UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Tecnica e Gestione dei sistemi industriali
Corso di Laurea Triennale in Ingegneria Meccatronica

TESI DI LAUREA

PROGETTAZIONE E VALIDAZIONE DELLE FUNZIONI DI SICUREZZA DELLA MACCHINA: NORMA EN IEC 62061:2021-07

Relatore:
Prof. Diego Dainese

Laureando:
Federico Toffoletto

Matricola: 1223956

Anno Accademico 2021-2022

Indice

Introduzione **5**

1 L'Unione Europea e il suo mercato interno **7**
1.1 Il contesto storico 7
1.2 Il mercato unico europeo 8
1.3 Gli atti legislativi 9
1.3.1 Il Vecchio Approccio 10
1.3.2 Il Nuovo Approccio 10
1.3.3 Le norme tecniche 11
1.3.4 Conformità e marcatura del prodotto 12

2 La Direttiva Macchine 2006/42/CE **15**
2.1 La trattazione della Direttiva 15
2.1.1 Campi di applicazione 15
2.1.2 Campi di esclusione 16
2.2 I Requisiti Essenziali di Salute e Sicurezza 18
2.3 Conformità della macchina 19
2.3.1 Documentazione 19
2.4 Norme armonizzate 22
2.4.1 Legame con la Norma ISO 12100 22
2.4.2 Legame con la Norma EN IEC 62061 23

3 La Norma EN IEC 62061: 2021-07 **25**
3.1 Introduzione alla Norma 25
3.2 Applicazioni della Norma 26
3.3 Passi necessari a costituire un SCS 28
3.4 Le funzioni di sicurezza 29
3.4.1 Analisi e riduzione del rischio 29
3.4.2 Gestione delle funzioni di sicurezza 30
3.4.3 Eventuali modifiche 31
3.4.4 Specifiche di una funzione di sicurezza 32

4 Progettazione di un SCS **33**
4.1 L'affidabilità dei sistemi di comando e i parametri impiegati 34
4.1.1 Il tasso di guasto 34
4.1.2 Il Main Time To Failure 35
4.1.3 Il parametro B_{10D} 36
4.1.4 Tolleranza ai guasti nell'hardware 36
4.1.5 Il fattore di copertura e il dispositivo di diagnostica 36
4.1.6 Causa di guasto comune 37
4.2 I sottosistemi 38
4.2.1 Le categorie di sicurezza 39

5 La validazione **41**
5.1 Analisi 43
5.2 Test 44

6 Software di sicurezza **45**
6.1 Parametrizzazione degli SCS 45
6.2 Software applicativi dei PLC di sicurezza 47
6.2.1 Software di livello 1 47
6.2.2 Software di livello 2 48
6.3 Costituzione del software 49
6.3.1 Uso dei moduli 49
6.3.2 Codifica 50
6.3.3 Attività di verifica 50
6.3.4 Modifiche e documentazione 52

7 La documentazione **53**
7.1 Documentazione tecnica 53
7.2 Informazioni per l'uso 54

8 Le differenze con l'edizione precedente **55**

9 Calcoli ed esempi **56**
9.1 La determinazione del Safety Integrity Level 56
9.1.1 Gravità del danno 56
9.1.2 Frequenza e durata di esposizione al danno 56
9.1.3 Probabilità che si verifichi un evento pericoloso 57
9.1.3 Probabilità di evitare o limitare il danno 57
9.1.5 Classe di probabilità del danno e attribuzione del SIL . . . 58
9.1.6 Altro metodo di determinazione 58
9.1.7 Calcolo del SIL nel caso di sottosistemi 59
9.2 Esempio di progettazione di un SCS 61
9.2.1 Sottosistema 1 62
9.2.2 Sottosistema 2 63
9.2.3 Sottosistema 3 63
9.2.3 SIL raggiunto dal sistema 64
9.2.4 Test di validazione 64

Conclusioni **65**

Bibliografia **66**

Elenco delle figure **67**

Elenco delle tabelle **68**

Introduzione

La seguente tesi ha lo scopo di illustrare una linea guida che indica i requisiti e le raccomandazioni da seguire nelle fasi di progettazione e validazione dei sistemi di comando e controllo con funzione di sicurezza, ricavate dalla norma EN IEC 62061: 2021-07 Sicurezza del macchinario - sicurezza funzionale dei sistemi di comando e controllo relativi alla sicurezza.

L'obiettivo principale rimane quello di ottenere un'affidabilità adeguata, per quanto riguarda le funzioni di sicurezza, a quella richiesta nella fase di valutazione del rischio, e avere inoltre la presunzione di conformità al Requisito Essenziale di Sicurezza della Direttiva Macchine relativo all'affidabilità nell'esecuzione delle funzioni di sicurezza di tali sistemi.

Questa concordanza in termini di tutela della salute degli utilizzatori garantisce l'immissione nel mercato europeo della macchina stessa, per questo la tesi è organizzata nei primi capitoli in un'analisi generale della struttura e della storia del mercato europeo, per poi terminare nel particolare con le fasi da seguire per una corretta progettazione e costituzione di un singolo elemento di comando con funzione di sicurezza.

La tesi si sviluppa in 9 capitoli:

- Il *Capitolo 1* si presenta come una panoramica sulle caratteristiche del mercato dove sarà immessa la macchina, ovvero quello europeo, attraverso un'analisi del contesto storico che ha portato alla scelta di intraprendere il mercato unico, e uno sguardo agli atti legislativi che regolano il flusso delle merci.

- Nel *Capitolo 2* viene illustrata la Direttiva Macchine in tutti i suoi dettagli, esaminando i suoi campi di applicazione ed esclusione, ed aspetti fondamentali inerenti l'argomento principale della trattazione come i requisiti essenziali di sicurezza, i legami con la norma ISO 12100 per la valutazione del rischio e con la norma EN IEC 62061.

- Il *Capitolo 3* rappresenta il cuore della tesi, ossia una premessa della norma EN IEC 62061 attraverso degli esempi di applicazione e le relazioni con altre norme. In termini del tutto generali sono descritti poi i passi da seguire per costituire un sistema di sicurezza, ognuno dei quali sarà poi approfondito nei seguenti capitoli

- Nel *Capitolo 4* vengono elencate delle misure da tenere in considerazione per constrastare i guasti sistematici e i relativi parametri che consentono di stimare l'affidabilità di un sistema. Infine vengono trattati i sottosistemi come componenti elementari che legati tra loro costituiscono un sistema di comando e controllo con funzione di sicurezza.

- Nel *Capitolo 5* sono elencate e spiegate le varie fasi che portano alla validazione di un sistema di sicurezza, in modo che soddisfi le specifiche dichiarate nella fase di progettazione.

- Nel *Capitolo 6* viene trattato il software di sicurezza, sia in termini di parametrizzazione di dispositivi come scanner, che come programmazione dei PLC di sicurezza impiegati per la diagnostica dei sistemi affinchè abbiano il comportamento desiderato in materia di sicurezza. Come nel caso delle strutture hardware sono poi analizzate i processi di convalida.
- Il *Capitolo 7* elenca la documentazione che deve accompagnare il sistema di sicurezza al momento dell'immissione nel mercato rispettando il RESS 1.7.4 della Direttiva Macchine
- Il *Capitolo 8* tratta le differenze con l'edizione precedente e con l'altra norma di riferitmento per i sistemi di comando e controllo con funzione di sicurezza, ovvero la ISO 13849.
- Nel *Capitolo 9* vengono effettuati dei calcoli ai fini di esempio per ricavare il livello di affidabilità e per la progettazione di un SCS.

Capitolo 1

L'Unione Europea e il suo mercato interno

1.1 Il contesto storico

L'Unione Europea così come la conosciamo oggi è nata da un susseguirsi di fasi, partite al termine della Seconda Guerra Mondiale, il cui scopo era quello di raggiungere un'unità continentale al fine di evitare ulteriori conflitti su suolo europeo e una cooperazione economica. Quest'ultimo aspetto è di fondamentale importanza dal momento che porterà in Europa il concetto di mercato unico, il cui principio cardine è la libera circolazione delle merci, garantendo la sicurezza e la salute delle persone e la tutela dell'ambiente. La storia dell'Unione, infatti, inizia con una serie di accordi prettamente economici, per poi espandersi anche nei campi di politica e giustizia.

A seguito della Seconda guerra mondiale, nel 1945, l'Europa era un continente devastato che dipendeva in larga misura dall'assistenza del mondo esterno. Infatti, gli Stati europei, che avevano dominato sino a quel periodo, conobbero un periodo di declino, mentre ad emergere furono le superpotenze USA ed Unione Sovietica, che si spartirono il territorio europeo legando a sé i governi dei diversi Stati ed influenzandone le scelte.
Negli anni a seguire i vari Paesi cercarono un'autonomia dalle due grandi potenze in modo tale da poter sviluppare e consolidare le proprie potenzialità economiche e politiche.

Un primo passo verso un'Europa unita si ebbe nell'aprile del 1951 quando venne fondata la CECA ovvero la Comunità Europea del Carbone e dell'Acciaio allo scopo di mettere in comune le produzioni di queste due materie prime tra Belgio, Francia, Germania Ovest, Italia, Lussemburgo e Paesi Bassi. La scelta di queste due materie prime era strategica dal momento che in questi Paesi c'erano dei giacimenti di queste materie prime, oltre a tale aspetto, c'era anche la volontà di controllare l'approvvigionamento di carbone e acciaio, elementi che erano alla base della costruzione di materiale bellico, in questo modo si impediva un eventuale riarmo segreto. Cosa più importante, venivano poste le basi per una libera circolazione delle merci, infatti a tutte quelle che rientravano nel settore carbosiderurgico, vennero abolite le barriere doganali. Questo accordo serviva anche per rinvigorire le economie allo scopo di inserire i Paesi nell'apparato politico internazionale.

Un ulteriore passo in avanti venne fatto nel 1957, quando il trattato precedente fu allargato ad altri settori economici, e venne istituita la Comunità Economica Europea a cui aderirono i Paesi facenti parte della CECA, ma in questo caso si creò un mercato comune basato sulla libera circolazione non solo di merci, ma anche di persone, servizi e capitali. Negli anni a seguire sono entrati a far parte anche altri Stati membri.

Il 7 febbraio 1992 viene firmato il trattato di Maastricht, in cui rispetto agli altri trattati, l'unione tra gli Stati si poggia su 3 pilastri:

1. *La Comunità Europea,* allo scopo di garantire il funzionamento del mercato unico e lo sviluppo del settore economico, oltre che perseguire ad un'unità anche monetaria;

2. *La politica estera e di sicurezza comune,* al fine di mantenere l'integrità e l'indipendenza dell'unione;

3. *Cooperazione in termini di giustizia e affari interni,* al fine di fornire ai cittadini un livello di sicurezza garantendone la libertà.

Dal 2007 con il trattato di Lisbona, l'unione di 27 Stati europei ha dato vita alla struttura attuale, l'Unione Europea.

1.2 Il mercato unico europeo

Dopo aver analizzato i passi cruciali che hanno portato alla nascita dell'Unione Europea, si illustrano, invece, le fasi che hanno portato alla costituzione del mercato unico europeo che rappresenta uno dei principali obiettivi dell'Unione, fin da quando sono state poste le basi per la sua nascita.

Tutto ha inizio nel 1957 con i Trattati di Roma, dove, oltre alla costituzione della CEE, gli Stati membri si impegnarono a creare un mercato unico attraverso un programma della durata di dodici anni. A tal proposito il 1° luglio 1968 venne introdotta l'unione doganale tra i Paesi membri dell'allora CEE, questo significava che le varie autorità doganali collaboravano tra loro come se fossero un'unica entità, cominciarono quindi ad applicare dei dazi doganali comuni per merci provenienti da Stati terzi, mentre vennero soppressi per le merci che circolavano tra i Paesi facenti parte della Comunità. Questo garantì un aumento del volume del commercio oltre che una maggior coesione tra i vari Stati.
Nonostante l'eliminazione delle barriere commerciali fra Stati permise un notevole sviluppo dell'economia europea, rimasero comunque dei limiti dovuti soprattutto ad una differenziazione di normative tecniche tra i vari Paesi, ovvero quello che viene definito il Vecchio Approccio. Per questo nel 1986 viene firmato l'Atto Unico Europeo, con entrata in vigore l'anno seguente, si tratta di un programma di 6 anni che puntava a risolvere questi ostacoli, definito Nuovo Approccio, in modo da costituire un mercato sempre più efficiente.

Nel 1993 il grande passo, ossia l'istituzione del mercato unico europeo, che si basa su quattro grandi pilastri, la libera circolazione di:

1. *Persone,* attraverso l'istituzione dello Spazio Schengen;

2. *Merci,* già in vigore con l'eliminazione delle barriere doganali;

3. *Servizi,* ovvero con la possibilità di esercizio di un'attività economica in uno Stato membro, diverso dal proprio Stato di origine;

4. *Capitali,* banalmente, il trasferimento di un importo monetario da un Paese all'altro.

È bene comunque sottolineare che nel 1960 alcuni Paesi europei che non desideravano o non potevano entrare a far parte della Comunità Economica Europea, istituirono un proprio mercato comune, ovvero l'associazione europea di libero scambio – EFTA – a cui partecipavano Austria, Danimarca, Norvegia, Portogallo, Svezia, Svizzera e Regno Unito, e al quale si aggiunsero successivamente Finlandia, Islanda e Liechtenstein. Lo scopo principale era una collaborazione economica tra questi Stati, alla pari del mercato unico della CEE.

Al fine di consolidare e rafforzare l'economia europea, quindi dell'intero continente, le divisioni tra EFTA e CE vennero cancellate e, nel 1994, venne istituito il SEE, ossia lo Spazio Economico Europeo, al fine di estendere le disposizioni del mercato unico comunitario anche ai Paesi facenti parte dell'EFTA.

1.3 Gli atti legislativi

L'Unione Europea, così come la conosciamo oggi si fonda sullo Stato di diritto, ciò significa che nessuna entità che la costituisce è al di sopra della legge, ovvero che tutte le azioni intraprese, nascono da trattati approvati da tutti gli Stati che ne fanno parte.

Un trattato è un accordo vincolante tra i paesi membri dell'UE. Esso definisce gli obiettivi dell'Unione, le regole di funzionamento delle istituzioni europee, le procedure per l'adozione delle decisioni e le relazioni tra l'UE e i suoi Paesi membri.

In ambito economico gli obiettivi dell'unione europea riguardano

- Creare un mercato interno;
- Conseguire uno sviluppo sostenibile basato su una crescita economica equilibrata e sulla stabilità dei prezzi;
- Rafforzare la coesione economica tra i paesi membri.

Per realizzare gli obiettivi elencati nei trattati, l'UE adotta diversi tipi di atti legislativi, di cui alcuni sono applicati in tutti i paesi dell'Unione, altri solo in alcuni, altri atti possono essere vincolanti, altri meno. Due fra gli atti legislativi principali sono:

Regolamento, è un atto legislativo vincolante che diventa obbligatorio appena è emesso, 20 giorni dopo la pubblicazione nella GUUE, la Gazzetta Ufficiale dell'Unione Europea, oppure nella data indicata nello stesso. Deve essere applicato in tutti i suoi elementi nell'intera Unione Europea.

I regolamenti vengono scritti nel momento in cui si ha la necessità che tutti i Paesi recepiscano nello stesso momento le medesime disposizioni. Proprio per non creare disomogeneità tra gli Stati, si sta cercando di emanare i regolamenti come atti legislativi principali.

Direttiva, è un atto legislativo che stabilisce un obiettivo che tutti i Paesi devono realizzare, però in questo caso spetta ai singoli Stati definire in che modo raggiungere tali obiettivi attraverso delle disposizioni nazionali. Non è obbligatoria nell'immediato, ma è comunque presente un periodo di recepimento e applicazione, ed anche una data ultima di ricezione. Ad una direttiva ogni stato può aggiungere le parti relative al controllo e alla sanzionatoria in caso di violazione.

Affinché una direttiva abbia effetto a livello nazionale, deve essere prevista una legge dello Stato membro, viene emanato un decreto attuativo che deve raggiungere gli stessi obiettivi della direttiva.

1.3.1 Il Vecchio Approccio

Il principale vantaggio del mercato unico europeo è la libera circolazione delle merci e, al momento della sua istituzione, si pensava potesse dare uno sviluppo all'economia europea. Nonostante però l'eliminazione delle barriere tariffarie (i dazi) tra i Paesi membri, restava un limite legato alla presenza di normative tecniche che risultavano diverse per ogni Stato, ovvero quei documenti che stabiliscono delle specifiche tecniche per le merci. Questo aspetto è definito come Vecchio Approccio, in vigore fino al 1986.

Secondo tale aspetto era previsto un approccio per prodotto, vale a dire che ogni Stato fissava dei vincoli che un prodotto doveva rispettare per poter essere commercializzato entro i suoi confini. Chiaramente questo era in contrasto con la politica di libero mercato poiché era comune che un prodotto fosse ritenuto commercializzabile in uno Stato ma non in un altro.

Inoltre, con questo approccio, le normative tecniche formulate erano molto dettagliate, era richiesto quindi uno studio approfondito della normazione prima di realizzare un prodotto e i tempi di emanazione delle stesse erano molto lunghi, inoltre, un costruttore doveva adattare il prodotto sulla base del Paese al quale sarebbe stato commercializzato, questo comportava dei costi aggiuntivi al fabbricante e un rallentamento alla costruzione delle merci che non andava di pari passo con l'evoluzione tecnologica.

1.3.2 Il Nuovo Approccio

Per agevolare la standardizzazione dei prodotti in termini di sicurezza ed evitare i lati negativi del Vecchio Approccio, dal 1985 è stato introdotto il Nuovo Approccio secondo il quale i dettagli tecnici dei prodotti sono sostituiti da Requisiti Essenziali di Sicurezza e Salute.
I RESS sono appunto dei requisiti obbligatori e inderogabili che i prodotti devono soddisfare in modo tale da:

- Tutelare la sicurezza e la salute dell'utilizzatore del prodotto;
- Garantire la libera circolazione del prodotto all'interno del mercato europeo.

Quest'ultimo punto esprime una miglioria rispetto al sistema precedente. Con l'introduzione dei RESS, si ha una omogeneità dei vari prodotti in ambito di sicurezza in tutta la zona del mercato europeo, anziché contare su dettagli tecnici espressi da ogni singolo Stato. Tali disposizioni, trattando elementi di sicurezza, sono di fondamentale importanza anche per intervenire con tempestività nella fase di progettazione al fine di eliminare o ridurre i pericoli del prodotto.

Nelle nuove direttive emanate, definite appunto Direttive di Nuovo Approccio, sono presenti quindi tali vincoli che i prodotti oggetto della direttiva debbono rispettare. In tal senso bisogna specificare che una direttiva di questo tipo esprime l'obiettivo finale del prodotto, ovvero che rispetti i RESS, senza però indicare le strade da percorrere per il raggiungimento di tale obiettivo. Le varie fasi operative da seguire per garantirne la conformità sono espresse nelle norme tecniche.

1.3.3 Le Norme Tecniche

Le norme armonizzate sono orientamenti facoltativi che forniscono specifiche tecniche dei prodotti per garantire la conformità al Requisito Essenziale di Salute e Sicurezza oggetto della norma. Sebbene siano volontarie, la loro applicazione dimostra che i prodotti raggiungono un certo livello di qualità, affidabilità e sicurezza.

Le norme vengono proposte o ratificate dai diversi enti di normazione che possono avere influenza internazionale, europea o sul solo territorio nazionale, tuttavia, possono collaborare tra di loro. Ogni ente di normazione ha il proprio ambito di competenza.

Enti internazionali

ISO, è la più importante organizzazione a livello mondiale per la definizione di norme tecniche per tutti i settori.

IEC, Commissione elettrotecnica Internazionale, riferimento per gli standard del settore elettrotecnico.

Enti Europei

CEN, Comitato Europeo di Normazione, riferimento per le norme tecniche di tutti i settori.

CENELEC, Comitato Europeo di Normazione Elettrotecnica, è il riferimento per il settore elettrotecnico.

Enti Nazionali

UNI, ente nazionale italiano di unificazione, svolge attività di normazione per tutti i settori.

CEI, Comitato Elettrotecnico Italiano, riferimento per il settore elettrotecnico.

Negli ultimi tempi si tende a creare delle norme di tipo IEC o ISO in modo da creare un ulteriore grado standardizzazione internazionale tra i vari prodotti realizzati. Poi ogni ente nazionale o sovranazionale, effettuerà delle modifiche al fine di adattarla al territorio corrispondente.
Gli enti nazionali possono emanare delle norme senza aver alcun riferimento dalle organizzazioni sovranazionali, a patto che per il prodotto in oggetto non sia prevista la libera circolazione al di fuori del Paese, ad esempio il CEI emana delle norme che riguardano gli impianti elettrici delle abitazioni, dato il tipo di applicazione, ha quindi valenza solamente all'interno del territorio nazionale.

Analizzando la Direttiva Macchine, le norme a lei armonizzate vengono suddivise in tre categorie dall'ISO:

Tipo A sono norme di sicurezza fondamentali, esprimono dei concetti di base o dei principi generali per la progettazione che possono essere applicati alle macchine. Un esempio può essere la ISO 12100, norma di riferimento per la valutazione e riduzione del rischio.

Tipo B sono norme di sicurezza generiche, trattano un solo aspetto di sicurezza o un tipo di protezione che può essere utilizzato, a loro volta si suddividono in:

- *B1* trattano aspetti particolari della sicurezza come le distanze di sicurezza, le temperature, rumore, vibrazioni;
- *B2* forniscono un'indicazione circa la progettazione e costruzione di particolari protezioni come, ad esempio, i comandi di controllo a due mani, dispositivi di interblocco o dispositivi di protezione sensibili alla pressione.

Tipo C norme di sicurezza delle macchine, contengono requisiti di sicurezza dettagliati per una particolare macchina o un gruppo di macchine. Sono redatte da un team di esperti tecnici che conoscono la progettazione della macchina, l'uso pratico della macchina, la storia degli incidenti e le tecniche attuabili di riduzione dei rischi.

1.3.4 Conformità e marcatura del prodotto

La responsabilità di conformità ai Requisiti Essenziali di Salute e Sicurezza di un dato prodotto ricade sul fabbricante stesso o su chi lo immette nel mercato. Per garantire tale conformità, che dovrà comunque essere comprovata, si possono seguire due strade.

La prima riguarda l'applicazione di norme armonizzate nella fase di progettazione e realizzazione, e questo garantisce una presunzione di conformità ai RESS oggetto delle norme. Per attestare la conformità sarà necessario menzionare nella documentazione tecnica di conformità le norme che sono state seguite.

La seconda via è in contrasto con la precedente, ovvero nel momento in cui i prodotti vengono realizzati senza applicare le norme tecniche. Questo comporta un'ulteriore difficoltà al momento della loro costituzione, poiché non si impiega una linea guida che descrive dettagliatamente le fasi da seguire, ed inoltre può

risultare complesso il fatto di dover dimostrare che il prodotto è comunque conforme ai RESS stabiliti nella valutazione dei rischi.

L'attestazione di conformità del prodotto avviene tramite un'autocertificazione del fabbricante, oppure è possibile prevedere una certificazione da un ente autorizzato e notificato dalle autorità governative nazionali ed europee. Questo risulta obbligatorio per i prodotti pericolosi, che rientrano soprattutto nell'ambiente medicale o che saranno installati nelle atmosfere esplosive o che fanno uso di gas o liquidi esplosivi. Tuttavia, anche in questo secondo caso lo stesso fabbricante deve costituire una dichiarazione di conformità anche se è intervenuto un organismo preposto, in modo tale da assumersi la piena responsabilità riguardo il rispetto dei RESS del proprio prodotto, serve anche per consentire la tracciabilità del prodotto stesso.

Oltre alla documentazione tecnica nella quale si dichiara la conformità ai Requisiti Essenziali di Sicurezza, è necessario apporre anche un marchio grafico CE. Tale marchio indica la Conformità Europea ai requisiti che sono previsti in materia di sicurezza, salute e tutela dell'ambiente e viene apposto per poter avere un'indicazione visibile e facilmente individuabile rispetto a tale materia. È un simbolo di destinazione, non di origine, ovvero attesta che quel dato prodotto può essere commercializzato all'interno dell'UE, mentre può comunque provenire da un Paese extra Unione Europea. Il marchio deve avere delle caratteristiche precise:

- Visibile;
- Indelebile, si eseguono delle prove di cancellazione con acqua e solventi, e il marchio non deve essere cancellato;
- Leggibile, sono previste delle misure minime delle lettere C ed E, tuttavia devono avere la stessa dimensione.

Figura 1.1 Simbolo grafico della marcatura CE

Con il Nuovo Approccio, non è prevista l'apposizione del marchio CE in tutti i prodotti. Alcuni richiedono altri tipi di marcature come, ad esempio, quelli del settore marittimo (il marchio è una ruota del timone) o per le apparecchiature da impiegare in ambienti esplosivi (logo EX).

Figura 1.2 Simbolo grafico della marcatura Atex

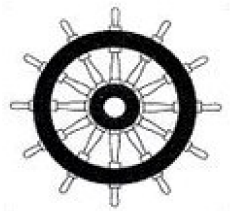


Figura 1.3 Simbolo grafico della marcatura per equipaggiamenti marittimi

Capitolo 2

La Direttiva Macchine 2006/42/CE

2.1 La trattazione della Direttiva

È una direttiva emanata dalla Comunità Europea nel 2006, mentre è entrata in vigore in Italia nel 2010 attraverso il decreto attuativo 17/2010. Nonostante sia passato un periodo di transizione di quattro anni prima di recepirla nel nostro Stato, anche la maggior parte dei Paesi membri l'ha recepita nello stesso periodo, garantendo quindi una certa uniformità tra le macchine che venivano realizzate. È una Direttiva Prodotto facente parte del Nuovo Approccio, il cui contenuto principale è un elenco di Requisiti Essenziali di Sicurezza e di Salute che devono essere assicurati per ogni tipo di macchina durante tutto il ciclo di vita della stessa, ossia dall' installazione fino allo smantellamento. Quindi tutte le macchine provviste di dichiarazione di conformità e, se prevista, marcatura CE, rispettano le disposizioni della presente Direttiva.

2.1.1 Campi di applicazione

La direttiva si applica ai seguenti prodotti:

- **Macchine,** *insieme equipaggiato o destinato ad essere equipaggiato di un sistema di azionamento diverso dalla forza umana o animale, composto di parti o componenti di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata.*
  Per macchine sono intese anche quelle non ancora collegate al sito di impiego o alle fonti di energia e movimento, e allo stesso tempo, una macchina pronta per essere installata, ma che può funzionare solo dopo essere montata su un mezzo di trasporto, in un edificio o in una costruzione. A titolo esemplificativo, un braccio robotico non costituisce una macchina perché potrebbe non avere un'applicazione specifica e rientra così nella categoria di quasi-macchina; invece, una gru che deve essere installata in un autocarro costituisce una macchina.

- **Attrezzature intercambiabili,** *dispositivo che, dopo la messa in servizio di una macchina o di un trattore, è assemblato alla macchina o al trattore dall'operatore stesso al fine di modificarne la funzione o apportare una nuova funzione nella misura in cui tale attrezzatura non è un utensile.*
  Si assembla quindi ad una macchina già messa in servizio al fine di modificarne una funzione esistente o apportare una nuova funzione. Quindi una macchina non è vincolata ad un singolo funzionamento specifico, ma possono essere modificate o integrate le funzioni per le quali è stata immessa nel mercato. Il fabbricante di tali attrezzature deve specificare nel manuale d'uso in quali macchine si possono assemblare, tenendo conto delle

caratteristiche della macchina stessa. Un esempio sono dei prolungamenti delle forche di un carrello elevatore, in cui il fabbricante ne indica i limiti, lasciando la possibilità all'utilizzatore di applicare altre forche non in dotazione senza effettuare una nuova valutazione complessiva secondo la Direttiva Macchine, purché rientrino nei limiti indicati dal fabbricante.

- **Componenti di sicurezza,** *un componente destinato ad eseguire una funzione di sicurezza, il cui guasto e/o malfunzionamento mette a repentaglio la sicurezza delle persone.*
  Comprendono elementi come i funghi di arresto, le barriere ottiche, i PLC di sicurezza.

- **Accessori di sollevamento,** *componenti e attrezzature non collegate alle macchine per il sollevamento, che consentono la presa del carico, disposti tra la macchina e il carico, o sul carico stesso, oppure destinati a divenire parte integrante del carico e ad essere immessi sul mercato separatamente.*
  Ne fanno parte le imbracature e le loro componenti.

- **Catene, funi e cinghie,** *progettate e costruite ai fini di sollevamento come parte integrante di macchine per il sollevamento o di accessori di sollevamento.*

- **Dispositivi amovibili di trasmissione meccanica,** *componenti amovibili destinati alla trasmissione di potenza tra una macchina semovente o un trattore e una macchina azionata, mediante collegamento al primo supporto fisso di quest'ultima.*
  In agricoltura è molto impiegato l'albero telescopico con due giunti cardanici alle estremità.

- **Quasi-macchine,** *insiemi che costituiscono quasi una macchina, ma che, da soli, non sono in grado di garantire un'applicazione ben determinata. Sono unicamente destinate ad essere incorporate o assemblate ad altre macchine o ad altre quasi-macchine o apparecchi per costituire una macchina disciplinata dalla direttiva.*
  Rientrano, ad esempio, i sistemi di azionamento.

2.1.2 Campi di esclusione

Rispetto a quella precedente, la Direttiva Macchine 98/37/CE, è stata fatta una maggior chiarezza riguardo il confine tra la Direttiva Macchine e la Direttiva Bassa Tensione. Secondo l'edizione precedente, la scelta di applicare la Direttiva Macchine, piuttosto che la LVD, ricadeva sulla valutazione del rischio prevalente, ovvero quello più gravoso. In quella attuale invece, rientrano tutte quelle macchine elettriche la cui tensione di alimentazione non è compresa in un intervallo di tensioni ben preciso. Tenendo conto che la Direttiva Bassa Tensione comprende delle tensioni di alimentazione comprese tra i 50V e 1000V in tensione alternata, e i 75V e i 1500V in tensione continua, ciò significa che un motore elettrico alimentato con tensione nominale pari a 12V (sia alternata che continua) rientra nella Direttiva Macchine, mentre un motore elettrico alimentato a 230V rientra nella Direttiva Bassa Tensione. È quindi necessario un approccio diverso a seconda del valore di alimentazione.

Oltre a questa differenziazione, ci sono anche delle categorie di prodotti che non rientrano in questa direttiva, anche se apparentemente sembrano rientrare nelle categorie del precedente paragrafo.

- **Componenti di sicurezza destinati ad essere impiegati come pezzi di ricambio,** sono componenti da utilizzare in sostituzione a quelli forniti dal fabbricante della macchina originaria;
- **Macchine per parchi giochi e divertimento;**
- **Macchine per usi nucleari,** che in caso di guasto possono provocare radioattività;
- **Armi,** incluse quelle da fuoco, e **macchine per uso militare;**
- **Macchine che rientrano in altre direttive,** come i trattori ad uso agricolo o forestale, automobili, o veicoli a due o tre ruote, veicoli da competizione, mezzi di trasporto per via aerea, ferroviaria o navigabile;
- **Macchine per uso di ricerca ed utilizzabili per periodi temporanei.**

Figura 2.1 Le macchine che sono installate in queste categorie di esclusione, invece, sono comprese nella Direttiva Macchine, ad esempio, le piattaforme elevatrici installate in un autocarro.

2.2 I Requisiti Essenziali di Salute e Sicurezza

Il contenuto principale della Direttiva è rappresentato dall'allegato 1, in cui è previsto un elenco dei Requisiti Essenziali di Sicurezza e di tutela della Salute (RESS).
Prima di poter procedere con la progettazione e costruzione della macchina, è necessario eseguire una valutazione dei rischi in modo tale da poter definire a quali RESS debba sottostare la macchina. Gli obblighi previsti dai RESS si applicano quindi solo se esiste il pericolo corrispondente per la macchina in questione rispetto al suo uso previsto o uso improprio ma facilmente prevedibile; significa che solo alcune parti dell'allegato 1 saranno prese in considerazione, tuttavia, alcune sono da applicare in ogni caso:

- **Principio d'integrazione della sicurezza nelle fasi di progettazione e costruzione,** secondo il quale le misure adottate per l'eliminazione di ogni rischio devono persistere durante l'intera esistenza della macchina, quindi nelle fasi di trasporto, montaggio, funzionamento previsto o uso scorretto e prevedibile, manutenzione e messa fuori servizio. Deve essere provvista di tutte le attrezzature ed accessori essenziali per poterla regolare ed utilizzarla in condizioni di sicurezza

- **Soluzioni opportune per la riduzione o eliminazione dei rischi,** il fabbricante o mandatario devono applicare dei principi secondo un ordine preciso:

    1. Eliminazione o riduzione dei rischi nella misura più ampia possibile secondo il principio di integrazione della sicurezza, nelle fasi di progettazione e costruzione;
    2. Adottare delle misure di protezione necessarie nei confronti dei rischi che non possono essere eliminati;
    3. Informare gli utilizzatori dei rischi residui dovuti all'incompleta efficacia delle misure di protezione adottate, attraverso delle segnalazioni, e specificando se è richiesta una formazione particolare dell'operatore e sono previsti dei dispositivi di protezione individuale.

- **Marcatura delle macchine,** devono essere previste delle indicazioni in modo visibile, leggibile e indelebile, tra cui la marcatura CE, l'anno di costruzione, ragione sociale ed indirizzo del fabbricante o del mandatario, ed eventualmente marcatura apposita per l'utilizzo in atmosfera esplosiva;

- **Istruzioni d'uso,** documento che deve accompagnare la macchina, scritte nella lingua ufficiale dello Stato membro in cui la macchina è immessa sul mercato. Sono previste anche delle regole di redazione e un elenco delle informazioni che devono essere contenute nelle istruzioni.

2.3 Conformità della macchina

Prima di immettere nel mercato o di mettere in servizio la macchina, il fabbricante o il mandatario devono adempiere a degli obblighi:

- Accertare che soddisfi i RESS pertinenti dell'allegato 1;
- Accertare che il fascicolo tecnico sia disponibile;
- Fornire le informazioni necessarie, in particolare le istruzioni;
- Eseguire le appropriate procedure di valutazione della conformità;
- Redigere la dichiarazione di conformità ed apporre la marcatura CE.

2.3.1 Documentazione

Prima di redigere la dichiarazione di conformità, è necessario che fabbricante o mandatario, costituiscano il fascicolo tecnico, che deve dimostrare la conformità della macchina ai requisiti della presente Direttiva, attraverso le informazioni inerenti la progettazione, fabbricazione e funzionamento della macchina. Nella pratica deve contenere tutti i dati utili sulle azioni messe in opera dal fabbricante per ottenere la conformità richiesta, questo avviene tramite:

- Una descrizione generale della macchina;
- Schemi e descrizione dei circuiti di comando, per comprendere il funzionamento della macchina;
- Disegni dettagliati, accompagnati da note di calcolo, misurazioni e risultati di prove;
- Documentazione relativa alla valutazione dei rischi;
- Norme e specifiche tecniche adottate per indicare i RESS coperti;
- Manuale di istruzioni della macchina.

Il fascicolo tecnico deve essere messo a disposizione delle autorità competenti degli Stati membri per almeno dieci anni dalla data di fabbricazione della macchina dell'ultima unità prodotta. Tuttavia, non è indispensabile che tutta la documentazione sia materialmente disponibile, è necessario che sia disponibile su richiesta e in tempi adeguati.

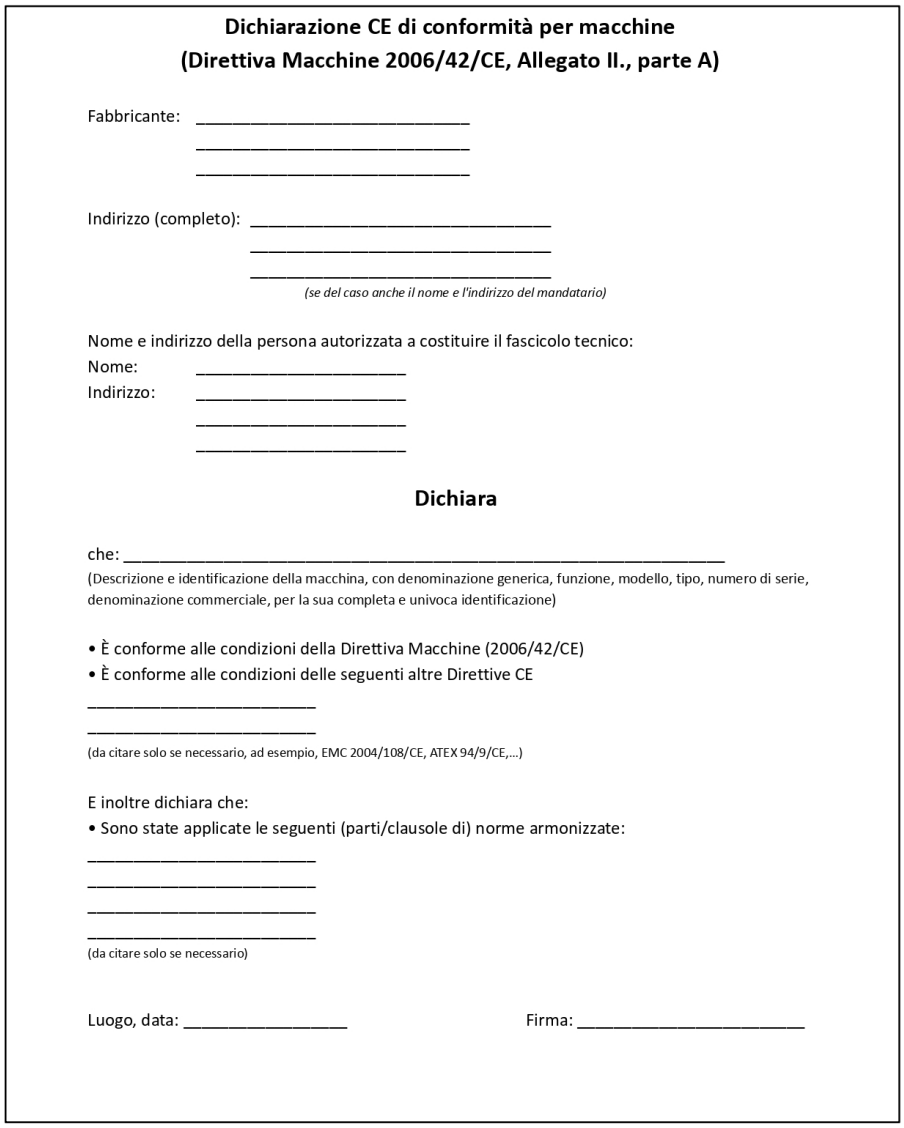
L'intera responsabilità di attestare la conformità delle macchine ricade sui fabbricanti o su chi le immette nel mercato, applicando una delle seguenti procedure:

- **Controllo interno della produzione;**
- **Esame CE del tipo,** dove un ente notificato verifica un modello rappresentativo della macchina attraverso controlli, misurazioni e prove;
- **Garanzia di qualità totale,** dove un ente notificato attesta il soddisfacimento di alcuni obiettivi, quali l'organizzazione della produzione, della progettazione, i controlli sul prodotto che saranno eseguiti durante e dopo la fabbricazione.

La dichiarazione di conformità riguarda la macchina nello stato in cui è stata immessa nel mercato, escludendo quindi componenti aggiuntivi. Inoltre, deve essere redatta secondo delle disposizioni descritte nella Direttiva stessa, ovvero stilata utilizzando la lingua ufficiale del Paese di utilizzo oppure deve essere fornita la traduzione in una o più lingue ufficiali della Comunità.

Il contenuto della dichiarazione deve riguardare:

- Ragione sociale e indirizzo completo del fabbricante o, in caso, del mandatario;
- Nome e indirizzo della persona autorizzata a costituire il fascicolo tecnico;
- Descrizione e identificazione della macchina, attraverso modello, numero di serie, funzione;
- Indicazione con la quale si dichiara che la macchina è conforme a tutte le disposizioni della Direttiva, ed eventualmente una dichiarazione di conformità ad altre direttive comunitarie;
- Riferimento alle norme armonizzate che sono state applicate;
- Eventuale nome, indirizzo e numero di identificazione dell'ente notificato che ha approvato la conformità.



Dichiarazione CE di conformità per macchine
(Direttiva Macchine 2006/42/CE, Allegato II., parte A)

Fabbricante: _____
_____
_____

Indirizzo (completo): _____
_____
_____
(se del caso anche il nome e l'indirizzo del mandatario)

Nome e indirizzo della persona autorizzata a costituire il fascicolo tecnico:
Nome: _____
Indirizzo: _____
_____
_____

Dichiara

che: _____
(Descrizione e identificazione della macchina, con denominazione generica, funzione, modello, tipo, numero di serie, denominazione commerciale, per la sua completa e univoca identificazione)

• È conforme alle condizioni della Direttiva Macchine (2006/42/CE)
• È conforme alle condizioni delle seguenti altre Direttive CE
_____
_____
(da citare solo se necessario, ad esempio, EMC 2004/108/CE, ATEX 94/9/CE,...)

E inoltre dichiara che:
• Sono state applicate le seguenti (parti/clausole di) norme armonizzate:
_____
_____
_____
_____
(da citare solo se necessario)

Luogo, data: _____ Firma: _____

Figura 2.2 Esempio di documento per la dichiarazione di conformità.

La marcatura CE è riconosciuto come l'unico marchio che garantisce la conformità della macchina ai requisiti della presente Direttiva. Deve essere apposta nelle immediate vicinanze del nome del fabbricante o del mandatario, se la verifica di conformità è stata effettuata da un ente notificato, è necessario aggiungere il numero di identificazione. I due elementi del marchio devono avere la stessa dimensione verticale, che non deve essere inferiore ai 5mm, in caso di riduzione o ingrandimento dello stesso, è necessario mantenere le proporzioni del simbolo.

2.4 Norme armonizzate

L'allegato 1 si compone di un gran numero di RESS, di cui i primi sono dei requisiti generali applicabili a molte tipologie di macchine, mentre altri hanno un carattere più specifico per macchine che hanno determinate applicazioni come quelle ad uso sanitario, per la lavorazione del legno o contro dei pericoli precisi come gli incendi o l'utilizzo di sostanze pericolose. Secondo l'articolo 7, al fine di ottenere una presunzione di conformità a determinati RESS e per rendere più agevole ai fabbricanti la prova di conformità, è opportuno disporre di norme armonizzate a livello comunitario per la prevenzione e riduzione dei rischi, le quali si applicano dalla progettazione alla costruzione delle macchine. Dato il numero elevato di requisiti, saranno molte anche le norme armonizzate a tale direttiva. In questa trattazione verranno analizzate le relazioni tra la Direttiva Macchine e due norme.

2.4.1 Legame con la norma ISO 12100

Sicurezza del macchinario — Principi generali di progettazione — Valutazione e riduzione del rischio

Tale norma di tipo A fornisce una panoramica sulla fabbricazione di macchine sicure per il proprio utilizzo previsto, in particolare specifica quelle che sono le metodologie necessarie a raggiungere un livello di sicurezza durante la fase di progettazione di una macchina, specifica i principi di valutazione e riduzione del rischio, al fine di aiutare i progettisti a raggiungere tale obiettivo.

Stando alla Direttiva Macchine, il mandatario o fabbricante deve garantire che sia effettuata una valutazione dei rischi per la macchina che intende immettere nel mercato.
La valutazione dei rischi di una macchina è il processo di analisi mediante il quale vengono individuati i pericoli presenti durante il ciclo di vita di una macchina, vengono poi valutati i rischi che questi possono causare e viene determinato se le misure di sicurezza adottate siano sufficienti a raggiungere un'adeguata riduzione del rischio. Tali misure di protezione riguardano l'identificazione dei Requisiti Essenziali di Sicurezza e di tutela della Salute applicabili sulla macchina e per i quali sarà necessario porre dei provvedimenti. Infatti, non tutti i RESS elencati nell'allegato 1 vanno rispettati, ciò cambia in base all'utilizzo del macchinario e il settore al quale è destinato.

La stima e il processo di riduzione del rischio, secondo tale norma, è un ciclo iterativo:

- **Stabilire i limiti della macchina,** che comprende l'uso previsto e scorretto ma prevedibile della stessa, l'ambiente di utilizzo e le caratteristiche degli operatori, limiti spaziali che comprendono l'intervallo di movimento degli elementi mobili della macchina e lo spazio richiesto per l'interazione con gli operatori, limiti temporali che comprendono il tempo di vita della macchina e gli intervalli di manutenzione della macchina e altri limiti ambientali come la temperatura, l'umidità e il livello di pulizia del luogo di installazione e la proprietà dei materiali che lavora la macchina;

- **Individuare i pericoli** che può dar origine la macchina e le situazioni pericolose che si possono manifestare durante l'intero ciclo di vita, tenendo

in considerazione le operazioni e le azioni da compiere sulla macchina, ma anche pericoli esterni dovuti ad esempio da eventi atmosferici;

- **Stimare i rischi** tenendo conto della gravità dell'eventuale lesione o danno alla salute e probabilità che si verifichi;
- **Valutare i rischi** al fine di stabilire se sia richiesta una riduzione del rischio conformemente all'obiettivo di tale Direttiva;
- **Eliminare o ridurre i rischi** attraverso l'applicazione di soluzioni precise di prevenzione e protezione elencate nei RESS della Direttiva Macchine, nelle relative norme armonizzate e secondo il principio d'integrazione della sicurezza

2.4.2 Legame con la Norma EN IEC 62061

Sicurezza del macchinario - sicurezza funzionale dei sistemi di comando e controllo relativi alla sicurezza

Questa norma garantisce la presunzione di conformità al RESS relativo ai sistemi di comando e controllo:

1.2.1 sicurezza ed affidabilità dei sistemi di comando

I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose.
In ogni caso essi devono essere progettati e costruiti in modo tale che:

- *Resistano alle previste sollecitazioni di servizio e agli influssi esterni;*
- *Un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose;*
- *Errori nella logica del sistema di comando non creino situazioni pericolose;*
- *Errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose.*

Particolare attenzione richiede quanto segue:

- *La macchina non deve avviarsi in modo inatteso;*
- *I parametri della macchina non devono cambiare in modo incontrollato, quando tale cambiamento può portare a situazioni pericolose;*
- *Non deve essere impedito l'arresto della macchina, se l'ordine di arresto è già stato dato;*
- *Nessun elemento mobile della macchina o pezzo trattenuto dalla macchina deve cadere o essere espulso;*

- *L'arresto manuale o automatico degli elementi mobili di qualsiasi tipo non deve essere impedito;*
- *I dispositivi di protezione devono rimanere pienamente efficaci o dare un comando di arresto;*
- *Le parti del sistema di controllo legate alla sicurezza si devono applicare in modo coerente all'interezza di un insieme di macchine e/o quasi macchine.*

In caso di comando senza cavo deve essere attivato un arresto automatico quando non si ricevono segnali di comando corretti, anche quando si interrompe la comunicazione.

Nella pratica, si valuta, in caso di rottura o avarie di un sistema di comando, il rischio che ne consegue e si prendono provvedimenti sulla base della sua entità.

Figura 2.3 Riguarda quindi tutto ciò che comprende l'interfaccia uomo-macchina e il rapporto tra output e input. Questi ultimi possono anche non essere generati dall'operatore stesso, si può trattare anche di segnali impliciti alla macchina, come un finecorsa che, se premuto, genera un input.

Capitolo 3

La norma EN IEC 62061: 2021-07

Sicurezza del macchinario - sicurezza funzionale dei sistemi di comando e controllo relativi alla sicurezza

3.1 Introduzione alla norma

Negli ultimi anni l'automazione e il progresso tecnologico hanno conosciuto un impulso notevole. Il risultato di tali sistemi, a fronte di un aumento della produzione, è stata una riduzione del lavoro dell'operatore e dei suoi sforzi. I sistemi di controllo delle macchine svolgono quindi un ruolo cruciale e diventa indispensabile affidare una grande importanza agli aspetti legati alla sicurezza di persone, ambiente o dell'infrastruttura stessa. I rischi associati al funzionamento dei sistemi di controllo e al funzionamento della macchina, devono essere ridotti attraverso il raggiungimento di un livello di sicurezza complessivo accettabile, come risultato della valutazione del rischio secondo la norma ISO 12100.

La norma fondamentale impiegata in questo ambito è lo standard internazionale IEC 61508 che disciplina l'intero ciclo di vita dei sistemi elettrici, elettronici ed elettronici programmabili relativi alla sicurezza, nelle fasi di progettazione, utilizzo e manutenzione.
È una norma non armonizzata con la Direttiva Macchine, ma il cui scopo è quello di fornire informazioni necessarie per una migliore comprensione delle norme che si applicano a tutti i settori industriali, vuole essere quindi un'introduzione alla sicurezza funzionale e una guida nell'applicazione degli standard specifici.
È usata quindi come base per lo sviluppo delle seguenti norme di prodotto relative ai sistemi elettrici, elettronici ed elettronici programmabili relativi alla sicurezza:

- EN 50129 relativa al settore ferroviario.
- EN 50156 impiegata per forni e caldaie che usano combustibili solidi, liquidi e gassosi.
- IEC 61511 per le industrie di processo quali raffinerie, impianti chimici, farmaceutici.
- IEC 60601 relativa alla sicurezza delle apparecchiature medicali
- DO 178 in ambito aerospaziale
- ISO 26262 riguarda i veicoli stradali
- IEC 61513 per il settore nucleare
- IEC 62061 applicabile nelle macchine

La norma IEC 62061 è l'oggetto principale di questo capitolo, tale standard è stato redatto prima a livello internazionale dall'ente IEC a partire dal 2016, e poi pubblicata nel 2021.
In ambito europeo, è stata recepita e approvata dal CENELEC, pubblicata successivamente nella Gazzetta Ufficiale dell'Unione nell'aprile del 2022, come norma armonizzata alla Direttiva Macchine, con la dicitura EN IEC 62061, che presenta gli stessi contenuti dello standard internazionale.

Seguendo l'ordine temporale, la prima edizione di tale norma è stata emanata nel 2005. Quella attuale la sostituisce completamente, ci sono comunque delle date precise che stabiliscono questo passaggio:

1. La prima edizione rimane applicabile fino al 26 aprile 2024.

2. L'edizione del 2021 doveva essere recepita a livello nazionale entro il 26 gennaio 2022, attraverso una pubblicazione di una norma nazionale o mediante approvazione di un ente. In Italia l'ente preposto è stato il CEI, che dovrà pubblicare quindi la versione italiana che avrà la stessa validità e gli stessi contenuti della pubblicazione IEC.

3.2 Applicazioni della Norma

Tale norma è rivolta ai progettisti di macchine e a chi è coinvolto nella convalida della stessa, al fine di stabilire un approccio di costruzione e dei requisiti necessari per raggiungere delle specifiche prestazionali di sicurezza richieste. Formula delle raccomandazioni per la progettazione, integrazione e validazione dei sistemi di controllo con funzione di sicurezza per le macchine che non sono trasportabili a mano durante il lavoro.

Con sistema di controllo si intende un sistema che risponde a dei segnali di input, che derivano dalla macchina stessa e/o da un operatore, generando dei segnali di output che garantiscono alla macchina di operare nel modo desiderato.

Da questa definizione del tutto generale, si analizzano ora quelli che sono i sistemi di comando e controllo con funzione di sicurezza, ovvero che

sono in grado di implementare una funzione di sicurezza, allo scopo di mantenere le condizioni di sicurezza della macchina o impedire un aumento immediato del rischio in relazione ad uno specifico evento pericoloso. All'atto pratico devono garantire un corretto e sicuro funzionamento sia durante il normale uso, che in condizioni di guasto.

Tali sistemi devono essere quindi progettati e realizzati per rilevare le condizioni di pericolo e riportare la macchina ad uno stato di funzionamento sicuro. Vengono definiti anche come Safety-related Control System (SCS).

Ci sono molte situazioni sulle macchine in cui i sistemi di controllo sono impiegati come parte integrante delle misure di sicurezza. Degli esempi tipici possono essere:

microswitch o finecorsa di sicurezza, sono installati su dispositivi di protezione mobili, la loro funzionalità è quella di evitare l'esecuzione di azioni pericolose dopo l'apertura del riparo stesso. Rispetto ai finecorsa funzionali, impiegati per rilevare la posizione e che potrebbero rompersi più facilmente, quelli di sicurezza hanno una struttura hardware più robusta in modo tale da diminuire le probabilità di guasto ed avere un'affidabilità maggiore. Essendo quindi certificato come componente di sicurezza rientra nella Direttiva Macchine.

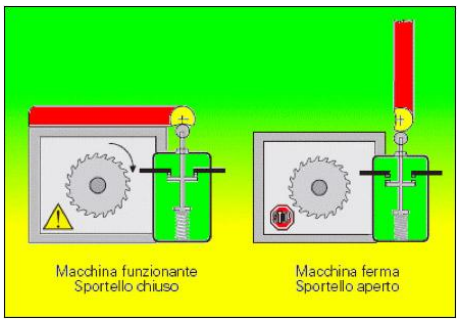


Figura 3.1 Esempio di funzionamento, all'apertura dello sportello, l'elemento mobile della macchina si arresta.

Figura 3.2 È usuale impiegare delle colorazioni vive per indicare gli SCS, come il rosso o il giallo.

Fungo di arresto rapido che se premuto consente di evitare o ridurre pericoli persistenti alle persone o danni al macchinario.

Un esempio ottimale di gestione degli eventuali pericoli in conseguenza ad un danneggiamento riguarda il fungo di arresto rapido. In questo caso, lo si installa con la caratteristica di normalmente chiuso, in modo che, se premuto, porti la macchina in una situazione di sicurezza. Valutando alcune situazioni di guasto che si possono verificare, come l'ossidazione dei contatti o il fatto che si possa strappare un filo, questo non deve comportare delle situazioni di pericolo. Dal momento che lo stato di sicurezza è presente quando si apre il fungo, in caso di sua rottura, esso risulta un contatto aperto e il circuito della macchina disalimentato, ponendola quindi nello stato di arresto di emergenza. In questo caso

quindi, l'evento di rottura o avaria di un sistema di comando, pone la macchina nella condizione di sicurezza.

Figura 3.3 Nel pannello di controllo di una macchina, risalta il fungo di arresto rapido, che, secondo la norma EN 60204: 2018 relativa all'equipaggiamento elettrico delle macchine, deve essere rosso su sfondo giallo per essere ben individuabile

3.3 passi necessari a costituire un SCS

Questo documento fornisce i punti necessari per realizzare correttamente tali sistemi e le relative funzioni di sicurezza:

- Analisi dei pericoli e valutazione dei rischi, il progettista considera se emergono dei rischi, anche nel caso di guasto del sistema e individua un grado di affidabilità per quella funzione;
- Riduzione del rischio mediante mezzi di comando;
- Individuazione delle funzioni di sicurezza per le parti del sistema di comando legate alla sicurezza;
- Progettazione, sia hardware che software, questo avviene in più fasi
    1. Determinazione del livello di affidabilità (SIL)
    2. Specifiche dei requisiti funzionali della funzione di sicurezza
    3. Fase di progettazione e realizzazione del sistema di sicurezza
    4. Determinazione del SIL raggiunto da ogni parte della funzione di sicurezza
    5. Verifica che il SIL raggiunto sia coerente con quanto richiesto, altrimenti è necessario ritornare alla fase di progettazione.
- Convalida, mediante prove ed analisi, se i risultati sono coerenti con i livelli di sicurezza ed affidabilità attesi, il processo è ultimato, altrimenti, sarà necessario eseguire un'ulteriore progettazione.

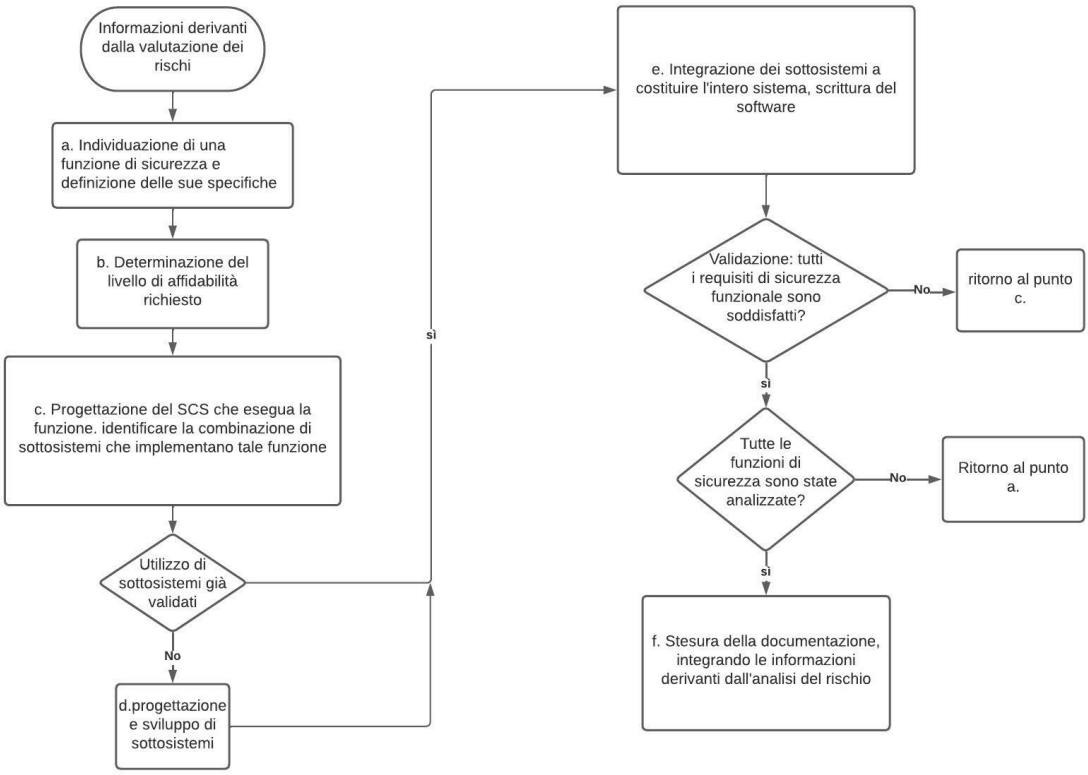


Figura 3.4 Il tutto viene riassunto attraverso un flow chart

3.4 Le funzioni di sicurezza

Si analizza il processo che porta alla definizione delle funzioni di sicurezza,
è una funzione della macchina o di un dispositivo che ha il compito di proteggere una parte di essi e che, guastandosi, può provocare un incremento immediato del rischio.
Occorre tenere conto di queste funzioni per perseguire l'obiettivo di eliminare/ridurre il più possibile il rischio che si verifichino situazioni potenzialmente dannose per l'operatore.

3.4.1 Analisi e riduzione del rischio

Il tutto comincia con una valutazione del rischio secondo la norma ISO 12100, questo è legato ad una relazione tra la gravità del possibile danno e la probabilità che si verifichi l'evento pericoloso, quest'ultimo parametro è funzione di tre aspetti:

1. Frequenza e durata di esposizione dell'operatore al rischio;
2. Probabilità di accadimento di un evento pericoloso;

3. Possibilità che si eviti o limiti il danno.

Attraverso dei metodi standard di valutazione del rischio come l'uso di una matrice, si può ottenere una sua stima pari al prodotto degli indici numerici attribuiti alla gravità del danno e alla probabilità di accadimento, lo scopo principale della misura applicata è quello di ridurre questi due aspetti. A partire da questa stima, si considera se una misura di riduzione è necessaria e, se del caso, come effettuarla.

1. **Progettazione,** già in questa fase si possono eliminare dei pericoli senza utilizzare delle funzioni di sicurezza, questo avviene attraverso una scelta adeguata delle caratteristiche costruttive e di design della macchina. Ad esempio, si può pensare di coprire un elemento in movimento come delle pulegge o degli ingranaggi attraverso dei carter.
2. **Protezione,** se invece la riduzione del rischio avviene attraverso dei sistemi di controllo, allora risulta necessario individuare le funzioni di sicurezza richieste. Stando all'esempio precedente, se è indispensabile accedere all'area in cui sono presenti le pulegge o gli ingranaggi, allora si installa un riparo mobile con un finecorsa di sicurezza la cui funzione è quella di togliere l'alimentazione alla macchina nel momento in cui il riparo è aperto.
3. **Informazione,** ovvero la gestione del rischio residuo, se il pericolo non viene gestito attraverso i due punti precedenti e quindi persiste, allora si deve provvedere ad informare correttamente gli operatori attraverso delle segnalazioni. Questa fase però non è molto contemplata in quanto si cerca di sviluppare le prime due fasi che garantiscono delle protezioni più efficaci.

3.4.2 Gestione delle funzioni di sicurezza
Il piano di sicurezza funzionale

Per poter ottenere le funzioni di sicurezza richieste per una data implementazione da parte di un sistema di controllo, è necessario che ogni SCS che viene progettato sia accompagnato da un piano di sicurezza funzionale.
Lo scopo principale è quello di fornire misure per prevenire errori di implementazione, deve quindi contenere le attività da svolgere per la costituzione di un SCS, dalla determinazione delle funzioni di sicurezza sino alla validazione del componente. Inoltre deve:

- Descrivere le strategie adottate per soddisfare i requisiti di sicurezza richiesti;
- Descrivere le strategie per ottenere la sicurezza funzionale nel caso di un software applicativo, con i risultati provenienti dallo sviluppo, verifica e validazione dello stesso;
- Identificare i soggetti preposti a svolgere le attività di costituzione di un SCS sulla base di parametri come l'esperienza pregressa, qualifica, conoscenza del settore applicativo e della tecnologia adottata, conoscenza del quadro giuridico e normativo di sicurezza;

- Stabilire le procedure necessarie a documentare e conservare le informazioni rilevanti delle funzioni di sicurezza. Queste informazioni contengono i risultati provenienti dall'identificazione del pericolo e valutazione del rischio, le procedure impiegate per ottenere e mantenere la sicurezza funzionale, comprese le eventuali modifiche che si possono operare in un SCS.

- Descrivere la strategia di gestione della configurazione, quindi tutte le attività che portano alla definizione della struttura finale di un SCS (integrazione di sottosistemi, definizione delle funzioni di sicurezza);

- Descrivere le operazioni da effettuare in caso di modifiche al componente o alla macchina;

- Stabilire un piano di verifica del componente, che deve includere una descrizione dettagliata riguardo le unità (addetti o enti) che devono eseguire la verifica, le tecniche e le apparecchiature impiegate, le attività svolte, i criteri di accettazione e i mezzi impiegati per valutare i risultati della verifica;

- Stabilire un piano di validazione che comprenda i risultati dalla prova di verifica, modalità di funzionamento della macchina e ambientazione di lavoro, requisiti e criteri rispetto ai quali deve essere convalidato il dispositivo, la strategia tecnica adottata per la validazione (test, analisi), azioni da intraprendere in caso di mancato rispetto dei criteri di accettazione;

3.4.3 Eventuali modifiche

È possibile che sia necessario implementare una modifica nell'SCS sia nella fase di progettazione della macchina, oppure anche quando la macchina è già stata immessa nel mercato, la richiesta di modifica si può manifestare quando:

- La specifica dei requisiti di sicurezza è cambiata;

- Obsolescenza del sistema;

- Modifiche da apportare alla macchina o ai suoi modi di funzionamento;

- Guasti, che portano ad una revisione dell'intero apparato di sicurezza.

Eventuali tarature o regolazione sugli stessi SCS che sono espresse nel proprio manuale di istruzioni, non sono considerate come modifiche.
Qualora venga implementata una modifica, il suo impatto in termini di effetti sulla sicurezza funzionale deve essere documentato. Questo comporta una appropriata fase di riprogettazione dell'hardware e/o del software e tutti i documenti redatti precedentemente, devono essere rivisti, opportunamente modificati e ripubblicati.

3.4.4 Specifiche di una funzione di sicurezza

Per ogni funzione di sicurezza di un SCS sono necessarie delle informazioni, in modo tale da poter agevolare la successiva fase di progettazione. Tuttavia, non tutte le informazioni saranno complete o del tutto disponibili prima della fase di progettazione, per cui questi aspetti potrebbero anche essere chiariti durante la fase stessa.
Queste caratteristiche si ricavano da un'analisi che in prima battuta ha carattere del tutto generale, per poi focalizzarsi sulla singola azione di sicurezza.
Si parte infatti dai risultati della valutazione del rischio e le funzioni di sicurezza individuate durante la fase di riduzione del rischio. Dopodiché si analizzano le caratteristiche della macchina come, ad esempio, le modalità di funzionamento, il tempo di ciclo, le condizioni dell'ambiente di installazione, il tipo e la durata dell'interazione con gli operatori (attività come manutenzione, regolazione, pulizia).
Infine si prendono in considerazione tutte le informazioni fondamentali che posso avere un'influenza sulla progettazione di un SCS che comprendono una descrizione dell'evento pericoloso che la funzione di sicurezza deve evitare, il comportamento richiesto dall'SCS a fronte di un proprio guasto ed infine tutte le relazioni tra le varie funzioni di sicurezza e con qualsiasi altra funzione. Le informazioni relative ad una funzione di sicurezza devono sicuramente comprendere:

1. **Specifica dei requisiti funzionali di sicurezza,** che riguarda una descrizione dettagliata della funzione. Comprende le condizioni della macchina nelle quali le funzioni di sicurezza risultano attive o disattivate, la priorità delle funzioni qualora si verificasse una contemporaneità nell'attivazione, la frequenza con la quale sono richieste le funzioni e il rispettivo tempo di risposta, una descrizione delle reazioni ad eventuali guasti.

2. **Integrità della funzione di sicurezza,** il parametro impiegato per esprimere il livello di affidabilità di una funzione di sicurezza è il SIL (Safety Integration Level). Esprime la capacità di eseguire le funzioni di sicurezza attraverso un indice numerico che va da 1 a 3. Il suo valore è strettamente legato alla valutazione del rischio e al parametro PFH, che rappresenta la probabilità al guasto per ora, con la conseguenza che non sia in grado di fornire la funzione di sicurezza richiesta.

Capitolo 4

Progettazione di un SCS

L'affidabilità è quindi in relazione con i guasti sistematici ovvero quelli prevedibili o comunque legati al tipo di applicazione della macchina, per i quali è possibile individuare una precisa origine.
I guasti sistematici più diffusi sono dovuti all'errore umano nella fase di progettazione, produzione, installazione o a causa di un uso errato della macchina. Tenendo conto di tutti questi aspetti, risulta necessario applicare delle misure in fase di progettazione:

- Ogni SCS deve essere progettato e implementato secondo il piano di sicurezza funzionale;
- Prestare molta attenzione nell'installazione dei componenti che costituiscono un sistema di sicurezza, soprattutto, da un punto di vista elettrico, nei cablaggi e nelle interconnessioni;
- Documentare, sulla base delle tecnologie adottate, il corretto utilizzo del SCS; devono essere tenuti comunque conto di eventuali usi impropri e modifiche;
- Corretta installazione e protezione in conformità alla norma IEC 60204 che fa riferimento all'equipaggiamento elettrico delle macchine, includendo quindi il rilevamento dei guasti verso terra;
- Ogni SCS deve essere progettato in modo che in caso di interruzione dell'alimentazione, venga mantenuto uno stato di sicurezza della macchina. Ad esempio, un'interruzione dell'alimentazione di un motore non deve causare un avvio imprevisto al ripristino della tensione che interessa il circuito. Molto semplicemente si può prevedere l'esecuzione del comando marcia/arresto del motore impiegando l'autoritenuta, oppure l'aggiunta di un pulsante di consenso.
- Impiegare delle misure per controllare gli effetti derivanti da qualsiasi comunicazione dati, questo riguarda soprattutto l'ambiente software e i comandi senza cavi. Le misure sono ad esempio l'utilizzo di ritrasmissioni, handshake, acknowledgement, arresto automatico della macchina quando si interrompe la comunicazione o per interferenze da elementi esterni;
- I sistemi di sicurezza che comportano anche una parte elettrica o elettronica, non devono essere influenzati da disturbi di tipo elettromagnetico. Un'analisi completa del rischio deve comprendere gli eventuali effetti di tali disturbi in modo tale da ottenere comunque un rischio accettabile. Questo viene comunque trattato nella norma IEC 61000 relativo alla compatibilità elettromagnetica.

4.1 L'affidabilità dei sistemi di comando e i parametri impiegati

L'affidabilità di un sistema si ricava su base statistica data da risultati di test oppure in base a calcoli da simulazioni, in linea generale i componenti di sicurezza devono avere un numero di guasti inferiore rispetto ai componenti ordinari, ovvero avere un'affidabilità maggiore.

4.1.1 Il tasso di guasto λ

La probabilità di un sistema a non guastarsi durante il suo funzionamento è misurata dal tasso di guasto, è rappresentato come il numero di guasti in un periodo di tempo fissato.
Il calcolo di questo parametro avviene mediante prove su **N** componenti, in cui si rilevano, per un dato intervallo di tempo **h**, gli **n** componenti che si guastano.

$$\lambda = \frac{n}{h}$$

Quello che si ottiene è un valore costante, utile per effettuare dei calcoli ed intraprendere delle scelte riguardo l'utilizzo del componente piuttosto che un altro in un'implementazione. Rappresenta solamente un'indicazione di massima sul comportamento dei dispositivi.
In realtà per ogni elemento preso in considerazione, tale tasso non assume una distribuzione lineare o costante, perché potrebbe cambiare, per uno stesso componente, sulla base del tipo di applicazione, le condizioni di esercizio e l'usura dello stesso, per cui si assume una distribuzione di tipo parabolico che viene detta "a vasca" in funzione del tempo.

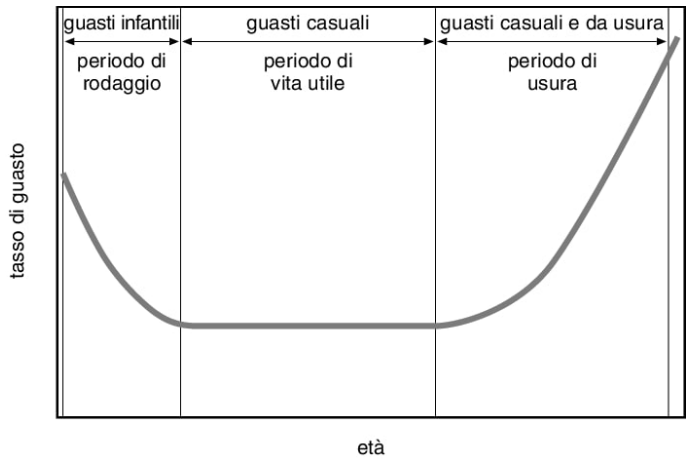


Figura 4.1 Il tasso di guasto si calcola come $\lambda(t) = \frac{n}{N(t)}$,dove N(t) rappresenta il numero di componenti che all'istante t sono effettivamente funzionanti

Si riconoscono 3 periodi fondamentali.

Periodo di rodaggio: con un tasso di guasto elevato, si manifestano i guasti infantili, quelli dovuti a dei piccoli difetti di costruzione non rilevati al momento dell'immissione sul mercato;

Periodo di vita utile: il tasso di guasto rimane costante, i possibili guasti sono di tipo casuale;

Periodo di usura: il tasso di guasto riprende a crescere perché il prodotto è giunto al suo fine vita, si tiene conto dell'usura, del danneggiamento dovuto agli anni di applicazione. I guasti in questo periodo di tempo vengono limitati dalla manutenzione preventiva che consiste nell'analizzare lo stato di salute del sistema attraverso delle verifiche e ispezioni di variabili misurabili ricavate dei sensori, come la temperatura, le vibrazioni.

Per le funzioni di sicurezza, il tasso di guasto da impiegare per ricavare l'affidabilità del sistema è quello relativo al tempo di vita utile, quindi un valore costante.

4.1.2 Il Main Time To Failure MTTF

Rappresenta il tempo medio fra due guasti (Failure). In generale nei componenti non riparabili, dopo il primo guasto si indica come MTTF dato che non possono essere ripristinati, mentre nei componenti riparabili viene rappresentato come MTBF, ossia Main Time Between Failure.

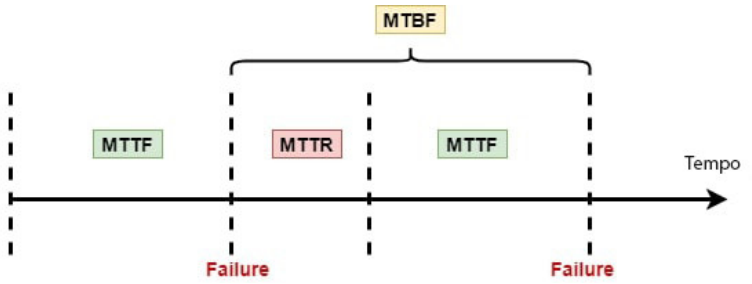


Figura 4.2 Si ricava la relazione tra i due parametri indicati, $MTBF = MTTF + MTTR$ dove MTTR rappresenta il tempo medio di riparazione del componente.

Analizzando invece i componenti destinati alle funzioni di sicurezza, l'indice MTTF appare molto elevato data la loro affidabilità maggiore, quindi, nel complesso, l'indice MTTR appare trascurabile e risulta possibile la coincidenza tra MTTF e MTBF.
Per il calcolo di questo indicatore si ha che $MTTF = \frac{1}{\lambda}$, è quindi l'inverso del tasso di guasto.
Questo ribadisce il fatto che i componenti di sicurezza abbiano un tempo medio tra due guasti molto elevato, dato che λ è un valore molto piccolo.

La determinazione di questo parametro segue un processo gerarchico dipendente dalle informazioni che si hanno a disposizione per ogni dispositivo:

1. Si esprime MTTF in base alle dichiarazioni del costruttore, attraverso le relazioni con gli altri parametri che possono essere indicati;

2. Per ogni categoria di componente (contattori, dispositivi meccanici o idraulici) si affidano dei valori standard derivanti da una tabella;

3. Assumere un valore pari a dieci anni.

4.1.3 Il parametro B_{10}

Per i componenti meccanici, pneumatici ed elettromeccanici, i costruttori forniscono un parametro che indica il numero medio di cicli di lavoro in cui nel 10% dei componenti analizzati si registra un guasto. È un indice fondamentale perchè da questo è possibile calcolare altri parametri:

T_{10}, che indica il tempo medio entro il quale si registra un guasto per il 10% dei componenti testati.

$$T_{10} = \frac{B_{10}}{n_{\text{op}}}$$

dove n_{op} indica il numero di cicli annuali previsti.

MTTF e di conseguenza λ

$$MTTF = \frac{B_{10}}{0.1 n_{\text{op}}}$$

Dei tre parametri appena elencati sono previsti anche i casi di guasti pericolosi per la sicurezza del macchinario. La dichiarazione di pericolosità viene attribuita dalle norme previste per i metodi di prova. Questi possono riguardare i contatti saldati in un contattore, oppure una variazione dei tempi di reazione ad un dato input.

4.1.4 Tolleranza di guasti nell'hardware

Nell'ambito dell'affidabilità hardware di un componente, giocano un ruolo fondamentale i parametri HFT e SFF.

HFT sta per Hardware Fault Tolerance e indica la capacità a svolgere una funzione di sicurezza, anche in presenza di guasti. Il valore che si attribuisce è numerico, e per un indice pari ad N, significa che al N+1 guasto si ha la perdita della funzione di sicurezza. Ad esempio il rilevamento di un guasto pericoloso di un qualsiasi sistema con tolleranza superiore allo zero garantisce comunque l'esecuzione della funzione richiesta.

SFF significa invece Safe Failure Fraction, e indica la percentuale di guasti considerati sicuri, rispetto a tutti i guasti che si possono manifestare (sicuri+pericolosi). La classificazione dei guasti in sicuri o pericolosi dipende dalle sue conseguenze, se pongono il sistema in una situazione pericolosa o meno, dalla progettazione effettuata e dai dati che si hanno a disposizione sul comportamento dei dispositivi a guasto.

4.1.5 Il fattore di copertura e il dispositivo di diagnostica

Per rilevare in tempo reale lo stato dei componenti di sicurezza si impiegano dei dispositivi di controllo basati sul feedback dei componenti. Questi possono essere i contatti ausiliari oppure relè di monitoraggio che esprimono lo stato dei contatti in un interruttore di potenza e sono in grado di rilevare un guasto e di segnalarlo attraverso una lampada, sarà poi l'operatore che porterà la macchina nello stato di emergenza, ad esempio premendo il fungo di arresto rapido. L'evoluzione di questi moduli di controllo sono i PLC di sicurezza che, a differenza dei primi, sono dei dispositivi più costosi e sofisticati, ma in grado di portare la macchina

nello stato di emergenza anche senza interventi di operatori. La bontà della diagnostica è misurata dal fattore di copertura DC, che esprime il rapporto tra la frequenza dei guasti pericolosi rilevata e quelli pericolosi totali.

$$DC = \frac{\sum \lambda_{\mathrm{DD}}}{\sum \lambda_{\mathrm{D}}}$$

In cui il numeratore rappresenta la somma dei guasti pericolosi rilevati, e a denominatore è presente la totalità dei guasti pericolosi.

Tuttavia la norma viene in aiuto al progettista attraverso dei valori tabulati di Diagnostic Coverage sulla base del sistema adottato per controllare l'esecuzione corretta delle funzioni di sicurezza. Ad esempio, con l'impiego di contatti ausiliari, la norma fissa un DC pari al 99%, che è il valore massimo ottenibile.

4.1.6 Causa di guasto comune

Un aspetto fondamentale necessario a garantire un grado di affidabilità notevole è quello della ridondanza, ovvero l'utilizzo di più dispositivi, anche diversi, per svolgere una determinata funzione, disposti in modo tale che il guasto in un elemento, non comprometta la totale funzione di sicurezza. Un esempio applicativo si rileva nei finecorsa di sicurezza da applicare alle barriere di protezione degli elementi mobili di una macchina. Si può prevedere l'impiego di due finecorsa di diversa tipologia, come uno di tipo induttivo e uno elettromeccanico, così a fronte di un bypass o rottura del primo, è comunque garantita la funzione di sicurezza dal secondo.

Nel momento in cui la modalità di installazione a doppio canale non viene impiegata si può incorrere nella causa di guasto comune, accade quando un evento produce il guasto contemporaneo di più elementi.

Per limitare questo evento si deve intervenire in fase di progettazione attraverso delle misure da applicare, che possono riguardare la diversità di tecnologia tra i dispositivi adottati, oppure la separazione tra apparecchi a singolo canale al fine di limitare eventuali problematiche termiche o di sovratensione ad entrambi. Ad ognuna di queste misure, che sono comunque elencate in una tabella viene espresso un contributo numerico. La somma dei vari contributi esprime la percentuale di guasti di modo comune (β) che si potrebbero manifestare rispetto ai guasti totali.

punteggio complessivo	β
≤ 35	10%
da 36 a 65	5%
da 66 a 85	2%
da 86 a 100	1%

Tabella 4.1 La norma IEC 61508 esprime un valore di β uguale o inferiore al 2% per cui è necessario raggiungere un punteggio complessivo maggiore a 65.

4.2 I sottosistemi

Dopo aver individuato il livello di affidabilità richiesto e le specifiche della funzione di sicurezza, si passa alla progettazione del sistema di sicurezza. Questo si compone di più componenti, i sottosistemi appunto, nei quali un loro possibile guasto si manifesta come un guasto pericoloso all'intero sistema che può minare quindi il funzionamento delle funzioni di sicurezza. Da questa suddivisione si evince che anche ogni funzione di sicurezza può essere scomposta in più sottofunzioni.

Figura 4.3 Esempio di una possibile scomposizione di un sistema in più sottosistemi. Un SCS può essere anche composto di un unico sottosistema, ad esempio un sensore che integra al suo interno anche un sistema output, come un relè

Per ogni funzione eseguita da un sottosistema è necessario definire i requisiti di sicurezza (in termini di tasso di guasto e affidabilità) e i segnali di input e output.
Queste informazioni consentono di aiutare il progettista nelle prime fasi di valutazioni nel caso in cui il sottosistema debba essere progettato, ma allo stesso tempo agevola la scelta del componente da integrare con altri a costituire un SCS qualora ce ne siano già nel mercato.

Le misure da adottare per la progettazione di un singolo elemento o per l'integrazione di questo all'interno di un sistema sono le medesime impiegate per un SCS. Si presta quindi attenzione a quanto dichiarato nel piano di sicurezza funzionale, e, in aggiunta, alle indicazioni date dal costruttore per il collegamento di più sottosistemi da un punto di vista hardware (informazioni sulle variabili di interfaccia, compatibilità tra loro e con l'ambiente di utilizzo, schermatura dei conduttori) e software al fine di evitare errori nella comunicazione dati.

Per stimare la capacità di ogni SCS a raggiungere un determinato livello di sicurezza ed affidabilità risulta necessario effettuare un'analisi di ogni sottosistema in modo da poter poi determinare tutti i guasti e la reazione corrispondente.

4.2.1 Le categorie di sicurezza

Il comportamento in condizioni di guasto dei singoli componenti di un SCS consente di individuare quattro categorie, sulla base dell'impiego di dispositivi di monitoraggio delle funzioni di sicurezza e in base al tipo di installazione dei dispositivi, se a singolo o doppio canale:

Categoria A: singolo canale senza un controllo delle funzioni di sicurezza

un guasto in un sottosistema o in un elemento che lo compone, causa un guasto nell'intera funzione di sicurezza. A questa architettura corrisponde ad un HFT pari a 0.

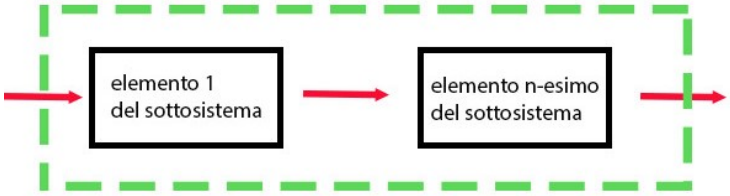


Figura 4.4 Architettura di categoria A.

Categoria B: doppio canale senza un controllo delle funzioni di sicurezza

Il sistema si compone di due o più elementi in ridondanza, il guasto di uno solo tra i componenti, non permette la perdita dell'intera funzione di sicurezza. Se gli elementi impiegati utilizzano la stessa tecnologia di funzionamento, allora solo una causa di guasto comune si traduce come una perdita delle funzioni di sicurezza. Questa architettura ha un HFT uguale a 1.

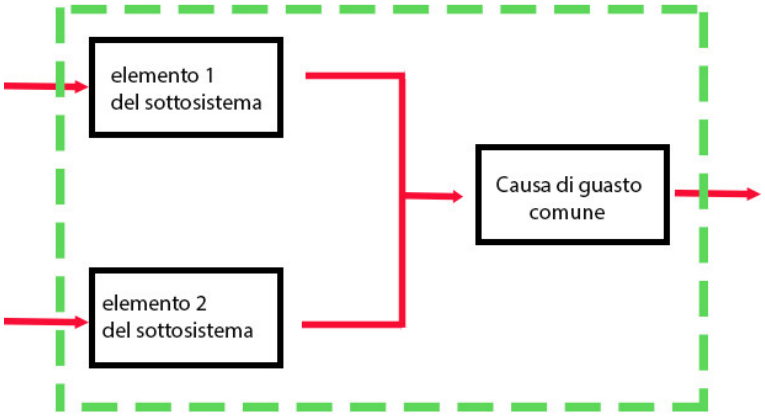


Figura 4.5 Architettura di categoria B.

Categoria C: singolo canale con un controllo delle funzioni di sicurezza

Essendo a singolo canale, un guasto pericoloso di un solo elemento causa un guasto pericoloso a tutta la funzione di sicurezza del sistema, presenta quindi un HFT pari a 0. Allo scopo di contrastare la perdita di un elemento, si inserisce un blocco diagnostico, che nel caso rilevi il guasto, attiva una reazione all'avaria. Questo garantisce un intervento tempestivo ed evita la perdita della funzione di sicurezza.

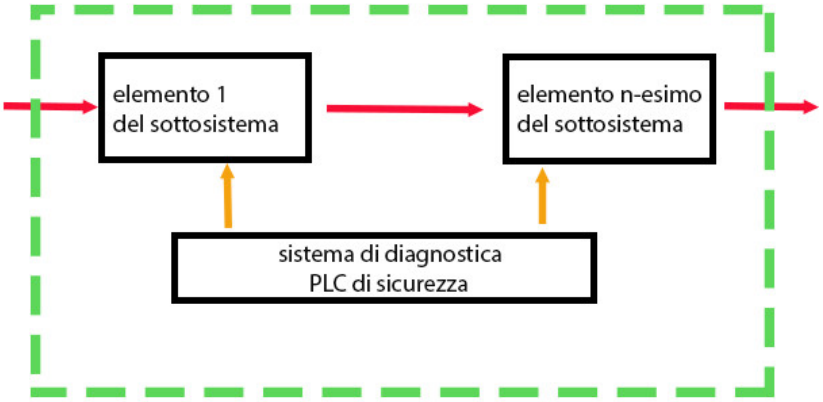


Figura 4.6 Architettura di categoria C.

Categoria D: doppio canale con controllo delle funzioni di sicurezza

È il sistema più completo e quindi il più costoso. In questo caso un guasto in un singolo dispositivo non causa la perdita dell'intera funzione di sicurezza. È inoltre presente un controllore in grado di rilevare i guasti e capace di iniziare il processo di reazione ai guasti. Il tasso HFT corrispondente è pari a 1.

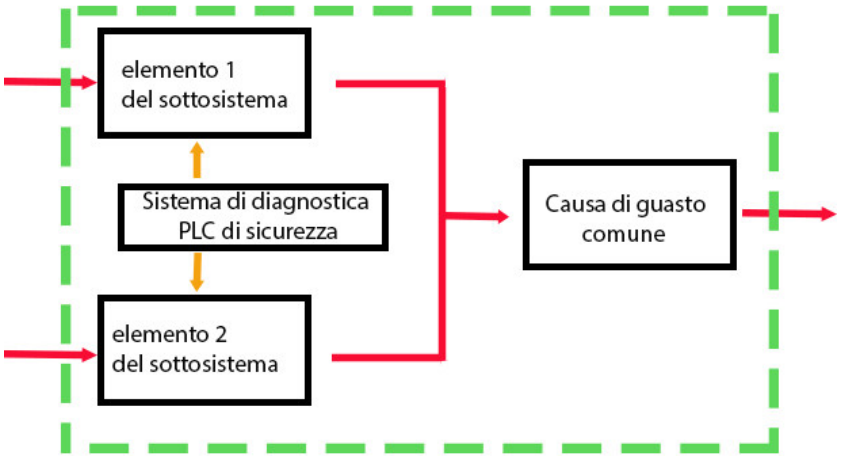


Figura 4.7 Architettura di categoria D.

Capitolo 5

La validazione

La validazione di un SCS comprende analisi, ispezioni e test per verificare che il sistema raggiunga il livello di affidabilità richiesto (SIL_r) e soddisfi le specifiche di sicurezza indicate nella fase di progettazione. Per ottimizzare i tempi di validazione è consigliato eseguirla di pari passo con le varie fasi di costituzione del SCS, in alcuni casi si preferisce eseguire la convalida al termine del processo, direttamente sulla macchina in cui sarà installato il sistema.

Nel momento in cui la validazione non viene superata, risulta necessario ritornare alla fase di progettazione per apportare delle modifiche. In particolare, i guasti sistematici possono essere ridotti già in questa fase, applicando le regole di buona tecnica, ovvero delle misure alle quali il progettista si deve attenere per assicurarsi una certa accettabilità del proprio prodotto in termini di durata, affidabilità e, appunto, sicurezza.
Il processo di verifica è quindi di tipo iterativo e può essere ripetuto più volte, soprattutto se un SCS integra al suo interno più sottosistemi, dal momento che ogni funzione di sicurezza dovrà essere convalidata, in questo caso la validazione si effettua inizialmente mediante analisi e test del singolo componente, per poi analizzare l'intero sistema dato dalle integrazioni tra questi, individuando eventuali incompatibilità e la reazione ai guasti dell'intero sistema.

Il metodo di convalida deve essere coerente con quanto indicato nel piano di validazione che identifica e descrive i requisiti per l'esecuzione della convalida, identifica i mezzi e le prove da impiegare per validare le funzioni di sicurezza specificate, le condizioni operative e ambientali durante le prove, le norme di prova da applicare.

Le informazioni richieste per la convalida varieranno con la tecnologia usata, con l'applicazione degli stessi SCS e del livello di affidabilità richiesto. Al termine della convalida è richiesta la redazione di un documento che indichi per ogni funzione di sicurezza i risultati ottenuti, al fine di convalidare il sistema.

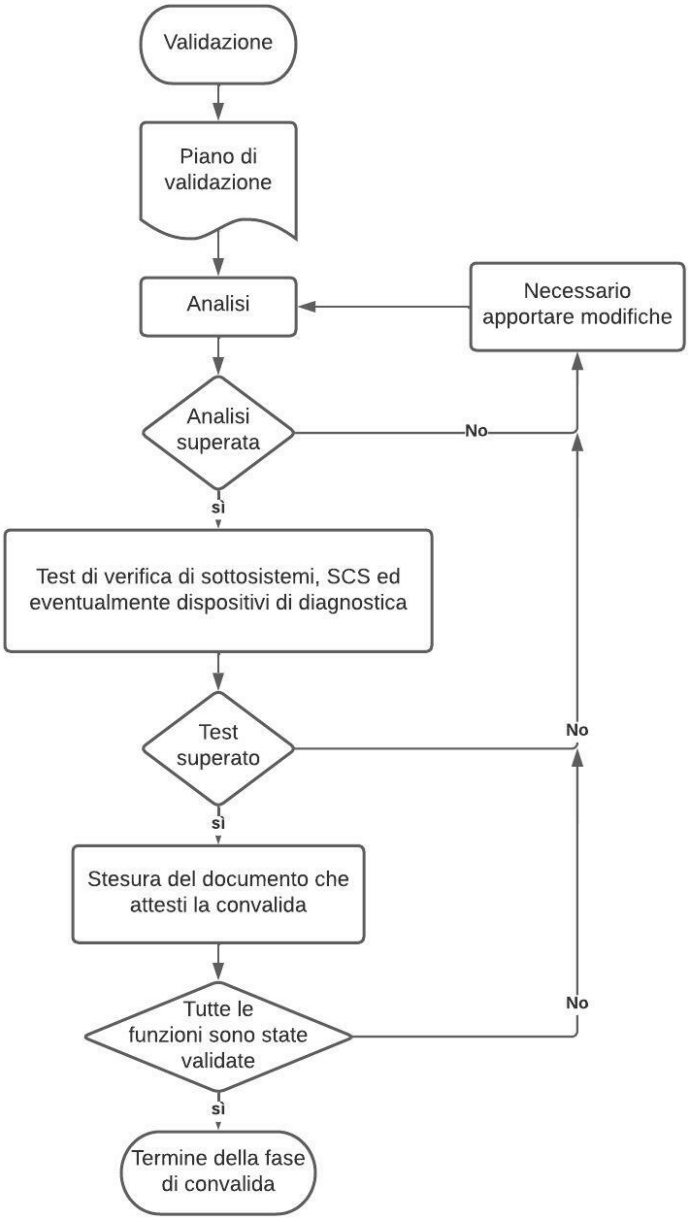


Figura 5.1 Schematizzazione della fase di convalida.

5.1 Analisi

È la prima parte della validazione e si compone di revisioni ed ispezioni del sistema al fine di garantire la coerenza e la completezza delle funzioni di sicurezza rispetto a quanto indicato nelle specifiche e alla destinazione d'uso. Per ottenere un'analisi soddisfacente è necessario disporre di informazioni circa la struttura del sistema, la funzione di sicurezza e le sue caratteristiche in termini di funzionalità ed integrità. Si hanno due possibilità di analisi:

- *T*op-down, di tipo deduttiva, adatta ad indagare gli eventi scatenanti che possono portare la macchina in uno stadio di funzionamento pericoloso. Partendo da un'analisi del tutto generale sui guasti che si possono manifestare sull'intero sistema, si individuano le possibili cause e le problematiche sui singoli sottosistemi che lo compongono. Si utilizza una struttura FTA, Fault Tree Analysis o albero dei guasti.

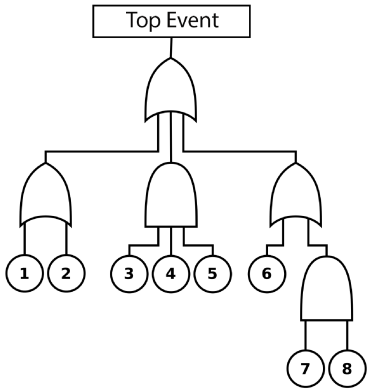


Figura 5.2 Albero dei guasti. Partendo dal guasto principale, Top Event, si individuano le possibili cause utilizzando una simbologia logica di tipo AND o OR, ad indentificare che il top event è una combinazione di guasti o difetti dei componenti del sistema.

- *B*ottom-up, metodo induttivo, adatto per determinare le possibili conseguenze individuate dai singoli guasti. Si adopera un sistema del tipo FMEA, Failure Mode Effect Analysis, dove, al contrario del precedente approccio, si individuano prima le possibili cause di guasto che potrebbero degradare o precludere il funzionamento della funzione di sicurezza.

Lo scopo di entrambi i metodi rimane quello di determinare misure di contrasto ai guasti o ai comportamenti indesiderati della macchina, attraverso la fase di progettazione.

5.2 Test

Le prove di convalida devono essere eseguite per integrare l'analisi del sistema. Devono seguire un procedimento logico scritto in un test plan che deve includere le specifiche di prova, le condizioni in cui devono essere eseguite le prove, che comunque devono essere il più vicino possibile all'ambiente di destinazione d'uso, la risposta delle uscite in base alla combinazione degli input e l'esito richiesto per approvare il sistema. L'ultimo aspetto è infatti quello di confrontare i risultati della prova con quanto atteso per garantire il funzionamento specificato e il raggiungimento degli obiettivi di performance. Si eseguono delle prove mediante guasti simulati sul componente stesso al fine di determinare il suo comportamento e la sua reazione. Le prove da intraprendere e i guasti da simulare sono elencati nelle norme specifiche di validazione come, ad esempio, la ISO 13849-2, queste possono comprendere delle prove di stress termico, attraverso un innalzamento della temperatura, meccanico, ad esempio mediante delle vibrazioni, o di tipo elettrico impiegando delle sovratensioni. È possibile eseguire la prova anche in ambienti del tutto sfavorevoli, in cui si ipotizza si possa verificare un guasto, come ad esempio per testare il suo comportamento a fronte di effetti delle sostanze chimiche, corrosione, agenti atmosferici.

Capitolo 6

Software di sicurezza

Con il progresso della tecnologia, si è ampliato l'uso di software che vengono impiegati principalmente per configurare i dispositivi di sicurezza e i PLC per il monitoraggio delle funzioni di sicurezza.
Lo scopo della norma è quello di produrre un software che sia leggibile, comprensibile, manutenibile, corretto, limitando l'introduzione di errori durante tutto il ciclo di vita del software, i bachi sono l'equivalente dei guasti per un sistema hardware, sono classificati come:

- **Errori di sintassi,** generati nella fase di scrittura del codice. Sono dovuti ad errori di ortografia o nell'uso delle istruzioni;
- **Errori di runtime,** si verificano nel momento in cui il programma viene eseguito, anche se il software non presenta errori di sintassi. Si manifesta quando il programma gestisce in modo errato le locazioni di memoria a cui ha accesso per leggere o scrivere dati;
- **Errori di logica,** che si manifestano nelle prime fasi di implementazione del software, dovuti principalmente ad una mancata comprensione del software e l'output generato non è quello richiesto.

6.1 Parametrizzazione degli SCS

Alcuni sistemi necessitano di una parametrizzazione per poter svolgere la propria funzione di sicurezza.
Lo scopo principale di questa tipologia di software è quella di trasferire correttamente i parametri specificati per una data funzione di sicurezza all'hardware che dovrà poi eseguire quella funzione richiesta.

Figura 6.1 Laser scanner impiegato come sistema di sicurezza

Un esempio tipico di parametrizzazione si ha nel campo degli scanner laser. In questo caso si nota la colorazione gialla a rappresentare un componente di sicurezza.

Viene impiegato per monitorare eventuali ingressi del personale in aree pericolose che altrimenti sarebbero protettete da protezioni rigide come griglie di sicurezza. Sono preferite a queste ultime nei casi in cui l'area da proteggere abbia una forma irregolare, infatti attraverso il software di configurazione è possibile adattarli a qualsiasi superficie.

Prendendo in considerazione i soli software in cui la parametrizzazione avviene tramite l'intervento di operatori, si possono manifestare molti errori, i valori di configurazione inseriti posso essere dipesi da:

- Errori di digitazione del valore della variabile da configurare o errata memorizzazione del parametro da parte del SCS;
- Errori durante la trasmissione dei parametri dal software al SCS dovuti ad esempio ad interferenze, ciò si manifesta soprattutto di fronte a comunicazioni wireless e questo può causare una configurazione dei parametri verso dispositivi errati;
- Guasti o errori nel software o nell'hardware del dispositivo di parametrizzazione;
- I parametri non vengono aggiornati dal software.

La configurazione deve avvenire per mano di operatori qualificati e a cui sia stato conferito il compito di parametrizzare gli SCS o i sottosistemi. Per questo nei software applicativi, che devono essere forniti dall'azienda costruttrice del componente, deve essere prevista un'autorizzazione di accesso mediante password. La configurazione mediante software deve essere un aspetto che rientra nella progettazione di un SCS, e quindi deve essere descritto nella specifica dei requisiti di sicurezza. Al fine di limitare gli errori in questa fase è necessario che un software di questo tipo garantisca delle operazioni di controllo:

- Verifica della corretta impostazione di ogni parametro in termini di valore minimo, valore massimo;
- Verifica che i parametri relativi alla sicurezza siano attendibili attraverso dei valori rappresentativi o mediante il rilevamento di valori non validi;
- Verifica che i mezzi siano forniti per prevenire modifiche non autorizzate.

6.2 Software applicativi dei PLC di sicurezza

L'impiego di PLC di sicurezza applicati alle macchine è indispensabile per monitorare continuamente lo stato degli ingressi per rilevare eventuali avarie o malfunzionamenti che potrebbero creare problemi nella macchina stessa o nei dispositivi collegati al PLC. Viene quindi impiegato come un circuito di sicurezza aggiuntivo progettato per limitare i danni ai dispositivi ad esso collegati in caso di guasto e per monitorare continuamente lo stato degli SCS e quindi l'integrità delle funzioni di sicurezza.

Tenendo conto del fatto che non esiste un software privo di errori, nella programmazione è indispensabile che tutte le attività che portano alla scrittura dello stesso, siano concentrate sulla prevenzione dei guasti durante il ciclo di vita del software.

Esistono tre tipologie di software di sicurezza, tuttavia questa norma tratta solo i primi due, il terzo viene trattato nella norma IEC 61508-3, rispetto ai primi richiede un grado notevole di competenze per la sua progettazione, è un software più complesso sia in termini di funzioni di sicurezza trattate, ma anche come dimensione del progetto stesso. Per avere una linea guida in tutte le fasi di costituzione del software, si utilizza una struttura statica definito "modello a V", formato da più blocchi, ognuno dei quali indica le attività da percorrere con l'obiettivo finale di raggiungere il livello di sicurezza richiesto e le specifiche di sicurezza indicate.

6.2.1 Software di livello 1

Il grado di affidabilità del software e delle funzioni di sicurezza che saranno controllate dallo stesso hanno un SIL 3 massimo. Rispetto alle altre due categorie, ha una complessità minore, dovuto principalmente al fatto che si impiega un linguaggio di programmazione definito "a variabilità limitata" (Limited Variability Language - LVL), in cui si implementano funzioni predefinite contenute in una libreria specifica data dall'applicazione o dal tipo di funzione di sicurezza che si vuole eseguire. Queste funzioni sono contenute in moduli pre-progettati e testati, ovvero delle unità funzionali che sono accessibili solo in termini di input e output, generalmente sono quindi delle funzioni o dei function block a cui mancano le connessioni con gli ingressi e le uscite; questi devono essere applicati secondo le istruzioni fornite dal produttore del sistema di sicurezza.

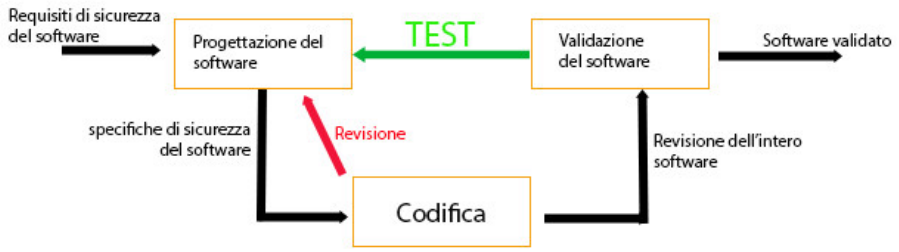


Figura 6.2 Modello a V di un software di livello 1

Il modello a V è molto semplice e costituito da sole tre parti, la progettazione del software, la codifica ed in infine il test complessivo. Già durante la codifica

avviene comunque una revisione di quanto effettuato in questa fase per convalidare le funzionalità del software rispetto alle specifiche di sicurezza dichiarate nella parte di progettazione. È fondamentale perché rende il processo di test finale più efficiente dato che una parte della validazione viene effettuata per verificare il prodotto già nelle fasi di sviluppo senza attendere il completamento del software, qualora la revisione non venga superata, è necessario tornare alla fase precedente.

6.2.2 Il software di livello 2

Il grado di affidabilità massimo raggiungibile è il SIL 2, rispetto al primo, è più complesso dato che utilizza un linguaggio di programmazione che può essere sia di tipo LVL che FVL, Full Variability Language, ossia a variabilità completa. Questo consente di implementare una grande quantità di funzioni che comprendono, oltre all'impiego dei moduli citati nel livello 1, anche l'implementazione di funzioni da parte del programmatore stesso.

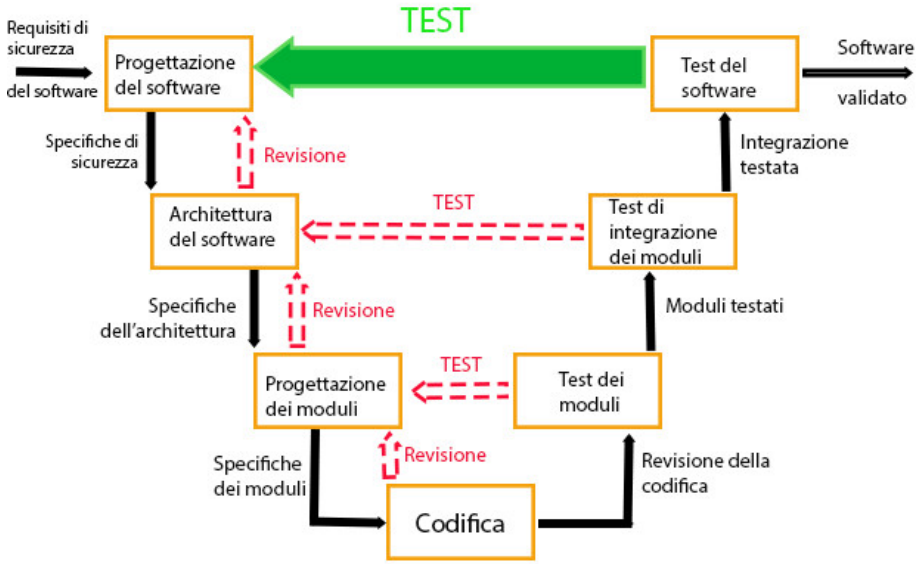


Figura 6.3 Modello a V di un software di livello 2. Si nota una maggior complessità rispetto a prima dato dal fatto che i moduli possono essere sostituiti da funzioni implementate dal programmatore, anche in questo caso per ogni fase si identifica una revisione.

6.3 Costituzione del software

Prima di procedere con la progettazione del software è necessario analizzare l'hardware che compone il sistema in esame, in particolare la sua struttura in termini di schema elettrico, input e output, modi di funzionamento della macchina nel quale sarà installato il sistema, eventuali interfacce con gli operatori che riguardano pulsanti, joystick, tastiere. Inoltre, a partire dalla valutazione dei rischi, si determinano le specifiche di sicurezza che devono essere implementate dal software ricavandone il loro funzionamento, le cause e gli effetti della funzione stessa (input e output), il tempo di risposta garantito e il livello di affidabilità da raggiungere. L'insieme delle specifiche va poi riunito in una check-list in modo da agevolare la validazione. Il processo che porta alla codifica di un software è di tipo sequenziale, partendo dalle specifiche delle funzioni, dovrà poi essere espressa l'architettura del software, ovvero l'insieme di function block o moduli che lo costituiscono.

6.3.1 Uso dei moduli

Nel momento in cui si utilizza un linguaggio di programmazione che sia il più intuitivo possibile, si fa ricorso ai moduli, ognuno dei quali al suo interno presenta una specifica funzionalità. Questo tipo di programmazione rende il software comprensibile a molti operatori e facilita la validazione poiché impiega una struttura prettamente grafica per implementare una funzione di sicurezza. Si vuole ora analizzare un semplice esempio di programmazione di una cella di produzione costituita da 3 attuatori e vari dispositivi di sicurezza.

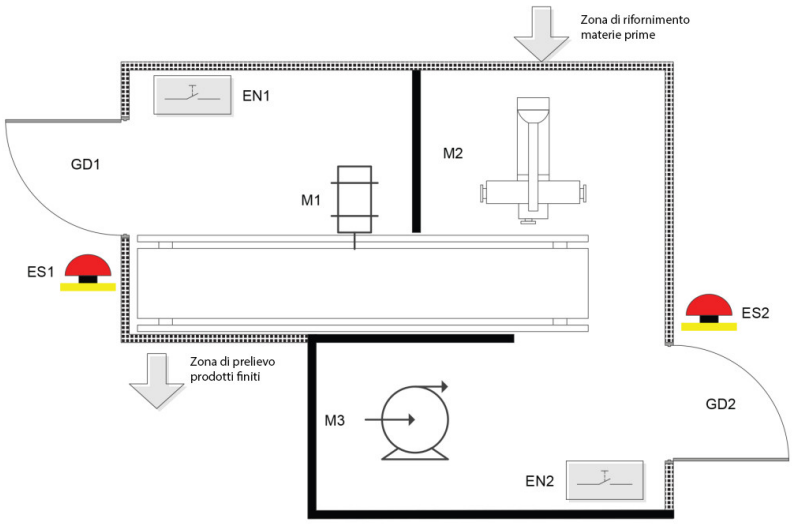


Figura 6.4 Piantina del sistema da analizzare

Si notano due funghi di emergenza (ES1 - ES2), i tre motori (M1 - M2 - M3), due punti di accesso alla cella con i rispettivi microswitch di sicurezza a segnalare lo stato delle porte (GD1 - GD2), due contatti che abilitano il sistema di controllo della velocità di rotazione dei motori (EN1 - EN2) .

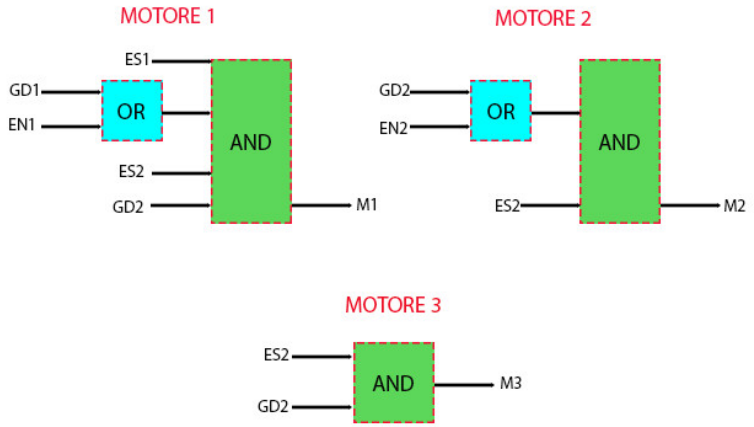


Figura 6.5 Moduli pre-progettati. In questo caso implementano una funzione logica (OR e AND), il programmatore deve collegare le funzioni con i rispettivi input, ossia i componenti di sicurezza, e con i rispettivi output, gli attuatori.

6.3.2 Codifica

Il software deve essere sviluppato tenendo conto delle specifiche espresse nella fase di progettazione e le regole di codifica che possono essere note e ben definite (standard) per un certo campo di applicazione, oppure essere interne al produttore. Tuttavia, ci sono delle regole sempre valide che consentono di ottenere un software molto chiaro e con una struttura definita, anche se la complessità è elevata, e soprattutto che ci sia una certa omogeneità tra i vari programmi anche se creati da aziende differenti. Questo risultato si raggiunge facendo in modo che la struttura del software segua un flusso logico, in modo tale che inizi dall'alto e segua la sequenza effettiva, si utilizzino gli stessi nomi per le variabili utilizzati nella fase di individuazione degli input e output della funzione, in particolare i nomi dei parametri stessi devono rappresentarne la funzione in modo chiaro, ogni parte dovrebbe avere una sezione di commento sufficiente a comprendere la funzione implementata.

6.3.3 Attività di verifica

Per ogni attività svolta precedentemente segue una verifica per accertare che siano rispettati i requisiti indicati, al termine si esegue una validazione finale dell'intero software così da attestare il rispetto delle specifiche di partenza. Questa attività si ripartisce quindi in due fasi:

1. Analisi statica: ispezione generale del software mediante revisione del codice, analisi del corretto flusso delle istruzioni. Lo scopo è quello di verificare che le specifiche dichiarate nella check-list siano soddisfatte.

2. Test dinamico: esecuzione del software in modo controllato, tale da dimostrare il comportamento desiderato e l'esclusione di comportamenti in-

desiderati, si effettua mediante test funzionali impiegando le black-box, white-box o grey-box.

Con la **black-box** si simulano le diverse possibili combinazioni degli ingressi del software e si va a verificare il comportamento delle uscite, senza avere la conoscenza della struttura interna del software. Si può fare anche tramite un banco di prova dove gli ingressi sono dei selettori, mentre le uscite sono indicate con delle lampade di segnalazione.

La **white-box** è l'esatto opposto della precedente, in questo caso viene analizzata la struttura interna del software e la sua logica di funzionamento, questo consente di capire cosa succede all'interno del codice sorgente e correggere ciò che non funziona, è necessaria una larga conoscenza del codice in modo da gestire al meglio eventuali errori che si manifestano.

La **grey-box** è una via di mezzo tra i due precedenti, quindi si verifica la correttezza del software a livello di input/output ed interfacce, andando ad analizzare e modificare eventualmente il codice sorgente.

Occorre quindi verificare che ciò che si voleva ottenere nelle prime fasi di progettazione, sia stato raggiunto. L'output di questa fase è un documento che riporta i risultati dei test effettuati che comprendono una simulazione del guasto e la relativa reazione a seconda dell'integrità della sicurezza richiesta. Si raccomanda di definire delle linee guida o comunque delle procedure generali che accompagni il processo di test, queste dovrebbero includere:

- Tipologia di prove da effettuare;
- Specifica dell'attrezzatura e degli strumenti impiegati;
- Luogo fisico del test in termini di simulazione al computer o attraverso un banco di prova oppure direttamente nella stessa macchina;
- Criteri di validazione della prova rispetto alle relative funzioni di sicurezza;
- Azioni correttive da intraprendere nel caso di test fallito.

Nel suo complesso, sia l'analisi statica che il test dinamico devono essere svolte da personale non direttamente coinvolto nella progettazione del software, possono essere anche enti esterni all'azienda che sviluppa il software. Questo garantisce che la persona terza possa svolgere un'accurata analisi del funzionamento del software, a differenza del programmatore che ne conosce il funzionamento e potrebbe quindi effettuare un'analisi poco scrupolosa. Questo aspetto, oltre ad esprimere la validazione, garantisce anche che il software sia scritto in forma chiara, leggibile e comprensibile ad operatori che non sono coinvolti direttamente nella sua stesura, e questo è uno dei principali obiettivi che ci si pone nelle prime fasi di elaborazione.

Test del software			
	Esito		*Note*
	Positivo	Negativo	
Il software è conforme alle specifiche di sicurezza			
Il software è conforme alle linee guida di codifica			
Le interconnessioni tra input e output sono corrette			
Il test I/O è stato eseguito con esito positivo			
Il test delle funzioni di sicurezza ha dato esito positivo			
I test di parametrizzazione degli SCS hanno dato esito positivo			
Data:			
Firma dell'esecutore:			

Tabella 6.1 Esempio di check-list per la validazione del software

6.3.4 Modifiche e documentazione

Qualora il test di validazione dia esito negativo, può risultare necessario effettuare delle modifiche al software. Prima di eseguirle, è indispensabile che tali modifiche siano oggetto di un'analisi di impatto che identifichi tutte le parti software coinvolte in questi cambiamenti, le necessarie attività di riprogettazione e validazione del software che saranno effettuate. Lo scopo ultimo rimane quello di mantenere il soddisfacimento delle specifiche di sicurezza.

Ogni modifica va poi documentata in modo tale da mantenere una traccia storica degli interventi fatti, per specificare quali cambiamenti sono stati introdotti, la motivazione che ha spinto ad effettuarli e quando sono stati implementati. Allo stesso modo, tutte le attività intraprese durante il ciclo di costituzione del software devono essere documentati per essere a disposizione dei soggetti interessati.

Capitolo 7

La documentazione

La norma in questione, oltre a trattare il RESS 1.2.1 della Direttiva Macchine, garantisce la presunzione di conformità con il RESS 1.7.4 relativo al contenuto delle istruzioni di una macchina, in particolare la documentazione che accompagna un SCS. Analizza i seguenti punti del requisito essenziale:

ciascun manuale di istruzioni deve contenere, se del caso, almeno le informazioni seguenti:

e) i disegni, i diagrammi, le descrizioni e le spiegazioni necessari per l'uso, la manutenzione e la riparazione della macchina e per verificarne il corretto funzionamento;

g) una descrizione dell'uso previsto della macchina;

i) le istruzioni per il montaggio, l'installazione e il collegamento, inclusi i disegni e i diagrammi e i sistemi di fissaggio e la designazione del telaio o dell'installazione su cui la macchina deve essere montata;

r) la descrizione delle operazioni di regolazione e manutenzione che devono essere effettuate dall'utilizzatore nonché le misure di manutenzione preventiva da rispettare;

s) le istruzioni per effettuare, in condizioni di sicurezza, la regolazione e la manutenzione, incluse le misure di protezione che dovrebbero essere prese durante tali operazioni.

La documentazione fornita con un sistema di controllo di sicurezza comprende una parte tecnica e una parte relativa alle informazioni per l'uso.

7.1 Documentazione tecnica

Questa parte non sarà distribuita alla vendita, ma rimane all'interno dell'azienda costruttrice contenuta nel fascicolo tecnico, deve contenere informazioni utili come:

- Specifiche delle funzioni di sicurezza dichiarate che sono in grado di fornire il sistema o il sottosistema, e le loro caratteristiche in termini di funzionamento e affidabilità;
- Procedure seguite durante le prove di validazione;
- Descrizione del comportamento in caso di guasto o perdita della funzione di sicurezza;

- Limiti d'impiego, condizioni ambientali d'uso;
- Misure contro i guasti sistematici come le regole di buona tecnica adottate nella fase di progettazione per contrastare risultati provenienti dalla valutazione dei rischi.

7.2 Informazioni per l'uso

Raccoglie una serie di informazioni utili per l'installazione, l'uso e la manutenzione del sistema, quindi da fornire con il prodotto quando lo si immette nel mercato, deve includere:

- Istruzioni di installazione e collegamento;
- Descrizione generale del dispositivo e di ogni sottosistema;
- Limiti operativi del SCS in termini di frequenza operativa e grandezze di interfacciamento, ad esempio di tipo elettrico (tensione di alimentazione), pneumatico o idraulico;
- Le condizioni ambientali d'uso (temperatura, vibrazioni, rumore, presenza di agenti chimici, eventi atmosferici);
- Descrizione relativa all'interfaccia con gli operatori (eventuali segnalazioni, allarmi o pannello di controllo che genera segnali di input);
- Descrizione delle funzioni di sicurezza implementate, inclusa la descrizione delle situazioni pericolose, modalità operativa richiesta e gli eventuali sottosistemi;
- Descrizione delle interazioni tra gli SCS e i sistemi di controllo della macchina;
- Vita utile e parametri tipici di affidabilità del componente;
- Informazioni relative alla sospensione delle funzioni di sicurezza, in particolare le disposizioni da adottare nel caso in cui l'attività di manutenzione escluda una funzione di sicurezza;
- Gli strumenti necessari per la manutenzione e rimessa in servizio delle attrezzature;
- Descrizione e frequenza dei test periodici al fine di confermare il corretto funzionamento o per rilevare eventuali guasti.

Capitolo 8

Le differenze con l'edizione precedente

La versione precedente della norma in esame trattava solamente i sistemi di controllo con funzione di sicurezza di tipo elettrico, elettronico o elettronico programmabile, mentre la formula attuale copre anche i settori non elettrici come quello pneumatico, idraulico e meccanico. Sono considerati quindi i possibili guasti:

- Elettrici, come cortocircuiti, mancato avviamento o arresto di motori, mancato sganciamento o azionamento di interruttori di potenza o relè.
- Idraulico o pneumatico, come perdita di pressione o ostruzione del filtro;
- Meccanico, come rottura di molle, allentamento di elementi fissi dovuti a vibrazioni, usura di cuscinetti.

Una differenza sostanziale si ha anche nella trattazione del software, infatti nell'edizione precedente, questo aspetto è trattato in maniera del tutto generale, fornendo delle linee guida per la codifica di un software senza esprimere una distinzione tra i vari livelli di complessità e applicazione e senza fornire un orientamento circa la validazione dello stesso (primo fra tutti il fatto che deve essere convalidato da una persona terza).

La norma EN IEC 62061 cita anche altre norme specifiche, tra le quali la norma EN ISO 13849, che tratta le parti dei sistemi di comando legati alla sicurezza. Essendo una norma emanata dall'ente ISO, significa che tratta delle tecnologie prettamente meccaniche. Quindi la suddivisione tra le due norme, in merito alla tipologia di sistemi di comando, un tempo era più marcata, e il progettista prendeva in considerazione una delle due norme sulla base della tecnologia prevalente in un sistema, anche se l'obiettivo finale rimane lo stesso ovvero l'affidabilità dei sistemi di comando con funzione di sicurezza.

La nuova edizione ha una copertura settoriale più ampia, è possibile così poter sostituire la norma ISO 13849, in modo da avere un'unica norma che il progettista può seguire per ottenere la conformità con il RESS specifico. Lo standard ISO 13849, persegue lo stesso scopo della norma EN IEC 62061, attraverso però delle strade e dei parametri differenti, come ad esempio l'indicatore di affidabilità del componente di sicurezza, identificato come PL o Performance Level.

SIL - EN IEC 62061	PL - ISO 13849
-	A
1	B
1	C
2	D
3	E

Tabella 8.1 Corrispondenza tra i due livelli di affidabilità delle due norme. Non c'è corrispondenza con il PLa perchè nella norma EN IEC 62061 è considerato come un indice di affidabilità troppo basso da contemplare nei sistemi di sicurezza

Capitolo 9

Calcoli ed esempi

9.1 La determinazione del Safety Integrity Level

Per il calcolo del livello di affidabilità, il SIL, sono richieste delle considerazioni riguardanti la stima del rischio, per ogni situazione pericolosa si prendono in considerazione:

- **Gravità del danno;**
- **Probabilità di accadimento del danno,** che a sua volta è funzione di frequenza ed esposizione al pericolo e possibilità di limitare o evitare il danno.

Per ognuna di queste si associano degli indici numerici che saranno poi fondamentali per l'attribuzione del SIL richiesto. Il metodo impiegato è simile alla matrice del rischio impiegata per effettuare una stima dello stesso.

9.1.1 Gravità del danno - Se

Viene associato il valore numerico da 1 a 4 in base al danno arrecato alla salute.

1 lesioni lievi in cui le cure di pronto soccorso senza intervento medico sono sufficienti, rientrano graffi e lievi contusioni;

2 lesione più grave ma comunque reversibile che richiede l'intervento di un medico; è possibile riprendere l'attività lavorativa dopo un breve tempo, ne fanno parte gravi lacerazioni o gravi contusioni;

3 lesione grave e anche irreversibile in modo tale che non sia possibile operare nella stessa mansione dopo la guarigione, come ad esempio perdita di dita o lesioni reversibili ma gravi come rotture degli arti;

4 lesione fatale o irreversibile tale che sarà impossibile continuare nello stesso lavoro dopo la guarigione, comprende la perdita di arti, perdita della vista parziale o totale.

9.1.2 Frequenza e durata di esposizione al danno - Fr

Questo parametro è determinato da diversi fattori, dipende in linea di massima dalla frequenza di transito di operatori nell'area considerata pericolosa e una durata media della presenza, rientrano quindi:

- Modalità di lavoro della macchina durante l'esposizione al danno (manuale, automatica);
- Tipologia di lavoro dell'operatore che ha portato al danno (manutenzione, riparazione);

- Tempo in cui l'operatore rimane nella zona pericolosa;
- Frequenza di accessi a tale zona.

Anche in questo caso viene fissato un valore numerico che va da 1 a 5.

Frequenza e durata dell'esposizione (Fr)		
Frequenza	**Tempo di esposizione**	
	≥10min	<10min
≥1 per h	5	5
<1 per h oppure ≥1 al giorno	5	4
<1 al giorno oppure ≥1 per 2 settimane	4	3
<1 per 2 settimane oppure ≥1 all'anno	3	2
<1 all'anno	2	1

Tabella 9.1 Attribuzione numerica alla frequenza

9.1.3 Probabilità che si verifichi l'evento pericoloso - Pr

Questa viene stimata in base ai comportamenti prevedibili della macchina rilevanti per il pericolo, ovvero è necessario rilevare il rischio al quale è esposto un operatore se non è eseguita una funzione di sicurezza da parte di un SCS. Questo non è quindi un indice quantificabile dallo stesso progettista, però è comunque richiesta un'analisi di tutte le problematiche che si possono incontrare, eventuali abilità o conoscenze richieste dagli operatori vanno indicate nelle informazioni per l'uso.

Probabilità di accadimento	**Valore numerico (Pr)**
Molto elevata	5
Probabile	4
Possibile	3
Raramente	2
Trascurabile	1

Tabella 9.2 Attribuzione numerica probabilità che si verifichi un evento pericoloso

9.1.4 Probabilità di evitare o limitare il danno - Av

Questo indicatore è prevalentemente determinato dal comportamento dell'operatore (distrazioni, stress), dalle sue abilità o conoscenze in materia di sicurezza, e dalla sua abilità a reagire al pericolo.
Ma una parte è dipesa anche dalle caratteristiche dell'evento pericoloso stesso come la sua evoluzione nel tempo (rapida o lenta), la natura del componente in cui si manifesta l'evento pericoloso, come lame, tubature calde o elettricità, possibilità di riconoscere un evento pericoloso, ad esempio una sbarra di materiale conduttore non cambia il suo aspetto visivo se si manifesta un guasto elettrico o meno, oppure un ambiente rumoroso può impedire ad un operatore di sentire l'avvio di un macchinario.

Quindi, nel complesso, dipende da eventi sia quantificabili attraverso un'analisi del rischio ed altri che dipendono dal comportamento umano. Nella sua classificazione si individua il fatto che il pericolo sia riconoscibile e se c'è tempo sufficiente per intervenire o lasciare l'area pericolosa.

Probabilità di evitare o limitare il danno (Av)	
Impossibile	5
Raramente	3
Probabile	1

Tabella 9.3 Attribuzione numerica alla probabilità di evitare o limitare il danno

9.1.5 Classe di probabilità del danno (CI) e attribuzione del SIL

Per ogni pericolo si calcola la probabilità di danno come somma degli indici numerici dati dalla probabilità che si verifichi e che si limiti il danno e la frequenza e durata di esposizione al danno.

$$CI = Fr + Pr + Av$$

Questo combinato con la gravità del danno consente di determinare il SIL richiesto per una funzione di sicurezza attraverso una matrice

Gravità - Se	**Classe di probabilità - Cl**												
	3	4	5	6	7	8	9	10	11	12	13	14	15
4	SIL 1		SIL 2						SIL 3				
3						SIL 1			SIL 2			SIL 3	
2									SIL 1			SIL 2	
1												SIL 1	

Tabella 9.4 Attribuzione SIL. Si notano dei punti in cui l'integrità della funzione di sicurezza è omessa perchè assumerebbe un valore inferiore al minimo, ed è quindi non rilevante per la sicurezza

9.1.6 Altro metodo di determinazione

Attraverso la seguente tabella, è comunque possibile determinare un livello di SIL sulla base delle relazioni tra le grandezze tipiche impiegate nell'ambito dell'affidabilità di un sistema: il Main Time To Failure e di conseguenza il tasso di guasto da cui si ricava il Safety Failure Fraction, e la tolleranza ai guasti hardware.

Safe Fault Fraction - SFF	**Hardware Fault Tolerance - HFT**		
	0	1	2
< 60%		SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	
≥ 99%	SIL 3		

Tabella 9.5 Attribuzione del SIL impiegando due parametri fondamentali

L'indicatore SFF si ottiene dalla formula:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

Dove $\lambda_{\mathbf{S}}$ rappresenta il tasso di guasti sicuri;

$\sum \lambda_{\mathbf{S}} + \sum \lambda_{\mathbf{D}}$ è il tasso di guasti complessivo (sicuri + pericolosi);

$\lambda_{\mathbf{DD}}$ indica il tasso di guasti pericolosi che vengono rilevati dalle funzioni diagnostiche;

$\lambda_{\mathbf{D}}$ è il tasso di guasti pericolosi.

9.1.7 Calcolo del SIL nel caso di sottosistemi

Nel caso di un SCS costituito da più sottosistemi, ognuno qualificato con il proprio SIL e PFH, il livello di affidabilità raggiungibile è limitato da:

1. Somma di tutti i PFH di ogni elemento;
2. Il SIL massimo raggiungibile deve essere uguale o inferiore al SIL più basso tra tutti i sottosistemi.

Tendendo conto che il SIL viene anche assegnato in base al valore di PFH secondo la seguente tabella

SIL	**PFH** $[\frac{1}{h}]$
1	$< 10^{-5}$
2	$<10^{-6}$
3	$<10^{-7}$

Tabella 9.6 SIL limitato ai valori del PFH

si può calcolare il SIL complessivo di più sottosistemi come nell'esempio

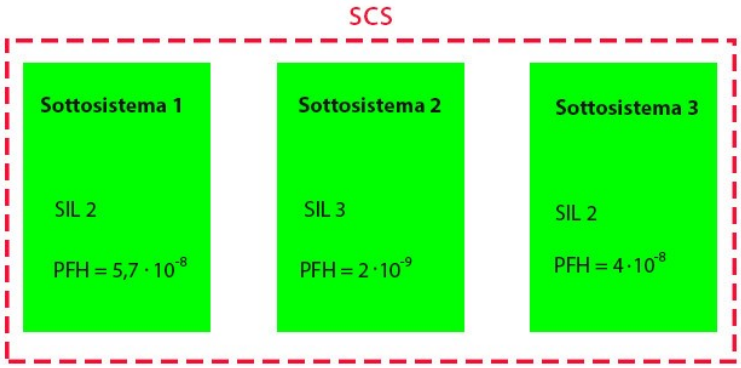


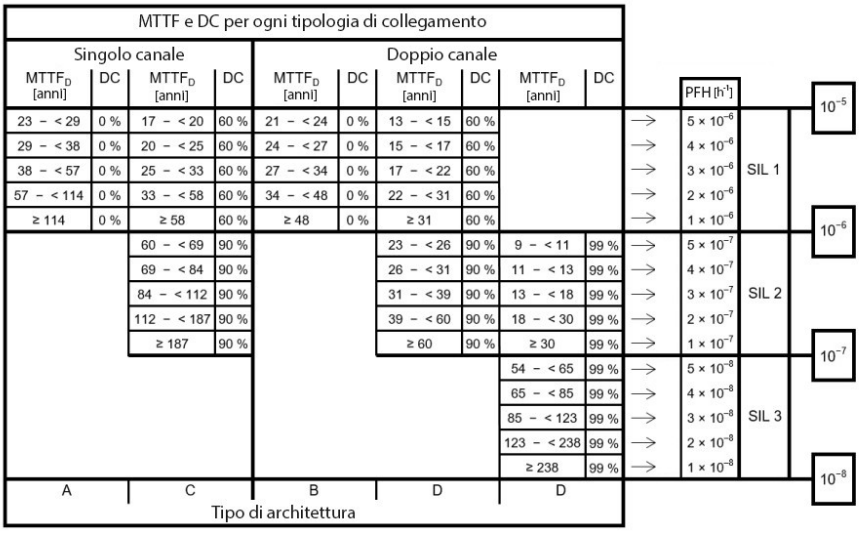
Figura 9.1 Determinazione del SIL per un SCS costituito da più sottosistemi

da cui si ricava:

1. il SIL più basso è pari al livello 2 del primo e terzo sottosistema
2. la probabilità di guasti $\sum PFH = 5,7 \cdot 10^{-8} \frac{1}{h}$ che rientrerebbe nella categoria SIL 3.

Dato che il SIL massimo raggiungibile deve essere limitato a quello più basso di ogni sottosistema, in questo caso sarà assegnato un SIL 2 all'intero SCS.

Un altro metodo che può essere impiegato è la seguente tabella, che consente di stimare il PFH attraverso il fattore di copertura e il MTTF e di conseguenza, come nella Tabella 9.6, assegnare il SIL corrispondente



MTTF e DC per ogni tipologia di collegamento													
Singolo canale				Doppio canale									
$MTTF_D$ [anni]	DC	$MTTF_D$ [anni]	DC	$MTTF_D$ [anni]	DC	$MTTF_D$ [anni]	DC	$MTTF_D$ [anni]	DC		PFH [h^{-1}]		
23 – < 29	0 %	17 – < 20	60 %	21 – < 24	0 %	13 – < 15	60 %			→	5×10^{-6}		10^{-5}
29 – < 38	0 %	20 – < 25	60 %	24 – < 27	0 %	15 – < 17	60 %			→	4×10^{-6}		
38 – < 57	0 %	25 – < 33	60 %	27 – < 34	0 %	17 – < 22	60 %			→	3×10^{-6}	SIL 1	
57 – < 114	0 %	33 – < 58	60 %	34 – < 48	0 %	22 – < 31	60 %			→	2×10^{-6}		
≥ 114	0 %	≥ 58	60 %	≥ 48	0 %	≥ 31	60 %			→	1×10^{-6}		10^{-6}
		60 – < 69	90 %			23 – < 26	90 %	9 – < 11	99 %	→	5×10^{-7}		
		69 – < 84	90 %			26 – < 31	90 %	11 – < 13	99 %	→	4×10^{-7}		
		84 – < 112	90 %			31 – < 39	90 %	13 – < 18	99 %	→	3×10^{-7}	SIL 2	
		112 – < 187	90 %			39 – < 60	90 %	18 – < 30	99 %	→	2×10^{-7}		
		≥ 187	90 %			≥ 60	90 %	≥ 30	99 %	→	1×10^{-7}		10^{-7}
								54 – < 65	99 %	→	5×10^{-8}		
								65 – < 85	99 %	→	4×10^{-8}		
								85 – < 123	99 %	→	3×10^{-8}	SIL 3	
								123 – < 238	99 %	→	2×10^{-8}		
								≥ 238	99 %	→	1×10^{-8}		10^{-8}
A		C		B		D		D					
Tipo di architettura													

Tabella 9.7 Metodo semplificato per l'assegnazione del SIL

Anche questo metodo è impiegato nel caso di sottosistemi, in cui si determina il DC dell'architettura pari al fattore di copertura più basso tra quelli che la costituiscono, e il MTTF dell'architettura pari a quello più basso o uguale alla media geometrica dei parametri, $MTTF_{\text{SCS}} = \sqrt{MTTF_1 \cdot MTTF_2}$

Ad esempio:

- SCS costituito da due sottosistemi collegati a formare un'architettura D. $DC_1 = 90\%$ e $DC_2 = 90\%$, $MTTF_{1,2} = 60anni$, secondo la tabella vi corrisponde un SIL 2.
- SCS costituito da due sottosistemi collegati a formare un'architettura D. $DC_1 = 99\%$ e $DC_2 = 99\%$, $MTTF_1 = 200anni$ e $MTTF_2 = 20anni$, di conseguenza $MTTF_{\text{SCS}} = \sqrt{200 \cdot 20} = 63,2anni$, secondo la tabella il sistema raggiunge un SIL 3.

9.2 Esempio di progettazione di un SCS

Il seguente paragrafo vuole essere un esempio generale riguardo la procedura di progettazione di un SCS che opera una funzione di arresto di sicurezza nel momento in cui viene aperto il riparo mobile che protegge gli operatori da un motore in rotazione, secondo lo schema e la suddivisione in sottosistemi seguente.

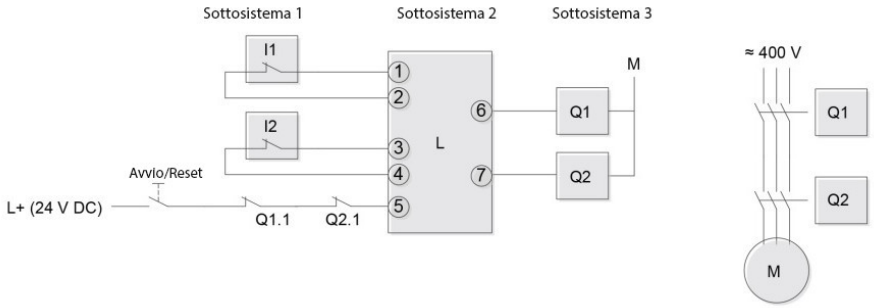


Figura 9.2 Scomposizione del sistema in più sotto parti

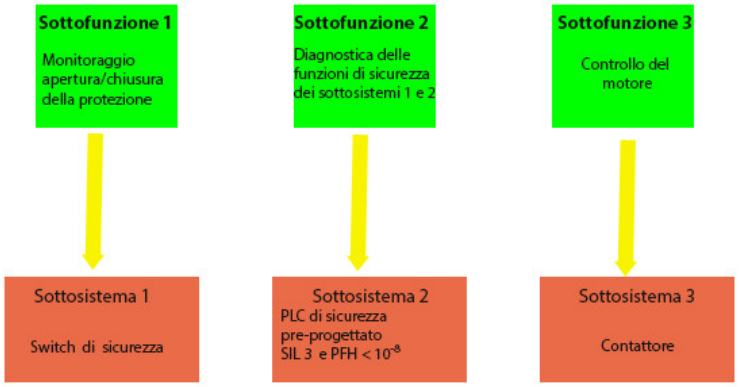


Figura 9.3 Composizione di ogni sottosistema con relative funzioni di sicurezza implementate

Il sottosistema 1 è costituito da due switch uguali che indicano lo stato del riparo (aperto-chiuso) collegati tra loro con l'architettura di tipo D, quindi sono due componenti posti in ridondanza ed è presente il sistema di diagnostica, rappresentato dal sottosistema 2. Il terzo è costituito da due interruttori di potenza che alimentano il motore solo nel momento in cui il riparo risulta chiuso, anche questi costituiscono un'architettura di categoria D.

Il primo passo da svolgere riguarda la definizione delle specifiche delle funzioni di sicurezza:

*D*escrizione	Quando la porta di protezione verrà aperta, il motore elettrico si fermerà
*A*vvio/Reset	È richiesta l'azione di un operatore
*P*riorità	Priorità maggiore rispetto a tutte le altre funzioni di sicurezza. Al di sotto solo dello stop di emergenza
*F*requenza d'uso	10 volte all'ora, il sistema lavora 16h al giorno, per 250 giorni all'anno
*T*empo di risposta	Non più di 500ms dall'apertura della protezione. Deve essere diseccitato il motore e fermato il suo albero, considerandolo autofrenante
*R*eazione ad un eventuale guasto	Arresto immediato, se il rilevamento del guasto avviene al riavvio del sistema, il riavvio stesso non deve essere eseguito
*A*mbiente di installazione	Ambito industriale, presenza di polvere, vibrazioni del sistema
*S*IL richiesto	SIL 2
*A*rchitettura	Uso di architetture di tipo D per ottenere un HFT pari a 1

Tabella 9.8 Tabella che raccoglie le specifiche della funzione di sicurezza

9.2.1 Sottosistema 1

Essendo un'architettura di categoria D, presenta un HFT pari a 1. Vengono presi in considerazione il comportamento degli interruttori ed eventuali reazioni ai guasti, in modo da poter classificare questi ultimi come guasti sicuri o pericolosi.

- **Il contatto rimane chiuso oppure si chiude autonomamente o non si aprirà più,** questi rappresentano tre situazioni di guasti pericolosi.
- **Il contatto si apre involontariamente oppure rimane aperto,** queste sono due tipiche situazioni di guasto senza effetto, dal momento che la reazione è una disalimentazione del motore, nel momento in cui la protezione è già chiusa, non rappresentano quindi un guasto nè sicuro, nè pericoloso.

Complessivamente si ricava che i guasti sicuri non sono presenti, per cui $\lambda_S = 0$, oltre a ciò, dato che il sistema è composto anche di un dispositivo di diagnostica, si ottiene $SFF = DC_{\mathbf{1}}$; secondo tale relazione, i guasti pericolosi sono in realtà dei guasti rilevabili così che non abbiano il potenziale per mettere il sistema in uno stato pericoloso. Dagli indici tabulati per la stima del fattore di copertura si ricava $DC_1 = 99\%$ per entrambi i contatti. Secondo quanto indicato nella Tabella 9.5, vi corrisponde un SIL 3.

La determinazione del tasso di guasto viene ricavato dal parametro B_{10D} che viene indicato pari a 2000000 di cicli.

- **Numero di cicli di lavoro all'anno**

$$n_{\text{op1}} = \frac{d_{\text{op}} \cdot h_{\text{op}} \cdot 3600 \frac{s}{h}}{t_{\text{cycle}}}$$

$$n_{\text{op1}} = \frac{250 giorni \cdot 16 \frac{h}{giorno} \cdot 3600 \frac{s}{h}}{360 s} = 40000 \frac{cicli}{anno}$$

- **Main Time To Failure - dangerous**

$$MTTF_{\text{D1}} = \frac{B_{10\text{D}}}{0{,}1 \cdot n_{\text{op}}}$$

$$MTTF_{\text{D1}} = \frac{2000000 cicli}{0{,}1 \cdot 40000 \frac{cicli}{anno}} = 500 anni$$

Dal calcolo di questi parametri, anche secondo la Tabella 9.5, il sottosistema raggiunge un SIL 3

9.2.2 Sottosistema 2

È un dispositivo di diagnostica pre-progettato che presenta un SIL 3 ed un PFH $< 10^{-8} \frac{1}{h}$

9.2.3 Sottosistema 3

Anche in questo caso, come nel primo sottosistema, presenta un HFT pari a 1. Dal momento che sono anch'essi due dispositivi con la stessa funzionalità del sottosistema 1, ossia aprire o chiudere un circuito, presentano la stessa tipologia di guasti, dunque $SFF = DC_{\mathbf{3}}$, dove, secondo il valore tabulato per la stima del fattore di copertura, si ottiene $DC_3 = 99\%$. Secondo quanto indicato nella Tabella 9.5, vi corrisponde un SIL 3.

La determinazione del tasso di guasto viene ricavato dal parametro B_{10D} che viene indicato pari a 1300000 di cicli.

- **Numero di cicli di lavoro all'anno**

$$n_{\text{op1}} = \frac{d_{\text{op}} \cdot h_{\text{op}} \cdot 3600 \frac{s}{h}}{t_{\text{cycle}}}$$

$$n_{\text{op1}} = \frac{250 giorni \cdot 16 \frac{h}{giorno} \cdot 3600 \frac{s}{h}}{360 s} = 40000 \frac{cicli}{anno}$$

- **Main Time To Failure - dangerous**

$$MTTF_{\text{D1}} = \frac{B_{10\text{D}}}{0{,}1 \cdot n_{\text{op}}}$$

$$MTTF_{\text{D1}} = \frac{1300000 cicli}{0{,}1 \cdot 40000 \frac{cicli}{anno}} = 325 anni$$

Dal calcolo di questi parametri, anche secondo la Tabella 9.5, il sottosistema raggiunge un SIL 3.

9.2.4 SIL raggiunto dal sistema

In accordo con la formula $PFH_{\text{SCS}} = \sum PFH_{\text{sottosistema}}$, si ottiene
$PFH_{\text{SCS}} = PFH_1 + PFH_2 + PFH_3 = 10^{-8} + 10^{-8} + 10^{-8} = 3 \cdot 10^{-8}$
Secondo la Tabella 9.4, il sistema complessivamente raggiunge un SIL 3, valore superiore a quello richiesto e uguale ai livelli di affidabilità di ogni sottosistema.

9.2.5 Test di validazione

L'ultimo passo è indispensabile per verificare che le specifiche di sicurezza dichiarate siano soddisfatte, questo viene fatto attraverso una prova del funzionamento dell'intero SCS e poi singolarmente per ogni sottosistema.
La prova che si applica all'intero SCS è un test funzionale a verificare che una volta aperta la porta di protezione, il motore si arresta, e una volta chiusa il motore non si riavvia autonomamente.
Nel caso dei sottosistemi si possono applicare delle sovratensioni ai contatti del primo e del terzo al fine di testare la loro tenuta oppure sconnettere uno dei due contatti che crea la ridondanza e verificare che il tutto funzioni ugualmente, è possibile scollegare i contatti ausiliari dell'ultimo sottosistema al fine di verificare la reazione del sistema di diagnostica ad un eventuale guasto.

Prove Funzionali			
	Esito		*Note*
	Positivo	Negativo	
Motore fermo all'apertura della porta di protezione			
Il motore non si riavvia alla sola chiusura della porta di protezione			
Riavvio del motore grazie ad un intervento di un operatore e alla chiusura della porta			
Arresto immediato del motore, non più di 500ms			
Prove di efficienza dei comandi di arresto di emergenza (eventuali funghi di arresto rapido) anche per testare la priorità delle varie funzioni implementate			
Il motore non si riavvia a fronte di un ritorno della tensione dopo un'eventuale disalimentazione			
Prove di continuità del circuito equipotenziale			
Riavvio non consentito al manifestarsi di un guasto (test del PLC di sicurezza)			
Data:			
Firma dell'esecutore:			

Tabella 9.9 Esempio di un report di validazione

Conclusioni

La trattazione e l'analisi di questa norma svolti come tesi di laurea si sono rivelati positivi sotto tanti punti di vista, primo fra tutti il fatto che potrà avere un risvolto nell'ambito lavorativo al termine del mio percorso di studi.

Ho voluto sviluppare un argomento che riguardasse la sicurezza delle macchine perché lo considero un tema fondamentale per ottenere un'interazione uomo-macchina che sia sempre più efficace e proficua, e anche perché, dal mio punto di vista, è tutt'oggi un tema non sufficientemente affrontato nelle aziende, visti gli innumerevoli infortuni sul lavoro anche molto gravi.

Bibliografia

La storia dell'Unione Europea e il suo mercato interno
https://european-union.europa.eu/principles-countries-history/history-eu_it
https://eur-lex.europa.eu/homepage.html

Direttiva Macchine 2006/42/CE

Norma EN IEC 62061: 2021 Safety of machinery — Functional safety of safety-related control systems

Norma EN IEC 62061: 2005 Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

Norma ISO 12100: 2010 Safety of machinery — General principles for design — Risk assessment and risk reduction

Norma EN ISO 13849-1: 2015 Safety of machinery — Safety-related parts of control systems

Elenco delle figure

1.1 Simbolo grafico della marcatura CE 13
1.2 Simbolo grafico della marcatura Atex 14
1.3 Simbolo grafico della marcatura per equipaggiamenti marittimi . . 14
2.1 Campo di applicazione/esclusione della Direttiva Macchine 17
2.2 Dichiarazione di conformità 21
2.3 Applicazione della norma EN IEC 62061: 2021 24
3.1 Esempio di applicazione di un SCS 27
3.2 Esempi di SCS 27
3.3 Fungo di emergenza 28
3.4 Schema di realizzazione SCS 29
4.1 Curva del tasso di guasto 34
4.2 Relazione tra MTTF, MTBF e MTTR 35
4.3 Esempio di scomposizione di un SCS 38
4.4 Architettura di categoria A 39
4.5 Architettura di categoria B 39
4.6 Architettura di categoria C 40
4.7 Architettura di categoria D 40
5.1 Schema delle fasi di validazione di un SCS 42
5.2 Esempio di un albero dei guasti 43
6.1 Esempio di parametrizzazione di un SCS - il laser scanner 45
6.2 Modello a V di un software di livello 1 47
6.3 Modello a V di un software di livello 2 48
6.4 Piantina del modello preso come esempio 49
6.5 Uso dei moduli preprogettati nella programmazione 50
9.1 Esempio di attribuzione del SIL con più sottosistemi 59
9.2 Scomposizione del sistema in esame 61
9.3 Componenti e funzioni di ogni sottosistema in esame 61

Le seguenti derivano dalla norma EN IEC 62061: 2021 e sono state tradotte dall'inglese all'italiano

Figura 3.4
Figura 4.3
Figura 4.4
Figura 4.5
Figura 4.6
Figura 4.7
Figura 5.1
Figura 6.2
Figura 6.3
Figura 6.4
Figura 6.5
Figura 9.1
Figura 9.2
Figura 9.3

Elenco delle tabelle

4.1 Relazione tra gli indici delle cause di guasto di modo comune . . . 37
6.1 Report di validazione del software 52
8.1 Corrispondenza tra SIL e PL 55
9.1 Attribuzione numerica alla frequenza di esposizione al danno . . . 57
9.2 Attribuzione numerica alla probabilità di verifica di un evento pericoloso 57
9.3 Attribuzione numerica alla probabilità di limitare o evitare il danno 58
9.4 Attribuzione del SIL 58
9.5 Attribuzione del SIL attraverso HFT e SFF 58
9.6 Limitazione del SIL attraverso PFH 59
9.7 Attribuzione del SIL attraverso MTTF e DC 60
9.8 Specifiche di una funzione di sicurezza 62
9.9 Report di validazione 64

Tutte le tabelle elencate derivano dalla norma EN IEC 62061: 2021 e sono state tradotte dall'inglese all'italiano.