Università degli studi di Modena e Reggio Emilia

Dipartimento di Ingegneria “Enzo Ferrari”

Corso di Laurea Magistrale in Ingegneria Informatica



Modellazione di un sensore di rilevamento fuga 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:

1. Introduzione
   1. Obiettivo del lavoro e spiegazione dell’ambito di progetto
2. Fault Analysis
   1. Analisi del rischio
   2. Fault tree
   3. Descrizione e cause del fault
3. Riduzione del rischio
   1. PLr
   2. SIL
   3. Mean Time to failure
4. Script Codesys
   1. Schema a blocchi dell’applicazione
   2. Script
5. Conclusioni
   1. Ottimizzazioni e miglioramenti futuri

# Introduzione:

In questo elaborato presentiamo l’analisi del rischio e degli errori di un sistema di rilevamento della temperatura all’interno di una cisterna di GPL.

Nel momento in cui la temperatura supera una soglia critica, simulata manualmente, il sistema andrà ad azionare una pompa di raffreddamento. Il raffreddamento della cisterna è stato modellato con un timer. In caso in cui la pompa è in fault si è scelto di effettuare un rilascio controllato in atmosfera per diminuire la pressione, e quindi la temperatura, all’interno della cisterna.

L’obiettivo è quello di modellare tale caso reale con uno script codesys che permetta di controllare e gestire eventuali problematiche ed effettuare tutte le analisi del caso in modo da prevenire ed aumentare il 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, eccetera. 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 parecchi aspetti si assomigliano tanto è vero 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:

Per il progetto da noi esposto, si deve evitare il più possibile il rilascio, pur controllato, del gas in atmosfera poiché è un evento molto delicato

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.

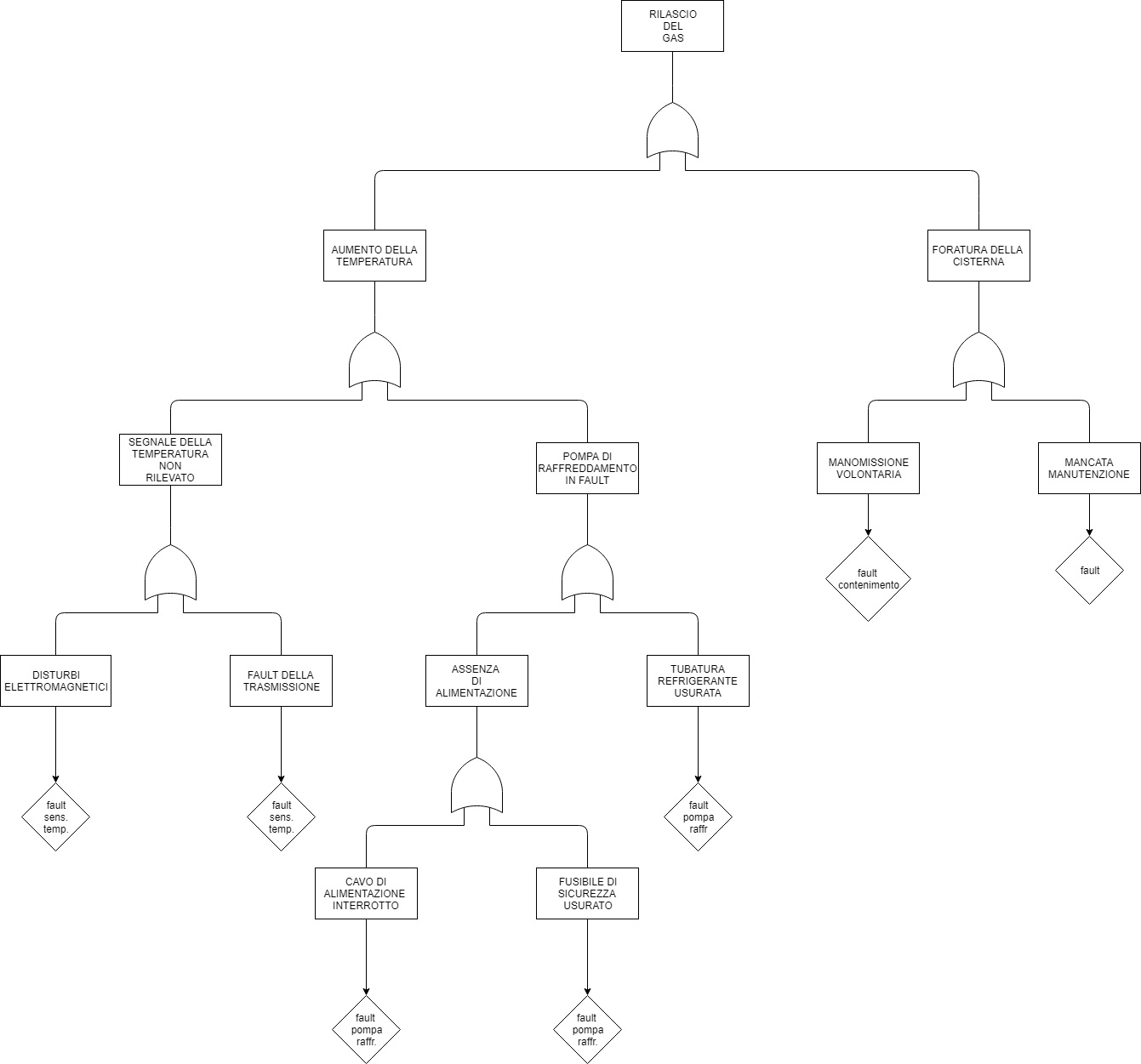


Nella nostra analisi si vuole che un errore o malfunzionamento sia molto raro, più precisamente “occasionale” oppure “remoto”.

Fissata la categoria del malfunzionamento è possibile quindi ottenere la **classe di rischio**.

La classe più adeguata al nostro progetto è la *seconda* poiché il fault del sistema è sempre un evento indesiderabile, ed il costo da sostenere per ottenere un miglioramento è molto elevato

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



Dallo schematico sono state riportate alcune delle principali cause di guasto. Partendo dall’evento del rilascio del gas, si sono sviluppate in modo top down tutte le possibili cause di tale problematica. Da questo grafico si riescono a capire le zone di azione 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 il circuito 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 nomenclati come fault generici.

# Riduzione Del Rischio:

## PLr:

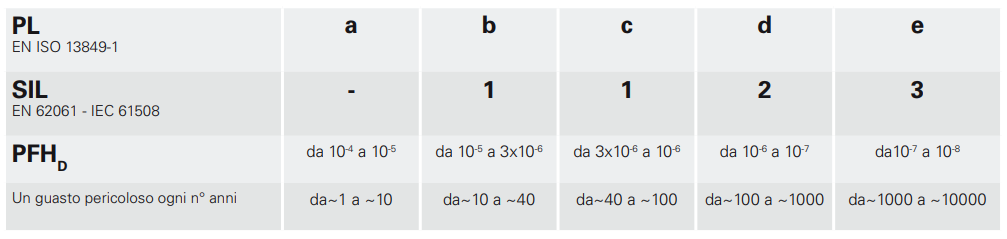
PL (Performance Level) è il livello discreto utilizzato per specificare la capacità delle SRP/CS di eseguire una funzione di sicurezza in condizioni prevedibili. È espresso mediante cinque livelli (“a”, “b”, “c”, “d”, “e”) ad affidabilità crescente.

Per SRP/CS si intende la parte di un 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.

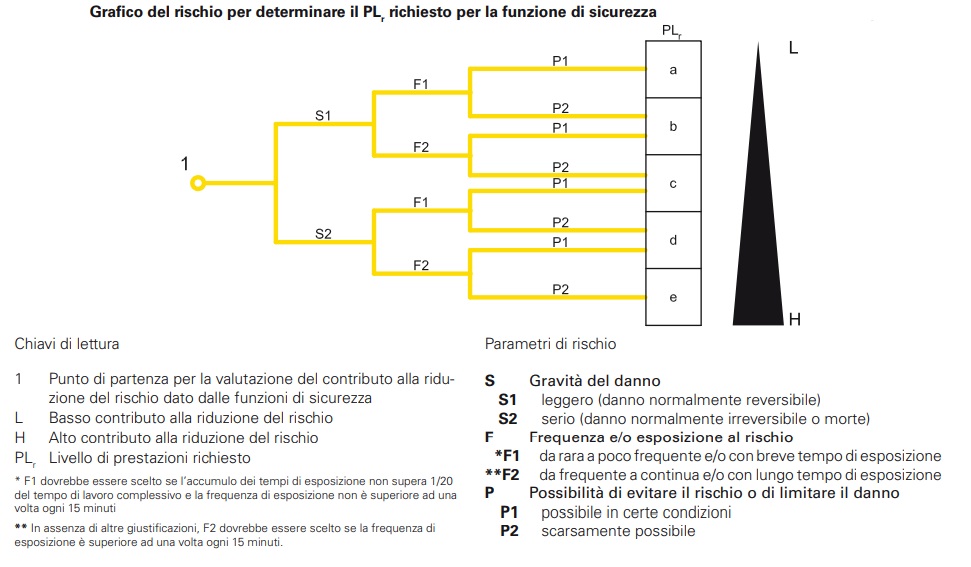
Il PLr (required Performance Level) è invece è il livello di prestazione da raggiungere al fine di conseguire la riduzione del rischio richiesta per ciascuna funzione di sicurezza. Il PLr indica, quindi, quanto dovrà essere affidabile la SRP/CS.

La determinazione del PLr (required Performance Level) 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 (required Performance Level), ad esempio d (PLr = d) oppure e (PLr = e).



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 PLr (Required Performance Level) per la funzione di sicurezza che andrà a proteggere quella parte di macchina.

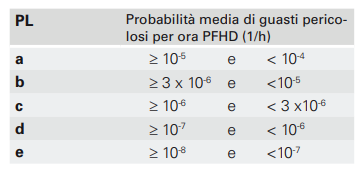
Il costruttore del macchinario, partendo dal punto 1 del grafico e rispondendo alle domande S, F e P identificherà il PLr per la funzione di sicurezza in esame. Dovrà poi realizzare un sistema per proteggere l’operatore della macchina che abbia un livello di prestazione PL uguale o migliore di quello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

Nel nostro caso di analisi, abbiamo:

* Gravità del danno:
  + S2 (rilascio del gas in atmosfera, irreversibile)
* 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 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 1x10-6 e 1x10-7 ovvero all’incirca 1 guasto pericoloso mediamente ogni 100-1000 anni.

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.

Per prendere spunto su cosa scrivere sto seguendo questi link

<https://www.pizzato.it/media/images/catalog/item/File/Pdf/Document/introduzione_sicurezza.pdf>

<https://www.inail.it/cs/internet/docs/alg-pubbl-sistemi-comando-macchine-secondo-norma.pdf>

<https://anieautomazione.anie.it/wp-content/plugins/acd-attach-document/acd-get-document.php?post_ID=522&file_name=2.pdf>

<https://www.ap-publishing.com/wp-content/uploads/2011/06/307_Ispesl_macchine_functional_safety.pdf>