a $<10^{-1}$	da $\geq 10^{-6}$ a $<10^{-5}$
2	da $\geq 10^{-3}$ a $<10^{-2}$	da $\geq 10^{-7}$ a $<10^{-6}$
3	da $\geq 10^{-4}$ a $<10^{-3}$	da $\geq 10^{-8}$ a $<10^{-7}$
4	da $\geq 10^{-5}$ a $<10^{-4}$	da $\geq 10^{-9}$ a $<10^{-8}$

Considerata la trasversalità e la complessità del tema affrontato, si è considerato opportuno suddividere la Norma in sette parti:

– le prime tre si occupano di definire il processo di valutazione della sicurezza e del rischio e di implementare le funzioni di sicurezza;

– le successive quattro forniscono le definizioni necessarie alla corretta interpretazione della Norma e presentano esempi applicativi della stessa, in particolare con riferimento al calcolo dei SIL, indicano criteri di progetto e gestione per migliorare l'affidabilità dell'hardware e del software che realizzano le funzioni di sicurezza.

L'impatto industriale della IEC 61508 è già considerevole: sono oggi disponibili sul mercato internazionale apparecchiature e sistemi di protezione di impianti di processo industriale conformi alla CEI EN 61508 e molte attività di ingegneria, per le fasi di sviluppo e verifica del progetto delle apparecchiature e degli impianti in cui esse saranno installate, sono organizzate secondo i criteri dettati dalla suddetta Norma.

Per estendere ulteriormente l'applicabilità e la trasversalità della CEI EN 61508, è stata emessa l'Edizione 2 che presenta talvolta sostanziali revisioni dell'Edizione 1 della Norma, che la porta a norma di riferimento per le metodologie di sviluppo di tutti i sistemi con requisiti di sicurezza che possono essere affrontati con l'utilizzo di sistemi E/E/PE. In particolare, sebbene non preveda sostanziali modifiche nel criteri di controllo del ciclo di vita in sicurezza (se non raggruppando vaie fasi previste per i Sistemi relativi alla Sicurezza – SRS – non strumentati) e nei valori ammessi per le probabilità di fallimento delle funzioni di sicurezza per i diversi valori di SIL, prevede invece dei requisiti normativi per la valutazione dei rischi e per la determinazione dei relativi SIL, che sono portati da Appendici informative a Requisiti normativi all'interno della Norma. Inoltre sono stati previsti sostanziali cambiamenti nella definizione dei requisiti dei risultati delle diverse fasi del ciclo di vita in sicurezza. In questo modo la norma intende rendere più rigoroso il processo di progettazione, sviluppo e verifica. Sono inoltre considerate nuove tecnologie, come gli ASIC (Application Specific Integrated Circuits) e i FPGA (Field Programmable Gate Array), e linguaggi di sviluppo, di tipo Data Driven e Object Oriented, non compresi nella Norma in Edizione 1. Infine sono stati introdotti dei criteri di prove periodiche parziali PST (Partial Stroke Test) che con adeguati livelli di copertura (Proof Test Coverage), possono diluire gli intervalli delle prove periodiche TI (Test Interval), ovvero migliorare il SIL nei tempi di missione richiesti.

La Norma CEI EN 61511

La Norma CEI EN 61511 è la norma specifica per l'industria di processo, comprendente, in particolare: il settore chimico, quello della raffinazione, quello della produzione della carta, quello della produzione di energia elettrica (escludendo le centrali nucleari, che, come già visto, hanno una normativa specifica).

La Norma rispecchia la struttura ed i contenuti della Norma generica CEI EN 61508, ma fornisce prescrizioni maggiormente dettagliate e puntuali per la strumentazione di misura e controllo dei processi industriali. Essa deve essere comunque applicata, come già osservato, in congiunzione con la norma generica, in quanto fa riferimento a quest'ultima per le metodologie generali e per le specificazioni dei singoli componenti.

La Norma riprende i concetti base di ciclo di vita in sicurezza e di SIL e introduce i criteri di progetto dei sistemi strumentati di sicurezza (SIS) per l'industria di processo. Semplificando, si può affermare che mentre la Norma CEI EN 61511 è soprattutto orientata ai progettisti, integratori e utilizzatori dei SIS, la Norma CEI EN 61508 è utilizzata dai produttori e fornitori dei dispositivi impiegati nei SIS.

La norma è strutturata in tre parti:

– la prima parte è la norma vera e propria, che contiene le definizioni e i requisiti dell'hardware del software per i sistemi strumentati di sicurezza;

– la seconda parte è una guida di applicazione della prima;

– la terza parte fornisce linee guida per la determinazione dei SIL.

Anche questa Norma CEI EN 61511 è stata revisionata ed emessa in Edizione 2 recependo in toto i requisiti di ridondanza previsti dall'Edizione 2 della CEI EN 61508 in relazione al SIL richiesto utilizzando componenti "prior use" e "proven use" ovvero componenti di dimostrata affidabilità provati anteriormente in utilizzazioni similari.

LINEA GUIDA PER L'APPLICAZIONE DELLA NORMA DELLA SERIE CEI EN 61511 Sicurezza funzionale – Sistemi strumentati di sicurezza per il settore dell'industria di processo

1 Scopo e campo di applicazione

1.1 Scopo della guida

La presente Guida non intende sostituire la Norma di riferimento, ma fornisce suggerimenti pratici e raccomandazioni per l'applicazione degli articoli della Norma internazionale IEC 61511, recepita come Norma europea EN 61511 e come Norma italiana CEI EN 61511, per il soddisfacimento dei requisiti di sicurezza funzionale dei sistemi strumentati per gli impianti dell'industria di processo(1), dei quali qui di seguito si fornisce un'elencazione esemplificativa:

– impianti che provvedono alla trasformazione chimico-fisica della materia prima;
– impianti di produzione, trasmissione e distribuzione dell'energia elettrica;
– impianti di estrazione e trattamento del petrolio e derivati e del gas;
– impianti di chimica di base e di chimica fine;
– impianti di produzione farmaceutica, alimentare, di carta e cellulosa, di vetri e cemento;
– impianti di trattamento di metalli e minerali e di acque reflue.

Sebbene la CEI EN 61511 sia composta da tre parti:

1. che specifica i requisiti del sistema di sicurezza e del relativo hardware e software;
2. che illustra le modalità per l'applicazione della CEI EN 61511-1;
3. che riporta le indicazioni per la determinazione dei necessari livelli di integrità della sicurezza,

l'intero corpo normativo presenta ancora aspetti interpretativi ed anche metodologici specifici che si ritiene opportuno evidenziare e circostanziare nella presente linea guida, anche in riferimento alle prescrizioni generali contenute nella norma base CEI EN 61508.

Pertanto la presente linea guida potrà essere un corretto ausilio a quanti nelle diverse fasi del ciclo dell'impianto sono coinvolti nella tematica della sicurezza funzionale ed è quindi dedicata in particolar modo a tutti gli attori interessati che intervengono nelle diverse fasi del ciclo di vita: concezione, progettazione, sviluppo, installazione, esercizio e manutenzione.

(1) A seconda delle caratteristiche fisiche e di trattamento delle materie (materie prime, semilavorati e prodotti) il processo può essere:
- *Continuo*, dove i materiali/prodotti siano fluidi e vengano trattati senza interruzione di funzionamento, ovvero seguendo un ciclo tecnologico obbligato (sequenzialmente definito), o comunque lentamente variabile.
  Negli impianti di questo tipo, il flusso continuo della materia prima e del prodotto finito, gli stati di conversione e il trasporto sono intimamente fusi nelle attrezzature produttive costituenti l'impianto.
  L'impianto esegue un solo ciclo di lavorazione e fornisce una varietà di prodotto per un periodo di tempo determinato (ad esempio raffinerie, impianti chimici, centrali elettriche parte produzione, cementifici).
- *Discontinuo*, quando il trattamento richiede interruzione di funzionamento per cambiare materia prima o attrezzatura (ad esempio laminatoi, cartiere).
- *Batch*, quando il processo richiede differenti ricette e criteri di produzione (ad esempio farmaceutica, alimentare, tessile).
- *Discreto*, detto anche ciclo tecnologico non obbligato, cioè un processo in cui una stessa linea può essere destinata alla produzione di una varietà di prodotti diversi (industria manifatturiera).
- *Non industriale*, cioè qualsiasi processo riguardante trasporti, ambiente e comunicazioni.

La linea guida, partendo dagli articoli della norma di riferimento CEI EN 61511-1, fornisce criteri pratici per l'interpretazione e l'attuazione dei requisiti, chiarendo gli aspetti non sufficientemente trattati nella norma di riferimento e illustrando negli Allegati alcuni casi applicativi sul ciclo di vita in sicurezza, sulla determinazione dei livelli di integrità della sicurezza e sull'esercizio e manutenzione dei sistemi integrati per la sicurezza funzionale.

Scopo della Guida è altresì quello di individuare criteri di riferimento progettuali consolidati per tipologie di apparecchiature e sottosistemi a cui siano associabili determinati Livelli di Integrità di Sicurezza (SIL). Ad esempio, si citano i sistemi di protezione contro la sovra-velocità di compressori e turbine, sistemi di protezione di reattori in cui possono essere presenti reazioni fuggitive, sistemi di protezione di colonne di distillazione contro possibili anomalie di processo (sovra-riempimenti, sovra-pressioni) e altri sistemi di protezione.

1.2 Campo di applicazione

Il campo di applicazione della Guida coincide ovviamente con il campo di applicazione della Norma di riferimento CEI EN 61511-1, di cui si richiamano qui di seguito i punti essenziali.

La Norma di riferimento si applica alla implementazione, all'allocazione, al progetto di dettaglio (hardware e software), alla verifica e alla gestione dei sistemi strumentati di sicurezza per impianti di processo industriali.

Tali sistemi sono costituiti da apparecchiature, dispositivi e sottosistemi che assicurano che siano mantenute nel tempo le funzioni di sicurezza per cui sono stati progettati. Sono compresi, in questa catena, i sensori, i risolutori logici con funzione di protezione e gli elementi finali (attuatori e valvole).

Una corretta implementazione della Norma favorisce la conformità dell'impianto a tutti gli aspetti di legge legati alla prevenzione e gestione della sicurezza.

Attualmente il rispetto di tali disposizioni non è sempre agevole, poiché l'impianto legislativo relativo non è sempre organico e lineare, con sovrapposizioni tra norme e decreti non facili da gestire; la norma rappresenta comunque lo stato dell'arte in materia di concezione, progettazione, installazione ed esercizio dei processi industriali.

Un grosso vantaggio nell'applicazione della CEI EN 61511-1 risiede nel raggiungimento degli obiettivi da attuare per i rapporti di sicurezza per la salvaguardia dell'ambiente in impianti trattanti sostanze pericolose(1) e per la salvaguardia del personale, dell'ambiente e dei beni in impianti trattanti sostanze infiammabili e/o fluidi ad elevate pressioni.(2)

La Norma si riferisce inoltre ai requisiti da ottenere per i sistemi di allarme e blocco automatico, per i parametri operativi critici, per i blocchi di emergenza degli impianti tecnologici (3).

La Norma è essenzialmente applicabile ai SIS (Sistemi Strumentati di Sicurezza) che utilizzano tecnologia elettrica/elettronica/elettronica programmabile, ma può essere anche utile come riferimento, per apparecchiature e dispositivi non strumentati correlati (ad esempio: bunker, valvole di sicurezza, dischi di rottura, ecc.).

(1) Per esempio per ottemperare ai requisiti previsti dal D.Lgs. 334/99 "Attuazione Direttiva 96/82/CE " Seveso"

(2) Per esempio per ottemperare ai requisiti previsti dalla Direttiva ATEX (94/9 CE ora "rifusa" come 2014/34/UE) e dalla Direttiva PED (94/9-98/37CE ora "rifusa" come 2014/29/UE)).

(3) Disposizioni del DM 04/05/1998 (decreto attuativo DPR 12.1.98), *blocchi di emergenza degli impianti tecnologici*

1.3 Struttura ed utilizzo della Guida

La Guida è costituita essenzialmente da un testo e da vari allegati:

- il testo sintetizza e chiarisce, dove necessario articolo per articolo, la Norma di riferimento CEI EN 61511-1 e pertanto scorre in parallelo agli articoli di questa Norma;
- gli Allegati forniscono invece alcuni dettagli ed esemplificazioni sull'analisi del rischio, sulla definizione del SIL richiesto al SIS per attuare la riduzione necessaria del rischio ed in genere sulla concezione, progettazione, installazione e collaudo del SIS, nonché sulle prove periodiche di esercizio per mantenere il SIL richiesto.
- L'Allegato A fornisce elementi per il lettore non esperto per l'applicazione della norma specifica CEI EN 61511 e di quella generica CEI EN 61508. Questo Allegato ha un carattere particolare: esso non intende approfondire aspetti specifici della Guida, ma piuttosto fornire un esempio tipico di applicazione della Norma CEI EN 61511 ad un impianto semplice; pur essendo perfettamente in linea con la Guida, segue un approccio semplificato, che può aiutare coloro che per la prima volta affrontano una problematica così complessa. A costoro si consiglia di leggerlo, prima di approfondire la Guida completa per l'applicazione al loro impianto. Esso può essere invece tralasciato da coloro che hanno già avuto occasione di occuparsi di sicurezza funzionale di apparati e sistemi per gli impianti di processo industriali.
- L'Allegato B descrive le attività di ingegneria da svolgere in fase di progettazione di un impianto di processo industriale, in relazione alla sicurezza funzionale, considerando le fasi di: fattibilità, base e dettaglio.
- L'Allegato C illustra i criteri di individuazione delle funzioni strumentate di sicurezza (SIF) durante le fasi di sviluppo del progetto dell'impianto, sulla base degli schemi semplificati di flusso del processo e dei loops fondamentali di regolazione e di protezione.
- L'Allegato D definisce i criteri di valutazione delle SIF per alcune tipologie di apparecchiature di processo, quali, colonne di distillazione, reattori fuggenti, forni, turbine, caldaie, ecc.
- L'Allegato E classifica la tipologia della componentistica dei sottosistemi costituenti il sistema strumentato di sicurezza (SIS) e determina i vincoli di ridondanza di architettura richiesti, sviluppando degli esempi di calcolo per verificarne la conformità al livello di integrità di sicurezza (SIL) richiesto.
- L'Allegato F definisce ed elenca le prove di accettazione richieste, sia in fabbrica (FAT) che in sito (SAT), e le prove di integrazione in sito (SIT).
- L'Allegato G fornisce criteri e metodologie atte a qualificare e a quantificare le conseguenze derivabili dai potenziali rischi in termini di danni all'ambiente, danni al personale interno ed esterno all'impianto e danni alla struttura e all'attrezzatura dell'impianto.
- L'Allegato H riporta metodi analitici di calcolo della probabilità di guasto su domanda (PFD) delle principali architetture previste per i sistemi strumentati di sicurezza (SIS) quali, architetture 1oo1, 1oo2, 2oo2, 2oo3, ecc., al fine di determinare la conformità rispetto al livello di integrità di sicurezza (SIL) richiesto.
- L'Allegato I, complementare all'Allegato H, riporta alcune tabelle che permettono di determinare agevolmente se la PFD risponde ai requisiti del SIL in relazione al rateo di guasti (λ), alla frazione di guasti comuni (β), alla copertura diagnostica (DC) e all'intervallo temporale delle prove periodiche (TI) previste.
- L'Allegato L riporta alcune tabelle pratiche di confronto tra le principali architetture dei SIS, con diversi tipi di ridondanza, al variare dei principali parametri che influenzano il SIL: copertura diagnostica dei sottosistemi del SIS, e intervallo delle prove periodiche.
- L'allegato M riporta infine la metodologia e i benefici delle prove periodiche parziali (PST) che, se condotte all'interno delle prove periodiche totali, possono migliorare da un lato il SIL nominale, o dall'altro lato mantenere per più lungo tempo il SIL nominale richiesto.

La Guida è indirizzata ai progettisti dell'impianto (processo, strumentazione & controllo, HSE), ai costruttori e agli installatori dei sistemi strumentati di sicurezza, agli utilizzatori dell'impianto nelle diverse fasi (esercizio e manutenzione fino alla dismissione dei sistemi strumentati di sicurezza), ispettori delle autorità di controllo di sicurezza ed ambiente.

Per orientare il lettore, si riportano qui di seguito una tabella (Tabella 1) e alcuni diagrammi (Figure 1, 2 e 3), tratti dalla Norma di riferimento, che indirizzano all'utilizzazione delle varie parti della Norma CEI EN 61511, congiuntamente alla CEI EN 61508, in relazione alle attività da svolgere.

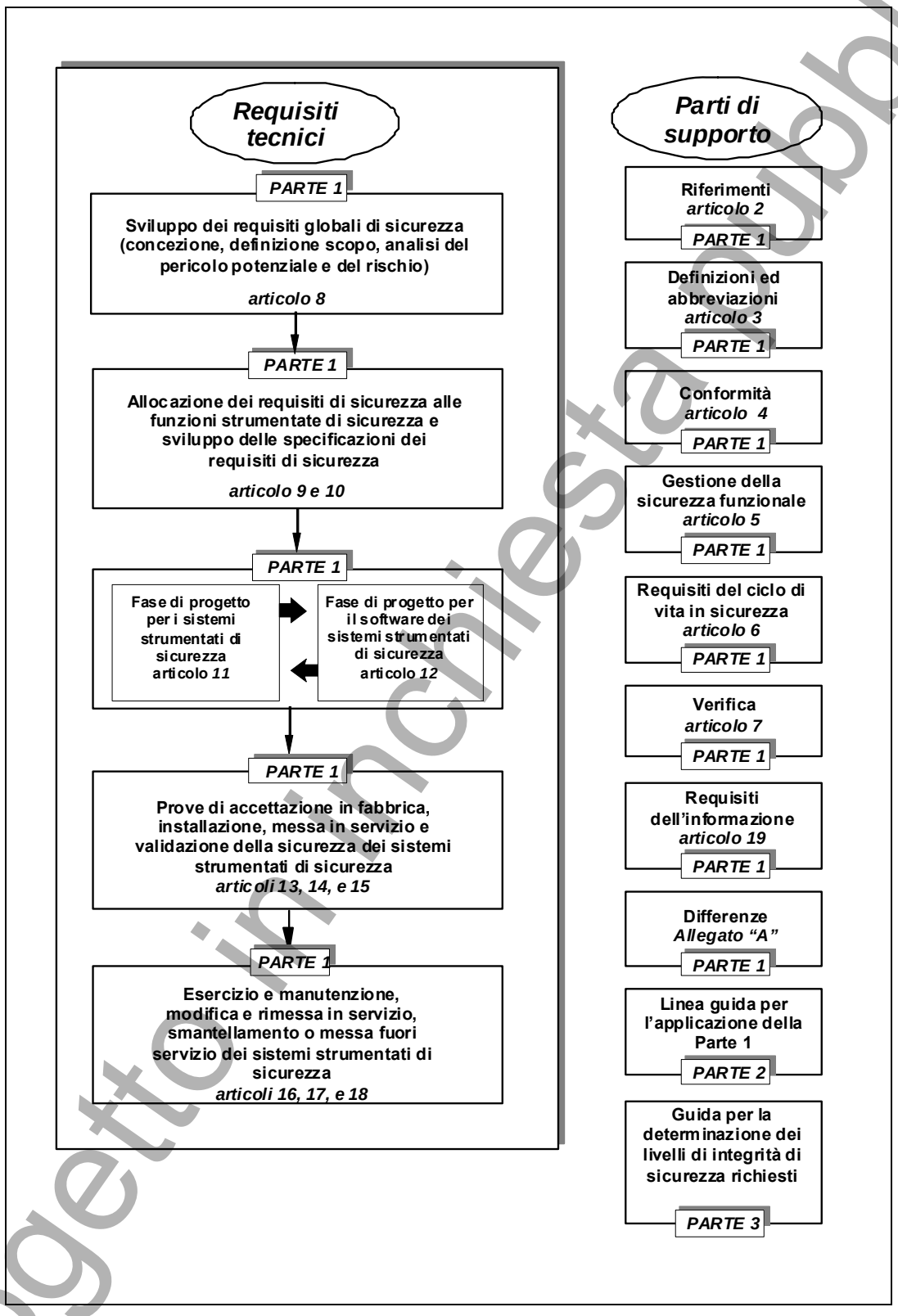


Figura 1 – Contenuti delle varie Parti e articoli della Norma CEI EN 61511

Tabella 1 -– Parti delle Norme 61511 e 61508 da utilizzare per le diverse attività relative alla sicurezza funzionale dei SIS per gli impianti di processo industriali

Attività	Norma CEI EN da utilizzare
Progettazione e realizzazione di sistemi strumentati di sicurezza (SIS)	61511-1 61511-2
Scelta di apparecchiature precedentemente provate	61508-2 61511-1
Progettazione e realizzazione delle apparecchiature per sistemi SIS	61508-2 61508-3
Verifiche di conformità delle apparecchiature per sistemi SIS	61508-2 61508-3
Progettazione e realizzazione del software intrinseco delle apparecchiature	61508-3
Progettazione e realizzazione del software applicativo	61511-1
Esercizio e manutenzione	61511-1 61511-2
Determinazione dei livelli di integrità della sicurezza	61511-3

Figura 2 – Relazioni tra CEI EN 61511 e CEI EN 61508

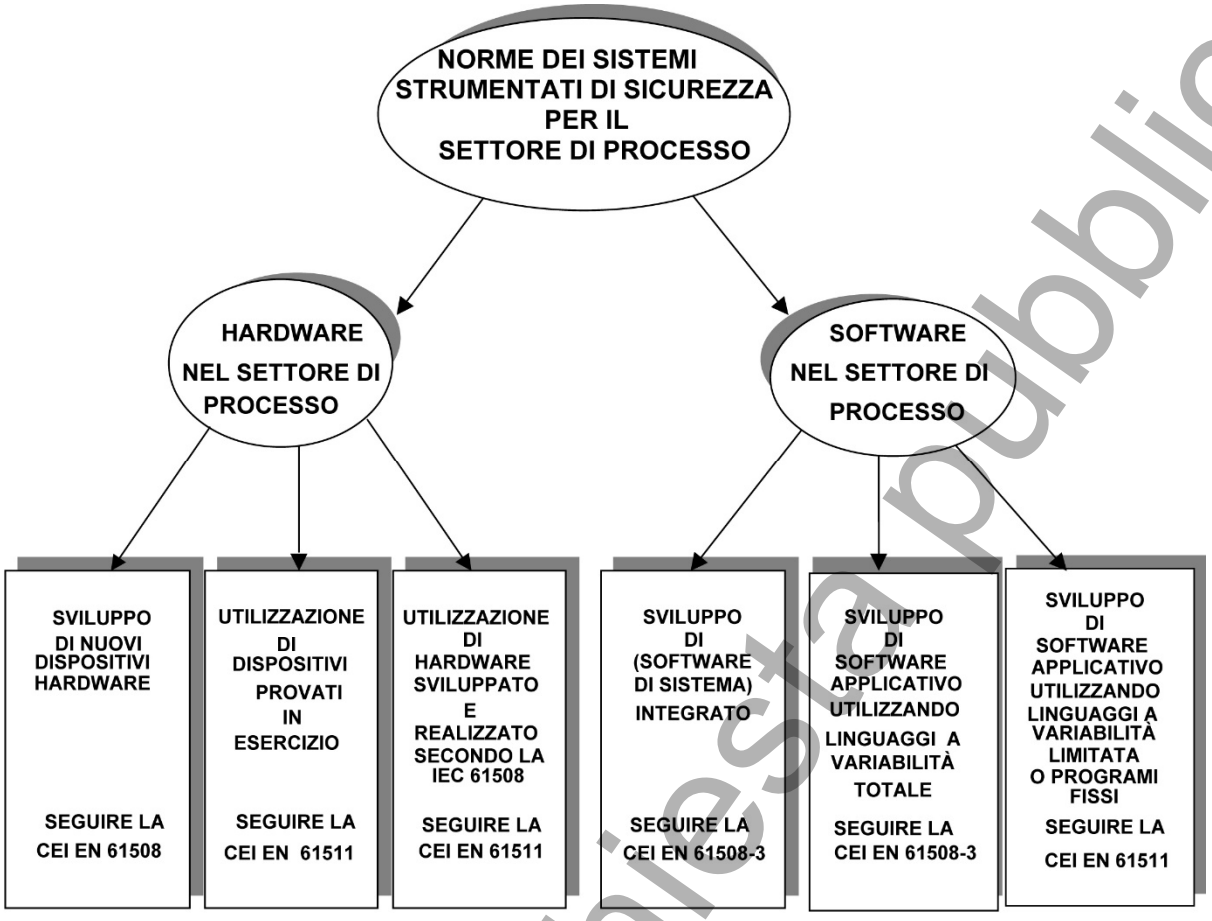


Figura 3 – Relazioni tra CEI EN 61511 e CEI EN 61508 in funzione dell'applicazione

2 Normativa di riferimento

Le norme di riferimento sono quelle riportate al corrispondente articolo 2 della Norma CEI 61511-1 o corrispondentemente nell'Allegato ZA delle corrispondenti norme CENELEC e CEI.

Tuttavia, per l'utilizzazione della presente Guida, può essere utile consultare, in relazione all'applicazione, oltre alle norme già citate nell'Introduzione, anche alcune delle seguenti norme (per semplicità si fa solo riferimento alle norme internazionali IEC):

- Serie IEC 60300, per gli aspetti generali di fidatezza di apparecchiature e di sistemi;
- Serie IEC 61131, per i controllori logici programmabili;
- Serie IEC 60770, per i trasmettitori industriali di misura;
- Serie IEC 60534, per le valvole di regolazione industriali;
- Norma IEC 62381 "Prove di accettazione in fabbrica (FAT), prove di accettazione in sito (SAT) e prove di integrazione in sito (SIT) sui sistemi di automazione degli impianti di processo industriali";
- Norma IEC 62382 "Verifica della funzionalità elettrica e dei collegamenti fra strumenti".

Le seguenti altre norme possono essere di ausilio:

- DIN V VDE 19250: Fundamental safety aspects to be considered for measurement and control protective equipment;
- ISA 8401: Application of safety instrumented systems for the process industries.

3 Abbreviazioni e definizioni

3.1 Abbreviazioni

Le abbreviazioni utilizzate nella presente Linea Guida sono derivate dalla CEI EN 61511-1 e sono riportate in Tabella 2 (in corsivo neretto quelle aggiunte).

Tabella 2 – Abbreviazioni e loro significato in inglese ed in italiano

Abbreviazione	Significato in Inglese	Significato in Italiano
AC/DC	Alternating Current/Direct Current	Corrente alternata/corrente continua
ALARP	As Low As Reasonable Practicable	Basso quanto ragionevolmente praticabile
ANSI	American National Standard Institute	Organismo di normazione americano
BPCS	Basic Process Control System	Sistema di controllo di processo base
DC	Diagnostic Coverage	Copertura diagnostica
DCS	***Distributed Control System***	***Sistema di controllo distribuito***
DIN	***Germany* Organization of Standardization**	***Organizzazione di normazione tedesca***
E/E/PE	Electrical/Electronic/ Programmable Electronic	Elettrico/elettronico/elettronico programmabile
E/E/PES	Electrical/Electronic/Programmable Electronic System	Sistema elettrico/elettronico/elettronico programmabile
EMC	Electro-Magnetic Compatibility	Compatibilità Elettromagnetica
EN	***European Normative***	***Normativa europea***
ESD	***Emergency Shut Down***	***Fermata di emergenza***
ESV	***Emergency Shut Valve***	***Valvola di blocco di emergenza***
EUC	***Equipment Under Control***	***Apparecchiatura sotto controllo***
FAT	Factory Acceptance Testing	Prove di accettazione in fabbrica
FGS	*Fire Gas System*	*Sistema di rivelazione gas e incendio*
FPS	*Fire Protection System*	*Sistema di protezione gas e incendio*
FMEA	***Failure Mode Effect Analysis***	***Analisi dei modi di avaria e degli effetti relativi***
FMECA	***Failure Mode Effect & Criticality Analysis***	***Analisi dei modi di avaria ed effetti e criticità relativi***
FMEDA	***Failure Mode Effect & Diagnostic Analysis***	***Analisi dei modi di avaria ed effetti e diagnostica relativi***
FPL	Fixed Program Language	Linguaggio di programmazione fisso
FS	Fail Safe	A prova di guasto
FT	Fault tollerant	Tollerante il guasto
FSA	***Functional Safety Assessment***	***Valutazione della sicurezza funzionale***
FSM	***Functional Safety Manager***	***Gestore della sicurezza funzionale***
FTA	Fault Tree Analysis	Analisi con metodo dell'albero dei guasti
FVL	Full Variability Language	Linguaggio a variabilità totale
HAZID	***Hazard Identification***	***Metodo di identificazione dei pericoli***
HAZOP	***Hazard And Operability Study***	***Metodo di Analisi dei Rischi ed operabilità***
HFT	Hardware Fault Tolerance	Tolleranza ai guasti hardware
HMI	Human Machine Interface	Interfaccia uomo macchina
H & RA	Hazard & Risk Analysis	Analisi dei pericoli e dei rischi
HRA	Human Reliability Analysis	Analisi dell'affidabilità umana
HSE	Health, Safety Environment	Ufficio ambiente, sicurezza e salute
H/W	Hardware	Hardware

(continua)

Abbreviazione	Significato in Inglese	Significato in Italiano
IEC	International Electrotechnical Commission	Commissione Elettrotecnica Internazionale
IEV	International Electrotechnical Vocabulary	Vocabolario Elettrotecnico Internazionale
IPL	***Independent Protection Layer***	***Livello di protezione indipendente***
ISA	Instrumentation and Automation Society	Assoc. automazione e strumentazione (USA)
ISO	International Organization of Standardization	Organismo Internazionale di Normazione
LOPA	***Layer Of Protection Analysis***	***Analisi del livello di protezione***
LVL	Limited Variability Language	Linguaggio a variabilità limitata
MooN	"M" Out Of "N"	Architettura "M" canali su "N"
MRT	***Mean Repair Time***	***Tempo medio di riparazione (componente)***
MTTF	***Medium Time To Failure***	***Tempo medio tra guasti***
MTTR	***Medium Time To Restoration***	***Tempo medio di ristabilimento (loop)***
NFPA	***National Fire Protection Association***	***Associazione protezione incendio (USA)***
NP	Non Programmable	Non programmabile
PCS	***Process Control System***	***Sistema di controllo del processo***
PFD	Probability of Failure on Demand	Probabilità di guasto su domanda
PFD_{avg}	Average Probability Of Failure On Demand	Probabilità media di guasto su domanda
PL	***Protection Layer***	***Livello di protezione***
PLC	Programmable Logic Controller	Controllore logico programmabile
PRA	Preliminary Risk Assessment	Valutazione preliminare dei rischi
PSD	Process Shut Down	Fermata del processo
PST	***Partial Stroke Tests***	***Prove parziali***
PTC	***Proof Test Coverage***	***Copertura delle prove parziali***
QA	Quality Assurance	Assicurazione qualità
QRA	Quantitative Risk Analysis	Analisi quantitativa dei rischi
RRF	Reduction Risk Factor	Fattore di Riduzione del Rischio
RTD	Resistance Thermal Detector	Termoresistenza
SAT	***Site Acceptance Test***	***Prove di accettazione in sito***
SFF	Safe Failure Fraction	Frazione dei guasti sicuri
SIF	Safety Instrumented Function	Funzione strumentata di sicurezza
SIL	Safety Integrity Level	Livello di integrità di sicurezza
SIS	Safety Instrumented System	Sistema strumentato di sicurezza
SIT	***Site Integration Test***	***Prove di integrazione in sito***
SLC	***Safety Life Cycle***	***Ciclo di vita in sicurezza***
SP	***Safety Plan***	***Piano di sicurezza***
SrS	***Safety related System***	***Sistemi relativi alla sicurezza***
SRS	Safety Requirement Specifications	Specifiche dei requisiti di sicurezza
S/W	Software	Software
TC	***Thermocouple***	***Termocoppia***
TI	***Time Interval (between tests)***	***Intervallo di tempo (tra prove)***
UPS	***Uninterrupted Power Supply***	***Sistema di alimentazione di continuità***

(fine tabella)

3.2 Definizioni

Per le esigenze del presente documento, si applicano le definizioni della Norma di riferimento CEI EN 61511-1 e della CEI EN 61508-4.

4 Conformità alla norma

La conformità alla Norma di riferimento CEI EN 61511-1 richiede che siano rispettati tutti gli articoli da 5 a 19 della Norma stessa. La presente Guida, in modo complementare a quanto già contenuto nella CEI EN 61511-2, cercherà, articolo per articolo, di meglio chiarire come i requisiti in essi indicati possano essere soddisfatti.

5 Gestione della sicurezza funzionale

5.1 Obiettivi

Come chiaramente indicato nella Norma di riferimento, in questo articolo vengono identificate le attività di gestione che sono necessarie per assicurare che la sicurezza funzionale sia garantita.

Sebbene la Norma di riferimento sia abbastanza chiara ed esaustiva per questi aspetti, si ritiene opportuno integrare questo articolo con alcune indicazioni e chiarimenti che ne facilitino l'applicazione.

La gestione della sicurezza funzionale deve considerare essenzialmente i principi per la riduzione del rischio e l'approccio generale del ciclo di vita in sicurezza.

L'attività di gestione della sicurezza funzionale prevede che sia messo a punto, da parte della Funzione Gestione della Sicurezza Funzionale, un Piano di Sicurezza (Safety Plan), che considera le diverse fasi del Ciclo di Vita in Sicurezza (Safety Life Cycle), a partire dalla fase di progetto concettuale dell'impianto fino alla sua dismissione.

Lo svolgimento delle varie fasi del ciclo di vita dei Sistemi Strumentati di Sicurezza (SIS), per le applicazioni di sicurezza funzionale generali deve seguire il percorso normalizzato dalla CEI EN 61508 (Figura 4), mentre per le applicazioni di sicurezza funzionale specificatamente dedicate all'industria di processo, oggetto della presente Guida, il percorso indicato dalla CEI EN 61511 (Figura 5).

Il Piano di Sicurezza può essere inserito in una sezione del piano di qualità, essere un documento separato, oppure essere costituito da vari documenti che possono includere procedure o metodi di lavoro propri della società.

Obiettivo del Piano Sicurezza, indipendentemente dal tipo di progetto, è quello di:

- definire gli obiettivi di ciascuna fase del ciclo di vita e le informazioni necessarie per il loro sviluppo;
- individuare i metodi e i criteri per lo sviluppo di ciascuna fase;
- definire tutte le attività operative e i relativi tempi di attuazione e priorità in relazione al ciclo di vita in sicurezza;
- individuare i criteri di verifica della conformità dei Sistemi Strumentati di Sicurezza (SIS) alla Specificazione dei Requisiti di Sicurezza (SRS);
- individuare i criteri (procedure) per la gestione delle non conformità agli obiettivi di ciascuna fase;
- individuare le funzioni competenti per sviluppare ciascuna fase, ad esempio mediante una Matrice di Responsabilità.

Per maggiori dettagli si vedano anche gli Allegati della presente Guida.

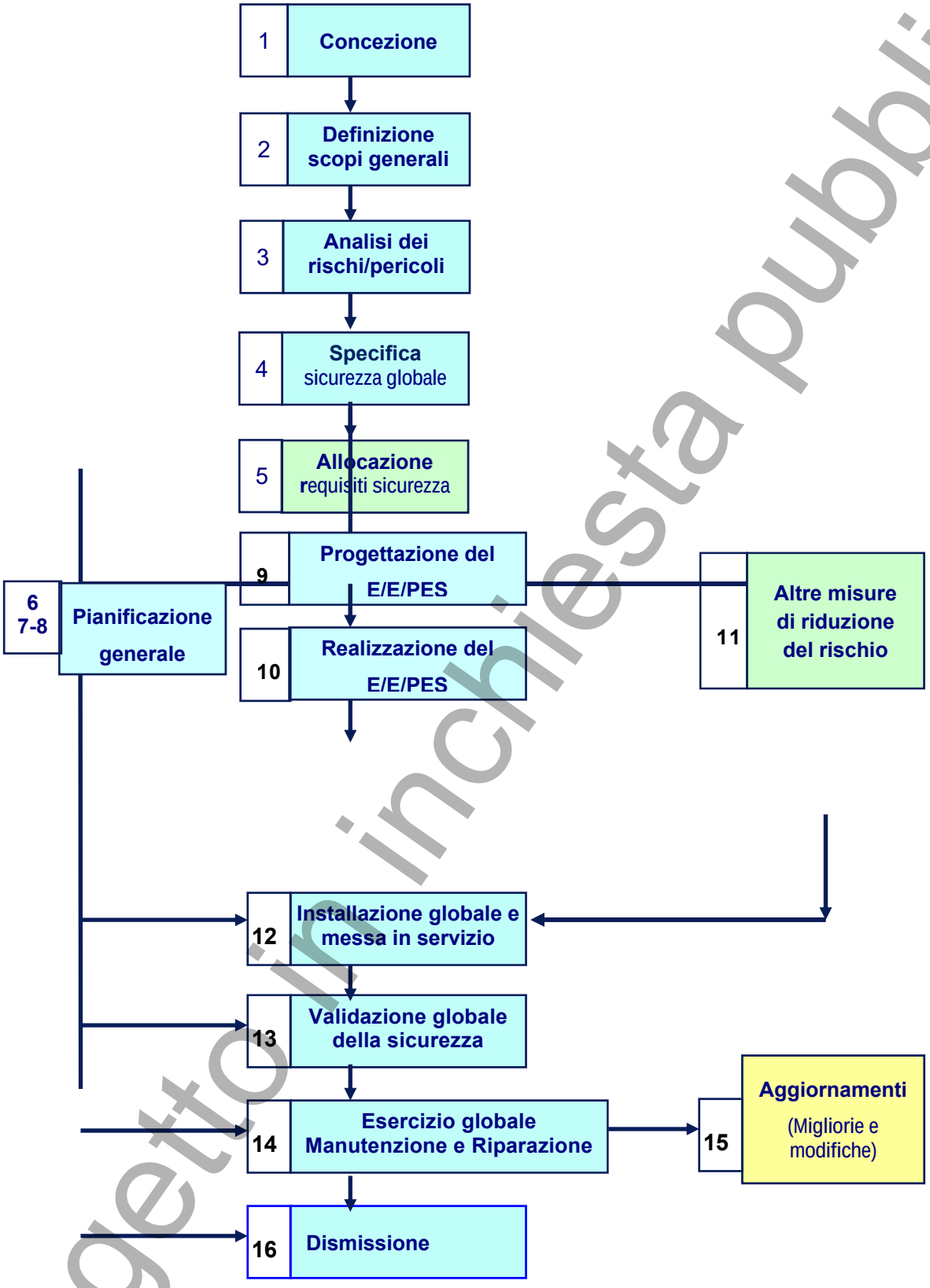


Figura 4 – Ciclo di vita in sicurezza dei sistemi E/E/PES secondo la Norma CEI EN 61508

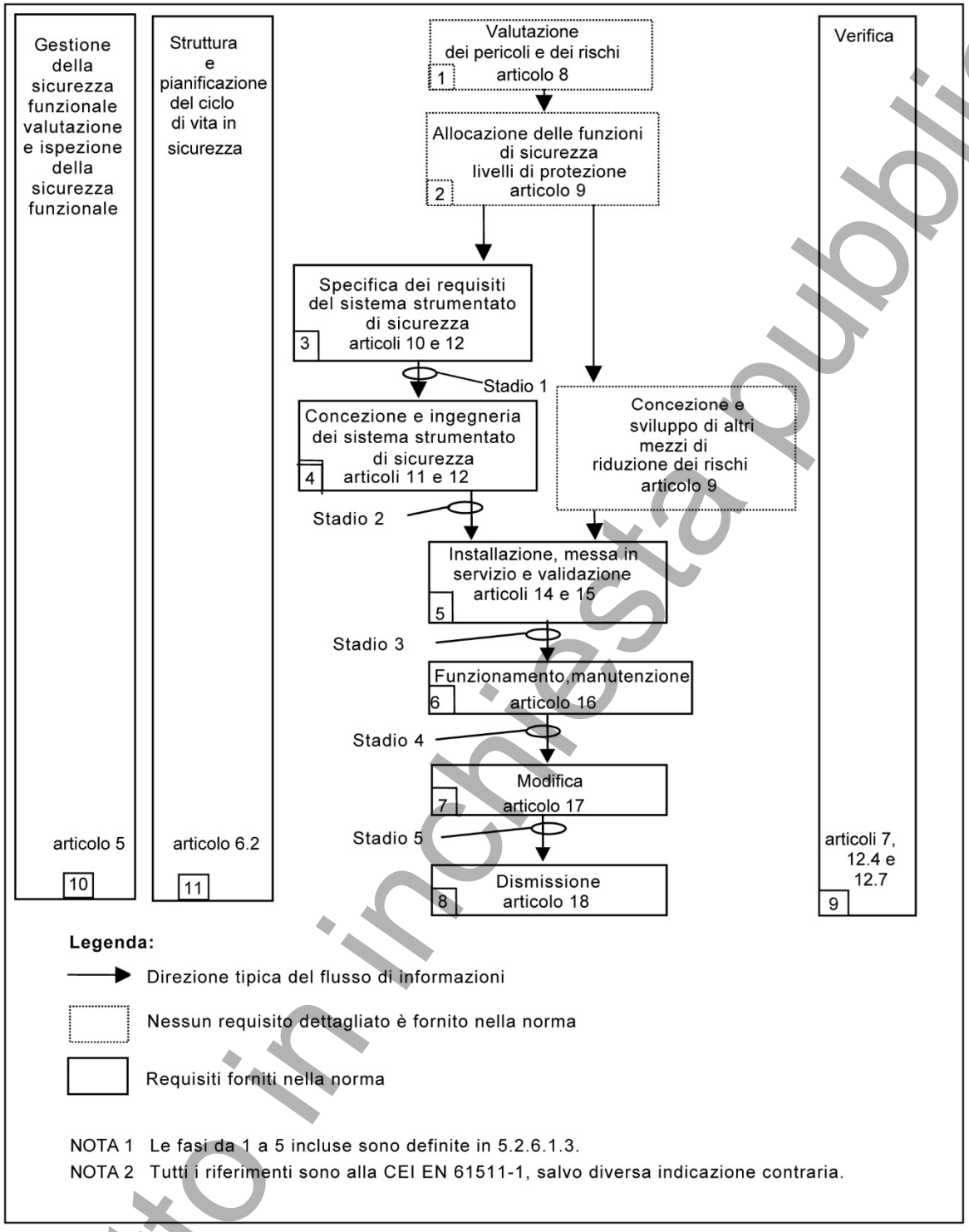


Figura 5 – Fasi del ciclo di vita in sicurezza di un SIS e stadi di valutazione della sicurezza funzionale secondo la Norma CEI EN 61511

5.2 Requisiti

Nella fase di organizzazione del Piano di Sicurezza, il Responsabile dell'attività dovrà evidenziare le politiche generali e le strategie che la Società intende applicare per assicurare, durante le attività, gli obiettivi di sicurezza e della continuità del servizio. Con riferimento al Ciclo di Vita in Sicurezza (Figura 5), il Piano di Sicurezza dipende dal tipo di progetto e dalla fase di sviluppo (pre-fattibilità, fattibilità, di base, di dettaglio, modifica).

Il Responsabile della Gestione della Sicurezza Funzionale definirà il livello di competenza e di indipendenza per le attività di Valutazione della Sicurezza Funzionale ed è responsabile di tutte le attività che competono alla analisi dei rischi e alla pianificazione della sicurezza.

La definizione dei criteri progettuali e gestionali che si possono assumere definitivi, o quasi, già nelle fasi preliminari di progetto consente di minimizzare i costi totali ed i tempi di messa in servizio dell'impianto in oggetto. I criteri sopra accennati possono essere anche di responsabilità di Società terze, qualora detentrici di licenze proprietarie. In ogni caso dovranno essere rispettati eventuali vincoli legislativi o standard aziendali ritenuti necessari dal Responsabile della Gestione della Sicurezza Funzionale.

La Tabella 3 riporta un esempio di Matrice di Responsabilità, definita dal Responsabile della Gestione della Sicurezza Funzionale, articolata nelle Competenze e nelle Funzioni coinvolte, che possono essere interne od esterne alla Società in relazione alle risorse disponibili e in funzione del livello di rischio.

5.2.1 Generalità

Il Sistema di Gestione della Sicurezza Funzionale deve assicurare che siano utilizzati sistemi strumentati di sicurezza che abbiano le capacità di mantenere il processo in uno stato sicuro.

5.2.2 Organizzazione e risorse

È necessario preliminarmente avviare una verifica interna alla Società per individuare eventuali deviazioni rispetto alle Norme inerenti la Gestione della Sicurezza Funzionale in termini di organizzazione e di risorse.

Sulla base del tipo di impianto nel Piano di Sicurezza sono individuate per ogni fase del Ciclo di Vita le risorse per lo sviluppo delle attività. La verifica della correttezza degli obiettivi per ogni fase è sotto la responsabilità del Responsabile della Sicurezza Funzionale, ma non la correttezza tecnica che è sotto la responsabilità della Funzione di Valutazione della Sicurezza Funzionale, che si avvarrà di appropriate Liste di Controllo adeguatamente predisposte per la valutazione e la verifica della disponibilità di Funzioni professionali competenti in relazione alla tipologia dell'impianto da realizzare.

5.2.3 Valutazione del rischio e gestione del rischio

La valutazione del rischio dell'impianto, condotta dalla funzione responsabile, deve essere documentata e resa disponibile.

In funzione della fase di sviluppo (progetto di nuovi impianti o modifica di impianti esistenti), il Responsabile della Gestione della Sicurezza Funzionale, avvalendosi delle competenze di esperti nei vari campi di attività, determina i livello di rischio dell'impianto sulla base di una Lista di Controllo (esemplificata nella Tabella 4).

Per la definizione del livello di rischio, devono essere coinvolte competenze adeguate alla severità del livello di integrità di sicurezza (SIL) richiesto.

Tabella 3 – Matrice di Responsabilità delle Competenze e Funzioni coinvolte per lo sviluppo delle attività del ciclo di vita in sicurezza

Fasi del Ciclo di Vita in Sicurezza	Competenze	Funzioni	Responsabilità
1) Valutazione dei pericoli e dei rischi	Specifiche conoscenze di HSE (Health, Safety & Environment) + conoscenza del processo dell'impianto oggetto dell'impianto	HSE Project Leader	Corretta e completa valutazione dei pericoli e dei rischi dell'impianto
2) Allocazione delle funzioni di sicurezza ai livelli di protezione	Specifiche conoscenze di HSE (Health, Safety & Environment) + conoscenza del processo dell'impianto oggetto dell'impianto	HSE Project Leader	Corretta allocazione delle funzioni di sicurezza ai livelli di protezione
3) Specifica dei requisiti del SIS	Specifiche conoscenze di HSE (Health, Safety & Environment) + conoscenza del processo dell'impianto oggetto dell'impianto + conoscenza di strumentazione e controllo di processo	HSE Project Leader + Instrumentation & Control Project Leader	Definizione, per ogni SIS, dei requisiti di sicurezza funzionale necessaria
4) Concezione ed ingegneria del SIS	Specifica conoscenza di ingegneria di strumentazione e controllo di processo	Instrumentation & Control Project Leader	Definizione delle specifiche di progettazione per l'acquisto dei componenti dei SIS, per la loro configurazione (dove applicabile), verifica ed installazione
5) Installazione, messa in servizio e validazione del SIS	Specifica conoscenza di strumentazione e controllo di processo, di precommissioning e commissioning di SIS	Site Instrumentation & Control Project Leader	Installazione, messa in servizio e validazione del SIS
6) Funzionamento e manutenzione del SIS	Conoscenza manutenzione di strumentazione e sistemi di controllo di processo	Resp.manutenzione strumentazione e sistemi di controllo processo/impianto	Corretta manutenzione dei SIS
7) Modifica del SIS	Specifica conoscenza di strumentazione e controllo di processo, di precommissioning e commissioning di SIS	Resp.manutenzione strumentazione e sistemi di controllo processo/impianto	Corretta esecuzione e validazione delle modifiche
8) Dismissione del SIS	Specifica conoscenza di strumentazione e controllo di processo, di precommissioning e commissioning di SIS	Resp.manutenzione strumentazione e sistemi di controllo processo/impianto	Responsabile del mantenimento dei requisiti di sicurezza necessari durante le attività di smantellamento
9) Verifica del SIS	In ogni fase devono essere effettuate le verifiche necessarie per il passaggio alla fase successiva, le competenze devono essere specifiche della fase in oggetto	Le stesse funzioni delle fasi sotto verifica oppure funzioni terze	Corretta verifica per il passaggio alla fase successiva del ciclo
10) Valutazione della sicurezza funzionale del SIS	Specifiche conoscenze di HSE + conoscenza del processo dell'impianto	HSE Project Leader	Valutazione della sicurezza funzionale del SIS realizzato

Tabella 4 – Lista di Controllo per la definizione del rischio dell'impianto

Elementi della Lista di Controllo	Competenze	Funzioni	Responsabilità
Diagrammi e dati operativi del processo	Specifiche conoscenze di processo ed idraulica del sistema	Process Project Manager e/o Technical Manager	Rispetto delle leggi fisiche e termodinamiche del processo
Planimetrie di impianto	Requisiti di sicurezza per la predisposizione delle apparecchiature (incendio, mantenibilità, ecc.)	Technical Manager	Rispetto della corretta disposizione delle attrezzature per la protezione passiva antincendio
Identificazione dei pericoli e problematiche operative	Specifiche conoscenze del processo in esame dal punto di vista operativo ed di ingegneria e tecniche di identificazione dei pericoli	Technical Manager e/o HSE Manager	Corretta identificazione dei pericoli collegati all'utilizzo ed all'ingegneria dell'impianto
Identificazione degli eventi a rischio e determinazione frequenze	Specifiche conoscenze HSE (Health, Safety & Environment) e conoscenza dell'impianto	HSE Manager	Identificazione degli eventi a rischio correlati alla vita operativa dell'impianto
Analisi delle conseguenze	Specifiche conoscenze HSE e dell'area in cui è inserito l'impianto	HSE Manager	Identificazione delle conseguenze degli eventi a rischio sulle persone, le proprietà e l'ambiente
Calcolo del rischio per gli eventi identificati	Specifiche conoscenze HSE	HSE Manager	Calcolo matematico dell'indice di rischio per ogni evento identificato e verifica dell'accettabilità secondo criteri di legge o contrattuali.

5.2.4 Pianificazione della sicurezza

L'attività di pianificazione della sicurezza rientra nelle mansioni del Responsabile della Gestione della Sicurezza Funzionale e deve essere coerente nello sviluppo dell'impianto sulla base delle risultanze delle attività relative all'analisi dei rischi e alla conseguente allocazione dei sistemi di sicurezza.

I sistemi di sicurezza possono essere passivi, attivi e strumentati in uno schema di Barriere di Protezione Indipendenti (Independent Protection Layers - IPL). La possibilità di valutare alternative di IPL è condotta dal Responsabile della Valutazione della Sicurezza Funzionale in accordo con il Responsabile della Gestione della Sicurezza Funzionale. Questa analisi dovrà essere condotta già nelle prime fasi del progetto ed in funzione del tipo di progetto, e si dovrebbero privilegiare preliminarmente le possibili soluzioni per un progetto "intrinsecamente sicuro" dal punto di vista del processo.

Sulla base delle risultanze della analisi condotta e tenuto conto dei criteri di accettabilità del rischio specificati in ambito societario e/o eventualmente dalla Pubblica Amministrazione, vengono definiti i criteri di sicurezza e le opportune IPL. La decisione sulle eventuali alternative dei criteri di sicurezza è demandata al Responsabile della Sicurezza Funzionale, su approvazione di intervento sullo sviluppo dl progetto del Responsabile della Gestione della Sicurezza Funzionale.

Per maggiori dettagli sui criteri di progettazione dei sistemi di sicurezza si veda l'Allegato B.

5.2.5 Implementazione e monitoraggio

L'implementazione dei sistemi di sicurezza è sviluppata nella fase 2 del ciclo di vita in sicurezza (vedere Figura 5).

Lo sviluppo delle attività richiede la preliminare specificazione dei Livelli di Integrità di Sicurezza (SIL) dei Sistemi Strumentati di Sicurezza (SIS) a fronte del livello di rischio accettabile. Questa specificazione è condotta a valle dell'analisi di rischio.

È importante che a valle dello studio di sicurezza sia prevista una fase di revisione delle risultanze da parte del Responsabile della Valutazione della Sicurezza Funzionale. Dovrà essere disponibile un Rapporto, condiviso con il Responsabile della Gestione della Sicurezza Funzionale, in cui potranno essere proposte modifiche per una revisione dell'analisi del rischio in funzione della scelta fra alternative di base o di dettaglio (tipologia e numero delle IPL).

La specificazione del Livello di Integrità di Sicurezza (SIL) e delle Funzioni Strumentate di Sicurezza (SIF) richiede che siano quantificate le stime degli Eventi Pericolosi Principali (Top Events) individuati. In tal modo è possibile specificare il livello di riduzione del rischio a fronte dell'accadimento degli Eventi Pericolosi Principali. Quanto sopra vale qualora non si adottino soluzioni di protezione (controllo) standard, per determinati EUC (compressori, turbine, sistemi di intercettazione per determinati livelli di sicurezza specifica, ecc.).

5.2.6 Valutazione, audit e revisione

L'attività di valutazione dei sistemi di sicurezza è di responsabilità del Responsabile della Funzione di Gestione della Sicurezza Funzionale e deve essere condotta per ciascuna fase evidenziata in Figura 5. Ad essa è demandata anche la verifica che tutte le fasi di sviluppo del progetto dei sistemi di sicurezza siano state condotte e tutte le revisioni richieste siano state attuate fino alla fase di esercizio, mediante appropriate Liste di Controllo.

5.2.7 Gestione e configurazione del SIS

L'attività prevede che sia stato redatto un Manuale di Sicurezza ove siano indicate le modalità di gestione dei sistemi di sicurezza, i criteri di verifica periodica (frequenza e modalità di esecuzione) e la gestione dei guasti per garantire nel contempo la sicurezza al livello previsto. Si rimarca la necessità di stesura di procedure per i criteri di messa in servizio dei Sistemi Strumentati di Sicurezza (SIS).

A titolo informativo vengono nel seguito presentate le attività di tipo tecnico e procedurale da seguire nel caso che debbano essere elaborate opportune procedure aziendali mancanti.

Le attività fondamentali che devono essere condotte durante il ciclo di vita in sicurezza sono di seguito riportate nelle linee generali. Parte delle attività sono di stretta competenza del Gestore (Utente Finale) dei SIS, altre possono essere demandate a Terzi per lo sviluppo di fasi del ciclo di vita fino al Progetto e/o messa in servizio. In particolare:

a) l'informazione a tutte le Funzioni interessate all'Attività (Progetto e Gestione) delle politiche e le strategie per assicurare gli obiettivi della sicurezza ed affidabilità unitamente ai criteri e modalità per il loro raggiungimento. Questa attività richiede l'attuazione di uno schema di comunicazione delle informazioni necessario affinché tutti coloro che sono coinvolti nell'attività abbiamo sviluppato una cultura ed una chiara percezione operativa degli aspetti di sicurezza e dell'affidabilità;
b) la predisposizione di uno schema del flusso informativo e le procedure specifiche per attivarlo;
c) l'individuazione delle Funzioni (interne e/o esterne all'Azienda) alle quali è demandata la responsabilità di sviluppo e di revisione dei sistemi di sicurezza (hardware e software) per tutte le fasi del ciclo di vita in sicurezza(1);
d) la predisposizione di criteri/procedure per assicurare che tutte le parti coinvolte nelle attività del ciclo di vita siano competenti professionalmente;

(1) Incluse tutte le attività ai fini autorizzativi

e) l'addestramento del personale demandato alla ricerca, diagnosi e riparazione dei guasti;

f) l'addestramento del personale di esercizio con particolare riferimento ai sistemi di sicurezza in funzione dei livelli di integrità di sicurezza (SIL) dei sistemi strumentati di sicurezza (SIS) installati;

g) la definizione dello schema di formazione per l'aggiornamento tecnico periodico del personale di manutenzione dei sistemi di sicurezza;

h) l'informazione a tutti coloro che sono stati autorizzati alla Funzione di Responsabilità della Gestione delle attività previste (Responsabile della Gestione della Sicurezza Funzionale) del livello di responsabilità che vi compete;

i) la definizione delle procedure per analizzare le prestazioni del processo e l'efficacia della manutenzione, in particolare, per:

   – riconoscere guasti sistematici che possano inficiare la sicurezza funzionale dei SrS/SIS, incluse le procedure utilizzate durante le attività di manutenzione di routine che consentono la individuazione di guasti ripetitivi,

   – verificare se le frequenze delle richieste di intervento dei sistemi di sicurezza o la frequenza dei guasti che si verificano siano coerenti con le stime condotte in fase di progetto dei sistemi di sicurezza;

j) la predisposizione dello schema delle ispezioni (audit) che sono previste per verificare i requisiti della sicurezza funzionale dei sistemi di sicurezza; in particolare:

   – la frequenza delle ispezioni,

   – i criteri sul livello di indipendenza delle Funzioni che conducono le ispezioni,

   – la documentazione che deve essere verificata nelle ispezioni;

k) la definizione delle procedure previste per attuare modifiche ai sistemi di sicurezza;

l) la definizione delle procedure per le approvazioni e la individuazione della Funzione autorizzata a condurre la modifica/dismissione dei SIS;

m) la definizione delle procedure che devono essere attuate affinché un sistema di sicurezza non sia messo in servizio prima delle opportune autorizzazioni;

n) la definizione delle procedure che devono essere definite in caso che i SIS non siano efficienti alla verifica periodica (o per guasti rilevati);

o) la predisposizione dei programmi di formazione ed esercitazione per le emergenze previste nel progetto dell'Attività (Manuale di Gestione della Sicurezza);

p) in relazione al progetto dei SIS si dovranno prevedere:

   – le attività relative alla valutazione della Sicurezza Funzionale:

      i la specificazione delle tecniche e dei criteri da utilizzare per lo sviluppo del progetto dei sistemi di sicurezza con specifico riferimento alle clausole delle Norme,

      ii l'analisi dei rischio,

      iii l'individuazione di tutte le fasi del ciclo di vita in cui siano prese in considerazione i sistemi di sicurezza per gli aspetti hardware e software,

      iv la definizione delle procedure per la gestione della configurazione dei sistemi di sicurezza durante tutto lo sviluppo del ciclo di vita in sicurezza,

      v l'individuazione della fase alla quale deve essere implementato formalmente il sistema di controllo;

- le attività di gestione della Sicurezza Funzionale:
  - i la pianificazione e la verifica di tutte le fasi del Piano di Sicurezza (SP),
  - ii le procedure per assicurare che siano stati analizzati i rischi nelle previste fasi del ciclo di vita e che siano state adottate ed attuate le raccomandazioni emerse dalle suaccennate analisi sulla base delle valutazione del Responsabile della Sicurezza Funzionale (FSA) per ridurre la probabilità di accadimento di eventi pericolosi,
  - iii le procedure per la gestione delle informazioni di controllo relative a situazioni pericolose individuate nella fase di analisi del rischio,
  - iv le procedure e le tecniche specifiche da adottare dalle Funzioni competenti per assicurare l'attuazione e la validazione dei SIS in conformità ai requisiti progettuali ed operativi in tutte le diverse fasi del Piani di Sicurezza.

6 Requisiti del ciclo di vita in sicurezza

6.1 Obiettivi

Gli obiettivi di questo articolo sono quelli di definire e organizzare tutte le attività del ciclo di vita in sicurezza dell'impianto.

6.2 Requisiti

Lo schema del Ciclo di Vita in Sicurezza prevede che siano condotte le attività di sviluppo dei sistemi di sicurezza dalla fase di "concezione" a quella di "dismissione". Tali fasi dipendono dal tipo di impianto e dalla tipologia delle attività che devono essere condotte (pre-fattibilità. fattibilità, modifica, progetto base o di dettaglio).

Per ogni fase devono essere individuate le funzioni tecniche ed organizzative responsabili e le informazioni necessarie per lo sviluppo dell'attività; i risultati delle attività condotte e gli eventuali commenti per ottenere la conformità agli obiettivi sono verificati dal Responsabile della "Gestione della Sicurezza Funzionale" e validati dal Responsabile della "Valutazione della Sicurezza Funzionale".

La Tabella 5, derivata dalla CEI EN 61511-1, fornisce una vista di insieme generale delle attività da svolgere nel ciclo di vita in sicurezza di un SIS, riportando per ogni fase di sviluppo:

- gli obiettivi della fase del ciclo di vita;
- l'articolo di riferimento normativo;
- gli ingressi specifici della fase;
- le uscite richieste della fase.

Tabella 5 – Vista d'insieme semplificata del ciclo di vita della sicurezza di un SIS (vedasi Tabella 2 della CEI EN 61511-1 per ulteriori dettagli)

Fase o attività del ciclo di vita della sicurezza		Obiettivi	Articolo dei requisiti della CEI EN 61511-1	Ingressi	Uscite
Numero fase nella Figura 5	Titolo				
1	Valutazione del pericolo e del rischio	Determinare i pericoli e gli eventi pericolosi processo e apparecchiature associate, ed i requisiti relativi alla riduzione del rischio e le richieste funzioni di sicurezza	8	Concezione del processo, configurazione, squadre di persone, obiettivi di sicurezza	Descrizione dei pericoli, della(e) funzione(i) di sicurezza richiesta(e) e della riduzione del rischio necessaria
2	Allocazione delle funzioni di sicurezza ai livelli di protezione	Allocazione delle funzioni di sicurezza ai livelli di protezione e per ogni funzione strumentata di sicurezza, l'associato SIL	9	Descrizione della(e) funzione(i) di sicurezza richiesta(e) e dei requisiti di SIL	Descrizione dell'allocazione dei requisiti di sicurezza
3	Specificazione dei requisiti di sicurezza del SIS	Specificare i requisiti per ogni SIS, in termini di funzioni strumentate di sicurezza richieste per ottenere la sicurezza funzionale richiesta	10	Descrizione dell'allocazione dei requisiti di sicurezza	Requisiti di sicurezza del SIS; requisiti di sicurezza del software
4	Concezione ed ingegneria del SIS	Concepire il SIS per soddisfare i requisiti delle funzioni strumentate di sicurezza e di integrità di sicurezza	11 e 12.4	Requisiti di sicurezza del SIS e del software	Concezione del SIS e pianificazione dell'integrazione del SIS
5	Installazione, messa in servizio e validazione del SIS	Integrare e provare il SIS Validare che il SIS soddisfi i tutti i punti i requisiti di sicurezza, in termini di funzioni strumentate di sicurezza e di integrità di sicurezza richiesta	12.3, 14, 15	Concezione del SIS e pianificazione dell'integrazione del SIS Requisiti di sicurezza del SIS e pianificazione della validazione del SIS	SIS in conformità con le prove di integrazione del SIS Risultati attività di installazione, di messa in servizio e di validazione
6	Funzionamento e manutenzione del SIS	Assicurare che la sicurezza funzionale del SIS è conservata durante il funzionamento e la manutenzione	16	Requisiti e concezione del SIS Pianificazione del funzionamento e manutenzione SIS	Risultati delle attività di funzionamento e di manutenzione
7	Modifica del SIS	Correggere, adattare o migliorare il SIS, affinché il livello di integrità di sicurezza richiesto sia ottenuto e mantenuto	17	Requisiti di sicurezza del SIS revisionati	Risultati della modificazione del SIS
8	Dismissione	Assicurare un appropriato riesame da una organizzazione del settore ed assicurare che il SIF rimanga appropriato	18	Requisiti di sicurezza e informazioni di processo conformi alla costruzione	SIF dichiarato fuori servizio
9	Verifica del SIS	Provare e valutare le uscite delle diverse fasi del SIS, per assicurare la coerenza nei confronti degli ingressi e delle uscite richieste	7, 12.7	Piano per la verifica del SIS, per ogni fase	Risultati della verifica del SIS, per ogni fase
10	Valutazione della sicurezza funzionale del SIS	Investigare ed arrivare ad un giudizio sulla sicurezza funzionale ottenuta dal SIS	5	Pianificazione della valutazione del SIS Requisiti della sicurezza del SIS	Risultati della valutazione della sicurezza funzionale del SIS

7 Modalità di verifica

7.1 Obiettivi

Il Responsabile della Gestione della Sicurezza Funzionale dovrà verificare, secondo opportuni moduli (da sviluppare o in accordo alle specifiche di Controllo di Qualità, se esistenti), che siano ottenuti gli obiettivi previsti in ogni fase del ciclo di vita in sicurezza con criteri e modalità opportune (da specificare) ed inoltre dovrà curare la gestione delle non conformità (da specificare).

7.1.1 Requisiti

Le attività di verifica di ogni fase devono essere condotte sulla base del livello di sicurezza dell'impianto.

7.1.1.1 Verifica

Nel Piano di Sicurezza devono essere indicati i punti chiave di verifica da parte delle Funzioni Responsabili Tecniche e Gestionali, almeno nelle principali fasi seguenti del ciclo di vita in sicurezza del SIS (vedasi anche per una vista di insieme la Figura 5):

a) nella specificazione dei requisiti del SIS;

b) nella progettazione ed ingegnerizzazione del SIS;

c) nella selezione e implementazione del software del SIS;

d) nella istallazione e messa in servizio del SIS;

e) nella modificazione del SIS;

f) nella dismissione del SIS.

7.1.1.2 Risultati della verifica

La verifica del raggiungimento dei risultati deve essere condotta fase per fase secondo quanto indicato in 7.1.1.1 precedente; il raggiungimento, opportunamente documentato, dei risultati previsti per ogni fase consente il passaggio alla fase successiva in accordo al Piano di Sicurezza.

8 Analisi dei pericoli potenziali e dei rischi del processo

8.1 Obiettivi

L'analisi dei pericoli potenziali e dei rischi del processo costituisce la base dello sviluppo dei sistemi relativi alla sicurezza e, in particolare, dei Sistemi Strumentati di Sicurezza (SIS).

L'analisi può essere condotta in modo qualitativo e/o quantitativo in funzione del livello di dettaglio della documentazione e quindi della fase del ciclo di vita in sicurezza.

L'analisi comporta i seguenti passi:

a) identificazione degli eventi pericolosi principali (Top Events);

b) identificazione delle cause principali che concorrono o li determinano (sequenze degli eventi incidentali) nelle diverse fasi del processo (stazionarie, transitorie);

c) identificazione delle funzioni di sicurezza richieste per ottenere la necessaria riduzione dei rischi e dei pericoli;

d) definizione delle barriere di protezione indipendenti (IPL) che sono previste compresi i sistemi strumentati di sicurezza (SIS);

e) definizione dei criteri di allocazione delle funzioni di sicurezza alle barriere di protezione e dei relativi livelli di integrità di sicurezza (SIL).

Queste attività sono condotte da gruppi di lavoro multidisciplinari che dispongono della necessaria competenza nell'analisi dei rischi.

La valutazione, e quindi il livello di competenza professionale, dipende dal tipo di impianto e dal livello di rischio individuato, sia nel caso di realizzazione di nuovi impianti che nel caso di modifica di impianti esistenti.

8.2 Requisiti

La valutazione del rischio viene normalmente eseguita in due fasi successive: una analisi preliminare (Preliminary Risk Assessment - PRA) più o meno approfondita a seconda del tipo di attività (studio di fattibilità o progetto di dettaglio) e una analisi successiva più operativa.

Per l'analisi del rischio vedasi anche direttamente la CEI EN 61511-3.

8.2.1 Valutazione dei rischi e dei pericoli

L'analisi preliminare (PRA) permette di individuare i seguenti elementi:

– Elenco degli Eventi Pericolosi Principali (Top Events),

– Elenco delle apparecchiature interessate dagli Eventi Pericolosi Principali,

– Conseguenze degli Eventi Pericolosi Principali,

– Elenco delle "sequenze incidentali" che conducono agli Eventi Pericolosi Principali (la sequenza incidentale consente di individuare anche le IPL),

– Livelli di protezione a fronte degli Eventi Pericolosi Principali.

Per quanto riguarda invece la successiva analisi operativa, la norma di riferimento non descrive in dettaglio le metodologie specifiche, essa però fa riferimento ai metodi comunemente utilizzati fornendo indicazioni per la loro applicazione.

Le tecniche e metodologie che possono essere utilizzate sono quelle normalmente applicate e consolidate negli studi di sicurezza degli impianti di processo:

– HAZOP

– FMEA

– MARKOV (quantitativo)

– Albero dei Guasti (qualitativo e quantitativo)

– Analisi ad Albero dei Guasti (qualitativo e quantitativo)

In particolare, negli studi di sicurezza è usuale utilizzare l'HAZOP (Hazard and Operability Study) per l'individuazione degli eventi pericolosi e l'Albero dei Guasti (Fault Tree) qualitativo per la integrazione delle informazioni ricavate dall'HAZOP e per la quantificazione delle frequenze attese degli eventi pericolosi individuati.

La valutazione quantitativa del rischio richiede oltre al livello di probabilità di accadimento anche la valutazione della gravità dalle sue conseguenze utilizzando per esempio la FMEA (Failure Mode and Effect Analysis).

A valle dell'analisi del rischio devono essere svolte le seguenti principali attività.

Determinazione della riduzione del rischio necessaria

Una prima azione da condurre è quella di ridurre il più possibile i rischi intrinseci al processo nel rispetto degli eventuali vincoli progettuali o di Licenza.

Viene quindi calcolato il fattore di riduzione del rischio come il rapporto tra il rischio determinato dall'analisi del rischio dell'impianto così ottimizzato e il rischio tollerabile (o accettabile).

Il proprietario dell'impianto definisce le soglie di accettabilità del rischio in conformità alle regolamentazioni di legge.

Scelta delle barriere di protezione

La riduzione del livello di rischio deve essere realizzata con Barriere di Protezione Indipendenti (IPL) non strumentate e, se necessario, mediante Funzioni Strumentate di Sicurezza (SIF) realizzate da Sistemi Strumentati di Sicurezza (SIS), aventi un Livello di Integrità di Sicurezza (SIL) adeguato.

Determinazione del livello di Integrità di sicurezza (SIL)

La valutazione del SIL dei SIS è individuata sulla base di riferimenti progettuali (Piping & Instrumentation Diagram: P&ID o P&I – Diagrammi Causa - Effetto) e di specifiche.

La valutazione del SIL (o del Fattore di Riduzione del Rischio - RRF) può essere basata su dati di EUC tipici (o loop tipici: portate, livelli, ecc.) a cui è possibile attribuire a priori un SIL. In caso di EUC non tipici, deve essere condotta una analisi specifica sulla base degli eventi pericolosi individuati allo scopo di ridurre il rischio nella regione tollerabile con IPL e/o SIS.

Allocazione dei SIS

L'allocazione dei SIS è un'attività che deve essere avviata fin dalla prima fase dell'analisi del rischio in funzione della tipologia dell'impianto.

In funzione del grado di sviluppo del progetto (pre-fattibilità, fattibilità, progetto di base, di dettaglio) e della disponibilità di documentazione, possono essere utilizzati diversi metodi di analisi di tipo qualitativo-quantitativo. Una metodologia base per la individuazione delle Funzioni di Sicurezza (non solo strumentate) è il LOPA (Layer Of Protection Analysis).

L'applicazione della metodologia LOPA si basa sui risultati dell'HAZOP, tenendo conto dei pericoli individuati e della documentazione relativa all'impianto (schemi P&I), e dei seguenti aspetti:

- Sicurezza intrinseca;
- Utilizzazione di sistemi passivi e/o attivi;
- Efficacia delle barriere di protezione (almeno 10^{-1});
- Tolleranza al guasto;
- Indipendenza dei sistemi;
- Riduzione dei costi di gestione;
- Individuazione delle SIF.

In generale, le metodologie per la valutazione del SIL di una SIF sono basate su metodi per l'analisi di affidabilità degli impianti, come riportato nella CEI EN 61511-3 e nella CEI EN 61508-5.

Nelle reali applicazioni sono individuabili metodi generali precisi e consolidati: in particolare, la Tecnica dell'Albero dei Guasti consente di sviluppare criteri per sistemi di controllo e di protezione che hanno componenti comuni. Nel caso invece di sistemi di protezione indipendenti, oltre alla tecnica dell'Albero dei Guasti, sono utilizzabili tecniche basate su modelli di Markov (CEI EN 61508-6).

In pratica però, già a partire dall'analisi HAZOP è possibile applicare la consolidata metodologia LOPA per individuare i SIL delle SIF.

È importante, inoltre, evidenziare che la determinazione dei SIL quantificata pone l'attenzione sulla precisione delle stime, sia prendendo in considerazione le Tabelle 2 e 3 della CEI EN 61508-2 sia la Tabella 6 della CEI EN 61511-1. È evidente, infatti, che la stima numerica è fondamentale per la tolleranza minima alle anomalie HFT (Hardware Fault Tolerance).

In particolare, si deve notare (con riferimento alla CEI EN 61508-2):

– la classica strada Route $_{1H}$ che prevede la determinazione dell'HFT di componenti semplici nella Tabella 2 e degli altri componenti nella Tabella 3;

– la nuova strada Route $_{2H}$ che considera invece componenti già provati anteriormente (prior use e proven use) che prevede la determinazione dell'HFT secondo il paragrafo 7.4.4.3.1 purché rispondenti ai requisiti riportati al paragrafo 7.4.4.3.3 (strada di selezione prevista nella Tabella 6 della nuova Edizione 2 della CEI EN 61511-1).

Modelli di calcolo certificati (benchmark)

In assenza di dati certificati o prior use, si può fare riferimento in modo cautelativo a dati relativi ai tassi tipici di guasto di vari tipi di apparecchiature disponibili nella letteratura tecnica, come quelli riportati nella Tabella 6.

Tabella 6 – Dati tipici di tassi di guasti per i principali componenti per l'industria di processo

Componente	Tasso tipico guasto per ora
Analizzatore	5.0×10^{-6}
Analizzatore IR	7.0×10^{-5}
Analizzatore UV	1.0×10^{-6}
Compressore	3.0×10^{-6}
Contattore	5.5×10^{-7}
Contatto elettrico	1.1×10^{-8}
Controllore logico programmabile industriale (PLC)	5.0×10^{-6}
Controllore logico programmabile di sicurezza (PES)	1.0×10^{-6}
Disco rottura (con sovrappressione)	1.0×10^{-6}
Disco rottura (in ingresso - senza sovrappressione)	1.0×10^{-5}
Disco rottura (in uscita - senza sovrappressione)	5.0×10^{-6}
Errore umano (operatore, secondo CEI EN 61511-3)	1.0×10^{-1}
Fine corsa	3.6×10^{-6}
Estintore	7.2×10^{-6}
Livellostato	3.6×10^{-6}
Motore bassa tensione	1.0×10^{-6}
Pompa petrolchimica	3.0×10^{-5}
Pressostato	3.6×10^{-6}
Pulsante di emergenza	2.0×10^{-7}

(continua)

Componente	Tasso tipico guasto per ora
Relè	5.0×10^{-8}
Sensore di calore	5.0×10^{-7}
Sensore di fiamma	1.6×10^{-6}
Sensore di fumo	8.0×10^{-7}
Sensore di gas catalitico	1.8×10^{-6}
Sistema cablato di sicurezza (logica a relè)	1.0×10^{-7}
Soglia di intervento A/D	5.0×10^{-8}
Soglia di Intervento IR/UV	2.0×10^{-6}
Solenoide	9.0×10^{-7}
Termocoppia	1.0×10^{-6}
Trasduttore I/P (corrente/pressione)	2.9×10^{-6}
Trasmettitore di livello (ΔP)	5.0×10^{-7}
Trasmettitore di pressione (P)	4.0×10^{-7}
Trasmettitore di temperatura (T)	1.0×10^{-7}
Trasmettitore combinato (P,T)	2.0×10^{-7}
Trasmettitore elettronico (Smart)	5.0×10^{-7}
Valvola di antincendio	5.0×10^{-6}
Valvola di blocco (SV)	1.0×10^{-6}
Valvola di controllo (CV)	1.0×10^{-6}
Valvola di direzione (DCV)	1.0×10^{-7}
Valvola di isolamento singola (CIV)	4.0×10^{-7}
Valvola di isolamento tripla (PMV)	1.0×10^{-7}
Valvola di isolamento sottomarina (SSIV)	1.0×10^{-7}
Valvola di scarico (BDV)	2.0×10^{-6}
Valvola master	8.0×10^{-7}
Valvola wing	8.0×10^{-7}

(fine tabella)

8.2.2 Valutazione dei guasti pericolosi del BPCS

Se il sistema di controllo di processo base BPCS non è conforme alla CEI EN 61511-1, il suo tasso di guasto su domanda deve cautelativamente essere considerato superiore a 10^{-1} (≥0,1).

8.2.3 Valutazione e registrazione dei rischi e dei pericoli

La valutazione e la registrazione dei rischi e dei pericoli dovrebbe essere condotta assegnando degli opportuni valori numerici. Nel caso di utilizzazione di approcci grafici vedere invece la CEI EN 61511-3.

9 Allocazione delle funzioni di sicurezza alle barriere di protezione

9.1 Obiettivi

L'allocazione delle funzioni di sicurezza alle barriere di protezione prevede essenzialmente di:

- determinare le Funzioni Strumentate di Sicurezza (SIF) richieste;
- determinare, per ogni SIF il Livello di Integrità di Sicurezza (SIL) richiesto.

9.2 Requisiti relativi al processo di allocazione

9.2.1 Allocazione delle funzioni strumentate di sicurezza (SIF)

Per ogni funzione di sicurezza, una volta stabilito che deve essere un Funzione Strumentata di Sicurezza (SIF), si deve stabilire il suo modo di funzionamento, Continuo o su Domanda: Vedasi Figura 6.

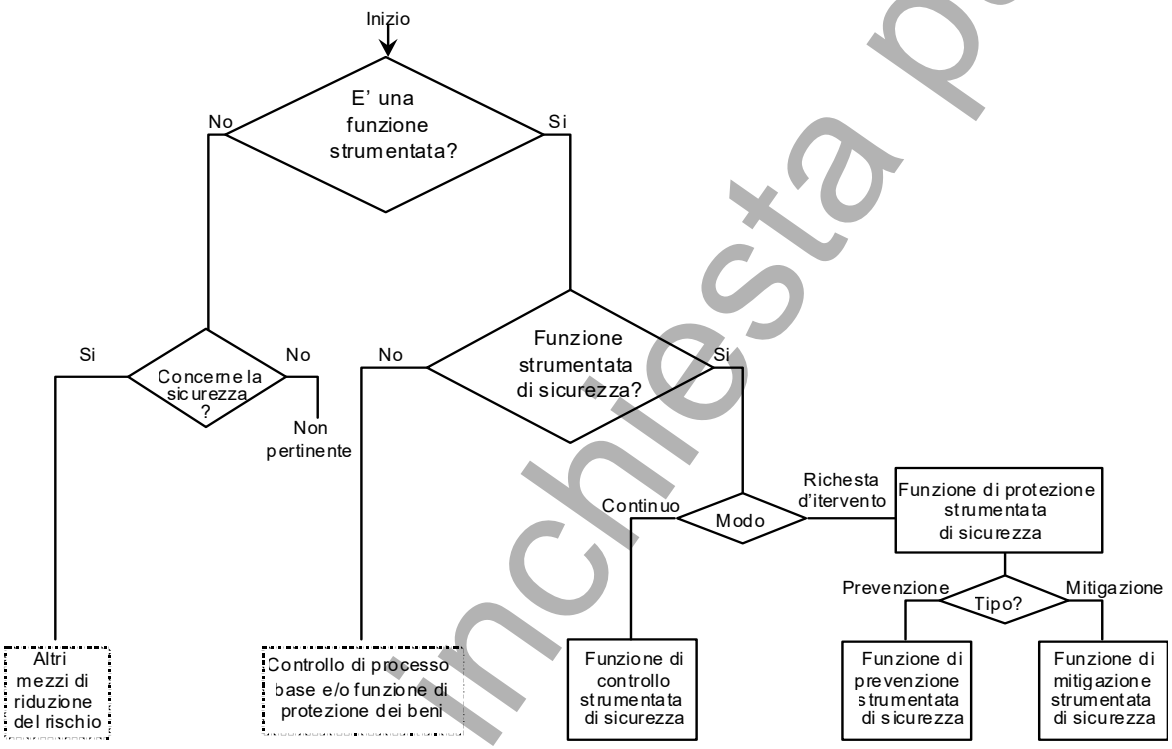


Figura 6 – Relazioni tra le funzioni strumentate di sicurezza e le altre funzioni

9.2.2 Determinazione del Livello di integrità di sicurezza (SIL)

Il Livello di Integrità di Sicurezza (SIL) deve essere determinato per ogni SIF in relazione alla riduzione del rischio richiesta:

Vedasi in generale la CEI EN 61511-3 ed in particolare gli Allegati A e H.

9.2.3 Metodologia di individuazione del SIL

Il SIL deve essere individuato con le Tabelle 2 e 3 della CEI EN 61511-1 a seconda del tipo di funzionamento su domanda o continuo della funzione strumentata di sicurezza.

9.2.4 Tabelle di individuazione del SIL

Per la individuazione del SIL delle SIF vedasi rispettivamente Tabella 4 e 5 della CEI EN 61511-1 qui riportate nel riquadro per comodità di lettura in Tabella 7.

Tabella 7 – Individuazione dei Livelli di Integrità di Sicurezza (SIL) delle Funzioni Strumentate di Sicurezza (SIF) a seconda del loro modo di funzionamento "su domanda" o "continuo"

Tabella 4 – CEI EN 61511-1
Livelli di integrità di sicurezza: probabilità di guasto su domanda della SIF

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

Tabella 5 – CEI EN 61511-1
Livelli di integrità di sicurezza: frequenza di guasti pericolosi della SIF

FUNZIONAMENTO IN MODO CONTINO	
Livello di integrità di sicurezza (SIL)	**Obiettivo della frequenza di guasti pericolosi (guasti per ora)**
4	da $\geq 10^{-9}$ a $<10^{-8}$
3	da $\geq 10^{-8}$ a $<10^{-7}$
2	da $\geq 10^{-7}$ a $<10^{-6}$
1	da $\geq 10^{-6}$ a $<10^{-5}$

Inoltre, a titolo di guida, si riporta nel seguito la Tabella 8 per una indicazione di massima dei minimi SIL che si dovrebbero riscontrare in tipiche applicazioni negli impianti off-shore.

NOTA Nei casi in cui sia richiesto un SIL maggiore di 4 occorre procedere ad un riesame dell'applicazione (ad esempio, del processo e degli altri livelli di protezione) per determinare se qualche rischio possa essere ridotto in modo tale da condurre ad un'applicazione con un SIL massimo di 4.

Il riesame deve valutare se:

- il processo o apparecchiature possono essere modificati per eliminare o ridurre alla fonte i rischi;
- possono essere introdotti ulteriori mezzi di riduzione del rischio, non basati sulla strumentazione;
- la gravità della conseguenza può essere ridotta, riducendo la quantità dei materiali presenti.

Se dopo l'ulteriore riesame è ancora richiesto un SIL maggiore di 4, occorrerà prendere in considerazione, per raggiungere il richiesto requisito di integrità di sicurezza, l'utilizzazione di una serie di strati di protezione attivi (SIS o BPCS) che riducano il livello di rischio nella zona accettabile.

IMPORTANTE:

La valutazione dei rischi PRA (Preliminary Risk Analysis) e la determinazione del SIL (Safety Instrumented System) dovrebbero essere condotte e verificate da personale competente.

Vedasi Tabella 4 e 5 della norma CEI EN 61508-1 qui riportate a compendio nella Tabella 7 bis, che prevedono i livelli minimi di indipendenza del personale incaricato alla valutazione sicurezza funzionale durante le varie fasi del ciclo di vita di sicurezza riportate nella Figura 4.

Il livello minimo di indipendenza di coloro che svolgono la valutazione della sicurezza funzionale, è riportato nelle predette tabelle che devono essere interpretate come segue:

- ✓ X: il livello di indipendenza specificato è il minimo per la conseguenza specificata o il livello di integrità di sicurezza richiesto;
- ✓ X1 e X2: vedasi Nota;
- ✓ Y: il livello di indipendenza specificato è considerato insufficiente.

NOTA Nel contesto delle tabelle riportate nella Tabella 7 bis le caselle marcate X, X1, X2 e Y devono essere utilizzate come base per determinare il livello di indipendenza:

Per le caselle marcate X1 e X2, X1 o X2 sono applicabili (non entrambi), a seconda di una serie di fattori specifici per l'applicazione;

In particolare i fattori che renderanno più appropriato X2 di X1 sono:

- **La mancanza di esperienza precedente con un design simile;**
- **Maggior grado di complessità;**
- **Maggior grado di novità del design;**
- **Maggior grado di novità della tecnologia.**

Tabella 7 bis - Livelli minimi di indipendenza del personale incaricato alla valutazione della sicurezza funzionale

Tabella 4 – CEI EN 61508-1
Livelli minimi di indipendenza per le fasi da 1 a 8 e da 12 a 16 della Figura 4

Minimo livello di indipendenza	Conseguenza (1)			
	A	B	C	D
Persona indipendente	X	X1	Y	Y
Dipartimento indipendente		X2	X1	Y
Organizzazione indipendente			X2	X

(1) A: Lesioni lievi temporanee a una o più persone;
B: Lesioni gravi permanenti a una o più persone, decesso di una persona;
C: Decesso di diverse persone;
D: Decesso di moltissime persone.

Tabella 5 – CEI EN 61508-1
Livelli minimi di indipendenza per le fasi da 9 a 10 della Figura 4
(Per la fase 11 la IEC 61508-1 non da prescrizioni essendo altre misure di riduzione del rischio)

Minimo livello di indipendenza	Livello di integrità sulla scurezza SIL			
	1	2	3	4
Persona indipendente	X	X1	Y	Y
Dipartimento indipendente		X2	X1	Y
Organizzazione indipendente			X2	X

Tabella 8 – Tipici minimi SIL richiesti per SIF per impianti off-shore

Sicurezza Funzionale	SIL	LIMITAZIONI FUNZIONALI PER I REQUISITI DEL SIL E COMMENTI
Segregazione Processo (mediante PSD) ➢ (chiusura di diverse valvole)	1	La funzione parte quando viene attivato il PSD e include tutte le valvole necessarie alla segregazione del processo NOTA I sensori possono essere inclusi o esclusi a secondo della tipologia di PSD (ved. sotto PALL).
Funzione PSD: *LAHH/PAHH* ➢ (chiusura di una valvola critica)	2	La funzione parte quando viene attivato il PSD a seguito di situazioni anomale rilevate dai sensori e include la valvola finale critica. NOTA In questo caso viene considerata la situazione di avere una linea di ingresso all'EUC, diversamente saranno impiegate diverse valvole.
Funzione PSD *TALL/TAHH* ➢ (chiusura di una valvola critica)	2	La funzione parte quando il sensore di temperatura rileva situazioni anomale e include la valvola finale critica. NOTA Anche in questo caso viene considerata la situazione di avere una linea di ingresso all'EUC, diversamente saranno impiegate diverse valvole.
Funzione PSD: *PALL* ➢ (protezione primaria contro perdite)	NA	In queste applicazioni di funzione PSD non è richiesto alcuno specifico SIL e si applica in particolare a rilevamento di perdite di gas che generalmente non provocano alcun inasprimento del fenomeno. NOTA Nessun requisito particolare di SIL è pure richiesto nel caso di basse pressioni. Quando questa funzione è attivata da una causa iniziante qualsiasi, allora tale funzione dovrebbe essere di SIL 1 come nel caso della segregazione del processo visto al rigo 1.
Sezionamento ESD ➢ (chiusura di una valvola ESD)	2	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari alla chiusura della valvola ESD: – nodo ESD; – valvola ESD incluso attuatore e solenoide.
Depressurizzazione: ➢ (apertura di una valvola di scarico)	2	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari all'apertura della valvola scarico: – nodo ESD; – valvola scarico incluso attuatore e solenoide.
Isolamento di pozzo: ➢ (chiusura di un pozzo)	3	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari per la chiusura del pozzo: – nodo ESD (testa pozzo nel pannello controllo); – valvola wing (WV) e valvola master (MV) incluso attuatore e solenoide; – valvola di fondo pozzo (DHSV), incluso attuatore e solenoide.
Isolamento di riserva: ➢ (chiusura di una riserva)	2	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari per la chiusura della riserva: – nodo ESD; – valvola ESD incluso attuatore e solenoide. La QRA dovrebbe verificare se sono richiesti più e restrittivi requisiti si SIL 3 a causa delle dimensioni, lunghezze, numero di fluidi componenti la riserva e la linea connessa (flowline).
Rilevamento incendio: ➢ (generazione di segnale di allarme)	2	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari alla rivelazione incendio: – sensori (fiamma, fumo, temperatura); – nodo F&G (Fire & Gas).
Rivelazione gas: ➢ (generazione di segnale di allarme, processamento e segnale trasmesso)	2	I requisiti del SIL devono essere applicati anche ai sottosistemi necessari alla rivelazione gas: – sensori gas; – nodo F&G.

9.3 Requisiti del sistema di controllo di processo base come livello di protezione

9.3.1 Rappresentazione del sistema di controllo base di processo (BPCS).

Il BPCS può essere identificato, come un primo anello di protezione del processo come illustrato in Figura 7.

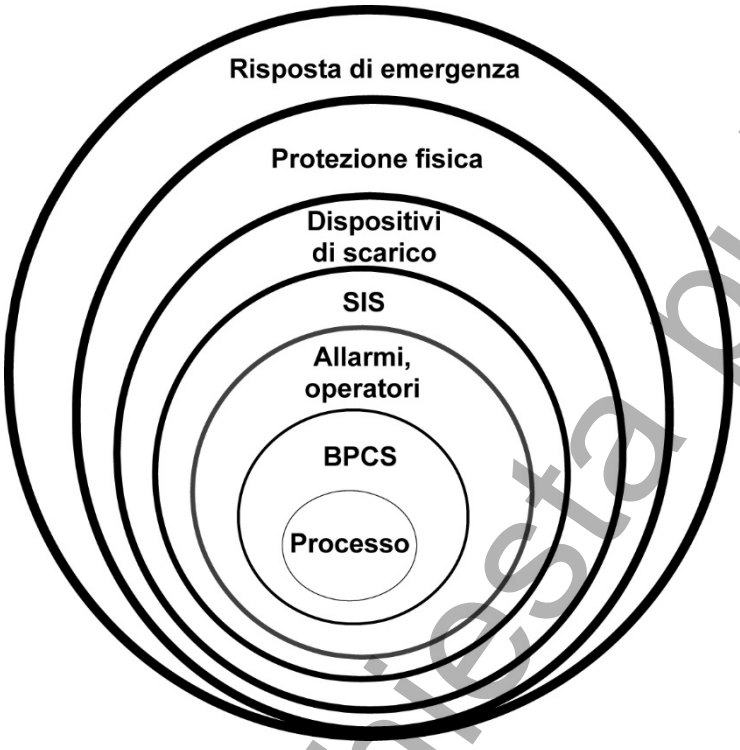


Figura 7 – Metodi tipici di riduzione del rischio riscontrati in impianti di processo

9.3.2 Fattore di riduzione del rischio normale per un BPCS

Un BPCS non conforme alla CEI EN 61511 o CEI EN 61508, utilizzato come barriera di protezione deve essere considerato con fattore di riduzione del rischio inferiore a 10.

9.3.3 Fattore di riduzione del rischio speciale per un BPCS

Un BPCS conforme alla CEI EN 61511 o CEI EN 61508, utilizzato come barriera di protezione può essere considerato superiore a 10, solo se concepito per soddisfare ai requisiti di queste norme.

9.4 Requisiti per prevenire guasti di causa e di modo comune e guasti dipendenti

Seguire le indicazioni riportate nell'analogo paragrafo della CEI EN 61511-1.

10 Specificazione dei requisiti dei sistemi strumentati di sicurezza (SIS)

10.1 Obiettivi

L'obiettivo è di specificare i requisiti relativi alla(e) funzione(i) strumentata(e) di sicurezza (SIF) dei Sistemi Strumentati di Sicurezza (SIS).

10.2 Requisiti generali

Per i requisiti generali del SIS seguire le indicazioni riportate nell'analogo paragrafo della CEI EN 61511-1.

10.3 Requisiti relativi alla sicurezza del SIS

Per i requisiti generali del SIS seguire le indicazioni riportate nell'analogo paragrafo della CEI EN 61511-1.

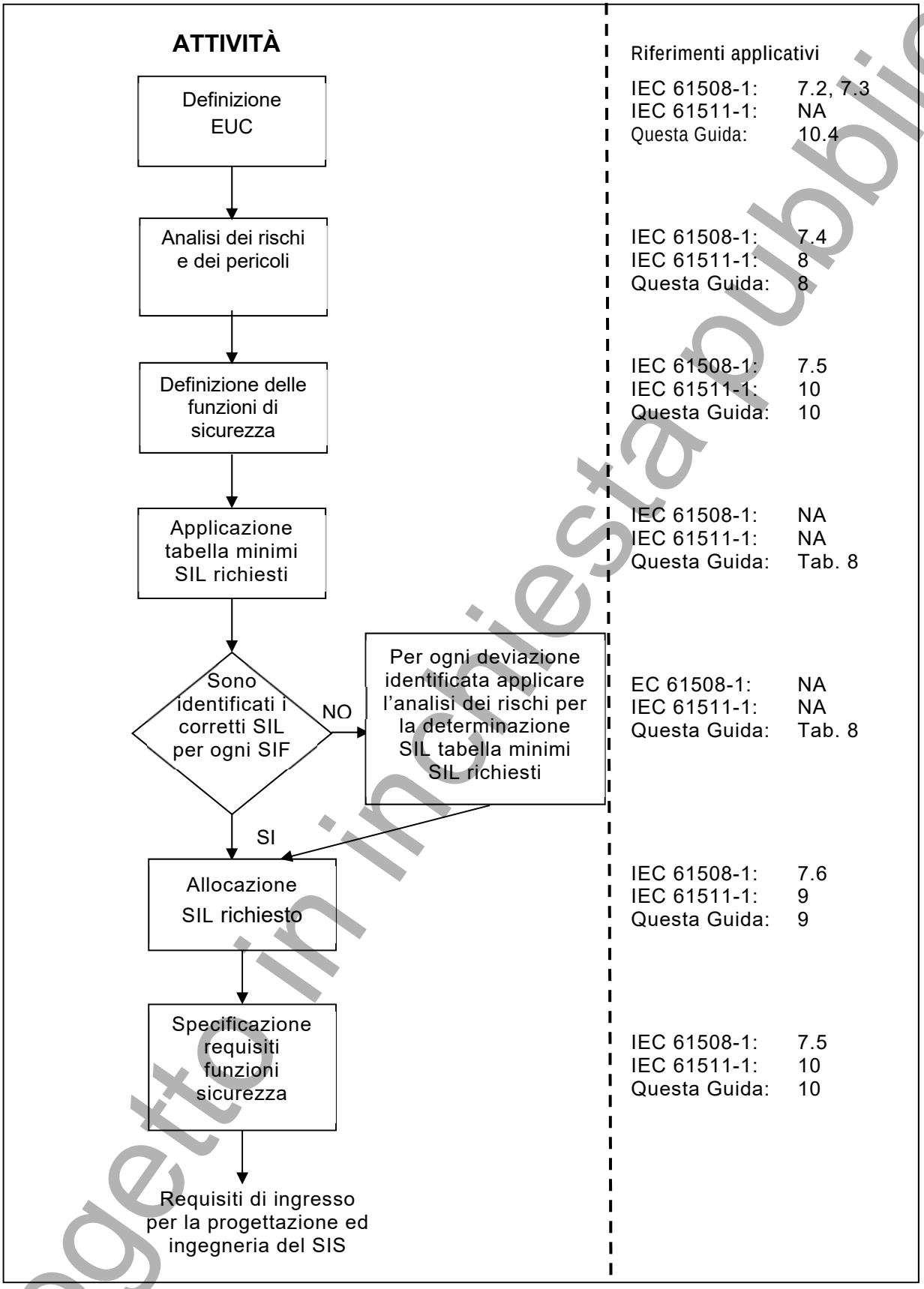
10.4 Linea guida per la definizione dei requisiti dei SIS

L'Apparecchiatura sotto Controllo (Equipment Under Control - EUC), ovvero l'apparecchiatura protetta dal Sistema Strumentato di Sicurezza (SIS) e dagli altri Sistemi relativi di Sicurezza (SrS) deve essere generalmente protetta anche nelle seguenti condizioni/funzioni:

- Fermata di emergenza
- Scarico di emergenza
- Isolamento di emergenza
- Rilevamenti di gas/incendio
- Spegnimento di incendio, ecc.

La Figura 8 riporta a titolo illustrativo un esemplificativo schema di flusso per lo sviluppo dei requisiti del Sistema Strumentato di Sicurezza (SIS) dei richiesti Livelli di Integrità di Sicurezza (SIL) delle Apparecchiature sotto Controllo (EUC), partendo dall'analisi dei rischi e dei pericoli.

Vedasi l'Allegato A per un approccio pratico sullo sviluppo delle fasi del ciclo di vita di concezione e di progettazione di un piccolo impianto, ovvero di un semplice SIS; per impianti più complessi vedasi invece gli Allegati successivi.



11 Progettazione ed ingegnerizzazione del SIS

11.1 Obiettivi

L'obiettivo della progettazione ed ingegnerizzazione del SIS è quello di concepire uno o più SIS per ottenere la(e) funzione(i) strumentate(e) di sicurezza (SIF) che soddisfino il (i) livello(i) integrità di sicurezza (SIL) previsto(i).

11.2 Requisiti generali

Per i requisiti generali seguire le indicazioni riportate nell'analogo paragrafo della CEI EN 61511-1.

11.3 Requisiti relativi al comportamento del sistema nella rilevazione di una anomalia

Per i requisiti in oggetto seguire le indicazioni riportate nell'analogo paragrafo della CEI EN 61511-1.

11.4 Requisiti relativi alla tolleranza alle anomalie dell'hardware

11.4.1 Generalità

La norma richiede che per le funzioni strumentate di sicurezza, i sensori, il risolutore logico e gli elementi finali abbiano un livello minimo di tolleranza ai guasti hardware in relazione al SIL richiesto alla funzione stessa.

Si osservi che con tolleranza ai guasti hardware di un componente, o sottosistema SIS, si intende la capacità del sistema di mantenere integra la sua capacità di eseguire correttamente le funzioni di sicurezza richieste anche in presenza di un certo numero di guasti dannosi. In particolare per un sistema che tollera "N" guasti dannosi nel caso di "N+1" guasti dannosi il sistema perde la sua capacità di eseguire le funzioni di sicurezza richieste.

Nell'ambito della norma la minima tolleranza ai guasti hardware è stata definita con l'intento di prevenire potenziali difetti nella progettazione della SIF che possono risultare, sia dal numero di assunzioni fatte durante la progettazione stessa, sia dall'incertezza della frequenza di guasto dei componenti, o sottosistemi, utilizzati nelle varie applicazioni di processo.

Si osservi inoltre che la norma in oggetto fornisce i requisiti minimi di tolleranza ai guasti hardware, vi possono essere dei casi, vedere paragrafo 11.9 della CEI EN 61511-1, in cui in funzione dell'applicazione, della frequenza di guasto dei componenti e dell'intervallo di prova periodica della SIF, sia richiesta della ridondanza aggiuntiva.

11.4.2 Suddivisione del SIS in sottosistemi indipendenti

Qualora il sistema strumentato di sicurezza SIS sia suddiviso in vari sottosistemi (cioè, sensori, risolutori logici, elementi finali) occorre che ogni sottosistema sia conforme all livello di integrità di sicurezza SIL richiesto.

11.4.3 Tolleranza ai guasti hardware HFT

La tolleranza ai guasti hardware in relazione al SIL richiesto può essere determinata in accordo con:

- i requisiti 7.4.4.2 (Route $_{1H}$) della CEI EN 61508-2 oppure,
- i requisiti 7.4.4.3 (Route $_{2H}$) della CEI EN 61508-2 oppure,
- i requisiti da 11.4.5 a 11.4.9 della CEI EN 61511-1, praticamente allineati ai requisiti della Route $_{2H}$ della CEI EN 61508-2.

11.4.4 Determinazione delle modalità di guasto dei sottosistemi del SIS

Quando si determina la tolleranza ai guasti hardware HFT si possono escludere certi tipi di guasto caratterizzati da una probabilità di accadimento molto bassa in relazione al livello di integrità di sicurezza SIL richiesto. Ogni esclusione però deve essere giustificata e documentata.

11.4.5 Determinazione della tolleranza dei guasti hardware HFT del SIS

Come riportato in 11.4.3, si possono scegliere due strade per la determinazione dell'HFT dei sottosistemi del SIS:

1) La Route $_{1H}$

che prevede di utilizzare normali componenti, e suddividerli in relazione alla loro complessità, in due sottosistemi:

- Sottosistema A:

  un sottosistema per i cui componenti si verificano insieme le seguenti condizioni:

  - *sono ben definite e note le possibili modalità di guasto, e*
  - *è completamente determinato il loro comportamento in condizioni di guasto, e*
  - *dall'esperienza di utilizzo precedente sono disponibili dati statistici sufficienti per convalidare le probabilità di guasto dichiarate.*

- Sottosistema B:

  un sottosistema per i cui componenti almeno una delle condizioni di cui sopra non sono verificate.

Pertanto la CEI EN 61508-2 prevede per la determinazione dell'HFT del SIS Tabella 2 e Tabella 3, qui sotto riportate per comodità in Tabella 9.

Tabella 9 - Individuazione della tolleranza minima ai guasti hardware per sottosistemi A e B secondo CEI EN 61508-2 (Route $_{1H}$)

Tabella 2 – CEI EN 61508-2
Integrità di sicurezza dell'hardware: Vincoli architetturali per sottosistemi relativi alla sicurezza di Tipo A

Frazione del Guasti Sicuri (SFF)	Tolleranza minima ai guasti hardware		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% ÷ < 90%	SIL 2	SIL 3	SIL 4
90% ÷ < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Tabella 3 – CEI EN 61508-2
Integrità di sicurezza dell'hardware: Vincoli architetturali per sottosistemi relativi alla sicurezza di Tipo B

Frazione del Guasti Sicuri (SFF)	Tolleranza minima ai guasti hardware		
	0	1	2
< 60%	non permesso	SIL 1	SIL 2
60% ÷ < 90%	SIL 1	SIL 2	SIL 3
90% ÷ < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

2) La Route $_{2H}$

che prevede invece di utilizzare speciali componenti provati anteriormente, selezionati conformemente alla CEI EN 61508-2 oppure alla CEI EN 61511-1 paragrafo 11.5 che prevede dispositivi:

– Proven in use:

Provati in uso sulla base di progettazione del produttore(ad esempio, limite di temperatura, umidità, vibrazioni, ecc.)

– Prior use:

Provati prima su processi con ambienti operativi specifici similari a quello richiesto.

Un dispositivo da campo viene considerato prior use quando:

– L'elenco viene aggiornato e monitorato regolarmente;
– I dispositivi vengono aggiunti solo quando l'esperienza operativa sufficiente è stata ottenuta;
– I dispositivi vengono rimossi quando mostrano di non eseguire la funzione in modo soddisfacente;
– L'ambiente operativo è incluso nella lista, se del caso.

La Tabella 10, riporta a tal proposito il minimo Hardware Fault Tolerance HFT per architetture dei sottosistemi, in relazione al tipo di richiesta di intervento, ovvero della tipologia della domanda suddivisa in tre categorie:

continua (quasi sempre), alta (>1 volta/anno) o bassa (< 1 volta /anno).

Tabella 10 - Tolleranza minima ai guasti hardware HFT in funzione del tipo di domanda secondo CEI EN 61511-1 (Route $_{2H}$)

Tabella 6 – CEI EN 61511-1
Minimo Hardware Fault Tolerance HFT per i vari sistemi di sicurezza
(1), (2), (3), (4)

SIL	Minimo richiesto HFT
1 ogni modo	0
2 bassa domanda	0
2 alta o continua domanda	1
3 ogni modo	1
4 ogni modo	2

(1) Stralcio del paragrafo 11.4.6:

Per un sottosistema SIS che utilizza solo linguaggi fissi di programmazione (FPL), per esempio sensori e attuatori tipo smart, e non utilizza dispositivi programmabili con linguaggi a variabilità totale (FVL) o limitata (LVL), se è accertato che l'applicazione dei requisiti di HFT riportati in tabella, comporterebbe guasti aggiuntivi conducendo a una diminuzione della sicurezza globale del processo, è allora possibile ridurre l'HFT. Tale circostanza dev'essere propriamente giustificata. La giustificazione dovrà fornire evidenza che l'architettura proposta è idonea allo scopo e rispetta i requisiti d'integrità di sicurezza richiesti.

(2) Stralcio del paragrafo 11.4.7:

Se l'HFT risulta 0 applicando 11.4.6, la scelta deve fornire evidenza che i relativi modi di guasti pericolosi sono stati evitati oltre ai guasti sistematici.

(3) Stralcio del paragrafo 11.4.8:

I dispositivi programmabili FVL e LVL devono avere coperture diagnostiche maggiori del 60 %.

(4) Stralcio del paragrafo 11.4.9

11.5 Requisiti relativi alla scelta dei componenti dei sottosistemi

11.5.1 Obiettivi

Scopo del presente paragrafo e di definire:

- i requisiti e criteri per la selezione dei componenti o dei sottosistemi da utilizzare come parti di un SIS;
- i requisiti che un componente o un sottosistema devono soddisfare per poter essere integrati nell'architettura di un SIS;
- i criteri di accettabilità di un componente o di un sottosistema in termini di SIF e di integrità di sicurezza.

11.5.2 Requisiti generali

In generale occorre considerare quanto segue:

1) I componenti o sottosistemi (sensori, risolutori logici ed elementi finali) selezionati per far parte di un SIS per applicazioni da SIL 1 a SIL 4, inclusi, dovranno essere o progettati e realizzati in accordo alla CEI EN 61508, parti 2 e 3 per quanto applicabile, oppure, selezionati in accordo ai requisiti del paragrafo da 11.5.3 a 11.5.6 della CEI EN 61511-1.
2) I componenti o sottosistemi (sensori, risolutori logici ed elementi finali) selezionati per far parte di un SIS devono essere scelti in base alle specifiche del fornitore e considerando anche le circostanze di utilizzazione riportate nel paragrafo 11.9 della CEI EN 61511-1.

11.5.3 Requisiti relativi alla scelta dei componenti precedentemente utilizzati

È possibile utilizzare componenti e sottosistemi che non siano stati esplicitamente progettati e realizzati in accordo alla CEI EN 61508, purché questi siano provati dal fornitore (proven use) e provati prima in applicazioni similari (prior use).

In particolare deve esserci una adeguata evidenza che i componenti ed i sottosistemi considerati siano adatti ad essere utilizzati in sistemi strumentati di sicurezza. Nel caso di dispositivi da campo vi potrà essere ad esempio una significativa esperienza di utilizzo operativo sia in applicazioni di sicurezza che in applicazioni non di sicurezza.

Il livello di dettaglio dei dati statistici storici del precedente utilizzo del dispositivo in oggetto deve essere adeguato alla complessità del componente stesso ed alla probabilità di guasto necessaria per ottenere il livello di integrità di sicurezza SIL richiesto dalla funzione strumentata di sicurezza SIF che si vuole realizzare.

L'analisi di adeguatezza dovrà considerare e valutare quanto segue:

- il sistema di gestione della qualità del produttore del componente o sottosistema;
- la completezza e l'adeguatezza delle specifiche del componente o del sottosistema;
- le prestazioni del componente o del sottosistema in un contesto operativo e fisico simili a quello in cui si intende utilizzarli;
- la dimensione del campione alla base dei dati storici di utilizzo.

Nel caso di dispositivi di campo (sensori ed elementi finali, ad esempio) sono possibili le seguenti osservazioni:

- la funzione che svolgono, ad esempio misurare una portata oppure interrompere un flusso, sono le medesime sia in applicazioni di sicurezza che in applicazioni non di sicurezza, pertanto per la valutazione delle loro prestazioni è dunque possibile considerare anche i dati storici di utilizzo in applicazioni non di sicurezza;
- gli utilizzatori sono soliti registrare le informazioni relative alla vita operativa dei dispositivi utilizzati in appositi elenchi che solitamente includono solo quei dispositivi approvati per l'uso nei loro impianti; un dispositivo viene dichiarato idoneo all'utilizzo nell'impianto in oggetto a fronte di una serie storica di prestazioni positive in applicazioni di sicurezza e non di sicurezza.

Queste liste possono essere considerate a supporto e dimostrazione delle prestazioni risultanti dall'utilizzo operativo del dispositivo qualora:

a) siano mantenute aggiornate regolarmente;

b) i dispositivi di campo vengono aggiunti alla lista solamente quanto maturano una esperienza di utilizzo operativo sufficiente;

c) i dispositivi di campo che non forniscono prestazioni adeguate vengono rimossi alla lista;

d) la lista riporta anche il tipo di applicazione di processo.

11.5.4 Requisiti relativi alla scelta dei componenti programmabili FPL

Per la scelta dei componenti o sottosistemi programmabili FPL valgono i criteri ed i requisiti precedentemente espressi nei paragrafi precedenti 11.5.2 e 11.5.3. oltre a quanto espressamente evidenziato nel presente paragrafo.

Qualora non si utilizzassero tutte le funzionalità offerte dal componente o sottosistema programmabile in oggetto è necessario che queste siano analizzate allo scopo di accertare che non siano in grado di compromettere la funzione strumentata di sicurezza richiesta.

L'analisi di adeguatezza del componente o sottosistema, sia da un punto di vista hardware che software, deve prendere in considerazione quanto segue:

- caratteristiche dei segnali di ingresso e di uscita;
- modalità di utilizzo;
- funzionalità e configurazioni utilizzate;
- utilizzo precedente in applicazioni e contesti fisici simili.

Per applicazioni SIL 3 va effettuata una valutazione formale del componente o del sottosistema FPL in accordo a 5.2.6.1 della CEI EN 61511-1, in modo tale da dimostrare che:

- il dispositivo FPL sia in grado di svolgere la funzione richiesta e che il suo utilizzo precedente abbia mostrato che la sua probabilità di guastarsi, sia a causa di guasti hardware casuali sia a causa di guasti hardware o software sistematici, in modo da causare un evento pericoloso quando utilizzato come parte di un sistema strumentato di sicurezza, è sufficientemente basso;
- il suo hardware ed il suo software sono sviluppati in accordo agli standard applicabili;
- il dispositivo FPL è stato utilizzato oppure provato in configurazioni rappresentative dell'utilizzo che se ne intende fare nel sistema strumentato di sicurezza.

Per applicazioni SIL 3 inoltre il produttore deve rendere disponibile il manuale di sicurezza del dispositivo che ne riporti le eventuali limitazioni di impiego, le indicazioni per la manutenzione e per la rilevazione dei guasti. Il manuale di sicurezza deve coprire le configurazioni tipiche del dispositivo FPL e le modalità d'impiego per le quali è progettato.

11.5.5 Requisiti relativi alla scelta dei componenti programmabili LVL

I requisiti riportati nel presente paragrafo possono essere applicati solamente a risolutori logici PE utilizzati per realizzare sistemi strumentati di sicurezza che realizzano funzioni di sicurezza di livello SIL 1 e SIL 2.

Nel caso di componenti programmabili LVL oltre ai requisiti riportati nel presente paragrafo, devono essere applicati anche i requisiti di 11.5.4.

Qualora ci fossero delle differenze tra il contesto operativo e fisico di utilizzo del componente o del sottosistema in oggetto tra le esperienze di uso precedente ed il suo utilizzo come parte di un sistema strumentato di sicurezza, queste vanno identificate e devono essere oggetto di una valutazione specifica (analisi e prove), atta a dimostrare che la probabilità di guasto sistematico quando il dispositivo è utilizzato in un sistema strumentato di sicurezza è sufficientemente bassa.

L'esperienza operativa di utilizzo necessaria a considerare adatto un dispositivo programmabile LVL deve essere identificata considerando quanto segue:

- il SIL richiesto alla funzione strumentata di sicurezza;
- la complessità e le funzionalità del componente o del sottosistema.

Per applicazioni SIL 1 e SIL 2 è possibile utilizzare un risolutore logico PE per applicazioni di sicurezza, ossia un risolutore logico PE per applicazioni industriali generiche configurato espressamente per essere utilizzato in applicazioni di sicurezza, qualora fossero rispettati anche i seguenti requisiti addizionali:

- sono identificate e note tutte le modalità di guasto non sicure;
- per tutte le modalità di guasto identificate vengono adottate tecniche di configurazione per renderle sicure;
- il software incorporato ha un passato significativo, e positivo, per applicazioni di sicurezza;
- sono utilizzate protezioni contro le modifiche accidentali oppure da parte di persone non autorizzate.

Inoltre, per applicazioni SIL 2 di un risolutore logico PE va effettuata una valutazione formale della sicurezza funzionale in modo tale da dimostrare che:

- il dispositivo è in grado di svolgere la funzione richiesta e che il suo utilizzo precedente ha mostrato che la sua probabilità di guastarsi, sia a causa di guasti hardware casuali sia a causa di guasti hardware o software sistematici, in modo da causare un evento pericoloso quando utilizzato come parte di un sistema strumentato di sicurezza è sufficientemente basso;
- sono stati messi in atto provvedimenti per rilevare anomalie durante l'esecuzione dei programmi e per iniziare la reazione appropriata; questi provvedimenti devono comprendere tutti i punti seguenti:
  - monitoraggio della sequenza del programma;
  - protezione con codice contro le modifiche o rilevamento delle anomalie con monitoraggio in linea;
  - conferma del guasto o diversa programmazione;
  - controllo del campo delle variabili o controllo di plausibilità dei valori;
  - approccio modulare;
  - sono state utilizzate norme di codificazione appropriate per il software incorporato e di utilizzazione;
  - è stato provato in configurazioni tipiche, con scenari di prova rappresentativi dei profili operazionali previsti;
  - sono stati utilizzati moduli software e componenti verificati con cura;
  - il sistema ha subito analisi e prove dinamiche;
  - il sistema non utilizza intelligenza artificiale o riconfigurazione dinamica;
  - sono state realizzate prove di inserzione di anomalia documentate.

11.5.6 Requisiti relativi alla scelta dei componenti programmabili FVL

In questo caso occorre che il risolutore logico PE sia progettato e realizzato in accordo alla CEI EN 61508 parti 2 e 3.

11.5.7 Ulteriore guida per la scelta dei componenti di un SIS

Alla luce di quanto esposto nei punti precedenti sono possibili le seguenti considerazioni realizzative e pratiche nella scelta dei componenti per un sistema strumentato di sicurezza.

Per quanto riguarda i **sensori** comunemente utilizzati nell'industria di processo è possibile la seguente schematizzazione:

1) Trasmettitori, termoelementi (TC/RTD) e dispositivi con soglia di intervento a "interruttore" (termostati, pressostati, livellostati, flussostati, magnetotermici, ecc.), sono considerabili sottosistemi di tipo "A".
2) Termoelementi e dispositivi "interruttori", sono, in termini conservativi, considerabili aventi una copertura diagnostica limitata (SFF inferiore al 60%).
3) Trasmettitori SMART sono considerabili aventi una copertura diagnostica media (SFF tra il 60% e il 90%).

Pertanto, alla luce delle considerazioni di cui sopra è possibile applicare la Tabella 2 della CEI EN 61508-2 (riportata nella Tabella 10 al paragrafo 11.4.5) ottenendo lo schema riportato in Tabella 11.

Tabella 11 – Integrità di sicurezza hardware: Costrizioni architetturali si sottosistemi relativi alla sicurezza Tipo A
(Rielaborazione della Tabella 2 della CEI EN 61508-2 per sensori)

Tipo sensore	Tolleranza ai guasti hardware		
	0	1	2
Interruttori	SIL 1	SIL 2	SIL 3
Termoelementi TC/RTD	SIL 1	SIL 2	SIL 3
Trasmettitori SMART	SIL 2	SIL 3	SIL 3

Attualmente sono disponibili sul mercato un certo numero di sensori costruiti esplicitamente in accordo alla CEI EN 61508, parti 2 e 3, e dotati di opportuno certificato emesso da enti terzi (laboratori, organismi di certificazione), internazionalmente riconosciuti che ne attestano l'idoneità per un certo livello di SIL.

Per quanto riguarda la condivisione di sensori tra BPCS e SIS si raccomanda di procedere come segue:

- valutare ed evitare le possibili cause di guasti comuni (otturazione prese e collegamenti di processo, corrosione ed erosione, alimentazioni);
- in linea di principio è sconsigliato utilizzare lo stesso sensore per funzioni a BPCS e funzioni di sicurezza realizzate dal SIS anche se la norma non lo proibisce;
- per i SIL 2, 3 e 4 il livello di sicurezza richiesto è tipicamente raggiunto mediante la separazione tra i sensori del SIS e quelli del BPCS; i sensori possono essere identici o diversi;
- il confronto tra i valori misurati dai sensori del SIS e quelli misurati dai sensori del BPCS, mantenendo comunque le opportune segregazioni, è utile in quanto aumenta la copertura diagnostica;
- l'utilizzo di principi di misura differenti per l'ottenimento della ridondanza è visto positivamente, tuttavia viene esposto e sottolineato il principio che "non si deve sacrificare la affidabilità per ottenere la diversità dei dispositivi di misura".

I sensori di tipo "smart" è necessario che siano protetti dalla scrittura in modo tale da evitare che i loro parametri di configurazione e calibrazione siano inavvertitamente modificati da stazioni remote. La possibilità di scrittura può essere consentita qualora sia svolta una analisi di sicurezza mirata a tale scopo che prenda in considerazione anche il fattore umano di non rispetto delle procedure.

Per semplicità, si sconsiglia comunque di rendere disponibile la funzionalità di scrittura per sensori "smart" facenti parte di sistemi strumentati di sicurezza.

Per quanto riguarda i **risolutori logici** comunemente utilizzati nell'industria di processo sono possibili le seguenti osservazioni.

Considerando risolutori logici ad elettronica programmabile (PE), si osserva che per questo sottosistema è attualmente possibile una scelta tra una vasta gamma di PLC certificati in accordo alla CEI EN 61508 parti 2 e 3. In particolare sono disponibili sul mercato PLC dotati di dichiarazione di conformità alle norme prodotta da Organismi di Certificazione Indipendenti, presso laboratori internazionalmente riconosciuti per i livelli di sicurezza SIL 2 e SIL 3. Si suggerisce di orientare le proprie scelte verso risolutori logici coperti da dichiarazione, essendo l'applicazione dei contenuti di 11.5.4 e 11.5.5 della CEI EN 61511-1 estremamente onerosa e di difficile applicazione.

È importante sottolineare come un risolutore logico ad elettronica programmabile sia, in genere, un sistema complesso composto dall'hardware del PLC vero e proprio, tipicamente solo questa parte è coperta dalla dichiarazione del risolutore logico, deve essere sempre verificato che gli elementi impiegati siano quelli descritti nella dichiarazione, un elemento diverso squalifica l'intera composizione.

Anche gli accessori, in genere di produttori diversi da quello del PLC, quali barriere, relè di interposizione e morsettiere con relativi cablaggi devono essere anche loro idonei al livello di sicurezza necessario.

L'involucro o quadro di contenimento deve essere idoneo ai fini della compatibilità elettromagnetica.

All'interno del quadro non devono essere presenti apparecchiature non pertinenti al SIS.

Per quanto riguarda la separazione delle funzioni tra BPCS e SIS si suggerisce di procedere come segue:

- *per l'ottenimento dei SIL 1 e 2, il BPCS ed il SIS possono essere due sottosistemi facenti parte dello stesso sistema (purchè certificato) o differenti;*
- *per l'ottenimento dei SIL 3 e 4, il BPCS ed il SIS vengono normalmente realizzati con sistemi tra di loro diversi.*

Per quanto riguarda gli **elementi finali**, comunemente utilizzati nell'industria di processo, sono possibili le seguenti osservazioni.

Le valvole di blocco comunemente usate sono considerabili sottosistemi di tipo A.

È pertanto possibile applicare la Tabella 2 della CEI EN 61508-2 (riportata nella Tabella 9 a paragrafo 11.4.5) ed in accordo ai valori di affidabilità tipici si può adottare il seguente schema:

- *per SIL 1 è possibile utilizzare una valvola sola purché l'intervallo di prova periodica non sia maggiore di 2 - 4 anni;*
- *per SIL 2 è possibile utilizzare una valvola sola purché sia possibile effettuare una prova in linea almeno ogni 6 - 12 mesi; se per motivi di processo oppure di operabilità ciò non fosse possibile, allora occorre la ridondanza dell'elemento finale (1oo2, di cui la seconda valvola può essere una valvola di controllo con l'aria intercettata da una solenoide facente parte dell'anello SIS);*
- *per SIL 3 è necessaria la ridondanza dell'elemento finale (1oo2, di cui la seconda valvola può essere una valvola di controllo con l'aria intercettata da una solenoide facente parte dell'anello SIS).*

11.6 Dispositivi da campo

11.6.1.1 Installazione

Gli accessori, quali collegamenti primari, collettori (manifold), accessori di valvole, supporti, staffe di sostegno, barilotti, collegamenti pneumatici, necessari per l'installazione in campo dei sensori e degli elementi finali, devono essere scelti e montati in modo tale da minimizzare i guasti che possono derivare da errate misure o comportamenti degli elementi finali a causa di particolari condizioni di processo ed ambientali.

In fase di progettazione si dovrà dunque tenere in considerazione fattori quali:

- il possibile congelamento di alcuni fluidi sia per condizioni ambientali che per ragioni di processo;
- la corrosione dei materiali;
- la possibile presenza di solidi in sospensione;
- i fenomeni di polimerizzazione;
- i fenomeni di riscaldamento (cooking);
- i fenomeni di condensa nei primari.

11.6.2 Alimentazione

Per assicurare l'integrità delle funzioni di sicurezza vanno considerati anche gli aspetti relativi alla alimentazione dei circuiti.

Per i risolutori logici questi devono essere alimentati da fonte sicura e privilegiata quale UPS (gruppo di continuità statico di tipo no-break). Se necessaria l'interposizione di convertitori di tensione (c.c./c.c. o c.a./c.c.), è importante che siano di tipo ridondanti, dimensionati ognuno con il 30% di riserva e idonei al livello di sicurezza necessario.

Per quanto riguarda i sensori, quali i trasmettitori e gli attuatori, quali i posizionatori, si suggerisce di alimentarli direttamente dalle schede di uscita del risolutore logico. Nel caso in cui, per la natura del sensore, sia necessaria una alimentazione separata occorre sincerarsi che questa sia disponibile sempre da una fonte sicura come UPS.

Qualora si fosse obbligati ad utilizzare circuiti di ingresso o di uscita funzionanti a lancio di corrente (energize to trip), si suggerisce di utilizzare funzionalità quali il monitoraggio della linea attraverso piccole correnti pilota per assicurarsi della continuità del circuito stesso.

Nel caso di circuiti normalmente energizzati non è invece necessario l'utilizzo della funzionalità di monitoraggio della continuità delle linea, per semplicità ed efficienza, l'impiego di questa seconda soluzione è pertanto consigliato in sostituzione al lancio di corrente.

Anche per i segnali di comando l'alimentazione deve essere sempre disponibile da fonte sicura come UPS.

11.6.3 Collegamenti elettrici

Per le connessioni tra dispositivi di campo e gli ingressi o le uscite del risolutore logico si suggerisce di utilizzare collegamenti dedicati per ciascun dispositivo con cavi aventi caratteristiche almeno conformi alla CEI 20-36.

Si suggerisce inoltre di segregare già a livello campo le connessioni del SIS da quelle degli altri sistemi di automazione e controllo, come ad esempio il BPCS. Si suggerisce quindi di utilizzare, percorsi diversi per il sistema SIS, l'impiego di vie cavi protette e cassette di giunzione in campo dedicate, multicavi dedicati ed eventuali armadi di smistamento cavi (marshalling) dedicati al solo SIS.

11.7 Interfacce

Nessuna ulteriore guida.

11.8 Requisiti manutentivi

Nessuna ulteriore guida.

11.9 Quantificazione dei guasti casuali

Nessuna ulteriore guida.

12 Requisiti del software

L'articolo normativo considera:

- tre tipi di software:
  - il software applicativo;
  - il software di utilità, cioè, i mezzi software utilizzati per sviluppare e verificare il software applicativo;
  - il software incorporato, cioè, il software fornito come parte del PE,
- tre tipi di linguaggi di sviluppo del software:
  - linguaggio di programmazione fisso (FPL);
  - linguaggio a variabilità limitata (LVL);
  - linguaggio a variabilità totale (FVL).

I riferimenti normativi per lo sviluppo e la modifica del software applicativo sono i seguenti:

- CEI EN 61511 per applicazioni fino a SIL 3 utilizzando FPL o LVL;
- CEI EN 61508 per applicazioni di SIL 4 oppure utilizzando FVL.

Per applicazioni fino a SIL 3, il software, così come il manuale di sicurezza del costruttore, che definisce come il sistema PE possa essere applicato in tutta sicurezza, deve essere selezionato e applicato in conformità ai requisiti della CEI EN 61511-1, riportati ai paragrafi seguenti:

- 11.5, per la selezione e applicazione del software applicativo;
- 12.4.4, per la selezione del software incorporato.

Data la complessità della materia si suggerisce di seguire gli omologhi paragrafi della CEI EN 61511 parte 1 e 2, tenendo sempre in considerazione il ciclo di vita di sviluppo del software riportato in Figura 9 (ovvero Figura 12 della CEI EN 61511-1).

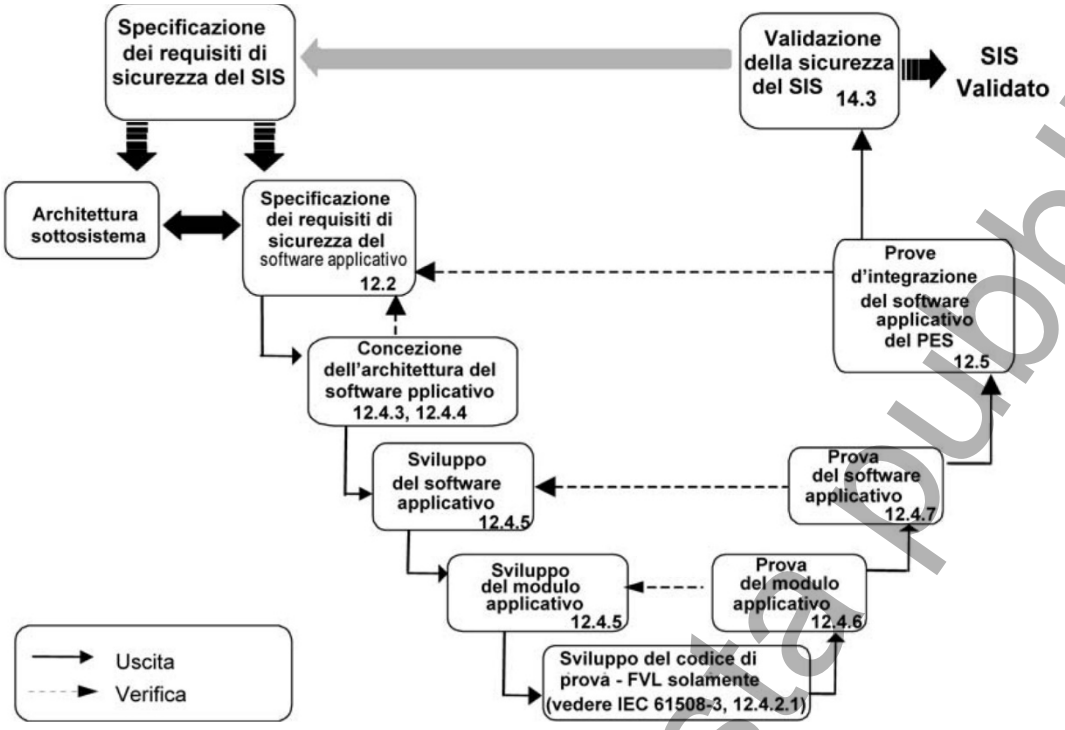


Figura 9 – Ciclo di vita di sviluppo del software (modello a V: CEI EN 61511-1)

13 Prove di accettazione in fabbrica (FAT)

13.1 Obiettivi

Lo scopo delle prove di accettazione in fabbrica (FAT) è di collaudare il sistema di elaborazione delle logiche di protezione, insieme al relativo software, per assicurare che soddisfi la specifica dei requisiti di sicurezza. Il collaudo del sistema di elaborazione delle logiche di protezione, prima della sua installazione sull'impianto, consente di identificare prontamente eventuali errori e di correggerli.

13.2 Raccomandazioni

Per la migliore riuscita delle prove seguire le raccomandazioni riportate nelle Note 1÷4 della CEI EN 61511-1 al paragrafo 13.2.1 e pianificarle come riportato nel successivo 13.2.2 (l'Allegato F riporta a tal proposito un approccio sistematico della pianificazione, schedulazione e registrazione delle FAT).[(1)]

Si fa notare, che la richiesta e la necessità delle FAT dovrebbe essere specificata durante la fase di concezione del progetto e dovranno essere presenziate dall'Assessor (Valutatore) e/o dal Rappresentante del Cliente.

Come linea guida dovrebbero essere almeno pianificate le seguenti attività:

- tipo di prova da eseguire;
- descrizione della prova e parametri di prova;
- ambiente di prova e mezzi di prova;
- configurazione del risolutore logico;
- criteri di accettazione di prova;
- procedure per le eventuali azioni correttive;
- competenza del personale di prova;
- locazione fisica di prova.

(1) Per le Prove di Accettazione in Fabbrica (FAT), Accettazione in Sito (SAT) e di Integrazione in Sito (SIT) vedere anche CEI EN 62381

Per ogni prova condotta, si dovrebbero considerare i punti seguenti:

- la versione della pianificazione di prova che è stata utilizzata;
- le caratteristiche e le prestazioni della funzione strumentata di sicurezza in prova;
- le procedure e le descrizioni delle prove condotte;
- la registrazione cronologica delle attività di prova;
- i mezzi, le apparecchiature e le interfacce utilizzate.

Tutti i risultati di prova devono essere registrati riportando:

- gli scenari di prova;
- i risultati di prova;
- e se gli obiettivi di prova sono stati raggiunti.

14 Installazione e messa in servizio del SIS

14.1 Obiettivi

Gli obiettivi dell'installazione e della messa in servizio del SIS sono i seguenti:

- il SIS sia installato in accordo ai disegni e alle specifiche di installazione;
- il SIS sia messo in servizio pronto per la validazione della sicurezza finale.

14.2 Requisiti

14.2.1 Pianificazione delle attività

Per ottemperare agli obiettivi richiesti, è necessario pianificare preventivamente le attività in termini almeno di:

- procedure e istruzioni delle attività da condurre;
- schedulazione temporale delle diverse attività;
- identificazione del personale e delle organizzazioni preposte alle attività stesse.

14.2.2 Installazione dei componenti

Tutti i componenti del SIS devono essere installati secondo il piano di progettazione e di installazione.

14.2.3 Messa in servizio

I controlli minimi durante le varie fasi di messa in servizio sono i seguenti:(1)

- verificare che nessun dispositivo sia stato danneggiato durante il trasporto;
- verificare la corretta installazione e l'eventuale messa a terra dei dispositivi;
- verificare che tutti gli strumenti siano stati opportunamente calibrati;
- verificare che tutti i dispositivi di campo siano funzionanti;
- verificare che tutti gli I/O del risolutore siano correttamente funzionanti e cablati ai relativi dispositivi in campo;
- verificare che tutte le interfacce con altri sistemi o periferiche siano funzionanti.

(1) Per le prove di controllo delle catene strumentate (loop check) vedere anche la CEI EN 62382.

14.2.4 Registrazioni

Tutte le attività dovrebbero essere registrate mediante opportuni moduli debitamente compilati dagli esecutori e controfirmati dai responsabili delle attività, ed ogni modulo dovrebbe almeno contenere le seguenti informazioni:

- identificativo dei componenti soggetti all'attività;
- tipo di attività effettuata e riferimento alla relativa procedura/istruzione;
- riferimento alle specifiche ed ai disegni necessari per l'esecuzione dell'attività;
- elenco delle verifiche effettuate a controllo della corretta esecuzione dell'attività;
- elenco degli strumenti di misura impiegati per la verifica dell'attività, il cui elenco almeno il modello, la matricola ed il suo numero di certificato di taratura;
- l'indicazione finale di attività completata, oppure da completarsi successivamente.

14.2.5 Deviazioni

Nel caso che si riscontri che l'istallazione reale non sia conforme alla concezione, allora le differenze devono essere valutate da una persona competente e l'impatto probabile sulla sicurezza deve essere determinato.

In questa situazione possono manifestarsi due casi:

- se le differenze non hanno alcun impatto sulla sicurezza, allora le informazioni di concezione devono essere aggiornate seguendo lo stato "come costruito";
- se invece le differenze hanno un impatto sulla sicurezza, allora l'installazione deve essere modificata per soddisfare ai requisiti di concezione.

In questo ultimo caso seguire le indicazioni riportate successivamente all'articolo 17.

15 Validazione della sicurezza del SIS

15.1 Obiettivi

Gli obiettivi della validazione del SIS è di validarne l'istallazione e messa in servizio, ovvero prevedere tutta una serie di attività di ispezione e collaudi finalizzati alla verifica che tutte le funzioni strumentate di sicurezza rispettino i requisiti riportati nella specifica dei requisiti di sicurezza del SIS.

15.2 Requisiti

15.2.1 Pianificazione generale delle attività

È necessario che sia preventivamente preparata una pianificazione delle attività di validazione del SIS, che dovrebbe contemplare almeno quanto segue:

- la procedura per l'esecuzione delle attività di validazione, completa dei riferimenti ai documenti e ai disegni necessari per la corretta esecuzione delle varie attività;
- le attività di validazione necessarie affinché si possa dimostrare che il SIS sia conforme a quanto richiesto dalla specifica dei requisiti di sicurezza;
- la identificazione di tutte le modalità operative di processo per le quali si dovrà validare il comportamento del sistema strumentato di sicurezza, quali:
  - lo start-up, le modalità automatiche, manuali, semi-automatiche e a regime,
  - il blocco, il ripristino dai blocchi e la manutenzione,
  - tutte quelle condizioni di marcia anomale ragionevolmente prevedibili, come ad esempio quelle identificate nella fase di analisi dei rischi;
- la programmazione temporale delle attività;
- l'identificazione del personale, degli uffici e delle organizzazioni di cantiere che saranno responsabili delle varie attività svolte.

15.2.2 Pianificazione addizionale delle attività per la validazione del software

Per i dettagli della pianificazione, vedere i requisiti richiesti da riscontare riportati in 12.2 della CEI EN 61511-1.

15.2.3 Precisione di misura degli strumenti utilizzati

Nel caso che la validazione contempli l'utilizzazione di mezzi e strumenti di misura, questi devono essere tarati per confronto con campioni di misura riferibili al sistema internazionale di misura e con una incertezza di misura appropriata all'applicazione.

15.2.4 Pianificazione dell'attività di validazione

Come minimo dovranno essere oggetto di validazione del SIS i seguenti aspetti:

- il comportamento del SIS sia in condizioni di marcia normali dell'impianto di processo sia in condizioni di marcia anormali, quali, ad esempio, l'avviamento ed il blocco, che saranno identificate nella specifica dei requisiti di sicurezza;
- che gli altri sistemi eventualmente presenti, quali il BPCS ad esempio, non interferiscano con il comportamento del SIS;
- che il SIS si comporti in accordo ai requisiti funzionali, hardware e software espressi nella specifica dei requisiti di sicurezza;
- che la documentazione del SIS sia consistente con quanto installato;
- che le funzioni strumentate di sicurezza si comportino come da specifica anche in presenza di valori non validi delle variabili di processo;
- che le sequenze di blocco vengano attivate correttamente sia in automatico che eventualmente manualmente;
- che tutte le indicazioni di allarme siano correttamente visualizzate sui dispositivi del caso (pagine grafiche e sommari allarmi del BPCS, pannelli locali, pannelli annunciatori di allarmi ad esempio) ;
- che eventuali sequenze eventi siano correttamente configurate;
- che il ripristino dei blocchi avvenga secondo quanto indicato nella specifica dei requisiti di sicurezza;
- che le eventuali funzioni di derivazione (by-pass) funzionino correttamente;
- che le procedure di manutenzione riportino gli intervalli di prova periodica;
- che le funzioni diagnostiche del SIS ed i relativi allarmi funzionino correttamente;
- che in caso di perdita, e di successivo ritorno, delle fonti di alimentazione il SIS si comporti come richiesto dalla specifica dei requisiti di sicurezza;
- che i requisiti relativi alla immunità elettromagnetica, EMC, siano stati rispettati.

15.2.5 Risultati della validazione del software

I risultati di validazione del software devono dimostrare che tutti i requisiti di sicurezza specificati in 12.2 della CEI EN 61511-1 sono correttamente soddisfatti.

15.2.6 Risultati della validazione del SIS

L'esecuzione delle varie attività di validazione e dei relativi risultati dovrà essere registrata mediante la compilazione di opportuni moduli di esecuzione attività debitamente controfirmati dalle figure chiave coinvolte nell'esecuzione delle stesse.

Il modulo di registrazione o certificazione dell'esecuzione di una attività di validazione dovrà, come minimo contenere le seguenti informazioni:

- identificativo e versione del piano di validazione utilizzato;
- tipo di attività di validazione effettuata con riferimento alla procedura/istruzione;
- identificativo dei componenti soggetti all'attività;
- riferimento alle specifiche ed ai disegni necessari per l'esecuzione dell'attività;
- elenco dettagliato delle verifiche effettuate a controllo della corretta esecuzione dell'attività con riportato il risultato di ciascuna verifica a confronto con il relativo risultato atteso (riportato nella procedura di esecuzione dell'attività in oggetto);
- elenco degli strumenti di misura impiegati per la verifica dell'attività, il cui elenco almeno il modello, la matricola ed il suo numero di certificato di taratura.
- indicazione di attività completata, oppure da completarsi; in questo secondo caso andranno elencate in dettaglio le attività a completamento che dovranno essere svolte affinché si possa ritenere conclusa l'attività.

15.2.7 Risultati discrepanti

Nel caso insorgessero discrepanze tra il risultato ottenuto ed il risultato atteso, allora si renderebbe necessaria una ri-analisi ad un passo precedente del ciclo di vita in sicurezza e si dovrà darne evidenza sul modulo/certificato di tale decisione, mentre se si rendessero necessarie delle richieste di modifica si dovrebbero seguire le indicazioni riportate successivamente all'articolo 17.

15.2.8 Azioni dopo la validazione del SIS

Al termine delle attività di validazione e prima che nell'impianto siano presenti le cause di rischio che il SIS ha il compito di mitigare, si dovranno:

- riportare tutte le derivazioni (by-pass) nella loro posizione normale;
- rimuovere tutte le eventuali forzature di segnali e dovrà essere inibita la possibilità di ulteriori forzature di segnali;
- riportare tutte le valvole di isolamento nella posizione contemplata dalle procedure di avviamento (start-up);
- rimuovere tutti gli eventuali fluidi e materiali utilizzati per le prove.

16 Esercizio e manutenzione del SIS

16.1 Obiettivi

Gli obiettivi della conduzione e manutenzione del SIS sono i seguenti:

- assicurare che il SIL richiesto per ogni funzione strumentata di sicurezza è mantenuto durante il funzionamento e la manutenzione;
- esercire e manutenere il SIS in maniera tale che la sicurezza funzionale della concezione sia mantenuta.

16.2 Requisiti

16.2.1 Pianificazione della manutenzione

La pianificazione della manutenzione dovrebbe prevedere i punti seguenti:

- le attività di funzionamento normali ed anormali;
- le attività di prove di efficienza periodiche;
- le attività di manutenzione preventiva e di riparazione;
- le procedure e le tecniche da usare per il funzionamento e la manutenzione;
- le persone, i dipartimenti e le organizzazioni responsabili di queste attività;
- la formazione e l'addestramento del personale di manutenzione;
- la differenziazione della competenza del personale per manutenere diversi SIL;
- le misure di compensazione effettuate per mantenere l'integrità dei diversi SIL;
- l'analisi periodica dei dati e risultati di manutenzione conseguiti.

16.2.2 Procedure di manutenzione

Le procedure di funzionamento e di manutenzione devono essere sviluppate in accordo con la pianificazione della sicurezza e devono fornire i punti seguenti:

- le azioni periodiche che devono essere effettuate allo scopo di mantenere la sicurezza funzionale del SIS "come concepito";
- le azioni e le costrizioni necessarie per prevenire uno stato di non sicurezza e/o per ridurre le conseguenze di un evento pericoloso durante la manutenzione;
- le informazioni che necessitano di essere mantenute relativamente ai risultati delle verifiche e delle prove effettuate sul SIS;
- le procedure di manutenzione da seguire quando avvengono anomalie o guasti nel SIS, incluse le procedure per rapportare ed analizzare i guasti;
- l'assicurazione che le apparecchiature di prova utilizzate durante le attività normali di manutenzione siano correttamente tarate e mantenute.

16.2.3 Procedure di riferimento

Verificare in tutte le condizioni di funzionamento e di manutenzione che il SIS operi secondo le procedure di riferimento per le quali è stato concepito e progettato.

16.2.4 Procedure di operatività in presenza di bypass

Nessuna ulteriore guida.

16.2.5 Procedure di manutenzione e operatività

Nessuna ulteriore guida.

16.2.6 Formazione del personale

Gli operatori devono essere formati sul funzionamento e sulla manutenzione del SIS almeno sui punti seguenti:

- comprensione dei differenti livelli di integrità di sicurezza SIL;
- conoscenza delle differenti funzioni strumentate di sicurezza SIF;
- comprensione dello specifico funzionamento del sistema strumentato di sicurezza SIS e da quali potenziali pericoli protegge l'impianto;
- conoscenza dei punti di intervento (trip) e l'azione risultante che è presa dal SIS;
- comprensione del funzionamento di tutti i commutatori di derivazione (by-pass) ed in quali circostanze queste derivazioni devono essere utilizzate;

- funzionamento dei commutatori di fermata manuale e delle attività di avviamento ed in quali circostanze questi commutatori manuali devono essere attivati;
- spiegazione del comportamento da tenere quando l'attivazione di un allarme di diagnostica qualsiasi (per esempio, quale azione deve essere intrapresa quando un allarme del SIS è avvenuto ed indica che vi è un problema nel SIS).

16.2.7 Autorizzazione e registrazione dei bypass

Nessuna ulteriore guida.

16.2.8 Addestramento del personale

Il personale di manutenzione deve essere formato in maniera adeguata per mantenere le prestazioni funzionali globali del SIS (hardware e software) ai loro obiettivi di integrità e per tale scopo deve essere preferibilmente addestrato:

- sullo stesso SIS in fase di prove di accettazione in fabbrica (FAT);
- sullo stesso SIS in fase di prove di accettazione in sito (SAT);
- diversamente su simulatori di processi analoghi.

16.2.9 Discrepanze di funzionamento

Le discrepanze tra il comportamento atteso ed il comportamento reale del SIS devono essere analizzate e, dove necessario, devono essere fatte delle modifiche in maniera tale che la sicurezza richiesta sia mantenuta.

16.2.10 Revisione delle procedure

Le procedure di funzionamento e di manutenzione possono richiedere revisioni, a seguito delle verifiche funzionali e delle prove periodiche sul SIS.

16.2.11 Procedure per le prove periodiche

Queste procedure devono essere scritte e sviluppate perché in generale ogni SIF possa rilevare:

- il funzionamento corretto per ogni sensore ed elemento finale;
- l'azione logica corretta;
- gli allarmi e le segnalazioni corrette.

16.2.12 Identificazione parti di ricambio del SIS

Nessuna ulteriore guida.

16.2.13 Revisione operatività e manutenzione del SIS

Nessuna ulteriore guida.

16.2.14 Suggerimenti per le procedure per le prove periodiche

In particolare si dovrebbero condurre delle prove funzionali per verificare almeno:

- la funzionalità di tutti i dispositivi di ingresso;
- le soglie di intervento di ogni ingresso;
- la logica associata ad ogni ingresso;
- la logica associata a più ingressi;
- le logiche e le funzioni di allarme;
- la corretta sequenza della logica;
- la velocità di risposta del SIS;

- la funzionalità di tutti gli elementi finali;
- il tempo di risposta degli elementi finali;
- i mezzi manuali per portare il sistema in uno stato sicuro;
- le funzioni di auto diagnostica;
- la funzionalità completa del SIS;
- la funzionalità del SIS dopo le prove.

16.3 Prove periodiche ed ispezioni

16.3.1 Prove periodiche

Le prove periodiche devono essere condotte utilizzando una procedura scritta (vedere 16.2.8) per evidenziare le anomalie non rilevate dalla diagnostica che impediscono al SIS di funzionare in accordo con la specificazione dei requisiti di sicurezza.

La frequenza delle prove periodiche deve essere quella che è stata decisa utilizzando il calcolo della PFD_{avg}.

Periodicamente (a intervalli determinati dall'utilizzatore) la frequenza di prova deve essere rivalutata sulla base di diversi fattori, inclusi dati di prova storici, esperienze di impianto, degradazione dell'hardware ed affidabilità del software.

16.3.2 Ispezioni

Ogni SIS deve essere periodicamente ispezionato visivamente, per assicurare che vi sia nessun cambiamento non autorizzato e nessun deterioramento osservabile (per esempio, bulloni o coperchi di strumenti mancanti, staffe arrugginite, fili scoperti, condutture rotte, tracciature di calore rotte, e mancanza di isolamento).

16.3.3 Documentazione delle prove periodiche ed ispezioni

L'utilizzatore deve conservare le registrazioni che attestano che le prove periodiche e le ispezioni sono state realizzate come richiesto e deve registrare almeno:

- la descrizione delle prove e delle ispezioni effettuate;
- le date delle prove e delle ispezioni;
- il nome della(e) persona(e) che ha (hanno) effettuato le prove e le ispezioni;
- il numero di identificazione del sistema provato (per esempio, numeri di linea "loop", numero di targa, numero di apparecchiatura, e numero di SIF);
- i risultati delle prove e delle ispezioni (per esempio, condizioni di "come trovato" e "come lasciato").

17 Modifica del SIS

17.1 Obiettivi

Gli obiettivi di questo articolo sono i seguenti:

- assicurare che le modifiche di ogni SIS siano correttamente pianificate, revisionate ed approvate prima di procedere alla modifica; e
- assicurare che l'integrità di sicurezza richiesta del SIS sia mantenuta nonostante ogni modifica fatta sul SIS.

17.2 Requisiti

Prima di effettuare ogni modifica al sistema strumentato di sicurezza, le procedure di autorizzazione e di controllo delle modifiche devono essere disponibili e devono includere un metodo chiaro per identificare il lavoro richiesto, le competenze richieste ed i pericoli che possono derivare.

Preliminarmente deve essere condotta una analisi per determinare l'impatto sulla sicurezza funzionale, come risultato della modifica proposta e quando l'analisi dimostra che la modifica proposta avrà un impatto sulla sicurezza, si deve ritornare alla prima fase del ciclo di vita in sicurezza influenzato dalla modifica.

La necessità di modifica potrebbe essere richiesta per i motivi seguenti:

- cambiamento delle soglie di intervento (trip);
- cambiamento delle condizioni di processo (set-point);
- variazione della legislazione di riferimento;
- variazione della specificazione dei requisiti di sicurezza;
- correzioni di errori del software incorporato o applicativo;
- variazione della revisione del software;
- prevenzione di guasti sistematici;
- riduzione di intervento del SIS.

La procedura di modifica deve essere scritta e deve includere almeno le informazioni seguenti:

- una descrizione della modifica e il motivo del cambiamento;
- i pericoli identificati che possono essere presi in considerazione;
- una analisi dell'impatto dell'attività di modifica sul SIS;
- tutte le approvazioni richieste per i cambiamenti;

A seguito della modifica deve essere redatto un rapporto di intervento che include almeno le informazioni seguenti:

- uno storico della configurazione modificata;
- le prove utilizzate per verificare che la modifica è stata correttamente implementata e che il SIS funziona come richiesto;
- le prove utilizzate per verificare che la modifica non ha introdotto un effetto avverso sulle parti del SIS (o su altri sistemi) che non sono state modificate.

18 Dismissione del SIS

18.1 Obiettivi

Gli obiettivi di questo articolo sono i seguenti:

- assicurare che prima della dismissione del servizio attivo di ogni SIS, che una revisione appropriata sia stata condotta e che sia stata ottenuta l'autorizzazione richiesta; e
- assicurare che le funzioni strumentate di sicurezza richieste, rimangano operative durante le attività di dismissione.

18.2 Requisiti

Prima di effettuare la dismissione devono essere disponibili le procedure di autorizzazione che devono includere un metodo chiaro per identificare il lavoro richiesto e per identificare i pericoli che possono derivare.

Preliminarmente deve essere effettuata una analisi per valutare l'impatto sulla sicurezza funzionale come risultato dell'attività di dismissione proposta.

Tale analisi deve includere una aggiornata valutazione del pericolo e del rischio, sufficiente per determinare l'ampiezza e la profondità, che le fasi successive del ciclo di vita in sicurezza devono aver bisogno di coprire.

La valutazione deve inoltre considerare:

- la sicurezza funzionale durante l'esecuzione delle attività di smantellamento; e
- l'impatto della dismissione del SIS sulle adiacenti unità e servizi di impianto.

19 Requisiti relativi alle informazioni ed alla documentazione

19.1 Obiettivi

Nessuna ulteriore guida.

19.2 Requisiti

Nessuna ulteriore guida.

19.3 Esempio di strutturazione della documentazione

La Figura 10 riporta una tipica esemplificazione della documentazione partendo da:

- i requisiti di riduzione del rischio;
- la regolamentazione legale;
- la normazione tecnica;
- la tecnologia sviluppata,

per produrre la descrizione documentale delle diverse fasi di sviluppo del SIS, dalla sua concezione, alla sua istallazione, verificazione, modificazione e dismissione.

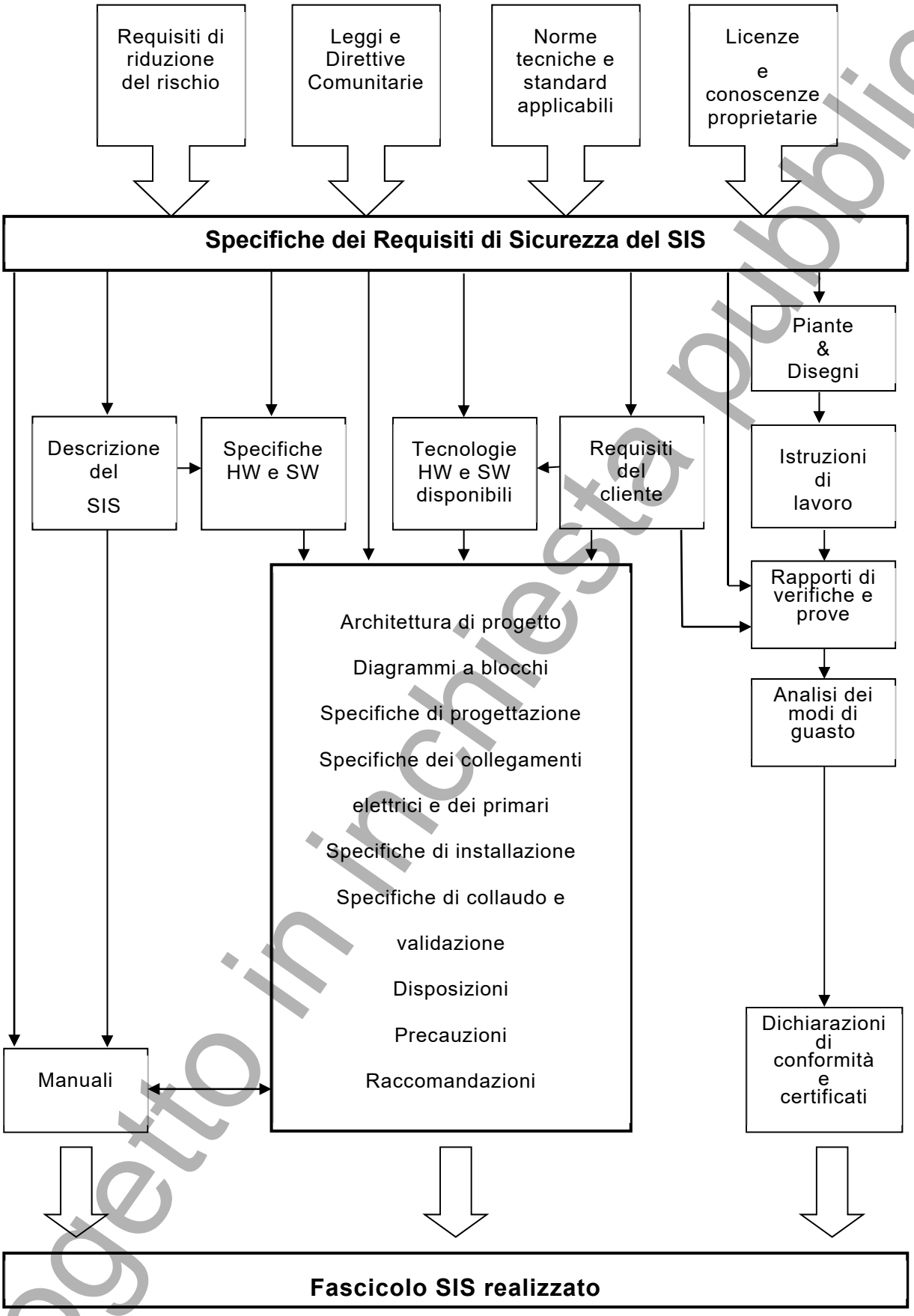


Figura 10 – Tipica possibile strutturazione della documentazione del SIS

Allegato A

Sviluppo delle fasi del ciclo di vita in sicurezza per un piccolo impianto (dalla individuazione dei rischi alla definizione del sistema strumentato di sicurezza)

A.1 Premessa

La sicurezza negli impianti si ottiene con la stratificazione successiva di sistemi di prevenzione e protezione: in questo modo, i potenziali pericoli sono limitati da sistemi di natura diversa che intervengono in caso di fallimento dei sistemi degli strati sottostanti (vedasi Figura A.1), e, normalmente, le azioni dei sistemi di sicurezza aumentano di "intensità" a mano a mano che si passa da uno strato inferiore a quello superiore, fino ad arrivare all'evacuazione del personale.

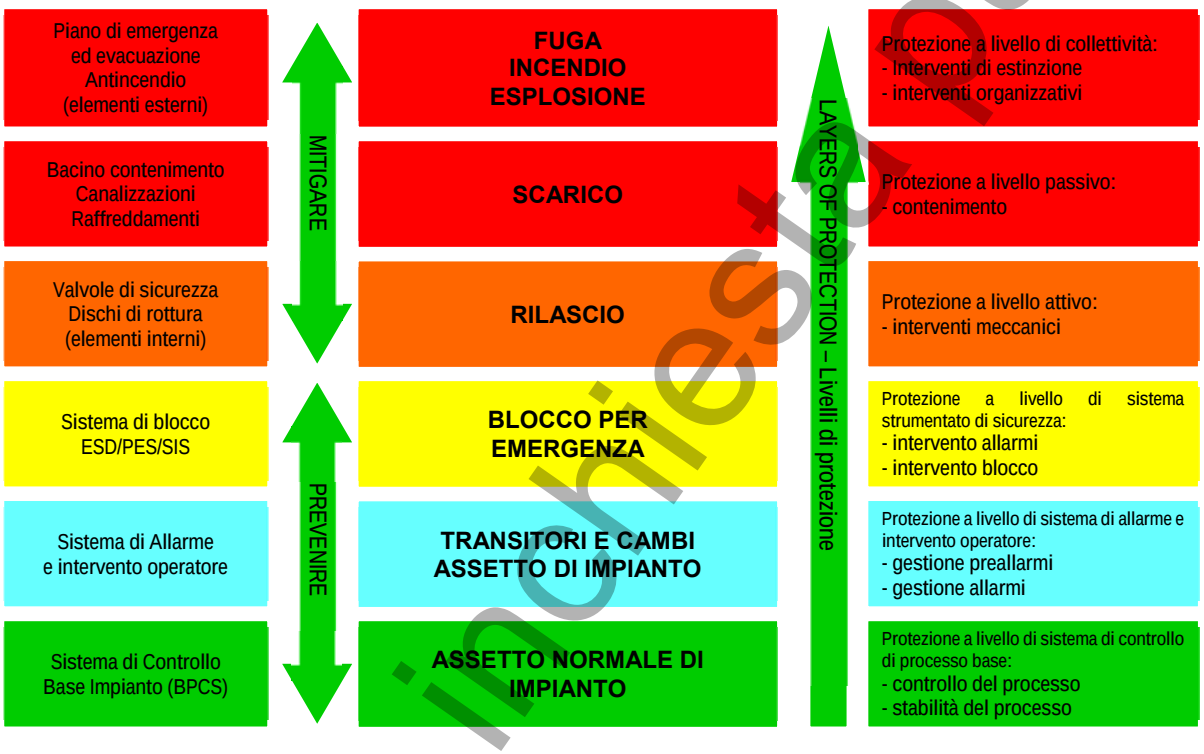


Figura A.1 - Stratificazione dei sistemi di protezione degli impianti industriali

Per esempio, le azioni del Sistema di Controllo di Processo Base (BPCS) sono normali azioni di regolazione, e, nel caso il processo sfugga al sistema di controllo BPCS, interviene dapprima il sistema di allarme che allerta l'operatore, che dovrà intervenire per portare l'impianto in condizioni di sicurezza; se però anche il sistema di allarme fallisce interviene il sistema di blocco ESD/PES, ovvero il Sistema Strumentato di Sicurezza (SIS), che comporta il blocco di una parte di impianto con conseguenti interruzioni del processo e, quindi, perdite economiche.

Gli strati successivi di intervento sono:

- di tipo meccanico, di protezione per rilascio (valvole di sicurezza);
- di tipo contenimento, di protezione per scarico (bacini e canalizzazioni);
- di tipo organizzativo per emergenza ed evacuazione (e con sistemi antincendio).

I Sistemi Strumentati di Sicurezza (SIS) sono normalmente del tipo E/E/PES (Sistemi Elettrici/Elettronici/Elettronici Programmabili) disciplinati in applicazioni generali dalla CEI EN 61508 e nell'industria di processo dalla CEI EN 61511.

Per sistema E/E/PES si intende quella catena di componenti che va dal sensore in campo (trasduttore o trasmettitore) al risolutore logico in sala controllo (Logic Solver: Logica cablata - relè - o programmabile - PLC) e quindi all'elemento finale in campo (valvola e attuatore).

Il sistema E/E/PES che realizza le funzioni di sicurezza del SIS è caratterizzato da un valore di SIL (Livello di Integrità di Sicurezza) che può variare da SIL 1, per impianti poco pericolosi, a SIL 4, per impianti ad alto rischio (che riducono il manifestarsi potenziale delle conseguenze dei rischi pericolosi rispettivamente di almeno 10 e 10 000 volte (Vedasi Tabella A.2)); al crescere del SIL aumentano ovviamente i costi economici, ingegneristici ed organizzativi per la realizzazione del sistema di sicurezza.

Risulta pertanto evidente che è fondamentale una corretta valutazione dei requisiti di sicurezza necessari per l'impianto o per l'Apparecchiatura sotto Controllo (EUC), secondo un approccio sistematico della concezione e progettazione dei SIS riportata nelle normative seguenti:

- CEI EN 61508, per le applicazioni comuni nell'industria in genere;
- CEI EN 61511, per le applicazioni particolari nell'industria di processo;

che prevedono un Ciclo di Vita in Sicurezza (Safety Life Cycle), che congloba anche l'installazione, l'avviamento, l'esercizio, la manutenzione fino alla dismissione dell'impianto.

Tutte le attività devono essere condotte secondo un Piano di Sicurezza (Safety Plan) che contempla tutte le fasi del ciclo di vita in sicurezza, ovvero almeno le principali seguenti:

1) individuazione dei rischi associati alla gestione dell'impianto di processo;
2) valutazione della riduzione del rischio per portarlo a un livello tollerabile;
3) individuazione delle eventuali funzioni strumentate di sicurezza (SIF);
4) determinazione dei livelli di integrità di sicurezza (SIL) delle SIF;
5) definizione dei componenti dei sistemi strumentati di sicurezza (SIS);
6) progettazione e realizzazione dei SIS;
7) installazione e avviamento dei SIS;
8) validazione funzionale dei SIS;
9) conduzione, manutenzione e modificazione dei SIS;
10) dismissione finale dei SIS.

Il sistema strumentato di sicurezza si compone solitamente dei seguenti elementi:

- sensori di misura : Sensors
- risolutore logico : Logic solver
- elementi finali : Final elements

Scopo di questo Allegato è di definire, a fronte dei rischi potenziali di un piccolo impianto, la necessaria funzione strumentata di sicurezza SIF, il necessario livello di integrità di sicurezza SIL e il relativo sistema strumentato di sicurezza SIS che ne implementa la funzionalità e la sicurezza (e pertanto sviluppare le prime 5 attività), fornendo nel contempo una pratica esemplificazione procedurale ed operativa.

Per impianti più complessi e per un generale approfondimento di tutte le altre attività correlate alla sicurezza, si faccia riferimento al testo completo della Guida e agli ulteriori Allegati proposti nel prosieguo.

A.2 Individuazione, quantificazione e classificazione dei rischi

Individuazione dei rischi

Una fase fondamentale del ciclo di vita del sistema strumentato di sicurezza consiste nell'identificazione delle fonti di rischio nell'impianto cui il SIS è destinato e nella quantificazione dei relativi rischi.

Tale attività comporta un'analisi preliminare dei possibili rischi e pericoli, sia di origine interna all'impianto, sia di origine esterna, secondo la metodologia **Preliminary Risk Analysis (PRA)**

Tale analisi deve essere:

- Sistematica;
- Razionale;
- Completa;
- Documentata.

La metodologia utilizzata si basa sul lavoro di gruppo di diversi esperti con differenti esperienze e competenze e può essere sviluppata secondo i due seguenti approcci.

- **HAZOP (considera le deviazioni del processo)**
- **FMEA (considera i guasti dei componenti)**

I due approcci sono di tipo qualitativo e discorsivo e non fanno ricorso a tecniche matematiche.

L'approccio **HAZOP (Hazard and Operability Study)** considera la funzione che un particolare elemento dell'impianto svolge nel processo e viene applicato linea per linea (sistematicità), formulando delle domande basate sulle "parole guida" applicate a tutte le variabili della linea (con completezza).

Parole guida per l'analisi

- niente, assenza di
- troppo (più del necessario)
- troppo poco
- oltre che, in aggiunta
- invece di, diverso da
- il contrario, l'opposto di

Variabili di processo

- temperatura
- pressione
- portata
- livello

L'approccio **FMEA (Failure Mode Effect Analysis)** si basa invece sul quesito:

"Cosa succede se…? (What if …?)":

- decomposizione dell'impianto o apparecchiatura nei suoi componenti fisici;
- analisi delle modalità di guasto elemento per elemento, valutando per ogni possibile guasto quali sono le manifestazioni e le conseguenze, e le possibili contromisure.

Quantificazione dei rischi

La fase successiva all'individuazione e analisi qualitativa dei pericoli è la quantificazione del rischio associato.
Il rischio **(R)** associato ad un dato evento, che comporti un danno, può essere descritto attraverso un calcolo probabilistico che considera i seguenti fattori:

(F) frequenza attesa dell'evento (espressa normalmente in numero di eventi all'anno)

(M) magnitudo (ampiezza) del danno dell'evento considerato: si può esprimere con varie "unità di misura" (morti, feriti, euro, dollari)

R = F x M

Mentre la frequenza attesa può essere stimata o mutuata in base a esperienze su impianti uguali o similari, la magnitudo può essere quantificata riferendosi alle diverse conseguenze dell'evento, che vanno dal danno alle cose, alla morte di persone; questa quantificazione è però molto complessa, essendo difficile definire una unità di misura che renda comparabili eventi con conseguenze diverse.

Comunque, ricavando dalla formula del rischio R = F x M, la frequenza F, mantenendo costante il rischio R, si ottiene una iperbole. Dalla formula del rischio si evince ovviamente che sono considerati egualmente rischiosi eventi catastrofici ma poco frequenti, esempio 10 000 morti ogni 100 anni, ed eventi molto frequenti di bassa magnitudo, esempio 100 incidenti anno ognuno dei quali causa 1 morto.

Per penalizzare comunque gli incidenti catastrofici si può usare una espressione:

$R = F \times M^n$ con $n > 1$

Essendo il rischio (R) funzione di due fattori: Frequenza (F) e Magnitudo (M), la sua riduzione si ottiene:

- riducendo F con la Prevenzione
- riducendo M con la Protezione

- La **Frequenza** di accadimento di eventi dannosi si riduce con opere di prevenzione (per esempio, sistemi SIS), cioè con azioni che impediscano all'impianto il raggiungimento delle condizioni di pericolo.

  Per esempio, un sistema di rivelazione gas (Fire Gas System: FGS), è un sistema di prevenzione che rivela, con allarme, una concentrazione anomala di gas prima che questa raggiunga il livello minimo di esplosività.

- La **Magnitudo** si riduce con opere di protezione, che mitigano le conseguenze degli eventi.

  Per esempio, un sistema di protezione incendio (Fire Protection System: FPS), è invece un sistema automatico di spegnimento che interviene quando l'incendio è già in atto, limitandone però le conseguenze.

A.3 Valutazione della riduzione di rischio necessaria

Generalità

La riduzione necessaria del rischio è la riduzione che deve essere realizzata per conformarsi al rischio tollerabile (livello di sicurezza obiettivo del processo) per una specifica situazione di impianto.

La Figura A.2 evidenzia:

- il **Rischio del processo**, ovvero il rischio esistente per gli eventi specificati per il processo, per il sistema di controllo di processo base e per i fattori umani, senza considerare nessuna funzione di protezione di sicurezza.
- il **Rischio tollerabile**, ovvero il livello di sicurezza obiettivo del processo, che è accettato in un dato contesto in relazione a valori fissati dalla società.
- il **Rischio residuale**, ovvero il rischio di un evento pericoloso dopo l'aggiunta delle funzioni di protezione di sicurezza.

Il rischio del processo normalmente dipende dal rischio intrinseco del processo, ma tiene anche in considerazione la riduzione del rischio del suo sistema di controllo di processo base (BPCS).

Inoltre, la Figura A.2 illustra i possibili mezzi di protezione che possono essere utilizzati per ridurre la frequenza dell'evento pericoloso (prevenzione) e/o le sue conseguenze (protezione) ad un livello di rischio residuale, inferiore a quello tollerabile per il processo.

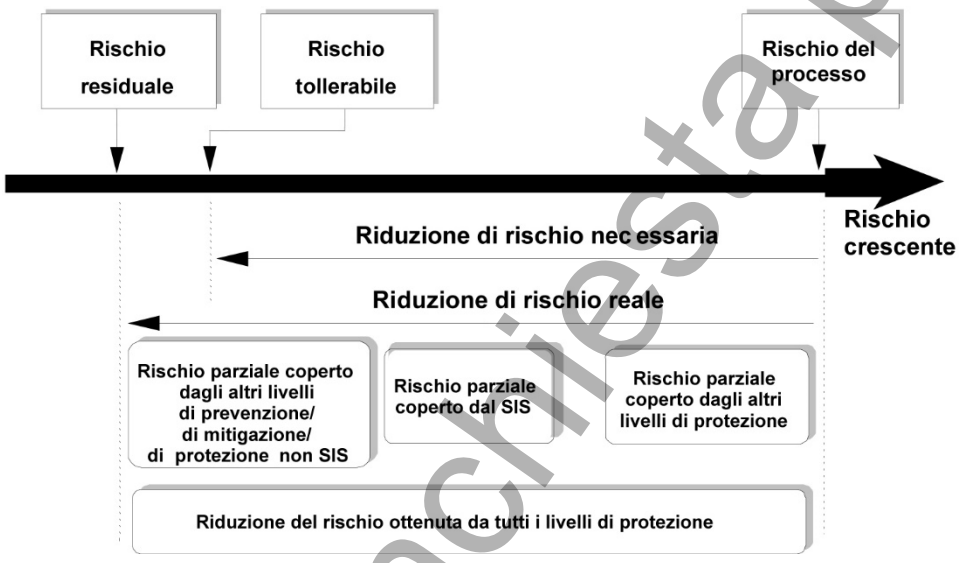


Figura A.2 – Concetti generali sulla riduzione del rischio

Analisi preliminare dei rischi

L'analisi del rischio del processo può portare tipicamente a queste conclusioni (vedasi Figura A.3):

a) il rischio è così grande da essere inaccettabile; o

b) il rischio è, o è stato reso, così piccolo da diventare trascurabile; o

c) il rischio si pone tra i due punti sopra riportati a) e b) ed è, o è stato ridotto fino al livello più basso possibile, tenendo in considerazione sia i vantaggi raggiunti e sia i costi necessari per ogni ulteriore riduzione.

Con riferimento al punto c), la metodologia ALARP raccomanda di ridurre i rischi finché "ragionevolmente praticabile" o, in altri termini, fino ad un livello "basso quanto praticabile" (As Low As Reasonably Practicable - ALARP).

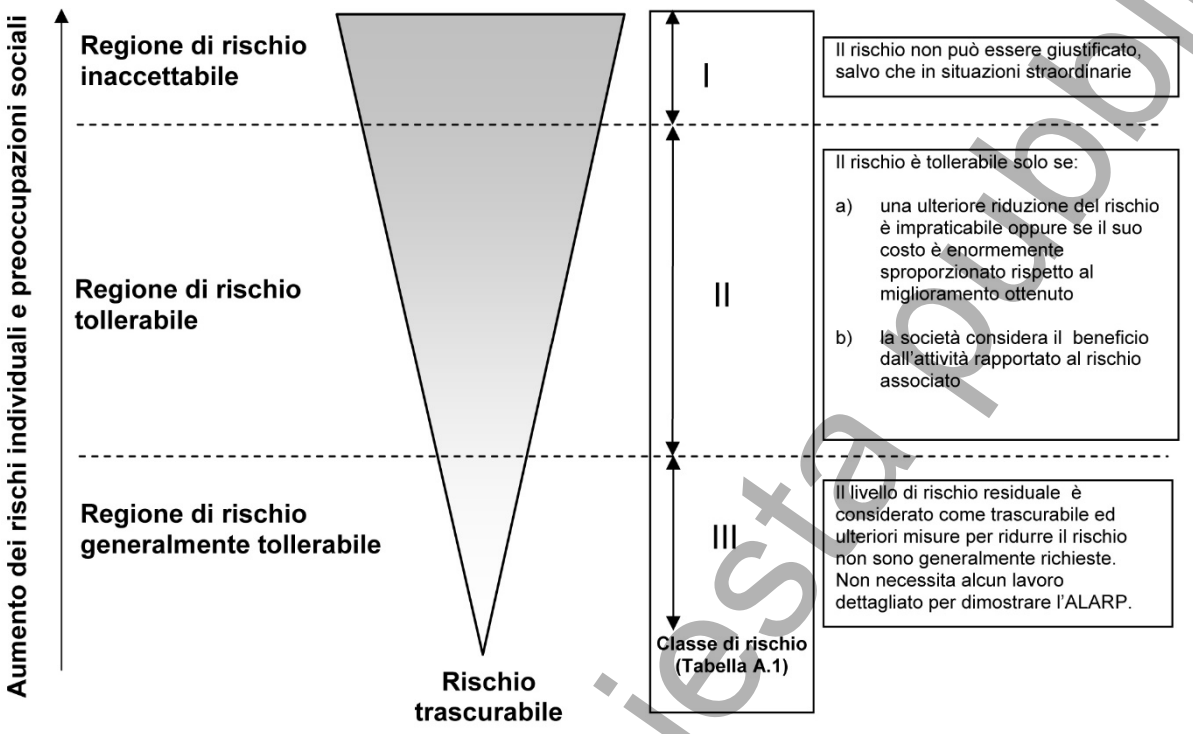


Figura A.3 – Regione dei rischi e metodologia ALARP

Classificazione generale dei rischi

Per poter applicare il principio ALARP, è necessario definire le 3 regioni della Figura A.3 in termini di probabilità e di conseguenza di un incidente, ovvero in altrettanti classi di rischio:

- la classe di rischio I che si situa nella regione inaccettabile;
- la classe di rischio II che si situa nella regione ALARP;
- la classe di rischio III che si situa nella regione generalmente tollerabile.

Questa classificazione dovrà essere oggetto di una discussione e di un accordo tra le parti interessate, per esempio: le autorità competenti nei confronti della sicurezza (comuni, regioni, stato), i responsabili degli impianti (aziende, società), i lavoratori e le comunità esposte ai rischi.

La Tabella A.1 permette di determinare la classe di rischio (I, II, o III) utilizzando il concetto ALARP, in funzione della probabilità dell'evento pericoloso e della gravità della conseguenza.

Tabella A.1 – Esempio di classificazione dei rischi

Probabilità evento pericoloso	Classe di rischio			
	Conseguenza catastrofica	Conseguenza critica	Conseguenza marginale	Conseguenza trascurabile
Molto probabile (> 1/y)	I	I	I	II
Probabile (< 1/y)	I	I	II	II
Possibile (<0,1/y)	I	II	II	II
Remota (<0,01/y)	II	II	II	III
Improbabile (<0,001/y)	II	III	III	III
Incredibile (<0,0001/y)	II	III	III	III

La Tabella A.1 fornisce comunque solo una classificazione potenziale dei rischi fornendo implicitamente la richiesta di una funzione strumentata di sicurezza (SIF) per portare la classe di rischio inaccettabile I almeno nella regione tollerabile con classe di rischio II, però non fornisce esplicitamente il livello di integrità di sicurezza (SIL) della SIF che dovrà essere determinata mediante una ulteriore analisi quantitativa o almeno qualitativa dei rischi potenziali.

Determinazione qualitativa del SIL

Una semplice analisi qualitativa dei rischi potenziali dell'impianto che può invece determinare anche il relativo livello di integrità di sicurezza SIL richiesto, è il metodo qualitativo a grafo di rischio introdotto dalla norma tedesca DIN 19250 e riportato anche come possibile metodo dalla CEI EN 61511-3.

Tale metodo si basa sul concetto di un insieme di classi dei requisiti, che stabilisce il legame tra livello di rischio e le misure da adottare per prevenire e controllare gli effetti dannosi.

Le classi dei requisiti sono 8 (Figura A.4 che riporta anche l'equivalente SIL)

Il valore minimo è AK 1, per applicazioni a rischio minimo, fino alla classe AK 8, per le applicazioni a rischio estremo.

Le classi AK (DIN) corrispondono a quelle internazionali SIL (IEC) come segue:

- AK 2, AK 3 ≡ SIL 1
- AK 4 ≡ SIL 2
- AK 5, AK 6 ≡ SIL 3
- AK 7 ≡ SIL 4
- AK 8 ≡ SIL 4 però con altre barriere di protezione

L'approccio DIN per definire la classe si basa sulla risposta a 4 domande:

C) Conseguenze del rischio:

- C1: ferite ad una persona
- C2: ferite gravi a più persone/morte di una persona
- C3: morte di alcune persone
- C4: parecchie persone morte (catastrofe)

F) Frequenza dell'esposizione al rischio:

- F1: da raramente a poco frequente
- F2: da frequente a continuo

P) Possibilità di sottrarsi all'incidente:

- P1: possibile a certe condizioni
- P2: difficilmente possibile

W) Probabilità dell'evento:

- W1: molto bassa
- W2: bassa
- W3: relativamente alta

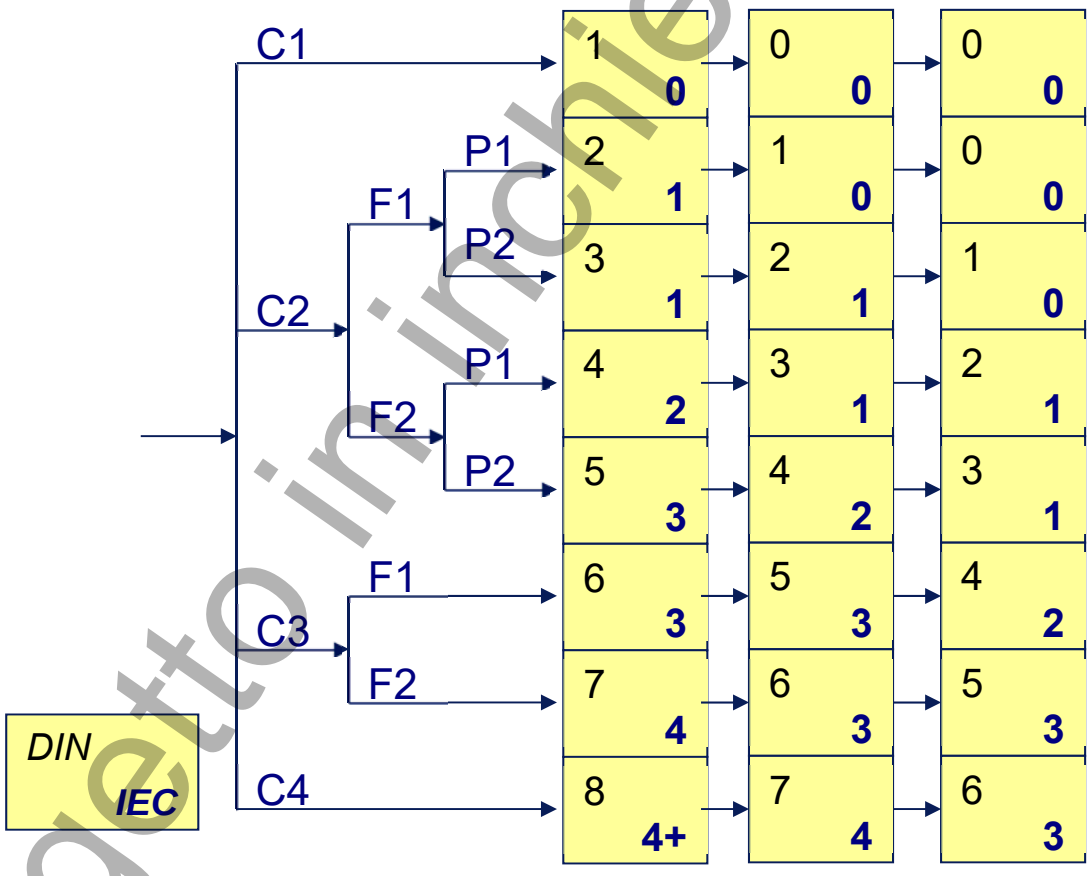


Figura A.4 - Schema per determinare le classi DIN 19250 (AK) e IEC 61511 (SIL)

NOTA - 0 significa nessuna classificazione SIL; 4+ significa SIL 4 con altre barriere di protezione

Esempio numerico sulla riduzione del rischio

Si ritiene un rischio accettabile (Ra) di incidenti pari a 10^{-6}/anno.

Se l'unità d'impianto analizzata ha un rischio di incidente (Ri) mortale pari a 1 su 1 000 anni, calcolato tenendo conto delle azioni preventive del sistema di controllo (BPCS: DCS o PLC) e dei sistemi di allarme e di sicurezza superiori, installando un SIS "infallibile" la probabilità di evento mortale tenderebbe a "zero" perché metterebbe l'unità in sicurezza ogni volta che il processo si avvicina alle condizioni pericolose.

Il SIS infallibile sarebbe quindi perfetto, ma la perfezione non esiste!
Si deve sempre prevedere che il sistema possa fallire l'intervento PFD: (Probability of Failure on Demand)

Se per ipotesi il SIS ha 1 probabilità di guasto ogni 1 000 richieste di intervento (PFD=10^{-3}), per ogni 1 000 possibili incidenti mortali, solo 1 sfugge al SIS e causa un "effettivo" incidente mortale.

Se l'unità ha inoltre un Ri di 1 su 1 000 anni, come supposto, per avere 1 000 possibili incidenti si dovrà aspettare 1 000 000 di anni e pertanto il rischio ridotto (Rr):

Rr = Ri x PFD = 10^{-3} x 10^{-3} = 10^{-6} (ovvero 1/1 000 000 anni).

Il sistema si può guastare in molti modi ma quello che interessa quantificare sono i guasti che inibiscono la funzione principale del SIS, che sono solo una aliquota di tutti i possibili guasti, e solitamente l'imperfezione del SIS si misura con la probabilità che un guasto latente impedisca la funzionalità del sistema in caso di necessità di intervento.

Quindi, il rischio ridotto (Rr) deve essere inferiore al rischio accettabile (Ra):

Ri x PFD $\leq$ Ra PFD $\leq$ Ra / Ri … PFD $\leq 10^{-3}$

In altre parole il SIS riduce il rischio di un fattore 1 / PFD:

Risk Reduction Factor = 1 / Probability of Failure on Demand

in questo caso RRF deve essere > 10^3 per soddisfare la richiesta iniziale.

A.4 Determinazione dei livelli di integrità delle funzioni di sicurezza

Generalità

Ogni strumento e quindi anche ogni funzione strumentata di sicurezza è soggetta a malfunzionamenti e/o guasti.

I guasti si possono suddividere in:

- **guasti sicuri** (di modo sicuro) quando le conseguenze del guasto provocano danni accettabili;
- **guasti pericolosi** (di modo pericoloso) quando le conseguenze del guasto provocano danni non accettabili.

Guasti sicuri

I guasti sicuri possono essere classificati in:

- palesi,
- attivanti,

e generano:

- perdite economiche,
- interventi dei sistemi di blocco (ESD) misurati in frequenza di interventi di blocco.

Guasti pericolosi

Quelli pericolosi possono essere classificati in:

- inibenti,
- nascosti,

e

- devono essere trovati con prove,
- possono impedire l'intervento delle funzioni di sicurezza,

in quanto comportano la perdita di vite ed apparecchiature, misurata come probabilità di guasto a richiesta d'intervento (PFD).

Comportamenti in casi di guasti

Comportamento Fail Safe:
Nel caso di guasto riconosciuto dalle misure passive o dall'autodiagnostica, il sistema si porta in uno stato sicuro (stabile).

Comportamento Fault Tolerant:
Nel caso di guasto riconosciuto dalle misure passive o dall'autodiagnostica, il sistema continua a funzionare con prestazioni ridotte, assicurando le funzioni critiche.

In assenza di riparazione, la protezione è attiva, ma un successivo guasto potrebbe avere *conseguenze pericolose.*

L'applicazione di sistema di sicurezza Fail Safe presuppone che il processo sia concepito per avere uno stato sicuro raggiungibile in caso di guasto o deenergizzazione del sistema di sicurezza.

L'esperienza maturata nell'industria di processo dimostra che i dispositivi utilizzati in modo da intervenire togliendo l'alimentazione hanno una percentuale di guasti di modo sicuro compresa tra il 60% ed il 90%.

Per questo motivo gli attuatori ed i sensori impiegati per la sicurezza sono "alimentati" quando l'impianto è operativo ed in caso di pericolo, l'impianto viene "fermato" e portato in sicurezza togliendo le fonti di alimentazione del sistema di sicurezza (energia elettrica ed aria alimentazione).

L'approccio **Fault Tolerant** si applica invece ai sistemi che non hanno uno stato di sicurezza predefinito, per cui tutti i guasti sono pericolosi ed il concetto di deenergizzazione non è applicabile.

L'approccio Fault Tolerant prevede che il componente guasto diventi ininfluente ai fini dell'operatività del sistema di sicurezza, e ciò comporta la ridondanza funzionale dei vari componenti del sistema basata su un algoritmo di votazione seguente:

- **La diagnostica è basata sul confronto dei risultati ottenuti tra due o più componenti funzionalmente uguali:** se la differenza tra i risultati dei diversi componenti esce dal campo di accettabilità significa che si ha un guasto.
- **In caso di guasto si scarta il risultato che non concorda con la maggioranza dei risultati:**
  questo significa che il confronto deve essere fatto tra almeno tre risultati, poiché il confronto tra due soli non permette di individuare quello sbagliato.

La copertura diagnostica e la frazione di guasti sicuri (DC e SFF)

*La **Diagnostic Coverage (DC)*** di un componente o sottosistema è definita come il rapporto tra rateo medio dei guasti casuali hardware dannosi ma rilevabili dalla autodiagnostica e rateo medio dei guasti casuali hardware dannosi totali (Figura A.6):

la Diagnostic Coverage non include i guasti rivelati durante le prove periodiche

$$DC = \sum \lambda_{DD} / \sum \lambda_D = \sum \lambda_{DD} / \left(\sum \lambda_{DD} + \sum \lambda_{DU} \right)$$

dove:

λ_D = rateo medio di guasti dannosi rilevabili o non dalla autodiagnostica (=λ_{DD}+λ_{DU})

λ_{DD} = rateo medio di guasti dannosi rilevabili (detected) dalla autodiagnostica

λ_{DU} = rateo medio di guasti dannosi non rilevabili (undetected) dalla autodiagnostica

La ***Safe Failure Fraction (SFF)*** di un componente o sottosistema è definito invece come il rapporto tra la somma del rateo medio dei guasti casuali hardware sicuri e dei guasti casuali hardware dannosi ma rilevabili, e il rateo medio dei guasti casuali hardware totali (sicuri e dannosi)

$$SFF = \left(\sum \lambda_S + \sum \lambda_{DD} \right) / \left(\sum \lambda_S + \sum \lambda_D \right) = \left(\sum \lambda_S + \sum \lambda_{DD} \right) / \left(\sum \lambda \right)$$

dove:

λ_S = rateo medio dei guasti sicuri (safety)

λ = rateo medio totale dei guasti sicuri e dannosi (=λ_S+λ_D)

Per i componenti e sottosistemi complessi (tipicamente PLC) si assume come realistica una ripartizione tra 50% di guasti sicuri (λ_S) e 50% di guasti dannosi (λ_D).

L'introduzione del concetto di SFF permette di fatto di rendere meno onerosi i vincoli sulle architetture imposti dalla Tabella 10 (ripresa dalle Tabelle 2 e 3 della 61508-2).

Infatti, assumendo realistica la ripartizione 50% tra guasti sicuri e guasti dannosi e assumendo per esempio che il 30% dei guasti dannosi sia rilevabile dall'auto diagnostica, si ha:

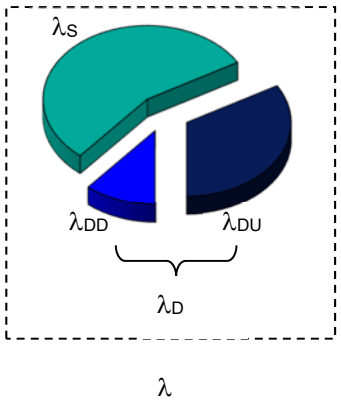
DC = 30%
e quindi applicando la formula precedente, si avrà:

SFF = (50% + [50% x 30%]) / (50% + 50%) = 65%
con un evidente guadagno sui vincoli imposti sulle architetture.

Elevando opportunamente la copertura diagnostica DC al 90% si ha invece:

SFF = (50% + [50% x 90%]) / (50% + 50%) = 95%

Ovviamente i valori di DC e di SFF per i componenti o sottosistemi che verranno usati in una catena di strumentazione per applicazioni di sicurezza dovranno essere dati dai Fornitori di Componenti e certificati da competenti Agenzie di Certificazione.



Definizione dei guasti

λ = rateo medio totale dei guasti sicuri e dannosi (=λ_S+λ_D)

λ_S = rateo medio dei guasti sicuri

λ_D = rateo medio di guasti dannosi (=λ_{DD}+λ_{DU})

λ_{DD}= rateo medio di guasti dannosi rilevabili dalla diagnostica

λ_{DU}= rateo medio di guasti dannosi non rilevabili dalla diagnostica

Parametri correlati

$$DC = \sum \lambda_{DD} / \sum \lambda_D$$

$$SFF = \left(\sum \lambda_S + \sum \lambda_{DD}\right) / \left(\sum \lambda_S + \sum \lambda_D\right)$$

Figura A.6 – Definizione dei guasti e parametri correlati

Definizione del Livello di Integrità di Sicurezza (SIL)

Nel caso in cui l'analisi del rischio del processo preveda una Funzione Strumentata di Sicurezza (SIF) per ridurre il rischio del processo in una regione accettabile o tollerabile, attraverso la Tabella 7 (che riporta le Tabelle 3 e 4 della IEC 61511-1), si può determinare il Livello di Integrità di Sicurezza (SIL) della Funzione Strumentata di Sicurezza (SIF).

Per una pratica esemplificazione di determinazione del SIL di una SIF vedasi nel prosieguo.

Definizione del Sistema Strumentato di Sicurezza (SIS)

Il Sistema Strumentato di Sicurezza (SIS) è il sistema che realizza le funzioni di sicurezza necessarie a garantire la sicurezza dell'Equipment Under Control (EUC), cioè del processo e/o dell'impianto, ed a mantenerlo in condizioni di sicurezza anche in caso di malfunzionamento del sistema di controllo di processo base (BPCS) e del sistema di osservazione e gestione allarmi (Figura A.7).

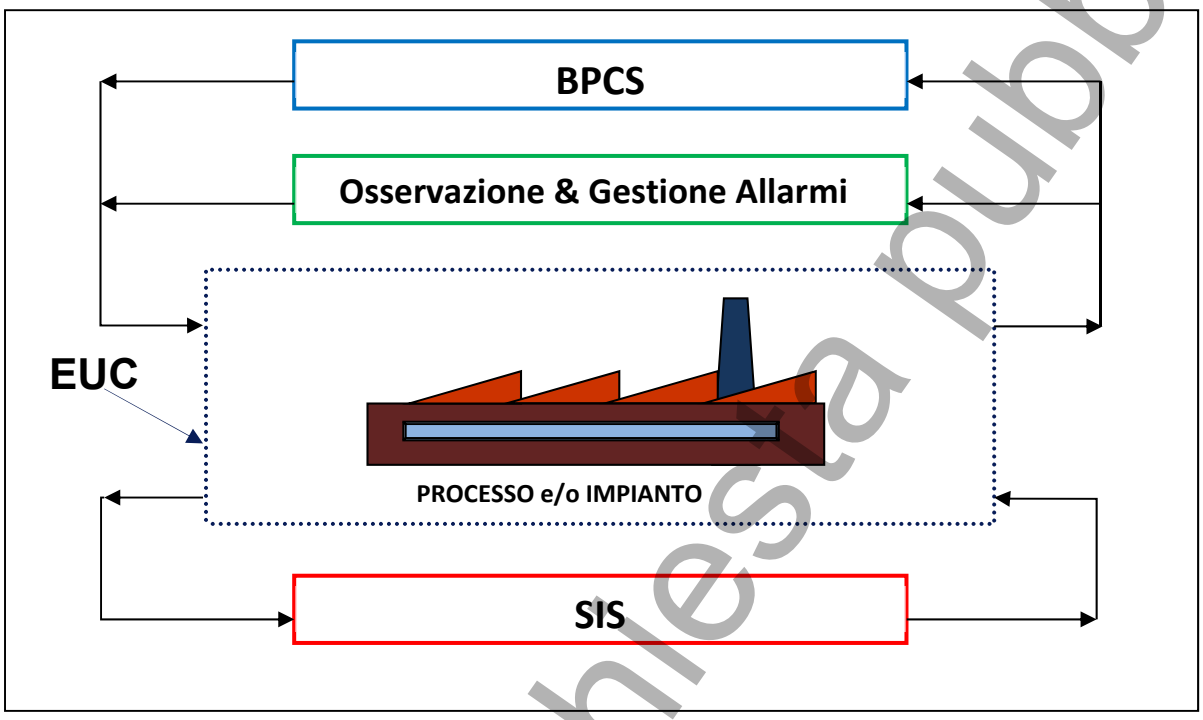


Figura A.7 – Illustrazione della definizione del Sistema Strumentato Sicurezza (SIS)

Le Tabelle 9 e 10 della presente Guida, specificano le tolleranze minime ai guasti o alle anomalie dell'hardware da adottare per i malfunzionamenti, per i diversi SIL e quindi, come predetto, sarà compito degli analisti e dei progettisti definire quale è il SIL ritenuto necessario per le diverse catene di strumentazione e dimostrare che la catena stessa è stata realizzata in modo da soddisfare le richieste.

Il progetto del sistema strumentato di sicurezza (SIS), non può quindi limitarsi a soddisfare i requisiti funzionali dettati dalle unità di processo ma deve soprattutto soddisfare i requisiti di integrità di sicurezza (SIL) individuati e richiesti per garantire che il processo funzioni sempre in uno stato sicuro.

A.5 Esempio di definizione di un Sistema Strumentato di Sicurezza (SIS)

Un SIS deve essere definito secondo le seguenti fasi (vedasi Figura A.8)

1. Valutazione preliminare del rischio interno ed esterno all'impianto PRA
2. Individuazione del rischio delle deviazioni del processo HAZOP
3. Riduzione del rischio attraverso una funzione di sicurezza SIF
4. Individuazione del livello di integrità di sicurezza della funzione SIL
5. Determinazione della probabilità media di guasto su domanda di intervento PFD
6. Individuazione dell'affidabilità e sicurezza della funzione o catena considerata SIS

allo scopo di portare il rischio in una regione accettabile di progettazione (attraverso per esempio la precitata metodologia ALARP) individuando la catena necessaria per tale scopo (loop), attraverso i suoi tipici elementi costitutivi:

- sensori di misura;
- risolutore logico;
- elementi finali,

i cui dati di affidabilità e disponibilità devono essere forniti dai costruttori e/o certificati da agenzie di certificazione preposte (per esempio: Offshore Reliability Databook).

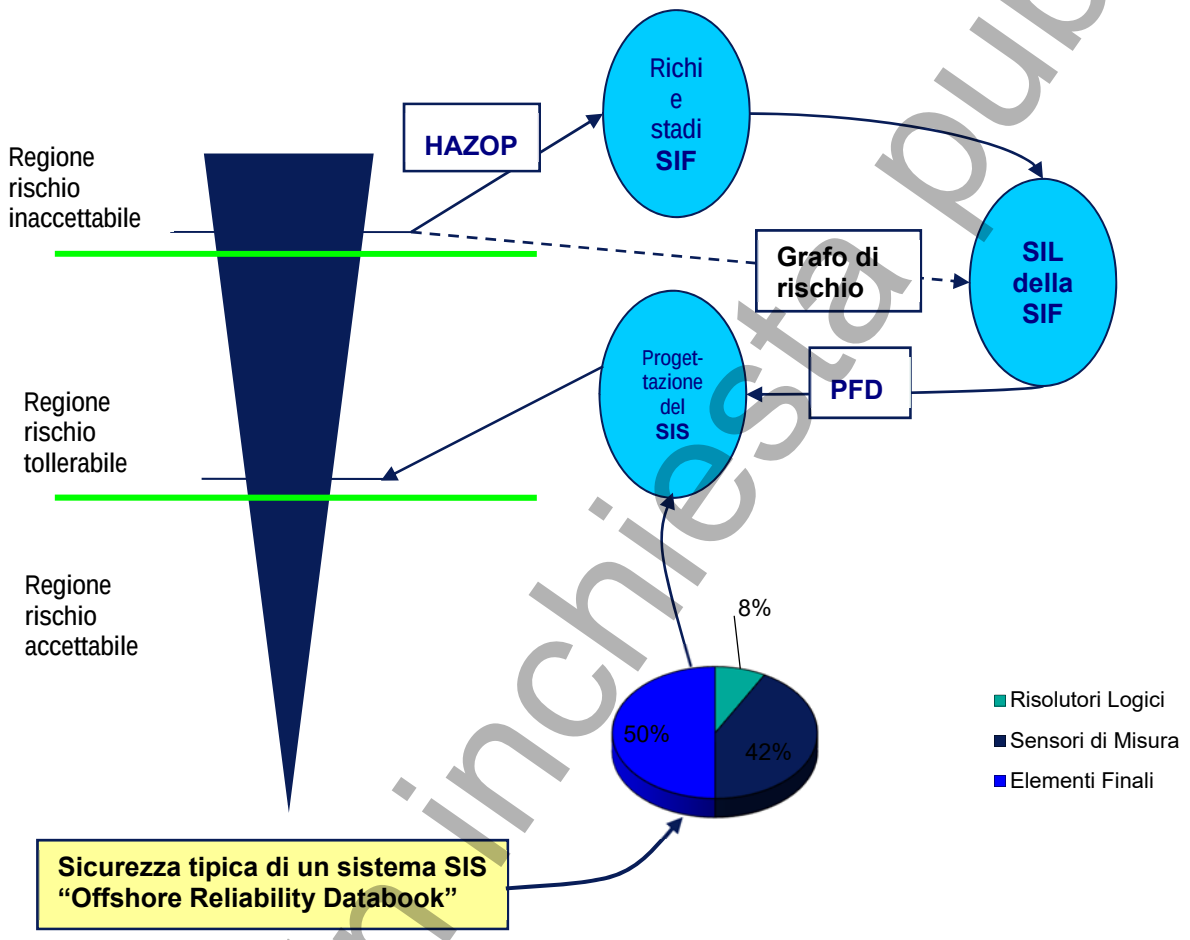


Figura A.8 – Sintesi della definizione di un Sistema Strumentato di Sicurezza (SIS)

Secondo l'Offshore Reliability Databook, la Probabilità di Guasto su Domanda (PFD) in Figura A.8 è dovuta tipicamente ai seguenti contributi:

- 42% per i sensori di misura
- 8% per i risolutori logici
- 50% per gli elementi finali

Nel caso dell'industria di processo, la Probabilità di Guasto su Domanda (PFD) del SIS è dovuta generalmente invece ai seguenti contributi (vedasi Figura A.9):

- PFD_S = 35% per i sensori di misura
- PFD_L = 15% per i risolutori logici
- PFD_{FE} = 50% per gli elementi finali

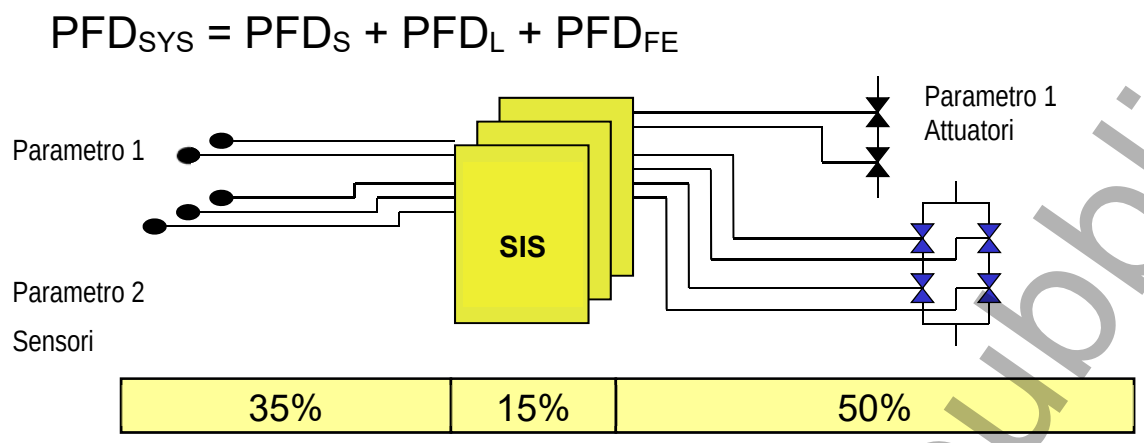


Figura A.9 – Tipici valori di PFD nell'industria di processo

Il grado di severità dei Livelli di Integrità di Sicurezza (SIL) richiesti nell'industria di processo (raramente a SIL 4, che impone l'adozione della CEI EN 61508) nei confronti del miglioramento della PFD è illustrato graficamente in Figura A.10:

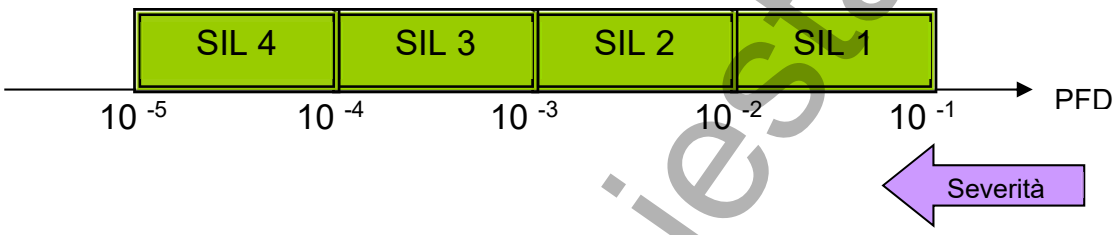


Figura A.10 – Miglioramento della PFD in relazione al livello di SIL

Mentre la Tabella A.2 riporta per i vari livelli di SIL il campo di Probabilità di Guasto su Domanda (PFD) e il relativo Fattore di Riduzione del Rischio (RRF):

Per SIS funzionanti in modo continuo vedasi invece direttamente la Tabella 7 (ovvero la Tabella 4 della CEI EN 61511-1).

Tabella A.2 – Valori normalizzati di PFD e RRF in funzione del SIL

Livello di Integrità di Sicurezza (SIL)	Probabilità di Guasto su Domanda (PFD)	Fattore di Riduzione di Rischio (RRF)
SIL 4	$\geq 10^{-5} \div <10^{-4}$	$> 10^{4} \div \leq 10^{5}$
SIL 3	$\geq 10^{-4} \div <10^{-3}$	$> 10^{3} \div \leq 10^{4}$
SIL 2	$\geq 10^{-3} \div <10^{-2}$	$> 10^{2} \div \leq 10^{3}$
SIL 1	$\geq 10^{-2} \div <10^{-1}$	$> 10^{1} \div \leq 10^{2}$

A.6 Metodologia di calcolo di un Livello di Integrità di Sicurezza (SIL)

Una volta che l'analisi del rischio ha definito l'esigenza di una Funzione Strumentata di Sicurezza (SIF) per la sicurezza di un processo industriale e ne è stato individuato il Fattore di Riduzione del Rischio (RRF) e quindi il suo Livello di integrità di Sicurezza (SIL), occorre scegliere una architettura idonea del Sistema Strumentato di Sicurezza (SIS), che risponda al livello richiesto del SIL in accordo alla Tabella 10, ovvero alla Tabella 6 della CEI EN 61511-1, che prescrive la tolleranza minima ai guasti hardware dei componenti operanti in modo continuo o su domanda (normalmente su bassa domanda per gli impianti dell'industria di processo).

Normalmente, le tipiche architetture previste per i sottosistemi sono le seguenti:

- 1oo1 con votazione 1 su 1
- 1oo2 con votazione 1 su 2
- 1oo2D con votazione 1 su 2 però con Diagnostica incrociata
- 2oo2 con votazione 2 su 2
- 2oo3 con votazione 2 su 3

Per queste architetture la CEI EN 61508-6 fornisce le specifiche PFD dei sottosistemi (la cui somma, ovvero la PFD dell'intero sistema, dovrà essere inferiore al richiesto SIL: (Vedasi Tabella A.2)), in funzione dei loro parametri caratteristici:

- λ tasso di guasto totale per ora
- λ_D tasso di guasto dannoso per ora
- β frazione di guasti comuni
- β_D frazione di guasti comuni rilevati dalla diagnostica
- DC copertura diagnostica specifica del sottosistema
- MRT tempo medio di riparazione del componente
- MTTR tempo medio di ristorazione del sistema
- TI intervallo tra le prove periodiche

dove i singoli parametri devono essere determinati (vedasi anche Allegato H):

- λ e λ_D da dati certificati o da prove in utilizzazione, vedasi per esempio Tabella 6 o Offshore Reliability Databook,
- β da esame delle caratteristiche di progettazione dei sottosistemi, in relazione alle possibilità di guasto di modo e di causa comune,
- β_D da esame dalle caratteristiche di autodiagnostica dei sottosistemi, vedasi per esempio Tabella D.4 della CEI EN 61508-6,
- DC da esame del tipo ed intensità della diagnostica dei sottosistemi, vedasi per esempio Tabella C.2 della CEI EN 61508-6,
- MRT generalmente per difetto posto uguale all'MTTR (sebbene talvolta sia minore)
- MTTR generalmente per difetto inizialmente posto uguale ad 8 ore, rivedibili se del caso,
- TI valore da stabilirsi in funzione dell'impianto/processo, generalmente per difetto inizialmente posto pari a:
  - 1 anno per sistemi funzionanti in modo su domanda,
  - 3 mesi per sistemi funzionanti in modo continuo,

  riducibili o aumentabili all'occorrenza, per ottenere la richiesta PFD.

Con tali dati è possibile rilevare dalle Tabelle CEI EN 61508-6 (o dall'Allegato I, che ne riporta le più importanti Tabelle) le singole PFD:

- per sistemi funzionanti in modo su domanda:
  Tabelle B.2, B.3, B.4, B.5 rispettivamente per TI pari a 0.5, 1, 2 e 10 anni;
- per sistemi funzionanti in modo continuo:
  Tabelle B.10, B.11, B.12, B.13 rispettivamente per TI pari a 1, 3, 6 e 12 mesi;

il tutto evidenziato ed illustrato secondo lo schema di flusso riportato in Figura A.11:

Vedasi anche Allegato H per un calcolo analitico anziché tabellare della PFD.

(*) Vedasi anche Allegato I.

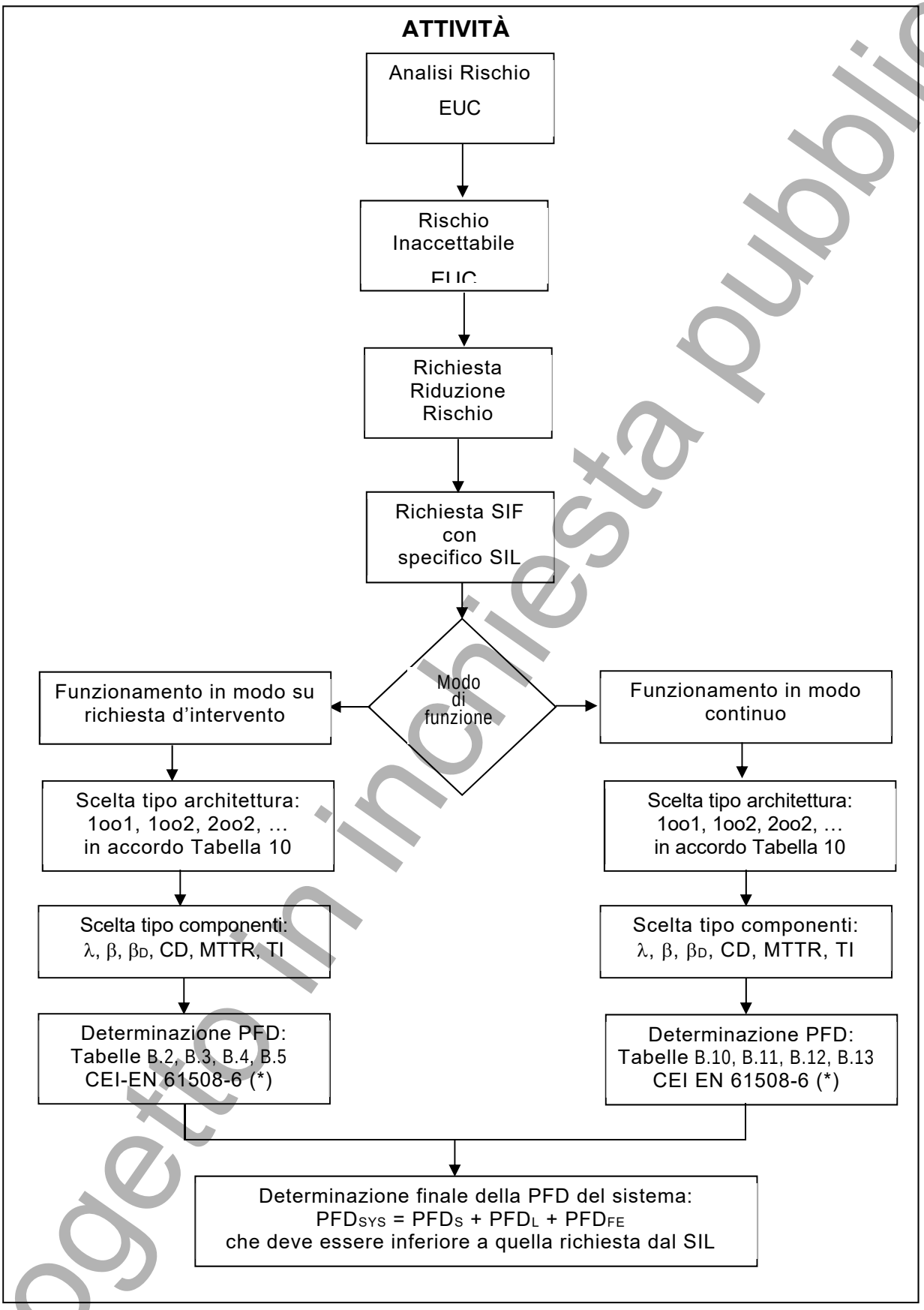


Figura A.11 – Schema di flusso per la determinazione tabellare della PFD dei sottosistemi componenti il Sistema Strumentato di Sicurezza SIS

A.7 Esempio di calcolo di un Livello di Integrità di Sicurezza (SIL)

Dall'analisi del rischio di un processo (per esempio, condotta secondo la metodologia HAZOP illustrata precedentemente in Figura A.8) è emersa la necessità di un Sistema Strumentato di Sicurezza (SIS), che necessita di un Livello di Integrità di Sicurezza SIL 2, perché si vuol avere un Fattore di Riduzione del Rischio (RRF) di almeno 100 (vedasi Tabella A.2), per portare il processo ad operare in uno stato sicuro, ovvero in una regione di rischio tollerabile.

Si supponga che la richiesta di partenza dell'architettura del SIS sia la seguente:

(anche se basterebbe per tutti i sottosistemi 1oo1 per Tabella 6, CEI EN 61511-1):

a) un gruppo di 3 sensori normali di pressione analogici con ridondanza 2oo3:

   per diminuire gli interventi spuri di fermata del processo perché sono a logica maggioritaria;

b) un gruppo di 2 risolutori logici programmabili PES con ridondanza 1oo2D:

   sempre per diminuire gli interventi spuri di fermata del processo perché sono mutualmente diagnosticati;

c) un gruppo di due valvole, una di blocco (shut) e l'altra di scarico (vent):

   a singola architettura 1oo1 conforme alla Tabella 6 , CEI EN 61511-1;

Vedasi Figura A.12: Esempio tratto dall'Appendice B paragrafo B.3.2.4 della CEI EN 61508-6 con supposto tasso di guasto dannoso $\lambda_D = \lambda/2$.

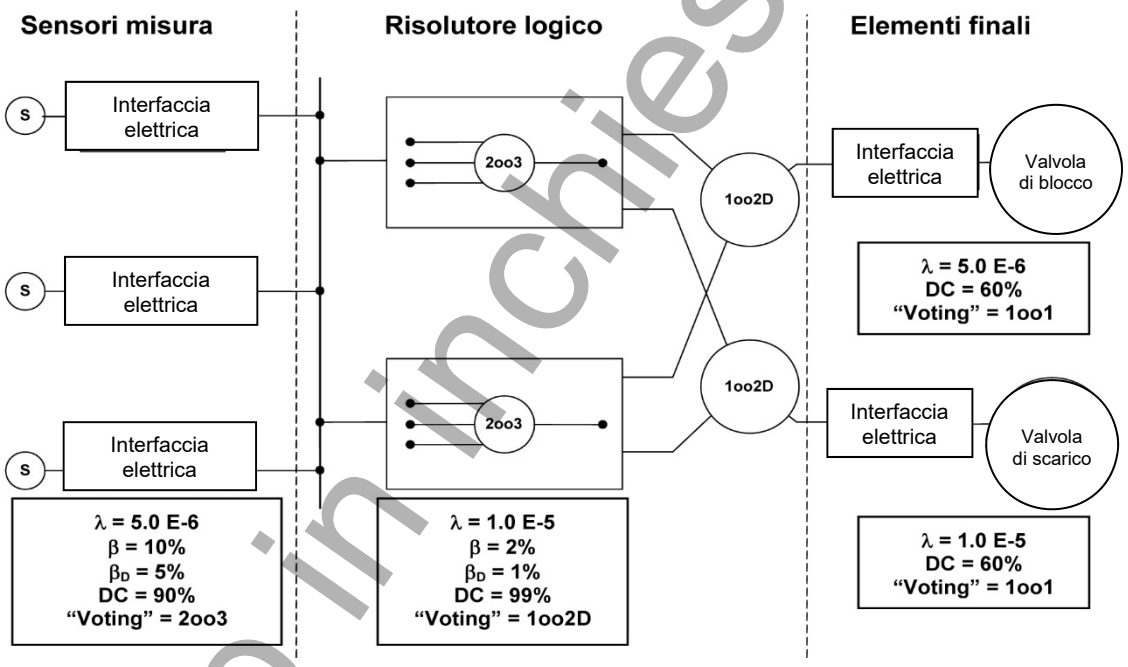


Figura A.12 – Esempio di architettura di un SIS (Figura B.14 – CEI EN 61508-6)

Pertanto, il sistema è scomponibile in tre sottosistemi:

- sottosistema dei sensori, realizzato con ridondanza 2oo3;
- sottosistema del risolutore logico, realizzato con ridondanza 1oo2D;
- sottosistema degli attuatori, realizzato con ridondanza 1oo1.

Per una valutazione iniziale SIL si parte con i seguenti parametri:

- un intervallo delle prove periodiche del sistema (TI) annuale;
- un tempo medio di ristabilimento del sistema (MTTR) di 8 ore;
- i parametri caratteristici $\lambda_D = \lambda/2$, e β, β_D e DC specifici previsti per i sottosistemi.

Ogni sottosistema contribuisce per una parte alla PFD del sistema complessivo:

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$

dove il PFD di ogni sottosistema è ricavabile dalle Tabelle della CEI EN 61508-6 in relazione ai suoi parametri caratteristici:

– λ_D, β, β_D, DC, MTTR, TI

per sottosistemi funzionanti in modo su domanda. (vedasi anche le Tabelle in Allegato I).

Determinazione dell'intervallo di prova (TI) per l'architettura scelta:

a) Supponendo inizialmente un intervallo di 1 anno:

Determinazione della PFD dei sensori di misura PFD_S

Architettura	**DC**	**λ_D= 2.5 E-06**		
		β =2% β_D=1%	**β =10% β_D=5%**	**β =20% β_D=10%**
2oo3	0 %	6.8 E-04	1.5 E-03	2.5 E-03
	60%	1.6 E-04	5.1 E-04	9.4 E-04
	90%	2.7 E-05	1.2 E-04	2.3 E-04
	99%	2.5 E-06	1.2 E-05	2.4 E-05
Tabella estratta dalla Tabella B.3 della CEI EN 61508-6				

Determinazione della PFD del risolutore logico PFD_L

Architettura	**DC**	**λ_D= 0.5 E-05**		
		β =2% β_D=1%	**β =10% β_D=5%**	**β =20% β_D=10%**
1oo2D	0 %	1.1 E-03	2.7 E-03	4.8 E-03
	60%	2.0 E-04	9.0 E-04	1.8 E-03
	90%	4.5 E-05	2.2 E-04	4.4 E-04
	99%	4.8 E-06	2.4 E-05	4.8 E-05
Tabella estratta dalla Tabella B.3 della CEI EN 61508-6				

Determinazione della PFD degli attuatori finali PFD_{FE}

Architettura	**DC**	**λ_D= 2.5 E-06**	**λ_D= 0.5 E-05**
1oo1	0%	1.1 E-02	2.2 E-02
	60%	4.4 E-03	8.8 E-03
	90%	1.1 E-03	2.2 E-03
	99%	1.3 E-04	2.6 E-04
Tabella estratta dalla Tabella B.3 della CEI EN 61508-6			

Con le architetture riportate precedentemente in Figura A.12 per i tre sottosistemi in esame ed assumendo un intervallo di prova di un anno si ha, come sopra evidenziato nelle Tabelle tratte dalla Tabella B.3 della CEI EN 61508-6, che la PFD del sistema risulta:

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} = 2{,}3x10^{-4} + 4{,}8x10^{-6} + (4{,}4x10^{-3} + 8{,}8x10^{-3})$

ovvero:

$PFD_{SYS} = 1{,}3 \times 10^{-2} \equiv$ SIL 1 (Vedasi Tabella A.2).

In sostanza la PFD del sistema è pari a quella degli attuatori (elementi finali), dato che gli altri contributi sono almeno di due ordini di grandezza inferiori.

Il SIL del sistema non essendo accettabile, si può aumentare in due modi:

(1) *Con un intervallo di test (TI) di tutto il sistema di sei mesi (8 ore MTTR) si ricava:*

Determinazione della PFD dei sensori di misura PFD_S

Architettura	**DC**	**λ_D= 2.5 E-06**		
		β =2% β_D=1%	**β =10% β_D=5%**	**β =20% β_D=10%**
2oo3	0 %	2.3 E-04	6.5 E-04	1.2 E-03
	60%	6.3 E-05	2.4 E-04	4.6 E-04
	90%	1.2 E-05	5.7 E-05	1.1 E-04
	99%	1.3 E-06	6.5 E-06	1.3 E-05
Tabella estratta dalla Tabella B.2 della CEI EN 61508-6				

Determinazione della PFD del risolutore logico PFD_L

Architettura	**DC**	**λ_D= 0.5 E-05**		
		β =2% β_D=1%	**β =10% β_D=5%**	**β =20% β_D=10%**
1oo2D	0 %	3.7 E-04	1.2 E-03	2.3 E-03
	60%	9.5 E-05	4.5 E-04	8.9 E-04
	90%	2.2E-05	1.1 E-04	2.2 E-04
	99%	2.6 E-06	1.3 E-05	2.6 E-05
Tabella estratta dalla Tabella B.2 della CEI EN 61508-6				

Determinazione della PFD degli attuatori finali PFD_{FE}

Architettura	**DC**	**λ_D= 2.5 E-06**	**λ_D= 0.5 E-05**
1oo1	0 %	5.5 E-03	1.1 E-03
	60%	2.2 E-03	4.4 E-03
	90%	5.7 E-04	1.1 E-03
	99%	7.5 E-05	1.5 E-04
Tabella estratta dalla Tabella B.2 della CEI EN 61508-6			

Per cui ora risulta:

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} = 1{,}1 \times 10^{-4} + 2{,}6 \times 10^{-6} + (2{,}2 \times 10^{-3} + 4{,}4 \times 10^{-3})$

ovvero:

$PFD_{SYS} = 6{,}7 \times 10^{-3} \equiv$ SIL 2

(2) *Con la ridondanza 1oo2 dell'elemento finale di scarico, quello a minor affidabilità, ed assumendo β = 10% e β_D = 5% si ricava invece:*

Architettura	**DC**	**λ_D= 0.5 E-05**
		β = 10% e β_D = 5%
1oo2	0 %	2.7 E-03
	60%	9.7 E-04
	90%	2.3 E-04
	99%	2.4 E-05
Tabella estratta dalla Tabella B.3 della CEI EN 61508-6		

Per cui infine risulta:

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} = 2{,}3x10^{-4} + 4{,}8x10^{-6} + (4{,}4x10^{-3} + 9{,}7x10^{-4})$

ovvero:

$PFD_{SYS} = 5{,}6x10^{-3} \equiv$ SIL 2

Ottenendo in entrambi i casi risultati PFD similari e conformi al SIL 2 di progetto:

PFD < 10^{-2} (Vedasi Tabella A.2).

SIGNIFICATO DELLE SIGLE UTILIZZATE

1oo1	1 di 1 architettura non ridondante
1oo2	1 di 2 architettura ridondante
1oo2D	1 di 2 architettura ridondante diagnostica
1oo3	1 di 3 architettura diagnostica
2oo2	2 di 2 architettura completamente ridondante
2oo3	2 di 3 architettura ridondante a maggioranza
λ	Tasso di guasto totali per ora (= 1/MTTF)
λ_D	Tasso di guasto dannosi per ora (=λ/2)
β	Causa comune di frequenza di guasto
β_D	Causa comune rilevata da diagnostica
BPCS	Sistema base di controllo di processo
DC	Copertura diagnostica
FS	A prova di guasto
FT	Tolleranza al guasto
MRT	Tempo medio di riparazione (componente)
MTBF	Tempo medio tra due guasti
MTTF	Tempo medio al guasto
MTTR	Tempo medio di ristabilimento (loop)
PES	Sistema elettrico programmabile
PFD	Probabilità di guasto su richiesta d'intervento
RRF	Fattore di riduzione di rischio
SIF	Funzione strumentata di scrittura
SIL	Livello di integrità di sicurezza
SIS	Sistema strutturato di sicurezza
SFF	Frazione di guasti sicuri
TI	Intervallo di prova

Allegato B

Sviluppo del progetto dei sistemi di sicurezza di un impianto di processo industriale

Premessa

Il progetto di un impianto di processo industriale richiede competenze sistemistiche e multidisciplinari e lo sviluppo delle sue fasi (concettuale, di prefattibilità, esecutivo), risulta valido ed efficace solo se è possibile conoscere le specificità del processo produttivo che si attua nell'impianto in esame, l'ambito in cui esso sarà realizzato, gli attori coinvolti, le esigenze dell'utilizzatore finale.

È importante, inoltre, conoscere se l'impianto è destinato a se stessi o ad altri e se sarà realizzato da terzi.

Il progetto deve inoltre tener conto dello stato dell'arte e dei vincoli economici e temporali (Figura B.1).

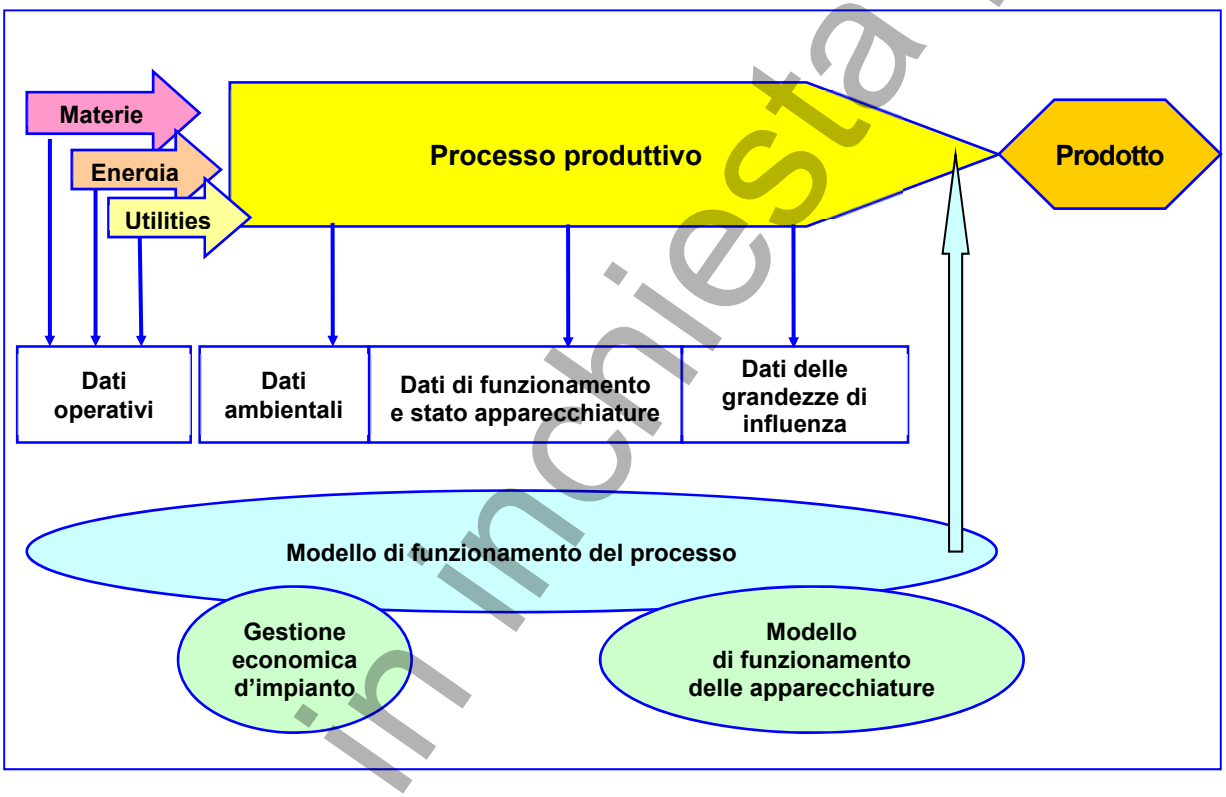


Figura B.1 – Esempio di schema degli obiettivi della logica dei flussi informativi

Lo schema illustrato in figura mostra l'importanza fondamentale della disponibilità di un modello di funzionamento del processo e dell'acquisizione di tutti i dati ambientali, di tutti i dati operativi delle apparecchiature e di tutti i campi delle grandezze di influenza.

Lo schema è valido sia per la progettazione di un nuovo impianto che per una modifica di un impianto esistente: nel secondo caso il vincolo maggiore è rappresentato dalle caratteristiche delle apparecchiature esistenti e dal loro stato d'uso e conservazione.

Inoltre la validità di un progetto è oggi misurata anche dall'aver considerato la dismissione dell'opera realizzata.

Un aspetto fondamentale del progetto è l'analisi della sicurezza dell'impianto, che, a fronte di una soglia di accettabilità del rischio, deve individuare le azioni progettuali e gestionali per ridurlo a valori non superiori al valore di soglia prefissato.

È questa una attività che dipende dalla conoscenza approfondita dell'impianto e si evolverà ed affinerà durante le fasi di sviluppo del progetto, tenendo conto che, in generale, l'introduzione di un nuovo intervento introduce un rischio aggiuntivo che si somma a quello esistente. Ovviamente, tanto più è elevato il livello di rischio intrinseco (senza tenere conto dei sistemi di protezione), tanto più è necessario introdurre livelli o barriere di sicurezza (indipendenti), in numero sufficiente a raggiungere l'obiettivo prefissato di riduzione del rischio.

Scopo di questo Allegato è quello di dettagliare, rispetto a quanto contenuto nel testo della presente Guida, i criteri di progetto dei sistemi strumentati (SIS) preposti alla riduzione del rischio negli impianti di processo industriali.

B.1 Il Piano di Sicurezza (PdS)

Viene definito dal Responsabile della "*Gestione della Sicurezza Funzionale"* un Piano di Sicurezza (PdS), nel quale vengono individuate, per le diverse fasi del progetto, le attività che devono essere condotte e definiti i criteri di gestione e verifica degli aspetti tecnici relativi al progetto, all'installazione, alla messa in servizio e al mantenimento dei requisiti di progetto dei SIS durante l'esercizio dell'impianto, fino alla dismissione del SIS stesso o dell'impianto.

A monte delle attività di ciascuna fase devono essere preliminarmente condotte le seguenti due attività fondamentali:

- raccolta delle informazioni necessarie per lo sviluppo delle altre attività;
- definizione delle funzioni tecniche ed organizzative responsabili per le diverse attività.

A valle delle attività di ciascuna fase, devono essere previsti i seguenti punti:

- analisi dei risultati ottenuti dalle attività previste;
- valutazioni e studi di azioni per il raggiungimento della conformità agli obiettivi previsti.

Le risultanze di ogni fase sono verificate dal Responsabile della "*Gestione della Sicurezza Funzionale"* e validate dal Responsabile della "*Valutazione della Sicurezza Funzionale*".

Il PdS è modificabile nel tempo in funzione dei contenuti delle fasi, purché vengano mantenuti il progetto di base e il calendario previsto per l'esecuzione delle attività.

B2 Fasi di valutazione del rischio

La valutazione del rischio di un nuovo progetto o della modifica di un progetto esistente individua il livello di rischio accettabile e fornisce la base di sviluppo del PdS.

La classificazione del livello del rischio è definita da un *Indice Globale di Rischio (Overall Risk Index).*

In funzione del livello di rischio, devono essere individuati almeno due percorsi di sviluppo del PdS, a ciascuno dei quali devono essere associate diverse modalità di verifica delle attività previste nel PdS.

Fase A: Sviluppo della fase preliminare di fattibilità (Feasibility)

Sono condotte, in questa fase, le scelte di base del progetto, inclusi gli aspetti generali di rischio per l'Uomo, l'Ambiente ed i Beni (perdite economiche per fermate accidentali). Qualora non sia possibile acquisire dati e informazioni precise, ci si basa su assunzioni e presunzioni in qualche modo rilevanti ai fini dell'assetto impiantistico, da considerarsi equivalenti vista la semplicità dello stadio di sviluppo del progetto, da verificare e rimuovere progressivamente nell'eventuale prosieguo del progetto.

La descrizione delle Funzioni di Sicurezza (Safety Functions: SF) e dei Livelli di Integrità di Sicurezza (Safety Integrity Level: SIL) associati ai Sistemi di Sicurezza (Safety related Systems: SrS) è condotta già nella fase di Progetto di Fattibilità. In questa fase possono essere individuate le SF e i relativi SrS in termini quali-quantitativi (ovvero le relative Barriere di Protezione Indipendenti – Indipendent Protection Layers: IPL). In questa fase di sviluppo è definita l'allocazione preliminare delle Funzioni Strumentate di Sicurezza (Safety Instrumented Funtions: SIF), così come l'allocazione ottimale (di massima) dei SrS e delle SF.

La descrizione delle SIF, dei SIL associati e delle relative specificazioni di sicurezza SRS (Safety Requirements Specifications) dei SIS (Safety Instrumented Systems) è, invece, condotta in fase di Progetto di Base (Basic), mentre la descrizione di dettaglio dei SIS (HW/SW) è condotta in fase di Progetto di Dettaglio.

Gli obiettivi generali e specifici di Sicurezza/Ambiente di riferimento per l'interno e l'esterno dell'impianto sono:

- Definizione degli Obiettivi di Sicurezza/Ambiente da parte dell'Utente Finale.
- Descrizione del Fattore di Servizio dell'Impianto.

In questa fase la stima del rischio preliminare d'Impianto è condotta, per semplicità, dal Responsabile della "Gestione della Sicurezza Funzionale". Lo schema di valutazione è, infatti, basato su una tipica "lista di controllo" dalla quale possono essere tratte conclusioni generali sul livello di rischio intrinseco associato all'Attività e sul rischio residuo, una volta che sono state previste le Barriere di Sicurezza Indipendenti (IPL). La valutazione consente di individuare il livello di rischio: Alto, Medio e Basso, unicamente in funzione delle conseguenze potenziali associate all'Attività inserita nel contesto di Impianto o di Sito. La individuazione delle IPL costituisce una fase decisiva per lo sviluppo dl progetto nella Fase di Fattibilità.

La disponibilità degli schemi semplificati (PFD) e la descrizione generale di processo consentono di individuare i sistemi di controllo fondamentali e di protezione sia tecnologica che di tipo generale (SrS).

In questa fase è determinante la valutazione di criteri di sicurezza legati elle specifiche caratteristiche di processo; in altre parole sulla possibilità di disporre di processi che anche in caso di ipotizzabili eventi di guasti e/o anomalie interne od esterne legate a variabili di processo o degli ausiliari, non comportano condizioni di rischio.

Questa fase di analisi costituisce un primo riferimento per lo sviluppo del PRA (Preliminary Risk Assessement). Sulla base di questi infatti è possibile pervenire ad una stima di massima del livello di sicurezza offerto dalle IPL a fronte degli Eventi Pericolosi (Top Events) globali individuati nella fase di PRA. Le risultanze sono necessariamente parziali ed in genere, non sufficienti per assicurare la completezza dell'analisi, ma sono sufficienti ad assicurare almeno gli obiettivi di sicurezza a fronte dei criteri di accettabilità dell'utente.

L'attività principale nella Fase di Fattibilità è quindi la conduzione dell'Analisi del Rischio Preliminare (PRA) che comprende la classificazione preliminare, condotta sulla base di una lista di controllo (check list) appropriata il cui livello autorizzativo è del Gestore della Sicurezza Funzionale (Functional Safety Manager: FSM).

La struttura ed i criteri di base della lista di controllo non comportano un livello di specializzazione della Valutazione della Sicurezza Funzionale (Functional Safety Assessment: FSA) in quanto il tipo e contenuti del documento deve essere compatibile con la funzione FSM ai fini decisionali.

Le informazioni che dovranno, pertanto, essere disponibili, sono almeno:

- l'elenco e quantità delle sostanze utilizzate nei processi, le relative schede di sicurezza (SDS) e la permanenza up degli stoccaggi intermedi;
- l'indicazione della tipologia dei processi utilizzati con riferimento ai possibili rischi sia per le sostanze utilizzate ed immagazzinate (incendio, esplosione, rilasci tossici) di possibilità di upset (pressioni, temperature) di reazioni anomale con conseguenti effetti sulla sicurezza della stabilità delle apparecchiature (reazioni fuggenti) e/o sull'ambiente (rilasci in atmosfera, al suolo) sulla formazione di composti anomali intermedi pericolosi, dei rischi per l'uomo e l'ambiente in caso di perdita di contenimento.

Questa analisi considererà le seguenti informazioni o documenti:

1) lo schema di processo semplificato in cui sono riportati tipologie e quantitativi delle sostanze utilizzate e/o immagazzinate. Nello schema di processo devono essere indicati i sistemi di controllo principale ed i sistemi di protezione previsti (PSV, PRD, Sistemi di blocco e le relative funzioni, criteri particolari di progettazione per la sicurezza, ecc.);
2) la descrizione del processo con evidenziazione dei possibili rischi associati (vedasi Tabella 2 del DM 9.5.2001– Valori di soglia):
   - Incendio,
   - Esplosione (miscele infiammabili all'interno degli apparecchi),
   - Getti di fuoco (jetfire/fireball),
   - Rilascio infiammabile/tossico,
   - Processi fuggenti (runaway),
   - Perdita di contenimento per possibile stress/corrosione.

   La descrizione del processo deve evidenziare eventuali fasi critiche per gli aspetti di sicurezza ed i criteri generali di sicurezza adottati per farne fronte: protezioni passive ed attive. Ad esempio: sistemi di contenimento (bunkers), sistemi antincendio, barriere di vapore/acqua, sistemi di regolazione automatici, sistemi di blocco, valvole di sicurezza, dischi di rottura, tipologia degli scarichi (atmosfera, convogliati: blowdown, closedrain);
3) la qualità delle materie prime, dei prodotti chimici (chemicals), dei prodotti di riciclo (eventuali) e dei metodi per la verifica di conformità alle specifiche e delle utilities (energia elettrica, acqua grezza, vapore, azoto, aria strumenti, aria servizi, acqua demineralizzata, ecc.);
4) la novità o l'esperienza del processo in altri impianti realizzati e l'esperienza storica per gli aspetti di sicurezza e di regolarità di esercizio (fattore di servizio: guasti accidentali, fermate per ragioni di processo: sporcamenti, intasamenti);
5) i criteri di base dei processi con riferimento alla eventuale sicurezza intrinseca (sostanze, stabilità delle reazioni);
6) i criteri di base previsti per la riduzione della probabilità che si verifichino gli eventi pericolosi potenziali (Top Events) e/o la magnitudo delle conseguenze, nel caso essi si verifichino (barriere indipendenti passive e/o attive);
7) la stima della frequenza (alta, non escludibile, remota) dei suaccennati eventi e della severità delle conseguenze (livelli di irraggiamento termico, sovrappressioni per onda d'urto, concentrazioni pericolose per le sostanze tossiche e relative distanze) in assenza delle eventuali barriere di sicurezza;
8) la valutazione dell'efficacia delle IPL in termini di stima della riduzione del rischio (probabilità e/o frequenza degli eventi incidentali potenziali). Dovranno essere indicati i riferimenti per la riduzione del livello di rischio per tipologia di IPL eventualmente previste.

Inoltre:

1) Dovranno essere specificate le caratteristiche delle Funzioni Strumentate di Sicurezza (Safety Instrumented Functions: SIF) la tipologia delle apparecchiature e caratteristiche progettuali (vedasi "Requisiti dei sistemi di sicurezza": CEI EN 61511-1, art. 10) dei sistemi strumentati che le realizzano.
2) Dovrà essere definito il massimo numero e durata degli interventi di blocco intempestivo accettabile dell'impianto attribuibile ad essi (trip nuisances) che non coinvolga aspetti di sicurezza e/o ambiente (Blocchi intempestivi possono condurre a condizioni di rischio).
3) Dovranno essere evidenziate eventuali alternative di progetto delle IPL in termini di ottimizzazione di allocazione; sulla base di un bilancio costi/efficacia (costi dovranno essere comprensivi della stima di quelli imputabili all'esercizio: manutenzione, prove periodiche, ricambi, gestione della sicurezza in caso di indisponibilità dei sistemi di protezione, ecc.).
4) Per ogni eventuale alternativa di progetto dovranno essere individuati gli impatti relativi ai livelli di rischio ipotizzabili (sicurezza, ambiente, regolarità di marcia), il grado di severità e le misure impiantistiche previste per ridurli a livelli accettabili secondo le direttive dell'utente (Matrice di rischio e di riduzione con le IPL).
5) Il criterio di valutazione dei livelli di rischio relativi alla sicurezza, ambiente e conseguenze di fermate accidentali sarà conforme ai requisiti richiesti dall'utente.
6) Dovrà essere disponibile un Rapporto relativo agli aspetti di sicurezza e di regolarità di marcia i cui contenuti sono quelli desunti dalle informazioni fornite dall'utente.
7) Eventuali Rapporti di Sicurezza, studi specifici di sicurezza disponibili e studi di Impatto Ambientale.
8) Dovranno infine essere specificati i ricambi strategici necessari a garantire i valori di MTTR.

I livelli di rischio individuabili ai fini dello sviluppo del PdS sono qualificati in tre livelli:

- Basso : (L - Low);
- Medio : (M – Medium);
- Alto : (H - High).

ed in relazione della frequenza di accadimento devono essere previste opportune Barriere di Protezione Indipendenti (IPL) per conseguire dei corretti livelli di riduzione del rischio (RRF) come evidenziato in Tabella B.1

In funzione della classificazione preliminare, basata sulle informazioni disponibili è possibile individuare la classe di rischio con la tecnica ALARP della CEI EN 61511-3:

I – Inaccettabile

II – Tollerabile

III – Accettabile

Tabella B.1 – Tipici livelli di riduzione del rischio (RRF) per i diversi livelli di rischio (L/M/H) e per frequenza di accadimento per anno

Frequenza per anno	L	M	H
$10^{-2} \div 10^{-3}$	10	100	1 000
$10^{-1} \div 10^{-2}$	100	1 000	10 000
$< 10^{-1}$	1 000	10 000	100 000

Le definizioni di livello di rischio Alto, Medio e Basso sono definiti in base ai criteri di severità delle conseguenze (Metodo *"speditivo"*) dei potenziali eventi incidentali(1).

Lo schema relativo alla valutazione delle IPL riguarda fondamentalmente le attività classificabili nell'ambito di rischio Medio/Alto (M/H), ovvero per la classe di rischio I/II.

Le barriere indipendenti sono classificabili in due categorie principali:

a) sistemi di prevenzione;

b) sistemi di contenimento degli effetti;

mentre non si considerano le Barriere di tipo "organizzativo"(2)

A queste barriere di protezione contro eventi di danno (guasto) è difficile associare un SIL, pertanto si ammette che la realizzazione sia totalmente efficiente (ad esempio lo spessore dei muri di un Bunker, di una Sala Controllo realizzata contro le esplosioni di vapori e nubi di gas infiammabile).

Per quanto attiene, invece, le Valvole di Sicurezza (Pressure Safety Valve: PSV) esiste una pur minima probabilità di mancato intervento su richiesta d'intevento. Questa probabilità dipende da molti fattori, quali le condizioni di installazione, del tipo di fluido (sporcante) delle verifiche periodiche ispettive condotte dagli enti esterni preposti.

Lo schema di analisi può essere basato sulla applicazione della riduzione del rischio (LOPA) individuata dalle IPL a fronte della soglia di accettabilità prevista per la tipologia delle conseguenze prevedibili degli eventi iniziatori ipotizzabili.

Nella Tabella B.2 sono riportati tipici livelli di riduzione (media) del rischio di particolari IPL.

Tabella B.2 – Tipici livelli di riduzione del rischio (RRF) per particolari IPL

IPL	BPCS (a)	ALLARMI (b)	SIS (c)	NRV (d)	PSV (e)	PRD (f)	F & G (g)	BUNKER
RRF	**10**	**10**	**10-10 000**	**10**	**10-50**	**100**	**100**	**1000**

(a) Stima media di riduzione del rischio controllabile dal BPCS dovuto ad anomalia di processo
(b) Stima tipica di riduzione del rischio per intervento operatori a gestire gli allarmi
(c) Riduzione del rischio da SIL 1 a SIL 4
(d) Valvole di non ritorno (Non Return Valve)
(e) Valvole di sicurezza (Pressure Safety Valve)
(f) Dischi di rottura (Pressure Rupture Disk)
(g) Sistemi antincendio (Fire & Gas: FGS)

(1) In particolare, una Descrizione può essere la seguente:
- Eventi a Basso impatto: conseguenze trascurabili sul personale all'interno dello Stabilimento
- Eventi a Medio impatto: conseguenze non trascurabili sul personale all'interno dello Stabilimento
- Eventi a Alto impatto: conseguenze non trascurabili sulla popolazione all'esterno dello Stabilimento.

(2) Le Barriere di sicurezza di tipo *organizzativo* (Procedure, Qualifiche professionali e Mansioni, Formazione, ecc.) anche se costituiscono una barriera ai fini di prevenire e/o mitigare eventi pericolosi, non sono classificabili, tuttavia, come strumenti ai fini autorizzativi. Questi, in ogni caso, costituiscono un requisito previsto per la Gestione/Modifica dei SIS/SrS ed oggetto del "Manuale Aziendale di Gestione della Sicurezza".

Il Calcolo del Livello di rischio e di conseguenza, la classificazione di Attività a "Basso" o "Medio/Alto" rischio può essere individuato sulla base delle informazioni di processo e di base di progetto, applicando il criterio *"speditivo"* che consente la definizione dell'area coinvolta dall'evento (i) pericoloso (i) ipotizzato (i) specifico (i) per quella categoria di apparecchiature previste nel progetto e della severità delle conseguenze per l'Uomo, l'Ambiente ed i Beni.

La Tabella B.3 riporta per la Fase A di sviluppo della fattibilità le varie fasi evolutive con la funzione responsabile, la descrizione degli obiettivi e la procedura e/o specifica di riferimento.

Tabella B.3 – Funzioni responsabili, descrizioni obietti e procedure/specifiche per la Fase A di Ingegneria di Fattibilità

Fase A	Funzione Responsabile	Descrizione degli obiettivi della Fase	PROCEDURA/ SPECIFICA
A.1	Ambiente e Sicurezza (HSE)	Sviluppa e formalizza il "Piano di Sicurezza" (PdS) identificando per ciascuna attività tempi e le responsabilità.	
A.2.	Ambiente e Sicurezza (HSE)	Conduce una Analisi di Sicurezza Preliminare (PRA) sulla base della Documentazione di Fattibilità relativamente ad una Nuova Attività o Modifica (Check List). Tale analisi comprende: a) un "Riesame della Tecnologia" ed, in particolare: – Analisi di Sicurezza Intrinseca – Identifica (se del caso) eventuali alternative di processo (b) Definizione del Livello di Rischio della Nuova Attività: – Alto (H), Medio (M), Basso (L), basato sulle caratteristiche di sicurezza intrinseca della Nuova Attività (modifica). In funzione del livello di "rischio intrinseco" della Nuova Attività ed in particolare nel caso di Medio o Alto Rischio è attivata la Funzione di Esperto della Sicurezza Funzionale (FSA) e definito il livello di competenza (Tabella 5, CEI EN 61508-1). – In questa fase sono definite le informazioni base di sicurezza relative all'iter autorizzativi (Non aggravio di rischio, Rapporto di sicurezza, Impatto Ambientale, ecc.) (c) Per Alto e/o Medio Rischio è condotta una: – Valutazione possibili scenari incidentali – Descrizione degli Obiettivi di Sicurezza/Ambiente e Fattore di Servizio – Determinazione delle IPL – Verifica raggiungibilità degli Obiettivi di Sicurezza sulla base delle IPL – Nel caso che non sia prevedibile il raggiungimento degli obiettivi di sicurezza previsti saranno introdotte nuove IPL e/o modifiche di processo con successiva verifica del possibile raggiungimento degli obiettivi. (d) Emissione di un Rapporto sulle caratteristiche di sicurezza della Nuova Attività ai fini degli obiettivi di accettabilità dell'Utente Finale	Metodo "Speditivo" & LOPA per le IPL
A.3	INGEGNERIA	Raccoglie i Rapporti delle verifiche di cui ai punti precedenti e li trasmette insieme al Progetto di Fattibilità (feasibility) per la fase di sviluppo del progetto di massima (basic)	
A.4	GESTORE PROGETTO	Identifica in via preliminare, tutti gli adempimenti di legge (autorizzazioni, valutazioni dei rischi, pratiche diverse) da osservare per la realizzazione del progetto con relativa tempistica (prima dell'inizio lavori, prima dell'avviamento, ecc.) e le eventuali limitazioni di carattere ambientale	

Già in questa fase possono essere individuati livelli di riduzione del rischio tenuto conto della peculiarità delle barriere generali di protezione (IPL) previste dal Progetto di Fattibilità. Inoltre sono individuabili i tipici SIL attribuibili a determinate Unità di Impianto (Colonne di distillazione(1), Reattori fuggenti_runway) o Sistemi di Sicurezza di particolari Unità d'Impianto o macchine (Sistemi di Gestione dei Bruciatori: BMS di Caldaie e Forni, Sovravvelocità_Overspeed Turbine, Centrifughe, ecc.).

In questa fase possono essere valutate (se esistenti o praticabili economicamente) alternative fondamentali di processo ai fini di pervenire alla sicurezza intrinseca del processo (inherent safety). Un processo intrinsecamente sicuro evita la realizzazione di sistemi di sicurezza ad alta integrità con problematiche gestionali di mantenimento nel tempo delle caratteristiche prestazionali e relativi costi(2).

La riduzione del rischio intrinseco F può essere ottenibile mediante la realizzazione di più Barriere di Sicurezza Indipendenti (IPL).

Ad esempio, nel caso di rischio Medio (M), l'obiettivo di sicurezza è raggiunto mediante 2, 3 o 4 Barriere Indipendenti (IPL) a secondo se le conseguenze dell'evento incidentale ipotizzato sia di Bassa, Media od Alta severità.

Nel caso di Attività il cui livello di rischio ricade in Medio/Alto (M/H), la valutazione del Rischio residuo e quindi della raggiungibilità degli obiettivi prefissati è di responsabilità della "Valutazione della Sicurezza funzionale" (Functional Safety Assessment).

Si assume che una IPL contribuisca alla riduzione del rischio almeno di un fattore 10.

Le risultanze della Analisi del Rischio Preliminare (PRA) costituiscono la base dello sviluppo dei Sistemi relativi alla Sicurezza (SrS) dei SIS ed oggetto del Rapporto, che dovrà contenere almeno:

- la definizione di Alto, Medio e Basso Impatto definite in base ai criteri di severità delle conseguenze (Metodo *"speditivo"*) degli eventi pericolosi;(3)
- la soluzione progettuale di base fra eventuali alternative, sulla base del rischio residuo, dell'impatto ambientale e del fattore di servizio atteso;
- l'elenco degli eventi pericolosi individuati (Top Events) caratteristici dell'attività, tenuto conto delle possibili interazioni con altre Sezioni di Impianto in caso di modifica o installazione in un sito industriale esistente;
- le cause principali che vi concorrono (eventi incidentali di base).

Sulla base delle risultanze della analisi condotta e sui criteri di accettabilità del rischio specificati o su riferimento dell'utente o (ed in armonia) con quelli eventuali della autorità competenti, vengono definiti i criteri di sicurezza e le IPL (alternative).

(1) Per le colonne di distillazione che lavorano a pressione (protette dalle PSV contro la sovrappressione), si deve, in realtà, valutare la tipologia del progetto ed in particolare, se è possibile lo scarico in atmosfera o no e, in questo caso, tenere conto dei criteri di progetto della rete di scarico (dimensionamento: API 520 e 521, Codici di Pratica, Basic Practices, ecc.).

(2) Un "sistema intrinsecamente sicuro" è una apparecchiatura interconnessa con altre unità e/o linee di processo e servizi (energia elettrica, aria strumenti, acqua, ecc.) che in caso di ipotizzabili anomalie e/o guasti interni e/o esterni al sistema od apparecchiatura, ipotizzando non evidenzia situazioni di pericolo per l'uomo, l'ambiente ed i beni. Ad esempio, un reattore chimico che può comportare reazioni "fuggenti" in caso di anomalia della regolazione di parametri di processo non realizza un processo "intrinsecamente sicuro". Un reattore, invece che in caso di ipotizzabili anomalie del controllo conduce allo "spegnimento" della reazione senza nessuna conseguenza, costituisce un "sistema intrinsecamente sicuro".

(3) In particolare, una Descrizione può essere la seguente:
- Eventi a Basso impatto: conseguenze trascurabili sul personale all'interno dello Stabilimento
- Eventi a Medio impatto: conseguenze non trascurabili sul personale all'interno dello Stabilimento
- Eventi a Alto impatto: conseguenze non trascurabili sulla popolazione all'esterno dello Stabilimento.

Mediante Codici di Pratica, Basic Practices, Standard Specifici per apparecchiature, linee e componenti, è possibile quindi procedere alle seguenti fasi:

- Individuazione delle barriere di sicurezza Indipendenti (Independent Protection Layers: IPL) ed in particolare delle Funzioni Strumentate di Sicurezza (Safety Instrumented Functions: SIF) in modo da assicurare che siano raggiungibili gli obiettivi di sicurezza (e Fattore di Servizio) a fronte degli eventi pericolosi individuati (e/o noti) e in relazione sulla efficacia ai fini del raggiungimento degli obiettivi previsti.
- Le IPL in questa fase di analisi preliminare possono essere anche parzialmente dipendenti (ad esempio: il Sistema di Controllo di Processo Base- BPCS); nella successiva Fase di Progetto di Massima (Progetto Basic) saranno definiti gli specifici SIS relativi alle previste SIF.
- Le macchine ed apparecchiature rilevanti per assicurare il livello di regolarità di marcia previsto e le scorte strategiche.
- Gli EUC (Equipment Under Control) rilevanti come potenziali cause di evento pericoloso diretto e/o indiretto.
- La individuazione del SIL dei sistemi di protezione nel caso di specifiche apparecchiature tipiche (Reattori, Forni, Caldaie, Turbine, Colonne di distillazione, ecc.).
- Eventuali raccomandazioni tecniche di miglioria di progetto ai fini della sicurezza e fattore di servizio.

Nel caso che "l'Analisi Preliminare del Rischio" (PRA) comporti la classificazione come Medio/Alto, il livello di rischio Medio o Alto e le valutazioni sulla efficacia delle IPL sono oggetto del "Responsabile della Sicurezza Funzionale".

Il livello di rischio della Attività è riferito al massimo livello individuato.

Fase B: Sviluppo del progetto base di massima (Basic Engineering)

Lo sviluppo del Progetto Base di massima (Basic), è un passaggio che richiede un successivo affinamento delle soluzioni a seguito della disponibilità di maggiori informazioni e dati riguardo all'impianto che si verrà a realizzare.

Si possono pertanto prevedere delle verifiche e valutazioni relativamente alla Descrizione ed Allocazione delle Funzioni Strumentate di Sicurezza (SIF) tenuto conto di tutte le IPL.

Sulla base delle SIF saranno definiti i relativi Livelli di Integrità di Sicurezza (SIL) ed i previsti Sistemi di Strumentati di Sicurezza (SIS).

Il processo di allocazione ottimizza tipologia ed architetture dei sistemi delle protezioni a fronte degli Eventi Pericolosi (Top Events) individuati già nella Fase di Fattibilità (Top Events di tipo "generale" associati alle caratteristiche di processo e tipologia di base delle apparecchiature previste) e successivamente, nella fase di Progetto di Massima e del Fattore di Servizio (specificato nella Fase di Fattibilità).

I risultati attesi dalla attività condotta nella fase di basic sono fondamentalmente:

1) Individuazione i Sistemi relativi di Sicurezza (SrS) e Strumentati (SIS) e le relative specificazioni funzionali delle Funzioni Strumentate di Sicurezza (SIF).
2) EUC (Equipment Under Control): apparecchiature e componenti oggetto di rischio potenziale.
3) Allocazione dei SRS e delle SIF nell'ambito delle Barriere di Sicurezza Indipendenti IPL (Independent Protection Layer).
4) Descrizione dei SIL delle SIF individuate.
5) Descrizione dei requisiti dei SIS delle SIF.
6) Matrice Causa/Effetti e Diagrammi Funzionali.
7) Sistemi di Sicurezza Strumentati (SIS).
8) Eventuali altri SRS (Sistemi non strumentati di Sicurezza).

9) Frequenze medie annue degli eventi di rischio individuati (Top Events) criticità emerse tecnico/gestionali ed azioni per superarle.

10) Frequenze e durate medie annue degli eventi di fermata accidentale dell'Attività, criticità emerse tecnico/gestionali ed azioni per superarle.

11) L'attività prevede che sia stato redatto la versione preliminare del Manuale di Sicurezza (Safety Manual) ove verranno indicate le modalità di gestione dei sistemi di sicurezza, i criteri di verifica periodica (frequenza e modalità di esecuzione), la gestione dei guasti per garantire nel contempo la sicurezza al livello previsto. La stesura di procedure per i criteri di messa in servizio dei sistemi di sicurezza includerà i manuali o le schede di sicurezza che dovranno essere forniti dai costruttori delle apparecchiature approvate o dagli utilizzatori dei sistemi "prior use".

Le attività riportate nella seguente Tabella B.4 devono essere completate prima della consegna del Progetto di Massima (Basic) definitivo, non appena le informazioni necessarie siano disponibili.

Tabella B.4 – Funzioni responsabili, descrizioni obiettivi e procedure/specifiche per la Fase B di Ingegneria di Base

Fase B	Funzione Responsabile	Descrizione	PROCEDURA/ SPECIFICA
B.1	Ambiente e Sicurezza (HSE)	Aggiorna il PdS (Safety Plan) assegnando anche le responsabilità per la predisposizione della documentazione per le autorizzazioni	
B.2	Ambiente e Sicurezza (HSE)	a) Effettua una analisi di rischio dettagliata (HAZOP, FMEA od altre tecniche specifiche in relazione alla tipologia del progetto) b) Effettua la revisione BASIC sulle risultanze della analisi qualitativa dell'HAZOP con eventuali commenti e raccomandazioni da adottare nel progetto desunte dall'Analisi Quantitativa del Rischio (QRA) c) In questa Fase sono individuate le SIF e valutati i relativi SIL necessari per la riduzione dei rischi ai valori previsti in fase di Fattibilità. – Specifica nei dettagli tutti i Sistemi di sicurezza ("Safety related Systems": SrS, compresi i SIS) e le relative IPL (Barriere di Sicurezza Indipendenti) – Calcola i SIL delle SIF (livello di riduzione dei frequenze di rischio degli Eventi Pericolosi (Top Events) individuati – Valuta le frequenze attese dei Top Events e verifica la conformità con gli obiettivi previsti in fase di Fattibilità – Effettua la revisione degli Alberi di Guasto sulle risultanze della analisi qualitativa dell'Albero dei Guasti con allocazione delle SIF e calcolo dei SIL (analisi quantitativa) – Emette le specifiche di base dei SIS – In questa fase sono adottati criteri di base di progetto per i SIS (e relativi SIL delle SIF associate) relativi a "tipici" per apparecchiature e sistemi (Colonne di distillazione, Reattori con processi "runaway", BMS, "overspeed" di turbine, F & G, ecc.) – Specifica gli accessori per la PED (SIS) – Specifica i sistemi per l'ATEX (SIS) – Specifica i manuali operativi e le procedure di sicurezza per l'esercizio (compresi i SIS: frequenza delle prove periodiche, scorte, procedure per la messa in servizio dei SIS delle prove per la "validazione", le procedure che devono essere seguite dall'esercizio in caso di disservizio riscontrato nell'esercizio o durante le prove periodiche) Le informazioni disponibili in questa fase possono coincidere, per contenuti e metodologie, con quanto eventualmente richiesto dal DLgs 334/99 (Legge Seveso) e successive. Modificazioni/integrazioni (per esempio aggiornamento del rapporto di sicurezza, richiesta di non-aggravio di rischio, ecc.). NOTA Le informazioni prodotte saranno anche utilizzate per l'approntamento/aggiornamento degli SSO (standard di sicurezza operativa)	HAZOP FMEA ecc.
B.4	INGEGNERIA	Effettua revisione del Documento di Valutazione dei Rischi (per esempio, 626/94) ed aggiorna se del caso la valutazione ATEX	
B.5	GESTORE PROGETTO	Raccoglie i risultati delle analisi effettuate, le eventuali prescrizioni di Enti Esterni e li allega al BASIC definitivo che trasmette per la fase di DETTAGLIO Identifica in via definitiva gli adempimenti di legge da osservare per il progetto e la documentazione da predisporre e redige CRONOPROGRAMMA. Non appena disponibile invia la documentazione agli Enti proposti e ne segue l'iter	

Fase C: Sviluppo del progetto di dettaglio (Detail Engineering)

Successivamente alla fase di Basic, con l'avanzare del progetto e confermati i capisaldi d'impianto come il processo, la scelta e la disposizione delle apparecchiature superato si arriva alla fase di Ingegneria di Dettaglio dove sono completati prima dell'esercizio della nuova/modificata unità almeno le attività elencate in Tabella B5.

Tabella B.5 – Funzioni responsabili, descrizioni obiettivi e procedure/specifiche per la Fase C di Ingegneria di Dettaglio

Fase C	Funzione Responsabile	Descrizione	PROCEDURA/ SPECIFICA
C.1	Ambiente e Sicurezza (HSE)	Aggiornare il PdS assegnando anche le responsabilità per la predisposizione della documentazione per le autorizzazioni	
C.2	INGEGNERIA	Valutare, verificare ed eventualmente revisionare l'analisi SIL dei SIS sulla base dei documenti di progetto	
C.3	Ambiente e Sicurezza (HSE)	Curare prima dell'avviamento la Revisione di Sicurezza e la Vallidazione del SIS	
C.5	GESTORE PROGETTO	Inoltrare ove necessario le autorizzazioni necessarie prima dell'avviamento e curarne l'iter; in caso di problematiche avvisare tempestivamente (indicare …)	
C.6	INGEGNERIA	Emettere le specifiche di dettaglio del SIS	

Vengono così prodotte:

a) Descrizione del modo di funzionamento della SIF:
   - Controllo di sicurezza *continuo* (continuos mode) metrica: λ (1/y). Si assume che la SIF operi in continuo, se la frequenza presunta di intervento richiesta sia *inferiore alla metà* dell'intervallo delle prove periodiche previste.
   - Intervento di emergenza su domanda (on demand): PFD (-). Si assume che la SIF operi su domanda, se la frequenza presunta di intervento richiesta sia superiore alla metà dell'intervallo delle prove periodiche previste.

b) Descrizione dei ratei di guasto rilevati pericolosi (top per la sicurezza).

c) Descrizione dei ratei di guasto rilevati non pericolosi (top per l'affidabilità: blocchi intempestivi).

d) Descrizione dei ratei di guasto non rilevati pericolosi (top per la sicurezza).

e) Descrizione dei ratei di guasto non rilevati (top per l'affidabilità: blocchi intempestivi).

f) Descrizione dei ratei di riparazione dei componenti.

g) Descrizione dei ratei di intervento ammissibili max.

h) Descrizione dei ratei di guasto sistematico.

i) Descrizione dei ratei di guasto di modo comune dei componenti se in assetto ridondante (Costruttore).

j) Descrizione dei ratei di guasto di modo comune per assetti di loops.

k) Descrizione della Frazione di Guasti Sicuri (SFF) in accordo alla Tabella 5 della CEI EN 61511-1, per componenti programmabili (PE).

l) Descrizione del livello di copertura diagnostica DC (Diagnostic Coverage).

m) Descrizione della modalità di intervento del sistema di protezione in caso di guasto probabile e/o mancanza di alimentazione elettrica, aria strumenti (fail safe)

n) Possibilità di monitoraggio dello stato di corretto funzionamento del componente.

o) Valore del SIL se apparecchiatura dotata di dichiarazione di conformità.

p) Dati tipici relativi ai ratei di guasto "pericolosi" λ_{DU} (1/h) di alcuni componenti di sistemi di regolazione e protezione desunti dal confronto di Banche Dati.

La Figura B.2 illustra in sintesi lo sviluppo delle attività durante tutte le vari fasi di ingegneria del progetto.

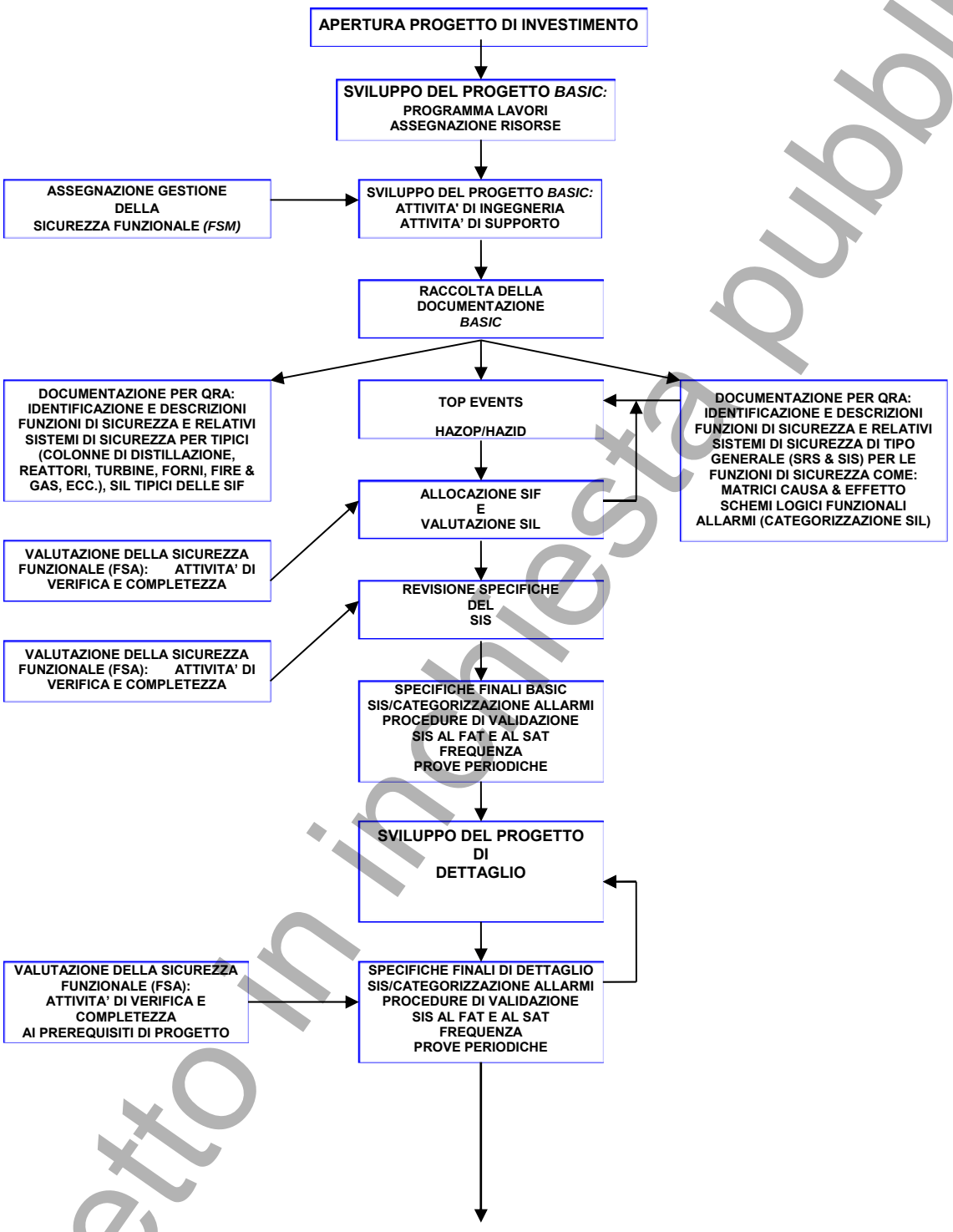


Figura B.2 – Esempio di sviluppo attività delle fasi di progetto

Allegato C

Criteri di individuazione delle SIF nella fase di sviluppo del progetto

C.1 Premessa

La individuazione delle SIF richiede che siano disponibili dati ed informazioni a un sufficiente dettaglio, che è disponibile solo a partire dalla fase di progetto di Basic.

La disponibilità degli schemi semplificati di flusso del processo e la descrizione generale di processo consente di individuare loops fondamentali di regolazione e di protezione. Sulla base di questi (SrS) infatti è possibile pervenire ad una stima di massima del livello di sicurezza offerto dalle IPL a fronte degli Eventi Pericolosi globali (Top Events) individuati nella fase di Preliminary Risk Analysis (PRA). I risultati sono necessariamente parziali ed in genere, non sufficienti per assicurare la completezza dell'analisi, ma per assicurare almeno gli obiettivi di sicurezza ai fini autorizzativi.

Nella fase di Basic gli obiettivi devono essere confermati attraverso la revisione e completamento dell'analisi di rischio sia per gli obiettivi di sicurezza, sia per il fattore di servizio.

La descrizione dei SIL richiede, implicitamente, che siano individuate tutte le SIF.

C.2 Metodologia di individuazione

La individuazione degli eventi anomali e delle cause e la valutazione delle frequenze degli eventi pericolosi, individuati nell'analisi di rischio, sono normalmente condotte applicando le consolidate tecniche dell'HAZOP (Hazard and Operability Study) e Fault Tree o Albero dei Guasti (vedasi anche in proposito CEI EN 61511-3).

Questa metodologia è generale e consente di trattare sistemi molto complessi ed è utilizzata nelle analisi di rischio in vari settori industriali da circa 30 anni[(1)].

Obiettivi dell'analisi HAZOP[(2)] è la individuazione delle potenziali anomalie che possono verificasi nel processo e le conseguenze che ne derivano. L'HAZOP consente la individuazione delle cause e delle misure manuali/automatiche di intervento (Blocchi) e di rilevamento delle anomalie (indicazioni ed allarmi in sala controllo/locale). La tecnica dell'HAZOP prevede raccomandazioni per evitare (o, quantomeno, ridurre la probabilità) la possibilità di verificarsi delle anomalie.

(1) È stata ed è applicata in modo estensivo per le analisi di sicurezza degli impianti nucleari.

(2) È importante sottolineare che l'analisi di affidabilità (l'analisi di rischio contempla necessariamente una analisi di affidabilità e la conoscenza approfondita della disciplina) comporta l'utilizzo di molte tecniche integrate, a seconda della specifica applicazione. L'HAZOP è una di queste e in genere, è integrata da una analisi Event Tree/FMECA (Failure Mode Effect & Criticality Analysis). Infatti, è possibile da una analisi Event Tree/FMECA, definire in modo univoco il Fault Tree (si veda, ad esempio: il codice "Risk Spectrum" che consente di definire completamente il Fault Tree automaticamente (Event Tree Linking).

Le tecniche sopra citate consentono di individuare:

- una elevata percentuale di *eventi anomali potenziali* (HAZOP/FMECA): Top Events di sicurezza (gli stessi del Rapporto di Sicurezza);
- il *numero e la frequenza* dei Top Events per gli aspetti di sicurezza/ambiente (tramite i Fault Tree);
- le *apparecchiature* potenzialmente oggetto di rischio (EUC) ed i sistemi di controllo e protezione relativi ;
- il tipo e numero di barriere di sicurezza: SrS, SIF, SIL associati e relativi SIS;(1)
- il numero e frequenza/durata dei blocchi intempestivi (Fault Tree);
- eventuali interventi tecnico-gestionali per assicurare(2) gli obiettivi di sicurezza/ambiente e fattore di servizio.

NOTA Il processo di valutazione degli obiettivi di cui sopra può richiedere una attività di revisione e/o valutazione di soluzioni progettuali di dettaglio alternative. Infatti, la verifica della indipendenze delle Barriere di Sicurezza si può valutare sulla base del progetto esecutivo e della componentistica, analizzando la documentazione del progetto Basic e Detail).

La disponibilità degli schemi meccanici di processo (P & I) e delle specifiche di base delle apparecchiature e componenti di Impianto (modifica) consente di individuare i loops di regolazione e di protezione, quindi le SIF.

Tuttavia, nell'ottica di valutazione dei SIL delle SIF, è necessario, distinguere due problematiche principali: :

- la prima, riguarda gli aspetti progettuali del SIS (che realizzano le SIF) indipendentemente dalla sua allocazione;
- la seconda, invece, deve tenere opportunamente conto di questi aspetti, ma in un contesto più ampio di sistema che è quello di una sezione o sottosistema di impianto nell'ottica della stima globale delle frequenze dei Top Events.

Per quanto riguarda il primo aspetto, inoltre, è necessario verificare la indipendenza o meno del SIS o di componenti che lo costituiscono, da altri sistemi di protezione o controllo.

Nel caso di indipendenza dei componenti del SIS da altri sistemi la stima del SIL può essere condotta utilizzando metodologie di sufficiente dettaglio, che consentano di definire le architetture dei loop di protezione (o del modo di controllo di sicurezza: high demand mode).

La Figura C.1 illustra i risultati della metodologia di indagine di funzionamento normale ed anormale del processo HAZOP, nella tecnica di analisi del livello di protezione LOPA (Layer of Protection Analysis), richiesto dal processo in esame.

In particolare la Figura C.1 illustra una tipica struttura di Top Event relativo ad un evento alla cui possibilità possono concorrere più eventi primari con relative IPL.

(1) La individuazione dei componenti del SIS è deducibile dalla documentazione di BASIC. Dalla componentistica è agevole sviluppare - per semplicità pratica - l'RBD (Reliability Block Diagram) in quanto descrive in termini logici direttamente dallo schema di processo, lo schema di affidabilità. L'RBD è equivalente al Fault Tree (in termini matematici: Teorema di Neumann) e descrive in logica positiva (di funzionamento e non di guasto) quali sono i componenti che devono funzionare correttamente (secondo le specifiche) per assicurare la prestazione della funzione di sicurezza. L'RBD, inoltre consente di tenere conto di componenti ridondanti diversi, di diverso rateo di guasto (rilevato non rilevato, SFF), di riparazione (Medium Time To Repair, MTTR) e di tempo di intervallo (Time Interval, TI) delle prove periodiche (Proof Tests).

(2) Gli obiettivi e relativi costi sono – nei margini delle tolleranze ammissibili – già definite nella fase di pre-fattibilità per le necessarie autorizzazioni al finanziamento della nuova attività (modifica).

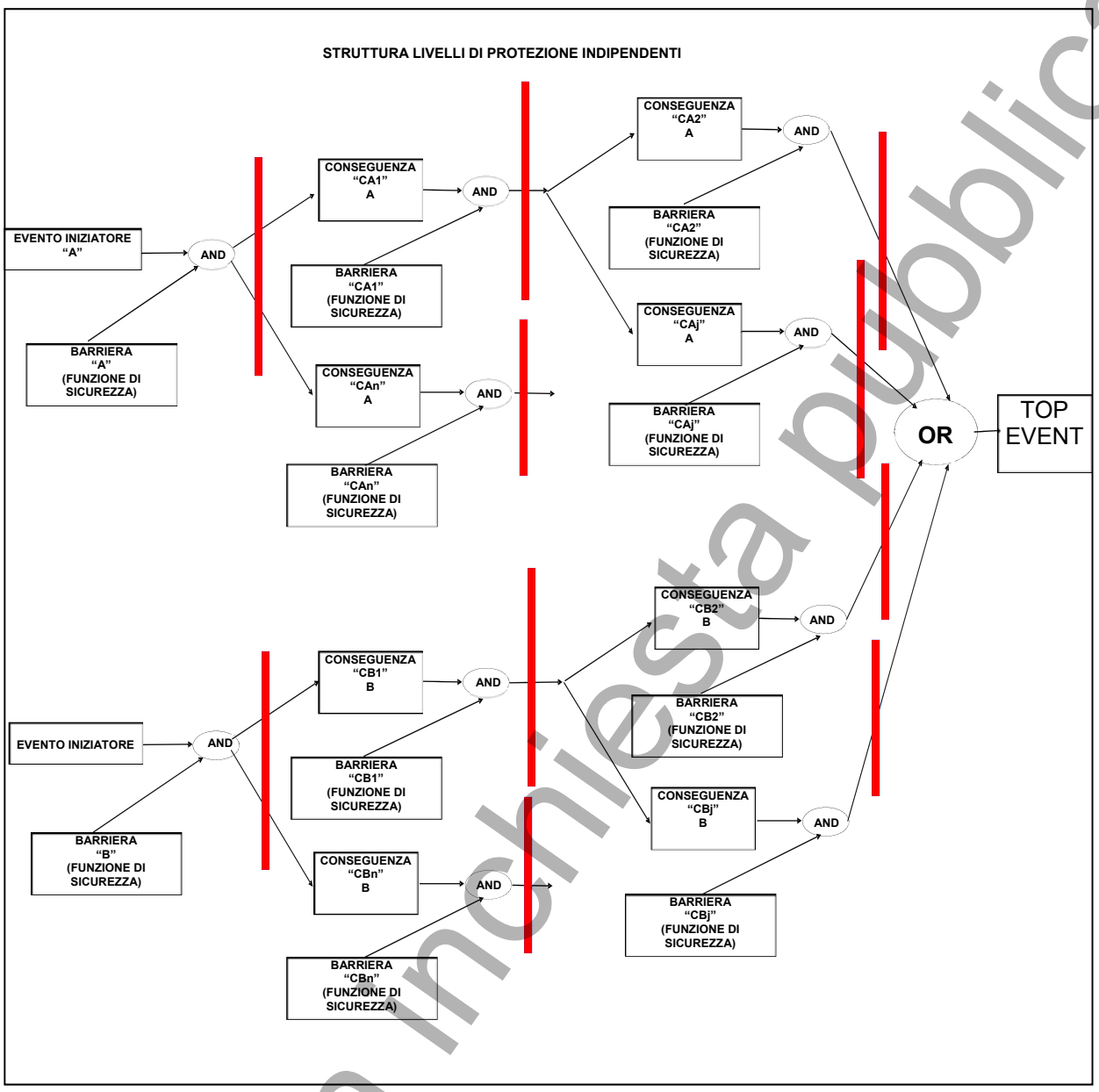


Figura C.1 – Tipica struttura di protezione derivata da una analisi dei livelli di protezione (LOPA) a valle di una metodologia di indagine del processo (HAZOP)

Allegato D

Criteri di valutazione dei SIL delle funzioni strumentate di sicurezza (SIF)

D.1 Premessa

Per valutare i Livelli di Integrità di Sicurezza SIL delle Funzioni Strumentate di Sicurezza SIF, si devono preliminarmente condurre le seguenti fasi di analisi:

I) Individuazione di unità di processo "tipiche" delle quali sono noti i rischi specifici (Top events) e le sicurezza di progetto (nel caso) intrinseche, nonché gli aspetti di sicurezza totalmente od in parte già coperti da normative:

- Colonne di distillazione
- Reattori con processi fuggenti (runaway)
- Reattori in cui determinati disservizi possono condurre di seguito a fenomeni di polimerizzazione anomala con perdita economica
- Forni
- Turbine (API)
- Caldaie (EN 764)
- Macchine specifiche (EN 62061)

Queste Unità od Apparecchiature sono assunte come "standard" e di cui sono consolidati i criteri di protezione contro gli eventi pericolosi (Top Events) e le relative barriere di protezione indipendenti (IPL): sistemi di controllo, di protezione (sistemi di blocco) valvole di sicurezza. Sulla base del livello di rischio e della soglia di accettabilità del(i) Top Event(s) si calcola il SIL della (SIF) quale barriera di protezione indipendente.

Il SIL verificato corrisponde al SIL di riferimento per un'Unità tipica. Per tutte le Unità analoghe si riferirà al livello di SIL sopra verificato per le Funzioni di Sicurezza dell'Unità.

Questo approccio vale anche per le macchine (ad esempio le Turbine) mentre per le Unità di processo o nuove Apparecchiature di cui non si ha esperienza pregressa, si applica il criterio della Analisi Quantitativa del Rischio QRA (Quantitative Risk Assessment).

Lo schema proposto per la classificazione del SIL delle SIF nel caso di applicazione della tecnica del QRA si basa sulla metodologia quali-quantitativa, partendo dal presupposto che determinate attività sono normalmente condotte in fase di Basic.

La documentazione necessaria è costituita da P&I preliminari redatti dalla divisione Tecnologia (o disponibili su Documenti del Licenziatario) e descrizione del Processo in cui siano evidenziati gli aspetti di sicurezza progettuale (Intrinseca) ed i criteri di sicurezza.

II) Analisi HAZOP modificato con inserimento delle IPL (quantificate) su uno schema LOPA.

III) Individuazione dei Top Events sulla base dei Dati Storici ed HAZOP.

IV) Individuazione delle singole cause che possono condurre al Top Event senza le relative IPL ed a ciascuna causa definire l'obiettivo di accettabilità della frequenza del Top Event.

V) Costruzione della catena che conduce al Top Event, tenendo conto delle IPL per ciascuna catena.

VI) Costruzione della logica OR di tutte le catene per ciascuna causa (e relative IPL) che conducono al Top Event.

VII) Definizione dell'Albero dei Guasti (ad Alto Livello) che conduce al Top Event.

VIII) Descrizione dei sistemi di controllo di sicurezza/protezione e descrizione in termini di Reliability Block Diagram (RBD). Da osservare che la descrizione dal punto di vista affidabilistico dell'RBD è strettamente legata alla descrizione della componentistica che deve essere funzionante per assicurare le funzioni del SIS che realizza. Questa descrizione è più semplice per il progettista, perché simile a quella di progetto del sistema. Da un secondo punto di vista, la descrizione con RBD di un sistema SIS è perfettamente equivalente, da un punto di vista matematico, a quella dell'Albero dei Guasti (secondo il Teorema di Neumann).

D.2 Esempio: Colonne di distillazione

Le colonne di distillazione costituiscono Unità di processo che sono, in generale, caratterizzate da specificità, con riferimento ai rischi potenziali associati all'esercizio.

Si distinguono due tipologie di progetto:

- Distillazione in "pressione",
- Distillazione "sotto vuoto".

La descrizione dei Sistemi di Protezione e del livello di Sicurezza Funzionale associati alle Funzioni Strumentate di Sicurezza (SIF) di una colonna con esercizio in *pressione* è definita sulla base dei *rischi potenziali* imputabili al progetto ed esercizio del sistema succitato.

Oltre gli aspetti di protezione contro gli incendi, l'attrezzatura a pressione richiede la verifica delle valvole di sicurezza contro eventi di sovrappressione.

Dalla analisi di una elevata casistica di progetti e applicazioni, i Top Events individuati dall'esercizio di una colonna in pressione possono essere classificati come "tipici":

1) altissima pressione colonna;
2) "inondazione colonna (flooding);
3) "sezionamento colonna".

Top Event n. 1: Altissima pressione colonna:

Le protezioni normalmente adottate contro l'evento 1) è la valvola di sicurezza; nel caso che lo scarico della valvola sia convogliato con in materiali adatti al fluido (nel caso di gas liquidi) può essere previsto un sistema di blocco indipendente dal controllo della pressione.

Nel caso in cui le valvole prevedano lo scarico diretto in atmosfera (da verificare con le normative adottate di progetto - Basic Practices), deve essere specificato il livello di integrità del sistema di blocco contro la sovrappressione e l'altissimo livello.

Se λ_{Target} è la soglia di sicurezza assunta del Top Event contro l'altissima pressione, il Fattore di Riduzione del Rischio (RRF = 1/SIL) diventerà $\lambda_{Target} = \lambda \times IPL \times SIL$, avendo indicato con SIL il Livello di Integrità di Sicurezza dei SIS a fronte della riduzione della frequenza dell'evento di altissima pressione, tenuto conto delle Barriere di Sicurezza Indipendenti previste (IPL): Sistema di Controllo, Intervento dell'Operatore su Allarmi, Blocco Automatico, Valvole di Sicurezza.

Assumendo che sia definibile una variabilità della frequenza di perdita del controllo della pressione per cui si richiede un intervento di protezione contro la sovrappressione, lo schema normalmente adottato contro questo evento per il loop è realizzato con la logica funzionale di blocco riportata nella Matrice Causa/Effetti. La Funzione di Sicurezza individuata è la *"riduzione della pressione"* a valori inferiori della taratura della PSV (SIF).

L'architettura del sistema di protezione contro la pressione è normalmente realizzato da un SIS costituito da:

a) un sensore di pressione (pressostato);
b) una logica di blocco;
c) valvole di intercettazione della carica e del calore ai ribollitori.

Il SIL di questa Funzione di Sicurezza costituisce una IPL unitamente al BPCS, gli Allarmi e la Valvola di Sicurezza (PSV).

Analoga considerazione vale per i condensatori (EUC) per quanto attiene il controllo del livello (marcia/arresto pompe).

Le Basic Practices richiederebbero che se è previsto un controllo di livello con funzione di blocco, il sistema di blocco sia indipendente. Questa considerazione tiene conto che in caso di disservizio del sistema di controllo le conseguenze siano accettabili sia dal punto di vista sicurezza/ambiente, sia per i possibili danni ai beni.

NOTA Nella valutazione del SIL di una SIF, si deve tenere conto che una Funzione di Sicurezza (SF) non è sempre realizzata da un SIS, ma anche da un SrS, in genere.

Infatti, se si considera la funzione di sicurezza "Marcia/Arresto di una Pompa" per un Controllo di Livello, è necessario definire il sistema di protezione/comando e il motore/pompa.

Se qualunque di questi componenti non risulta efficiente al momento dell'intervento, la Funzione di Sicurezza fallirà la prestazione per cui è stata realizzata. Sarà, pertanto, necessario considerare nella stima della metrica associata alla Funzione di Sicurezza anche il motore e la pompa, oltre che il sistema elettrico (Contattore) e strumentale (SIS: loop di strumentazione dal sensore al relè di interfaccia ELE/STRU).

Top Event n. 2: Inondazione colonna:

Relativamente a questo secondo Top Event di inondazione "flooding" valgono le medesime considerazioni.

Infatti, sono identificabili le IPL costituite dal BPCS, Allarmi e SIS. Si assume che in caso di altissimo livello della colonna, il riempimento "overfilling" sia convogliato a scarico "blowdown" (compatibile con il fluido alle condizioni di scarico).

Nel caso ciò non fosse (scarico all'atmosfera) il Top Event richiede un diverso Target. La riduzione del Rischio è sempre realizzata dalle IPL.

Top Event n. 3: Sezionamento colonna:

Il *Sezionamento della Colonna* è attuato in condizioni di emergenza di impianto e fondamentalmente, in caso di incidente "rilevante".

La funzione di Sezionamento della Colonna si assume come l'unica Barriera di Sicurezza Indipendente efficace. Il SIL della SIF è 3 (possibilmente 4).

In questo caso si vuole notare che la Norma EN 61511-1 al paragrafo 9.3 sconsiglia la realizzazione di un SIS con SIL 4, perché non solo è difficilmente realizzabile, ma anche perché difficilmente gestibile per assicurarne nel tempo il livello, pertanto il SIL associato alla Funzione di Sezionamento della Colonna in Oggetto, sarà, quindi SIL 3.

La conformità ai requisiti di SIL 3 è vincolata principalmente dalla valvola di sezionamento fondo colonna (una sola valvola). Infatti, la conformità della valvola di sezionamento al SIL 3 richiede o una ridondanza (doppia valvola) come valvola classificabile "proven use" e "prior use" (ai sensi dei requisiti della EN 61508 o EN 61511) oppure una certificazione in accordo ai requisiti della EN 61508-2.

La riduzione del rischio normalmente accettata è solitamente da 1 000 a 10 000 volte.

Da quanto sopra consegue che se si assume una frequenza di Target per l'evento di "Mancato sezionamento grandi capacità" di 10^{-7}/anno, il rischio residuo non potrà essere inferiore a 10^{-3}/anno.

D.3 Esempio: Reattori con processi fuggenti "runaway" (EUC)

I Reattori in cui sono possibili reazioni runaway prevedono IPL costituite da BPCS, Allarmi ed un sistema di blocco indipendente (SIS).

Il Top Event ipotizzato, in caso di mancanza di intervento dei sistemi di protezione, è il "Collasso del Reattore per Altissima Temperatura".

La SIF realizzata dal SIS (sistema di blocco) è la intercettazione della carica in ingresso, dell'uscita e dello scarico a blowdown.

Nella matrice Causa/Effetti sono riportate le funzioni sopraccitate.

L'intervento efficace delle azioni di cui sopra realizza la Funzione di Sicurezza. Essa, quindi costituisce una Barriera di Protezione Indipendente (IPL). Normalmente esiste il solo blocco come barriera di sicurezza contro l'evento di Collasso del Reattore; infatti le valvole di sicurezza non sono efficaci contro questo evento.

Ne consegue che l'obiettivo di sicurezza adottato contro il possibile verificarsi di questo evento non è raggiungibile con la sola barriera strumentale.

Basta pensare che, se la sola barriera di sicurezza è fornita dal sistema di blocco, ad esso è attribuito il massimo livello SIL 3 praticamente realizzabile da una sola SIF.

La stima del Top Event, assumendo che non si possa escludere un disservizio di controllo nell'arco di una decina di anni (ottimistico) risulterà:

$\lambda_{Top} = \lambda Contr. \times SIL\ 3 = < 0{,}1 \times 10^{-4} = < 10^{-5}$ occorrenze per anno.

Il SIL di questa singola Funzione di Sicurezza non può essere superiore a 3, quindi con una riduzione da 1 000 a 10 000 volte. La frequenza del Top Event può essere prossima alle soglie di *remota possibilità*, ma non di *escludibilità* (10^{-7}/anno). In tal caso, è necessario intervenire con modifiche di processo o con barriere a monte per ridurre la probabilità del disservizio. Nel caso, invece, che la soglia di accettabilità delle conseguenze dell'evento di collasso del reattore (non si esclude la possibilità di accadimento dell'evento di collasso del reattore) sia dell'ordine di 10^{-5}/anno, anche una sola SIF con SIL 3 sarebbe sufficiente.

Requisiti di conformità del loop di protezione per SIL 3:

È richiesta la ridondanza delle valvole se classificabili "prior use", è sufficiente una Valvola singola se questa è provvista di dichiarazione di conformità alla EN 61508-2; il Sistema di sensori e/o Logica di blocco (sia analogico che digitale: bus di campo certificati SIL 3) consente normalmente di assicurare l'utilizzo (capability) per SIL 3.

Nel caso che non sia possibile raggiungere l'obiettivo (target) prefissato normalmente non inferiore a 10^{-6} - 10^{-7}/anno, è necessario introdurre IPL interne (ad esempio, l'incremento di sicurezza funzionale del BPCS con riduzione della frequenza della possibile anomalia del sistema di controllo che richiede l'intervento della protezione) ed esterne all'EUC (nel caso di cause esterne di processo che possano contribuire all'evento anomalo) oppure apportare modifiche di processo (tecnologia).

Allegato E

Architetture di sottosistemi per tipici livelli di SIL di determinate SIF

E.1 Premessa

La stima del SIL di una SIF dipende dai dati relativi a potenziali guasti casuali e sistematici (HW & SW) e dalla efficacia della diagnostica, in altre parole dalla frazione di guasti sicuri (SFF) che si rilevano in caso di richiesta o durante il funzionamento di un sistema di controllo o protezione di sicurezza con perdita della Funzione.

Considerando un tipico loop di protezione, gli elementi fondamentali sono costituiti da:

- sensori misura;
- risolutori logici;
- elementi finali;
- accessori (quali interfaccia con il processo, morsettiere, ecc.).

È necessario distinguere due situazioni:

1. Componenti a cui è associato un SIL conforme alla Norma CEI EN 61508-2 Route $_{1H}$, soluzione prevista per normali componenti
2. Componenti a cui è associato un SIL conforme alla Norma CEI EN 61508-2 Route 2_H, soluzione prevista per speciali componenti provati anteriormente "proven use" e "prior use", soluzione prevista anche dalla CEI EN 61511-1

Inoltre, per i componenti a cui è associato un SIL è necessario distinguere a quale categoria sono assimilabili (vedasi a tal proposito la Tabella E.1):

- Bassa complessità (Tipo A)
- Alta complessità (Tipo B)

Tabella E.1 – Tipica classificazione ad alta e bassa complessità dei componenti

COMPONENTE Bassa complessità Tipo A	COMPONENTE Alta complessità Tipo B
Relé elettromeccanico	Analizzatori
Fine corsa meccanico	Fine corsa elettronico
Trasmettitore pneumatico	Trasmettitore elettronico
Logica di controllo non programmabile	Logica di controllo programmabile
Valvola di regolazione standard	Valvola regolazione con posiz. elettronico programm.
Valvola di sicurezza	Valvola sicurezza con pilota elettronico programmabile
Disco di rottura	Sistema di comunicazione digitale di campo (fieldbus)
Soglia elettronica	Moduli interfaccia digitali di sistemi misura e controllo
Barriera elettronica a sicurezza intrinseca	
Interruttore di potenza	
Contattore elettromeccanico	
Sistemi di allarme cablati (hardwired)	

E.2 Tipi di architetture

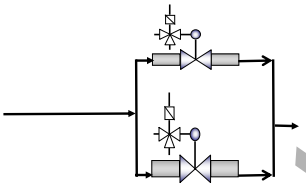
Per i tipi di architetture si rimanda alle precedenti Tabelle 9 e 10, rispettivamente per soluzioni architetturali secondo la Route $_{1H}$ e secondo la Route $_{2H}$.

E.3 Esempio di calcolo del SIL

Sia da verificare la compatibilità di un sistema SIL 2 composto dai seguenti elementi:

- Elementi Finali : compatibili SIL 2 in architettura 1oo2
- Sensori : compatibili SIL 2 in architettura 1oo2
- Risolutore logico : compatibile SIL 3 in architettura 1oo1

Il sottosistema Elementi Finali è composto da 2 valvole di blocco e relative elettrovalvole in architettura 1oo2 come da schema:



Il sottosistema è ridondante ed è costituito da una valvola di blocco e relativa elettrovalvola e l'azione prevista dalla SIF è quella di assicurare la portata.

In caso di blocco in chiusura di una valvola, la portata (SIF) è assicurata dall'apertura della seconda valvola.

Caso del Calcolo del SIL del sistema con componenti SIL 2:

a) Compatibilità del SIL:

   Risulterà per il singolo canale la compatibilità per SIL 2, in quanto ciascun componente è compatibile per SIL 2.

b) Verifica probabilistica SIL 2:

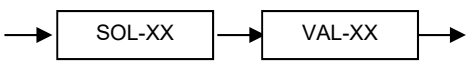
   Dai dati del Costruttore del Solenoide dell'elettrovalvola e della Valvola di blocco si assume (il dato preciso deve essere fornito dal Costruttore o dalla Certificazione) che le PFD siano, rispettivamente:

$PFD_{Sol} = 3.10^{-3}$

$PFD_{Val} = 5.10^{-3}$

Lo schema di disponibilità

è:



Per cui si avrà:

$PFD_{Elemento\ Finale} = 5.10^{-3} + 3.10^{-3} = 8.10^{-3}$

Valore che rientra nel campo del SIL 2.

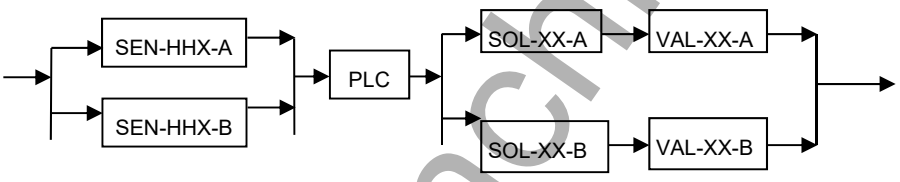
Se si considera invece che i singoli componenti sono di Tipo A a "bassa complessità" sempre compatibili per il SIL 2, ma con queste caratteristiche specifiche fornite dal costruttore per il completo elemento finale e dall'Utente per l'esercizio dell'impianto:

- λ = 10^{-6} : ovvero tasso di guasto totale per ora
- λ_D = $\lambda/2$: ovvero tasso di guasto dannoso per ora (supposto)
- β = 20 % : ovvero frazione di guasti comuni
- β_D = 10 % : ovvero frazione di guasti comuni rilevati dalla diagnostica
- DC = 0 % : ovvero copertura diagnostica specifica del sottosistema
- MTTR = 8 h : ovvero tempo medio di riparazione del sistema
- TI = 1 y : ovvero intervallo tra le prove periodiche

si ottiene nel caso di ridondanza completa dell'elemento finale (con architettura 1oo2, che ottempera alla minima ridondanza di una unità prevista dalla Tabella 9), per applicazioni in SIL 2 di componenti con tipica frazione dei guasti sicuri SFF < 60%), un sistema con PFD_{1oo2} pari a $4{,}4 \cdot 10^{-4}$ (vedasi anche Allegato H ed I, ovvero Tabella B.3 della CEI EN 61508-6) e quindi compatibile con SIL 3.

Analoga analisi può essere condotta anche per sensori di Tipo A compatibili per il SIL 2 (con stesse caratteristiche operative e funzionali) nel caso di ridondanza con architettura 1oo2.

Supponendo di avere un risolutore logico (PLC) di Tipo B ad "alta complessità" compatibile per il SIL 3 (con architettura 1oo1, che ottempera alla possibilità di non ridondanza prevista dalla Tabella 10 ovvero dalla Tabella 3 della CEI EN 61508-2, per applicazioni in SIL 3 di componenti con tipica frazione dei guasti sicuri SFF>99%), lo schema di disponibilità dell'intero sistema, sarà il seguente:



ove la Probabilità di Guasto su Domanda (PFD) del sistema è data dalla seguente:

$PFD_{Sistema} = PFD_{Sensori} + PFD_{Logica} + PFD_{Elementi\ Finali}$

ovvero:

$PFD_{SYS} = PFD_{S\ @1oo2} + PFD_{L\ @1oo1} + PFD_{FE@1oo2}$

dove le singole PFD, calcolate in relazione all'architettura prevista, valgono:

$PFD_{S\ @1oo2} = 4{,}4 \cdot 10^{-4}$ valore calcolato dall'architettura duale (ridondante)

$PFD_{L\ @1oo1} = 5 \cdot 10^{-4}$ valore fornito dal costruttore (non calcolato)

$PFD_{FE@1oo2} = 4{,}4 \cdot 10^{-4}$ valore calcolato dall'architettura duale (ridondante)

per cui in ultima analisi risulta una PFD del sistema pari a:

$PFD_{SYS} = 4{,}4.10^{-4} + 5.10^{-4} + 4{,}4.10^{-4} = 1{,}38.10^{-3}$

ovvero compatibile con il SIL 2.

Pertanto un sistema di protezione costituito da sensori ed elementi finali ridondanti in architettura 1oo2 e conformi SIL 2 con un solo risolutore logico (PLC) conforme SIL 3, è compatibile con il SIL 2.

Da quanto sopra, ne consegue però che in caso di sottosistemi a singolo canale (sensori ed elementi finali non ridondanti) costituiti sempre dagli stessi componenti:

- Sensori conformi a SIL 2 : con PFD_{S} = $5 \cdot 10^{-3}$ (per esempio)
- Risolutore logico a SIL 3 : con PFD_{L} = $5 \cdot 10^{-4}$ (fissato prima)
- Elemento Finale conforme a SIL 2 : con PFD_{FE} = $8 \cdot 10^{-3}$ (calcolato prima)

risulterebbe invece:

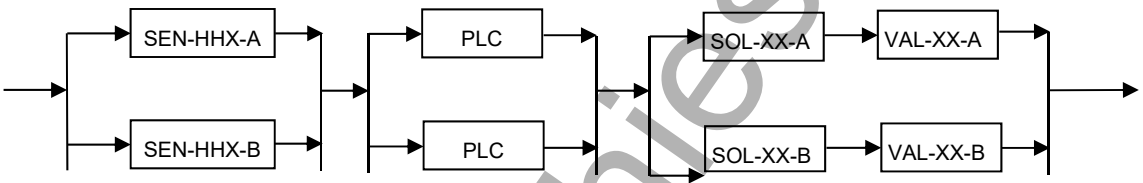
$PFD_{SYS} = PFD_{S} + PFD_{L} + PFD_{FE} = 5 \cdot 10^{-3} + 5 \cdot 10^{-4} + 8 \cdot 10^{-3} = 1{,}35 \cdot 10^{-2}$

ovvero solo compatibile con il SIL 1 e perciò non idoneo all'applicazione SIL 2.

Caso di calcolo del SIL del sistema con componenti SIL 2 "Route $_{2H}$"

In questo caso si può utilizzare la Tabella 6 della CEI EN 61511-1 (Tabella 10), anziché le Tabelle 2 e 3 della CEI EN 61508-2 (Tabella 9), che è più vantaggiosa, in quanto si basano sull'impiego di componenti già provati anteriormente ("proven use" e"prior use") e pertanto con disponibilità di dati statistici sufficienti per convalidare le probabilità di guasto dichiarate.

Nell'ottica di verificare il SIL di un sistema ridondato, si ricadrebbe, in questo caso e nelle ipotesi validità delle condizioni di conformità ai requisiti di 11.5 della stessa CEI EN 61511-1.



In riferimento sempre alla CEI EN 61511-1 e applicando un SIS con sottosistemi ridondati a logica 1oo2 e pertanto con HFT=1, le singole PFD dei sottosistemi sono pari a:

$PFD_{S\ @1oo2} = 4{,}4 \cdot 10^{-4}$ valore calcolato in precedenza

$PFD_{L\ @1oo2} = 4{,}4 \cdot 10^{-5}$ valore ora calcolato (Tabella B.3: CEI EN 61508-6)

$PFD_{FE@1oo2} = 4{,}4 \cdot 10^{-4}$ valore calcolato in precedenza

per cui in questa ultima analisi risulta una PFD del sistema pari a:

$PFD_{SYS} = 4{,}4 \cdot 10^{-4} + 4{,}4 \cdot 10^{-5} + 4{,}4 \cdot 10^{-4} = 9{,}24 \cdot 10^{-4}$

ovvero compatibile con il SIL 3.

Pertanto un sistema di protezione costituito da componenti distinti, ridondanti e conformi SIL 2 con un risolutore logico (PLC) conforme SIL 3, pur esso ridondato, rende tutto il sistema compatibile con il SIL 3.

Questo grazie al credito di ridondanza previsto solitamente dalla Route $_{2H}$ con componenti provati anteriormente rispetto la Route $_{1H}$ con componenti normali di ci non si conoscono effettivamente i parametri affidabilistici in utilizzazione.

Limitazioni

La stima del SIL di un sistema di controllo o di protezione di sicurezza richiede una attenta analisi ed applicazione degli articoli normativi. Ciò conduce ad una stima numerica che costituisce un fattore determinante del progetto delle architetture dei sistemi di sicurezza.

La stima probabilistica non deve essere vanificata dal concetto probabilistico soprattutto se esso è obiettivo di una valutazione più ampia e complessa quale quello relativa alla stima dei Top Events, in cui i sistemi di protezione giocano un ruolo decisivo.

I due aspetti devono essere separati:

- SIL delle SIF, e
- Frequenza dei Top Events.

Nella stima della PFD (o analogamente, della frequenza, per i sistemi di controllo di sicurezza) può verificarsi il caso che il valore numerico sia prossimo ad un limite del campo del SIL.

Da un punto di vista pratico, ciò comporterebbe un impatto significativo a livello impiantistico per gli aspetti di eventuali ridondanze (programmi di verifiche periodiche, scorte a magazzino, ecc.), per cui l'utente finale può porsi il problema decisionale della valutazione del SIL effettivo.

A questo proposito bisogna sempre tenere presente che il SIL valutato con le procedure delle Norme, prevedono ridondanze minime. I fattori importanti che possono condurre ad una decisione corretta, per gli aspetti di sicurezza sono legati oltre che al valore della stima del SIL alla sua prossimità al limite del campo, ma anche dal livello di SIL in oggetto e soprattutto dalla pratica rispondenza delle soluzioni tecnologiche ai consolidati assetti impiantistici per quel tipo di applicazioni.

Le potenziali azioni alternative consistono in:

- intervento sul tempo delle prove periodiche;
- ridondanza del canale;
- incremento delle SIF.

Ciascuna di esse deve essere valutata in funzione del livello di rischio a cui fanno fronte le SIF.

Note e Suggerimenti:

a) Non si può ottenere senza ridondanza per il sistema un SIL maggiore di quello dei sottosistemi.

b) Evitare possibilmente di impiegare sottosistemi che operano in prossimità del limite del proprio SIL.

c) Utilizzare ridondanze per incrementare il SIL specifico dei componenti dei sottosistemi.

d) Utilizzare comunque le ridondanze minime previste dalla Tabelle 6 CEI EN 61511-Tabella 10).

Allegato F

Linea guida per le prove di accettazione

F.1 Premessa

Le prove di accettazione in fabbrica devono essere effettuate sulla versione disponibile e definita del sistema strumentato di sicurezza (SIS).

Le prove di accettazione in fabbrica devono essere effettuate in accordo al loro piano di attuazione, al fine di dimostrare il corretto funzionamento delle logiche del SIS.

Nei casi di risultati di prova negativi, si deve documentare ed analizzare i motivi dell'insuccesso, mettendo in atto le azioni correttive più opportune.

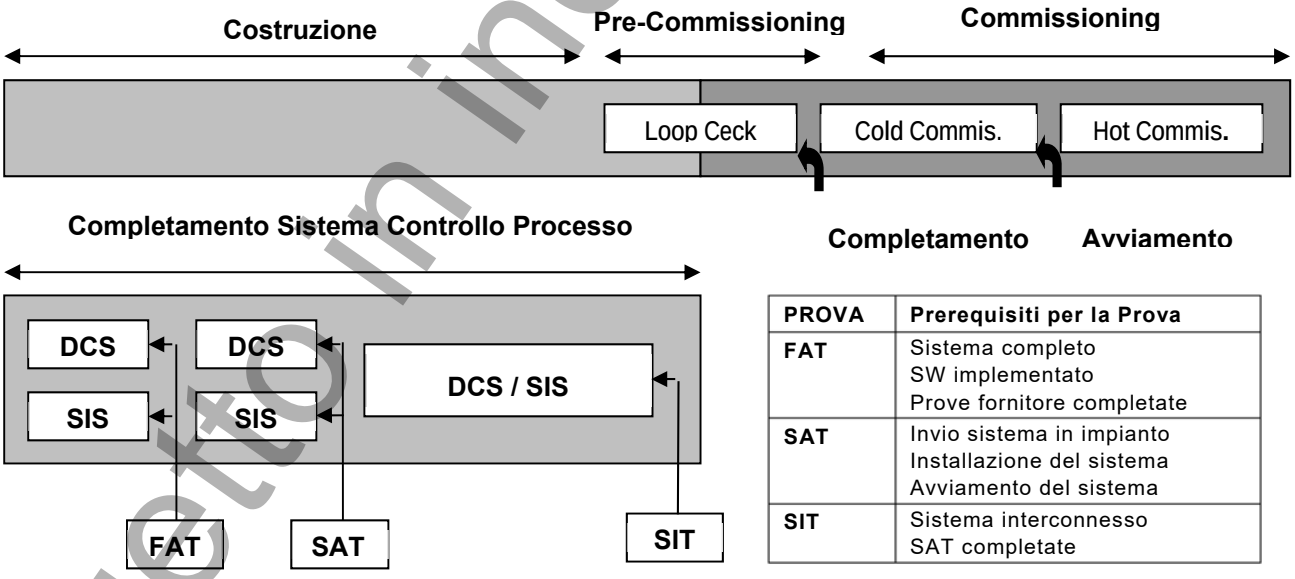
Le prove che non possono essere condotte fisicamente devono essere dimostrate tramite ragionamenti formali che spiegano i motivi per cui il SIS soddisfa i requisiti, gli obiettivi o le limitazioni imposte.

Un riferimento normativo importante relativamente alle prove di accettazione è rappresentato dalla recente norma IEC 62381: "Automation Systems in the Process Industry:

- Factory Acceptance test (FAT)
- Site Acceptance Test (SAT)
- Site Integration Test (SIT)

e dalla ulteriore norma IEC 62382: "Electrical and instrumentation loop check" ovvero "Verifica collegamento elettrico tra strumenti".

La seguente Figura, tratta dalla IEC 62381, ben evidenzia la sequenza delle prove sopra descritte durante la fase di costruzione ed avviamento (Loop Check e Commissioning) del Sistema di Controllo DCS e del relativo Sistema Strumentato di Sicurezza SIS.



PROVA	Prerequisiti per la Prova
FAT	Sistema completo SW implementato Prove fornitore completate
SAT	Invio sistema in impianto Installazione del sistema Avviamento del sistema
SIT	Sistema interconnesso SAT completate

La responsabilità della stesura delle modalità di esecuzione della prova è del Contrattista (integratore di impianto), la responsabilità per l'esecuzione della prova è del Costruttore (costruttore quadro e sviluppatore software applicativo).

La prova deve essere presenziata dal rappresentante del Cliente Utilizzatore e dovrebbe essere ispezionata dal Valutatore (Assessor).

I risultati delle prove di collaudo in fabbrica devono essere documentati, specificando:

a) il tipo di prova;

b) i risultati della prova;

c) se gli obiettivi ed i criteri della prova sono stati raggiunti.

Per una tipica rapportazione delle verifiche e prove vedasi anche le due seguenti Tabelle, tratte sempre dalla IEC 62381.

Verifiche documenti

Rif.	Documento esaminato	Risultati Prova	NOTE
N		☐ P ☐ F ☐ NA	

Verifiche funzionali

Rif.	Descrizione Prova	Risultati Prova
N		☐ P ☐ F ☐ NA

P = Pass: OK

F = Fail: KO

NA = Not Applicable: Non Applicabile

F.2 Lista di Controllo per FAT

Modalità di esecuzione delle prove, loro descrizione ed esempio di dati di prova.

Voce	Dati	Descrizione
01	Dipendenza da altri sistemi/interfacce.	Il quadro può operare in modo autonomo (stand alone), interagisce direttamente (hardwired) e attivamente con gli altri sistemi E' inoltre collegato via rete ethernet separata da firewall e server al BPCS. Il collegamento fornisce informazioni di diagnostica e stati di funzionamento per animazione pagine video di supervisione.
02	Ambiente di prova e strumenti	– Officina elettromeccanica con temperatura 20°C, umidità 50% – Alimentazione 23V c.a./50Hz da rete – Alimentazione 110V c.c. da ponte raddrizzatore – Personal Computer XXX modello YY – Multimetro digitale XXX modello YY numero di serie 810192 – Generatori di corrente XXX modello YYY numero di serie ZZZ – Trasmettitore e sensore di temperatura XXX modello YYY numero di serie ZZZ – Calibratore elettronico XXX modello YYY numero di serie ZZZ – Termoigrometro XXX modello YYY numero di serie ZZZZ – Multimetro XXXX modello YYYY numero di serie ZZZ – Dispositivo per prove elettriche XXX numero di serie
03	Configurazione del sistema di elaborazione delle logiche di sicurezza	Basato su prodotto XXXXXXX in configurazione fault tolerant SIL N° per ingressi tripli (allegato disegno).
04	Criteri di prova sulla base dei quali verranno giudicati i risultati delle prove	Descrivere …
05	Procedure per azioni correttive da implementare in caso di esito negativo	Come dal Piano di qualità della Progettazione Rev.xx

(continua)

Voce	Dati	Descrizione
06	Livelli di competenza del personale coinvolto nelle prove	Responsabile fornitura Contrattista (integratore di impianto) Responsabile integratore di sistema Responsabile fornitura HW (costruttore quadro) Responsabile fornitura SW (sviluppatore software applicativo) Rappresentante Cliente (Utilizzatore) Ispettore/Valutatore (Assesor)
07	Località dove sono effettuate fisicamente le prove	Società XXXX, via……., città…..

(fine tabella)

F.3 Documentazione di Collaudo per FAT

Elenco documentazione di riferimento per il corretto svolgimento delle prove.

Voce	Descrizione	Riferimento
01	Specifica dei requisiti di Sicurezza (Safety requirement Specification)	– Avviamento/arresto generale di impianto-Specifica di processo XXX Rev. 00 – Procedure di gestione impianto-descrizione e gestione dei dispositivi di blocco di emergenza XXXXXX Rev. 00
02	Descrizione del SIS	Certificato/Dichiarazione di conformità emessa da zzzzz (Ente Notificato)) No.: xxxxxxxxxxx datato gg.mm.aa
03	Riferimento al P&I	– Process Flow Diagram di impianto XXXXXX Rev. 00 – Main Interlock System Simplified Diagram XXXXXX Rev. 00
04	Specifica di Progetto Funzionale (Functional Design Specification)	– I/O list ESD XXXXXXX Rev. 00 – I/O list blocchi XXXXXX Rev. 00 – Schemi logici automazione XXXXXX Rev. 00 – Descrittivo Automazione e Controllo XXXXXXXX Rev. 00
05	Disegni del Quadro	XXXXXXXXXXXX Rev. 00
06	Specifica Hardware & Software	Specifica Tecnica xxxxxxxx, revisione 01
07	Manuali	Manuale Equipment 1, Manuale Package 2, manuale gruppo 4, manuale sistema 6
08	Documentazione di fascicolo	– Certificato terza parte e rapporti – Certificato conformità CE – Altro certificato ENTE – Elenco componenti critici per … – Copia foglio dati alimentazione – Copia foglio dati relé – Copia foglio dati interruttori – …….
09	Norme e Regole Tecniche (Standards & Regulation)	89/106/CE CE Marcatura 89/336/CE EMC Direttiva 93/68/CE LV Direttiva 94/9/CE ATEX Direttiva EN-CEI 61508 EN-CEI 61511
10	Requisiti di riduzione del rischio (Risk Reduction Requirements)	Documento Valutazione Rischio, XXXXXX Rev. 00

F.4 Prove standard per FAT

Voce	Descrizione Prova	Risultato
01	Prove da eseguirsi durante l'assemblaggio della struttura di supporto del quadro: a) Controllo Visivo e Dimensionale b) Controllo verniciatura c) Controllo dello spessore della lamiera d) Prove di funzionamento meccanico e) Controllo grado di protezione	Descrivere come primo esame visivo l'idoneità della carpenteria e della eventuale custodia come colore, aspetto, gradi di protezione IP XX Vedere disegno xxxxxxxx Rev. 00 pag. XX
02	Prove da eseguirsi durante l'assemblaggio della struttura di supporto del quadro: a) Verifica allacciamento morsettiere di interfaccia b) Verifica facile accessibilità e rimozione dei singoli componenti c) Verifica del circuito di terra	Verificare la positiva/negativa prova di rigidità dielettrica nel rapporto prova xxxxxxxx
03	Prove di verifica idoneità materiali alle condizioni ambientali incluso immunità da EMC.	Controllare da certificazioni o dichiarazioni, i seguenti punti: – Dichiarazione CE di conformità del quadro – Dichiarazione di conformità dei prodotti XXXX serie YY – L'apparecchiatura con temperatura di funzionamento più alta è la CPU che con condizioni ambientali nominali di 20°C e senza ventilazione forzata questa raggiunge i 40°C (Allegare mappa temperature rilevate). – L'interfaccia con temperatura di funzionamento più bassa sono i relé che con condizioni ambientali di 20°C e senza ventilazione forzata questa raggiunge i 30°C (Allegare mappa temperature rilevate). – Il quadro è dotato di termostato per segnalazione di allarme che si richiede sia impostato per intervento a temperatura di 45°
04	Controllo delle apparecchiature: a) Controllo visivo e dimensionale b) Verifica dati di targa c) Verifica grado di protezione	a) Positivo b) Numeri di serie …… c) Installate all'interno del quadro, idonee all'uso
05	Ispezione finale: a) Controllo 'osservanza delle specifiche b) Controllo visivo e dimensionale c) Controllo costruzione a regola d'arte d) Controllo accessori e) Controllo targhettatura f) Controllo documentazione hardware	a) Positivo b) Positivo c) Positivo d) Positivo e) Positivo f) La documentazione presente ha recepito tutte le note di collaudo e sarà revisionata a seguito FAT
06	Verifica calibratura e taratura della strumentazione necessaria per effettuare le prove	Il costruttore HW/SW dichiara che tutta la strumentazione è regolarmente verificata come da procedura operativa del manuale di qualità aziendale XXXXXXX.

(continua)

Voce	Descrizione Prova	Risultato
07	Hardware System: a) Controllo circuito di terra b) Verifica alimentazioni, connessioni, tensioni ed assorbimenti c) Controllo connessioni sistemi periferici d) Controllo connessioni interfacce e) Prove sottosistemi f) Prove ingressi ed uscite digitali g) Prove ingressi ed uscite analogiche h) Prove interfacce bus di campo e canali di comunicazione	Hardware System: a) Positivo b) Positivo, assorbimento misurato su una linea campione 24V c.c.XX A, V c.a. 230 YY A c) Positivo, per i canali di comunicazione Ethernet d) Positivo, positivo le interfacce rispondono correttamente, incluso i convertitori di temperatura xxxxxxxx e) Positivo, provato 100% dei relé f) Positivo, provato 100% dei segnali g) Positivo, provato 100% dei segnali h) Non Applicabile
08	Test del software standard a) Verifica e annotazione del firmware incorporato (embedded software) b) Verifica ed annotazione del pacchetto di programmazione (utilità software) c) Verifica di compatibilità dei prodotti installati	a) CPU xxx Rel. 0 DI-AI yyy Rel. 0 DO-AO zzz Rel.0 b) Positivo in versione 00 c) Positiva, riferimento Allegato 1 al rapporto di certificazione XXXXX

(fine tabella)

F.5 Prove Funzionali per FAT

Voce	Descrizione Prova	Risultato
01	Prova di tutte le funzioni di sicurezza in accordo ai Requisiti di Sicurezza	…….
02	Selezione degli ingressi che attivano tutte le logiche funzionali specificate: Per esempio. prove funzionali secondo i diagrammi Causa-Effetto, inclusa la configurazione delle votazioni NooN	……..
03	Gestione degli errori dei segnali d'ingresso, es. ingresso fuori scala	Verificato generazione segnale di cattiva qualità (bad quality)
04	Simulazione di guasti a livello di sistema e di singolo modulo e relativo ritorno alle condizioni di normale funzionamento: a) guasti di ingresso di tipo "circuito aperto" o "corto circuito" b) guasti di uscita di tipo "circuito aperto" o "corto circuito" c) perdita di una scheda di ingresso d) perdita di una CPU e) perdita di entrambe le CPU f) perdita delle comunicazioni g) perdita di una scheda di uscita h) mancanza di alimentazione	Verifica a livello funzionalità intrinseche di prodotto (test da ripetersi al SAT). a) non applicabile b) positivo c) positivo d) positivo, entrambe le CPU commutano e) positivo, immediatamente le uscite vanno a 0 logico, contatti aperti. f) Positivo g) positivo, immediatamente le uscite vanno a 0 logico, contatti aperti: Se la scheda viene reinserita dopo circa 30 s le uscite sono riattivate. h) Positivo, per caduta alimentatore 230/24 "A", senza buco di alimentazione l'unità rimane alimentata da "B".
05	Tempo di risposta del sistema, inteso come tempo che intercorre dal cambiamento di stato dell'ingresso al cambiamento di stato dell'uscita relativa, inclusa la strumentazione di campo inclusa nello scopo di fornitura	Test da ripetersi al SAT. Dato dichiarato al FAT relativo al solo Risolutore Logico (Logic Solver) XX millisecondi.
06	Simulazione di una situazione di emergenza con contemporanea insorgenza di più allarmi, per esempio su almeno 25% dei segnali di ingresso	…….

Al termine delle prove verificare la completezza del fascicolo, riportare i numeri di serie degli elementi, apporre il sigillo di FAT sulle porte di programmazione del PES del SIS.

Inserire una copia della documentazione di FAT nel quadro provato, tale fascicolo dovrà essere sempre presente all'interno del quadro.

La documentazione delle FAT è parte del fascicolo di validazione del SIS di impianto.

F.6 Istruzioni dopo FAT

Le prove di messa in servizio (commissioning) potranno iniziare mentre le azioni correttive sono in atto, a seconda dei risultati delle prove di collaudo in fabbrica.

F.7 Conclusioni delle FAT

A conclusione delle FAT si può procedere all'installazione del sistema sull'impianto.

Data	Luogo	Costruttore	Contrattista	Cliente/Valutatore

F.8 SAT & SIT

Le SAT (prove di accettazione in sito) e le SIT (prove di integrazione sul sito) vengono condotte sull'impianto secondo la seguente tabella che riporta le attività e i controlli da svolgersi all'interno dell'esecuzione in opera incluso le fasi successive di esercizio.
La documentazione delle SAT e delle SIT è parte del fascicolo di validazione del SIS di impianto.

Elenco attività SAT e SIT				
Fase di realizzazione impianto		**Descrizione Prova**	**Apparecchiature da provare**	**Scopo**
COMPLETAMENTO MECCANICO	**COMPLETAMENTO DELLA COSTRUZIONE**	Ispezione visiva e verifiche dimensionali	– Strumenti e valvole; – Apparecchiature; – Elementi primari di portata.	Verificare eventuali rotture, danni o parti mancanti di strumentazione ed apparecchiature e segnalare eventuali non conformità con la specifica tecnica
		Prove funzionali e tarature	– Strumenti; – Termometri, termocoppie e termoresistenze; – Interruttori.	Verificare la funzionalità e la conformità con le specifiche
		Prove dei collegamenti elettrici	– Cavi interrati; – Cavi principali, secondari e di interconnessione; – Cavi riscaldati; – Rete di terra.	Verificare l'integrità e l'installazione
		Prove dei collegamenti di processo e di quelli per il tracciamento vapore	– Collegamento di processo; – Tracciamento con vapore.	Verificare l'installazione dei materiali e la tenuta
		Prove dei circuiti pneumatici	– Collegamenti pneumatici; – Rete di distribuzione aria strumenti.	Verificare l'installazione, l'impiego corretto dei materiali usati e la tenuta
		Ispezione dell'installazione	– Strumenti e valvole; – Apparecchiature Package, ecc.	Verificare che l'installazione sia completa, priva di danneggiamenti, ben protetta ed eseguita a regola d'arte
	PRECOMMISSIONING	Ispezioni, prove e tarature per il precommissioning	– Verifica strumenti tarati e non; – Verifica interruttori tarati e non; – CV, PCV e attuatori pneumatici; – Valvole di sicurezza; – Valvole motorizzate; – FE, FO,PI, TI; strumenti in linea; – Soffiatura rete aria strumenti; – Prima accensione e prova funzionale sistemi, apparecchi, e package; – Prova funzionale dei "loops" dei sistemi di controllo ed acquisizione; – Prova funzionale dei "loops" dei sistemi di sicurezza	Verificare che la strumentazione sia pronta per il commissioning Si suggerisce l'impiego dei moduli A, B, C, D allegati alla Norma CEI EN 62382
COMMISSIONING AVVIAMENTO		Prove funzionali delle sequenze e rapporto di avviamento	– Tutti i sistemi (prove funzionali); – Tutti i sistemi (rapporto di avviamento)	Dimostrare che tutti i sistemi e la strumentazione lavora in modo appropriato ed in accordo con la documentazione di progetto
IMPIANTO IN MARCIA		Prove prestazionali di impianto	– Tutti i sistemi	Registrazione delle prestazioni ed eventuali migliorie, affinamenti
IMPIANTO IN ESERCIZIO		Conduzione di impianto	– Manutenzione – Tuning – Modifiche – Decommissioning	Prove di intervento PES come da manuale sicurezza. Aggiornamento PES in funzione delle modifiche o della sostituzione di componenti dello stesso

Allegato G

Analisi quantitativa e qualitativa dei rischi

G.1 Premessa

L'analisi dei rischi può essere essenzialmente di due tipi:

- Analisi quantitativa
- Analisi qualitativa

G.2 Determinazione quantitativa

Relativamente alla determinazione quantitativa, occorre preliminarmente definire i livelli di sicurezza obiettivo per l'impianto oggetto di studio. Tali livelli pur facendo riferimento a matrici di rischio di tipo generale, normalmente utilizzate nell'analisi di rischio devono, in ogni caso, essere definiti per ogni progetto. Nella definizione dei criteri si definisce con quale frequenza si accettano rilasci di sostanze tossiche, e/o inquinanti, ferimento di operatori e/o soggetti esposti, danneggiamento di apparecchiature. La definizione dei livelli di sicurezza obiettivo è delicata e deve essere effettuata preliminarmente all'attività di analisi. L'impatto della definizione dei livelli obiettivo è sostanziale oltre che per gli aspetti inerenti l'HSE (Health Safety Environment) anche per l'aspetto economico del progetto.

Il primo passo da effettuare è la valutazione del rischio PRA (Preliminary Risk Assessment) che porta a classificare i rischi in tre livelli tipici che devono essere valutati con la metodologia ALARP (As Low As Reasonable Praticable), ovvero quantificare i possibili rischi e se questi non ricadono nella "area generalmente accettabile" (vedasi anche per maggiori dettagli l'Allegato A della CEI EN 61511-3).

A tal fine è necessario condurre una attenta analisi HAZOP (Hazard of Operation) per individuare in dettaglio le cause e gli effetti delle possibili anomalie allo scopo di ridurne l'incidenza sull'esercizio dell'impianto (vedasi anche per maggior dettagli l'Allegato C della CEI EN 61511-3).

L'HAZOP è una procedura formale, rigorosa, schematica e sistematica che viene utilizzata per analizzare la Sicurezza e l'Operabilità degli Impianti Chimici o assimilabili tali, dove vengano processati fluidi e/o solidi (sostanze chimiche, soluzioni acquose, vapore, ecc.).

Scopo dello studio HAZOP è quello di identificare le possibili deviazioni/scostamenti dal normale funzionamento operativo, che possano, causare danni e/o problemi di sicurezza a persone o cose o ostacolare l'operabilità dell'impianto, verificare l'adeguatezza e la rispondenza alla regola dell'arte applicabile e di proporre, ove necessario, alcuni interventi per aumentare la sicurezza e la conduzione dei sistemi.

Attraverso l'analisi dell'HAZOP è possibile identificare i possibili Eventi Principali (Top Events) e gli eventi incidentali connessi alle variazioni dei parametri di processo.

Eventi che possono comportare nel caso di mancato funzionamento delle protezioni scenari che comportano il rilascio di sostanze pericolose e sono quindi relativi ad esempio a:

- Sovrappressioni;
- Sovratemperature;
- Basse temperature (infragilimento).

Identificati gli Eventi Principali, si passa ad identificare la loro frequenza di accadimento. Tale attività può essere effettuata mediante l'applicazione della metodologia di analisi dell'Albero dei Guasti (Fault Tree Analysis).

Allo scopo di effettuare tale attività occorre preliminarmente raccogliere i dati di affidabilità per ogni elemento potenzialmente presente nel relativo albero di guasto, avendo cura di identificare accuratamente tutte le cause e le protezioni previste. In particolare, nell'effettuare l'analisi delle protezioni è opportuno verificarne l'indipendenza. Uno stesso evento incidentale può presentare diverse protezioni e, a tale scopo, al fine di ben definire il livello SIL richiesto, è fondamentale identificare ogni funzione di protezione presente, verificarne l'indipendenza o meno da altre funzioni allo scopo di effettuare una corretta valutazione di ogni singola funzione.

Quindi occorre definire la frequenza di accadimento di uno scenario incidentale mediante la Metodologia ad Albero degli Eventi.

Gli scenari incidentali derivanti da un evento iniziatore (sia esso dovuto a deviazione di processo oppure a perdita casuale di contenimento) sono individuati mediante la tecnica degli Alberi degli Eventi. Gli stessi Alberi degli Eventi consentono il calcolo della probabilità di accadimento di ogni singolo scenario e ne descrivono l'evoluzione considerando:

- la presenza di intercettazione;
- la presenza di un innesco immediato;
- la presenza di un innesco ritardato ed in questo ultimo caso si può avere:
  - esplosione della nube (UVCE),
  - esplosione della nube (UVCE),

La probabilità di esplosione della nube (UVCE), come noto sulla base della letteratura tecnica specialistica internazionale, dipende essenzialmente dalla geometria del luogo ove la nube si estende e dalla massa entro i limiti di esplosività; secondo quanto suggerito dall'ultimo Decreto Ministeriale in materia (DM 20/10/1998), si considera possibile la esplosione in ambiente parzialmente confinato, quale quello di impianto, quando la quantità di vapore entro i limiti di infiammabilità sia maggiore di 1,5 tonnellate.

Sulla base delle indicazioni disponibili in letteratura per quanto riguarda la probabilità di innesco immediato di rilasci di liquidi infiammabili si può fare riferimento a tabelle che in funzione del tipo di rilascio gassoso, o liquido e della portata di rilascio stabiliscano la probabilità di innesco immediato o ritardato.

In caso di mancato innesco immediato del fluido rilasciato, si potrà quindi formare una nube infiammabile che potrà dare luogo, se innescata, a esplosione (UVCE) o a combustione rapida (Flash Fire), in funzione della quantità di sostanza infiammabile e delle condizioni di confinamento presenti.

La probabilità di innesco ritardato e di sviluppo del fenomeno in uno degli scenari ipotizzabili (UVCE o Flash Fire), possono essere ricavate dalla letteratura: generalmente si arriva a definire una probabilità di Flash Fire o di formazione di una UVCE, in funzione della massa infiammabile attesa.

Valutazione delle Conseguenze

Lo stadio successivo è la definizione delle conseguenze di ogni scenario incidentale. Tale attività può essere effettuata mediante l'utilizzo di modelli di calcolo delle conseguenze che consentono una volta definita la sostanza soggetta a rilascio, le condizioni ambientali di riferimento, le condizioni di processo (temperatura e pressione) e le condizioni di rilascio di definire le conseguenze attese in termini di irraggiamento termico (da "pool fire" e/o "jet fire"), sovrapressioni, raggiungimento delle concentrazioni infiammabili (flash fire) e/o tossiche.

I valori di riferimento per la valutazione degli effetti sopra esposti sono riportati nella seguente Tabella G.1, congruentemente con quanto richiesto dalla normativa vigente in Italia (D.M.15/5/96 e D.M. 20/10/98).

Tabella G.1 – Soglie e livelli di danno a Persone e Strutture

Soglie di Danno a Persone e a Strutture		Livello di Danno				
		Elevata letalità	**Inizio letalità**	**Lesioni irreversibili**	**Lesioni reversibili**	**Danni alle Strutture Effetti Domino**
Scenario Incidentale	**Incendio** (radiazione termica stazionaria)	12,5 kW/m^2	7 kW/m^2	5 kW/m^2	3 kW/m^2	12,5 kW/m^2
	Flash-Fire(1) (radiazione termica istantanea)	LFL(2)	1/2 LFL	---	---	---
	UVCE(3) (sovra-pressione di picco)	0.3 bar (0.6 bar in spazi aperti)	0,14 bar	0,07 bar	0,03 bar	0,3 bar
	BLEVE(4) **Fireball** (radiazione termica variabile)	raggio sfera Fuoco (pool fire)	350 kJ/m^2	200 kJ/m^2	125 kJ/m^2	100 m da parco bombole; 600 m da stoccaggio in sfere; 800 m da stoccaggio in cilindri
	Rilascio Tossico	LC_{50} 30 min(5)	---	IDLH(6)	---	---

Flash-Fire = Incendio di vapori infiammabili;
LFL = Lower Flammable Limit (limite inferiore di infiammabilità);
UVCE = Unconfined Vapor Cloud Explosion (esplosione di vapori non confinata);
BLEVE = Boiling Liquid Expanding Vapour Explosion (esplosione di vapori sviluppati da gas liquefatto);
LC_{50} 30 min = Letal Concentration (concentrazione letale) per inalazione nel 50% dei soggetti esposti per 30 min. Il valore di LC_{50} utilizzato è quello relativo all'uomo per esposizione di 30 minuti.
IDLH = Immediately Dangerous for Life and Health - Limite di concentrazione di sostanza tossica a cui l'individuo sano, in seguito a 30 minuti di esposizione, non subisce danni irreversibili alla salute per inalazione.

In aggiunta ai valori di soglia sopra riportati, si può analizzare anche il raggiungimento del valore di irraggiamento di 37,5 kW/m^2, al quale si può assumere che si abbia probabilità di effetto domino pari al 100%.

I dati elaborati nell'effettuazione dell'analisi delle conseguenze sono i seguenti:

- condizioni di rilascio (pressione, temperatura);
- portata di efflusso;
- quantità totale rilasciata per la durata del rilascio;
- frequenze dei singoli scenari derivanti da albero degli eventi;
- massa entro i limiti di esplosibilità;
- diametro di pozza per i "pool fire";
- lunghezza di fiamma per i "jet fire;
- Distanze sottovento, agli effetti soglia sopra riportati, dal punto di rilascio, per:
  - flash fire;
  - pool fire;
  - jet fire;
  - UVCE;
  - dispersione tossica.

La definizione delle conseguenze consente di stabilire gli impatti sul personale esposto, sull'impianto, l'insorgere di eventuali ulteriori scenari (effetti domino) e può così consentire anche la definizione degli effetti ambientali attesi.

Allo scopo di rendere l'analisi più rapida si può effettuare per quanto riguarda la determinazione delle conseguenze una valutazione semiquantitativa, facendo riferimento a algoritmi speditivi (ad esempio API 581, Capitolo 7: Consequence Analysis) e/o a dati incidentali di riferimento se disponibili.

Sulla base dei livelli obiettivo definiti per il progetto, si verifica quindi che la probabilità di mancato intervento su domanda delle protezioni consenta di raggiungere gli obiettivi di accettabilità definiti, e si identifica la necessità di eventuali miglioramenti in caso contrario.

G.3 Determinazione Qualitativa

Le funzioni di protezione da analizzare possono essere identificate sulla base:

- delle matrici causa effetto;
- dei diagrammi di processo strumentati.

Ogni singola funzione di protezione, associata alla sicurezza, è analizzata separatamente utilizzando le seguenti informazioni:

- identificativo della logica e numero identificativo dell'anello ("loop") nel P&I;
- scopo della funzione di sicurezza;
- apparecchiatura protetta dalla funzione di sicurezza;
- numero di targa ("tag number"), tipo di targa, numero identificativo del P&I e servizio dell'elemento che compone il loop. Gli elementi del loop sono:
  - elementi sensori;
  - risolutore logico;
  - elementi finali.

Queste informazioni possono essere raccolte ad esempio in un foglio dati che può essere utilizzato per registrare l'analisi successiva, finalizzata a individuare:

- causa di malfunzionamento della logica di protezione;
- conseguenze del mancato funzionamento della logica o loop di protezione;
- fattori attribuiti;
- SIL richiesto;
- eventuali raccomandazioni.

Quando gli stessi elementi sensori attivano più di un elemento finale tutti gli elementi sono raccolti ed analizzati nello stesso foglio dati. L'analisi successive relative al fallimento del loop deve riguardare ogni singolo elemento ed il gruppo di analisi deve assegnare le conseguenze del malfunzionamento (mancato intervento) di ogni singolo elemento. L'assegnazione del SIL sarà poi effettuata sull'elemento più gravoso in termini di protezione individui esposti, ambiente o perdita economica.

G.4 Classificazione dei guasti

La metodologia di classificazione è divisa in due parti:

- classificazione dei guasti rilevati (interventi spuri);
- classificazione dei guasti non rilevati (guasti su richiesta d'intervento).

Nella fase di allocazione qualitativa del SIL, una volta valutata la frequenza della possibile necessità di intervento della funzione di protezione, si utilizzano i diagrammi di rischio per la valutazione delle conseguenze e del SIL associato. Qualora l'analisi di rischio del mancato intervento su domanda di una funzione di protezione non porti all'allocazione del SIL, la funzione può essere rimossa dal sistema di emergenza e trasferita al controllo di processo (BPCS).

Le conseguenze di un di un intervento spurio o di un guasto su richiesta d'intervento sono analizzati e registrate per ogni funzione. Nel caso in cui il mancato intervento su domanda comporti conseguenze diverse a seconda del tipo di guasto, si analizzano tutte le conseguenze e il SIL più conservativo sarà quello da utilizzare per la funzione di sicurezza.

In presenza di funzioni di sicurezza indipendenti in grado di intervenire in caso di mancato intervento su domanda della funzione di protezione elettrica / elettronica / elettronica programmabile (ad esempio, valvole di sicurezza: PSV), le conseguenze del guasto della funzione di protezione sono valutate trascurando la presenza di questa protezione aggiuntiva; il SIL risultante può essere ridotto di 1, per tenere conto del contributo di queste protezioni indipendenti.

G.5 Classificazione dei Guasti Spuri

Frequenza della Deviazione del Processo/Intervento del Sistema di Protezione

La gravità di una deviazione di processo può essere definita sulla base del tempo necessario per ripristinare completamente le condizioni produttive per la valutazione dei costi degli interventi guasti spuri, questi devono essere definiti considerando le conseguenze economiche a seguito delle interruzioni possibili ad esempio si potranno avere:

- deviazioni minori, tempo di interruzione inferiore alle *n* ore, se nell'impianto a seguito dell'intervento spurio della protezione non si hanno conseguenze economiche significative entro tali n ore considerate;
- deviazioni moderate, tempo di interruzione oltre le n ore ed x giorni, la definizione del numero dei giorni dipende strettamente dalla tipologia di processo, da quali ulteriori fermate di impianto comporta e dal costo economico in termini di mancato guadagno dell'impianto;
- deviazioni maggiori, tempo di interruzione tra i x ed y giorni, la definizione del numero dei giorni dipende strettamente dalla tipologia di processo, da quali ulteriori fermate di impianto comporta e dal costo economico in termini di mancato guadagno dell'impianto, dagli impatti che la fermata dell'impianto può comportare anche in termini ambientali e di extra costi accessori eventuali.

G.6 Classificazione dei Guasti su Domanda

Frequenza della Domanda/Intervento del Sistema di Protezione

Diverse possono essere le ragioni di intervento del sistema di protezione, includendo le deviazioni di processo e gli errori degli operatori. La frequenza della domanda influirà sulla classificazione del SIL del sistema di protezione; a parità di conseguenze, un sistema che si prevede attivato frequentemente avrà maggiori richieste di sicurezza rispetto ad uno che si prevede essere attivato solo una volta.

Sono solitamente considerati 3 livelli di domanda di intervento della protezione, con altrettanti valori numerici (rispettivamente W1, W2, W3), come segue:

- Probabilità Remota (very slight probability) (W1): minore di una volta ogni 10 anni;
- Probabilità Occasionale (slight probability) (W2): una volta ogni 1-10 anni;
- Molto Probabile (relatively high probability) (W3): più di una volta all'anno.

La scelta del fattore di frequenza deve essere fatto sulla base della documentazione di processo disponibile (PRA e HAZOP) e/o sulla base dell'esperienza della squadra di valutazione della sicurezza funzionale.

Il valore W2 è normalmente utilizzato per i guasti tipici del sistema di protezione (trasmettitore, logica ed elemento finale).

Qualora la dinamica delle conseguenze dopo il guasto del sistema di protezione consenta l'intervento dell'operatore sulla base di allarmi ed indicazioni, può essere utilizzata la frequenza W1.

La scelta di W1 deve essere comunque giustificata e registrata.

La classificazione dei SIL deve essere effettuata in relazione a queste tre conseguenze:

- sui danni al personale : vedasi Figura G.1
- sui danni ambientali : vedasi Figura G.2
- sui danni economici : vedasi Figura G.3

Senza alcun carattere di esaustività si riportano nel prosieguo alcuni spunti di riflessione sull'esame delle situazioni concomitanti ad anomalie di processo, una volta identificate le conseguenze del mancato intervento su domanda della protezione, che influenzano la sicurezza del personale, la difesa dell'ambiente e la salvaguardia economica degli impianti (per ulteriori approfondimenti in merito vedasi anche l'Allegato D della CEI EN 61511-3).

Figura G.1 – Classificazione del SIL per i danni al Personale

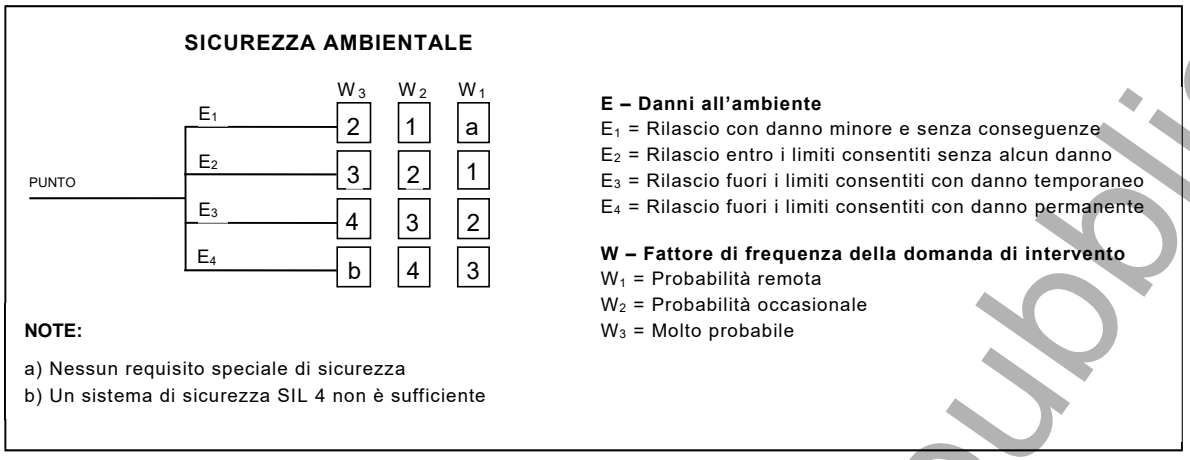


Figura G.2 – Classificazione del SIL per i danni Ambientali

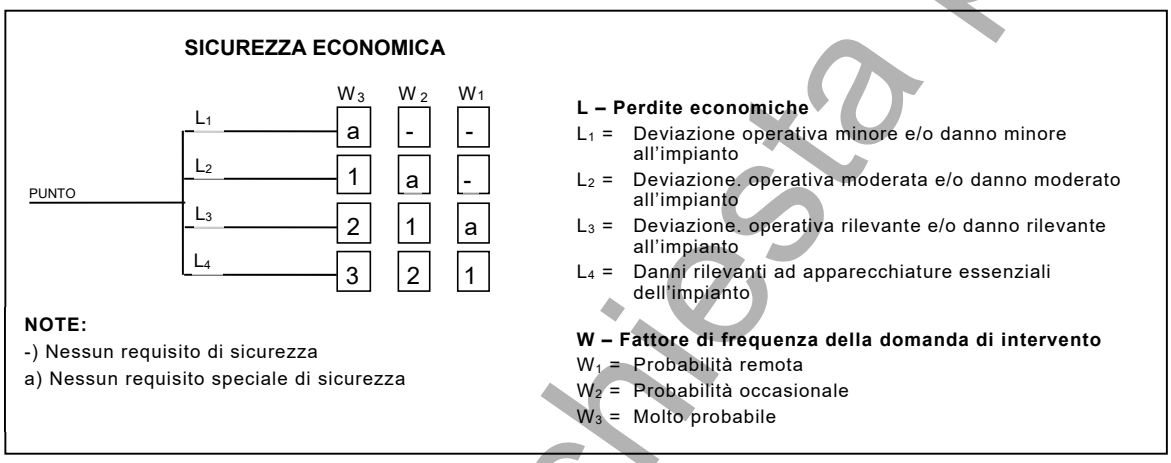


Figura G.3 – Classificazione del SIL per i danni Economici

G.7 Sicurezza del personale

Per la valutazione dei rischi per il personale presente sull'impianto si usa la matrice di Figura G.1, che prende in esame i seguenti fattori:

Conseguenze:

- C1 – ferite lievi;
- C2 – ferite gravi a più persone/morte di una persona;
- C3 – morte di diverse persone;
- C4 – morte di molte persone.

Frequenza di Esposizione:

- F1 – da rara a frequente (ad esempio, l'area non è normalmente presidiata dal personale continuamente);
- F2 – da frequente a permanente (ad esempio, l'area è presidiata o il guasto su domanda può avvenire durante avviamenti locali).

Possibilità di sottrarsi al rischio:

- P1 – possibile in determinate condizioni (ad esempio, possibilità di vie di fuga nel rispetto della dinamica dell'evento);
- P2 – quasi impossibile.

Pertanto seguendo il diagramma di rischio di Figura G.1 attraverso i fattori predetti C, F e P è possibile pervenire alla classificazione SIL per la frequenza prevista W.

G.8 Danni all'ambiente

Per la valutazione dei rischi possibili all'ambiente si usa la matrice di Figura G.2, che considera i danni temporanei/permanenti all'ambiente in termini di rilascio di sostanze:

- Gassose : rilascio di gas e vapori tossici e/o infiammabili, aerosol, fuliggini, ecc
- Liquide : inquinanti o meno la falda freatica, fiumi, mare, ecc.
- Solide : ricaduta sostanze solide/frammenti per esplosione, incendio, ecc.

e considerando questi quattro livelli di danno:

- E1 – rilascio con danno minore senza alcuna conseguenza;
- E2 – rilascio entro i limiti consentiti senza danni all'ambiente;
- E3 – rilascio fuori dei limiti consentiti con danno temporaneo;
- E4 – rilascio fuori dei limiti consentiti con danno permanente.

Esempi di casi classificati in accordo alle classi sopra riportate sono i seguenti:

- Rilascio con danno minore senza alcuna conseguenza (E1):
  - Fuga moderata di gas da una flangia/valvola;
  - Perdita moderata di tenuta su liquido.
- Rilascio entro i limiti consentiti senza danni all'ambiente (E2):
  - Nube di vapore odorante;
  - Perdita da una guarnizione di liquido.
- Rilascio fuori i limiti consentiti con danni temporanei all'ambiente (E3):
  - Nube di aerosol che provoca danni temporanei alla flora e alla fauna;
  - Scarico di liquido pericoloso sul suolo senza danni alla falda freatica.
- Rilascio fuori i limiti consentiti con danni permanenti all'ambiente (E4):
  - Nube di vapori che provoca danni duraturi alla flora e alla fauna;
  - Scarico di liquido inquinante in fiumi e mari.

Pertanto, anche in questo secondo caso, seguendo il diagramma di rischio di Figura G.2 attraverso il livello attribuito al fattor predetto E è possibile pervenire alla classificazione SIL per la frequenza prevista W.

G.9 Perdita economica

Per la valutazione delle perdite economiche si usa la matrice di Figura G.3, che considera le perdite dovute essenzialmente ai seguenti fattori:

- mancate produzioni;
- danneggiamenti alle apparecchiature,

e considerando questi quattro livelli di danno:

- L1 - deviazione operativa minore e/o danni minori all'apparecchiatura;
- L2 - deviazione operativa moderata e/o danni moderati all'apparecchiatura;
- L3 - deviazione operativa rilevante e/o danni rilevanti all'apparecchiatura;
- L4 - danni rilevanti ad apparecchiature essenziali.

Esempi di casi classificati in accordo alle classi sopra riportate possono essere i seguenti:

- Deviazione operativa minore e/o danni minori all'apparecchiatura (L1):
  - Prodotto fuori specifica;
  - Cavitazione di pompe o basso livello di aspirazione;
  - Danni minori ad apparecchiature essenziali e/o moderati ad apparecchiature non essenziali con possibilità di continuare ad operare l'impianto;
- Deviazione operativa moderata e/o danni moderati all'apparecchiatura (L2):
  - Deviazione in un sistema di servizio con effetti sulle altre unità;
  - Liquidi in linee gas;
  - Rilascio medio o grande di quantitativi di prodotti di valore;
  - Alta pressione con relativo danno meccanico e perdita di prodotto (ad es.: tenute, guarnizioni);
  - Cavitazione di pompe ad alta velocità o multistadio;
- Deviazione operativa rilevante e/o danni rilevanti all'apparecchiatura (L3):
  - Rilascio immediato ad alta energia come ad esempio il passaggio istantaneo di vapore da alta a bassa pressione;
  - Fuoriuscita di fluido di processo;
  - Solidificazione di prodotto in tubazioni non riscaldate con conseguenti pesanti azioni correttive di manutenzione;
  - Riparazioni non costose di apparecchiature essenziali prive di apparecchiatura di scorta;
  - Riparazioni costose di apparecchiature essenziali con apparecchiatura di scorta o di apparecchiature non-essenziali.
- Danni rilevanti ad apparecchiature essenziali (L4):
  - casi come L2 o L3, ma con stima di danni economici superiori (oltre i milioni di Euro) ad es.: alto livello nel separatore di aspirazione di un compressore, basso livello in aspirazione ad una pompa multistadio, eccesso di velocità di una pompa, protezione di un forno o una caldaia;
  - danni provocati da una deviazione di processo con conseguente danno meccanico irreparabile di contenimento di prodotto (runaway, reazioni incontrollate, altissima temperatura o pressione).

Pertanto, anche in questo terzo e ultimo caso, seguendo il diagramma di rischio di Figura G.3 attraverso il livello attribuito al fattore predetto L è possibile pervenire alla classificazione SIL per la frequenza prevista W.

Si fa notare che nel diagramma di rischio di Figura G.3 non compare nè il SIL 4 nè la nota di insufficienza applicativa dello stesso SIL 4, in quanto i danni verso la perdita economica sono generalmente di più modesta entità rispetto quelli potenziali verso il personale e l'ambiente, che talvolta possono essere di natura fatale e/o catastrofica.

Allegato H

Calcolo analitico della probabilità di guasto su domanda (PFD)

H.1 Premessa

Questo Allegato fornisce una possibile tecnica per calcolare il PFD_{avg} per un SIS e si basa sulle seguenti considerazioni:

a) fornisce delle equazioni semplificate per valutare l'integrità del SIS[1)];

b) assume che i ratei di guasto degli elementi siano costanti per l'intero ciclo di vita;

c) assume lo stesso rateo di guasto per elementi uguali ridondati;

d) il rateo di guasto del sensore include ogni elemento dal modulo di ingresso dello strumento al modulo di ingresso dell'unità logica;

e) il rateo di guasto della logica include il modulo di ingresso, la logica, il modulo in uscita le sorgenti di potenza ed è normalmente fornito dal costruttore;

f) il rateo di guasto dell'elemento finale include ogni elemento dal modulo d'uscita della logica fino all'elemento finale stesso;

g) l'intervallo di prova o test (TI) molto più corto del tempo medio di guasto (MTTF);

h) la prova e riparazione degli elementi del sistema si ipotizza perfetta;

i) gli elementi finali (valvole) sono selezionati in modo tale che in caso di guasto secondo la specifica applicazione sia in modo sicuro;

j) i guasti di fornitura di energia sono ipotizzati essere in stato de-energizzato;

k) infine si ipotizza che nel caso di detenzione di un guasto pericoloso, il SIS gestisce il processo in modo sicuro o il personale d'impianto è in grado di prendere le opportune azioni correttive per assicurare un processo sicuro.

Le equazioni utilizzate nel seguente Allegato sono basate sulla CEI EN 61508-6 ed utilizzano gli stessi parametri e simbolismi, ovvero quelli riportati nella seguente Tabella H.1, che per comodità di riscontro alfabetico ed acronimo è presentata inalterata in inglese (ovvero Tabella B.1 della CEI EN 61508-6).

H.2 Procedura di calcolo

La valutazione di un Sistema Strumentato di Sicurezza (SIS) o di una sua porzione, comporta la stima di tutte le singole Probabilità di Guasto su Richiesta d'intervento (PFD) dei suoi componenti costitutivi, ovvero (Figura H.1):

a) Sensore;

b) Risolutore logico;

c) Elemento finale.

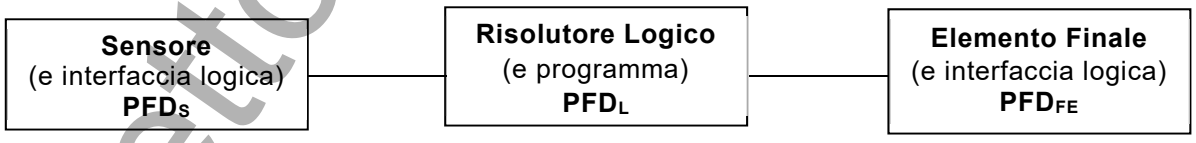


Figura H.1 – Schema a blocchi di un Sistema Strumentato di Sicurezza (SIS)

Per cui la PFD del sistema sarà la somma delle singole PFD dei sottosistemi, ovvero:

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$

1) I ratei di guasto riportati nelle formule per architetture ridondate sono per un singolo canale o elemento (cioè per trasmettitori 2oo3, il rateo di guasto utilizzato è per un singolo trasmettitore e non moltiplicato 3 volte).

Table B.1 – Terms and their ranges used in this annex
(applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3)

Abbre-viation	Term (units)	Parameter ranges in Tables B.2 to B.5 and B.10 to B.13
T_1	Proof test interval (hour)	One month (730 h)[1] Three months (2 190 h)[1] Six months (4 380 h) One year (8 760 h) Two years (17 520 h)[2] Ten years (87 600 h)[2]
MTTR	Mean time to restoration (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT.
MRT	Mean repair time (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)	0 % 60 % 90 % 99 %
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	2 % 10 % 20 %
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	1 % 5 % 10 %
λ_{DU}	Dangerous Undetected failure rate (per hour) of a channel in a subsystem	$0{,}05 \times 10^{-6}$ $0{,}25 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ $2{,}5 \times 10^{-6}$ 5×10^{-6} 25×10^{-6}
PFD_G	Average probability of failure on demand for the group of voted channels (If the sensor, logic or final element subsystem comprises of only one voted group, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively)	
PFD_S	Average probability of failure on demand for the sensor subsystem	
PFD_L	Average probability of failure on demand for the logic subsystem	

Tabella H.1 – Acronimi, termini e campi dei parametri caratterizzanti le PFD dei SIS (Tabella B.1 della CEI EN 61508-6)

In questa primaria valutazione si devono fare i seguenti passi:

- identificazione dell'evento pericoloso al quale il SIS fornisce un livello di protezione e dei componenti specifici della SIF che realizzano la protezione;
- identificazione del SIL per ogni SIF richiesta dall'evento pericoloso;
- lista degli elementi che possono avere un impatto per ogni SIF, tipicamente sarà la lista dei sensori e degli elementi finali identificati nell'analisi dei passi precedenti;
- e quindi attraverso l'architettura del SIS, si calcolerà il $PFD_{avg.}$ per ogni SIF combinando i contributi dei singoli componenti (sensori, risolutore logico, elementi finali) che possono avere un impatto sull'integrità della SIF.

Deve essere inoltre verificato che la PFD_{avg} soddisfi i requisiti Safety Requirements Specifications (SRS) di ogni SIF.

Se necessario deve essere modificato il SIS in termini di:

- ridondanza dell'architettura HW;
- intervallo di prova o di test TI,

e ripetere il calcolo fino a soddisfare i requisiti del SIL richiesto per la SIF specificata.

H.3 Calcolo della Probabilità di Guasto su Domanda del sistema PFD_{SYS}

La PFD_{SYS} si determina calcolando la PFD di tutti i componenti del Sistema Strumentato di Sicurezza SIS che garantisce la protezione rispetto ad un evento a rischio di processo, e combinando poi le singole PFD per ottenere la Probabilità di Guasto su Domanda dell'intero sistema PFD_{SYS}, attraverso la predetta formula (vedasi anche Figura H.1):

$$\mathbf{PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}}$$

dove: PFD_S è la PFD_{avg} del sensore (di misura)

PFD_L è la PFD_{avg} del risolutore logico

PFD_{FE} è la PFD_{avg} dell'elemento finale

mentre PFD_{avg} è la PFD media del relativo sottosistema del sistema SIS esaminato.

H.4 Equazioni di calcolo delle singole PFD per le principali architetture

Le principali architetture previste per realizzare il Livello di Integrità di Sicurezza SIL del SIS richiesto sono essenzialmente le seguenti:

- 1oo1 : ovvero singola senza alcuna ridondanza
- 1oo2 : ovvero a ridondanza OR
- 2oo2 : ovvero a ridondanza AND
- 1oo2D : ovvero a ridondanza OR, con reciproca diagnostica
- 2oo3 : ovvero a ridondanza maggioritaria

per le quali si riportano nel prosieguo le equazioni di calcolo delle singole PFD dei sottosistemi componenti il sistema SIS, in riferimento ai parametri riportati in Tabella H.1 (per maggiori dettagli in merito vedasi l'Allegato B della CEI EN 61508-6).

Per una pratica determinazione tabellare delle singole PFD, vedasi invece il successivo Allegato I (tratto dalla predetta CEI EN 61508-6).

Architettura 1oo1

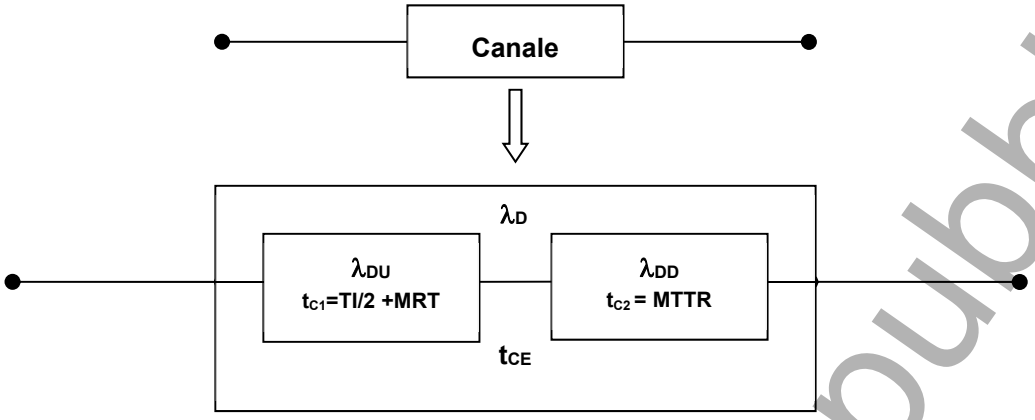


Figura H.2 – Architettura 1oo1 e relativo schema di affidabilità

Dalla Figura H.2, il tasso dei guasti pericolosi λ_D è fornito dalla relazione seguente:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

dove:

λ_{DU} = tasso dei guasti dannosi non rilevati

λ_{DD} = tasso dei guasti dannosi rilevati

λ = tasso dei guasti totali

Per cui è possibile calcolare il tempo di guasto equivalente del canale t_{CE} tramite la relazione seguente:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{TI}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

in cui:

TI = intervallo di tempo delle prove periodiche

MTTR = tempo medio di ristabilimento

Ricordando che per ogni architettura il tasso dei guasti pericolosi rilevati λ_{DD} e non rilevati λ_{DU} sono derivati dalle seguenti relazioni:

$$\lambda_{DD} = \frac{\lambda}{2} \cdot DC$$

$$\lambda_{DU} = \frac{\lambda}{2} \cdot (1 - DC)$$

dove DC è la Copertura Diagnostica del canale in esame.

Pertanto la PFD dell'architettura 1oo1 si può cosi formulare:

$$PFD_{1oo1} = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE}$$

Architettura 1oo2

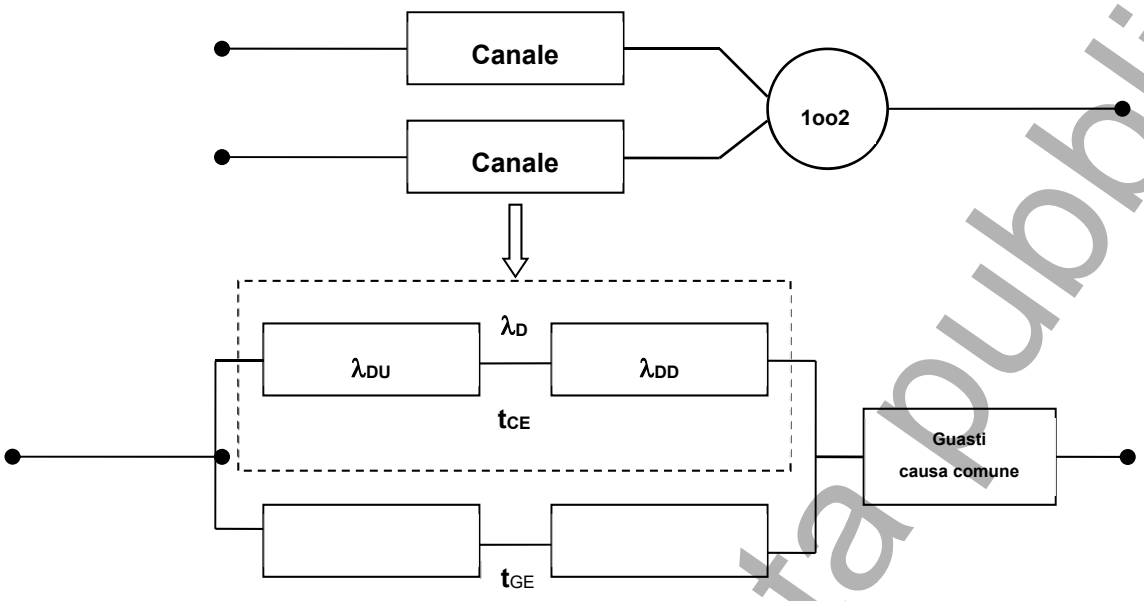


Figura H.3 – Architettura 1oo2 e relativo schema di affidabilità

Dalla Figura H.3, il tempo di guasto equivalente del canale t_{CE} è equivalente a quello calcolato in precedenza per l'architettura 1oo1, mentre il tempo di guasto equivalente del sistema è calcolabile tramite la relazione seguente:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{TI}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Per cui la PFD dell'architettura 1oo2 si può così formulare:

$$PFD_{1oo2} = 2 \cdot ((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MRT\right)$$

dove:

β = tasso dei guasti di modo e di causa comune non rilevati dalla diagnostica: dipende dalle caratteristiche di progettazione dei sottosistemi;

β_D = tasso dei guasti di modo e di causa comune rilevati dalla diagnostica: dipende dalle caratteristiche di auto diagnostica dei sottosistemi.

Per valori tipici di β e β_D vedasi Tabella H.1 (ovvero Tabella B.1 della CEI EN 61508-6).

Per ulteriori approfondimenti in merito vedasi gli Allegati B, C, D della CEI EN 61508-6.

NOTA Tale architettura 1oo2 è comunemente denominata anche a ridondanza OR.

Architettura 2oo2

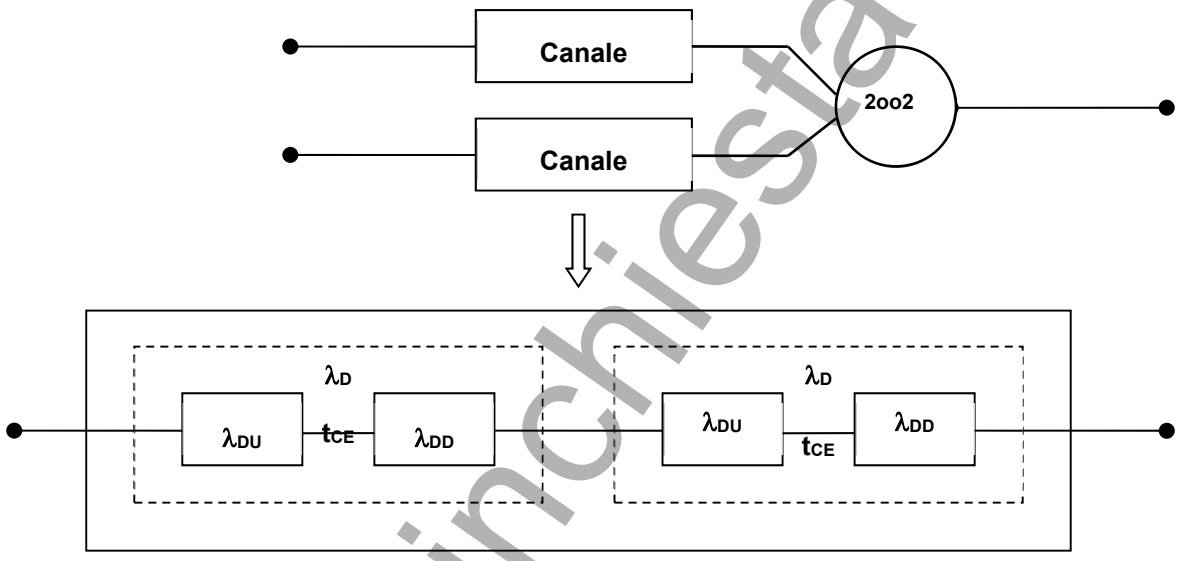


Figura H.4 – Architettura 2oo2 e relativo schema di affidabilità

Dalla Figura H.4, considerando i due canali in serie, si ha l'attivazione del sottosistema solo quando entrambi i canali si attivano.

Pertanto considerando il tasso dei guasti pericolosi λ_D ed il tempo di guasto equivalente del singolo canale t_{CE} equivalente a quello calcolato i precedenza per l'architettura 1oo1, in questo caso la PFD dell'architettura 2oo2 si può così semplicemente formulare:

$$\mathrm{PFD}_{2oo2} = 2 \cdot \lambda_D \cdot t_{CE}$$

NOTA Tale architettura 2oo2 è comunemente denominata anche a ridondanza AND.

Architettura 1oo2D

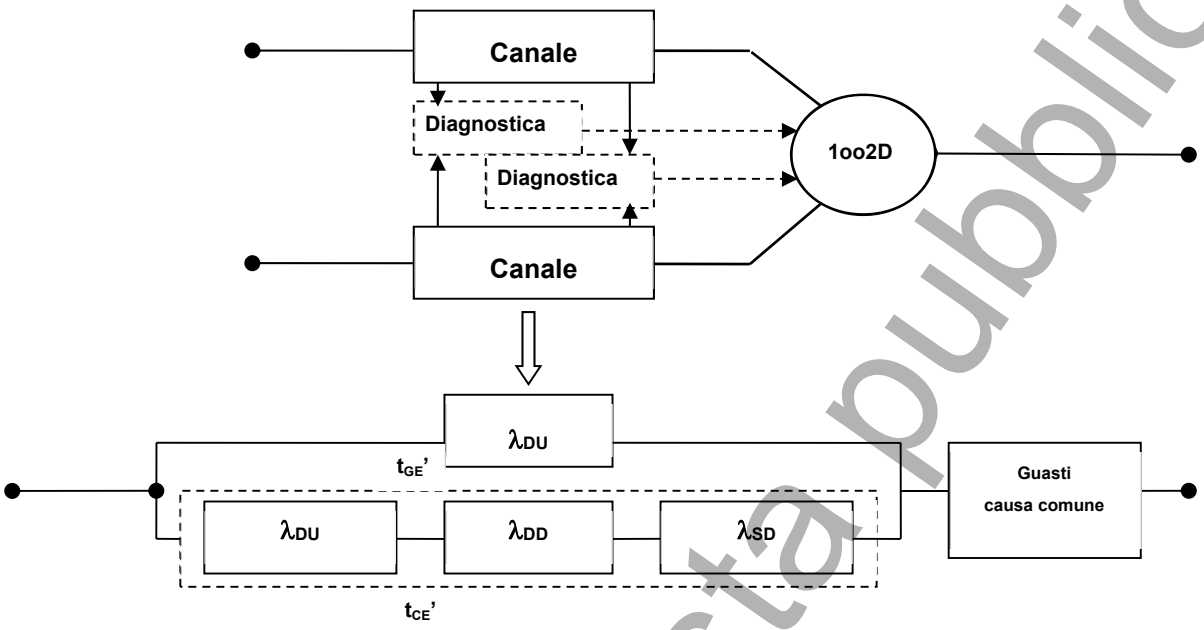


Figura H.5 – Architettura 1oo2D e relativo schema di affidabilità

In questa speciale architettura 1oo2D la diagnostica presente non è solo attiva come nelle altre architetture sul componente da diagnosticare, ma anche sull'altro e pertanto attraverso due diagnostiche indipendenti si possono rilevare su ogni canale sia stati di congruenza che stati di discrepanza, che portano il sottosistema in uno stato sicuro, migliorandone nel complesso l'affidabilità.

Dalla Figura H.5, ponendo il tasso dei guasti sicuri rilevati λ_{SD} pari a:

$$\lambda_{SD} = \frac{\lambda}{2} \cdot DC$$

si hanno due diversi tempi di guasto equivalente dei due comportamenti affidabilistico:

$$t_{CE'} = \frac{\lambda_{DU} \cdot \left(\frac{TI}{2} + MRT \right) + (\lambda_{DD} + \lambda_{SD}) \cdot MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$t_{GE'} = \frac{TI}{3} + MRT$$

Per cui la PFD dell'architettura 1oo2D si può così formulare:

$$PFD_{1oo2D} = 2 \cdot ((1-\beta) \cdot \lambda_{DU} \cdot ((1-\beta) \cdot \lambda_{DU}) + (1-\beta_D) \cdot \lambda_{DD} + \lambda_{SD}) \cdot t_{CE'} \cdot t_{GE'} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MRT \right)$$

NOTA Tale architettura 1oo2D, è analoga alla 1oo2, però essendo mutualmente diagnosticata evita i principali guasti spuri.

Architettura 2oo3

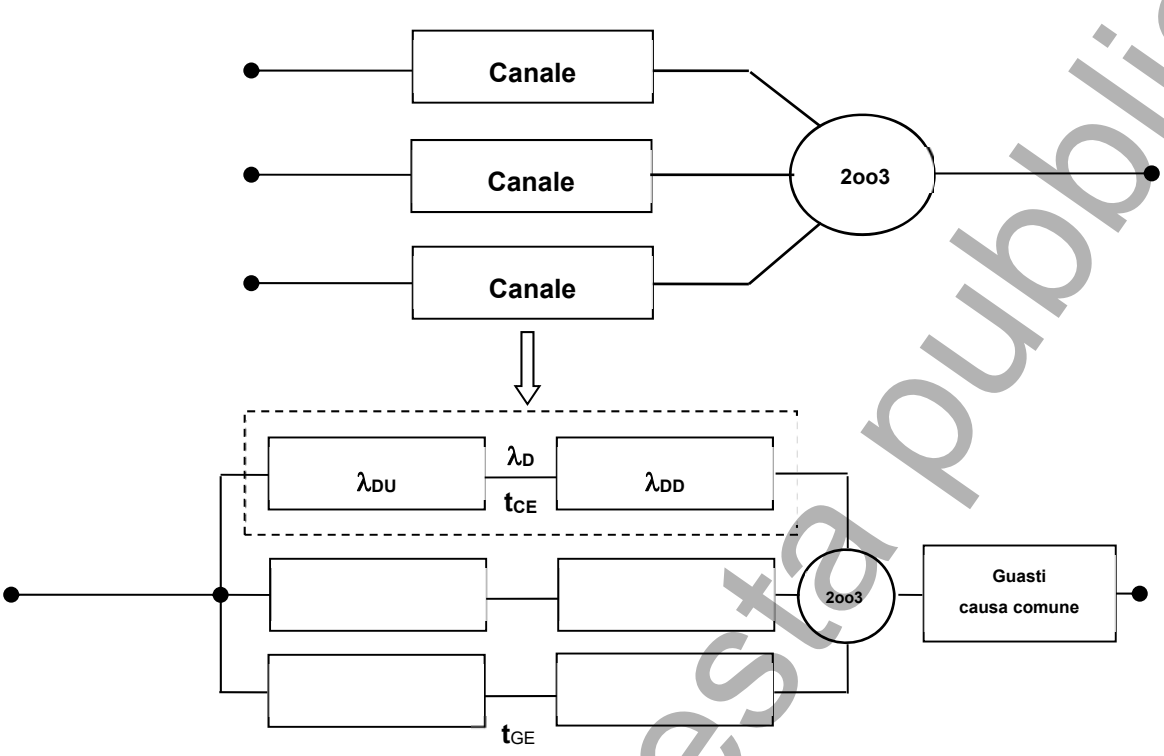


Figura H.6 – Architettura 2oo3 e relativo schema di affidabilità

In questa ultima architettura 2oo3, il sottosistema si attiva quando almeno due canali sono attivati e pertanto è meno sensibile ai gusti spuri del singolo canale.

Dalla Figura H.6, tenendo in considerazione i fattori t_{CE} e t_{GE} precedentemente calcolati per l'architettura 1oo2, la PFD della presente architettura 2oo3 si può così formulare:

$$PFD_{2oo3} = 6 \cdot ((1-\beta_D)\cdot\lambda_{DD} + (1-\beta)\cdot\lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MRT\right)$$

NOTA Tale architettura 2oo3, è comunemente denominata anche a ridondanza maggioritaria, ovvero a ridondanza MooN (dove M < N).

Equazioni Tabulate

I risultati delle equazioni canoniche viste in precedenza per le varie architetture esaminate:

1oo1
1oo2
2oo2
1oo2D
2oo3

sono tabulate per i diversi fattori caratteristici e funzionali nel prossimo Allegato I, derivata dalla CEI EN 61508-6.

Equazioni Semplificate

Equazioni semplificate, prive del termine dei guasti multipli durante le riparazioni, cause comuni di guasto ed errori sistematici, per parte delle architetture esaminate e per altre ulteriori architetture, sono invece riportate nel prosieguo:

1oo1 $$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2}$$

1oo2 $$PFD_{avg} = \frac{\left[(\lambda_{DU})^2 \times TI^2\right]}{3}$$

1oo3 $$PFD_{avg} = \frac{\left[(\lambda_{DU})^3 \times TI^3\right]}{4}$$

2oo2 $$PFD_{avg} = \lambda_{DU} \times TI$$

2oo3 $$PFD_{avg} = (\lambda_{DU})^2 \times TI^2$$

2oo4 $$PFD_{avg} = (\lambda_{DU})^3 \times TI^3$$

H.5 Considerazioni finali sull'affidabilità delle varie architetture presentate

Considerando le principali architetture ridondanti esaminate e più applicate, si può evidenziare, rispetto l'architettura base non ridondata 1oo1 (vedasi Tabella H.2, con MRT = MTTR), che:

- la 1oo2 è più affidabile, però nel contempo è più sensibile ai guasti spuri;
- la 2oo2 è meno affidabile, sebbene sia maggiormente insensibile ai guasti spuri;
- la 2oo3 è più affidabile, sebbene meno della 1oo2, ma meno sensibile ai guasti spuri.

Tabella H.2 – Confronto tra Probabilità di Guasto su Domanda PFD fra varie Architetture

Tasso guasto λ	Cop. Dia. DC	Guasti peric. λ_D	Guasti per.ril. λ_{DD}	Guasti non ril. λ_{DU}	Fatt. β	Fatt. β_D	Tempo MTTR (h)	Tempo TI (y)	PFD 1oo1	PFD 1oo2	PFD 2oo2	PFD 2oo3
1,00E-04	0,6	5,0E-05	3,0E-05	2,0E-05	10%	5%	8	1	8,8E-02	1,8E-02	1,8E-01	3,6E-02
5,00E-05	0,6	2,5E-05	1,5E-05	1,0E-05	10%	5%	8	1	4,4E-02	6,6E-03	8,8E-02	1,1E-02
1,00E-05	0,6	5,0E-06	3,0E-06	2,0E-06	10%	5%	8	1	8,8E-03	9,7E-04	1,8E-02	1,1E-03
5,00E-06	0,6	2,5E-06	1,5E-06	1,0E-06	10%	5%	8	1	4,4E-03	4,6E-04	8,8E-03	5,1E-04
1,00E-06	0,6	5,0E-07	3,0E-07	2,0E-07	10%	5%	8	1	8,8E-04	8,9E-05	1,8E-03	9,1E-05
5,00E-07	0,6	2,5E-07	1,5E-07	1,0E-07	10%	5%	8	1	4,4E-04	4,4E-05	8,8E-04	4,5E-05
1,00E-07	0,6	5,0E-08	3,0E-08	2,0E-08	10%	5%	8	1	8,8E-05	8,8E-06	1,8E-04	8,8E-06

Allegato I

Determinazione della probabilità di guasto su domanda (PFD) secondo le tabelle della CEI EN 61508-6

I.1 Premessa

Come precedentemente riportato in Figura A.11 in Allegato A e qualora non si proceda al calcolo analitico della Probabilità di Guasto su Domanda (PFD) come riportato precedentemente nell'Allegato H, la PFD dei vari sottosistemi componenti il Sistema Strumentato di Sicurezza (SIS) può essere determinata mediante le seguenti Tabelle (elencate da B.2 a B.13) tratte dalla CEI EN 61508-6, tramite i parametri caratteristici dei sottosistemi i cui simboli e definizioni sono riportati al termine dell'Allegato A e all'inizio dell'Allegato H nella Tabella H.1:

- B.2 per la determinazione della PFD in modo su domanda con intervallo di prova di 0,5 anni
- B.3 per la determinazione della PFD in modo su domanda con intervallo di prova di 1 anno
- B.4 per la determinazione della PFD in modo su domanda con intervallo di prova di 2 anni
- B.5 per la determinazione della PFD in modo su domanda con intervallo di prova di 10 anni
- B.10 per la determinazione della PFD in modo continuo con intervallo di prova di 1 mese
- B.11 per la determinazione della PFD in modo continuo con intervallo di prova di 3 mesi
- B.12 per la determinazione della PFD in modo continuo con intervallo di prova di 6 mesi
- B.13 per la determinazione della PFD in modo continuo con intervallo di prova di 12 mesi

e forniscono la PFD per un tempo medio di riparazione del sottosistema di 8 ore:

Le successive Tabelle forniscono invece criteri di valutazione dei parametri DC, β, β_D (che devono essere utilizzati per la determinazione della PFD nelle precedenti Tabelle):

- C2 per la determinazione del parametro DC
- D4 per la determinazione dei parametri β e β_D

I.2 Tabelle

Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see Note 2)	0 %	1,1E-04			5,5E-04			1,1E-03		
	60 %	4,4E-05			2,2E-04			4,4E-04		
	90 %	1,1E-05			5,7E-05			1,1E-04		
	99 %	1,5E-06			7,5E-06			1,5E-05		
1oo2	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (see Note 2)	0 %	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,3E-05			1,1E-04			2,3E-04		
	99 %	3,0E-06			1,5E-05			3,0E-05		
1oo2D (see Note 3)	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90 %	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99 %	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see Note 2)	0 %	5,5E-03			1,1E-02			5,5E-02		
	60 %	2,2E-03			4,4E-03			2,2E-02		
	90 %	5,7E-04			1,1E-03			5,7E-03		
	99 %	7,5E-05			1,5E-04			7,5E-04		
1oo2	0 %	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (see Note 2)	0 %	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,3E-03			1,1E-02		
	99 %	1,5E-04			3,0E-04			1,5E-03		
1oo2D (see Note 3)	0 %	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60 %	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90 %	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99 %	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04
2oo3	0 %	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	0 %	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	0 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (see Note 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (see Note 3)	0 %	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90 %	8,5E-07	2,6E-06	4,8E-06	4,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99 %	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,0E-06	2,8E-06	5,0E-06
2oo3	0 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	0 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	0 %	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (see Note 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (see Note 3)	0 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60 %	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90 %	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99 %	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	0 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (see Note 2)	0 %	8,8E-04			4,4E-03			8,8E-03		
	60 %	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D (see Note 3)	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
	60 %	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90 %	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99 %	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	0 %	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	0 %	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	0 %	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (see Note 2)	0 %	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (see Note 3)	0 %	1,1E-03	2,7E-03	4,8E-03	3,4E-03	6,6E-03	1,1E-02	6,7E-02	7,7E-02	9,0E-02
	60 %	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90 %	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99 %	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	0 %	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	0 %	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-03			1,1E-02			2,2E-02		
	60 %	8,8E-04			4,4E-03			8,8E-03		
	90 %	2,2E-04			1,1E-03			2,2E-03		
	99 %	2,2E-05			1,1E-04			2,2E-04		
1oo2	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (see Note 2)	0 %	4,4E-03			2,2E-02			4,4E-02		
	60 %	1,8E-03			8,8E-03			1,8E-02		
	90 %	4,4E-04			2,2E-03			4,4E-03		
	99 %	4,5E-05			2,2E-04			4,5E-04		
1oo2D (see Note 3)	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90 %	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99 %	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	0 %	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60 %	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	0 %	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60 %	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	4,4E-02			8,8E-02			>1E-01		
	90 %	1,1E-02			2,2E-02			>1E-01		
	99 %	1,1E-03			2,2E-03			1,1E-02		
1oo2	0 %	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60 %	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
2oo2 (see Note 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	8,8E-02			>1E-01			>1E-01		
	90 %	2,2E-02			4,4E-02			>1E-01		
	99 %	2,2E-03			4,5E-03			2,2E-02		
1oo2D (see Note 3)	0 %	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60 %	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90 %	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99 %	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	0 %	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60 %	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90 %	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
1oo3	0 %	4,7E-03	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60 %	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.10 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	2.1E-08	1.0E-07	2.0E-07	4.3E-08	2.0E-07	4.0E-07	2.7E-07	1.1E-06	2.1E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.5E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	0 %	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	8.1E-08	1.6E-07	2.6E-07	1.6E-07	3.2E-07	5.2E-07	8.7E-07	1.7E-06	2.7E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.5E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.2E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	6.6E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
1oo3	0 %	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.1E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.1E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	2.2E-08	1.0E-07	2.0E-07	4.9E-08	2.1E-07	4.1E-07	4.2E-07	1.2E-06	2.2E-06
	90 %	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07	6.4E-08	2.6E-07	5.1E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.2E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	8.2E-08	1.6E-07	2.6E-07	1.7E-07	3.3E-07	5.3E-07	1.0E-06	1.8E-06	2.8E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.6E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	9.0E-08	2.8E-07	5.3E-07	2.6E-07	6.3E-07	1.1E-06	4.5E-06	5.9E-06	7.6E-06
	60 %	2.6E-08	1.1E-07	2.0E-07	6.6E-08	2.2E-07	4.2E-07	8.5E-07	1.6E-06	2.5E-06
	90 %	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07	9.3E-08	2.9E-07	5.3E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.7E-09	2.6E-08	5.1E-08
1oo3	0 %	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	5.5E-07	2.5E-06	5.0E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.0E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.2E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.0E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.5E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	2.4E-08	1.0E-07	2.0E-07	5.7E-08	2.1E-07	4.1E-07	6.3E-07	1.4E-06	2.3E-06
	90 %	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07	7.8E-08	2.7E-07	5.2E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08
2oo2 (see note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	8.4E-08	1.6E-07	2.6E-07	1.8E-07	3.3E-07	5.3E-07	1.2E-06	2.0E-06	2.9E-06
	90 %	9.5E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	9.8E-07	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	1.3E-07	3.2E-07	5.5E-07	4.2E-07	7.7E-07	1.2E-06	8.4E-06	9.2E-06	1.0E-05
	60 %	3.3E-08	1.1E-07	2.1E-07	9.1E-08	2.4E-07	4.4E-07	1.5E-06	2.1E-06	2.9E-06
	90 %	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07	1.3E-07	3.2E-07	5.6E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	6.1E-09	2.6E-08	5.1E-08
1oo3	0 %	5.0E-08	2.5E-07	5.0E-07	1.0E-07	5.0E-07	1.0E-06	7.1E-07	2.7E-06	5.1E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.1E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.0E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.13 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one year and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see note 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.1E-09	1.0E-08	2.0E-08	4.3E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
2oo2 (see note 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D (see note 3)	0 %	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	1.6E-09	3.2E-09	5.2E-09	8.1E-09	1.6E-08	2.6E-08	1.6E-08	3.2E-08	5.2E-08
	90 %	1.9E-09	2.3E-09	2.8E-09	9.5E-09	1.2E-08	1.4E-08	1.9E-08	2.3E-08	2.8E-08
	99 %	2.0E-09	2.0E-09	2.1E-09	1.0E-08	1.0E-08	1.0E-08	2.0E-08	2.0E-08	2.1E-08
2oo3	0 %	1.1E-09	5.1E-09	1.0E-08	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.5E-08	1.0E-07
	60 %	4.1E-10	2.0E-09	4.0E-09	2.3E-09	1.0E-08	2.0E-08	5.0E-09	2.1E-08	4.1E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09
1oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	4.0E-10	2.0E-09	4.0E-09	2.0E-09	1.0E-08	2.0E-08	4.0E-09	2.0E-08	4.0E-08
	90 %	1.0E-10	5.0E-10	1.0E-09	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08
	99 %	1.0E-11	5.0E-11	1.0E-10	5.0E-11	2.5E-10	5.0E-10	1.0E-10	5.0E-10	1.0E-09

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (see note 2)	0 %	2.5E-06			5.0E-06			2.5E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	2.9E-08	1.1E-07	2.1E-07	7.4E-08	2.3E-07	4.2E-07	1.1E-06	1.7E-06	2.6E-06
	90 %	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07	1.0E-07	3.0E-07	5.4E-07
	99 %	5.1E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.6E-09	2.6E-08	5.0E-08
2oo2 (see note 2)	0 %	5.0E-06			1.0E-05			5.0E-05		
	60 %	2.0E-06			4.0E-06			2.0E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D (see note 3)	0 %	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	8.9E-08	1.7E-07	2.7E-07	1.9E-07	3.5E-07	5.4E-07	1.7E-06	2.3E-06	3.2E-06
	90 %	9.6E-08	1.2E-07	1.4E-07	1.9E-07	2.3E-07	2.8E-07	1.0E-06	1.2E-06	1.4E-06
	99 %	1.0E-07	1.0E-07	1.0E-07	2.0E-07	2.0E-07	2.1E-07	1.0E-06	1.0E-06	1.0E-06
2oo3	0 %	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	1.6E-05	1.6E-05	1.6E-05
	60 %	4.6E-08	1.2E-07	2.2E-07	1.4E-07	2.9E-07	4.7E-07	2.8E-06	3.2E-06	3.8E-06
	90 %	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.6E-08	1.0E-07	2.1E-07	3.9E-07	6.2E-07
	99 %	5.2E-10	2.5E-09	5.0E-09	1.1E-09	5.1E-09	1.0E-08	6.9E-09	2.7E-08	5.1E-08
1oo3	0 %	5.1E-08	2.5E-07	5.0E-07	1.1E-07	5.1E-07	1.0E-06	1.4E-06	3.2E-06	5.5E-06
	60 %	2.0E-08	1.0E-07	2.0E-07	4.0E-08	2.0E-07	4.0E-07	2.6E-07	1.0E-06	2.0E-06
	90 %	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07	5.1E-08	2.5E-07	5.0E-07
	99 %	5.0E-10	2.5E-09	5.0E-09	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08

NOTE 1 This table gives example values of PFH_G, calculated using the equations in B.3.3 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively (see B.3.3.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average frequency of a dangerous failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table C.2 – Diagnostic coverage and effectiveness for different elements

Component	Low diagnostic coverage	Medium diagnostic coverage	High diagnostic coverage
CPU (see Note 3)	total less than 70 %	total less than 90 %	
register, internal RAM	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
coding and execution including flag register	50 % - 60 %	75 % - 95 %	-
(see Note 3)	50 % - 70 %	85 % - 98 %	-
address calculation (see Note 3)	50 % - 60 %	60 % - 90 %	85 % - 98 %
program counter, stack pointer	50 % - 70 %		
	40 % - 60 %		
Bus			
memory management unit	50 %	70 %	90 % - 99 %
bus-arbitration	50 %	70 %	90 % - 99 %
Interrupt handling	40 % - 60 %	60 % - 90 %	85 % - 98 %
Clock (quartz) (see Note 4)	50 %	-	95 % - 99 %
Program flow monitoring			
temporal (see Note 3)	40 % - 60 %	60 % - 80 %	-
logical (see Note 3)	40 % - 60 %	60 % - 90 %	-
temporal and logical (see Note 5)	-	65 % - 90 %	90 % - 98 %
Invariable memory	50 % - 70 %	99 %	99,99 %
Variable memory	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Discrete hardware			
digital I/O	70 %	90 %	99 %
analogue I/O	50 % - 60 %	70 % - 85 %	99 %
power supply	50 % - 60 %	70 % - 85 %	99 %
Communication and mass storage	90 %	99,9 %	99,99 %
Electromechanical devices	90 %	99 %	99,9 %
Sensors	50 % - 70 %	70 % - 85 %	99 %
Final elements	50 % - 70 %	70 % - 85 %	99 %

NOTE 1 This table should be read in conjunction with Table A.1 of IEC 61508-2 which provides the failure modes to be considered.

NOTE 2 When a range is given for diagnostic coverage, the upper interval boundaries may be set only for narrowly tolerated monitoring means, or for test measures that stress the function to be tested in a highly dynamic manner.

NOTE 3 For techniques where there is no high diagnostic coverage figure, at present no measures and techniques of high effectiveness are known.

NOTE 4 At present no measures and techniques of medium effectiveness are known for quartz clocks.

NOTE 5 The minimum diagnostic coverage for a combination of temporal and logical program flow monitoring is medium.

Table D.4 – Calculation of β_{int} or $\beta_{D\ int}$

Score (S or S_D)	Corresponding value of β_{int} or $\beta_{D\ int}$ for the:	
	Logic subsystem	Sensors or final elements
120 or above	0,5 %	1 %
70 to 120	1 %	2 %
45 to 70	2 %	5 %
Less than 45	5 %	10 %

NOTE 1 The maximum levels of $\beta_{D\ int}$ shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this.

NOTE 2 Values of $\beta_{D\ int}$ lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.

Allegato L

Verifica pratica del SIL in funzione dell'architettura del SIS

L.1 Premessa

Questo Allegato riporta degli esempi tipici di identificazione di un certo SIL determinato come descritto precedentemente a seguito delle seguenti fasi:

- Valutazione preliminare del rischio : PRA
- Studio di analisi del rischio e operabilità : HAZOP
- Tecnica di riduzione del rischio quanto praticabile : ALARP
- Definizione dei Sistemi relativi alla Sicurezza : SrS
- Determinazione del Sistema Strumentato di Sicurezza : SIS
- Valutazione del Livello di Integrità di Sicurezza : SIL

esaminando varie tipiche architetture del SIS e calcolandone la Probabilità di Guasto su Domanda del sistema PFD_{SYS} a fronte delle seguenti singole PFD_{SUB} dei sottosistemi componenti i sistema stesso (vedasi anche Figura H.1):

$$\mathbf{PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}}$$

dove: PFD_S è la PFD_{avg} del sensore (di misura)
PFD_L è la PFD_{avg} del risolutore logico
PFD_{FE} è la PFD_{avg} dell'elemento finale

Puramente per scopo esemplificativo senza alcun carattere di specificità applicativa, nel prosieguo verranno presentate sotto forma tabellare delle tipiche soluzioni di possibili architetture del SIS, con componenti standard aventi le seguenti caratteristiche comuni per i diversi elementi costitutivi il SIS (ovvero per sensore, risolutore logico ed elemento finale):

Caratteristiche degli esempi	**Sigla**	**Parametri**
– Architetture tipiche previste	: MooN	: Varie
– Tasso di guasto medio per ora	λ	: $1 \cdot 10^{-5}$
– Copertura diagnostica dei componenti	: DC	: 0, 60,90, 99%
– Tasso di guasto modo comune in sistemi ridondati	: β	: 10%
– Tasso di guasto modo comune rilevati dalla diagnostica	: β_D	: 5%
– Intervallo di test delle prove periodiche	: TI	: 1 anno
– Tempo di ristabilimento del loop (e con MRT = MTTR)	: MTTR	: 8 ore

allo scopo di rilevare le variazioni del SIL ottenuto in relazione essenzialmente della architettura considerata e della copertura diagnostica prevista.

NOTA Nelle esemplificazioni condotte secondo le equazioni della CEI EN 61508-6 (Allegato H) si è supposta una distribuzione dei guasti come descritta in calce alla Figura H.2, cioè:

- Tasso dei guasti dannosi rilevati :λ_{DD} :DC · λ/2
- Tasso dei guasti dannosi non rilevati :λ_{DU} :(1-DC)·λ/2

ovvero in accordo alla norma di riferimento CEI EN 61508-6.

L.2 Esempi di determinazione del Livello di Integrità di Sicurezza SIL

1) Esempio di calcolo del SIL con Copertura Diagnostica DC del 0%

MooN del SUB	Guasti Totali λ	Copertura Diagnost. DC	Guasti pericolosi λ_D	Guasti rilevati λ_{DD}	Guasti non rilev. λ_{DU}	ParametroMTTR (h)	Intervallo TI (y)	PFD AVG (compon.)	PFD SYS (SIS)	SIL SYS (SIS)
1oo1	1,0E-05	0	5,0E-06	0,0E-06	5,0E-06	8	1	2,2E-02	6,6E-02	SIL 1
1oo2	1,0E-05	0	5,0E-06	0,0E-06	5,0E-06	8	1	2,7E-03	8,1E-03	SIL 2
2oo2	1,0E-05	0	5,0E-06	0,0E-06	5,0E-06	8	1	4,4E-02	1,3E-01	SIL 0
1oo2D	1,0E-05	0	5,0E-06	0,0E-06	5,0E-06	8	1	2,7E-03	8,1E-03	SIL 2
2oo3	1,0E-05	0	5,0E-06	0,0E-06	5,0E-06	8	1	3,8E-03	1,1E-02	SIL 1

2) Esempio di calcolo del SIL con Copertura Diagnostica DC del 60%

MooN del SUB	Guasti Totali λ	Copertura Diagnost. DC	Guasti pericolosi λ_D	Guasti Rilevati λ_{DD}	Guasti non rilev. λ_{DU}	Parametro MTTR (h)	Intervallo TI (y)	PFD AVG (compon.)	PFD SYS (SIS)	SIL SYS (SIS)
1oo1	1,0E-05	0,6	5,0E-06	3,0E-06	2,0E-06	8	1	8,8E-03	2,6E-02	SIL 1
1oo2	1,0E-05	0,6	5,0E-06	3,0E-06	2,0E-06	8	1	9,7E-04	2,9E-03	SIL 2
2oo2	1,0E-05	0,6	5,0E-06	3,0E-06	2,0E-06	8	1	1,8E-02	5,3E-02	SIL 1
1oo2D	1,0E-05	0,6	5,0E-06	3,0E-06	2,0E-06	8	1	9,0E-04	2,7E-03	SIL 2
2oo3	1,0E-05	0,6	5,0E-06	3,0E-06	2,0E-06	8	1	1,1E-03	3,4E-03	SIL 2

3) Esempio di calcolo del SIL con Copertura Diagnostica DC del 90%

MooN del SUB	Guasti Totali λ	Copertura Diagnost. DC	Guasti pericolosi λ_D	Guasti rilevati λ_{DD}	Guasti non rilev. λ_{DU}	Parametro MTTR (h)	Intervallo TI (y)	PFD AVG (compon.)	PFD SYS (SIS)	SIL SYS (SIS)
1oo1	1,0E-05	0,9	5,0E-06	4,5E-06	5,0E-07	8	1	2,2E-03	6,7E-03	SIL 2
1oo2	1,0E-05	0,9	5,0E-06	4,5E-06	5,0E-07	8	1	2,3E-04	6,8E-04	SIL 3
2oo2	1,0E-05	0,9	5,0E-06	4,5E-06	5,0E-07	8	1	4,5E-03	1,3E-02	SIL 1
1oo2D	1,0E-05	0,9	5,0E-06	4,5E-06	5,0E-07	8	1	2,2E-04	6,6E-04	SIL 3
2oo3	1,0E-05	0,9	5,0E-06	4,5E-06	5,0E-07	8	1	2,4E-04	7,2E-04	SIL 3

4) Esempio di calcolo del SIL con Copertura Diagnostica DC del 99%

MooN del SUB	Guasti Totali λ	Copertura Diagnost. DC	Guasti pericolosi λ_D	Guasti rilevati λ_{DD}	Guasti non rilev. λ_{DU}	ParametroMTTR (h)	Intervallo TI (y)	PFD AVG (compon.)	PFD SYS (SIS)	SIL SYS (SIS)
1oo1	1,0E-05	0,99	5,0E-06	5,0E-06	5,0E-08	8	1	2,6E-04	7,8E-04	SIL 3
1oo2	1,0E-05	0,99	5,0E-06	5,0E-06	5,0E-08	8	1	2,4E-05	7,2E-05	SIL 4
2oo2	1,0E-05	0,99	5,0E-06	5,0E-06	5,0E-08	8	1	5,2E-04	1,6E-03	SIL 2
1oo2D	1,0E-05	0,99	5,0E-06	5,0E-06	5,0E-08	8	1	2,4E-05	7,2E-05	SIL 4
2oo3	1,0E-05	0,99	5,0E-06	5,0E-06	5,0E-08	8	1	2,4E-05	7,3E-05	SIL 4

Dai 4 esempi sopra riportati pur con le semplificazioni ed approssimazioni fatte:

a) tasso di guasto medio considerato piuttosto elevato:
tenuto conto però di attuali applicazioni già esistenti;

b) di conseguenza copertura diagnostica da nulla a massima:
ovvero DC da 0 a 99%;

c) tassi medi dei guasti pericolosi rilevati dalla diagnostica tipici:
ovvero pari a DC/2 per il tasso totale di guasto λ;

d) tassi medi dei guasti pericolosi rilevati dalla diagnostica in sistemi ridondati:
ovvero β_D del 5% rispetto i guasti presunti di causa e modo comune β del 10%;

e) tempo medio di riparazione dei componenti del sistema di sicurezza:
MTTR di 8 ore;

f) intervallo delle prove periodiche:
TI di 1 anno;

g) architettura uguale per ogni sottosistema (SUB) costituenti il Sistema (SYS):
sebbene l'architettura dei sottosistemi possa essere di fatto diversa,

si possono trarre le seguenti considerazioni:

I) pur con una buona affidabilità di guasto certi sistemi non risultano affidabili SIL:
vedasi per esempio l'architettura 2oo2, nel 1) esempio;

II) all'aumentare della copertura diagnostica DC aumenta il livello del SIL:
di circa due unità di SIL passando da DC = 0% a DC = 99%, dal 1) al 4) esempio;

III) all'aumentare della ridondanza e copertura diagnostica aumenta pure il SIL:
arrivando anche ad un potenziale SIL 4, nell'esempio 4) con diverse architetture.

Bisogna però ricordare che comunque vanno rispettate le minime ridondanze previste in Tabella 9 (Route $_{1H}$) e Tabella 10 (Route $_{2H}$).

Inoltre si deve ricordare che, se nella valutazione della Probabilità di Guasto su Domanda dell'intero sistema PFD_{SYS} si dovessero avere dei valori in difetto rispetto al SIL richiesto, le soluzioni di seguito evidenziate possono essere adatte allo scopo:

a) ridondanze plurime su certi sottosistemi critici;

b) riduzione dell'intervallo di test delle prove periodiche;

c) diversificazione nelle tecnologie dei sottosistemi per evitare cause modo comune;

oltre ad usare componenti a più alta affidabilità e con maggiore copertura diagnostica.

Allegato M

Prove periodiche parziali dell'architettura del SIS

M.1 Premessa

Se nell'intervallo delle prove periodiche totali si effettuano delle prove periodiche parziali si può mantenere il SIL nominale per più tempo, oppure migliorare il SIL nominale nell'ambito della periodicità delle prove totali.

Se si distinguono i due seguenti parametri per l'intervallo delle prove:

- T1 : Partial Proof Test Interval, ovvero l'intervallo tra le prove parziali
- T2 : Total Proof Test Interval, ovvero l'intervallo tra le prove totali

e il parametro aggiuntivo per la copertura delle prove parziali:

- ✓ PTC: Proof Test Coverage (%)

prove parziali, che se condotte nell'intervallo delle prove totali, possono allungarne l'intervallo in relazione alla % di copertura di prova condotta PTC.

La formula per la determinazione della Probabilità di Guasto su Domanda per un sistema non ridondato 1oo1 con un determinato Proof Test Coverage PTC, diventa:

$$PFD_{1oo1(PTC)} = PTC \cdot \lambda_{DU} \cdot \frac{T1}{2} + (1 - PTC) \cdot \lambda_{DU} \cdot \frac{T2}{2}$$

Per PTC = 100% corrisponde alla forma classica approssimata perché manca il secondo termine in quanto le prove parziali sono totali;

ciò significa che si può spingere il T2 fino a 10 y se nel frattempo si fanno prove parziali a T1 efficaci con PTC verso 80-90%, oppure migliorare SIL per esempio nelle valvole con l'apertura/chiusura parziale delle valvole in esercizio, senza portare l'impianto in fermata.

M.2 Esempio

Si abbia una valvola con i parametri indicati in Tabella M.1, ove si noti:

- Nella prima riga, il mantenimento del SIL per un anno senza prove parziali
- Nella seconda riga, il miglioramento del SIL per un anno con prove parziali ogni mese aventi un ottimo PTC del 90%
- Nella terza riga, il non miglioramento del SIL per un anno con prove parziali ogni mese aventi uno scarso PTC del 50%.

Va da se che le prove parziali sono efficaci solo qualora possono simulare realmente le prove periodiche totali con un Proof Test Coverage PTC verso il 100%, significa aperture e chiusure parziali delle valvole del 20-30% atte a ben simulare il completo comportamento di apertura/chiusura.

Tabella M.1 – Esempio di prove parziali su valvole

Tasso guasto λ	Coppertura diagnostica **DC**	Guasti pericolosi **λd**	Guasti rilevati **λdd**	Guasti non rilev **λdu**	Parametro Copertura **PTC**	Parametro altro **1-PTC**	Parametro **MRT h**	Parametro **MTTR h**	Int. Par. T1 **y**	Int. Tot T2 **y**		**PFD** con PTC **1001**	**PFD** senza PTC **1001**
5,0E-06	0,6	2,5E-06	1,5E-06	1,0E-06	0	1	4	8	0	1	**SIL 2**	4,4E-03	4,4E-03
5,0E-06	0,6	2,5E-06	1,5E-06	1,0E-06	0,9	0,1	4	8	0,0833	1	**SIL 3**	7,7E-04	
5,0E-06	0,6	2,5E-06	1,5E-06	1,0E-06	0,5	0,5	4	8	0,0833	1	**SIL 2**	2,4E-03	

BIBLIOGRAFIA

[1] IEC 61513: Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems.

[2] EN 50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process

[3] EN 50128: Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

[4] EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[5] CEI EN 60601-1-4 Medical electrical equipment - Part 1-4: General requirements for safety - Collateral Standard: Programmable electrical medical systems

[6] CEI EN 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

[7] IEC/TS 61000-1-2: Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena

[8] CEI EN 61511: Functional safety - Safety instrumented systems for process industry sector:

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines for the application of IEC 61511
- Part 3: Guidance for the determination of the required safety integrity levels

[9] CEI EN 61326: Electrical equipment for measurement, control and laboratory use - EMC requirements:

- Part 3-1: Immunity requirements for equipment performing or intended to perform safety related functions (functional safety) - General industrial applications
- Part 3-2: Immunity requirements for equipment performing or intended to perform safety related function (functional safety) - Industrial applications with particular EM environment

[10] CEI EN 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

[11] ISO 13849: Safety of machinery – Safety related parts of control systems (SRPCS) (in preparation):

- Part 1: General principles for design
- Part 2: Validation

[12] Project IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety Requirements – Functional

[13] EN 50090-2-3: Home and Building Electronic Systems (HBES) - Part 2-3: System overview - General functional safety requirements for products intended to be integrated in HBES

[14] Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry -No.070, October 2004

[15] Guide to the application of IEC 61511 to safety instrumented systems in the UK process industries - Draft for committee and industry review - November 2006

La presente Norma è stata compilata dal Comitato Elettrotecnico Italiano e beneficia del riconoscimento di cui alla legge 1° Marzo 1968, n. 186.

Editore CEI, Comitato Elettrotecnico Italiano, Milano – Stampa in proprio

Autorizzazione del Tribunale di Milano N. 4093 del 24 Luglio 1956

Direttore Responsabile: Ing. R. Bacci

Comitato Tecnico Elaboratore

CT 65 – Misura, controllo e automazione nei processi industriali

Altre norme di possibile interesse sull'argomento

Progetto
C. 1225:2018-11 – Scad. 07-01-2019
Totale Pagine 149

Via Saccardo, 9
20134 Milano
Tel. 02.21006.1
Fax 02.21006.210
cei@ceiweb.it
www.ceiweb.it