UNIVERSITÀ DEGLI STUDI
DI PADOVA

Dipartimento di Tecnica e Gestione dei Sistemi Industriali

Corso di laurea triennale in Ingegneria Meccatronica

Tesi di laurea
triennale

Progetto e realizzazione di un sistema di test delle funzioni di sicurezza

Project and realization of a system
to test security functions

Relatore
Prof. *Dainese Diego*

Laureando: Comunian Giacomo
Matricola: 1218768

Anno Accademico: 2022-2023

Sommario

Introduzione

La presente tesi ha lo scopo di analizzare e studiare il comportamento in caso di guasto di una macchina dotata di sistemi di sicurezza.
Si parte dallo studio delle normative per capire i requisiti essenziali di sicurezza che deve avere la macchina, si passa dunque alla progettazione della stessa per poi realizzare un modello pratico che ne simula il funzionamento. Attraverso questo prototipo, si eseguiranno una serie di prove per verificare la validità delle scelte progettuali eseguite e capire in caso di guasto come si comportano le funzioni di sicurezza della macchina.
Si analizza il rischio della macchina e si studia il grado di efficacia dei sistemi di sicurezza introdotti.

La tesi è composta da 6 capitoli:

- Nel capitolo 1 vengono spiegati i concetti chiave delle direttive e delle norme che verranno utilizzate nei capitoli successivi. Si analizzano nello specifico la direttiva 2006/42/CE (Direttiva Macchine), la norma CEI EN 60204-1 (Equipaggiamento Elettrico del Macchinario), la norma CEI EN 62061 (Sicurezza dei Sistemi di Comando) e la norma CEI EN 61131-3 (Standard per i Controllori Logici Programmabili).

- Nel capitolo 2 si introducono le componenti di sicurezza, come il PLC Safety e le barriere fotoelettriche di sicurezza. Si valuta il campo d'applicazione e le differenze rispetto alle componenti senza standard di sicurezza.

- Nel capitolo 3 si inizia ad affrontare un caso pratico che verrà poi completato nel proseguo dei successivi capitoli. In questo capitolo, come caso d'esempio, si tratta la progettazione di un prototipo di ascensore per automobili.

- Nel capitolo 4 si passa alla realizzazione del caso in esame, si affronta sia la parte hardware che la parte software.

- Nel capitolo 5 si studia il comportamento del macchinario in caso di guasto. Si valuta l'efficacia dei sistemi di sicurezza e delle ridondanze utilizzate.

- Nel capitolo 6 si studia il rischio della macchina, si introduce il concetto di PL e di SIL per poi passare al calcolo dello stesso nel caso in esame.

CAPITOLO 1

Introduzione a norme e direttive

Per far sì che ogni prodotto possa esser sicuro e non nuocere alla salute delle persone, l'Unione Europea tramite le direttive, impone una serie di requisiti che ogni prodotto deve rispettare per esser commercializzato in territorio europeo e per garantirne la libera circolazione. Fino a maggio del 1985 ogni paese decideva in modo autonomo quali caratteristiche dovesse avere un prodotto per esser venduto nel proprio territorio nazionale, facendo ciò il libero scambio dello stesso prodotto nei diversi paesi risultava molto complesso e prodotti ritenuti idonei in un paese risultavano pericolosi in un altro, mettendo così in difficolta i fabbricanti (con fabbricante definiamo colui che immette il prodotto nel mercato). Proprio per questo motivo dal 1985 si è passati al "nuovo approccio" in cui gli aspetti che regolano l'immissione dei prodotti nel mercato Europeo non è più basato su un metodo costruttivo, ma bensì sulle caratteristiche finali che deve aver tale prodotto. Queste caratteristiche sono le stesse per ciascun paese dell'Unione Europea. L'obbiettivo che un prodotto deve raggiungere per esser considerato sicuro viene dettato dalla direttiva, i parametri perché tale obbiettivo venga raggiunto vengono forniti dalla norma tecnica.

1.1 Le norme armonizzate

Le norme armonizzate a una certa direttiva, sono norme che se seguite passo a passo portano alla presunzione di conformità ai requisiti essenziali della direttiva stessa. Non è obbligatorio seguire le norme armonizzate, purché il fabbricante sia in grado di dimostrare che il proprio prodotto rispetti tutti i requisiti essenziali delle direttive a cui è soggetto. In questo caso nella documentazione tecnica il costruttore deve dimostrare la validità delle soluzioni adottate e il pieno raggiungimento dei RES (Requisiti essenziali di sicurezza).

Le norme armonizzate vengono create su mandato della commissione Europea dai vari enti di normazione, i quali possono avere competenza a livello nazionale, europeo o internazionale. Ogni ente di normazione ha inoltre competenza per uno specifico settore tecnico.

Enti normatori:

- Enti nazionali:
  - **UNI** Ente nazionale italiano di unificazione, si occupa delle norme di tutti i diversi settori.
  - **CEI** Comitato Elettrotecnico Italiano, si occupa delle norme nel campo elettrotecnico.

- Enti Europei:
  - **CENELEC** Comitato Europeo di Normazione Elettrotecnica, si occupa a livello europeo delle norme rivolte al settore elettrotecnico.
  - **CEN** Comitato Europeo di Normazione, si occupa a livello europeo delle norme di tutti i diversi settori.
  - **ETSI** Istituto Europeo per le norme di Telecomunicazione.

- Enti internazionali:
  - **ISO** Organizzazione Internazionale per gli Standard, è l'organizzazione di riferimento a livello mondiale per la definizione delle norme di tutti i vari settori.
  - **IEC** Commissione Elettrotecnica Internazionale, si occupa degli standard mondiali relativi al settore elettrotecnico.

Le norme inoltre si suddividono in tre categorie, dette di tipo A, B o C.

- Norme di tipo A: Contengono concetti fondamentali, principi di progettazione e aspetti generali applicabili a tutte le macchine.
- Norme di tipo B: Trattano un aspetto specifico della sicurezza, sono a loro volta suddivise in due gruppi:
  - B1 Riguardano aspetti particolari della sicurezza.
  - B2 Riguardano i dispositivi di protezione.
- Norme di tipo C: Trattano i requisiti di sicurezza per tipologia di macchina.

1.2 La marcatura CE

La certificazione di Conformità Europea attesta che il prodotto è conforme ai requisiti di sicurezza e salute previsti dalle direttive o dai regolamenti comunitari di pertinenza. La

marcatura CE, qui di seguito l'immagine, dev'essere apposta dal fabbricante o dall'importatore del prodotto (qualora il produttore sia extra Unione Europea). La marcatura dev'esser apposta solo su prodotti che abbiano la certificazione di Conformità Europea.

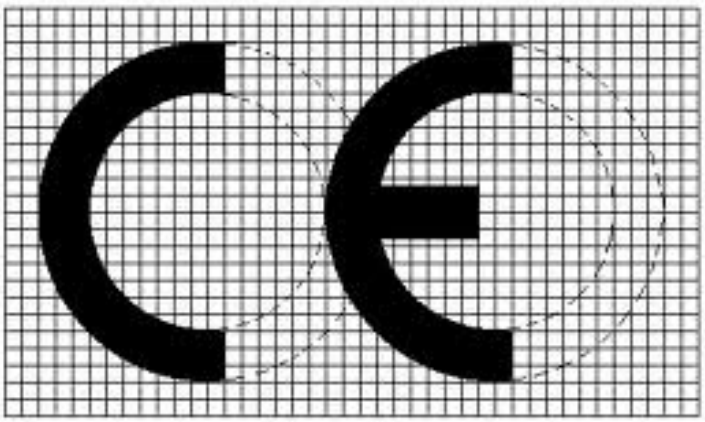


Figura 1.1 Simbolo marcatura CE

Ogni prodotto che è soggetto a determinate specifiche richieste dall'Unione Europea, può esser introdotto nel commercio Europeo solo se provvisto di certificazione; tuttavia è possibile produrre oggetti che non rispettano i requisiti richiesti dall'Europa, purché vengano venduti al di fuori del mercato europeo. Il fabbricante può in autonomia autocertificare la conformità del prodotto salvo in casi particolari, dove risulta obbligatorio rivolgersi ad organismi notificati, come ad esempio nel campo ATEX (ambienti ad atmosfera potenzialmente esplosiva).

Di seguito verranno analizzate le norme e le direttive applicate nel proseguo della tesi.

1.3 La Direttiva macchine 2006/42/CE

La direttiva macchine è una delle direttive più utilizzate in campo meccatronico, infatti è il testo di riferimento per tutte le macchine, quasi macchine e le componenti di sicurezza. Questa direttiva europea è stata recepita dall'Italia nel 2010 tramite il decreto attuativo 17/2010 anche sebbene fosse stata emanata dalla Comunità Europea già nel 2006.
Si definisce una macchina come *"un insieme equipaggiato di un sistema d'azionamento*

diverso dalla forza umana o animale diretta, composta di parti o componenti, di cui almeno una mobile collegati tra loro solidamente per un'applicazione ben determinata".
Per quasi macchine invece ci si riferisce a un insieme di parti e/o componenti che da soli non sono in grado di svolgere alcuna funzione in particolare e che per farlo necessitano di esser incorporati o assemblati ad altre macchine o quasi-macchine.

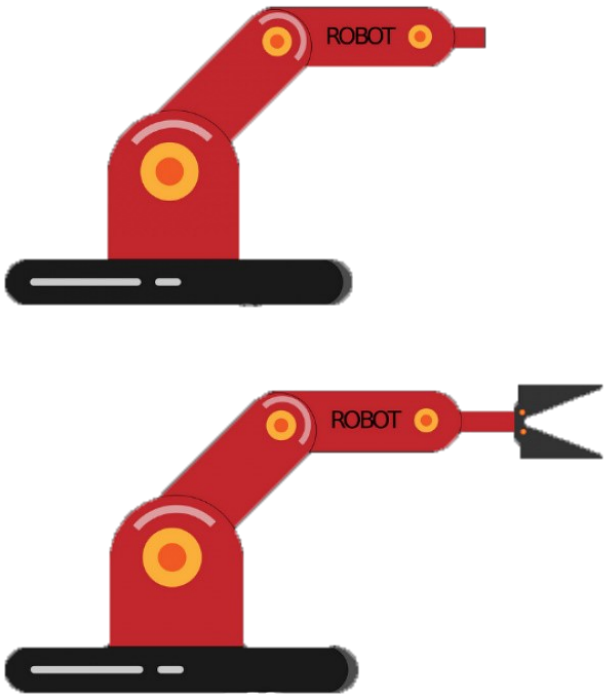


Figura 1.2 Distinzione macchina, quasi macchina

Un classico esempio per capire meglio la distinzione tra macchine e quasi macchine è rappresentato in figura 1.2. Il robot antropomorfo della prima immagine viene considerato una quasi macchina, in quanto da solo non è in grado di svolgere alcuna azione. Qualora invece gli venisse aggiunta una pinza allora avrebbe una funzione, diventando così una macchina a tutti gli effetti.
Le direttive e le normative che disciplinano le macchine e le quasi macchine sono le medesime, fare questa distinzione è importante perché gli obblighi del fabbricante cambiano in base al fatto che si tratti di una o dell'altra, cambia infatti l'iter certificativo di conformità ai RES.
Le macchine per esser immesse nel mercato a differenza delle quasi macchine, devono essere certificate CE. Inoltre ogni qualvolta si eseguano modifiche sostanziali alla macchina, bisogna eseguire nuovamente la marcatura CE, tranne nei casi in cui si stia

adeguando la macchina alle nuove normative, si stia sostituendo il quadro elettrico senza eseguire modifiche o per l'aggiunta di protezioni.
Nella direttiva troviamo inoltre un elenco di tutti i campi che esulano dalla sua competenza:

- Macchine a fine di ricerca
- Armi
- Giostre
- Veicoli
- Macchine che rientrano già in altre direttive

L'allegato 1 della direttiva macchine elenca tutti i requisiti essenziali di sicurezza (RES) che una macchina deve obbligatoriamente rispettare.
Nella fase di progettazione di ogni macchina bisogna innanzitutto procedere con una valutazione dei rischi che la macchina potrebbe creare, in modo da poter capire a quali RES la macchina deve sottostare.

1.4 Norma CEI EN 60204-1 Equipaggiamento Elettrico del Macchinario

Norma redatta da IEC a livello mondiale, successivamente rielaborata dal CENELEC trasformandola nella norma Europea EN 60204-1 per poi esser recepita dal CEI che la convertì in CEI EN 60204-1.
Questa norma si applica a tutti gli equipaggiamenti elettrici delle macchine non portabili a mano quando sono in moto, con tensioni inferiori a 1000V ac e 1500V dc con frequenze inferiori a 200Hz. La norma è armonizzata ai sensi della direttiva macchine (2006/42/CE) e della direttiva bassa tensione (2014/35/UE). Il rispetto di questa norma garantisce la conformità alle altre due direttive.
Stabilisce che il confine tra macchina ed equipaggiamento elettrico è il dispositivo di sezionamento della macchina (obbligatorio dai RES della direttiva macchine). La norma detta tutti quei parametri per la protezione dai pericoli elettrici e da tutti quelli correlati all'energia elettrica. Impone inoltre che un sistema tn-c non può essere utilizzato per un macchinario e che all'apertura del quadro elettrico bisogna che i dispositivi siano tutti con IP2x (protetto contro l'accesso delle dita) o superiore, altrimenti l'apertura del quadro dev'essere possibile solo quando il sezionatore risulta aperto.

1.5 Norma CEI EN 62061
Sicurezza dei Sistemi di Comando

La norma CEI EN 62061 è stata redatta da IEC a livello mondiale, successivamente rielaborata dal CENELEC trasformandola nella norma Europea EN 62061 per poi esser recepita dal CEI che la convertì in CEI EN 62061.
Questa norma non è armonizzata con la direttiva macchine, ma è usata come base per le norme di prodotto nel settore elettrico.
Un sistema di controllo, viene definito come: *"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".* I sistemi di comando con funzioni di sicurezza invece devono garantire inoltre un corretto e sicuro funzionamento sia durante il normale uso, che in situazioni di guasto.
La norma prevede che i sistemi di comando devono esser progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose:

- Devono resistere alle sollecitazioni e agli influssi esterni previsti.
- Un'avaria hardware o software non deve creare situazioni pericolose.
- Errori umani ragionevolmente prevedibili non creino situazioni pericolose.

La progettazione delle misure di sicurezza dev'essere fatta in cinque fasi:

- Fase 1: Analisi dei pericoli e valutazione dei rischi.
- Fase 2: Riduzione del rischio mediante mezzi di comando.
- Fase 3: Individuazione delle funzioni di sicurezza per le parti del sistema di comando legate alla sicurezza.
- Fase 4: Progettazione, sia hardware che software.
- Fase5: Convalida attraverso prove o/e analisi.

1.6 Norma CEI EN 61131-3
Standard per i Controllori Logici Programmabili

Norma di riferimento per i controllori programmabili, rappresenta il primo tentativo per creare uno standard di programmazione a livello mondiale nella programmazione industriale. Lo standard è basato sulla programmazione grafica, prevedendo cinque linguaggi di programmazione differenti che possono essere uniti tra loro:

- Ladder

- Sfc
- Instruction list
- Function block
- Structured test

Uno degli obbiettivi dello standard è anche quello di ridurre la varietà e l'ambiguità dei blocchi esistenti. Prevede due tipologie di software di sicurezza, i software di primo livello utilizzano solo blocchi presenti in libreria già preimpostati in cui si può intervenire solo sugli ingressi e le uscite degli stessi. I software di secondo livello invece sono più complessi, utilizzano un linguaggio a variabilità completa cioè oltre ai blocchi preimpostati, si possono utilizzare dei blocchi scritti dal programmatore.

CAPITOLO 2

Componenti di sicurezza

2.1 PLC Safety

Un PLC è un controllore a logica programmabile (Programmable Logic Controller), ha una serie di ingressi e una serie di uscite, tramite un software si è in grado di programmare lo stato delle uscite in base allo stato degli ingressi. Il PLC viene utilizzato principalmente nell'industria per il controllo e la gestione dei processi, tuttavia sta prendendo sempre più spazio anche nell'ambiente civile, come ad esempio nei sistemi domotici. Questo processore può essere programmato per svolgere tantissime funzioni e diverse tra loro. Qui di seguito è riportata un'immagine del PLC Logo della Siemens, ditta leader nel settore industriale per la produzione di PLC.

Figura 2.1 PLC non di sicurezza

Un PLC di sicurezza (PLC Safety) invece, è un particolare tipo di controllore progettato e certificato appositamente per garantire degli standard di sicurezza, così da soddisfare dei requisiti minimi imposti dalle direttive di sicurezza sul PL e SIL.
I PLC di sicurezza, come tutti gli altri dispositivi di sicurezza sono identificati dal colore giallo, in figura è riportato un esempio.

Figura 2.2 PLC Safety

Un problema dei PLC tradizionali riguarda i contatti delle uscite, trattandosi di uscite a relè può succedere che le lamelle dei contatti del relè si incollino tra loro, non garantendo quindi l'apertura dell'uscita quando la bobina non viene più eccitata. Questo fenomeno, può causare importanti problemi di sicurezza. Proprio per questo i PLC Safety a differenza dei normali processori usano uscite a transistor, in cui non ci sono movimenti meccanici che potrebbero causare malfunzionamenti.

Un PLC di sicurezza rispetto a uno non di sicurezza (PLC tradizionale) ha un costo più elevato. Il maggior prezzo è giustificato da una serie di accorgimenti (come quello delle uscite) ed a tutto un insieme di sistemi di ridondanza e autoverifica che un processore tradizionale non possiede, elementi che possono fare una sostanziale differenza in caso di guasto.

Un PLC di sicurezza a causa del suo costo spesso viene implementato nell'industria solo ove richiesto dalle normative anche se si potrebbe utilizzare in molti altri casi.

Un processore per essere considerato di sicurezza, dev'essere in grado di prevedere e gestire il 99% dei rischi possibili sul sistema, equivalente a un livello SIL3.

Il PLC Safety, prevede la possibilità di associare due porte di uscita hardware diverse per un singolo elemento logico d'uscita. Il PLC di sicurezza monitora continuamente gli ingressi e le uscite per rilevare eventuali anomalie. Ha la possibilità di caricare un nuovo software all'interno del processore senza variarne il funzionamento del programma in corso, e solo una volta terminato il caricamento chiede se si vuole procedere a interrompere il programma in run per far subentrare quello nuovo.

Il software di programmazione impedisce già in fase di scrittura del programma alcune logiche che potrebbero portare a delle problematiche, come ad esempio i loop.

Impedisce inoltre di lasciare dei blocchi con dei collegamenti logici vuoti, generando in fase di compilazione un errore.
Di seguito si affronta più nello specifico la programmazione di un PLC Safety della Pilz. La scrittura del programma, avviene tramite la programmazione di una serie di blocchi funzionali.

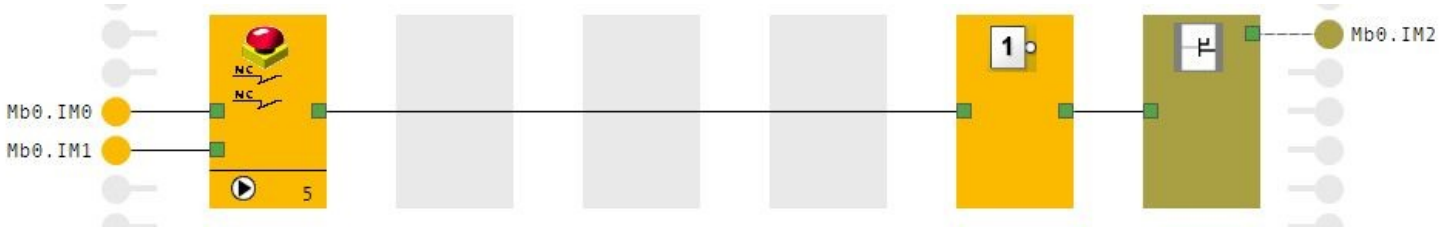


Figura 2.3 Esempio di programmazione

Nell'esempio riportato in figura, gli ingressi vengono rappresentati a sinistra e le uscite a destra. In questo caso si vede che gli ingressi IM_0 e IM_1 portano al processore il segnale di un arresto d'emergenza, il programma in questione è molto elementare, prevede che l'uscita IM_2 venga attivata con l'intervento del pulsante. Si è posta una porta logica NOT in serie, in quanto il segnale che proviene agli ingressi del processore è di tipo NC.

2.2 Barriere Fotoelettriche di sicurezza

Le barriere fotoelettriche di sicurezza sono dispositivi di protezione multi raggio. Questi dispositivi sono composti da un trasmettitore (TX) e da un ricevitore (RX) di raggi ad infrarossi, sono in grado di rilevare oggetti opachi (sopra una risoluzione R) nel caso questi attraversino il fascio di raggi. Quando l'oggetto attraversa la barriera, i raggi si interrompono in quell'area specifica, consentendo il rilevamento dell'oggetto.

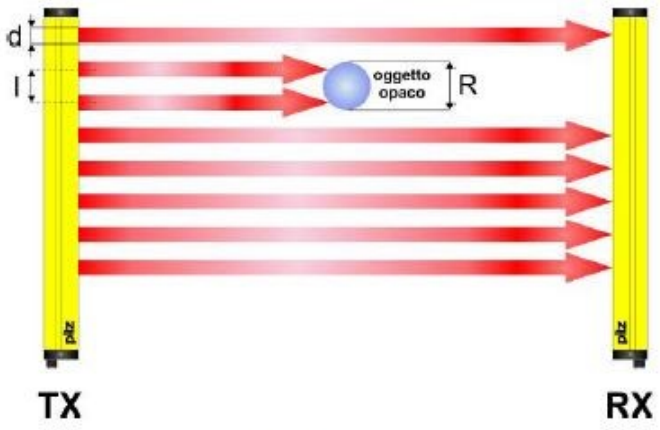


Figura 2.4 Funzionamento barriere fotoelettriche

Le barriere sono connesse direttamente al PLC Safety grazie a un connettore M12, ricevente e trasmittente non necessitano di esser connesse tra loro. Il trasmettitore per funzionare ha bisogno esclusivamente di un collegamento all'alimentazione di 24V dc. La ricevente invece oltre all'alimentazione (sempre in 24V dc) dispone di due uscite e di un ingresso di start. Le due uscite OSSD1 e OSSD 2 restituiscono un livello logico (a 24V dc) alto quando il fascio risulta continuo, mentre basso quando il fascio viene interrotto, dunque lavorano con una logica normalmente chiusa (NC). L'ingresso di start quando portato al livello logico alto, abilita le uscite al normale funzionamento, che altrimenti rimarrebbero sempre allo 0 logico.
Per risoluzione R dell'apparecchio, si intendono le dimensioni minime di un oggetto opaco per cui si è certi che venga rilevato dalle barriere, oscurando almeno un raggio del fascio. La risoluzione dipende esclusivamente dalle caratteristiche geometriche delle lenti, dall'interasse (i) e dal diametro (d). Grazie alla seguente formula siamo in grado di calcolare la risoluzione: R=d+i.
La risoluzione della barriera va scelta in funzione alla parte del corpo da proteggere, con una risoluzione di R=14mm si è in grado di proteggere il passaggio di un dito, con una risoluzione di R=30mm invece si è in grado di proteggere il passaggio di una mano.
Nel caso in esame si hanno a disposizione due diversi modelli di barriere fotoelettriche di sicurezza entrambe di marca Pilz:

- PSEN op2F
- PSEN op4F

La prima è in grado di rilevare il passaggio di oggetti con una dimensione maggiore o uguale a quella di una mano, mentre la seconda PSEN op4F è capace di rilevare oggetti

grandi quanto un dito o di dimensioni maggiori. Per i collegamenti in entrambi i casi si necessita di un connettore M12, che in base al modello e al fatto che sia ricevente o trasmittente deve aver 4, 5 o 8 pin.

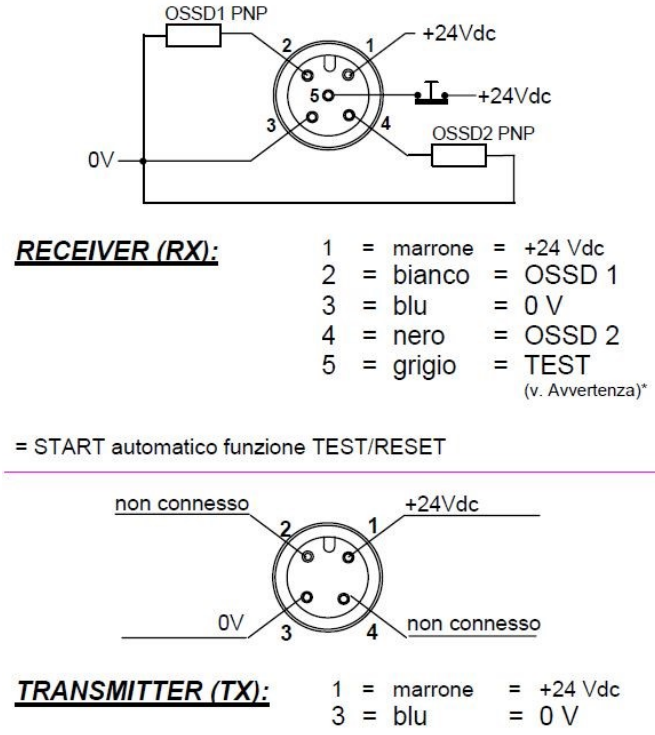
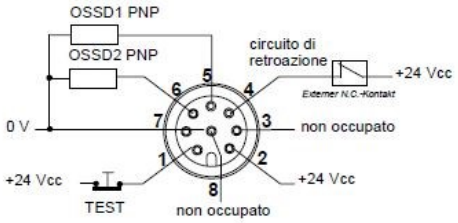


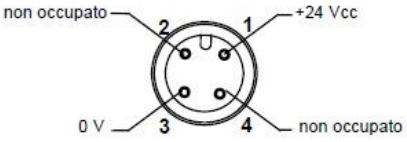
Figura 2.5 Schema collegamenti PSEN op2F

RECEIVER (RX):
Connettori M12, 8 poli



1 = bianco = TEST/START
2 = marrone =+24 Vcc
3 = verde = non occupato
4 = giallo = circuito di retroazione
5 = grigio = OSSD1
6 = rosa = OSSD2
7 = blu = 0 V
8 = rosso = non occupato

TRANSMITTER (TX):
Connettori M12, 4 poli



1 = marrone = +24 Vcc
2 = bianco = non occupato
3 = blu = 0 V
4 = nero = non occupato

Figura 2.6 Schema collegamenti PSEN op4F

CAPITOLO 3

Progettazione ascensore per automobili

Si vuole ora realizzare un esempio pratico, partendo dalla progettazione fino alla realizzazione di un prototipo equivalente alla macchina, valutando il grado di sicurezza raggiunto e analizzando il suo comportamento in caso di guasto.
In questo capitolo si analizza la fase di progettazione di un ascensore per automobili.

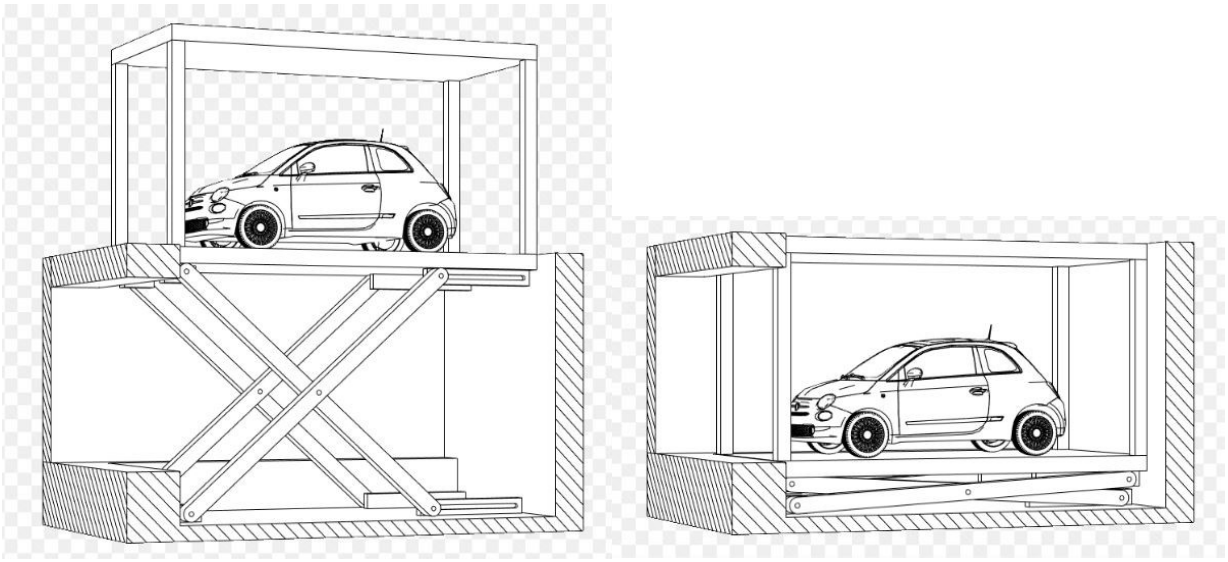


Figura 3.1 Funzionamento elevatore per auto

L'ascensore è a tutti gli effetti una macchina, in quanto è "*un insieme equipaggiato di un sistema d'azionamento diverso dalla forza umana o animale diretta, composta di parti o componenti, di cui almeno una mobile collegati tra loro solidamente per un'applicazione ben determinata".* L'ascensore dunque sarà soggetto alla direttiva macchine e dovrà obbligatoriamente rispettare tutti i requisiti essenziali dell'allegato 1 di sua competenza.

L'elevatore si muoverà tra due piani: piano terra (PT) e piano primo (P1). Per controllare il macchinario si ha una pulsantiera dotata di quattro pulsanti: uno per la salita (Sb_1), uno per la discesa (Sb_2), uno per l'arresto d'emergenza (Sb_0) e infine un pulsante (Sb_3) che

consente di dar il consenso alla macchina per partire la prima volta, dopo un'interruzione d'energia o a seguito di un arresto d'emergenza. Il pulsante della marcia dev'essere mantenuto premuto durante tutto il movimento del macchinario, in caso di rilascio del pulsante il macchinario si ferma. Non appena arrivati al piano il moto dell'elevatore, anche se il pulsante continua ad esser premuto, viene interrotto dai finecorsa di salita (FC_1, FC_2) o dai finecorsa di discesa (FC_3, FC_4).
Quando tramite il pulsante di riarmo (Sb_3) il macchinario ha ricevuto il segnale, accende la corrispondente luce blu (HH3) di consenso. In caso di interruzione dell'alimentazione bisogna nuovamente dargli il consenso, altrimenti anche se Sb_1 o Sb_2 vengono premuti il macchinario non esegue alcun movimento.
La macchina è dotata anche di due paia di barriere di sicurezza. Un paio si utilizzeranno per mettere in sicurezza l'ingresso al piano terra, mentre il secondo paio serviranno per mettere in sicurezza l'accesso al primo piano.

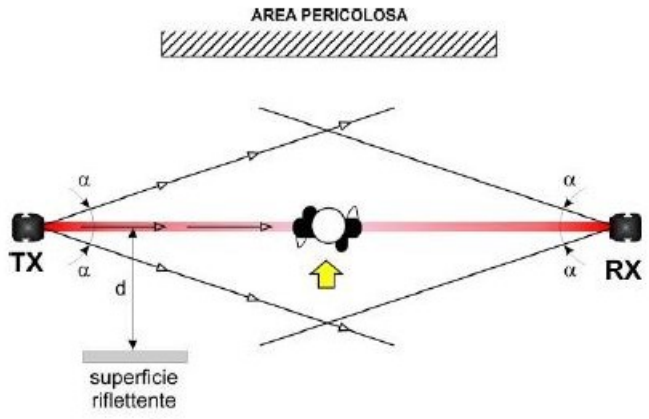


Figura 3.2 Raggio d'azione barriere fotoelettriche

Per il pulsante d'emergenza (Sb_0) si è deciso di utilizzare un pulsante a doppio contatto d'uscita a logica normalmente chiuso (NC). L'intervento del pulsante d'emergenza viene segnalato dalla corrispondente luce rossa (HH_0). Per terminare lo stato d'emergenza bisogna prima girare il pulsante d'emergenza in verso orario e successivamente dare nuovamente il consenso tramite il pulsante di riarmo.

Si ricorda inoltre che i finecorsa come i pulsanti d'arresto e le barriere fotoelettriche di sicurezza, lavorano in logica normalmente chiusi (NC), quindi a riposo equivalgono a un cortocircuito, viceversa quando intervengono equivalgono a un circuito aperto. Con

questa logica, in caso di malfunzionamento del dispositivo o d'interruzione del collegamento, ce ne si accorgere immediatamente e non come nel caso (NO) solo ad intervento dello stesso. Si rimanda alla lettura del capitolo 6 per una spiegazione più dettagliata.

Nei finecorsa, nelle barriere di sicurezza e nell'arresto di sicurezza si hanno due contatti che intervengono simultaneamente e che svolgono la stessa identica funzione ma in modo ridondante, dunque come si possono collegare al processore?

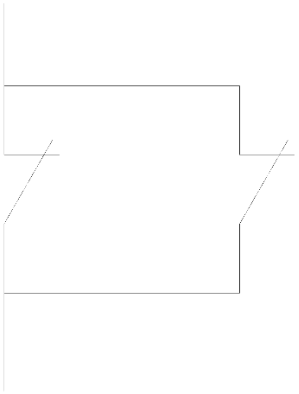


Figura 3.3 Contatti NC in serie
Figura 3.4 Contatti NC in parallelo

Se posti in serie il concetto della ridondanza verrebbe perso al primo guasto, il sistema potrebbe non sarebbe in grado di accorgersene continuando a funzionare. Invece se posti in parallelo il contatto non funzionante andrebbe ad interferire sul buon funzionamento del contatto funzionante, dunque il macchinario potrebbe creare gravi problemi di sicurezza. Proprio per questo motivo si è deciso di collegare tutti i contanti ridondanti su ingressi diversi del processore, e qualora restituissero due valori differenti, subito il processore è in grado di accorgersene, segnalando il guasto attraverso l'apposito indicatore luminoso (HH_1) di color giallo.
La normale marcia di salita o di discesa viene segnalata da un indicatore lampeggiante bianco (HH_2).
Per il macchinario si è scelto di utilizzare un motore trifase, il quale attraverso un'inversione di due fasi è in grado di cambiare il verso di rotazione.

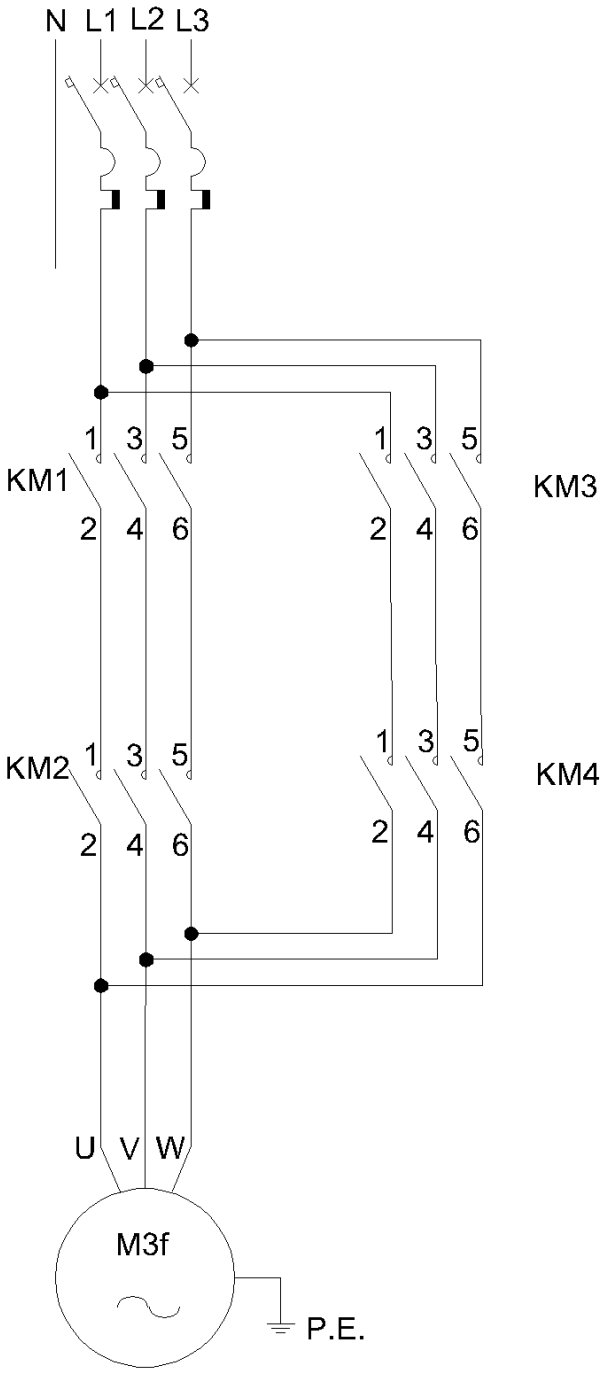


Figura 3.5 Schema di collegamento del motore

L'alimentazione al motore arriva tramite la chiusura dei teleruttori per la salita (KM_1, KM_2)

o per la discesa (KM_3, KM_4). I due teleruttori per marcia sono posti in serie, così da garantire l'apertura del circuito anche qualora uno dei due avesse le lamelle che si fossero incollate tra loro e creassero un malfunzionamento. Nella programmazione si è inserito un interblocco software tra i teleruttori della salita e quelli della discesa. Se questo interblocco non ci fosse, alla chiusura di tutti e 4 i teleruttori in contemporanea ci sarebbe un cortocircuito tra le fasi.

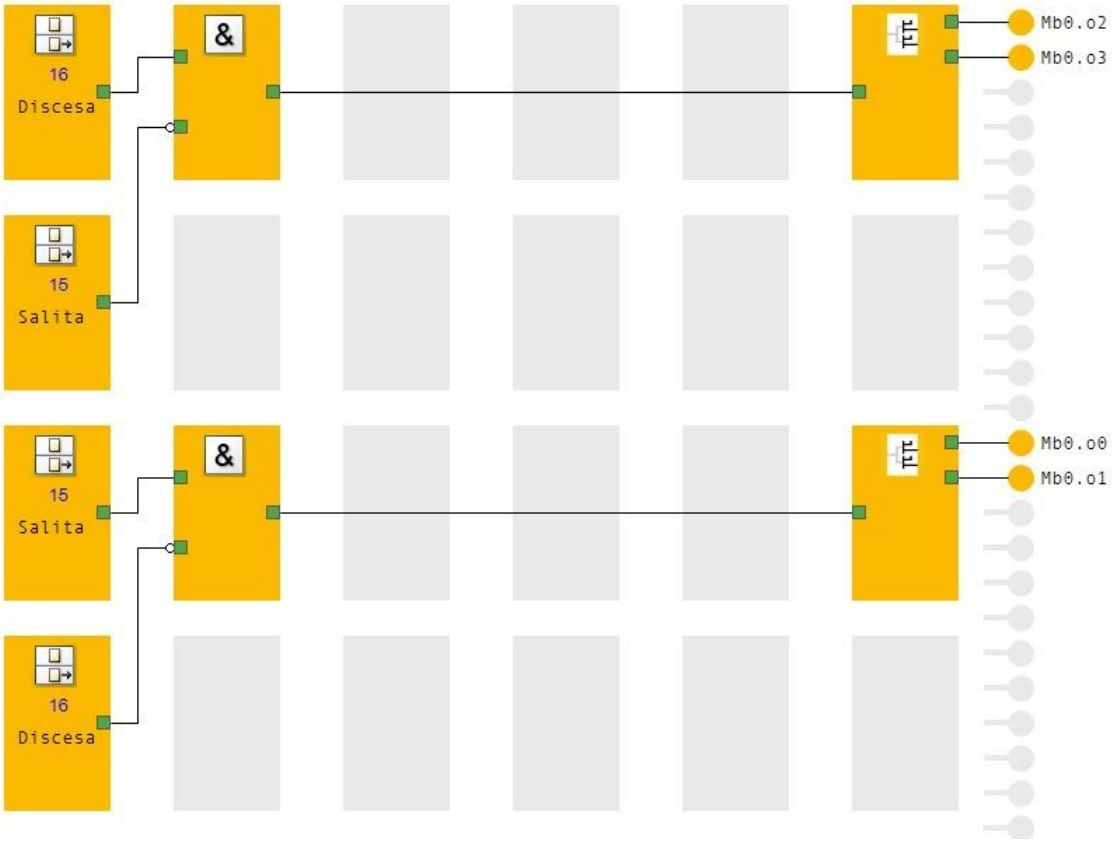


Figura 3.6 Interblocco teleruttori

Per una maggiore sicurezza si è deciso di aggiungere un secondo interblocco meccanico tra i teleruttori. Per realizzarlo si sono utilizzati i contatti ausiliari NC dei diversi teleruttori. L'alimentazione di KM1 è possibile solo se KM3 non è alimentato e viceversa, cosi come per i teleruttori KM2 e KM4.

Per il caso in esame, si è scelto l'utilizzo di un ascensore a pantografo. Il suo movimento è reso possibile grazie a dei pistoni a pressione, azionati da una pompa trifase (il motore sopra citato).

Figura 3.7 Funzionamento pistone - pantografo

Come scelta progettuale il quadro elettrico e la pompa per i pistoni sono stati posizionati a distanza dall'elevatore. La struttura mobile del macchinario dunque lavora con una bassissima tensione di sicurezza (24V dc) per l'alimentazione delle protezioni, dei pulsanti e delle luci di segnalazione. Ci troviamo dunque in categoria zero, pertanto la messa a terra è necessaria solo nel quadro elettrico e nel motore, ma non all'interno della parte mobile.

CAPITOLO 4

Realizzazione ascensore per automobili

In questo capitolo si è proceduto alla realizzazione di un prototipo che simula il funzionamento dell'ascensore. Si è partiti dalle nozioni del capitolo precedente per realizzarlo.

4.1 Realizzazione hardware

Si è deciso di controllare l'automazione tramite un processore Pilz, in particolare si è utilizzato il PNOZ M b0, si tratta di un PLC Safety.

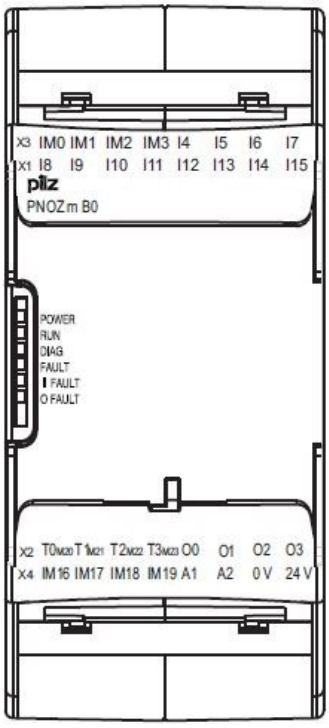


Figura 4.1 Pnoz M b0

Il processore è dotato di:

- 12 ingressi (I_4…I_{15})
- 4 uscite di sicurezza (O_0…O_3)
- 8 ingressi/uscite configurabili (IM_0…IM_3 – IM_{16}…IM_{19})
- 4 uscite ausiliarie ($T0_{M20}$, $T1_{M21}$, $T2_{M22}$, $T3_{M23}$)

Gli ingressi e le uscite sono tutte a 24V in corrente continua, l'alimentazione al processore arriva tramite i relativi pin (0, 24V), mentre l'alimentazione delle uscite arriva tramite altri due ingressi: A1 e A2 e dev'essere sempre a 24V dc.
Il processore è dotato di due morsetti aggiuntivi per l'alimentazione delle uscite in modo da tutelare l'alimentazione del processore da sbalzi di tensione. Questi sbalzi possono esser dovuti all'inserimento o al disinserimento di carichi importanti, che possono andare a danneggiare irreparabilmente il processore.

Il PLC Safety è dotato anche di uno schermo LCD e di alcuni led di segnalazione. Il display nel normale funzionamento mostra lo stato degli ingressi e delle uscite, qualora invece ci fosse un'anomalia mostra un messaggio d'errore, diverso in base al tipo di problema. Il processore ha anche delle spie led che segnalano il suo stato: power, run, diag, fault, ifault e ofault, segnalano inoltre eventuali anomalie insieme al display.

Per questa macchina si è deciso di configurare gli ingressi e le uscite nel seguente modo:

T_0= HH_0 Luce emergenza
T_1= HH_1 Luce anomalia
T_2= HH_2 Luce movimento
T_3= HH_3 Luce consenso

I_4= FC_1 Fine corsa salita n1 (NC)
I_5= FC_2 Fine corsa salita n2 (NC)
I_6= FC_3 Fine corsa discesa n1 (NC)
I_7= FC_4 Fine corsa discesa n2 (NC)
I_8= Sb_0 Pulsante d'emergenza contatto n1 (NC)
I_9= Sb_0 Pulsante d'emergenza contatto n2 (NC)
I_{10}= Sb_1 Pulsante salita (NO)

I_{11}= Sb_2 Pulsante discesa (NO)

I_{12}= Sb_3 Pulsante riarmo (NO)

I_{13}= BFT_1 Barriera di sicurezza PT contatto n2 (NC)

I_{14}= BFT_1 Barriera di sicurezza PT contatto n1 (NC)

I_{15}= BFT_2 Barriera di sicurezza P1 contatto n1 (NC)

IM_{16}= BFT_2 Barriera di sicurezza P1 contatto n2 (NC)

IM_{17}= CS_1 Consenso porta chiusa PT (NC)

IM_{18}= CS_2 Consenso porta chiusa P1 (NC)

IM_{19}= Nessun collegamento

O_0= KM_1 teleruttore salita n1

O_1= KM_2 teleruttore salita n2

O_2= KM_3 teleruttore discesa n1

O_3= KM_4 teleruttore discesa n2

$T0_{M20}$= Nessun collegamento

$T1_{M21}$= Nessun collegamento

$T2_{M22}$= Nessun collegamento

$T3_{M23}$= Nessun collegamento

Legenda:

NC= contatto normalmente chiuso

NO= contatto normalmente aperto

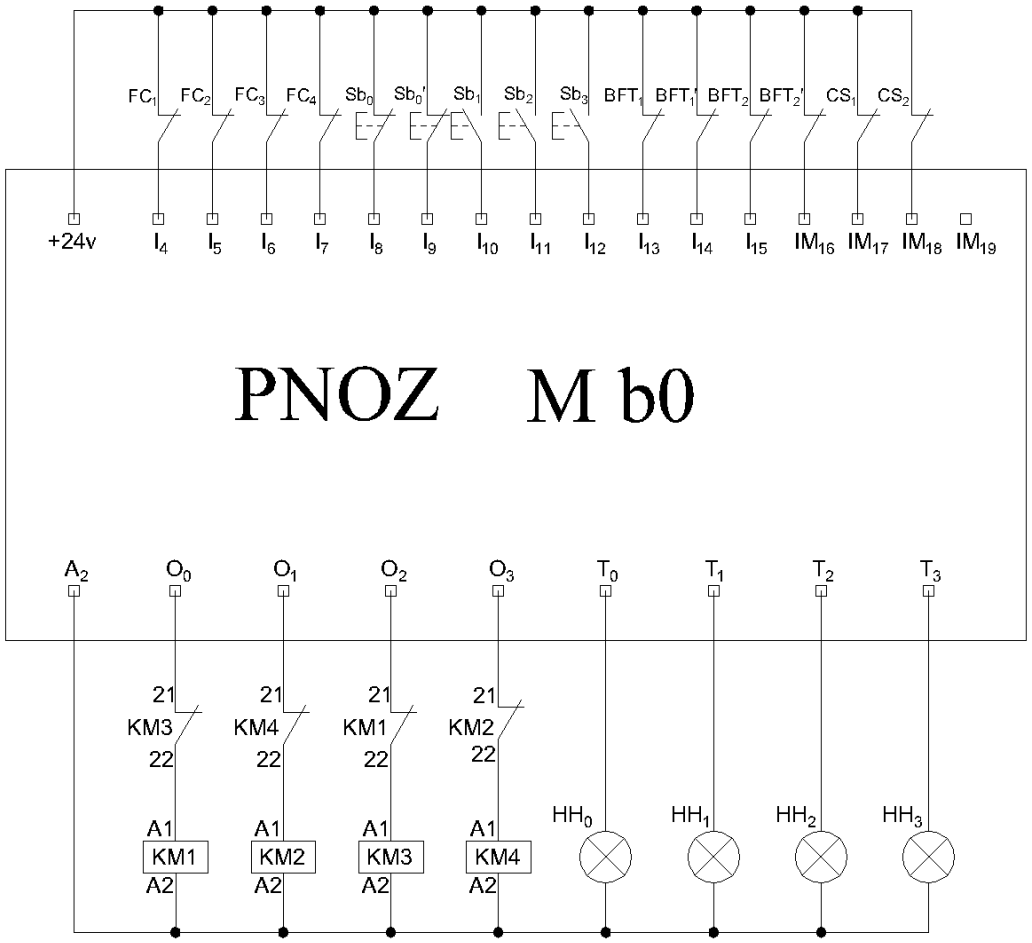


Figura 4.2 Schema collegamenti ingressi e uscite

Per mancanza d'ingressi e di uscite nel processore, si è deciso di considerare che l'apertura e la chiusura delle porte sia gestita da un altro sistema, il quale restituisce due segnali a logica NC che segnalano la completa chiusura delle due porte d'ingresso dell'ascensore (CS_1, CS_2). Qualora le porte non fossero chiuse, il movimento del macchinario verrebbe bloccato.

Si è realizzato su una base di compensato un modello equivalente all'ascensore, in cui sono presenti tutti i collegamenti degli ingressi e delle uscite del processore.

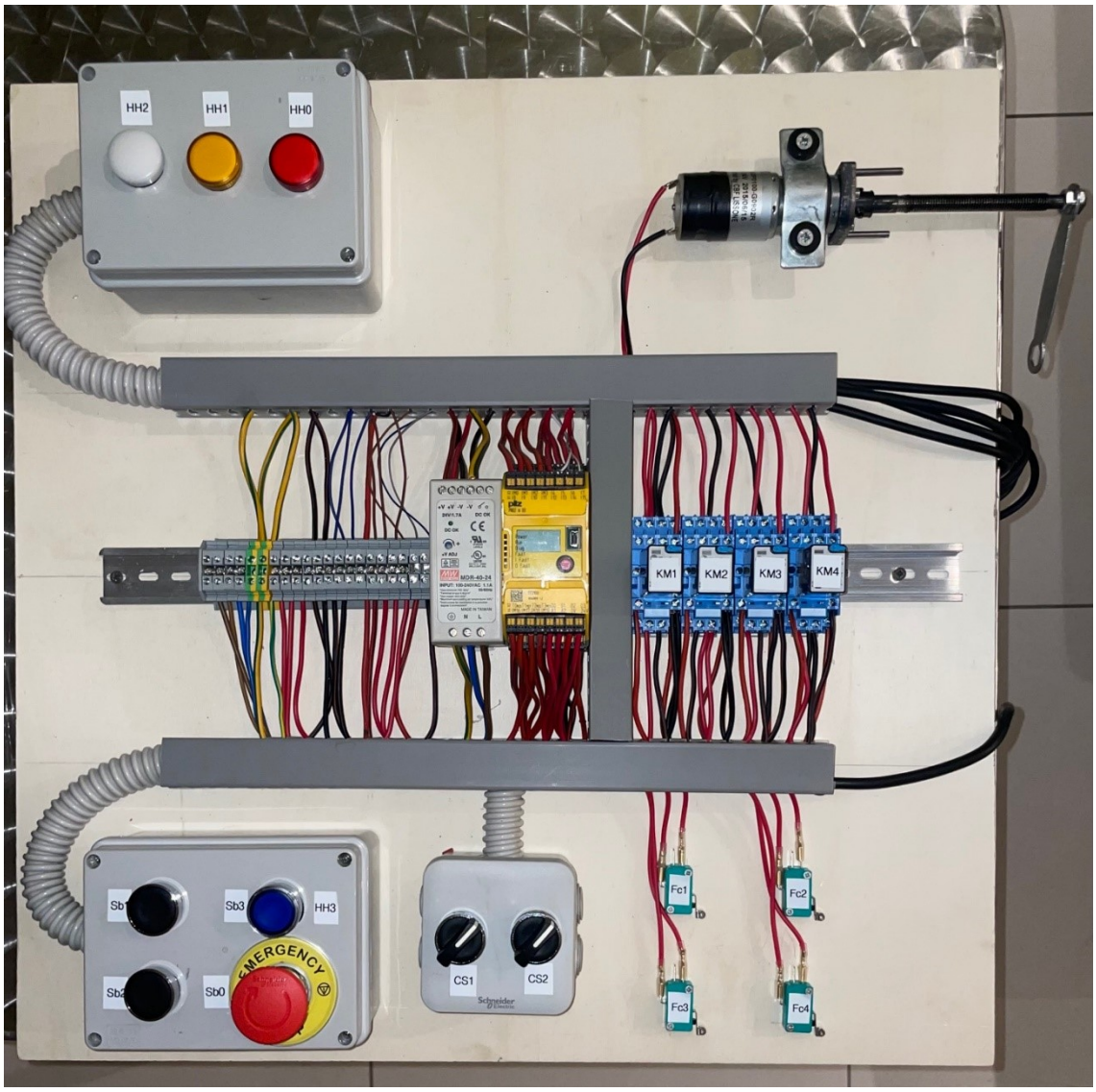


Figura 4.3 Realizzazione ascensore

Si è realizzato un supporto in legno a sostegno di tutte e 4 le barriere fotoelettriche di sicurezza.

Figura 4.4 Supporto barriere fotoelettriche di sicurezza

Le aste in legno del supporto devono essere perfettamente in linea e parallele tra loro, in modo che le barriere siano allineate, altrimenti anche se disallineate di qualche millimetro darebbero problemi nel funzionamento. Per far ciò si è utilizzata una bolla laser, un particolare tipo di bolla in grado di proiettare tramite un laser una perfetta linea orizzontale allineata con l'orizzonte e una linea perpendicolare ad essa.

Prima:

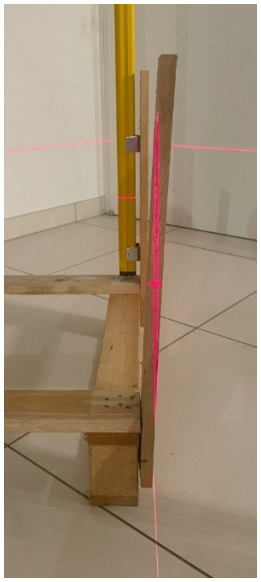


Figura 4.5 Raddrizzamento tramite bolla laser

Dopo:

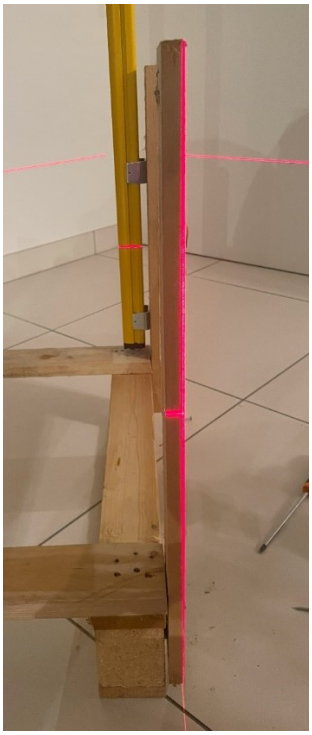


Figura 4.6 Raddrizzamento tramite bolla laser immagine 2

Trasmettitore e ricevitore delle barriere fotoelettriche 1 e 2, sono posizionati in modo alternato cosi che i ricevitori non ricevano i raggi trasmessi dal trasmettitore opposto. In questo caso non si sarebbe in grado di rilevare le interruzioni del fascio infrarossi.
Si è costruita una pulsantiera di comando contenente i tasti Sb1 (pulsante di salita), Sb2 (pulsante di discesa), Sb3 (pulsante di riarmo) e Sb0 (pulsante di emergenza). Sb3 è un pulsante luminoso, infatti è dotato al suo interno di HH3, la luce BLU che segnala il consenso.

Figura 4.7 Pulsantiera

Il modello è dotato di una seconda scatola contenente due interruttori che simulano il contatto d'ingresso in arrivo dalle porte relative al PT e al P1.

Figura 4.8 Consensi porte

Si è costruita una scatola contenente le tre luci di segnalazione, HH0 (spia di segnalazione di marcia), HH1 (spia di segnalazione anomalia) e HH2 (spia di segnalazione arresto d'emergenza).

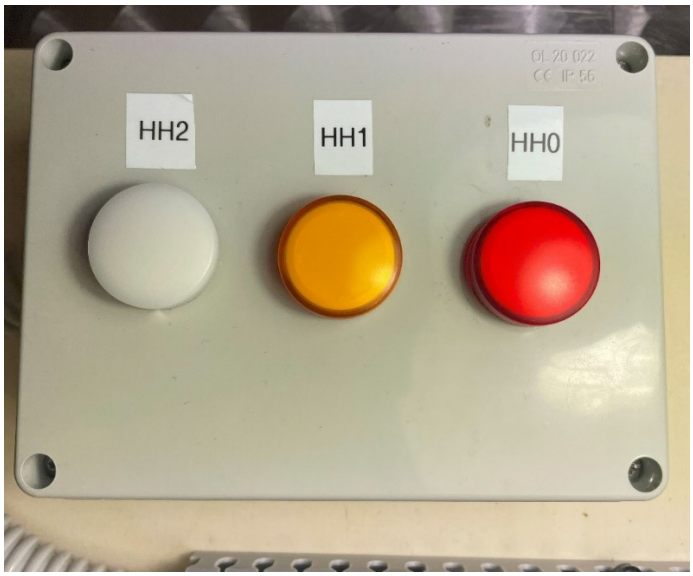


Figura 4.9 Spie luminose

I finecorsa sono stati collegati direttamente nel compensato, FC_1 e FC_2 sono i finecorsa per la salita, mentre FC_3 e FC_4 sono per la discesa.

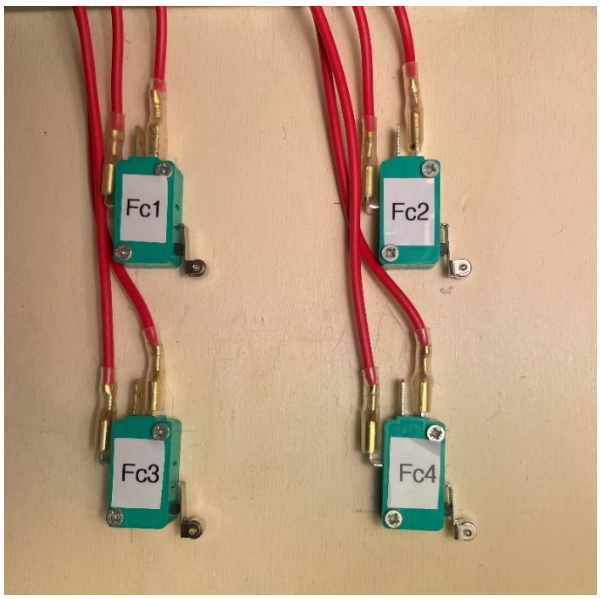


Figura 4.10 Finecorsa

Per simulare il motore trifase, si è usato un motore a 24V dc. Esso viene alimentato sempre grazie alla chiusura dei quattro teleruttori, i quali consentono anche il cambio di marcia grazie all'inversione delle due polarità.

Figura 4.11 Motore 24V dc

4.2 Scrittura del programma

Nella prima fase di programmazione, si definiscono tutti gli ingressi del PLC e si associano agli ingressi fisici. Sotto un esempio di come gli ingressi i13 e i14, corrispondono a due contatti di una barriera fotoelettrica di sicurezza. Per richiamarla nelle fasi successive della programmazione, si fa uso di riporti logici, in questo caso vediamo come il riporto numero 9 corrisponde alla barriera numero 1.

Figura 4.12 Associazione ingressi PLC

Un altro esempio di programmazione lo vediamo in figura 4.13, dove in questo caso si sta programmando la segnalazione dell'arresto d'emergenza. Si vede come al riporto della segnalazione di sicurezza (essendo un NC inseriamo una porta logica Not) viene associata l'uscita T_{0M20} (che tramite un timer ad impulsi, continua ad accendersi e spegnersi ogni 500 ms) e un messaggio nel display.

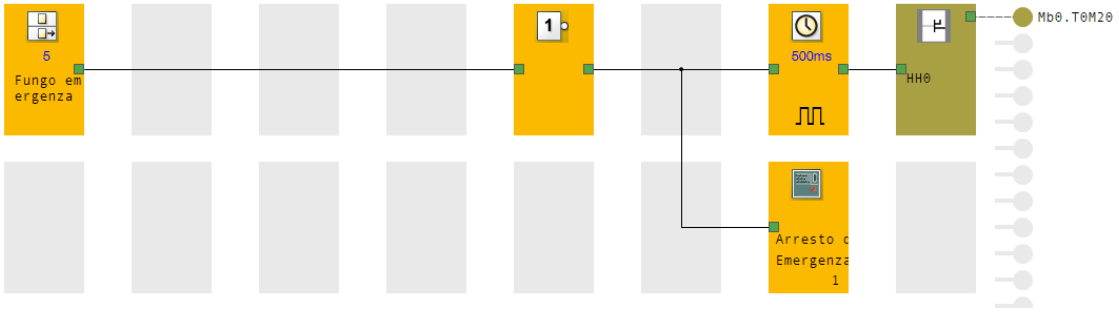


Figura 4.13 Ramo di programmazione

I messaggi nel display che sono stati programmati servono ad identificare meglio il tipo di anomalia o di emergenza rilevata dal processore. Nella figura 4.14 si vede come viene associato al display il messaggio numero 1: "Arresto d'emergenza".

ID	Messaggio
1	Arresto d'Emergenza
2	Errore FC Discesa
3	Errore FC Salita
4	Basculante P1 Aperto
5	Basculante PT Aperto
6	Errore BFT1
7	Errore BFT2
8	Errore arresto d'emergenza

Figura 4.14 Messaggi display

Figura 4.15 Display

Il software di programmazione quando connesso al PLC, consente di vedere in diretta lo stato logico degli ingressi, delle uscite e dei collegamenti tra essi. Si è usata questa modalità per eseguire una prima simulazione per verificare il buon funzionamento del programma. Nel capitolo successivo, si userà per entrare nelle logiche di programmazione e vedere come il software è in grado di rilevare gli errori.

Il progetto deve rispettare i RES (requisiti essenziali di sicurezza) della direttiva macchine. Infatti grazie alle scelte progettuali siamo in grado di affermare che:

- I sistemi di comando sono stati progettati e costruiti in modo da prevenire l'insorgere di situazioni pericolose.
  Si sono infatti usati tutti dispositivi di comando con certificazione CE, per tutti i sistemi di sicurezza si sono utilizzati sistemi a logica NC, in modo da prevenire eventuali malfunzionamenti.
- L'avviamento della macchina dev'essere possibile soltanto tramite un'azione volontaria di un operatore.
  Per avviare il macchinario è necessario che venga premuto il pulsante per armarlo e il movimento è permesso solo se viene mantenuto premuto tale pulsante (di salita o di discesa).
- Ogni macchina deve avere almeno un arresto d'emergenza.
  Nel caso in esame è il pulsante Sb0.
- Il comando d'arresto dev'essere prioritario rispetto ai comandi d'avviamento.
  Il rispetto di questo RES si è eseguito a livello software, infatti qualora il pulsante d'arresto venisse premuto, il movimento del macchinario non è consentito.
- Le misure di sicurezza devono eliminare ogni rischio durante l'esistenza della macchina.
  Grazie alle barriere fotoelettriche e alle porte d'ingresso e d'uscita, siamo in grado di garantire che il macchinario non rappresenta rischi di schiacciamento.
- I dispositivi di comando devono essere chiaramente visibili ed individuabili.
- Il macchinario deve aver mezzi che consentano di evitare che una persona possa esser rinchiusa dentro o se ciò fosse possibile, di mezzi per chiedere aiuto.
  L'utilizzo del macchinario non prevede la possibilità di movimento con persone all'interno. La pulsantiera di comando è stata appositamente posta al di fuori di esso in modo da garantire ciò. Quando il macchinario è fermo a un piano, le porte dello stesso piano rimangono aperte fino a che non venga premuto il pulsante di discesa o di salita.
- La macchina dev'essere munita di dispositivi che consentono di isolarla da qualsiasi fonte d'energia e devono poter esser bloccati sulla posizione di aperto. L'eventuale energia residua o immagazzinata dopo l'isolamento della macchina deve poter essere dissipata senza rischio per le persone.
  Questo RES lo possiamo considerare soddisfatto grazie al magnetotermico

posto sulla terna trifase d'ingresso. Non sono previste altre fonti d'energia al di fuori di quella elettrica. Dopo il sezionamento non sono presenti dispositivi in grado d'accumulare carica elettrica.

- Gli elementi accessibili della macchina devono essere privi di angoli e spigoli vivi.

Questi sono i principali RES dell'allegato 1 della direttiva macchine, che riguardano il caso in esame. Ogni macchinario che non rispetti i RES è da considerarsi difettoso.

CAPITOLO 5

Test delle funzioni di sicurezza in caso di guasto di un componente

In questo capitolo si vuole studiare il comportamento della macchina in caso di guasto. Si valuta l'efficacia dei sistemi di sicurezza e delle ridondanze utilizzate.

Le immagini sotto riportate sono delle istantanee del software di programmazione, si è utilizzata la modalità di visualizzazione degli ingressi e delle uscite in diretta. Il collegamento è di color verde quando lo stato logico è "HIGH", nero quando lo stato logico è "LOW".

Si analizza ora il comportamento dei singoli componenti del prototipo e se ne simula un guasto.

Guasto dei finecorsa:

I finecorsa lavorano in logica NC. Un eventuale guasto nel collegamento del finecorsa viene visto dal sistema come se il finecorsa stesso fosse intervenuto, dunque impedendo il movimento nella direzione in cui si è rotto. Il moto nella direzione opposta invece risulta ancora possibile, in quanto il mal funzionamento di un finecorsa non pregiudica il buon funzionamento di quelli nell'altra direzione.

Per garantire l'affidabilità del finecorsa si può installarne uno a doppio contatto, così qualora uno dei due contatti a seguito di un guasto non funzionasse, comunque l'altro riuscirebbe a garantirne l'affidabilità. Si può avere il medesimo risultato anche utilizzandone due diversi per ogni livello di arrivo dell'ascensore. Nel caso in esame si è preferito implementare il secondo metodo, realizzando il medesimo concetto di ridondanza.

Solitamente per aumentare il grado di sicurezza del macchinario, si prendono dei finecorsa che funzionano con tecnologie differenti, ad esempio un finecorsa di tipo magnetico e uno di tipo meccanico, in modo tale che un qualsiasi problema di tipo magnetico non vada a disturbare o inibire il buon funzionamento di entrambi contemporaneamente.

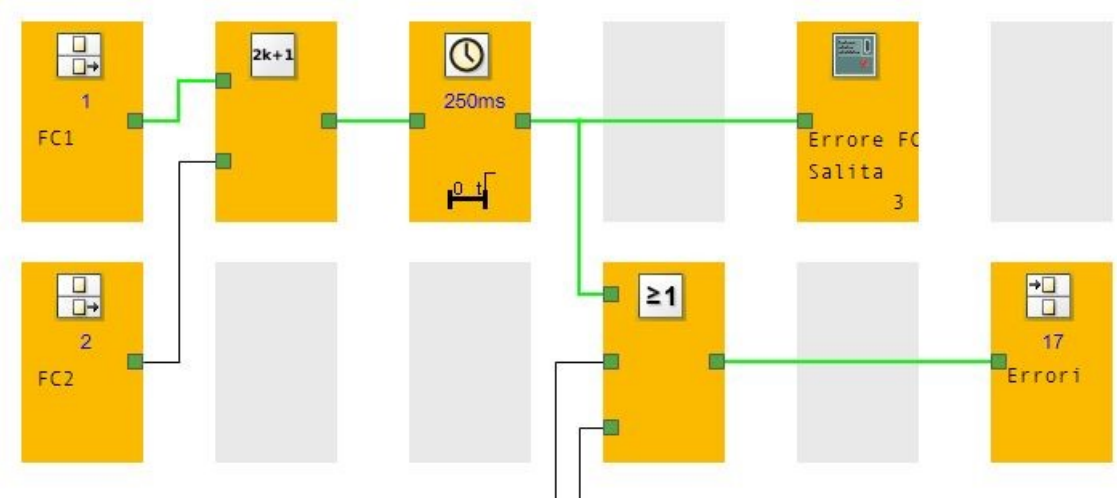


Figura 5.1 Guasto finecorsa

In figura 5.1 è riportato un esempio di malfunzionamento dei finecorsa, in cui FC1 risulta a riposo mentre FC2 è intervenuto. Questa situazione si può verificare a seguito di tre diversi guasti: (i) quando c'è un guasto nel collegamento di FC2, (ii) quando le lamelle di FC1 sono rimaste incollate tra di loro e FC1 è intervenuto oppure (iii) quando le lamelle di FC2 si son rotte nella posizione di aperto ed FC1 risulta a riposo.
Il blocco in figura segnato come 2k+1 è un XOR, restituisce un valore logico HIGH solo quando lo stato degli ingressi non coincide, come si può notare dalla tabella di verità sotto riportata.

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Tabella 5.1 Tabella di verità XOR

Si è posto inoltre un elemento di ritardo sulla segnalazione dell'errore, che serve per

togliere quelle minime non idealità sulla contemporaneità dell'intervento dei finecorsa, l'errore deve quindi persistere per un tempo superiore a 250ms perché venga avviata la segnalazione di guasto. L'errore viene segnalato dal display e dalla relativa spia HH1 (Luce anomalia).

Guasto dell'arresto d'emergenza:

Qualora si verificasse un guasto nel collegamento dell'arresto d'emergenza, dovuto ad esempio a un contatto allentato o a un cavo interrotto, il PLC immediatamente entra in emergenza, come se fosse stato premuto il pulsante.

Il pulsante d'arresto d'emergenza è provvisto di due contatti d'uscita, è stato progettato in modo che se le lamelle di un contatto rimanessero incollate tra loro, il secondo contatto sarebbe ugualmente capace di aprire il circuito.

Al processore sono state assegnati due diversi ingressi per i due contatti del pulsante d'emergenza (I_8, I_9), il programma è stato progettato in modo tale che al primo dei due contatti che passa allo stato logico LOW (logica NC) il PLC entra in emergenza. Qualora i due contatti presentassero uno stato discorde tra loro (Figura 5.2), oltre ad accendere la spia rossa dell'arresto d'emergenza, viene accesa anche la segnalazione del guasto. Per capire meglio di che guasto si tratta, il display mostrerà un messaggio d'errore che dettaglierà in maniera più esaustiva l'allarme.

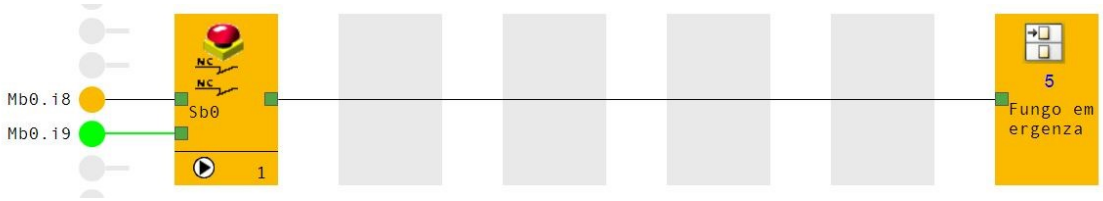


Figura 5.2 Guasto pulsante emergenza

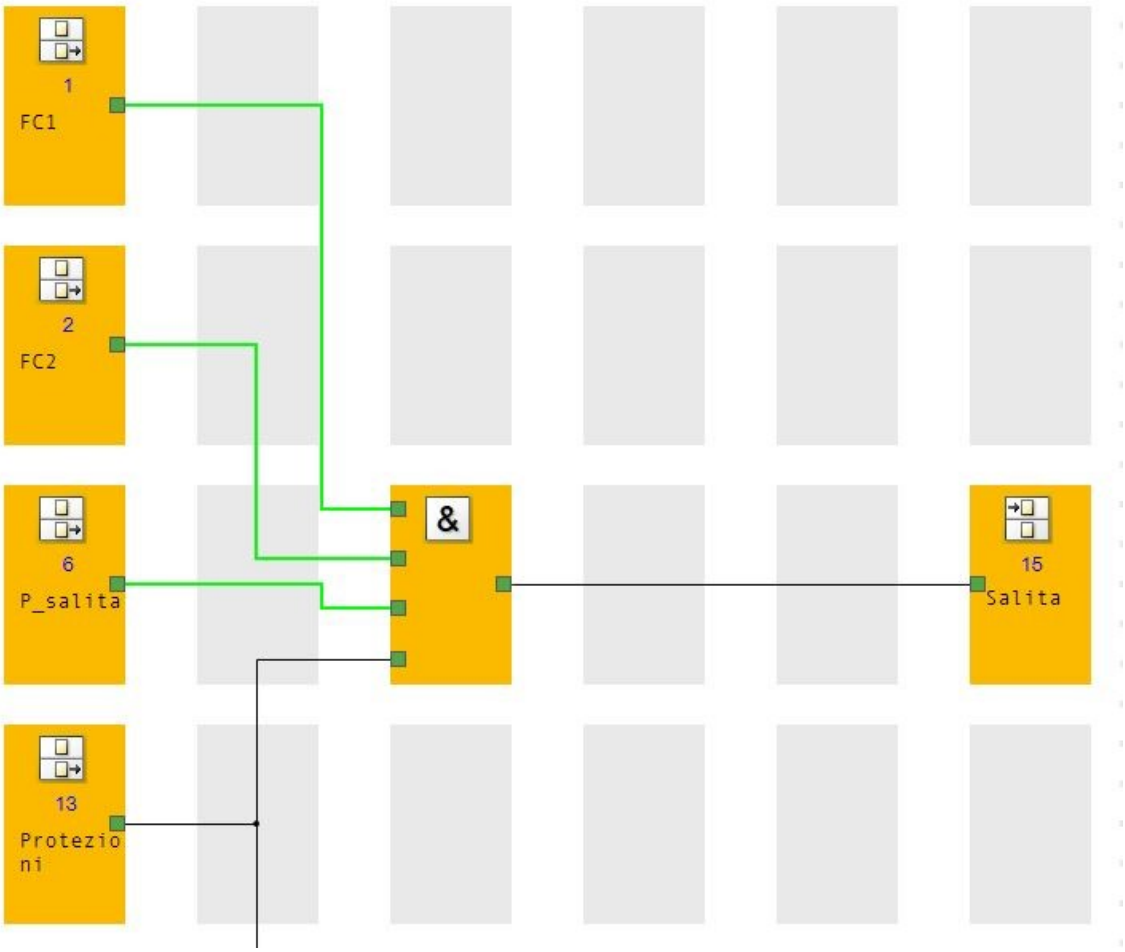


Figura 5.3 Guasto arresto d'emergenza

Dalla figura si vede come anche se il pulsante di salita è premuto, il movimento viene impedito dall'intervento delle protezioni.

Guasto dei pulsanti di salita, discesa e riarmo:

In questo caso non si è interessati ad avere ridondanza o un grado elevato di affidabilità, in quanto non svolgono funzioni di sicurezza. Il loro mal funzionamento non può comportare un pericolo per le persone o per il macchinario stesso, bensì può comportare il non funzionamento.

Il processore non è in grado di rilevare il guasto di uno di questi componenti, sarà l'operatore ad accorgersene quando il macchinario resta fermo.

Si può avere una ridondanza anche per questi componenti per evitare i fermi macchina, evitando così perdite in termini economici. Bisogna fare un'analisi dei costi benefici per

capire se effettivamente ha senso introdurre dei pulsanti NO a doppio contatto. Ciò comunque andrebbe a ridurre i fermi macchina ma non ad eliminarli completamente, in quanto sarebbe in grado di bypassare i guasti dovuti ai contatti che non si chiudono, ma non ai guasti dovuti alle lamelle che rimangono incollate tra loro.

Guasto barriere fotoelettriche di sicurezza:

Anche le barriere fotoelettriche di sicurezza quando sono a riposo presentano un'uscita con un valore logico HIGH, mentre quando il fascio viene interrotto l'uscita si porta a uno zero logico, il quale arresta il moto dell'elevatore. Si è dunque in grado di rilevare immediatamente ogni eventuale problema nel collegamento, in quanto al primo errore in uno dei due collegamenti, il moto dell'elevatore viene subito bloccato, segnalando nel display l'intervento delle barriere.

Le barriere utilizzate sono certificate CE per essere di sicurezza, ciò vuol dire che al loro interno sono provviste di sistemi di autoverifica che ad intervalli di tempo autoverificano il loro buon funzionamento e in caso di anomalie, portano le uscite OSSD1 e OSSD2 allo stato logico LOW.

Guasto segnale chiusura porte:

Se il collegamento in arrivo di consenso delle porte chiuse fosse interrotto, il macchinario non potrebbe muoversi, in quanto anch'esso come tutti gli altri sistemi di sicurezza funziona a logica NC.

Guasto teleruttori uscita:

Nella progettazione delle uscite si è fatta molta attenzione al garantire l'arresto anche in caso di guasto di un componente. Si sono posti in serie due teleruttori per ogni senso di marcia, in modo che se per un guasto uno dei due non dovesse interrompere l'alimentazione al circuito interverrebbe il secondo.

Un guasto sulle uscite del processore viene immediatamente segnalato tramite il display e l'apposito led. I teleruttori sono posti nelle uscite di sicurezza del processore, le quali sono provviste di sistemi di ridondanza all'interno del PLC che ne garantiscono il buon funzionamento.

Si è scelto di usare due uscite diverse del processore in modo tale che se un'uscita per un guasto rimanesse alimentata, il secondo teleruttore sarebbe in grado di togliere l'alimentazione al motore.

Se invece si fosse voluto garantire la continuità del servizio, rispetto all'affidabilità, i due teleruttori si dovevano mettere in parallelo.
Se i teleruttori venissero alimentati tutti insieme si verificherebbe un cortocircuito tra le fasi, andando a danneggiare il motore e il macchinario stesso, per evitare ciò si è posto un interblocco software e uno hardware (con interblocco si intende un blocco che impedisce l'alimentazione di un teleruttore quando n'è alimentato un altro dell'altro ramo).
Agendo sul pulsante di test azzurro posto in cima al teleruttore, evidenziato in figura 5.4 si possono chiudere i contatti d'uscita del teleruttore in modo manuale, andando a bypassare la bobina di alimentazione. Si può capire che un teleruttore è alimentato grazie al quadratino rosso evidenziato in figura 5.4.

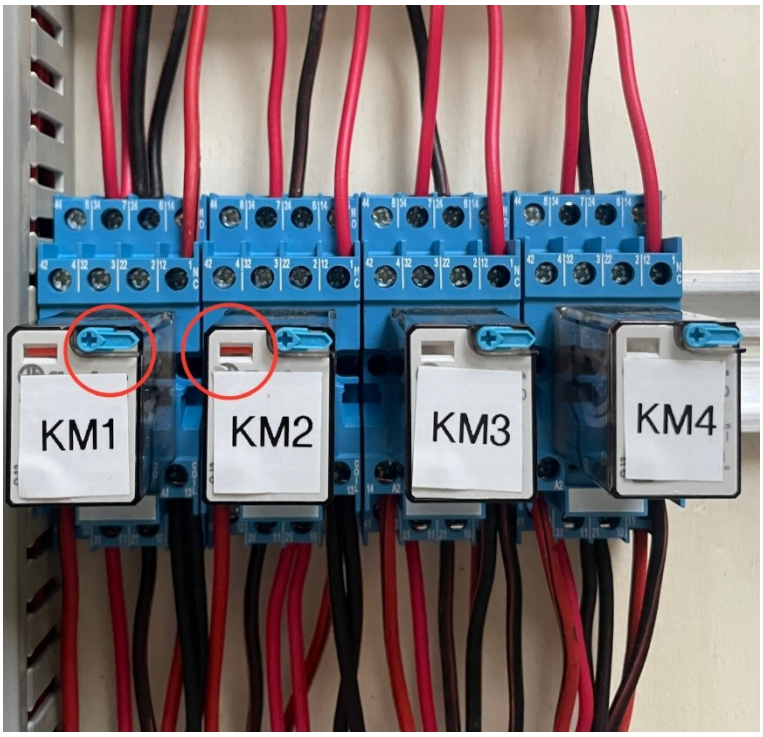


Figura 5.4 Teleruttori accesi

Si vuole ora simulare il guasto di un teleruttore in cui i contatti rimangono incollati tra loro. Grazie a un cacciavite andiamo ad agire sul pulsante di test di KM1 per alimentarlo, avendo posto i due teleruttori in serie, vediamo come il movimento del motore è impedito da KM2. Bisogna prestare molta attenzione quando si va ad alimentare in modo manuale i teleruttori, in quanto si vanno a bypassare tutti gli interblocchi posti.

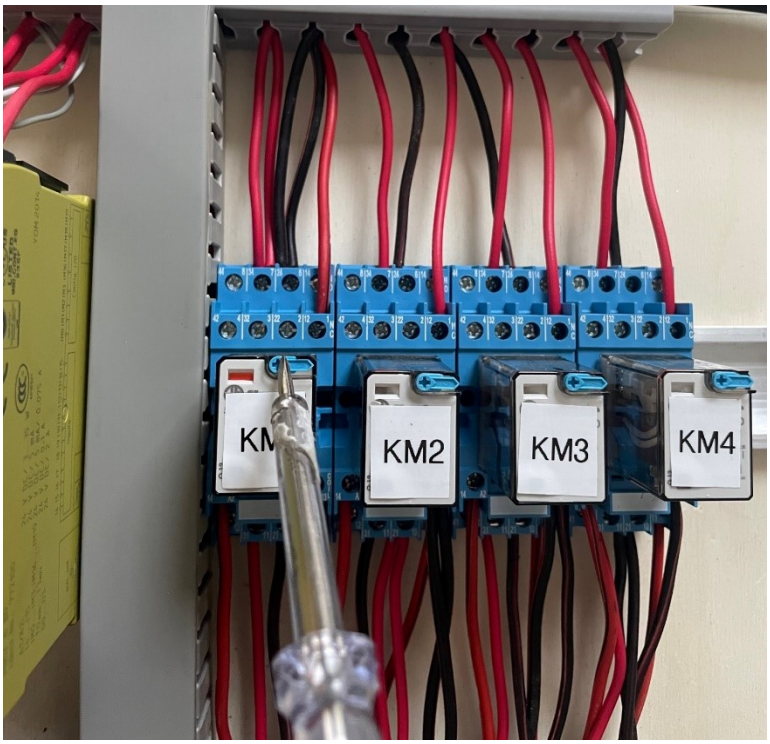


Figura 5.5 Guasto teleruttori

In caso di black out sull'alimentazione in ingresso, l'intero macchinario si ferma per mancanza di alimentazione. Quando l'alimentazione viene fornita nuovamente, il macchinario non parte in maniera incontrollata, ma bensì aspetta il consenso tramite il pulsante Sb_3.

CAPITOLO 6

Grado PL e grado SIL

Nella fase di progettazione di una macchina, bisogna ridurre il più possibile il rischio che può generare. Con il termine rischio, si valuta la combinazione di due fattori, la pericolosità e la gravità di un danno che la macchina può provocare; la pericolosità rappresenta la probabilità che si verifichi, mentre la gravità indica la serietà delle conseguenze.

In base ai rischi della macchina, si implementano dei circuiti con funzioni di sicurezza volti ad eliminarli o ad attenuarli. La valutazione del rischio di un macchinario avviene tramite la norma EN ISO 13849-1, la quale consente di determinare il PL (Performance Level) e la norma EN 62061 che consente di calcolare il SIL (Safety Integrity Level), ovvero il livello d'integrità della sicurezza. Il PL e il SIL sono due indici che ci consentono di valutare il livello di sicurezza di un macchinario, le due scale valutano il livello di prestazione di una funzione di sicurezza, ognuna ha un PL (o SIL) indipendente dall'altra, non esiste un PL o SIL globale della macchina.

Una funzione di sicurezza è una funzione che ha il compito di proteggere la macchina stessa o le persone nelle aree limitrofe.

Utilizzare una scala o l'altra è indifferente, esistono delle tabelle di conversione.

La scala del PL va da un valore "A", corrispondente ad un livello di sicurezza basso, fino ad arrivare ad un valore "E", corrispondente ad un livello massimo di sicurezza. SIL invece presenta 4 livelli d'integrità della sicurezza, con una scala da uno a quattro che rappresenta il maggior livello di sicurezza.

PL	**SIL**
A	Nessuna corrispondenza
B	1
C	1
D	2
E	3

TAB 6.1 Conversione PL-SIL

Scala PL:

- Livello A: è il livello più basso del PL.
- Livello B: possono essere realizzati mediante architetture a canale singolo senza monitoraggio.
- Livello C: possono essere utilizzate architetture a canale singolo senza monitoraggio con componenti ben collaudati.
- Livello D: Devono essere utilizzati principi di monitoraggio ed eventualmente anche di ridondanza.
- Livello E: si utilizzano circuiti ridondanti e monitorati.

Per capire che componenti bisogna utilizzare per la costruzione della macchina si deve capire che PL si deve raggiungere, tale livello viene identificato come PL-Richiesto (PL_R). Per calcolarlo si parte analizzando il problema, si deve capire la gravità della lesione che può provocare, la frequenza, il tempo d'esposizione al pericolo e qual è la probabilità di evitare o limitare il danno. Partendo dal punto 1 di figura 6.1 si sceglie:

S1= Bassa gravità lesione.
S2= Alta gravità lesione.
F1= Bassa esposizione al pericolo.
F2= Alta esposizione al pericolo.
P1= Alta probabilità di evitare la lesione.
P2= Bassa probabilità di evitare la lesione.

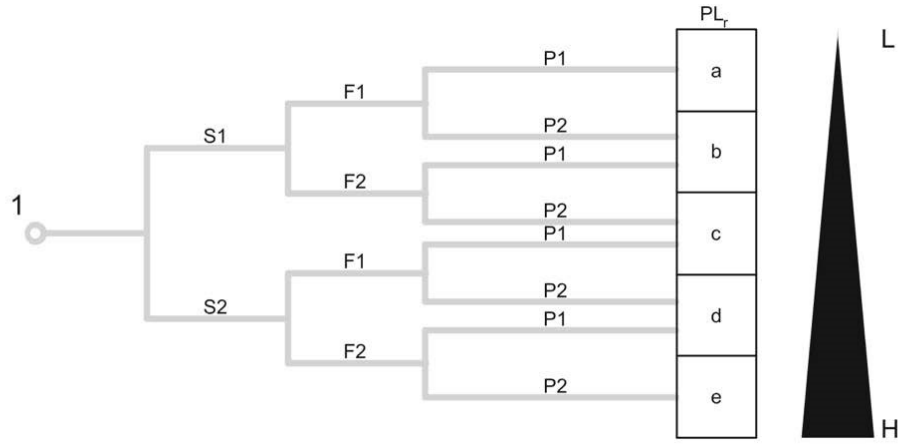


Figura 6.1 Calcolo PL_r

La macchina presenta PL_R diversi per ogni funzione di sicurezza, non esiste un PL_R generale. Dunque una certa funzione di sicurezza deve avere PL pari almeno al PL_R, si può ovviamente avere un grado superiore di sicurezza.
In una macchina in cui si ha un PLC di sicurezza, anche il software dovrà rispettare i requisiti di sicurezza, dovrà essere scritto rispettando le procedure date dalla norma. Il software non si può guastare ma può presentare degli errori, la norma prevede di adottare una scrittura che permetta di minimizzarli.

Le componenti di sicurezza hanno inoltre una categoria di sicurezza che ne identifica l'affidabilità:

- Categoria B: Componente base, sopporta sollecitazioni meccaniche.
- Categoria 1: Ha componenti ben provati.
- Categoria 2: Ha un controllo periodico delle funzioni di sicurezza.
- Categoria 3: Un'avaria non comporta la perdita delle funzioni di sicurezza.
- Categoria 4: Varie avarie non comportano la perdita delle funzioni di sicurezza.

Ogni categoria ha un range di PL a cui può corrispondere, in base al DC (copertura diagnostica del sistema) e al fatto che i componenti siano poco affidabili, affidabili o molto affidabili (rispettivamente verde, giallo o arancione nella figura 6.2). Grazie a questo grafico si è in grado di determinare il corrispondente PL.

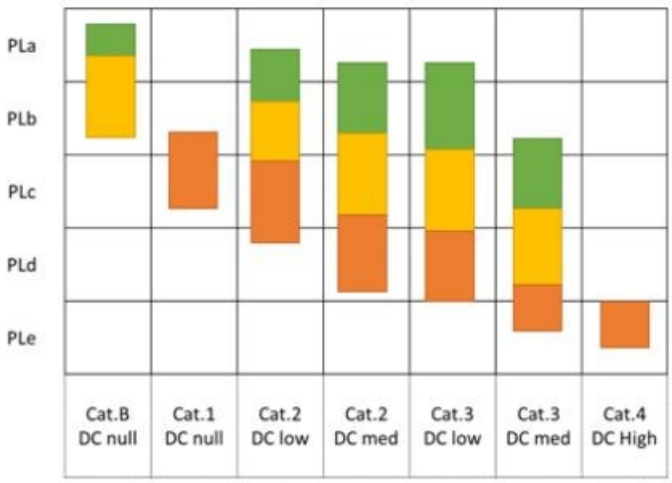


Figura 6.2 Categoria - PL

Calcolo PL caso studio

Si vuole ora calcolare il PL_R e il PL per le funzioni di sicurezza del caso studiato nei capitoli precedenti.

Si parte con il recuperare il PL dei singoli componenti che compongono le funzioni di sicurezza della macchina, i quali vengono forniti dal produttore di ogni componente.

Le funzioni di sicurezza della macchina sono:

- Arresto d'emergenza.
- Arresto per intervento dei finecorsa.
- Arresto per intervento delle barriere fotoelettriche di sicurezza.

L'arresto d'emergenza avviene tramite un pulsante d'emergenza a doppio contatto NC, il quale ha un PL=D e una categoria di sicurezza pari a 3. Il PL_r per questa funzione di sicurezza viene calcolato partendo dal punto 1 della figura 6.1, la gravità della lesione è alta, la frequenza e il tempo d'esposizione invece è basso, la probabilità di evitare o limitare il danno è bassa, dunque si ottiene un PL_r=D.

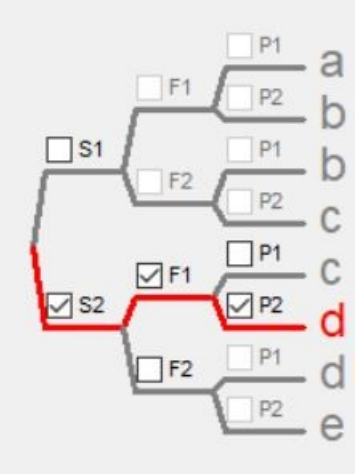


Figura 6.3 Calcolo PL_r caso studio

L'arresto tramite l'intervento dei finecorsa lavora con i 4 FC a singolo contatto NC, i quali presentano un PL=A e una categoria di sicurezza base (B). Il PL_r per questa funzione di sicurezza viene calcolato valutando che la gravità della lesione è alta, la frequenza e il tempo d'esposizione invece è basso, la probabilità di evitare o limitare il danno è bassa, dunque si ottiene un PL_r=D.

L’arresto tramite l’intervento delle barriere fotoelettriche di sicurezza lavora con due barriere con PL=D e categoria di sicurezza pari a 2. Il PL_r per questa funzione di sicurezza viene calcolato verificando che la gravità della lesione è alta, la frequenza e il tempo d’esposizione invece è basso, la probabilità di evitare o limitare il danno è bassa, dunque si ottiene un PL_r=D.

Per calcolare il PL effettivamente raggiunto dalle funzioni di sicurezza si utilizza il software: “Sistema”, programma sviluppato da IFA (Istituto per la salute, la sicurezza sul lavoro e dell’assicurazione per gli incidenti sul lavoro tedesco), che consente di realizzare un modello sulla base dei circuiti di sicurezza della macchina, permettendo di calcolare in automatico il PL raggiunto in base alle componenti utilizzate.

Figura 6.4 Schermata sistema

La figura 6.4 rappresenta uno screenshot del software, sulla sinistra possiamo vedere la macchina (“Ascensore”) e le varie funzioni di sicurezza che possiede e in ogni funzione sono riportati gli attori che ne fanno parte. Una volta configurati tutti gli elementi con i PL e le categorie di sicurezza forniti dai produttori, il software calcola il PL complessivo raggiunto della funzione di sicurezza e lo compare con il PL_r precedentemente impostato. Se PL>=PL_r restituisce una spunta verde, qualora invece PL<PL_r genera una croce rossa. Nel caso in esame si vede come l’arresto d’emergenza e l’arresto per intervento delle barriere fotoelettriche di sicurezza generi un risultato positivo (Figura 6.4 Tabella a destra), mentre per l’arresto dovuto all’intervento dei finecorsa il PL raggiunto è troppo basso.

Dall’analisi del PL è dunque emersa una criticità nella funzione d’arresto con i finecorsa

scelti, per risolvere questa vulnerabilità si deve procedere con la scelta di finecorsa con un PL superiore.
Si vuole ora simulare una scelta progettuale diversa, ovvero il caso in cui si sono utilizzati due finecorsa a doppio contatto d'uscita NC, come quello in Figura 6.5 che ha un PL=D e una categoria di sicurezza pari a 3.

Figura 6.5 Finecorsa doppio contatto NC

In questo caso andando a simulare su Sistema, come si può vedere dalla figura 6.6, il software restituisce un risultato privo di messaggi d'errore.

Figura 6.6 Schermata Sistema corretta

Conclusioni

Questa tesi ha cercato di porre l'attenzione sull'importanza delle funzioni di sicurezza di una macchina e di quanto sia fondamentale prevenire i malfunzionamenti in caso di guasto. A tal scopo si è analizzato un caso pratico, partendo dallo studio delle normative per capire i requisiti essenziali di sicurezza che deve avere la macchina, si è passati dunque alla progettazione della stessa per poi realizzare un modello pratico che ne simula il funzionamento. Sono stati successivamente effettuati dei test che hanno simulato il guasto delle diverse componenti di sicurezza al fine di analizzare il comportamento della macchina.

Grazie al caso studiato si è capita l'importanza di analizzare il rischio creato da una macchina già nelle prime fasi di progettazione della stessa, andando a modificare eventuali scelte progettuali che non garantiscono un livello di sicurezza ottimale. Si è vista la differenza tra ridondanze volte a garantire una continuità operativa rispetto a ridondanze volte a garantire l'operatività delle funzioni di sicurezza della macchina.

La tesi potrebbe essere ampliata eseguendo uno studio delle funzioni di sicurezza per lo sviluppo di un ascensore adibito al trasporto di persone, andando ad analizzare ulteriori rischi e RES da rispettare.

Elenco delle tabelle

Elenco delle figure