

Università degli studi di Modena e Reggio Emilia

Dipartimento di Ingegneria “Enzo Ferrari”

Corso di Laurea Magistrale in Ingegneria Informatica



Modellazione di un sensore per il rilevamento di fuoriuscita di gas naturale, fault analysis e riduzione del rischio

PROGETTO DI CORSO

# Sommario

---

Sommario .....	2
Introduzione .....	3
a. Finalità del progetto .....	3
Fault analysis .....	5
a. Analisi del rischio.....	5
b. Fault tree analysis.....	6
c. Cause del fault.....	7
Riduzione Del Rischio.....	8
a. PLr – Required Performance Level.....	8
b. SIL richiesta alla funzione di sicurezza.....	10
c. MTBFd – Mean Time Between Failures dangerous .....	12
Software.....	14
a. Schema a Blocchi (FSM) .....	14
b. Script Codesys .....	16
Conclusioni.....	19

# Introduzione

## a. Finalità del progetto

---

Questo elaborato si pone l'obiettivo di analizzare e prevenire i possibili malfunzionamenti derivanti da un sensore di temperatura, presente all'interno di una cisterna contenente gas GPL, e da una pompa di refrigerazione utilizzata per decrementare la temperatura all'interno della camera contenente il combustibile.

Per garantire la sicurezza durante il trasporto, è necessario mantenere la temperatura al di sotto della soglia critica, a tale scopo, è stata inserita una pompa di raffreddamento, modellata attraverso un timer, che verrà azionata nel momento in cui la temperatura eccederà il valore massimo consentito. Nel caso in cui la pompa non dovesse assolvere correttamente il suo lavoro, verrà eseguito un rilascio controllato del gas in atmosfera per diminuire la pressione e di conseguenza anche la temperatura all'interno della cisterna per evitare una possibile esplosione della stessa.

Per la simulazione verrà realizzato uno script codesys che consentirà di controllare e gestire eventuali problematiche associate ai diversi componenti del sistema e di effettuare le analisi necessarie al miglioramento del livello di sicurezza.

Qualsiasi dispositivo o macchinario, per essere liberamente commercializzato all'interno dei paesi della Comunità Europea, deve soddisfare le prescrizioni delle direttive comunitarie. Esse stabiliscono i principi generali affinché i costruttori mettano in commercio prodotti che non siano pericolosi per gli operatori. L'insieme dei prodotti e dei diversi pericoli possibili è molto vasto e per questo nel corso del tempo sono state emanate diverse direttive. A titolo di esempio citiamo la direttiva bassa tensione 2014/35/UE, la direttiva sulle atmosfere esplosive 2014/34/UE, la direttiva sulla compatibilità elettromagnetica 2014/30/UE e via discorrendo. I pericoli derivanti dal funzionamento dei macchinari sono trattati dalla Direttiva Macchine 2006/42/EC.

Di particolare interesse sono le seguenti direttive:

- IEC 62061: che descrive gli standard di sicurezza dei sistemi di controllo elettrici, elettronici, ed elettrici programmabili impiegati in sistemi volti alla riduzione dei rischi
- ISO 13849-1: definisce le principali funzioni di sicurezza delle macchine (arresto di emergenza, interblocco del riparo mobile, ripristino, blocco del riparo, velocità ridotta)

Le due norme EN 62061 ed EN ISO 13849-1 hanno quindi una discreta sovrapposizione per quanto riguarda il campo applicativo e per diversi aspetti si somigliano così che esiste un legame tra i due diversi nomi simbolo (SIL e PL) che indicano il risultato dell'analisi secondo le due norme.

# Fault analysis

## a. Analisi del rischio

Un sistema si definisce sicuro solamente quando non reca danno alla vita umana o all'ambiente, perciò è bene studiare le conseguenze di un guasto.

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	$10^{-3}$ to $10^{-4}$
Occasional	Once in system lifetime	$10^{-4}$ to $10^{-5}$
Remote	Unlikely in system lifetime	$10^{-5}$ to $10^{-6}$
Improbable	Very unlikely to occur	$10^{-6}$ to $10^{-7}$
Incredible	Cannot believe that it could occur	$< 10^{-7}$

	Consequence			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

ottenere un miglioramento è molto elevato.

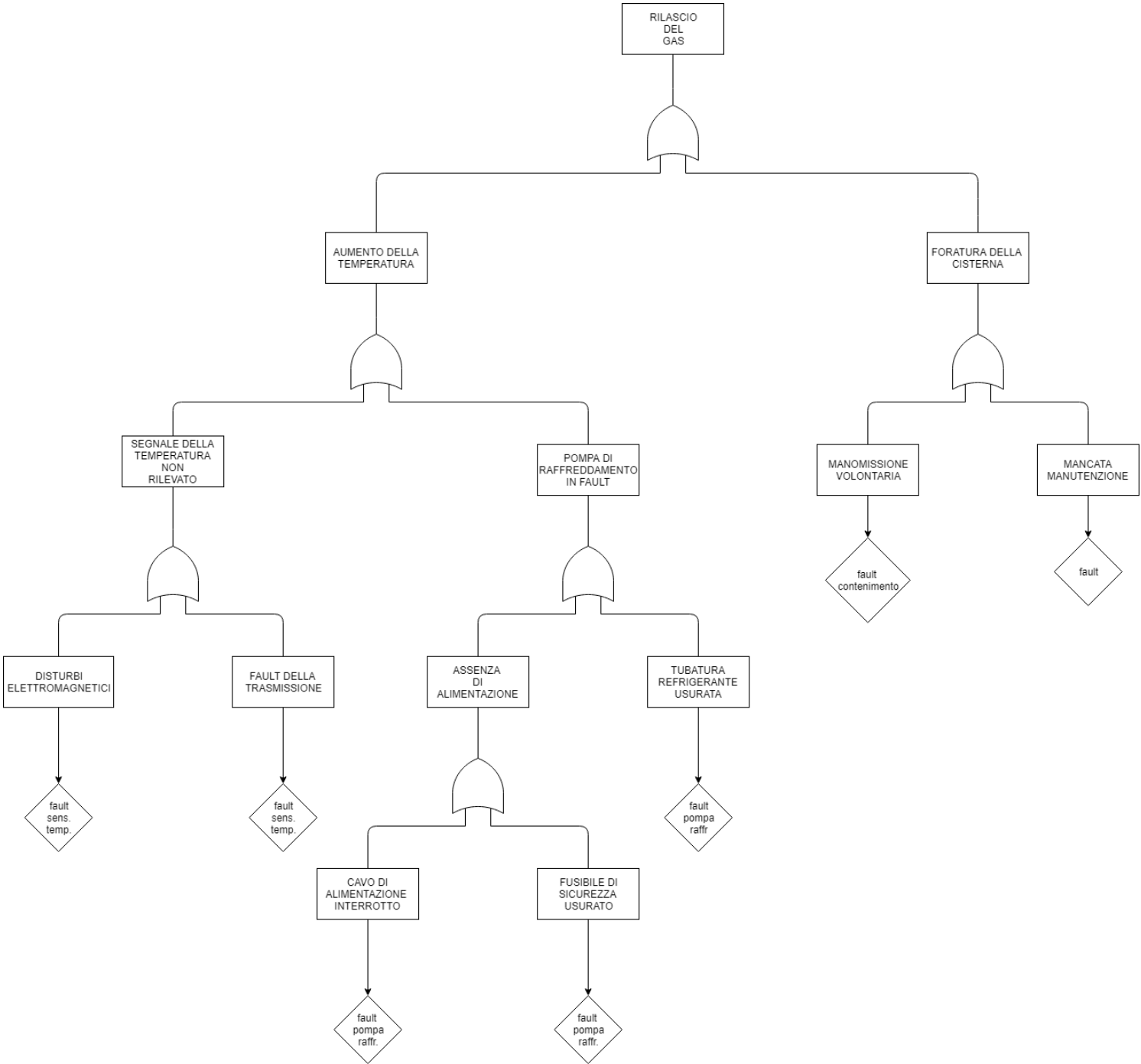
Nel sistema preso in analisi, è necessario evitare il più possibile il rilascio, pur controllato, del gas in atmosfera, poiché risulta essere un evento molto pericoloso per le persone e per l'ambiente.

Nel caso specifico si vuole che un errore o malfunzionamento sia molto raro, più precisamente “occasionale” oppure “remoto”, quindi, fissata la categoria del malfunzionamento è possibile ottenere la **classe di rischio**.

La classe più adeguata è la *seconda* poiché il fault del sistema è sempre un evento indesiderato ed il costo da sostenere per

b. Fault tree analysis

Vediamo da cosa possono scaturire i malfunzionamenti del sistema mediante la *fault tree analysis*:



### c. Cause del fault

---

All'interno della *fault tree analysis* sono state riportate alcune delle principali cause di guasto. Lo schematico è stato realizzato utilizzando un approccio top-down che parte dal rilascio del gas e poi si dirama passando ad analizzare tutte le possibili cause che potrebbero aver condotto a tale malfunzionamento. Dal suddetto grafico è possibile capire su quali aree agire per aumentare il livello di sicurezza. Ad esempio, per evitare che disturbi elettromagnetici compromettano la corretta comunicazione, è possibile adottare dei cavi schermati, oppure, se la pompa di raffreddamento non entra in azione a causa di un'assenza di alimentazione, è possibile diminuire la probabilità di quest'evento adottando circuiti ridondanti.

Nello schema sono presenti anche cause che non sono dovute a fault dei sistemi, ma causate da errata manutenzione o da manomissioni volontarie. In questo caso il fault non è categorizzabile all'interno di una precisa categoria, perciò sono stati nominati come fault generici.

# Riduzione Del Rischio

## a. PLr – Required Performance Level

Il PL (Performance Level) è il livello discreto utilizzato per specificare la capacità dei SRP/CS (Safety Related Parts of Control System) di eseguire una funzione di sicurezza in condizioni prevedibili. È espresso mediante cinque livelli (“a”, “b”, “c”, “d”, “e”) ad affidabilità crescente. Per SRP/CS si intende una parte del sistema di comando legata alla sicurezza, quindi la parte di un circuito di comando che risponde a segnali in ingresso legati alla sicurezza e genera segnali in uscita legati alla sicurezza.

Il PLr è invece il livello di prestazione da raggiungere al fine di conseguire la riduzione del rischio con un conseguente aumento dell'affidabilità per ciascuna funzione di sicurezza.

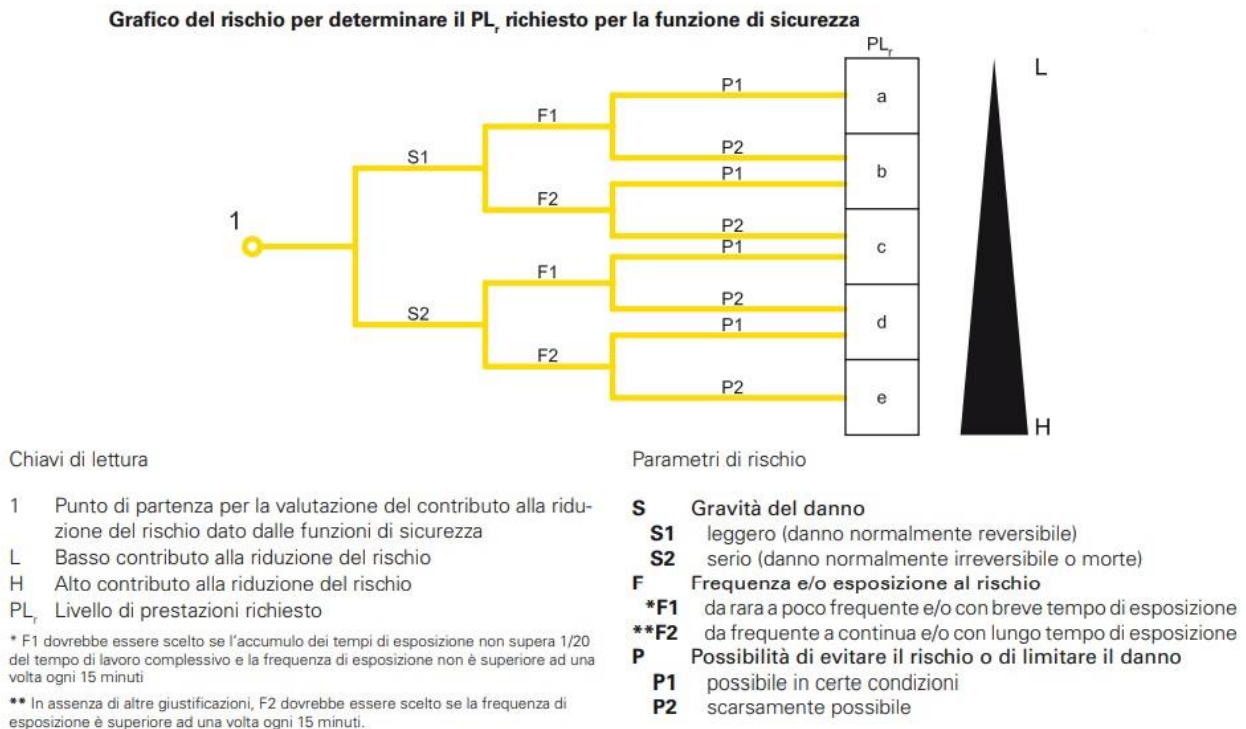
La determinazione del PLr è il risultato della valutazione dei rischi e si riferisce all'entità della riduzione del rischio a carico delle parti del sistema di comando legate alla sicurezza.

Quanto maggiore è l'entità della riduzione del rischio richiesta da parte della SRP/CS, tanto più elevato deve essere il PLr.

<b>PL</b> EN ISO 13849-1	<b>a</b>	<b>b</b>	<b>c</b>	<b>d</b>	<b>e</b>
<b>SIL</b> EN 62061 - IEC 61508	-	1	1	2	3
<b>PFH<sub>D</sub></b>	da $10^{-4}$ a $10^{-5}$	da $10^{-5}$ a $3 \times 10^{-6}$	da $3 \times 10^{-6}$ a $10^{-6}$	da $10^{-6}$ a $10^{-7}$	da $10^{-7}$ a $10^{-8}$
Un guasto pericoloso ogni n° anni	da ~1 a ~10	da ~10 a ~40	da ~40 a ~100	da ~100 a ~1000	da ~1000 a ~10000

La norma EN ISO 13849-1 fornisce al costruttore un metodo iterativo per valutare se i rischi di una macchina possano essere limitati ad un livello residuo accettabile mediante l'impiego di adeguate funzioni di sicurezza. Il metodo adottato prevede, per ogni rischio, un ciclo di ipotesi-analisi-validazione alla fine del quale si deve poter dimostrare che ogni funzione di sicurezza prescelta è adeguata al relativo rischio in esame.





Il primo passo consiste quindi nella valutazione del livello di prestazione richiesto da ogni funzione di sicurezza. La EN ISO 13849-1 utilizza un grafico per l'analisi del rischio di una funzione di una macchina (figura precedente) determinando, in funzione del rischio, anziché una categoria di sicurezza richiesta, un livello di prestazione richiesto o PL<sub>r</sub> (Required Performance Level) per la funzione di sicurezza che andrà a proteggere quella parte di macchina.

Il costruttore del macchinario, partendo dal punto 1 del grafico e rispondendo alle domande S, F e P identificherà il PL<sub>r</sub> per la funzione di sicurezza in esame. Dovrà poi realizzare un sistema per proteggere l'operatore della macchina che abbia un livello di prestazione PL uguale o migliore di quello richiesto.

Nel caso specifico, abbiamo:

- Gravità del danno:
  - S2 (rilascio del gas in atmosfera, irreversibile)
- Frequenza:
  - F1
- Possibilità di evitare il danno:
  - P2

Ottenendo quindi un PL<sub>r</sub> = d

I PL sono classificati in cinque livelli, da PL = a fino a PL = e al crescere del rischio ed ognuno di essi identifica un ambito numerico di probabilità media di guasto pericoloso per ora. Ad esempio, PL= d (come nel nostro caso) indica che la probabilità media di guasti pericolosi per ora è compresa tra  $1 \times 10^{-6}$  e  $1 \times 10^{-7}$  ovvero all'incirca 1 guasto pericoloso mediamente ogni 100-1000 anni.

PL	Probabilità media di guasti pericolosi per ora PFHD (1/h)			
<b>a</b>	$\geq 10^{-5}$	e	$< 10^{-4}$	
<b>b</b>	$\geq 3 \times 10^{-6}$	e	$< 10^{-5}$	
<b>c</b>	$\geq 10^{-6}$	e	$< 3 \times 10^{-6}$	
<b>d</b>	$\geq 10^{-7}$	e	$< 10^{-6}$	
<b>e</b>	$\geq 10^{-8}$	e	$< 10^{-7}$	

Per la valutazione del PL di un sistema di controllo servono più parametri ovvero:

1. La Categoria di sicurezza del sistema che a sua volta deriva dall'architettura (struttura) del sistema di controllo e dal suo comportamento in

caso di guasto

2. MTTFD dei componenti

3. DC o Copertura Diagnostica del sistema.

4. CCF o Guasti di causa comune del sistema.


## b. SIL richiesta alla funzione di sicurezza

Il SIL (Safety Integrity Level) determina il grado di affidabilità richiesto ad una SRFC (Safety Related Control Function), ovvero una funzione di controllo relativa alla sicurezza che ha come obiettivo la riduzione del rischio associato ad un particolare evento pericoloso.

Conseguenze	Gravità	Classe					Durata		Probabilità	Evitabilità
		3-4	5-7	8-10	11-13	14-15				
Morte, perdita braccio/occhio	4	SIL2	SIL2	SIL2	SIL3	SIL3	≤1 ora	5	Molto alta 5	
Permanente, perdita dita	3		OM	SIL1	SIL2	SIL3	da >1 ora a ≤ 1 giorno	5	Probabile 4	
Reversibile, cure mediche	2			OM	SIL1	SIL2	da >1 giorno a ≤ 2 settimane	4	Possibile 3	Impossibile 5
Reversibile, pronto soccorso	1				OM	SIL1	da > 2 settimane a ≤ 1 anno	3	Scarsa 2	Possibile 3
							> 1 anno	2	Trascurabile 1	Probabile 1

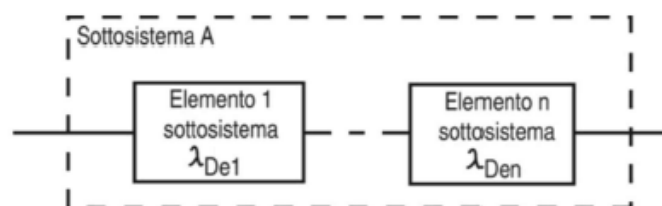
Nel caso analizzato all'interno della Fault Tree Analysis il SIL è stato determinato sulla base della seguente tabella, prendendo in considerazione: durata, probabilità ed evitabilità. La durata, nel caso analizzato, per il rilascio controllato del gas risulta essere inferiore ai 60 minuti perché occorre rilasciare soltanto una parte del gas contenuto affinché la pressione e la temperatura diminuiscano. La probabilità che questo evento prenda luogo è scarsa grazie ad analisi periodica della temperatura

e al raffreddamento dell'ambiente nel momento in cui la temperatura risulta essere superiore a quella consentita. Infine, è possibile che questo evento venga evitato grazie alle funzioni di sicurezza citate precedentemente. Il SIL associato, dopo l'analisi, risulta essere pari a 10, quindi è raccomandata una manutenzione periodica della pompa di raffreddamento e del sensore di temperatura per prevenire la mancata rilevazione della temperatura o la mancata refrigerazione dell'ambiente. Per individuare la classe di appartenenza è stata effettuata l'intersezione con la colonna delle conseguenze, la riga 3 riferita alle cure mediche e al valore ottenuto attraverso l'analisi dei parametri precedentemente elencati.



Conseguenze	Gravità	Classe					Durata		Probabilità	Evitabilità
		3-4	5-7	8-10	11-13	14-15				
Morte, perdita braccio/occhio	4	SIL2	SIL2	SIL2	SIL3	SIL3	≤1 ora	5	Molto alta 5	
Permanente, perdita dita	3		OM	SIL1	SIL2	SIL3	da >1 ora a ≤ 1 giorno	5	Probabile 4	
Reversibile, cure mediche	2			OM	SIL1	SIL2	da >1 giorno a ≤ 2 settimane	4	Possibile 3	Impossibile 5
Reversibile, pronto soccorso	1				OM	SIL1	da > 2 settimane a ≤ 1 anno	3	Scarsa 2	Possibile 3
							> 1 anno	2	Trascurabile 1	Probabile 1

L'architettura utilizzata per questo tipo di applicazione è l'architettura A che prevede una tolleranza nulla ai guasti e nessuna funzione di diagnostica. In particolare, risulta essere composta da due blocchi in serie logica, per cui il guasto di uno solo di essi determina la perdita della funzione di sicurezza. In questo caso è necessario approfondire i guasti riguardanti i singoli componenti per determinare la frequenza di guasti pericolosi associati al sottosistema.



### c. MTBFd – Mean Time Between Failures dangerous

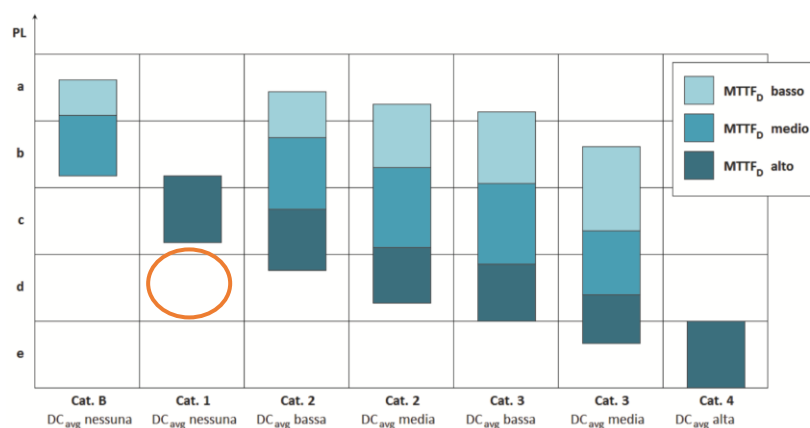
Il tempo medio tra due guasti pericolosi è un parametro di affidabilità applicabile a dispositivi meccanici, elettrici ed elettronici e ad applicazioni software.

Questo parametro risulta essere la somma di due tempi:

- Mean Time to Failure (MTTFd): è il parametro principale che definisce l'affidabilità di un componente. Esso rappresenta la durata di vita media di un componente prima di subire un guasto considerato pericoloso. Al MTTFd viene associato il tasso di guasto  $\lambda_d$  riferito solo ai guasti pericolosi. Per associare l'MTTFd al  $\lambda_d$ , la norma EN 13849 considera che il componente abbia già superato la prima fase di vita in cui la probabilità dei guasti è molto elevata, successivamente definisce un mission time in cui la probabilità che si verifichi un guasto risulta essere costante. Con queste ipotesi si può dimostrare che  $MTTFd = 1 / \lambda_d$ .
- Mean Time to Repair (MTTR): è il valore atteso del tempo di ripristino delle funzionalità. Può essere trascurato quando il tempo necessario per la sostituzione richiede un tempo trascurabile rispetto al fallimento del componente stesso.

Nel caso preso in esame sia il sensore di temperatura che la pompa di raffreddamento hanno un MTTFd molto alto, quindi il diagnostic coverage ( $DC = \lambda_{ad} / \lambda_d$ ), ossia il rapporto tra la frequenza dei guasti pericolosi rilevati  $\lambda_{ad}$  e la frequenza dei guasti pericolosi totali  $\lambda_d$  risulta sufficientemente bassa.

Possiamo procedere con la scelta della categoria seguendo la tabella riportata in basso.



Dalla analisi dei componenti la categoria più scelta è la 1, ovvero un'architettura a canale singolo, composta da:

- Un blocco di input o sensori (blocco I)
- Un blocco per l'elaborazione dati (blocco L)
- Un blocco di attuazione (blocco O)



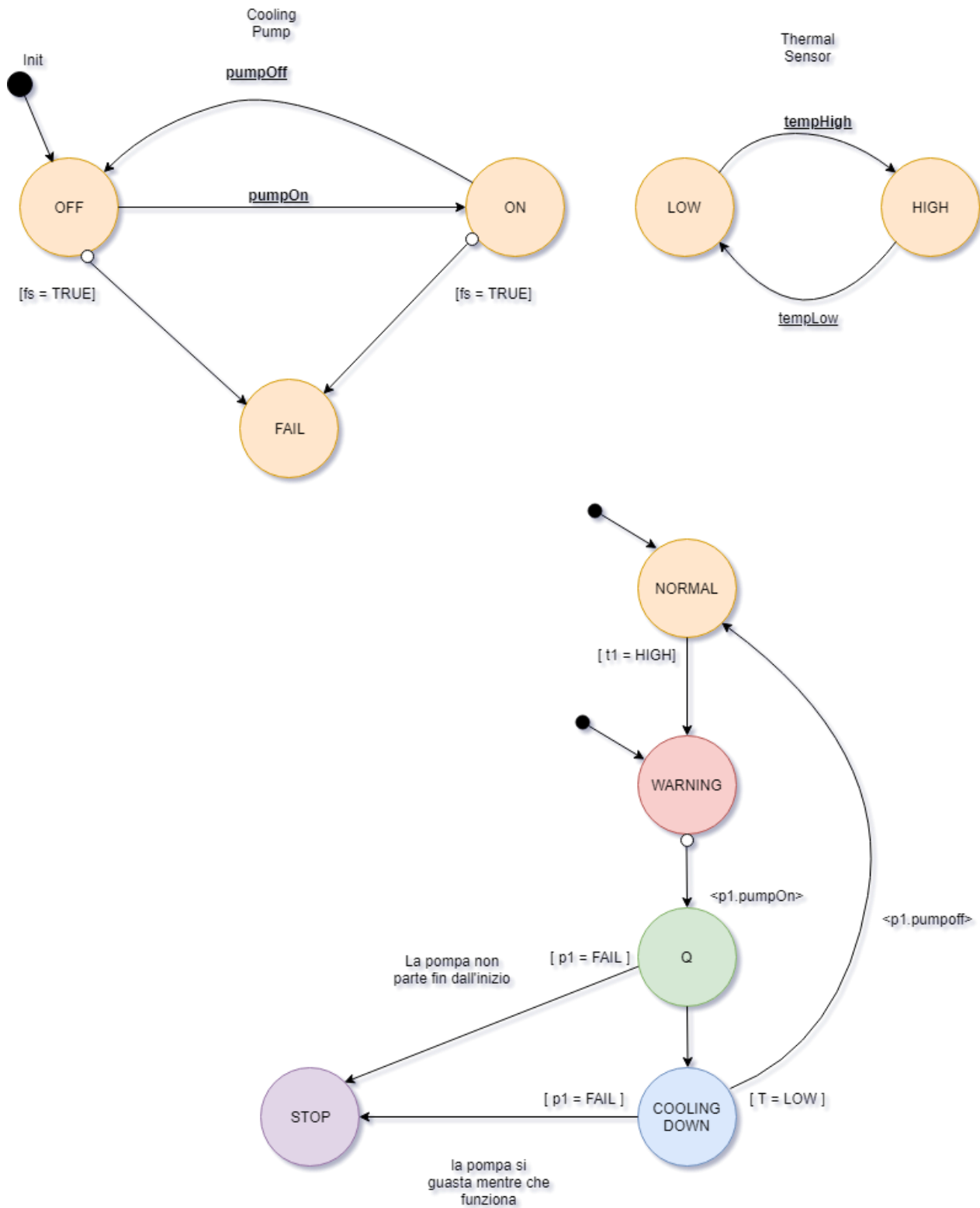
1. Non è prevista copertura diagnostica (DC)
2. MTTFd da basso a medio
3. CCF non applicabile

Un canale che soddisfa requisiti minimi di affidabilità in cui un guasto può portare alla perdita della funzione di sicurezza.

# Software

## a. Schema a Blocchi (FSM)

Mostriamo ora lo schema a blocchi del funzionamento della nostra applicazione:



Come si può vedere, il controller ha due stati iniziali possibili: “*Normal*” e “*Warning*” a seconda se la temperatura della cisterna è alta o bassa (iniettata manualmente).

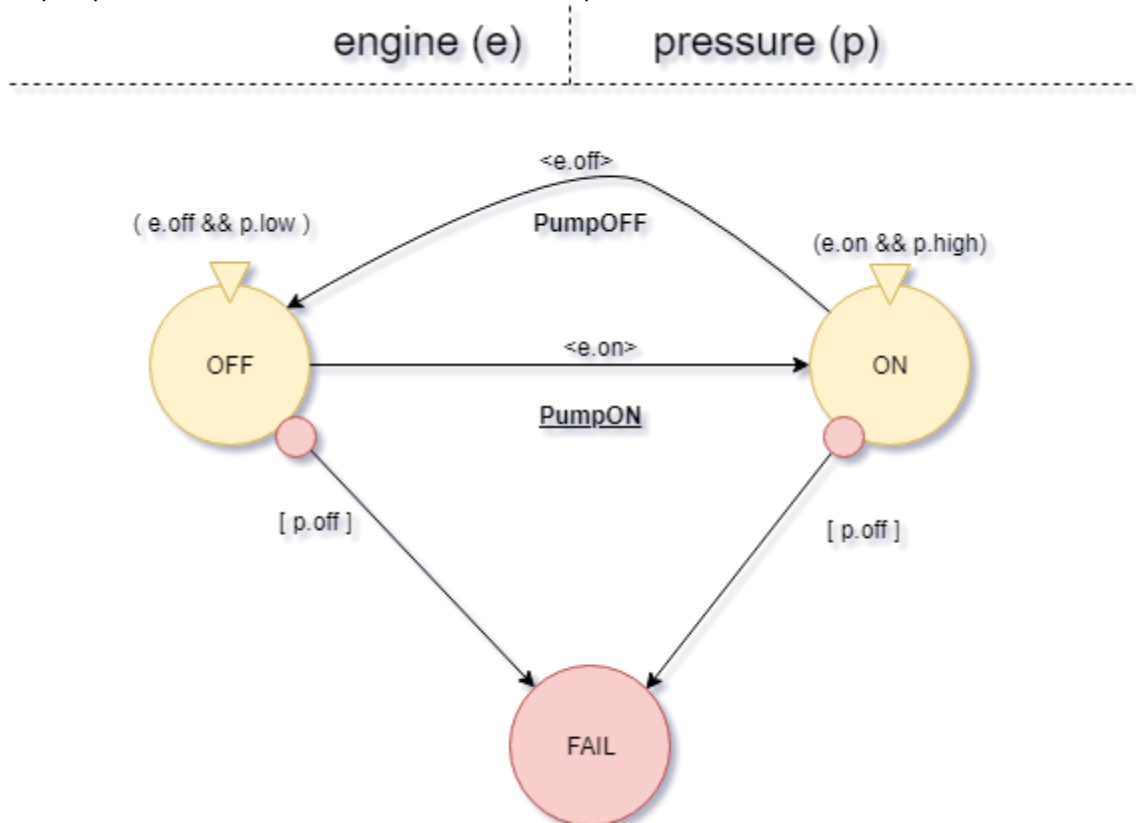
Degno di nota è lo stato *cooling down*, infatti, il sistema continuerà a risiedere in quello stato finché l’utente, durante la simulazione, non imposta manualmente il livello di temperatura basso.

L’azione manuale è necessaria per avere una maggiore attinenza alla realtà, infatti non è possibile sapere con certezza le tempistiche del raffreddamento, perciò abbiamo scelto di farlo manualmente.

Se durante il raffreddamento la pompa va in *fail* avviene il cambio di stato, e si va in quello di *stop* dove avviene il rilascio del gas; altrimenti se tutto ha funzionato correttamente si va in *normal* che descrive il corretto funzionamento.

Inoltre, dal diagramma, è possibile notare che vi sono due possibili stati iniziali, poiché non è detto che il sistema di controllo una volta azionato trovi sempre la temperatura al di sotto del livello critico.

La pompa di raffreddamento è stata modellata in questo modo:



Come si può notare dalla semantica degli stati, le *exit zone* possibili sono solamente quando:

1. La pompa è ON ma la pressione scende a zero
2. La pompa è OFF ma la pressione continua ad essere maggiore di zero

## b. Script Codesys

Vediamo ora l'implementazione su Codesys del caso in analisi

### *Function Block del Sensore di temperatura:*

```
1. FUNCTION_BLOCK SENSOR
2. VAR_INPUT
3.     tempHigh, tempLow : BOOL := FALSE;
4.     // tempHigh is run by button
5.     // tempLow come in by controller
6. END_VAR
7. VAR_OUTPUT
8.     Idle_S, Low_S, High_S : BOOL := FALSE;
9. END_VAR
10. VAR
11.     state : INT := 0;
12. END_VAR
13.
14. CASE state OF
15.     0:
16.         Idle_S := TRUE;
17.         state := 1;
18.         Idle_S := FALSE;
19.
20.     1:
21.         Low_S := TRUE;
22.         IF tempHigh THEN
23.             state := 2;
24.             Low_S := FALSE;
25.             tempHigh := FALSE;
26.         END_IF
27.
28.     2:
29.         High_S := TRUE;
30.         IF tempLow THEN
31.             High_S := FALSE;
32.             tempLow := FALSE;
33.             state := 1;
34.         END_IF
35. END_CASE
```

### *Function Block della pompa di raffreddamento:*

```
1. FUNCTION_BLOCK PUMP
2. VAR_INPUT
3.     Pumpon, Fail, Pumpoff : BOOL := FALSE;
4.     // Pumpon is activated by controller when temperature raise over a determinated thresh
5.     old
6. END_VAR
7. VAR_OUTPUT
8.     Idle_S, Off_S, Checkpump_S, On_S, Fail_S : BOOL := FALSE;
9. END_VAR
10. VAR
11.     T :TON();
12.     State : INT := 0;
13.     Dangerlight : BOOL := FALSE;
14.     // Dangerlight is on when pump fail
15.     // Fail is an outdoor event which simulate breakdown pump
16. END_VAR
17.
18.
19.
```



```

20. CASE State OF
21.   0:
22.     Idle_S := TRUE;
23.     state := 1;
24.     Idle_S := FALSE;
25.   1:
26.     Off_S := TRUE;
27.     IF Pumpon THEN
28.       State := 2;
29.       Off_S := FALSE;
30.     END_IF
31.   2:
32.     Checkpump_S := TRUE;
33.     IF NOT T.Q THEN
34.       T.IN := TRUE;
35.       T.PT := T#10S;
36.       T();
37.       IF Fail THEN
38.         State := 4;
39.         Checkpump_S := FALSE;
40.       END_IF
41.     ELSE
42.       T.IN := FALSE;
43.       T();
44.       State := 3;
45.       Checkpump_S := FALSE;
46.     END_IF;
47.   3:
48.     On_S := TRUE;
49.     IF Fail THEN
50.       State := 4;
51.       Fail := FALSE;
52.       On_S := FALSE;
53.     END_IF
54.     IF Pumpoff THEN
55.       state := 1;
56.       Pumpoff:=FALSE;
57.       On_S := FALSE;
58.     END_IF
59.   4:
60.     Fail_S := TRUE;
61.     Dangerlight := TRUE;
62. END_CASE

```

### Function Block del Controller:

```

1. FUNCTION_BLOCK CONTROLLER
2. VAR_INPUT
3. END_VAR
4. VAR_OUTPUT
5.   Idle_S, Normal_S, Warning_S, Cooling_Down_S, Stop_S, Drain_S : BOOL;
6. END_VAR
7. VAR_IN_OUT
8.   p : PUMP();
9.   t : SENSOR();
10. END_VAR
11. VAR
12.   drain_gas : BOOL := FALSE;
13.   State : INT := 0;
14.   T1 : TON();
15. END_VAR
16.

```

```

17.
18. CASE State OF
19.     0:
20.         Idle_S := TRUE;
21.         state := 1;
22.         Idle_S := FALSE;
23.     1:
24.         Normal_S := TRUE;
25.         IF t.High_S THEN
26.             state := 2;
27.             Normal_S := FALSE;
28.         END_IF
29.     2:
30.         Warning_S := TRUE;
31.         IF NOT T1.Q THEN
32.             T1.IN := TRUE;
33.             T1.PT := T#5S;
34.             T1();
35.         ELSE
36.             T1.IN := FALSE;
37.             T1();
38.             IF p.Fail_S THEN
39.                 state := 3;
40.                 Warning_S := FALSE;
41.             ELSE
42.                 State := 4;
43.                 p.Pumpon := TRUE;
44.                 Warning_S := FALSE;
45.             END_IF
46.         END_IF;
47.
48.     3:
49.         Stop_S := TRUE;
50.         drain_gas := TRUE;
51.     4:
52.         Cooling_Down_S := TRUE;
53.         IF NOT T1.Q THEN
54.             T1.IN := TRUE;
55.             T1.PT := T#5S;
56.             T1();
57.         ELSE
58.             T1.IN := FALSE;
59.             T1();
60.             IF p.Fail_S THEN
61.                 state := 3;
62.             END_IF
63.             IF p.On_S THEN
64.                 state := 1;
65.                 t.tempLow := TRUE;
66.                 p.Pumpoff := TRUE;
67.             END_IF
68.             Cooling_Down_S := FALSE;
69.         END_IF;
70. END_CASE

```

Oltre al codice abbiamo disposto una visualizzazione per poter verificare il corretto funzionamento della logica a stati:



dall'immagine si possono notare i due bottoni con i quali andiamo ad iniettare gli errori della pompa, e della temperatura.

Se la pompa non è in *fail* dopo aver compiuto il raffreddamento simulato con un timer, la temperatura torna bassa.

## Conclusioni

---

Questo lavoro di progetto ci ha permesso di capire come concettualizzare e sviluppare un progetto secondo le principali normative di legge internazionali, al fine di ottenere un prodotto *sicuro*.

Inoltre ci ha permesso di prendere confidenza con la programmazione dei PLC ancora oggi largamente adottati in campo aziendale.