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

Nicola Corbo | Fabrizio Di Blasi | Informatica industriale ed IoT | a.a 2018/2019

Sommario

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

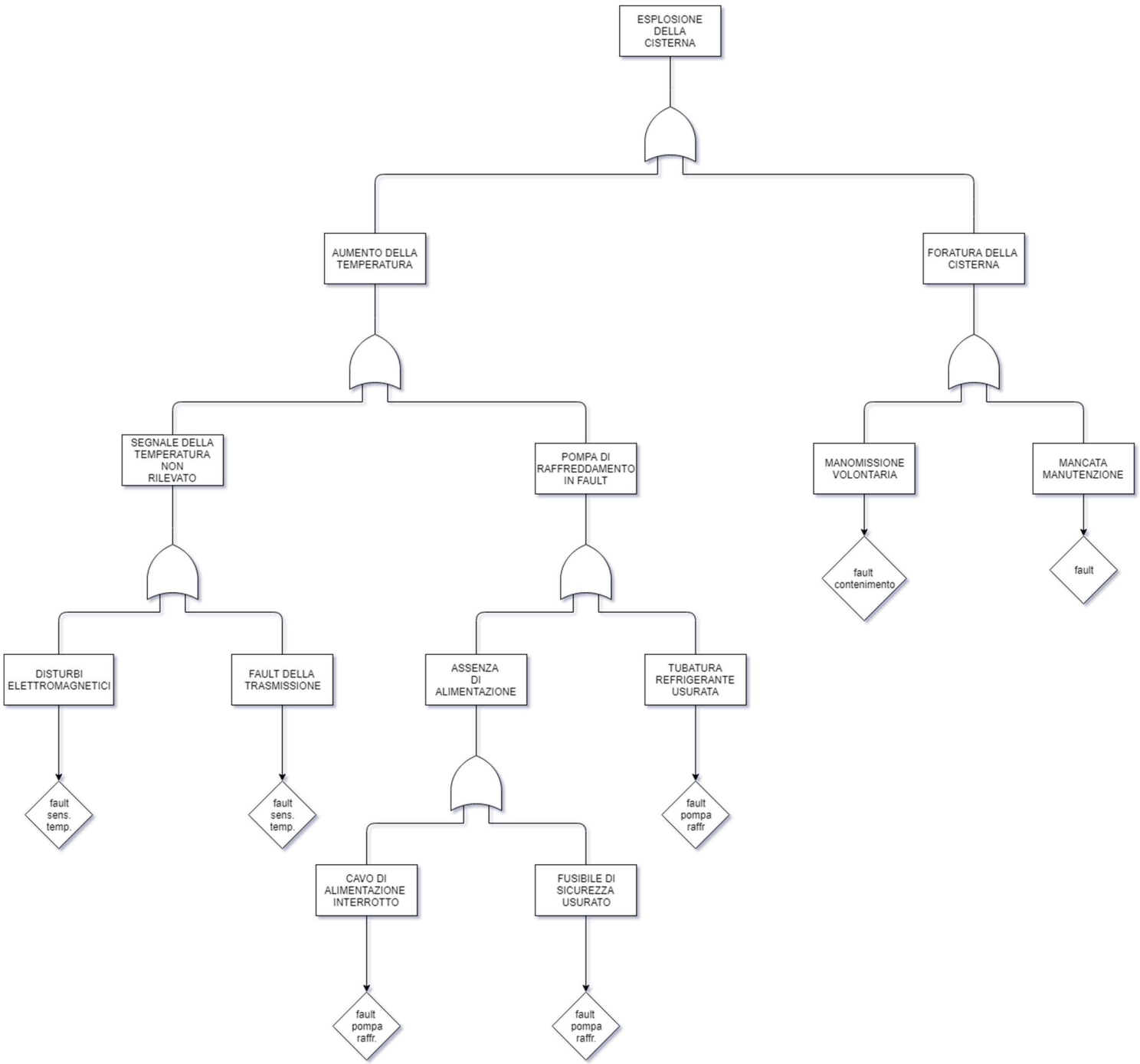
Nel sistema preso in analisi, è necessario evitare il più possibile l'esplosione della cisterna del gas, poiché risulta essere un evento molto pericoloso per le persone e per l'ambiente.

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 *prima* poiché il fault del sistema è sempre un evento indesiderato ed il costo da sostenere per ottenere un miglioramento è molto elevato.

b. Fault tree analysis

Vediamo da cosa possono scaturire i malfunzionamenti del sistema mediate 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 è 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.

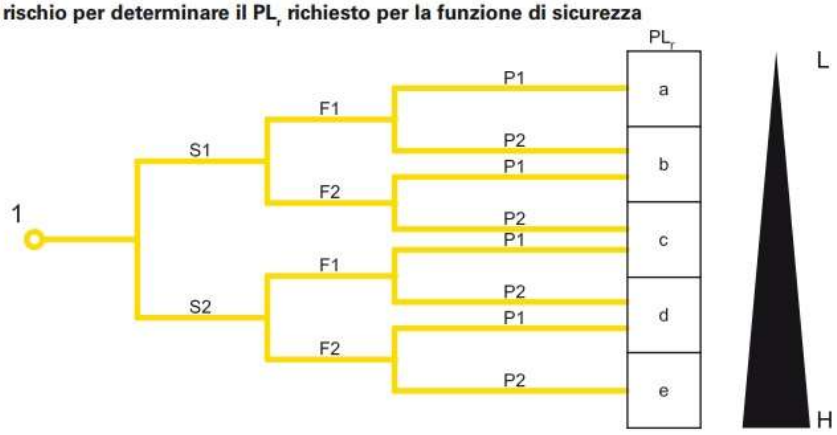
La determinazione del PLr è il risultato della valutazione dei rischi e si riferisce all'entità della riduzione del rischio a carico delle parti del sistema di comando legate alla sicurezza.

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

PL EN ISO 13849-1	**a**	**b**	**c**	**d**	**e**
SIL EN 62061 - IEC 61508	**-**	**1**	**1**	**2**	**3**
PFH_D	da 10^{-4} a 10^{-5}	da 10^{-5} a $3x10^{-6}$	da $3x10^{-6}$ a 10^{-6}	da 10^{-6} a 10^{-7}	da10^{-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.

Grafico del rischio per determinare il PL_r richiesto per la funzione di sicurezza



Chiavi di lettura

1 Punto di partenza per la valutazione del contributo alla riduzione del rischio dato dalle funzioni di sicurezza
L Basso contributo alla riduzione del rischio
H Alto contributo alla riduzione del rischio
PL_r Livello di prestazioni richiesto

* F1 dovrebbe essere scelto se l'accumulo dei tempi di esposizione non supera 1/20 del tempo di lavoro complessivo e la frequenza di esposizione non è superiore ad una volta ogni 15 minuti

** In assenza di altre giustificazioni, F2 dovrebbe essere scelto se la frequenza di esposizione è superiore ad una volta ogni 15 minuti.

Parametri di rischio

S **Gravità del danno**
S1 leggero (danno normalmente reversibile)
S2 serio (danno normalmente irreversibile o morte)
F **Frequenza e/o esposizione al rischio**
***F1** da rara a poco frequente e/o con breve tempo di esposizione
****F2** da frequente a continua e/o con lungo tempo di esposizione
P **Possibilità di evitare il rischio o di limitare il danno**
P1 possibile in certe condizioni
P2 scarsamente possibile

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 PLr (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 PLr 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 nostro caso di analisi, abbiamo:

- Gravità del danno (esplosione della cisterna):
  - S2
- Frequenza:
  - F1
- Possibilità di evitare il danno:
  - P2

Ottenendo quindi un PLr = d

I PL sono classificati in cinque livelli, da PL = a fino a PL = e in una scala crescente di rischio. Ognuno di essi identifica un ambito numerico di probabilità media di guasto pericoloso per ora.

PL	Probabilità media di guasti pericolosi per ora PFHD (1/h)		
a	$\geq 10^{-5}$	e	$< 10^{-4}$
b	$\geq 3 \times 10^{-6}$	e	$<10^{-5}$
c	$\geq 10^{-6}$	e	$< 3 \times 10^{-6}$
d	$\geq 10^{-7}$	e	$< 10^{-6}$
e	$\geq 10^{-8}$	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 Analisys 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 1 riferita ad eventi irreversibili 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	*SIL*2	*SIL*2	*SIL*2	*SIL*3	*SIL*3	≤1 ora	5	Molto alta 5	
Permanente, perdita dita	3		OM	*SIL*1	*SIL*2	*SIL*3	da >1 ora a ≤ 1 giorno	5	Probabile 4	
Reversibile, cure mediche	2			OM	*SIL*1	*SIL*2	da >1 giorno a ≤ 2 settimane	4	Possibile 3	Impossibile 5
Reversibile, pronto soccorso	1				OM	*SIL*1	da > 2 settimane a ≤ 1 anno	3	Scarsa 2	Possibile 3
							> 1 anno	2	Trascurabile 1	Probabile 1

c. MTBFd – Mean Time Between Failures dangerous

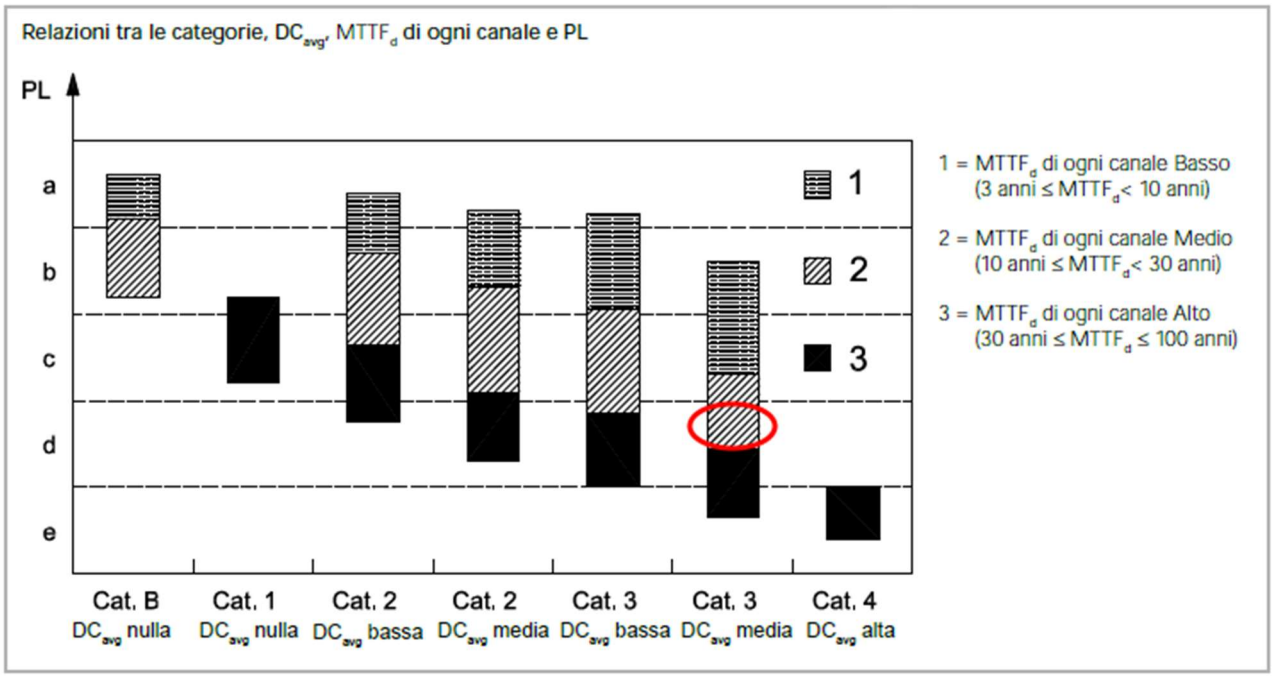
Il tempo medio tra due guasti pericolosi è un parametro di affidabilità applicabile a dispositivi meccanici, elettrici ed elettronici e ad applicazioni software.

Questo parametro risulta essere la somma di due tempi:

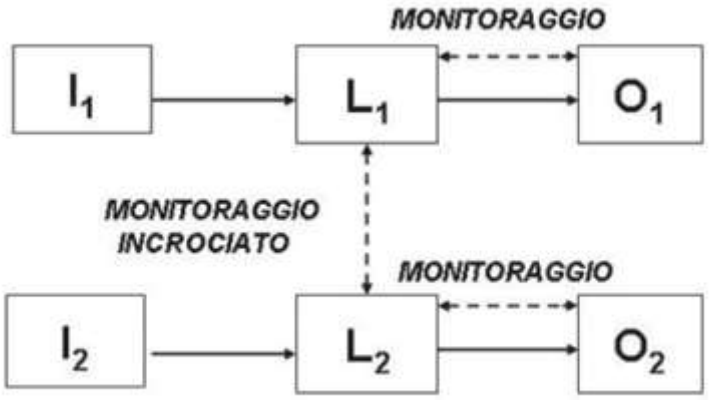
- Mean Time to Failure (MTTFd): è il parametro principale che definisce l'affidabilità di un componente. Esso rappresenta la durata di vita media di un componente prima di subire un guasto considerato pericoloso. Al MTTFd viene associato il tasso di guasto λ_d riferito solo ai guasti pericolosi. Per associare l'MTTFd al λ_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 / $\boldsymbol{\lambda_d}$.
- 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 = $\boldsymbol{\lambda_{dd}}$ / $\boldsymbol{\lambda_d}$**), ossia il rapporto tra la frequenza dei guasti pericolosi rilevati **$\boldsymbol{\lambda_{dd}}$** e la frequenza dei guasti pericolosi totali **$\boldsymbol{\lambda_d}$** risulta sufficientemente bassa.

Possiamo procedere con la scelta della categoria seguendo la tabella riportata in basso, sapendo che il nostro PLr = d.



Dalla figura possiamo vedere che adottando dei componenti con MTTFd = Medio, si ottiene una Categoria 3.



Per la categoria 3 si applicano i requisiti della categoria B e l'uso di principi di sicurezza ben provati. Le parti rilevanti per la sicurezza devono essere progettate in modo che: un singolo errore in una di queste parti non porti alla perdita della funzione di sicurezza (laddove il singolo errore venga rilevato). Quando si verifica un fault la funzione di sicurezza viene sempre svolta. Alcuni ma non tutti gli errori vengono rilevati. L'accumulo di errori non rilevati può portare alla perdita della funzione di sicurezza.

In ambito progettuale la categoria scelta è la B, 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.

Questa scelta è in contrasto con l'analisi dei rischi ma per scopi didattici si è scelto di modellare il nostro caso in esame con una struttura più semplice, come quella di tipo B.
Per poter raggiungere la categoria 3, si dovrà costruire un'architettura ridondante, che in caso di errore del componente primario non si vada a compromettere la funzione di sicurezza

d. PL e SIL

Rivedendo quindi la tabella che mette in relazione il SIL ed il PL otteniamo che:

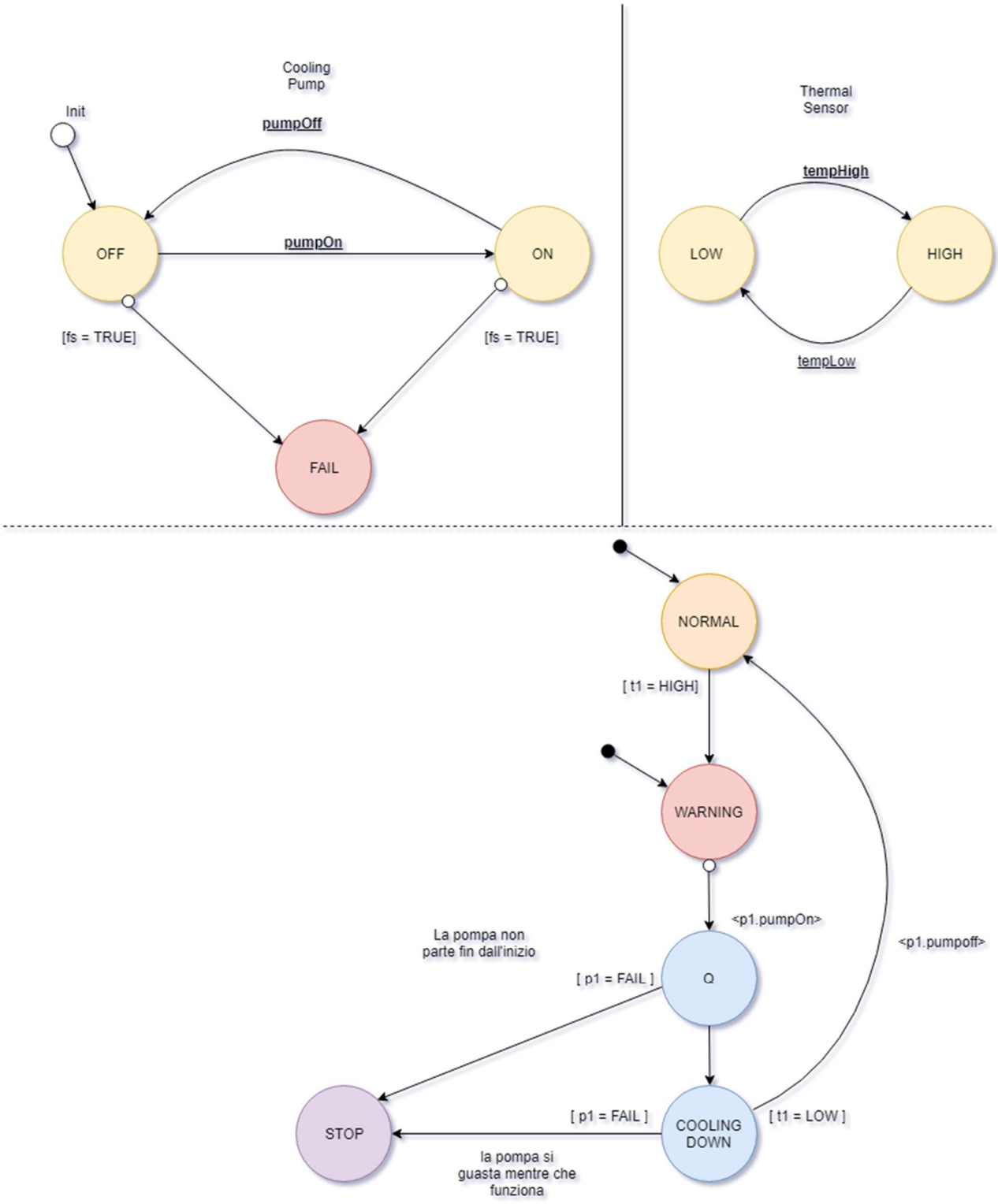
PL **(EN ISO 13849)**	**Probabilità media di un guasto pericoloso (PFH_D) [h^{-1}]**	***SIL*** **(IEC 61508)**
a	$10^{-5} \leq PFH_D < 10^{-4}$	Non definito
b	$3 \cdot 10^{-6} \leq PFH_D < 10^{-5}$	1
c	$10^{-6} \leq PFH_D < 3 \cdot 10^{-6}$	1
d	$10^{-7} \leq PFH_D < 10^{-6}$	2
e	$10^{-8} \leq PFH_D < 10^{-7}$	3

Il nostro PL è di tipo "d", inoltre, possiamo notare che il PLr (pari a "d") risulta minore o uguale del PL appena trovato.

Software

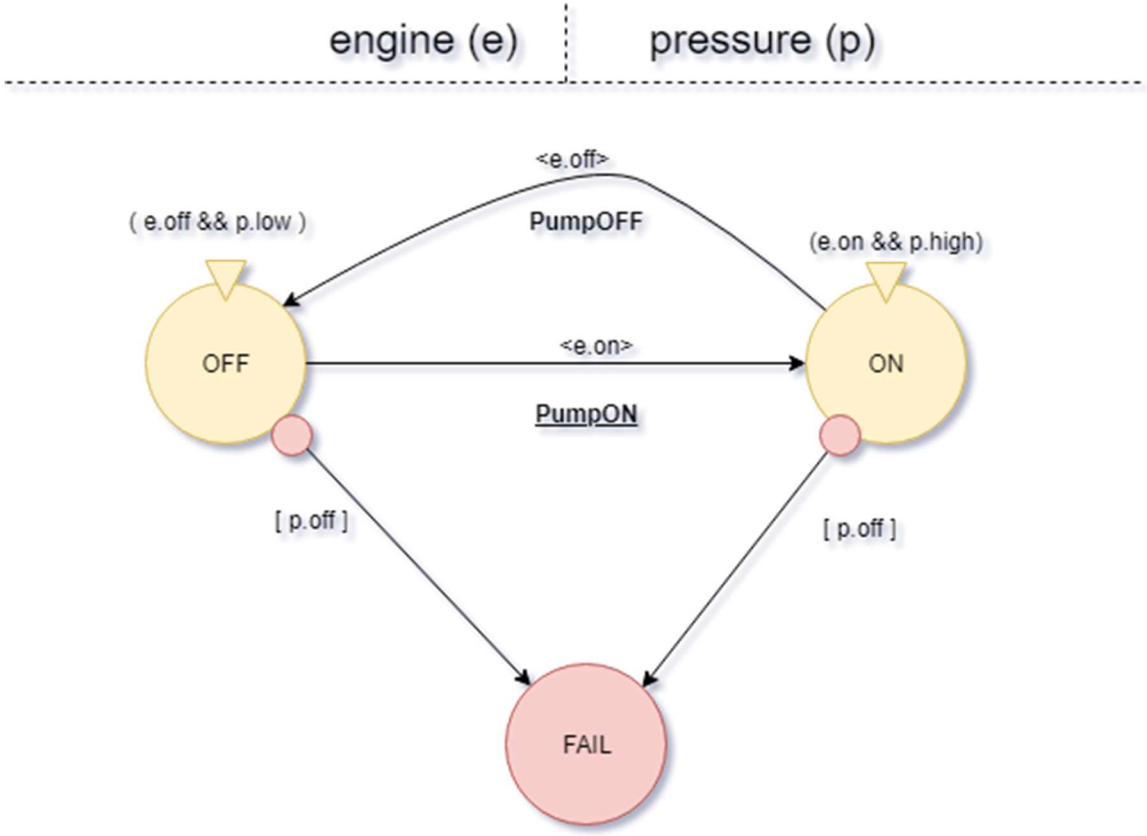
a. Schema a Blocchi (FSM)

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 finchè 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 reffreddamento, 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 sematica 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 : BOOL := FALSE;
4.      // tempHigh come in by button
5.  END_VAR
6.  VAR_OUTPUT
7.      Idle_S, Low_S, High_S : BOOL := FALSE;
8.  END_VAR
9.  VAR
10.     state : INT := 0;
11. END_VAR
12.
13. ----------------------------------------------------------------------------------------
    ------------------
14.
15. CASE state OF
16.     0:
17.         Idle_S := TRUE;
18.         state := 1;
19.         IF tempHigh THEN
20.             state := 2;
21.             Idle_S := FALSE;
22.         ELSE
23.             state := 1;
24.             Idle_S := FALSE;
25.         END_IF
26.     1:
27.         Low_S := TRUE;
28.         IF tempHigh THEN
29.             state := 2;
30.             Low_S := FALSE;
31.         END_IF
32.     2:
33.         High_S := TRUE;
34.         IF NOT tempHigh THEN
35.             High_S := FALSE;
36.             state := 1;
37.         END_IF
38. 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 threshold
5.  END_VAR
6.  VAR_OUTPUT
7.      Idle_S, Off_S, Checkpump_S, On_S, Fail_S : BOOL := FALSE;
8.  END_VAR
9.  VAR
10.     T :TON();
11.     State : INT := 0;
12.     Dangerlight : BOOL := FALSE;
13.     // Dangerlight is on when pump fail
14.     // Fail is an outdoor event which simulate breakdown pump
15. END_VAR
```

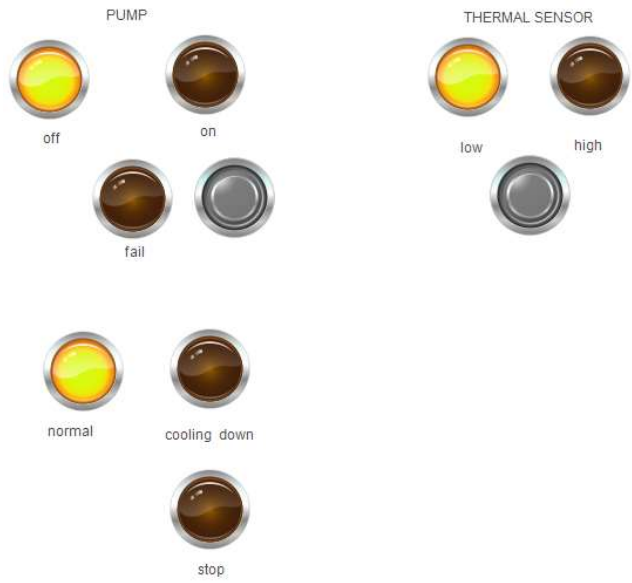
```
16.
17. ------------------------------------------------------------------------------------------
    ------------------
18.
19.
20. CASE State OF
21.     0:
22.         Idle_S := TRUE;
23.         state := 1;
24.         Idle_S := FALSE;
25.     1:
26.         Off_S := TRUE;
27.         IF Fail THEN
28.             State := 3;
29.             Fail := FALSE;
30.             Off_S := FALSE;
31.         END_IF
32.         IF Pumpon THEN
33.             State := 2;
34.             Off_S := FALSE;
35.             Pumpon := FALSE;
36.         END_IF
37.     2:
38.         On_S := TRUE;
39.         IF Pumpoff THEN
40.             state := 1;
41.             Pumpoff:=FALSE;
42.             On_S := FALSE;
43.         END_IF
44.         IF Fail THEN
45.             State := 3;
46.             Fail := FALSE;
47.             On_S := FALSE;
48.         END_IF
49.     3:
50.         Fail_S := TRUE;
51.         Dangerlight := TRUE;
52. END_CASE
```

Function Block del Controller:

```
53.
54. FUNCTION_BLOCK CONTROLLER
55. VAR_INPUT
56. END_VAR
57. VAR_OUTPUT
58.     Idle_S, Normal_S, Warning_S, Cooling_Down_S, Stop_S, Drain_S, Q_S : BOOL := FALSE;
59. END_VAR
60. VAR_IN_OUT
61.     p : PUMP();
62.     t : SENSOR();
63. END_VAR
64. VAR
65.     drain_gas : BOOL := FALSE;
66.     // When pump fail, train stop itself and tanks valves are opened
67.     State : INT := 0;
68.     T1 : TON();
69. END_VAR
70.
71. ------------------------------------------------------------------------------------------
    ------------------
72.
73.
```

```
CASE State OF
    0:
        Idle_S := TRUE;
        IF t.High_S THEN
            state := 2;
            Idle_S := FALSE;
        ELSE
            state := 1;
            Idle_S := FALSE;
        END_IF
    1:
        Normal_S := TRUE;
        IF t.High_S THEN
            state := 2;
            Normal_S := FALSE;
        END_IF
    2:
        Warning_S := TRUE;
        State := 5;
        p.Pumpon := TRUE;
        Warning_S := FALSE;
    3:
        Stop_S := TRUE;
        drain_gas := TRUE;
    4:
        Cooling_Down_S := TRUE;
               IF t.Low_S THEN
                   p.Pumpoff := TRUE;
                   Cooling_Down_S := FALSE;
                   state := 1;
               END_IF
               IF p.Fail_S THEN
                   Cooling_Down_S := FALSE;
                   state := 3;
               END_IF
           5:
               Q_S := TRUE;
               IF p.Fail_S THEN
                   state := 3;
                   Q_S := FALSE;
               ELSE
                   state := 4;
                   Q_S := FALSE;
               END_IF
       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.

Conclusioni

Dall'analisi dei rischi è possibile affermare che l'architettura selezionata, durante il corso, per la realizzazione del progetto non risulta adeguata al sistema sviluppato. Infatti, il sistema andrebbe migliorato attraverso l'inserimento di unità equivalenti in modo che l'accumulo degli errori non porti alla perdita della funzione di sicurezza. Infine, è possibile affermare che 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*.