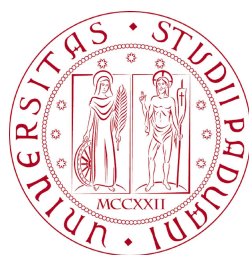


UNIVERSITÀ DEGLI STUDI DI PADOVA  
FACOLTÀ DI INGEGNERIA



*Finito di scrivere il giorno 19 aprile 2013 utilizzando L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub>*

UNIVERSITÀ DEGLI STUDI DI PADOVA  
FACOLTÀ DI INGEGNERIA

—  
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

—  
TESI DI LAUREA MAGISTRALE IN INGEGNERIA  
DELL'AUTOMAZIONE

PROGETTAZIONE DI UN  
DISPOSITIVO DIAGNOSTICO PER  
VALVOLE DI PROCESSO

RELATORE: CH.MO PROF. ING. ALESSANDRO BEGHI

CORRELATORE: CH.MO ING. STEFANO BERNARDI

LAUREANDO: DAVIDE MICHELOTTI

ANNO ACCADEMICO 2012-2013



*ai miei genitori Giorgio e Gabriella e a mia sorella Laura*



*“ Non esistono problemi; ci sono soltanto soluzioni. ”*

ANDRÉ GIDE





# Indice

<b>Sommario</b>	<b>XIII</b>
<b>Introduzione</b>	<b>XV</b>
<b>1 Safety Instrumented System</b>	<b>1</b>
1.1 Introduzione . . . . .	1
1.2 Generalità . . . . .	2
1.3 Classificazione guasti . . . . .	4
1.4 Requisiti e vincoli . . . . .	6
1.4.1 Requisiti quantitativi . . . . .	6
1.4.2 Vincoli architettonici . . . . .	14
1.4.3 Tecniche e misure per evitare guasti sistematici . . . . .	15
<b>2 Valvole di processo</b>	<b>17</b>
2.1 Introduzione . . . . .	17
2.1.1 Componenti principali di una valvola . . . . .	17
2.1.2 Classificazione di valvole in base alla funzione . . . . .	20
2.2 Valvole a sfera . . . . .	23
2.2.1 Seggi . . . . .	24
2.2.2 Principali tipologie di otturatori a sfera . . . . .	25
2.2.3 Coppia richiesta in valvole a sfera . . . . .	27
2.3 Attuatori in valvole a sfera . . . . .	28
2.3.1 Attuatori Single-Acting . . . . .	31
<b>3 HIPPS: High Integrity Pressure Protection System</b>	<b>35</b>
3.1 Introduzione . . . . .	35

3.2	Struttura di un sistema HIPPS . . . . .	36
3.3	Cause di Shut-Down . . . . .	39
3.4	Manutenzione in sistemi HIPPS . . . . .	40
3.4.1	Proof Test . . . . .	41
3.4.2	Partial Stroke Test . . . . .	43
<b>4</b>	<b>FMEDA: Failure Modes, Effect and Diagnostic Analysis</b>	<b>47</b>
4.1	Introduzione . . . . .	47
4.2	Svolgere una FMEA . . . . .	49
4.2.1	Formato FMEA . . . . .	49
4.2.2	FME(D)A . . . . .	50
4.2.3	Reliability Database . . . . .	52
4.3	Analisi FMEDA per valvole di isolamento . . . . .	53
4.3.1	Caso studiato . . . . .	56
4.4	Incidenza del Partial Stroke Test sul SIL . . . . .	58
<b>5</b>	<b>Progettazione dispositivo di PST</b>	<b>63</b>
5.1	Introduzione . . . . .	63
5.2	Configurazione Hardware . . . . .	64
5.3	Sviluppo software dispositivo diagnostico . . . . .	68
5.4	HMI: Human Machine Interface . . . . .	72
5.4.1	Modbus TCP/IP . . . . .	73
5.4.2	Configurazione del sistema diagnostico . . . . .	74
5.4.3	Calibrazione dispositivo . . . . .	77
5.4.4	Partial Stroke Test . . . . .	79
5.5	Diagnosi dei guasti . . . . .	81
5.5.1	Analisi On-Line . . . . .	82
5.5.2	Analisi Off-line . . . . .	83
5.6	Report analisi diagnostica di valvole a sfera . . . . .	86
5.6.1	On-line Error . . . . .	87
5.6.2	Off-line Error . . . . .	91
	<b>Conclusioni</b>	<b>97</b>

<b>A Specifiche tecniche controllore</b>	<b>101</b>
<b>Bibliografia</b>	<b>103</b>



# Sommario

I sistemi di sicurezza ricoprono da sempre un ruolo fondamentale nell'industria di processo. Ponendosi in parallelo al sistema di controllo riescono a prevenire e mitigare danni causati da eventi non gestibili dalla normale routine di controllo. Nel presente lavoro di tesi vengono presi in considerazione sistemi per la difesa da sovrappressioni, detti HIPPS, sviluppando un dispositivo diagnostico con l'intento di verificare periodicamente l'integrità del sistema senza inserire disturbi al processo controllato.



# Introduzione

In questa trattazione sono state approfondite le tematiche riguardanti i sistemi di sicurezza strumentati, sviluppando un dispositivo in grado di predire malfunzionamenti che potrebbero precludere la loro operatività. Il lavoro di tesi è stato sviluppato in collaborazione con Pietro Fiorentini S.p.A., azienda leader operante a livello internazionale nella progettazione, produzione e vendita di componenti, sistemi e servizi per il trattamento, la regolazione e la misura del gas naturale. Sono presenti in 11 stabilimenti italiani ed esteri, impiegando più di 800 persone in tutto il mondo. Nel primo capitolo della tesi, viene fornita una descrizione di come questi sistemi siano utilizzati nell'industria di processo fornendo i principali esempi esistenti. Inoltre, vengono analizzate le modalità di classificazione dei possibili guasti in sistemi di sicurezza relativamente allo standard IEC 61508 fornendo i requisiti e vincoli a cui devono sottostare per garantire la corretta esecuzione delle loro funzioni. Per quanto riguarda il secondo capitolo, vengono introdotte le valvole di processo che rappresentano i principali elementi finali utilizzati per porre il sistema in sicurezza. Viene riportata una breve descrizione delle tipologie di valvole presenti sul mercato con particolare attenzione alle valvole a sfera utilizzate per lo svolgimento del progetto. Successivamente vengono introdotti gli attuatori lineari di tipo fail-safe necessari in applicazioni di questo tipo. Essendo un lavoro di tesi sperimentale, nel terzo capitolo vengono introdotti i sistemi di sicurezza considerati durante il progetto. Viene fornita una dettagliata descrizione dei sistemi HIPPS e della loro struttura. Il principale aspetto considerato è quello relativo alla manutenzione basata sullo standard IEC 61508 che prevede l'esecuzione periodica di proof test. Infine, vengono trattate le modalità del test supplementare di Partial Stroke Test utilizzato nel dispo-

tivo diagnostico progettato. Per determinare gli effettivi benefici introdotti dal test parziale, il quarto capitolo analizza i modi di guasto che possono sorgere in sistemi valvola-attuatore determinando la copertura diagnostica del dispositivo sviluppato attraverso lo svolgimento di un'analisi FMEDA di valvola a sfera riportando infine i miglioramenti introdotti in termini di probabilità di guasto su richiesta. Il quinto capitolo si incentra sulla progettazione del dispositivo diagnostico realizzato, considerando le specifiche hardware e le funzionalità software dell'applicativo sviluppato in Labview. Viene fornita una dettagliata descrizione dell'interfaccia uomo-macchina necessaria all'utilizzo del controllore Real-Time compact RIO e delle modalità di configurazione iniziale del software. Sono quindi esposte le procedure utilizzate dal dispositivo per diagnosticare possibili malfunzionamenti suddividendole tra procedure on-line, eseguite durante il test, e quelle off-line. Infine vengono riportati i risultati sperimentali ottenuti e i test di fault insertion eseguiti sul sistema HIPPS.



# Capitolo 1

## Safety Instrumented System

In questo capitolo verranno discussi i principali aspetti dei sistemi di sicurezza strumentati progettati per attivarsi in caso di guasti allo scopo di proteggere persone, ambiente e beni materiali. Saranno dunque trattate le principali configurazioni esistenti in tale ambito ed infine verranno analizzate le modalità di classificazione dei sistemi SIS basate sullo standard IEC 61508.

### 1.1 Introduzione

La sicurezza delle persone è costantemente assicurata da sistemi SIS (Safety Instrumented System) dove dispositivi elettrici ed elettronici interagiscono con sistemi di tipo meccanico, idraulico o pneumatico. Tali sistemi sono, per esempio, frequentemente utilizzati nelle autovetture. Quando un guidatore preme il pedale del freno, la forza esercitata non è sufficiente per agire direttamente sul disco e quindi un dispositivo elettronico converte la forza del pedale in un segnale elettrico utilizzato per attivare i freni. Durante frenate violente viene attivato il sistema ABS che previene il bloccaggio delle ruote attraverso l'applicazione e il rilascio ripetuto del sistema frenante. Il sistema aiuta il guidatore a mantenere il controllo della vettura. In caso di perdita di controllo e di impatto con altri mezzi, l'elettronica presente rilascerà l'air bag riducendo il danno alla persona. Ovviamente i sistemi SIS hanno un campo di applicazione molto più ampio dell'esempio. Sono infatti di vitale importanza in impianti industriali nel determinare il verificarsi di

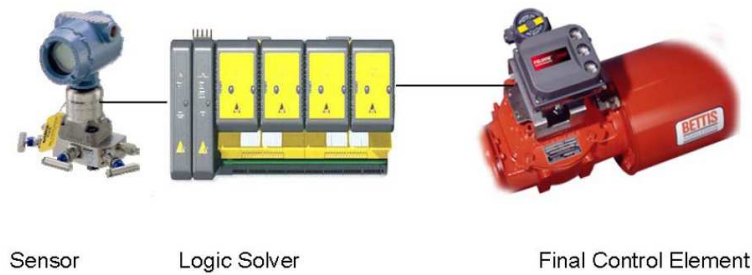


Figura 1.1: Struttura di Safety Instrumented System, [1]

un guasto mitigando le conseguenze a persone, ambiente e beni materiali.

## 1.2 Generalità

Un sistema SIS è definito come un livello di protezione indipendente dal processo che viene installato per mitigare i rischi connessi alla parte di impianto ritenuta pericolosa che si vuole controllare. Solitamente tali sistemi sono composti da tre parti principali: sensori, logic solver e gli elementi finali che possono essere ad esempio valvole di shut-down o freni di una vettura.

Tali sistemi sono utilizzati in molti settori come: sistemi di shut down di emergenza in impianti chimici, rivelazione di incendi o di fuoriuscite di gas, sistemi di posizionamento dinamico per navi e piattaforme offshore, sistemi ATS (Automatic Train Stop), sistema Air Bag e così via. Un sistema di sicurezza strumentato è composto da una o più funzioni di sicurezza SIF (Safety Instrumented Function) che consentono di raggiungere e mantenere in sicurezza il sistema a seguito di una specifica richiesta da parte del logic solver di processo. In aggiunta agli elementi di figura 1.1 un SIS solitamente comprende anche un'alimentazione elettrica indipendente, un'interfaccia utente, sistemi idraulici o pneumatici. Per fornire una guida allo sviluppo di SIS, la commissione Elettrotecnica Internazionale (IEC) ha creato lo standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety related systems". Tale standard tratta i sistemi industriali in generale e quindi fornisce una base per la progettazione e l'implementazione di sistemi di sicurezza. La generalità ha consentito lo sviluppo di standard più specifici come ad esempio IEC 61511 per l'industria di processo. Quello che differisce

maggiormente nei due standard è la descrizione dell'analisi quantitativa e del ciclo di vita degli apparati di sicurezza. Nello standard IEC 61508 sono inoltre descritte le principali funzioni a cui il sistema di sicurezza deve attenersi, che sono:

- Quando si verifica una deviazione del processo nell'apparato controllato da una data SIF, tale variazione deve essere rivelata dai sensori ed i relativi elementi finali devono essere attivati per portare in sicurezza il sistema.
- Il sistema deve essere attivato solamente se si presenta una reale necessità. Attivazioni non necessarie vengono dette Spurious Trip.

### **Esempio di sistema SIS in piattaforme petrolifere**

I sistemi di sicurezza strumentati in piattaforme petrolifere sono suddivisi in tre categorie:

1. Process Control System
2. Process Shutdown System
3. Fire and Gas detection and Emergency ShutDown System

L'obiettivo del sistema di controllo è quello di mantenere i valori delle variabili controllate entro prefissati limiti utilizzando valvole di controllo e regolatori basati su segnali quali temperatura, pressione, indicatori di livello. Quando il processo devia dal comportamento nominale il sistema di shutdown del processo viene attivato, chiudendo la parte di impianto associata. Le azioni richieste per ogni tipo di guasto sono programmate nel logic-solver. Tali azioni possono includere l'attivazione di allarmi, chiusura di valvole di shutdown o apertura di valvole di sfiato. Queste due categorie di sistemi descritte, vengono inserite a livello locale. Gli eventi che hanno la capacità di causare danni di grandi entità sono gestiti dal sistema ESD. Tali problemi includono perdite di gas, incendi e perdite di controllo dell'intero sistema. Le azioni richieste dal sistema ESD sono raggruppate in diversi livelli dipendenti dall'entità e dal luogo di rivelazione dell'anomalia. L'ultimo livello di emergenza richiede solitamente lo spegnimento dell'intera piattaforma e l'evacuazione di tutto il personale.

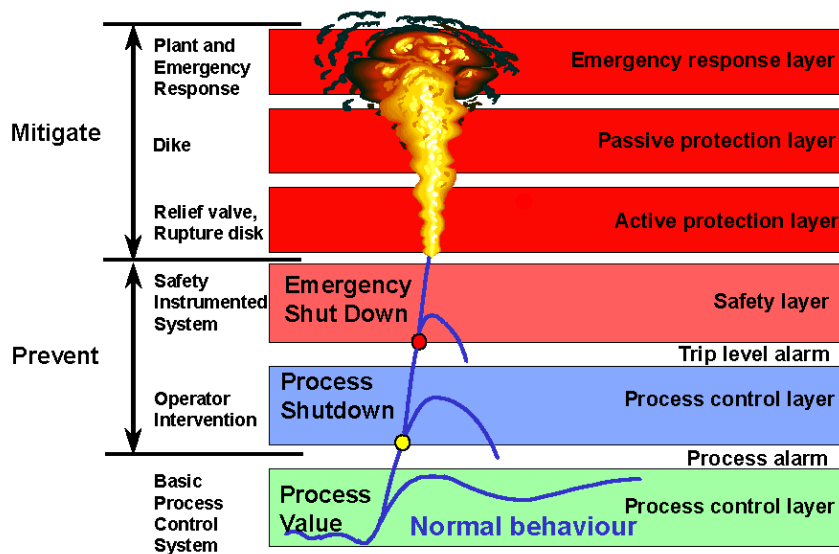


Figura 1.2

### 1.3 Classificazione guasti

Gli standard IEC 61508 [2] e IEC 61511 [3] suddividono i guasti di un sistema SIS in base alle cause che li generano ed in base alla pericolosità del guasto. Quest'ultima può essere suddivisa in:

- Dangerous Failure (D): guasti per i quali il SIS può non essere in grado di operare la funzione di sicurezza su richiesta. Tali guasti possono essere suddivisi in
  - Dangerous Undetected (DU): guasti che non consentono l'esecuzione della funzione di sicurezza e che sono rivelati quando giunge una richiesta dal logic solver per mettere in atto la procedura di sicurezza. Per tale motivo sono anche detti guasti dormienti.
  - Dangerous Detected (DD): pericolose anomalie del sistema che sono rivelate immediatamente quando si verificano, per esempio tramite test automatici.
- Safe Failure (S): sono danni al sistema non pericolosi che non compromettono al SIS di espletare le funzioni di sicurezza. Anch'essi vengono suddivisi

in:

- Safe Undetected (SU): guasti non pericolosi che non sono diagnosticati da test automatici.
- Safe Detected (SD): malfunzionamenti rivelati tramite diagnostica automatica che non vengono considerati pericolosi per l'esecuzione delle SIF.

La classificazione attraverso la causa del guasto è suddivisa in:

1. Random Hardware Failures: sono danni fisici che causano una variazione delle prestazioni del sistema dovuto alla degradazione fisica dei componenti. Si hanno
  - Aging Failure: tali guasti occorrono sono dati da cause direttamente legate all'arco temporale di utilizzo dei componenti. Per questo sono detti guasti primari.
  - Stress Failure: avvengono in base all'eccessivo stress sui componenti causati da fattori esterni o da errori umani durante l'utilizzo o la manutenzione dell'impianto
2. Systematic Failures: sono guasti non fisici che causano una deviazione delle specifiche del sistema senza che intervengano effetti di degrado dei componenti. Essi possono essere eliminati solamente da modifiche strutturali o procedurali del SIS. Tali problemi possono essere suddivisi in:
  - Design Failures: tali guasti si inseriscono durante lo sviluppo del sistema e inizialmente possono essere latenti. Ad esempio sensori che non discriminano tra richieste reali o false.
  - Interaction Failures: tali guasti vengono determinati da errori umani durante le operazioni di manutenzione o testing. Esempio può essere un loop lasciato inattivo dopo il termine di una fase di manutenzione.

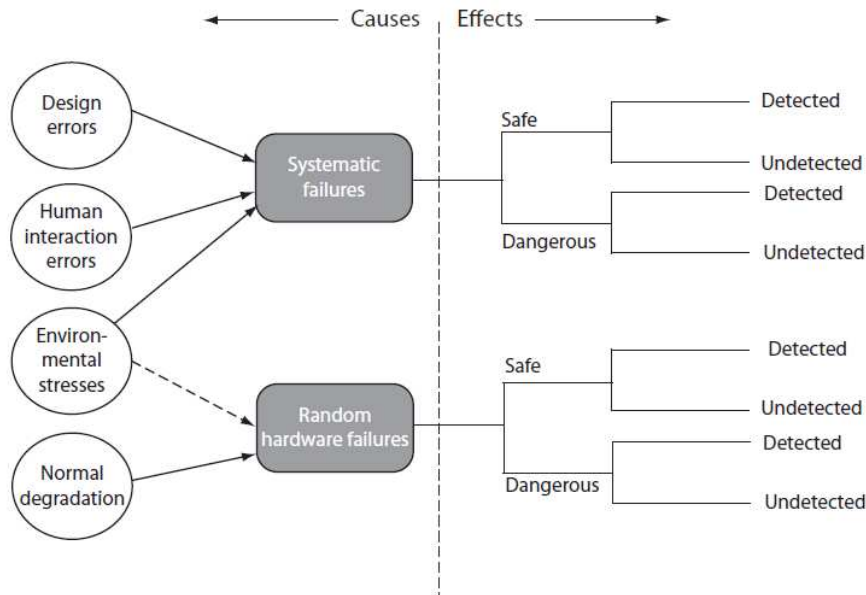


Figura 1.3: Classificazione dei guasti dello standard IEC 61508

## 1.4 Requisiti e vincoli

I sistemi strumentali di sicurezza devono soddisfare un insieme di requisiti che vengono descritti dal SIL (Safety Integrity Level) ovvero un insieme di regole richieste ad un sistema di sicurezza per garantire la corretta esecuzione delle sue funzioni in tutte le condizioni previste. Sono stati definiti quattro livelli nei quali il quarto è quello con i requisiti più severi. Lo standard IEC 61508 definisce tre principali parametri che devono essere soddisfatti allo scopo di ottenere il livello di SIL per cui il sistema è stato progettato. Tali parametri sono:

- Requisiti quantitativi
- Vincoli architettonici
- Requisiti riguardanti tecniche e misure per evitare e controllare i guasti sistemati

### 1.4.1 Requisiti quantitativi

I requisiti quantitativi presenti sullo standard IEC sono espressi in probabilità di fallimento su richiesta, cioè la probabilità che il sistema di sicurezza strumentato

fallisca nell'eseguire le sue operazioni a seguito di una richiesta dal logic solver. Allo scopo, consideriamo ora un componente che è inserito nel sistema di sicurezza al tempo  $t=0$ . Il dispositivo può essere ad esempio una valvola di sicurezza, un sensore o il logic solver. Solitamente i componenti vengono testati e se necessario riparati o sostituiti dopo intervalli di tempo regolari di lunghezza  $\tau$  prestabilita. Il tempo richiesto per le operazione di manutenzione viene considerato trascurabile. Dopo tali test il dispositivo è da considerarsi come nuovo. Sia  $T$  l'istante in cui si verifica un guasto DU sul componente preso in considerazione. L'indisponibilità del componente nell'intervallo  $(0, \tau]$  di assicurare la sicurezza del sistema è data da:

$$\begin{aligned} F(t) &= \Pr(\text{guasto DU si verifici in } (0, t]) \\ &= \Pr(T \leq t) \end{aligned}$$

dove  $F(t)$  è la funzione di distribuzione dell'evento  $T$ , solitamente di tipo esponenziale in quanto fornisce una buona descrizione del tempo di vita dei componenti. La densità di probabilità è data da

$$f(t) = \begin{cases} \lambda e^{-\lambda t} & \text{for } t > 0, \lambda > 0 \\ 0 & \text{altrimenti} \end{cases}$$

mentre la funzione di affidabilità del componente è:

$$R(t) = \Pr(T > t) = \int_t^{\infty} f(u) du = e^{-\lambda t} \text{ for } t > 0$$

Dato che ogni componente è considerato come nuovo dopo ogni operazione di manutenzione, gli intervalli temporali  $(0, \tau]$ ,  $(\tau, 2\tau]$ , ..., risultano identici dal punto di vista statistico. Allora, se al tempo  $t$  avviene una richiesta di attivazione del componente sotto analisi, l'indisponibilità di garantire la funzione di sicurezza denota la probabilità che il componente fallisca a rispondere adeguatamente alla richiesta. Per tale motivo tale quantità è solitamente detta  $PFD_t$  (Probability of Failure on Demand) al tempo  $t$ . In molte applicazioni non si è interessati alla  $PFD_t$  come funzione del tempo. E' sufficiente conoscere la media temporale

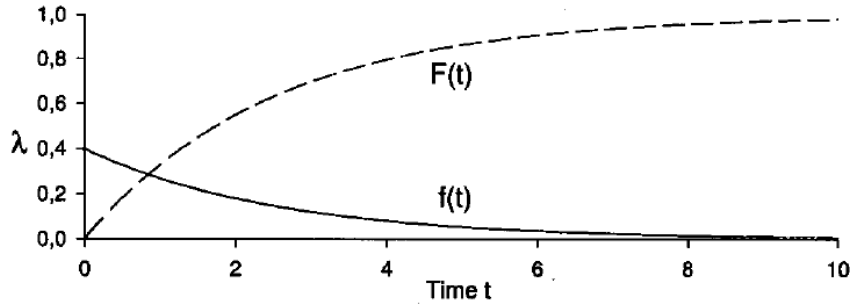


Figura 1.4: Distribuzione esponenziale con  $\lambda = 0.4$

denotata con  $PFD_{avg}$ . Basandosi sulla periodicit  della funzione di indisponibilit  la  $PFD_{avg}$    pari alla relativa media considerata in un intervallo di lunghezza  $\tau$ .

$$PFD_{avg} = \frac{1}{\tau} \int_0^{\tau} F(t) dt$$

Assumendo poi una distribuzione esponenziale per il periodo di vita del componente e una frequenza di guasto costante denotata con  $\lambda$ , intesa come guasti per ore operative *failure/hour*, definiamo  $R(t)$  come la funzione di sopravvivenza del componente rispetto ad un guasto Dangerous Undetected ottenendo:

$$PFD_{avg} = 1 - \frac{1}{\tau} \int_0^{\tau} R(t) dt$$

nel seguito verranno calcolate le probabilit  di fallimento per le configurazioni elementari che costituiscono la base del calcolo della PFD totale.

### Configurazione a singolo componente

Supponiamo che il dispositivo in considerazione abbia una costante di guasto pari a  $\lambda_{DU}$  e conseguentemente una funzione di sopravvivenza pari a  $R(t) = e^{-\lambda_{DU}t}$  allora la relativa PFD sar :



$$\begin{aligned}
PFD_{1oo1} &= 1 - \frac{1}{\tau} \int_0^{\tau} R(t) dt = 1 - \frac{1}{\tau} \int_0^{\tau} e^{-\lambda_{DU}t} dt \\
&= 1 - \frac{1}{\lambda_{DU}\tau} (1 - e^{-\lambda_{DU}\tau})
\end{aligned}$$

sviluppando  $e^{-\lambda_{DU}t}$  in serie di MacLaurin risulta:

$$\begin{aligned}
PFD_{1oo1} &= 1 - \frac{1}{\lambda_{DU}\tau} \left[ \lambda_{DU}\tau - \frac{(\lambda_{DU}\tau)^2}{2} + \frac{(\lambda_{DU}\tau)^3}{3!} + o(\lambda_{DU}\tau)^4 \right] \\
&\cong \frac{\lambda_{DU}\tau}{2}
\end{aligned}$$

Tale equazione è utilizzata frequentemente nella pratica e risulta essere conservativa.

### Configurazione 1oo2

Consideriamo ora due dispositivi dello stesso tipo con costante di guasto  $\lambda_{DU}$  che vengono testati con lo stesso periodo  $\tau$ . La configurazione del sistema viene detta 1-out-of-2 (1oo2) se è sufficiente che solo uno dei due componenti sia in grado di funzionare per preservare la funzione di sicurezza associata. La funzione di sopravvivenza risulta quindi:

$$R(t) = 2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t}$$

$$\begin{aligned}
PFD_{1oo2} &= 1 - \frac{1}{\tau} \int_0^{\tau} 2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t} dt \\
&= 1 - \frac{2}{\lambda_{DU}} (1 - e^{-\lambda_{DU}\tau}) + \frac{1}{2\lambda_{DU}\tau} (1 - e^{-2\lambda_{DU}\tau})
\end{aligned}$$

che approssimando attraverso la serie di Maclaurin risulta:

$$PFD_{1oo2} \cong \frac{1}{3} (\lambda_{DU}\tau)^2$$

### Configurazione 2oo3

Supponiamo ora di avere tre dispositivi con la stessa costante  $\lambda_{DU}$  di guasti pericolosi non rilevati e che il sistema sia testato nei medesimi intervalli temporali di periodo  $\tau$ . Sia la configurazione una 2oo3 dove almeno due componenti devono essere in grado di funzionare. Si ottiene quindi:

$$R(t) = 3e^{-2\lambda_{DU}t} - 2e^{-3\lambda_{DU}t}$$

$$\begin{aligned} PFD_{2oo3} &= 1 - \frac{1}{\tau} \int_0^{\tau} 3e^{-2\lambda_{DU}t} - 2e^{-3\lambda_{DU}t} dt \\ &= 1 - \frac{3}{2\lambda_{DU}}(1 - e^{-2\lambda_{DU}\tau}) + \frac{2}{3\lambda_{DU}\tau}(1 - e^{-3\lambda_{DU}\tau}) \end{aligned}$$

che approssimando risulta:

$$PFD_{2oo3} \cong (\lambda_{DU}\tau)^2$$

### Sistemi in serie

Dato che un sistema di sicurezza è solitamente composto da più dispositivi indipendenti in serie tra loro è utile determinare il comportamento della probabilità di fallimento dati due sistemi con costanti di guasto  $\lambda_{DU,1}$  e  $\lambda_{DU,2}$  supponendo che i test di manutenzione avvengano negli stessi periodi  $\tau$ . I due dispositivi essendo in serie, pregiudicano il funzionamento del sistema complessivo quando uno di questi non è in grado di funzionare. Possiamo affermare che il sistema è in configurazione 2oo2. La funzione di sopravvivenza è dunque:

$$R(t) = e^{-(\lambda_{DU,1} + \lambda_{DU,2})t}$$

$$\begin{aligned} PFD_{2oo2} &= 1 - \frac{1}{\tau} \int_0^{\tau} e^{-(\lambda_{DU,1} + \lambda_{DU,2})t} dt \\ &\cong \frac{(\lambda_{DU,1} + \lambda_{DU,2})\tau}{2} \\ &\cong \frac{\lambda_{DU,1}\tau}{2} + \frac{\lambda_{DU,2}\tau}{2} \end{aligned}$$

Quindi la serie di componenti indipendenti è in buona approssimazione la somma delle PFD dei singoli componenti. Viene ora riportata la tabella riassuntiva delle principali configurazioni utilizzate nella pratica.

$$PFD_{MooN} = \binom{N}{N-M+1} \frac{(\lambda_{DU}\tau)^{N-M+1}}{N-M+2}$$

KooN	N = 1	N = 2	N = 3	N = 4
M = 1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
M = 2		$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
M = 3			$\frac{3\lambda_{DU}\tau}{2}$	$2(\lambda_{DU}\tau)^2$
M = 4				$2\lambda_{DU}\tau$

Tabella 1.1: Approssimazioni di PFD per le principali architetture presenti sistemi di sicurezza

### Common Cause Failure

Fino a questo punto, abbiamo assunto che tutti i componenti siano indipendenti tra loro. Questo tuttavia può non rispecchiare la realtà. I sistemi di sicurezza hanno spesso un alto grado di ridondanza che influenza l'affidabilità del sistema rispetto a guasti causati da fattori comuni. E' dunque importante identificare potenziali cause di guasto comune per attuare le necessarie precauzioni e prevenire tali fallimenti del sistema. Una buona definizione di tali guasti è contenuta in [4] ed è: "Un fallimento dipendente nel quale due o più componenti si guastano contemporaneamente, o in un breve intervallo di tempo, dato da un diretto risultato di una causa in comune.". Per modellare il comportamento di queste dipendenze lo strumento più utilizzato è il modello  $\beta - factor$ . Tale modello definisce che una certa percentuale di tutti i fallimenti relativi al sistema siano del tipo CCF. Consideriamo ora un sistema di N identici componenti con costante di guasto,  $\lambda_{DU}$ . Usando la definizione di CCF un componente potrà guastarsi per:

- circostanze che riguardano lo specifico componente
- eventi esterni che portano al fallimento simultaneo di più componenti

Sia  $\lambda_{DU}^{(i)}$  la costante di guasto rispetto al fallimento dei singoli componenti e  $\lambda_{DU}^{(c)}$  quella relativa alle cause comuni, allora la costante di guasto risultante sarà la somma delle due:

$$\lambda_{DU} = \lambda_{DU}^{(i)} + \lambda_{DU}^{(c)}$$

e definiamo  $\beta$  come:

$$\beta = \frac{\lambda_{DU}^{(c)}}{\lambda_{DU}^{(i)} + \lambda_{DU}^{(c)}}$$

oppure

$$\beta = \Pr(CCF|Failure)$$

Data la mancanza dei dati necessari al calcolo del fattore  $\beta$ , esistono dei metodi basati sull'analisi della struttura del sistema considerato. Lo standard IEC 61508 (2000, Parte 6, Annex D), fornisce un metodo per stimare tale parametro in base a giudizi ingegneristici sul sistema. Allo scopo viene calcolata una funzione  $S = X + Y$  basata su delle interrogazioni che riguardano:

1. Separazione del sistema di sicurezza
2. Diversità e ridondanza
3. Complessità, design, applicazione del sistema
4. Analisi dei dati di guasto provenienti dal campo
5. Documentazione delle procedure da eseguire in caso di fallimenti del sistema di sicurezza
6. Competenza e conoscenza da parte degli operatori del sistema di sicurezza
7. Controllo dell'ambiente in cui è situato il sistema
8. Test effettuati sulla compatibilità ambientale del sistema

Il rapporto  $\frac{X}{Y}$  rappresenta la capacità delle diagnostiche a migliorare le difese contro i CCF. Dopo aver determinato i vari punteggi e ricavata la somma totale  $S$ , il fattore  $\beta$  viene ricavato dalla tabella 1.2

S	Logic subsystem	Sensor or final elements
120 or above	0.5%	1%
70 or 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%

Tabella 1.2: Valori di  $\beta$  rispetto alla somma dei punteggi S

### Malfunzionamenti rivelati mediante diagnosi automatica

Nei moderni sistemi di sicurezza strumentale, i malfunzionamenti possono essere rivelati attraverso una diagnosi automatica condotta da appositi dispositivi. Tale diagnostica si applica ad entrambe le tipologie di guasto (Dangerous e Safe) e viene eseguita così frequentemente che si può ipotizzare che i guasti vengano rilevati immediatamente. Sia  $\lambda_{DT,i}^{(j)}$  la costante di guasto del componente  $i$ -esimo nel sottosistema  $j$  che viene rivelata dalla diagnostica. Se ipotizziamo che ogni dispositivo sia indipendente dagli altri, la costante dei guasti del sottosistema  $j$  rivelati tramite la diagnostica sarà:

$$\lambda_{DT}^{(j)} = \sum_{i=1}^{n_j} \lambda_{DT,i}^{(j)}$$

Solitamente si è a conoscenza della copertura diagnostica che il dispositivo fornisce al sottosistema. Tale quantità è definita come:

$$c_{DT,i} = \frac{\lambda_{DT,i}}{\lambda_i}$$

espressa solitamente in percentuale e descrive la percentuale di guasti che la diagnostica è in grado di prevenire nel componente  $i$ -esimo. I guasti per i componenti si divideranno dunque nelle due categorie di guasti rivelabili o guasti non rivelabili ( $\lambda_{DU}$  e  $\lambda_{DD}$ ).

#### 1.4.1.1 Classificazione SIL per PFD

Sommando le PFD di tutti i sottosistemi indipendenti del SIS, si ottiene infine il parametro che definisce l'affidabilità del sistema. Attraverso tale valore viene

Safety Integrity Level	Probability of Failure on Demand
4	$\geq 10^{-5} to < 10^{-4}$
3	$\geq 10^{-4} to < 10^{-3}$
2	$\geq 10^{-3} to < 10^{-2}$
1	$\geq 10^{-2} to < 10^{-1}$

Tabella 1.3: Livello di sicurezza per funzioni operanti su richiesta, [2]

classificato il livello SIL come in tabella 1.3.

### 1.4.2 Vincoli architetturali

Il secondo criterio che deve essere soddisfatto per un SIS al fine di ottenere un dato SIL sono i vincoli architetturali. Tali vincoli si basano sulla struttura dei dispositivi del sistema e vengono definiti attraverso tre parametri:

- Hardware Fault Tolerance HFT;
- Safe Failure Fraction SFF;
- Tipologia del sistema A o B;

La SFF è data dalla formula

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_{TOTAL}}$$

e rappresenta la percentuale di guasti sicuri rispetto ai guasti totali del sistema. Se la SFF è bassa si avranno dei requisiti più severi per quanto riguarda l'HFT. Quest'ultimo, stabilisce il massimo numero di componenti guastati che possono essere presenti in un sottosistema affinché si abbia ancora la garanzia che la funzione di sicurezza associata sia in grado di funzionare. Per un sistema del tipo KooN si ha che la funzione di sicurezza è preservata se almeno K su N componenti sono in grado di funzionare e quindi l'HFT è dato da N-M. Per quanto riguarda i sistemi di tipo A o B, le tabelle mostrano i vincoli architetturali per sistemi di tale tipo. Considerando lo standard IEC 61508, i sistemi sono di tipo A se:

- tutti i possibili modi di guasto possono essere determinati per tutti i componenti;
- può essere determinato il comportamento dei sottosistemi soggetti all'azione di guasti.
- sono presenti sufficienti dati provenienti dal campo per dimostrare che le costanti di guasti rivelati (Detected) e guasti pericolosi non rivelati (Dangerous Undetected) convergono con quelle stimate.

Altrimenti il sistema deve essere considerato di tipo B.

Safe Failure Fraction [%]	Hardware Fault Tolerance		
	0	1	2
<60	SIL 1	SIL 2	SIL 3
60-90	SIL 2	SIL 3	SIL 4
90-99	SIL 3	SIL 4	SIL 4
>99	SIL 3	SIL 4	SIL 4

(a) Hardware safety integrity: vincoli architetturali per sistemi di tipo A, (IEC 61508-2 table 2)

Safe Failure Fraction [%]	Hardware Fault Tolerance		
	0	1	2
<60	not allowed	SIL 1	SIL 2
60-90	SIL 1	SIL 2	SIL 3
90-99	SIL 2	SIL 3	SIL 4
>99	SIL 3	SIL 4	SIL 4

(b) Hardware safety integrity: vincoli architetturali per sistemi di tipo B, (IEC 61508-2 table 3)

Tabella 1.4

### 1.4.3 Tecniche e misure per evitare guasti sistematici

Il terzo requisito è basato su tecniche e misure da utilizzare per evitare e controllare fallimenti sistematici. Lo standard IEC 61508 distingue tra guasti hardware

casuali e sistematici. I primi sono definiti come guasti che si verificano in un istante casuale come risultato di una o più cause di degradazione nei meccanismi del sistema. Un guasto sistematico è generato da precise cause deterministiche che possono essere eliminate solamente attraverso una modifica del design, del processo manifatturiero o delle procedure. Lo standard dichiara che gli errori sistematici devono essere trattati qualitativamente attraverso delle apposite tecniche che prevedono l'utilizzo di guide interne e procedure per supportare gli operatori durante le operazioni ordinarie e di manutenzione sul sistema.



# Capitolo 2

## Valvole di processo

### 2.1 Introduzione

Per definizione le valvole sono dei dispositivi meccanici progettati per controllare il flusso del fluido di processo. Tali apparati possono essere impiegati in applicazioni che utilizzano fluidi liquidi o gassosi. In base alle funzionalità e alle applicazioni richieste dall'industria di processo sono state progettate diverse tipologie di valvole di diverse dimensioni. Le più piccole possono stare comodamente in una mano mentre le più grandi possono arrivare a pesare fino a 10 tonnellate e avere un diametro di circa 6 metri. Le condotte utilizzate nell'industria petrolchimica presentano un diametro che può variare dai 0,5in fino ai 48in anche se il diametro più utilizzato è quello a 4in presente nel 90% dei casi. Nel progetto di tesi sono state trattate le valvole a sfera, ideali per un funzionamento di tipo on/off e quindi per una funzione di isolamento del processo a valle. L'attuazione di questi dispositivi meccanici può avvenire con diverse sorgenti di alimentazione come ad esempio quella idraulica o pneumatica e con diverse modalità di trasmissione del moto come ad esempio come avviene in attuatori lineari o rotativi in base alla natura della valvola.

#### 2.1.1 Componenti principali di una valvola

Lo spettro di utilizzo delle valvole si estende dal semplice rubinetto dell'acqua fino ad arrivare a valvole dotate di microprocessore che consentono il controllo del



Figura 2.1: Confronto tra una valvola a globo di 1in e una di 30in, [5]

fluido di processo. Le tipologie più comuni impiegate sono le valvole a saracinesca, a sfera e le valvole a farfalla. Tali apparati possono essere fabbricati con vari materiali come: acciaio, plastica, ottone, bronzo e speciali tipi di leghe. Vengono ora descritti i componenti principali delle valvole presenti sul mercato in modo da fornire una conoscenza di base sulle loro modalità operative.

- **Corpo valvola:** è costituito dalla struttura che contiene le parti interne alla valvola come lo stelo, le superfici di tenuta, fermi e isolanti a contatto con il fluido. Sono solitamente progettati in materiali metallici o plastici come ottone, bronzo, acciaio, PVC ma anche da leghe speciali adatte a lavorare in ambienti particolarmente ostili.
- **Cuffia:** parte che racchiude lo stelo e ne determina la sua sigillatura. Viene solitamente avvitata al corpo dopo l'inserimento delle parti interne allo scopo di bloccare i componenti del sistema. Per accedere alle parti interne della valvola è necessario dunque togliere tale cuffia come avviene ad esempio in caso manutenzione dell'otturatore. Valvole come quelle a sfera presentano il corpo valvola e la cuffia costituiti da un unico pezzo.

- **Porte:** rappresentano ingresso e uscita della valvola dove si verifica il passaggio di fluido di processo. Tali estremità sono ostruite dall'otturatore della valvola allo scopo di regolare il flusso. Solitamente vengono utilizzate valvole a due porte anche se sono disponibili sul mercato valvole fino a 20 porte. Infine, la connessione di valvole alle condotte o ad altri componenti avviene attraverso operazioni di filettatura, compressione, flange o per fusione sulle porte.



Figura 2.2: Esempio di valvola a tre porte

- **Attuatori:** le valvole possono essere controllate sia in modalità manuale che automatica attraverso l'utilizzo di appositi meccanismi azionati attraverso manovelle oppure attraverso attuatori di tipo idraulico o pneumatico. Alcune valvole, inoltre, non necessitano di un sistema di tale tipo in quanto lo contengono al loro interno come le valvole di sfogo o di non ritorno che sfruttano il fluido di processo per il loro funzionamento.
- **Otturatore:** Tale componente è un'ostruzione mobile interna al corpo valvola che consente di controllare il flusso. Dipendentemente dal tipo di valvola il corpo di chiusura può muoversi linearmente (globe valve) oppure ruotare attraverso lo stelo (ball valve). Dunque tale componente definisce sia la geometria che i movimenti della valvola e per questo ricopre un ruolo fondamentale nel determinare la scelta della tipologia di valvola in base alle condizioni operative in cui andrà ad inserirsi.

- **Seggi:** sono definiti come la zona interna al corpo valvola il cui contatto con l'otturatore assicura la tenuta del fluido. Nelle valvole lineari quest'ultimo viene a contatto con il seggio solamente a chiusura completa mentre in valvole rotative la superficie di contatto dipende dalla posizione della valvola e non è mai nulla. La classificazione di tali componenti differenzia tra seggi estratti direttamente dal corpo valvola oppure composti da materiali diversi, solitamente più teneri come il PTFE o plastiche dipendentemente della massima temperatura operativa.
- **Stelo:** trasmette il moto tra attuatore e otturatore solitamente attraversando il corpo valvola. Il movimento trasmesso può essere lineare oppure rotativo in base alla geometria dell'otturatore. Per garantire la tenuta di fluido nella valvola, vengono utilizzate guarnizioni tra stelo e cuffia.
- **Molle:** vengono utilizzate per posizionare l'otturatore in posizione di default. Ad esempio nelle valvole di sfogo si utilizza una molla che mantiene la valvola chiusa quando la pressione è all'interno di una soglia nota.

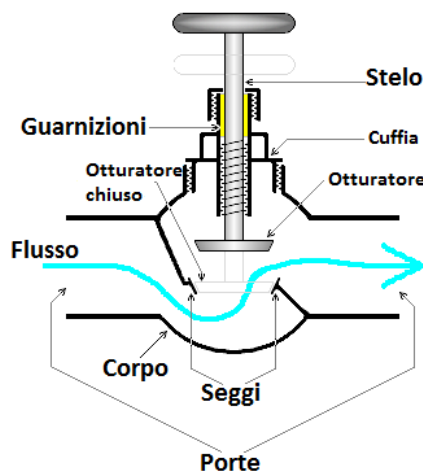


Figura 2.3: Principali elementi presenti in una valvola di processo

### 2.1.2 Classificazione di valvole in base alla funzione

In base alla natura della loro progettazione e alla capacità di gestire il fluido, le valvole possono essere suddivise in tre principali aree:

1. Valvole On-Off: hanno il compito di bloccare o rilasciare il fluido nelle condotte;
2. Valvole di non ritorno: consentono al flusso di scorrere solamente in una direzione;
3. Valvole di regolazione: regolano il flusso tramite il controllo dell'otturatore.

Un aspetto problematico nel suddividere le valvole per la loro funzionalità è dato dal fatto che una tipologia di valvole, come ad esempio le valvole a sfera o a saracinesca, possono rientrare in una, due oppure in tutte le categorie di classificazione e dunque durante la scelta, l'utente deve prestare particolare attenzione ad associare l'esatta tipologia per soddisfare le funzionalità richieste.

### **Valvole On-Off**

Tale categoria rappresenta valvole utilizzate per interrompere o rilasciare il flusso di processo. Le più utilizzate sono le valvole a saracinesca, a sfera e le valvole di sfogo. Solitamente vengono azionate manualmente anche se attualmente vi è un notevole incremento di valvole di blocco utilizzate in remoto attraverso un attuatore idraulico o pneumatico. Esse sono maggiormente utilizzate dove il flusso deve essere deviato rispetto ad un'area dove deve essere svolta un'attività di manutenzione oppure dove il personale deve essere protetto da potenziali rischi causati da malfunzionamenti del sistema. Ovviamente, se utilizzate per quest'ultimo scopo, vi è la necessità che le valvole sia in grado di azionarsi automaticamente appena si verificano delle anomalie. Per quanto riguarda le valvole di sfogo, esse sono essenzialmente valvole automatiche che si aprono solamente quando una pressione di soglia viene raggiunta nel sistema. Tali valvole sono quindi utilizzate per mitigare i danni causati da variazioni anomale della pressione.

### **Valvole di non ritorno**

Le valvole di non ritorno consentono al fluido di scorrere solamente nella direzione voluta. Il dispositivo viene progettato in modo tale da interrompere meccanicamente il fluido quando esso percorre le condotte nella direzione opposta a quella



Figura 2.4: Valvole di sfiato in azione

voluta. Solitamente vengono utilizzate per prevenire ritorni di fluido nel sistema che potrebbero danneggiare gli apparati connessi o creare disturbi nel controllo di processo. Tali valvole trovano il loro massimo impiego nel proteggere pompe o compressori quando vengono spenti.

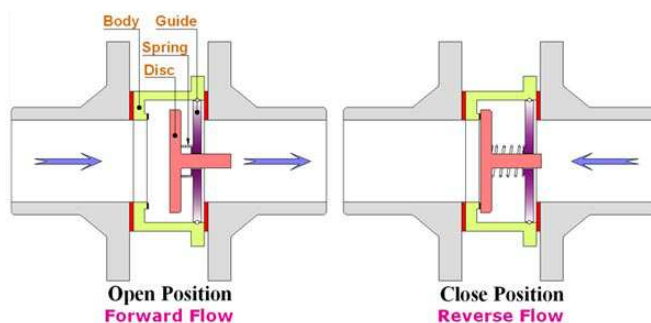


Figura 2.5: Esempio valvola di non ritorno

### Valvole di controllo

Le valvole di regolazione sono utilizzate per controllare il flusso, la temperatura oppure la pressione del sistema. Tali valvole possono essere posizionate in qualsiasi punto all'interno della propria escursione e mantenere tale posizione. Sebbene la maggior parte delle valvole di regolazione siano fornite con azionamento manuale, alcune sono equipaggiate con attuatori che forniscono un migliore posizionamento e la possibilità di essere controllate in modo automatico. L'importanza di tali valvole è data dal fatto che sono gli elementi finali più utilizzati nell'industria e

quindi sono parte integrante del loop di controllo dell'impianto che solitamente consiste in altri due componenti oltre che alla valvola stessa che sono i sensori e il controllore. I sensori vengono utilizzati per misurare una specifica variabile di processo e utilizzano dei trasmettitori per inviare segnali al controller. Quest'ultimo, dopo aver ricevuto l'input dal sensore verifica la deviazione rispetto al valore di set point e se necessario corregge l'andamento tramite la movimentazione della valvola.

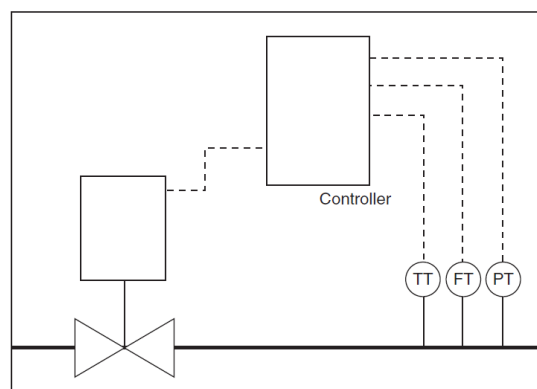


Figura 2.6: Schema di controllo con trasmettitori di flusso (FT), pressione (PT) e temperatura (TT) e relativo controllo sulla valvola di regolazione

## 2.2 Valvole a sfera

Le valvole a sfera sono una varietà di valvole a rubinetto dotate di un membro di chiusura formato da una sfera. Il seggio accoppiato alla sfera è circolare e quindi i carichi presenti su tale componente sono uniformi. Molte valvole a sfera sono fornite con seggi più morbidi rispetto alla sfera in modo da adattarsi facilmente alla sua superficie. Questo tipo di progettazione fa sì che le valvole a sfera abbiano una notevole capacità di tenuta.

La caratteristica di controllo del flusso in una valvola di questo tipo presenta, in alcuni casi, un andamento quasi lineare che favorisce il controllo in catena chiusa sulla parte di impianto considerata. Tuttavia se la valvola è lasciata parzialmente aperta per un lungo periodo di tempo sotto condizioni di elevato salto di pressione attraverso la sfera, il seggio tende a deformarsi causando un possi-

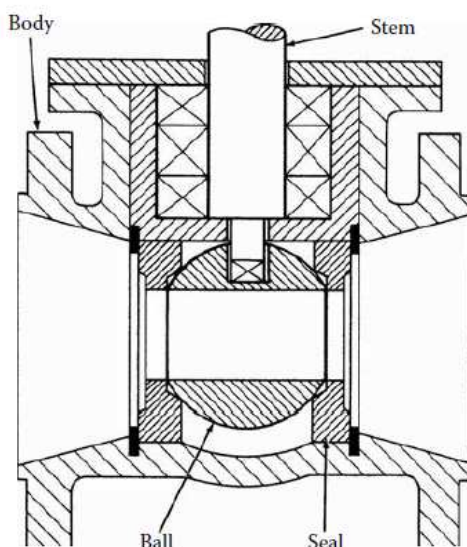


Figura 2.7: Struttura di una valvola a sfera

bile bloccaggio della valvola. Inoltre, dato che il movimento di attuatori lineari utilizzati per azionare la valvola deve essere convertito attraverso connessioni di tipo meccanico vengono introdotti fenomeni di isteresi e zone morte obbligando il progettista ad inserire dei posizionatori per il controllo. Si evince quindi che questo tipo di valvole si presta maggiormente a funzionamenti di tipo on-off.

### 2.2.1 Seggi

La sfera in una valvola di questo tipo è bloccata dai seggi presenti in ingresso e uscita del fluido. Quest'ultimi sono solitamente composti da materiali plastici identici su entrambi i lati. Il materiale più utilizzato è infatti il PTFE che fornisce buona resilienza ed attriti ridotti. In alcune progettazioni i seggi di polimero vengono rinforzati con quelli di metallo allo scopo di assicurare la tenuta della valvola in caso di danni dovuti ad alte temperature come ad esempio nel caso di incendi. Queste ulteriori guarnizioni di metallo sono utili anche in presenza di fluidi contenenti agenti abrasivi o corrosivi in grado di danneggiare i polimeri.

Uno dei principali metodi di progettazione del seggio è riportato in figura 2.10 il quale utilizza la forza generata dalla pressione del fluido che preme il sigillo contro una sfera supportata da un perno. Infine l'utilizzo di O-ring tra sfera



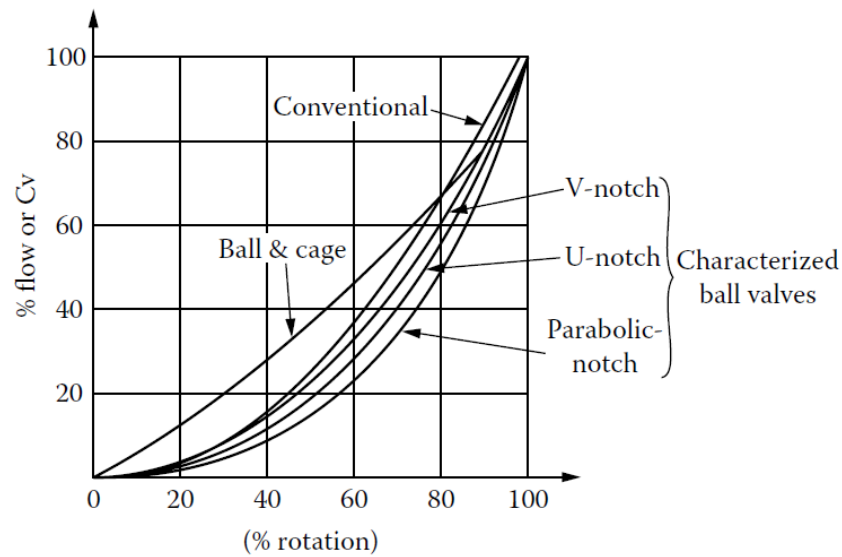


Figura 2.8: Curve caratteristiche del flusso in uscita per diverse tipologie di valvole a sfera

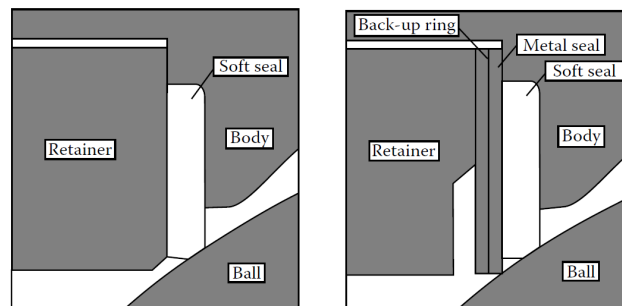


Figura 2.9: Confronto tra valvole con o senza ulteriori guarnizioni di back-up, [6]

e seggio permettono la tenuta del fluido. Quindi questa tipologia di valvole si presta maggiormente nel controllo di fluidi a pressione elevata. Inoltre, è possibile inserire un dispositivo che ruota leggermente le guarnizioni dei seggi ogni volta che viene azionata la valvola allo scopo di distribuirne la loro usura.

## 2.2.2 Principali tipologie di otturatori a sfera

In base alle specifiche richieste sono presenti sul mercato valvole V-notched, U-notched, anti-cavitation anti-noise. Queste valvole furono introdotte allo scopo di risolvere il problema di ostruzione causata da corpi estranei in applicazioni

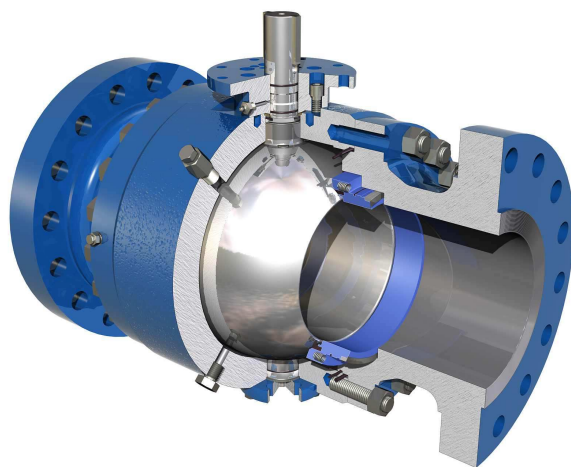


Figura 2.10: Trunnion Ball Valve

dell'industria cartaria. Essenzialmente, in questi tipi di valvole viene modificata la sfera in modo tale da utilizzarne solamente una porzione. L'arco della sfera può quindi essere modificato per determinare la caratteristica di flusso voluta. La valvola viene solitamente chiusa ruotandola dall'alto verso il basso anche se tale proprietà può essere rovesciata. Data l'asimmetria della sfera, queste valvole presentano problemi progettuali che non possono essere trascurati come avviene in valvole tradizionali. Infatti, se la pressione è troppo elevata ci possono essere problemi meccanici dati dalla flessione della sfera che introducono così movimenti lungo l'albero. Una tipica valvola U-notched è riportata in figura 2.11

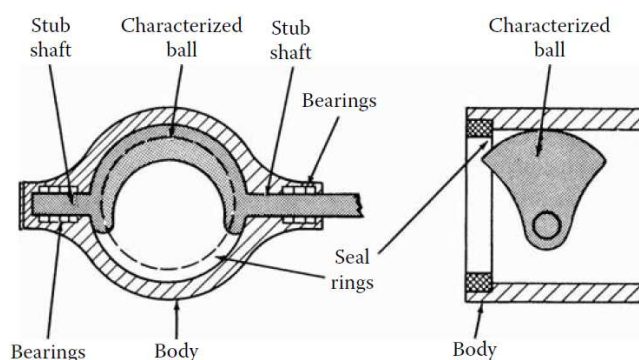


Figura 2.11: Schema di una valvola U-notched e principali componenti

Un altro possibile accorgimento progettuale rispetto alle valvole convenzionali è quello di inserire una componente anti-cavitation e anti-noise. Modificando la

sfera, come in figura 2.12, quando la valvola viene mossa, il fluido passa attraverso degli attenuatori creando vari salti di pressione. La dimensione, posizione e distribuzione dei fori sugli attenuatori permette di modificare le caratteristiche di flusso della valvola.

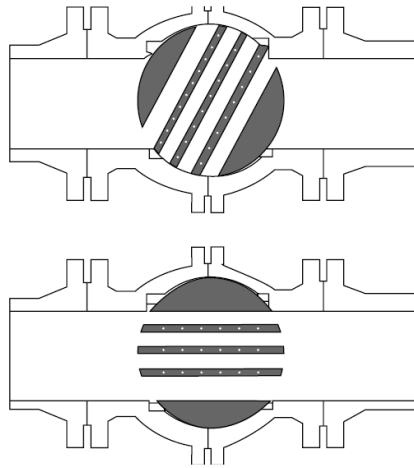


Figura 2.12: Piastre interne di attenuazione che riducono il rumore e la cavitazione. Possono infine modificare la caratteristica di flusso della valvola. [6]

### 2.2.3 Coppia richiesta in valvole a sfera

Prima che l'attuatore possa essere dimensionato è necessario determinare la coppia che si dovrà esercitare per muovere la valvola. La coppia operativa in valvole a sfera è influenzata da molti fattori alcuni dei quali dipendenti dalla progettazione e dai materiali utilizzati mentre altri relativi al tipo di applicazione. I primi includono tipo di materiale utilizzato nei seggi mentre quelli relativi all'applicazione includono la pressione del sistema, la frequenza delle operazioni e la natura del fluido che si sta controllando. Le due principali aree della valvola che determinano la coppia totale sono composte dallo stelo e dalla sfera. In entrambi i casi la coppia resistiva è data da attriti tra metallo e guarnizioni.

- Coppia sullo stelo: dipende principalmente dalla chiusura tra stelo e corpo valvola. Un'analisi dettagliata di tale parametro permette di migliorare le prestazioni e la vita della valvola. Infatti, si determinano perdite esterne se il fissaggio dello stelo è troppo allentato mentre in caso contrario si potrebbe

verificare un blocco della valvola causato da un aumento di coppia troppo elevato per consentirne il movimento.

- Coppia sulla sfera: data dall'attrito tra sfera e seggio risulta molto variabile a seconda delle condizioni operative. Ovviamente più alta è la pressione del fluido, più la sfera è spinta sui seggi e quindi tanto più elevata sarà la coppia necessaria al moto. Dato che materiali differenti presentano coefficienti di attrito diversi, la coppia tra sfera e seggi sarà funzione anche dei materiali utilizzati.

Nel complesso, anche il fluido di processo influenza tale parametro. Si verifica infatti che fluidi abrasivi tendono ad aumentare gli attriti sulla sfera mentre al contrario quelli oleosi possono diminuirla. La coppia necessaria alla valvola è massima all'inizio della sua apertura. Un andamento tipico della coppia in valvole a sfera è riportato in figura 2.13 e mostra che la coppia di chiusura è circa l'80% quella di apertura.

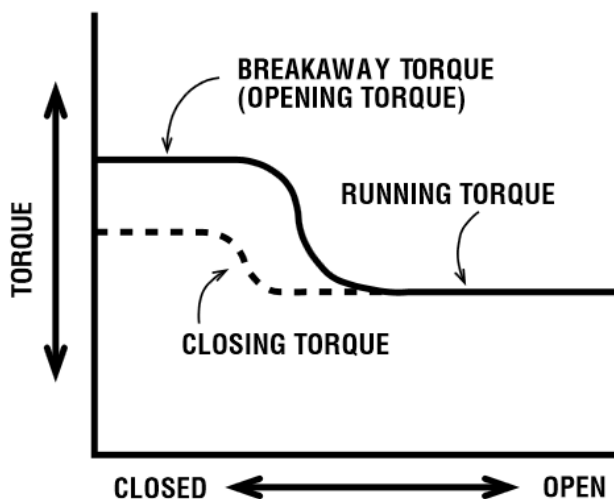


Figura 2.13: Andamento della coppia in valvole a sfera

### 2.3 Attuatori in valvole a sfera

La funzione di un attuttore è quella di controllare la posizione della valvola per garantire il corretto controllo del fluido di processo. Il controllo può essere del tipo

aperto/chiuso come nel caso di valvole di blocco oppure variare in una qualsiasi posizione di tale intervallo come accade nelle valvole di controllo. Per operare efficientemente, l'attuatore deve essere dimensionato in modo da rispondere prontamente ad un segnale di comando in ingresso. Sul mercato sono presenti molte tipologie di attuatori e quello pneumatico a diaframma è probabilmente il più utilizzato e meno costoso. Importanti sviluppi sono stati raggiunti nella progettazione di tali dispositivi al fine di migliorarne accuratezza e velocità. Data la presenza di valvole lineari e rotative sono state sviluppate diverse metodologie di trasmissione del moto che hanno dato vita a sistemi lineari, rotativi e di conversione del moto da lineare a rotativo come ad esempio i meccanismi di scotch-yoke e rack-and-pinion. In figura 2.14 sono riportate le diverse tipologie di attuatori attualmente presenti sul mercato.

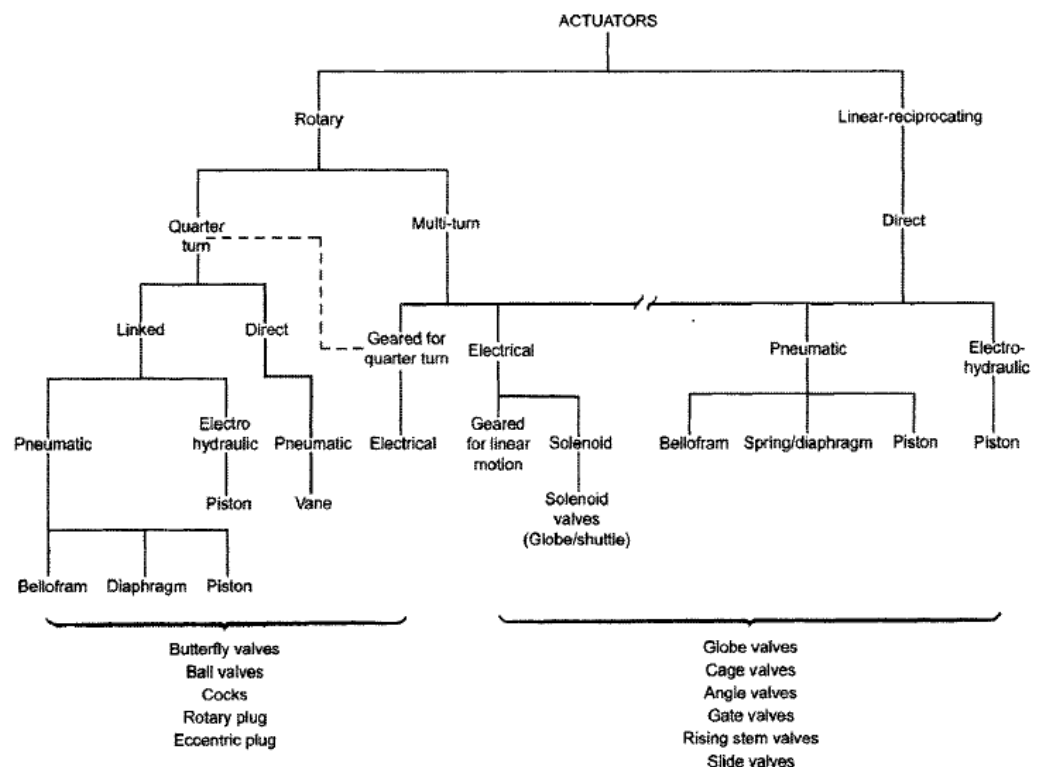


Figura 2.14: Tipologie di attuatori disponibili per valvole di processo, [7]

L'alimentazione più utilizzata per attuatori di questo tipo è sicuramente quella pneumatica in quanto è di facile reperibilità in un impianto industriale oppure può essere facilmente generata sul campo. Vi è inoltre la possibilità di utilizza-

re dei regolatori di pressione per assicurare un'alimentazione stabile. L'aria nei circuiti pneumatici deve essere trattata in modo da eliminare l'umidità presente, prevenendo problemi di ossidazioni o da presenza di cristalli di ghiaccio se la temperatura ne consente la formazione. Altri problemi possono sorgere in presenza di gocce d'acqua o olio che causano ostruzioni del flusso in fori con diametri ristretti. Quindi i sistemi di generazione ad aria compressa devono essere associati ad un sistema di rimozione di umidità verificando che il punto di rugiada in tale strumentazione sia minore della temperatura minima di tutto il circuito pneumatico. L'ISA consiglia di utilizzare un margine di sicurezza di 10°C sotto la minima temperatura operativa. I circuiti pneumatici sono solitamente molto estesi e le perdite di pressione possono variare considerabilmente in base alla richiesta di utilizzo. La zona di lavoro varia tipicamente tra 4 ÷ 10 bar. Le prestazioni effettive di un attuatore pneumatico possono quindi variare considerabilmente. Questi problemi possono essere risolti mediante l'utilizzo di attuatori elettrici nei quali l'alimentazione presenta variazioni trascurabili. Questi attuatori devono essere utilizzati quando la prontezza di attuazione è necessaria alla stabilità del processo. A differenza dell'alimentazione pneumatica, quella elettrica non viene prodotta nel sito ma prelevata da un fornitore causando un aumento dei costi di utilizzo. Se vi sono particolari situazioni in cui l'ambiente circostante la valvola deve essere preso in considerazione, ad esempio a causa di sostanze infiammabili, gli attuatori elettrici prevedono costi elevati per la messa in sicurezza dell'impianto a rischio sconsigliandone quindi l'uso. Infine, quando sono richieste forze elevate possono essere utilizzati attuatori elettro-idraulici. Tali sistemi utilizzano lo stesso principio di quelli pneumatici con la differenza che il fluido gestito non è comprimibile consentendo di sviluppare forze più elevate con minori spazi. La scelta del fluido nel circuito idraulico deve avvenire in particolare se l'attuatore è posto vicino a dispositivi ad alte temperature altrimenti non si hanno particolari restrizioni. Il circuito idraulico risulta comunque più complesso di quello pneumatico dato che è necessaria anche una linea di ritorno della pressione.

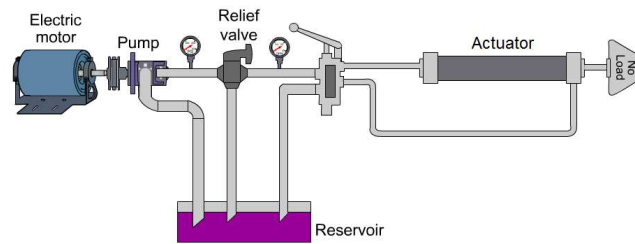


Figura 2.15: Schema di alimentazione in sistemi idraulici

### 2.3.1 Attuatori Single-Acting

Vengono ora considerati gli attuatori idraulici a singolo effetto (single-acting) in quanto sono i principali attuatori utilizzati quando è necessario che il sistema di sicurezza sia del tipo fail-to-close. Per il movimento del sistema viene utilizzato un *pistone* all'interno di un *cilindro* che viene mosso linearmente grazie alla spinta del fluido. Nel caso di funzionamento fail-to-close, viene utilizzata una *molla* che opportunamente dimensionata è in grado di chiudere completamente la valvola e mantenere la posizione al fine di isolare la linea a valle della valvola di blocco. La composizione di questi dispositivi si incentra sul cilindro metallico dove il pistone è in grado di muoversi. I materiali e le dimensioni del cilindro sono dimensionate al fine di sopportare la pressione idraulica a cui è soggetto durante il funzionamento. Le superfici interne vengono trattate in modo da avere tenuta di fluido attraverso le guarnizioni tra pistone e cilindro. Tale trattamento è necessario anche per ridurre i possibili danneggiamenti delle guarnizioni dati dal movimento del pistone. Quest'ultimo viene collegato all'asta tramite fusione o saldatura definendo così l'organo che trasmette il moto. Solitamente vengono trattati in modo da proteggerli da ossidazioni aumentando la vita dell'attuatore. I sistemi a singolo effetto prevedono che il movimento lineare del pistone dato dalla variazione della pressione del fluido avvenga solamente in una direzione. Il movimento inverso è dato dalla forza della molla presente nella parte opposta al pistone. Dunque quando viene incrementata la pressione nel cilindro, il pistone inizia il movimento e la molla inizia a comprimersi. Quando viene aperto il circuito idraulico la forza sul pistone decresce e il movimento inizia nell'istante in cui la forza generata dalla pressione eguaglia quella della molla compressa. Dato che

consideriamo valvole rotative, il movimento viene convertito in moto rotatorio solitamente attraverso i meccanismi di *Scotch-Yoke* o *Rack-and-Pinion*.

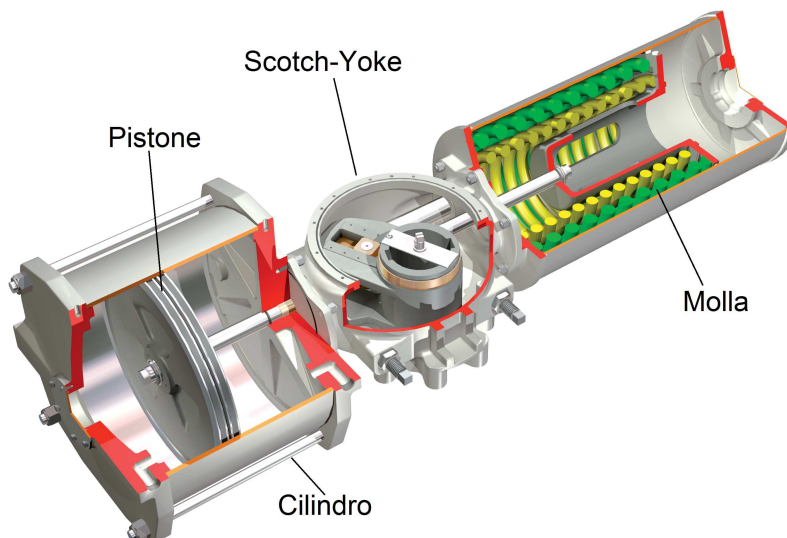


Figura 2.16: Attuatore idraulico a effetto singolo con meccanismo Scotch-Yoke

### Rack-and-Pinion

La conversione di moto avviene tramite una cremagliera. Il principale vantaggio in questo tipo di conversione è che la coppia in uscita è costante. Dato che vengono utilizzate ruote dentate si hanno effetti di dead band dati da backlash meccanico. Il rapporto di trasmissione del moto da lineare a rotativo è dato dalla formula

$$i = \frac{2\pi\varphi_{max}}{s_{max} \cdot 360^\circ}$$

dove

$\varphi_{max}$  massimo angolo di rotazione

$s_{max}$  massimo spostamento lineare

ora calcolando la forza esercitata sul pistone dalla pressione idraulica si ottiene:

$$F_{pistone} = i \cdot \tau_{albero} = p \cdot A - F_{attrito} \quad (2.1)$$

dove



$F_{pistone}$	forza sul pistone
$\tau_{albero}$	coppia sull'albero
$p$	pressione cilindro
$A$	area pistone
$F_{attrito}$	forza attrito

se è nota la coppia necessaria all'albero e si considera trascurabile la forza degli attriti allora è possibile determinare la taglia dell'attuatore invertendo la formula 2.1.

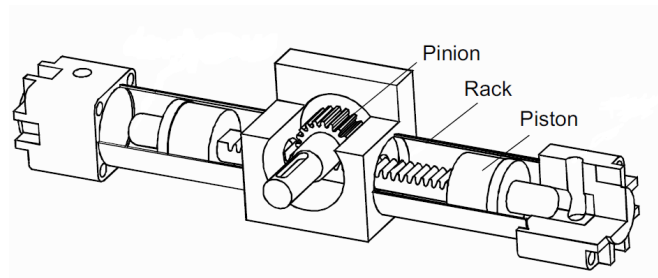


Figura 2.17: Schema del meccanismo Rack-and-Pinion, [8]

### Scotch-Yoke

In questo tipo di attuatori a singolo effetto si utilizza un meccanismo a giogo per convertire il movimento da lineare a rotativo. Un esempio di tali attuatori è mostrato in figura 2.16. La coppia in uscita non è costante come nel caso precedente ma aumenta quando il pistone si sposta dalla sua posizione centrale. Una tipico andamento in un attuatore Scotch-Yoke ad effetto singolo è riportato in figura 2.18. Per dimensionare l'attuatore, in questo caso è necessario verificare che la coppia sulla valvola sia sempre minore di quella dichiarata dal costruttore dell'attuatore.

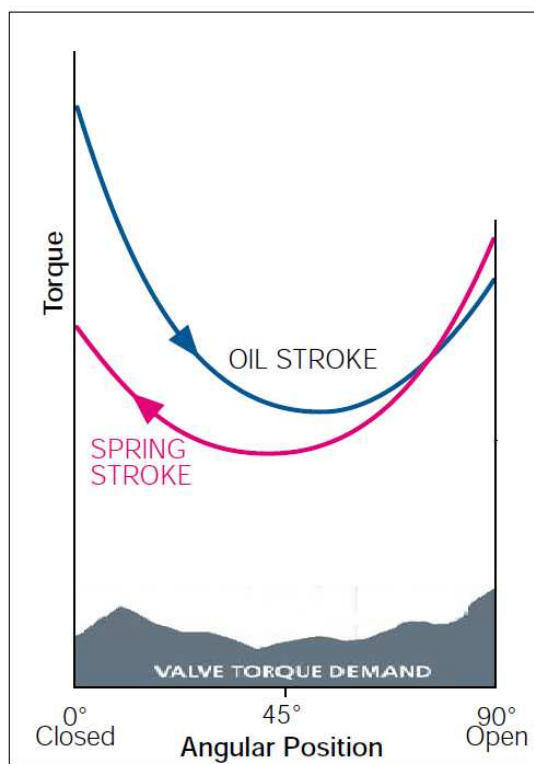


Figura 2.18: Coppia in uscita relativa ad un attuatore Scotch-Yoke ad effetto singolo

# Capitolo 3

## HIPPS: High Integrity Pressure Protection System

### 3.1 Introduzione

Un HIPPS, High Integrity Pressure Protection System, è un sistema di sicurezza strumentato (SIS) con lo scopo di isolare l'impianto nel caso si presentino sovrappressioni che possono sorgere sia a monte del sistema come nel caso di perdita di controllo del pozzo petrolifero, sia a valle nel caso di blocchi inaspettati del processo. Se si verifica lo stato di sovrappressione l'HIPPS dovrà tempestivamente isolare le condotte. Grazie a questa proprietà si verifica la possibilità di progettare il sistema a valle per pressioni minori di quella della sorgente a monte consentendo di utilizzare tubazioni con spessori minori. Data l'importanza del sistema che si interfaccia tra due diversi dimensionamenti delle condotte di monte e di valle, solitamente viene richiesto un livello SIL 3 oppure SIL 4 raggiunto attraverso l'introduzione di forti ridondanze. I principali vantaggi derivanti dall'utilizzo di un sistema HIPPS sono:

- Economici: vi è un notevole risparmio economico nella fabbricazione di linee di minor spessore con un conseguente alleggerimento complessivo delle tubazioni che può essere utile sia dal punto di vista economico che di installazione. In questo modo possono essere gestite pressioni e portate maggiori a costi ridotti.

- Ambientali: riduce possibili perdite di fluido con benefici sull'ambiente circostante.
- Sicurezza: la protezione e l'affidabilità dei sistemi HIPPS prevengono totalmente le sovrappressioni nelle condotte.

Per quanto riguarda i possibili svantaggi che può portare nell'impianto si ha:

- aumento di strumentazione vista come un'ulteriore complicazione all'impianto e sorgente di guasti tecnici
- introduzione di potenziali guasti in valvole o possibili perdite da parte di esse
- possibili complicazioni nel testare le valvole

Per aumentare la sicurezza dell'impianto nel caso in cui il sistema HIPPS fallisca nell'isolare il processo è necessario evitare che l'eccessivo aumento di pressione non causi la rottura dell'impianto a valle. Allo scopo in genere si pone una sezione rinforzata nelle condotte che seguono l'HIPPS. Tale sezione deve essere sufficientemente robusta e per questo si utilizzano tecniche di SRA (Security and Risk Analysis) in grado di determinare il livello di spessore necessario, [9].

## 3.2 Struttura di un sistema HIPPS

Il sistema HIPPS include tutti i dispositivi utilizzati per raggiungere la condizione di fail-safe desiderata. Quindi include l'intero loop di controllo che parte dai sensori sul campo, attraversa il logic solver e si chiude con gli elementi finali. Viene mostrata in figura 3.4 la struttura del sistema utilizzato per il lavoro di tesi. I componenti principali sono:

- **Sensori della pressione di linea:** sono presenti tre sensori di pressione delle condotte ed il fallimento di uno di essi non compromette il funzionamento dell'intera struttura in quanto la configurazione di voting è del tipo 2oo3.

- **Interlock manifold:** allo scopo di prevenire errori operazionali viene inserito un dispositivo meccanico con una chiave mobile che permette la chiusura e l'apertura delle valvole di ventilazione dei sensori di pressione con una sequenza predeterminata. Lo scopo è quello di consentire una calibrazione degli strumenti durante il funzionamento del sistema prevenendo così chiusure indesiderate dell'HIPPS.

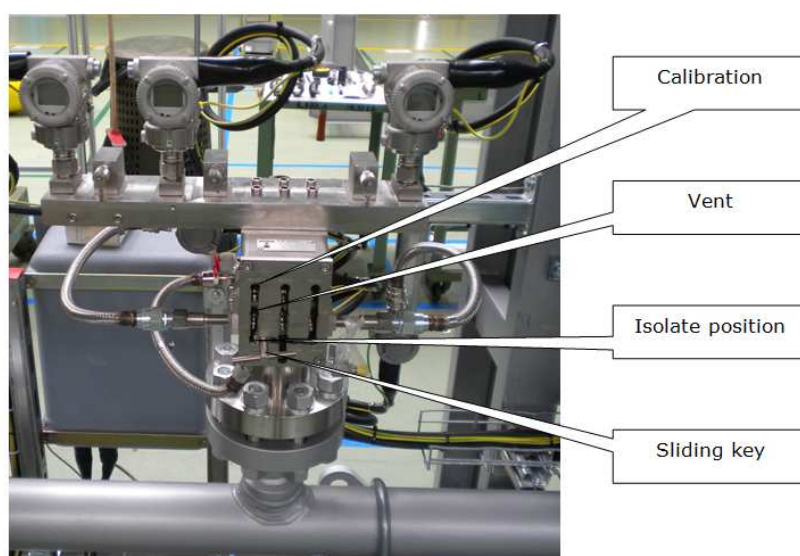


Figura 3.1: Interlock Manifold

- **Logic Solver:** consiste nell'insieme di dispositivi che controlla lo stato del sistema e aziona gli elementi finali in caso di rilevamento di sovrappressioni o malfunzionamenti.
- **Elementi finali:** sono rappresentati dal sistema composto da valvola e attuatore. Nel progetto preso in considerazione vi sono due valvole di blocco a sfera con due attuatori idraulici single-acting in configurazione fail-to-close. Si verifica quindi che è sufficiente il corretto funzionamento di una delle due valvole per proteggere il sistema a seguito di una richiesta del logic solver. Il sistema di alimentazione degli attuatori prevede un circuito idraulico comandato da valvole solenoidi. Sono poste due valvole solenoidi per comandare la valvole a sfera in caso di reale anomalia mentre vi è una terza valvola che consente di testare l'elemento finale attraverso Partial Stroke

Test o Full Stroke Test. Allo scopo è indispensabile osservare l'andamento di pressione e posizione delle valvole a sfera inserendo un sensore di pressione e posizione per ogni attuatore. Inoltre come ulteriore riscontro del corretto movimento della valvola vengono utilizzati tre limit switch che segnalano la posizione aperta, chiusa e intermedia dell'attuatore. Queste componenti verranno considerati nel capitolo implementativo in quanto rappresentano le variabili utilizzate per il controllo del sistema.

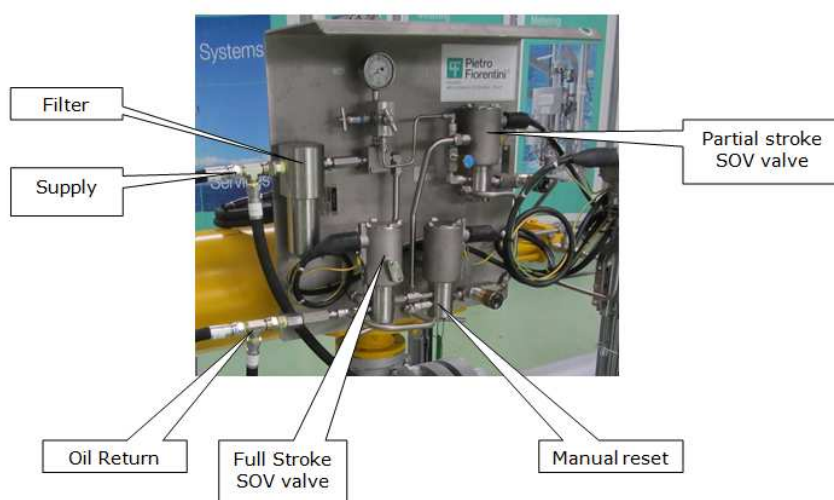


Figura 3.2: Circuito idraulico di controllo dell'elemento finale

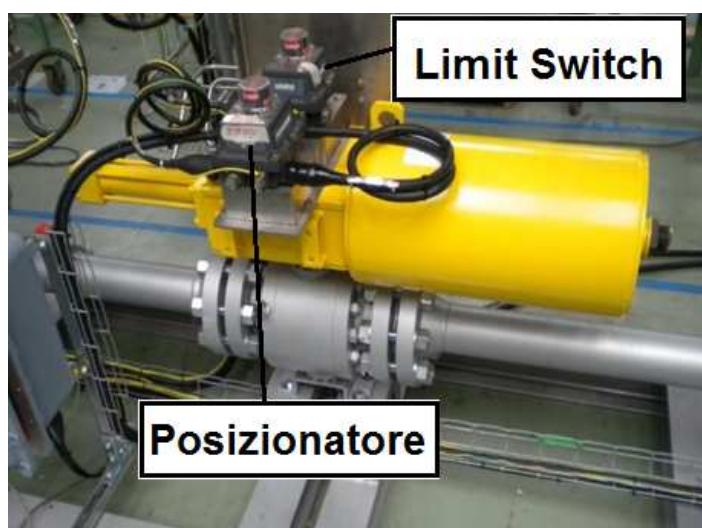


Figura 3.3: Trasmettitori di posizione e limit switch

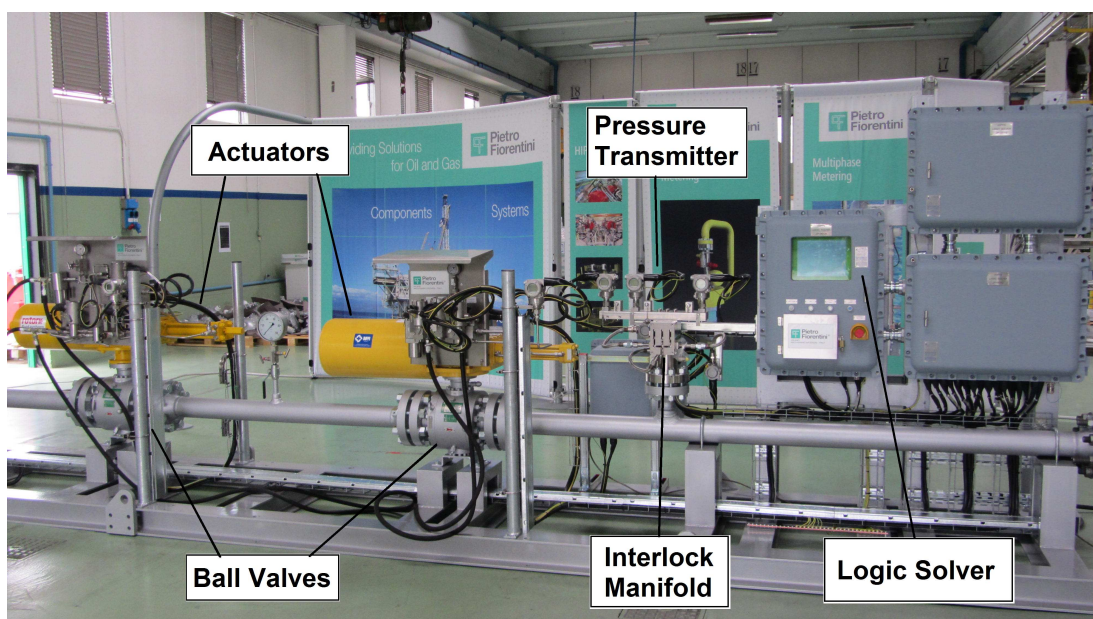


Figura 3.4: Sistema HIPPS

### 3.3 Cause di Shut-Down

Il valore dei sensori di pressione è l'input del sistema di voting utilizzato per verificare se nelle condotte è presente una pressione accettabile. Se il logic solver riconosce che un sensore è guasto o in manutenzione definisce tale componente non valido. Il sistema di voting determina la media delle pressioni considerate valide dal logic solver. Quando il valor medio è maggiore del massimo valore ammissibile oppure minore del minimo valore ammissibile il logic solver diseccita le valvole solenoidi isolando così il sistema a valle. Quando un trasmettitore di posizione viene segnalato come guasto o in manutenzione la pressione media viene determinata utilizzando i sensori complementari. Nel caso in cui vi siano due sensori disabilitati viene impostato un timer di durata pari al valore MTTR (Mean Time To Restoration), di default 24 ore, raggiunto il quale si verifica nuovamente lo stato del sistema e vengono eventualmente chiuse le valvole di blocco se l'errore persiste. Inoltre il sistema di voting compie un'analisi di discrepanza verificando se il valore tra due sensori è maggiore di una certa soglia per un determinato lasso di tempo e concludendo che la media del valore reale della pressione deve essere calcolata con i sensori che sono tra loro consistenti. Ovviamente nel caso

in cui tutti e tre i valori dei sensori non presentino valori comuni non è possibile verificare quale di questi sia esatto e il sistema viene immediatamente chiuso. Il PLC presente nel logic solver presenta anch'esso una diagnostica interna. Il segnale digitale utilizzato per comandare le solenoidi presenta una connessione diretta PLC-valvola solenoide consentendo di verificare la chiusura fisica del loop elettrico. Dato che il circuito di comando è ridondante per ogni solenoide, se il PLC verifica che entrambe le connessioni presentano problemi viene immediatamente isolato il sistema. Come ulteriore sicurezza per l'impianto viene posto un pulsante di emergenza sul cabinet del logic solver in grado di chiudere immediatamente le valvole a sfera.

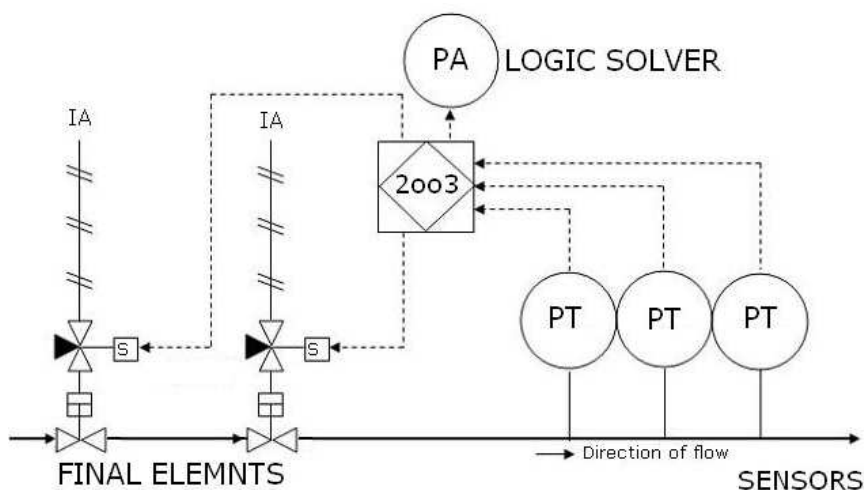


Figura 3.5: Schema di voting tramite l'utilizzo di tre sensori di pressione

### 3.4 Manutenzione in sistemi HIPPS

Lo standard IEC 61508 enfatizza l'importanza di considerare le modalità di test già nella fase di progettazione del sistema. Al fine di mantenere il livello SIL voluto, è necessario attuare dei test per assicurare il corretto funzionamento dei componenti del sistema. Se i dispositivi di sicurezza non fossero testati periodicamente, i guasti pericolosi verrebbero rilevati al verificarsi di una richiesta da parte del processo di attuare una data SIF ponendo così il sistema in uno stato di pericolo dato dall'indisposizione del SIS. Questi test sono eseguiti sia durante che dopo l'installazione del sistema e sono di fondamentale importanza per verificare



lo stato attuale del sistema. Il principale test effettuabile su un impianto viene detto proof test il quale come afferma lo standard IEC 61508 è un test eseguito periodicamente per rilevare malfunzionamenti in un sistema di sicurezza al fine di ripristinare il sistema considerandolo poi come nuovo. Solitamente questi test venivano fatti durante la chiusura di parte dell'impianto che avveniva annualmente. Le economie attuali hanno però forzato le industrie ad aumentare questi intervalli fino ad arrivare in certe situazioni a 8 anni. Questo fatto ha creato molti problemi nel testare i sistemi SIS dato che ha contribuito ad aumentare la complessità dei sistemi di sicurezza e delle metodologie di test. Di particolare interesse sono i test che riguardano le valvole di blocco dato che da un lato esse presentano notevoli difficoltà nei test e dall'altro rappresentano un contributo significativo al fallimento dei SIS.

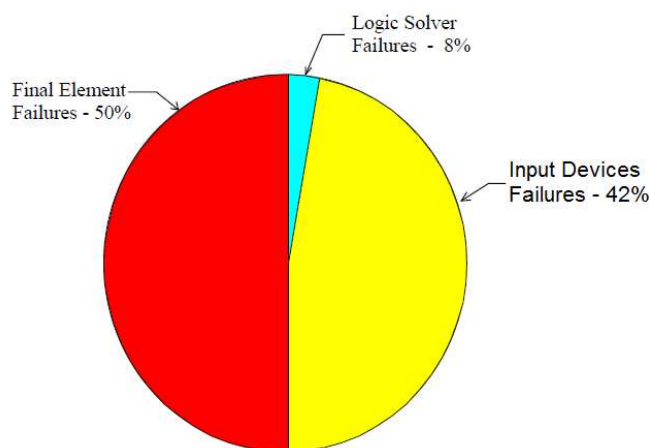


Figura 3.6: Incidenza del fallimento del SIS relativa ai suoi sottosistemi, [?]

### 3.4.1 Proof Test

Questi test possono essere classificati con diverse modalità. La più utilizzata è verificare se il test è di tipo integrale, cioè testare una parte dell'impianto come unica entità, oppure verifica lo stato testando le singole componenti solitamente in istanti differenti. La prima tipologia di test viene eseguita allo start up ma non è resa obbligatoria successivamente. Se vengono condotti test non integrali è comunque buona norma attuare periodicamente test sull'intera parte di impianto considerata per assicurare l'assenza di errori sistematici. Data la difficoltà di

testare le valvole di emergenza, uno dei più comuni test non integrali può essere quello di considerare le valvole solenoidi e il sistema attuatore-valvola come due entità separate.

### Off-Line Testing

Generalmente il problema di testare le valvole di sicurezza nei sistemi SIS richiede come minimo di chiudere completamente la valvola che si trova lungo le condotte nelle quali scorre il fluido di processo creando così disturbi all'impianto a valle. Come già osservato, queste operazioni venivano fatte durante le chiusure dell'impianto che ora risultano troppo distanti e quindi lo stato delle valvole non può essere trascurato durante questo periodo. Inoltre, la garanzia delle funzionalità di questi tipi di SIF e i loro intervalli di test modificano notevolmente il calcolo del livello SIL. Un test off-line è condotto quando il processo che deve essere protetto non è attivo. Uno dei vantaggi di questo tipo di test è che consente nel caso delle valvole di emergenza di performare un proof test che garantisce la verifica totale o quasi dello stato del sistema. L'andamento della PFD relativa a questi test è riportata in figura 3.7 dove si osserva che al termine di ogni test il sistema è considerata come nuovo.

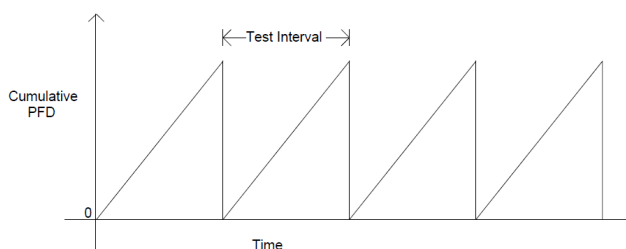


Figura 3.7: Andamento della PFD tramite l'utilizzo di un proof test off-line, [10]

Da un punto di vista pratico non è solito ridurre i regimi operazionali dell'impianto. Come precedentemente osservato, non è richiesto il test di tutti i componenti del SIS nello stesso istante. In particolare le valvole di sicurezza possono essere testate separatamente ad esempio quando vengono eseguiti shut-down periodici della parte di impianto che comprende anche le valvole in considerazione. Questi eventi possono consentire lo svolgere delle operazioni di chiusura completa

delle valvole garantendo di test necessari per mantenere un dato SIL. Problemi possono sorgere nel caso in cui questi shut-down siano troppo distanti tra loro e non si riesca a garantire il livello SIL del sistema di sicurezza. La soluzione consiste nel considerare due diverse metodologie che sono gli on-line test e il Partial Stroke Test.

### **On-Line Testing**

I test on-line sono eseguiti quando il processo controllato è attivo. Sono dunque necessarie delle considerazioni aggiuntive rispetto al caso off-line per gestire il fluido di processo. Una delle soluzioni più adottate è quella di utilizzare una valvola di bypass manuale anche se tende ad essere un metodo costoso e necessita delle precauzioni visto che durante le operazioni di test la valvola del SIS è fuori servizio. Uno degli aspetti positivi è che se il sistema di bypass riesce a sostituire la funzione di sicurezza, allora è possibile apportare le riparazioni necessarie e poi reinserirla nel loop del SIS. Un altro metodo può essere quello di utilizzare valvole di sicurezza parallele abilitandone alle operazioni una solo per volta. Risulta comunque una soluzione molto onerosa dal punto di vista economico e operativo. Si verifica quindi che i test on-line raramente coprono tutte le possibilità di guasto e non precludono la necessità di eseguire periodicamente i test off-line. Inoltre bisogna considerare l'indisponibilità del SIS in termini di rischio e del suo livello SIL. Il compromesso viene raggiunto attraverso l'introduzione del Partial Stroke Test.

#### **3.4.2 Partial Stroke Test**

Questa metodologia di test consiste nel chiudere la valvola di circa 10 ÷ 20% della sua escursione per poi riapirla. Grazie a questo movimento è possibile determinare importanti informazioni relative allo stato della valvola. Dal punto di vista del calcolo del livello SIL si è soprattutto interessati alla copertura diagnostica da parte del test sui guasti pericolosi. Dato che la valvola non chiude totalmente non è possibile verificare lo stato interno della valvola o eseguire test di perdite di fluido, quindi tale test non può essere classificato come un proof test completo

anche se verifica lo stato dei principali componenti del sistema valvola-attuatore. I vantaggi che si hanno attraverso l'introduzione di tale tipologia di test sono:

- Intervalli di test flessibili in quanto il processo viene disturbato relativamente dal movimento parziale
- Miglioramento della PFD per il sistema valvola-attuatore
- La valvola viene testata sul campo per varie modalità di guasto:
- La valvola viene mossa periodicamente: uno dei malfunzionamenti più comuni che si riscontrano in valvole di sicurezza è il bloccaggio dato dal mantenimento della posizione di completa apertura per un periodo prolungato. Movimentare la valvola è un metodo che viene utilizzato per prevenire il blocco del sistema soprattutto con fluidi che formano residui. L'esercizio che esegue il Partial Stroke Test sulla valvola può migliorare le possibilità di eseguire la funzione di chiusura se giunge una richiesta dal SIS. In aggiunta, questo tipo di problema si riscontra anche nelle valvole solenoidi utilizzate per comandare i circuiti pneumatici o idraulici migliorando così anche l'affidabilità dei componenti di controllo dell'attuatore.
- Rilevazione di possibili guasti futuri: alcuni sistemi di partial stroke test forniscono un elevato grado diagnostico e gli andamenti temporali dei test, utili per predire malfunzionamenti futuri. Questo tipo di riscontro può essere utilizzato per segnalare agli operatori la necessità di manutenzione del sistema e quindi prevenire non solo guasti pericolosi ma anche guasti che possono disturbare il processo.

### **Metodologie di Partial Stroke**

Vi sono tre principali tipologie di Partial Stroke Test che dipendono sostanzialmente dalle modalità con cui viene generato il movimento del sistema.

**Meccanico** questa tipologia di test parziale introduce un fermo meccanico collegato alla valvola di blocco che ne limita il movimento di una quantità prefissata. Questa parte meccanica può essere inserita all'interno dei componenti

della valvola oppure costituire un dispositivo esterno applicato durante il test. Questo tipo di componente viene spesso chiamato “jammer”. Solitamente sono semplici dispositivi economici che non richiedono elettronica. Ovviamente forniscono una diagnostica limitata al movimento predeterminato della valvola e non consentono al SIS di performare una richiesta di chiusura durante un eventuale test.



Figura 3.8: Partial Stroke Test meccanico inserito tra valvola e attuatore

**Controllo di posizione** questo sistema utilizza un posizionatore per muovere la valvola con un escursione predeterminata. Dato che molte valvole di emergenza non sono provviste di posizionatore questo metodo richiede l'installazione di ulteriore componentistica. Conseguentemente si hanno dei costi maggiori rispetto al metodo precedente. Un limit switch oppure un trasmettitore di posizione può essere utilizzato per documentare l'esecuzione del test.

**Controllore digitale** vengono utilizzati moderni controllori digitali in combinazione con le solenoidi della valvola di blocco oppure con solenoidi interne dedicate. Come nelle altre metodologie viene chiusa la valvola di una quantità predeterminata e nel caso in cui vi sia una reale richiesta da parte del SIS di chiudere le valvole di emergenza, il dispositivo riesce a bloccare il test e a porre il sistema in sicurezza grazie all'utilizzo di elettronica programmabile. Inoltre, possono essere programmati i vari test durante l'anno e le informazioni raccolte consentono di verificare l'andamento dello stato della valvola. Le curve che vengono registrate si riferiscono solitamente alla posi-

zione e pressione dell'attuatore nel tempo. Questi controllori sono in grado di fornire allarmi che indicano il deteriorarsi del sistema valvola-attuatore allo scopo di intervenire se necessario sul campo. In installazioni dove non è necessaria la supervisione del movimento della valvola durante il PST questi sistemi sono in grado di essere gestiti in remoto fornendo la possibilità di controllare ed analizzare i dati direttamente nelle sala di controllo aumentando così anche la sicurezza del personale.

# Capitolo 4

## FMEDA: Failure Modes, Effect and Diagnostic Analysis

In questo capitolo viene trattata la metodologia FMEDA di analisi dei possibili guasti in un dispositivo meccanico. L'analisi è stata fatta allo scopo di determinare la copertura diagnostica del dispositivo di Partial Stroke Test progettato e il relativo impatto sul sistema SIS in termini di probabilità di fallimento su richiesta.

### 4.1 Introduzione

Un'analisi FMEA, può essere descritta come una modalità sistematica per identificare modi di guasto in un sistema, componente o funzione e valutare l'effetto di tale guasto nei sistemi che si relazionano con quello in esame. L'obiettivo è quello di determinare le cause che generano i malfunzionamenti e le metodologie che possono essere attuate per eliminare o ridurre la probabilità di fallimenti. Una tecnica bottom-up come la FMEA è una procedura efficiente per identificare guasti ai componenti o malfunzionamenti nel sistema. La procedura FMEA è stata sviluppata per la prima volta dall'esercito americano nel 1949 ed utilizzata per verificare l'affidabilità dei sistemi di equipaggiamento. Oltre che nell'ambito militare tale procedura venne inizialmente applicata all'industria aerospaziale estendendosi poi all'industria di processo attraverso lo standard IEC 60812. Una procedura sistematica come quella di una FMEA è utile quando viene sviluppa-

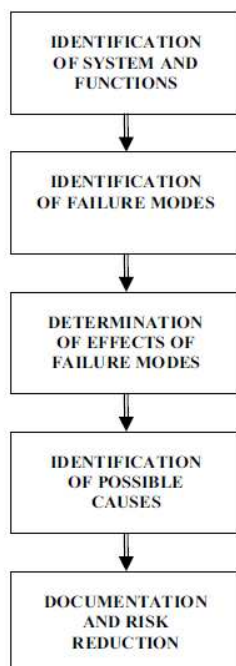


Figura 4.1: Principali fasi nell'analisi FMEA, [11]

to un nuovo prodotto o sistema. L'analisi cerca di dare delle risposte a domande quali: che errori possono sorgere nel sistema, con che entità e cosa può essere fatto per prevenire tali eventi. Quindi questo tipo di analisi fornisce utili informazioni in:

- identificare potenziali malfunzionamenti dati da errori di progettazione
- determinare gli effetti dei modi di guasto
- trovare le cause che generano il malfunzionamento.

In pratica, le risposte sono determinate dalla FMEA attraverso un processo di analisi iterativo, dove le principali fasi sono illustrate in figura 4.1. Lo step iniziale è quello di identificare lo scopo del sistema e le funzioni che devono essere analizzate attraverso FMEA. Il passo successivo è quello di identificare i potenziali modi di guasto mentre in seguito vengono analizzati gli effetti e le possibili cause dei malfunzionamenti. Infine avviene lo stesura della documentazione della procedura e vengono determinate le possibili azioni per ridurre i rischi dei modi di guasto identificati.



## 4.2 Svolgere una FMEA

Come detto, una analisi FMEA può essere molto efficiente nell'identificare modi di guasto in un sistema. Una delle principali ragioni che sostiene questo tipo di analisi è che il sistema può essere modificato per mitigare o ridurre la possibilità del verificarsi di malfunzionamenti. Per questi motivi, la fase di progettazione del sistema è la fase in cui la FMEA trova maggiori possibilità di migliorare il prodotto e dovrebbe essere eseguita quando variazioni nella progettazione possono ancora essere inserite senza distruggere l'intero progetto. Da quest'ultima osservazione si nota come al termine dell'analisi si abbiano a disposizione importanti informazioni rispetto all'affidabilità del sistema.

### 4.2.1 Formato FMEA

In figura 4.5 viene riportata un'analisi FMEA in formato tabulare. Ogni colonna presenta una specifica definizione del contenuto che riguarda:

**Colonna 1** Nome del componente sotto analisi. Dipendentemente dal tipo di FMEA può trattarsi di un componente, un modulo o un intero sistema.

**Colonna 2** Riporta la funzione del componente. Una buona descrizione consente una miglior documentazione delle operazioni del sistema in esame.

**Colonna 3** Viene considerato il livello di ridondanza del componente nel sistema in forma KooN.

**Colonna 4** Numero di componenti complessivi nel dispositivo analizzato.

**Colonna 5** Riporta il  $\beta$ -factor tra componenti dello stesso tipo. Viene posto ad 1 se si sta utilizzando un componente singolo oppure determinato in base alla configurazione attraverso i metodi riportati nel Capitolo 1.

**Colonna 6** Descrive i modi di guasto del componente. Dato che ad ogni componente possono essere associati più modi di guasto viene utilizzata una riga per ognuno di essi.

**Colonna 7** Rappresenta la frequenza di guasto del componente in  $\text{guasti/ora}$ .

**Colonna 8** Probabilità di guasto dell'insieme di componenti presenti nel sistema.

Se il  $\beta$ -factor è unitario viene moltiplicata la Failure Rate per il numero di componenti altrimenti per la quantità  $\beta$ -factor.

**Colonna 9** Riporta il database che contiene la probabilità di guasto utilizzata per il componente. Inoltre sono presenti altre informazioni come ad esempio la fonte utilizzata per la distribuzione dei modi di guasto.

**Colonna 10** Distribuzione dei modi di guasto del componente riportati in percentuale.

**Colonna 11** Probabilità di guasto relativa al singolo modo per il componente sotto analisi, si ottiene tramite la distribuzione dei modi di guasto in colonna 10.

**Colonna 12,13** Effetto causato dal modo di guasto sul sistema complessivo. Viene riportato sia testualmente che con il codice della normativa ISO 14224.

**Colonna 14** Classificazione pericolosità del guasto in base alla funzione di sicurezza considerata.

- S: guasti Safe che non precludono l'esecuzione della funzione di sicurezza
- D: guasti dangerous in grado compromettere il funzionamento del sistema SIS
- NE: guasti No Effect a componenti secondari che non comportano alcun problema per il SIS

#### 4.2.2 FME(D)A

La diagnostica intera ad un sistema SIS è una delle variabili da tenere in considerazione durante la classificazione della sicurezza intrinseca del componente in analisi. Una buona diagnostica migliora sia la sicurezza che l'affidabilità del sistema. Queste tecniche possono essere suddivise in due grandi categorie che sono

la diagnostica di riferimento e quella di confronto. La prima può essere eseguita tramite un'unica unità e la copertura diagnostica può variare considerabilmente da 0 fino ad arrivare a 0.99. Al contrario la diagnostica di confronto richiede due o più dispositivi e la copertura della rivelazione di guasti dipende dall'implementazione ma in generale varia tra lo 0.8 fino ad arrivare a 0.99. La diagnostica di riferimento sfrutta le caratteristiche note di un dispositivo correttamente funzionante analizzando ad esempio segnali di tensione, corrente, posizione, pressione, vibrazioni. Diagnostiche di questo tipo includono analisi acustiche, Partial Stroke Test e analisi nel dominio della frequenza. Per quanto riguarda la diagnostica comparativa essa si basa sulla consistenza dei dati provenienti da differenti unità verificando che i valori dei diversi segnali analizzati siano nei limiti prestabiliti consentendo ottenere un'elevata copertura rispetto ai guasti del sistema sotto controllo.

Dato che la diagnostica influenza notevolmente il calcolo della probabilità di guasto del sistema, l'abilità di valutarne l'efficienza risulta un fattore determinante che deve essere tenuto in considerazione. L'approccio dell'analisi FMEA può essere esteso al fine includere gli effetti della diagnostica che viene effettuata sul sistema, catalogando questo procedimento come FMEDA, Failure Mode, Effects and Diagnostic Analysis. Nell'analisi considerata di figura 4.5 vengono aggiunte le ultime 5 colonne che si riferiscono precisamente a:

**Colonna 15** Tipo di diagnostica utilizzata.

**Colonna 16** Copertura diagnostica sul modo di guasto considerato. Può variare tra 0 (guasto non diagnosticabile) e 1 (guasto identificabile completamente).

**Colonna 17** Tasso di guasto per malfunzionamenti non pericolosi

**Colonna 18** Tasso di guasto pericoloso diagnosticato attraverso l'unità diagnostica utilizzata. Viene determinato semplicemente moltiplicando il fattore di copertura diagnostica per il tasso di guasto associato al modo sotto analisi.

**Colonna 19** Guasti pericolosi non rilevati tramite diagnosi. Vengono determinati moltiplicando il tasso di guasto  $D$  per il complementare del valore di copertura diagnostica.

**Colonna 20** Tassi di guasto che non prevedono effetti sul sistema.

Grazie a questa suddivisione è possibile verificare l'incidenza della diagnostica sul sistema e determinare i benefici apportati sul calcolo della probabilità di guasto su richiesta. L'analisi FMEDA può essere molto efficiente anche se vi sono alcune limitazioni. Il metodo, infatti, analizza solamente la possibile diagnosi dei guasti che sono noti. Il problema riguarda soprattutto dispositivi innovativi nei quali non è possibile basarsi su un database contenente i tassi di guasto dei vari componenti. Per sistemi che necessitano di elevata affidabilità devono essere eseguite analisi approfondite che permettano di simulare guasti e verificare la reale copertura diagnostica del dispositivo, [12].

### 4.2.3 Reliability Database

Per portare a termine un'analisi FMEA è necessario essere a conoscenza dei tassi di guasto dei singoli componenti ed eventualmente della loro distribuzione. Allo scopo sono presenti sul mercato vari database che forniscono una stima delle frequenze di guasto per singoli componenti. Alcuni di questi, sono in grado di fornire la distribuzione dei modi di guasto e dei tempi di riparazione. I componenti vengono classificati in modo da non fornire informazioni sul produttore, modalità di costruzione del dispositivo e particolare specifiche dei componenti. In figura FIG viene riportata la suddivisione di una valvola a sfera presente in OREDA 2002. I tassi di guasto stimati nel database sono solitamente basati su eventi di guasto avvenuti realmente sul campo oppure dati da specifiche prove in laboratorio.

Un'altra importante raccolta di informazioni sull'affidabilità dei componenti è fornita dal Reliability Analysis Center (RAC) che analizza e fornisce importanti informazioni per una vasta gamma di dispositivi con particolare attenzione su componenti elettronici. I principali database distribuiti da tale ente sono:

- Electronic Parts Reliability Data (EPRD)
- Nonelectronic Parts Reliability Data (NPRD)
- Nonoperating Reliability Data (NONOP)
- Failure Mode/Mechanism Distributions (FMD)

**Table 17 Valves, Subdivision in Maintainable Items**

VALVES			
Valve	Actuator	Control and Monitoring	Miscellaneous
<ul style="list-style-type: none"> <li>• Bonnet</li> <li>• Closure member<sup>7</sup></li> <li>• Flange</li> <li>• Other valve components</li> <li>• Packing</li> <li>• Seals</li> <li>• Seat rings</li> <li>• Valve body w/internals</li> </ul>	<ul style="list-style-type: none"> <li>• Case</li> <li>• Diaphragm</li> <li>• Electric motor</li> <li>• Gear</li> <li>• Indicator</li> <li>• Instrument, position</li> <li>• Other actuator components</li> <li>• Pilot valve</li> <li>• Piston</li> <li>• Positioner</li> <li>• Seals (gaskets)</li> <li>• Spring</li> <li>• Stem</li> </ul>	<ul style="list-style-type: none"> <li>• Actuating device</li> <li>• Cabling &amp; junction boxes</li> <li>• Control unit</li> <li>• Instrument</li> <li>• Monitoring</li> <li>• Internal power supply</li> <li>• Valves</li> </ul>	<ul style="list-style-type: none"> <li>• Other</li> </ul>

Figura 4.2: Suddivisione componenti in valvole considerate da OREDA, [13]

Quest'ultimo è stato utilizzato nell'analisi eseguita sulla valvola a sfera per determinare la distribuzione dei modi di guasto dei singoli componenti. Il database utilizzato nel progetto per determinare i tassi di guasto è pubblicato da EXIDA nel quale i dati sono stati determinati mediante analisi FMEDA, dati del produttore del componente e mediante l'appoggio di altri database come OREDA e pubblicazioni del RAC. Questo database contiene principalmente dati su

- Sensori
- Interfacce di I/O
- Interfacce di comunicazione HART
- Logic Solvers
- Elementi finali

### 4.3 Analisi FMEDA per valvole di isolamento

Il modello probabilistico di elementi finali come le valvole a sfera viene determinato con le solite tecniche FMEDA descritte nelle sezioni precedenti. La classificazione dei modi di guasto e la determinazione dei relativi tassi avviene considerando principalmente:

VALVE COMPONENTS



COMPONENT		Valve Components, Ball - Severe Service		ITEM NO.	M.10.2
GENERAL INFORMATION					
COMPONENT TYPE	Valve Components				
COMPONENT SUB-TYPES	Ball - Severe Service				
DATA SOURCE FAILURE RATE	exida Comprehensive Analysis				
DATA SOURCE FAILURE MODES	exida Comprehensive Analysis				
REMARKS	Severe Service: abrasive particles exists in the process fluids / materials Minor Leak: acceptable for ANSI Class I, II and III valves Major Leak: not acceptable for any valve classification				
FAILURE RATE DATA					
				PER 10 <sup>9</sup> HOURS [FITs]	
COMPONENT USE CATEGORY	ALL PROFILES				
Obturator	1260				
Stem	400				
Seat ring	600				
Seat seal	400				
Trunnion	300				
FAILURE MODE DATA					
				[%]	
COMPONENT USE CATEGORY	FAILURE MODE				
	BIND	BREAK	MINOR LEAK	MAJOR LEAK	
Obturator	10	5	70	15	
Stem	30	10	50	10	
Seat ring	5	0	80	15	
Seat seal	0	0	95	5	
Trunnion	70	0	25	5	
USEFUL LIFE					
		[YEARS]	[CYCLES]		
Valve Components, Ball - Severe Service		10	10,000		

Figura 4.3: Database EXIDA relativo all'otturatore in una valvola a sfera, [14]

- Perdite esterne consentite
- Modalità fail-to-open o fail-to-close
- Copertura diagnostica, se presente

### **Livello di tenuta del fluido**

I requisiti relative alle massime perdite esterne di fluido consentite vengono specificate nello standard IEC 60534-4, [15]. Sono presenti sei diverse classi nelle quali la VI è quella più severa che indica il numero di bolle per minuti consentite durante un preciso test di perdita. In molti sistemi di sicurezza strumentati, un evento pericoloso può essere arrestato anche se la valvola presenta delle perdite. Se questo comportamento non è accettabile è necessario considerare una caratteristica di “tight shutoff”. Questo tipo di specifica aumenta il tasso di guasti pericolosi nel sistemi in quanto gran parte degli stress meccanici che danneggiano i seggi o la sfera causano potenziali fallimenti della funzione di sicurezza del sistema. Ovviamente i guasti su componenti che causano perdite esterne non vengono classificati come pericolosi nel momento in cui è consentita una piccola quantità di perdite.

### **Fail-to-Open o Fail-to-close**

La modalità di utilizzo della valvola di sicurezza incide sia sui tassi di guasto, sia sui modi. Uno degli elementi chiave da prendere in considerazione è la posizione che deve raggiungere la valvola al fine di porre il sistema nello stato di sicurezza. Solitamente, nel caso in cui si considerino sistemi di tipo fail-to-open il requisito di “tight shutoff” non è richiesto.

### **Copertura diagnostica**

La diagnostica può migliorare la sicurezza e l’affidabilità degli elementi finali. Nel Capitolo 3 sono state trattate differenti tecniche di Partial Stroke Test che rispondono allo stesso nome. Ovviamente la copertura diagnostica dipende da molti fattori che possono essere ricondotti a:

- Tipo di prodotto utilizzato
- Metodologia di Partial Stroke Test
- Condizioni in cui si applica la diagnostica
- Requisiti di “Tight Shutoff”

### 4.3.1 Caso studiato

Nel progetto di tesi è stato trattato il caso di una valvola a sfera utilizzata in sistemi HIPPS. Come già osservato il comportamento delle valvole utilizzate in questo contesto deve essere del tipo fail-to-close e per questo motivo vengono utilizzati attuatori con molle di sicurezza per garantire la chiusura anche in caso di perdita di alimentazione. In accordo con la normativa ISO 14224 sono emersi dall’analisi i possibili effetti finali sul sistema, che sono:

**FTC** Fail to Close. Causato da malfunzionamenti che prevengono la chiusura della valvola. Sono ovviamente guasti classificati come dangerous dato che la funzione di sicurezza nel caso in esame è l’isolamento del processo e la tenuta del fluido.

**SER** Minor in-Service Problems. Sono tutti quei malfunzionamenti di componenti che non compromettono la SIF.

**LCP** Leakage in Closed Position. Questo modo di guasto prevede la fuoriuscita di fluido in caso di completa chiusura della valvola. Dato che nel caso in esame viene considerata la tenuta del fluido come elemento indispensabile al SIS, questo guasto è classificato come pericoloso.

**ELP** External Leakage Process medium. Perdite di fluido di processo esterne al sistema. Dato che non rappresentano dei problemi che possono modificare il comportamento della SIF vengono considerati come guasti “no effect”.

Dato che lo scopo è verificare il miglioramento introdotto mediante l’utilizzo di un dispositivo di Partial Stroke Test, sono state analizzate le possibili coperture diagnostiche per ognuno dei quattro modi di guasto. Per quanto riguarda il modo



FTC, la copertura diagnostica è stata posta a 0.9 dato che in pratica si verifica che il blocco delle valvole è dato dall'eccessivo periodo di stazionamento in posizione di completa aperta e non per corpi estranei che possono arrestare la valvola in una posizione intermedia. Dato che la valvola durante questo tipo di test non viene chiusa completamente non è possibile verificare alcun tipo di perdita esterna o in posizione chiusa e quindi la copertura per i modi LCP e ELP è stata posta a 0. Infine, dato che i modi di guasto SER identificati per la valvola a sfera sono stati considerati come "no effect" non è possibile stabilire una diagnosi efficace senza osservare variazioni nel comportamento del sistema valvola-attuatore ed è quindi stata posta la copertura a 0. Una breve parte di analisi FMEDA eseguita sulla valvola a sfera è riportata in figura 4.5 mentre i risultati ottenuti sono riportati in tabella 4.1. Per quanto riguarda l'analisi dell'attuatore idraulico, vengono riportati in tabella 4.2 i risultati del produttore dell'attuatore utilizzato nel progetto che vanno quindi infine sommati ai valori precedenti per determinare i tassi di guasto totali del sistema valvola-attuatore.

Ball Valve Failure Rate				
$\lambda_S$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_{DU}$ [1/h]	$\lambda_{NE}$ [1/h]	PST Total Diagnostic Coverage [%]
0	$2,29 \cdot 10^{-7}$	$1.49 \cdot 10^{-7}$	$7.53 \cdot 10^{-7}$	60.64

Tabella 4.1: Risultati ottenuti attraverso analisi FMEDA di una valvola a sfera

Scotch-Yoke Actuator Failure Rate				
$\lambda_S$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_{DU}$ [1/h]	SFF PST	SFF without PST
$1.45 \cdot 10^{-7}$	$1.09 \cdot 10^{-8}$	$1.45 \cdot 10^{-8}$	97.7 %	90.9 %

Tabella 4.2: Risultati forniti dal costruttore dell'attuatore Scotch-Yoke idraulico, [16]

## 4.4 Incidenza del Partial Stroke Test sul SIL

Per verificare l'impatto del test parziale sulla PFD del sistema valvola-attuatore viene inizialmente analizzata la probabilità fornita dal sistema in assenza di diagnostica. L'equazione che determina la PFD media di un componente generico è funzione del tasso di guasti pericolosi stimati e lineare attraverso il periodo di proof test TI in ore, inoltre viene considerato il tempo medio di ripristino in ore, in cui il sistema di sicurezza è indisponibile per operazioni di manutenzione.

$$PFD_{avg} = \lambda_D \cdot \frac{TI}{2} + \lambda_D \cdot MTTR \quad (4.1)$$

Ora, se consideriamo la possibilità di muovere parzialmente la valvola con un intervallo di test  $TI_D$  diversa da quella utilizzata per il Full Stroke Test, allora la formula viene modificata come segue:

$$PFD_{avg} = \lambda_{DU} \cdot \left( \frac{TI}{2} + MTTR \right) + \lambda_{DD} \left( \frac{TI_D}{2} + MTTR \right) \quad (4.2)$$

dove  $\lambda_{DD}$  è la frequenza di guasti diagnosticabili, determinata attraverso l'analisi FMEDA fatta precedentemente, considerando che il proof test abbia una capacità diagnostica del 100%. Per esempio, consideriamo un'estensione del periodo di test completo TI da uno a due anni e introduciamo il test parziale con una frequenza di due volte per anno. La PFD senza diagnostica con TI pari a un anno è determinata dalla formula 4.1 e fornisce:

$$PFD_{avg} = \frac{\lambda_D}{2} \cdot h_{year} + \lambda_D \cdot MTTR \cong 0.5\lambda_D \cdot h_{year}$$

mentre per un test completo ogni due anni

$$PFD_{avg} = \lambda_D \cdot h_{year} + \lambda_D \cdot MTTR \cong \lambda_D \cdot h_{year}$$

Introducendo il PST e determinando la PFD attraverso la formula 4.2 si ottiene:

$$\begin{aligned} PFD_{avg} &= 0.4 \cdot \lambda_D (h_{year} + MTTR) + 0.6 \cdot \lambda_D \left( \frac{h_{year}}{4} + MTTR \right) \\ &\cong 0.55 \cdot \lambda_D \cdot h_{year} \end{aligned}$$

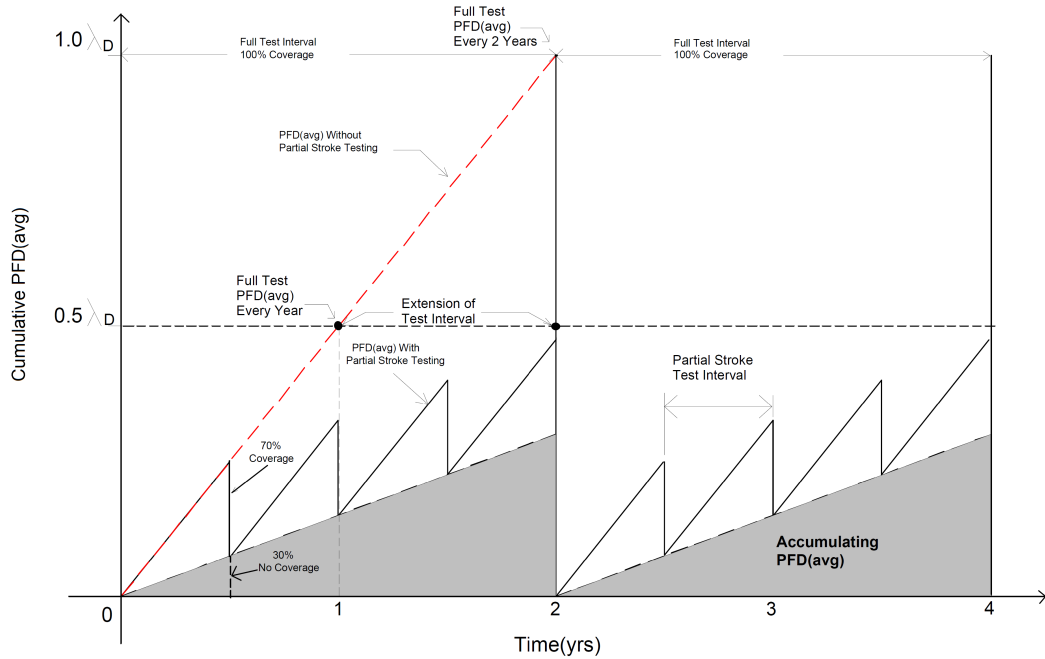


Figura 4.4: Andamento della PFD con implementazione di un PST a frequenza semestrale, [10]

Nella formula sopra è stata utilizzata una copertura diagnostica del 60% ottenuta dai risultati della FMEDA della valvola e attuatore. Il risultato mostra come la probabilità di fallimento nel caso di utilizzo di PST sia prossima a quella che prevede solamente il test completo con frequenza annuale. Si osserva quindi che questo tipo di test parziale può essere impiegato per estendere il periodo tra due Full Stroke Test.

Un altro approccio può essere quello di diminuire la probabilità di fallimento su richiesta mantenendo costante il periodo TI relativo al Full Stroke Test. Se assumiamo che il proof test venga eseguito annualmente e il test parziale con una frequenza di quattro volte ogni anno, la  $PFD_{avg}$  risulta:

$$\begin{aligned}
 PFD_{avg} &= 0.4 \cdot \lambda_D \left( \frac{h_{year}}{2} + MTTR \right) + 0.6 \cdot \lambda_D \left( \frac{h_{year}}{8} + MTTR \right) \\
 &\cong 0.275 \cdot \lambda_D \cdot h_{year}
 \end{aligned}$$

Il risultato evidenzia il miglioramento introdotto nell'aumentare la frequenza di PST dato che la PFD del sistema viene circa dimezzata. D'altra parte, è necessario

considerare i relativi incrementi dei costi relativi all'esecuzione della diagnostica e valutare le problematiche di indisponibilità della funzione di sicurezza durante l'esecuzione dei test programmati. Si conclude quindi che l'introduzione del PST vede come obiettivo primario quello di aumentare il periodo tra test a chiusura completa rispettando i vincoli del livello SIL prestabilito.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Item	Function	Local Architecture	No.	Beta	Failure mode	Failure Rate	Total Failure Rate	Ref.	Failure Distribution	Mode Failure Rate	Final Effect (text)	Final Effect acc. to ISO 14224	Class. SIL (S/D/NE)	Diagn.	DC	Lambda S	Lambda D (DD)	Lambda D (DU)	Lambda NE
Body	Corpo	1001	1	1,00	Broken	1,00E-08	1,00E-08	NSWC, FMD 97 Housing	30	3,00E-09	External Leakage	ELP	NE		0	0,00E+00	0,00E+00	0,00E+00	3,00E-09
			1	1,00	Scored / Dented	1,00E-08	1,00E-08		30	3,00E-09	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	3,00E-09
			1	1,00	Bent / Warped	1,00E-08	1,00E-08		30	3,00E-09	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	3,00E-09
			1	1,00	Bent / Warped (deformati on at seals area)	1,00E-08	1,00E-08		10	1,00E-09	External Leakage	ELP	NE		0	0,00E+00	0,00E+00	0,00E+00	1,00E-09
Seat Spring	Molle elicoidali a compressione	3004	40	0,09	Scored in spring section	5,00E-09	4,38E-10	EXIDA M.8.1 Pos. Retention, no sign. cycles or strokes	48,6	2,13E-10	Internal Leakage (at low pressure)	LCP	D		0	0,00E+00	0,00E+00	2,13E-10	0,00E+00
			40	0,09	Weakened	5,00E-09	4,38E-10		20	8,75E-11	Internal Leakage (at low pressure)	LCP	D		0	0,00E+00	0,00E+00	8,75E-11	0,00E+00
			40	0,09	Scored	5,00E-09	4,38E-10		11,4	4,99E-11	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	4,99E-11
			40	0,09	Sticking	5,00E-09	4,38E-10		8,6	3,76E-11	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	3,76E-11
			40	0,09	Excessive play	5,00E-09	4,38E-10		5,7	2,49E-11	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	2,49E-11
			40	0,09	Worn	5,00E-09	4,38E-10		5,7	2,49E-11	No Effect	SER	\		0	0,00E+00	0,00E+00	0,00E+00	0,00E+00
Ball	Sfera	1001	1	1,00	Deformati on => Binding / Sticking	6,30E-07	6,30E-07	EXIDA M.10.1	10	6,30E-08	Sticking - Movement not possible	FTC	D	Partial Stroke	0,99	0,00E+00	6,24E-08	6,30E-10	0,00E+00
			1	1,00	Broken	6,30E-07	6,30E-07		5	3,15E-08	Structural breakage: potentially dangerous for the safety function	FTC	D	Partial Stroke	0,9	0,00E+00	2,84E-08	3,15E-09	0,00E+00
			1	1,00	Surface damage => Minor leak	6,30E-07	6,30E-07		70	4,41E-07	No Effect	SER	NE		0	0,00E+00	0,00E+00	0,00E+00	4,41E-07
			1	1,00	Surface damage => Major leak	6,30E-07	6,30E-07		15	9,45E-08	TSO not assured	LCP	D		0	0,00E+00	0,00E+00	9,45E-08	0,00E+00

Figura 4.5: Esempio di analisi FMEA di una valvola a sfera



# Capitolo 5

## Progettazione dispositivo di PST

### 5.1 Introduzione

Obiettivo del progetto è la realizzazione di un dispositivo diagnostico per valvole a sfera utilizzabile con attuatori di tipo idraulico o pneumatico. I dispositivi diagnostici presenti oggi in commercio possono essere utilizzati solamente con una tipologia di attuatori limitandone così la generalità d'impiego. Il dispositivo diagnostico dovrà offrire e garantire l'interoperabilità tra attuatori. Il principale campo di utilizzo è quello dei sistemi SIS, in particolare in HIPPS. Il dispositivo svolgerà una pura funzione diagnostica e quindi non farà parte del loop di sicurezza del sistema associato non influenzando la PFD. Inoltre, il logic solver del SIS sarà in grado di monitorare la richiesta di chiusura della valvola parallelamente all'esecuzione del test preservando in ogni istante la funzione di sicurezza del sistema. Il dispositivo è stato progettato su sistemi HIPPS, trattati nel Capitolo 3, utilizzando le variabili di pressione e posizione dell'attuatore durante la chiusura parziale della valvola. Il loop in cui è stato inserito questo dispositivo prevede una valvola solenoide in grado di pilotare il circuito idraulico utilizzato per movimentare l'attuatore. Il controllo del sistema è determinato attraverso le variabili di posizione e pressione dell'attuatore fornite da due appositi trasmettitori inseriti nel sistema SIS come ulteriore garanzia di corretto funzionamento della funzione di sicurezza. Lo schema di controllo riportato in figura 5.1 mostra l'interconnessione dei principali sottosistemi utilizzati considerando le variabili

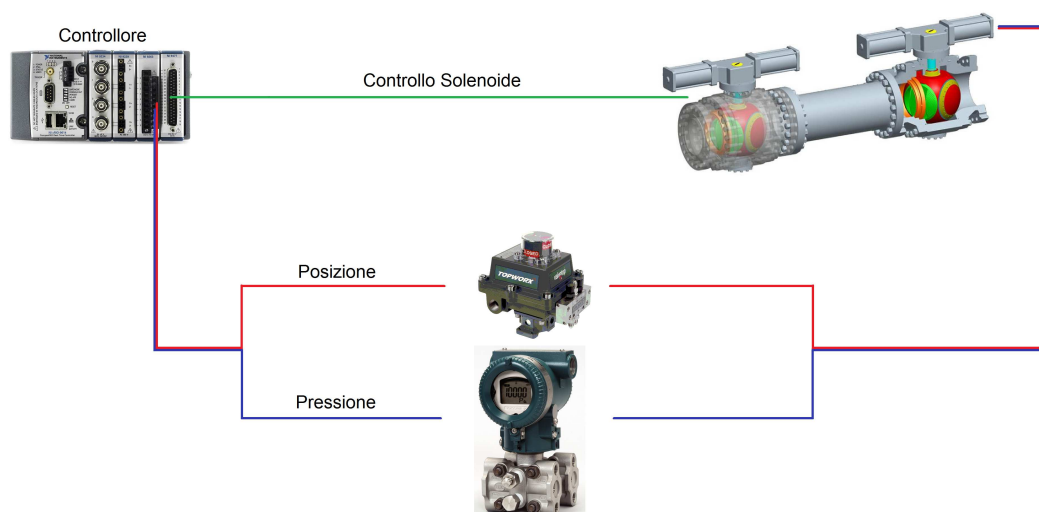


Figura 5.1: Loop di controllo del sistema di Partial Stroke Test

controllate di posizione e pressione e quella di controllo identificata dal comando alla solenoide del tipo on/off. Dato che si tratta di diagnostica Partial Stroke Test eseguita tramite un controllore digitale, il sistema è in grado di analizzare le curve di risposta compiendo una prima analisi completamente automatica al fine di fornire lo stato di degrado del sistema valvola-attuatore. Infine, vengono registrati tutti i test eseguiti in modo di consentire all'utente di valutare l'andamento del comportamento della chiusura parziale nel tempo.

## 5.2 Configurazione Hardware

Il sistema di diagnosi sviluppato durante il progetto, vede come elemento centrale il controllore CompactRIO 9004 della National Instruments. Date le sue ridotte dimensioni può essere utilizzato per eseguire svariate applicazioni come acquisizioni sul campo, monitoraggio e controllo di macchine industriali. Esso è costituito dalle seguenti parti assemblate in un unico case:



- Chassis NI-9103



Figura 5.2: Backplane NI-9103

- Controller Real-Time 9004



Figura 5.3: Real Time Controller NI-9004

- Moduli di I/O



Figura 5.4: Moduli I/O compatibili con chassis 9103

Il primo dei tre, rappresenta il cuore del sistema in quanto contiene il nucleo di I/O riconfigurabile (RIO) con 3 milioni di porte logiche programmabili. Il RIO FPGA (Field Programmable Gate Array) presenta una connessione con ogni modulo I/O ed è programmato con funzioni elementari che permettono di scrivere o leggere informazioni sui canali provenienti da ognuno di essi. Questo componente è collegato al controller real-time tramite un bus locale di standard PCI. Il controllore NI-9004 garantisce l'esecuzione on board di applicazioni Real-Time di tipo deterministico realizzate tramite l'ambiente di sviluppo Labview. Tra le principali caratteristiche vi sono: 64 MB di DRAM, 512 MB di memoria flash per la memorizzazione di dati, design realizzato per lavorare mantenendo la propria affidabilità anche in ambienti ostili con temperature comprese tra i -40 ed i 70°C. Come processore viene utilizzato un processore industriale Pentium a 400 MHz che garantisce analisi e elaborazione di funzioni ad una frequenza anche superiore ad 1kHz. I moduli I/O si collegano direttamente al RIO FPGA e costituiscono un sistema ad alte prestazioni che conferisce alle applicazioni di input/output realizzate tramite software le qualità e la flessibilità di un tradizionale circuito elettrico completamente dedicato a tali funzioni. Ogni modulo, inoltre, contiene internamente applicazioni di condizionamento del segnale che consentono, in molti casi, il collegamento diretto a sensori ed attuatori. La scheda digitale utilizzata per il controllo della valvola solenoide è la NI-9401 che presenta 8 canali digitali ad alta velocità (100 ns) e può assumere tre configurazioni: 8 ingressi, 8 uscite, 4 ingressi e 4 uscite ed è compatibile con la logica TTL. Per quanto riguarda l'acquisizione dei segnali analogici di pressione e posizione dell'attuatore, viene utilizzata la scheda NI-9201 che include 8 ingressi analogici ed è in grado di raggiungere una velocità di campionamento di 500 kS/s, presenta una risoluzione di 12 bit ed acquisisce segnali in tensione di intensità compresa tra -10 V e + 10 V. Le specifiche complete del sistema cRIO utilizzato viene riportato in Appendice A. Il controllore preso in considerazione è inserito nel loop di controllo come in figura 5.1 ed è direttamente collegato ai trasmettitori di pressione e posizione dell'attuatore che utilizzano un segnale analogico  $4 \div 20$  mA. Dato che viene utilizzata una scheda di acquisizione analogica in tensione, sono stati applicati al segnale di ingresso due isolatori che convertono il segnale per ottenere un range di  $1 \div 5$  V. Inoltre questi isolatori sono

utili dato che separano galvanicamente i circuiti che si collegano ai trasmettitori, come ad esempio i collegamenti presenti con il PLC del logic solver che controlla l'intero sistema HIPPS. Per quanto riguarda il segnale di controllo digitale della valvola solenoide viene inserito un relè a stato solido per pilotare i 24V necessari per il corretto funzionamento della solenoide. L'inserimento di questo elemento aggiuntivo è stato inevitabile in quanto la scheda di uscita digitale è predisposta per pilotare segnali TTL a 5V. Come già osservato, questa solenoide controlla il flusso all'interno del circuito pneumatico consentendo di caricare o scaricare la pressione nell'attuatore.

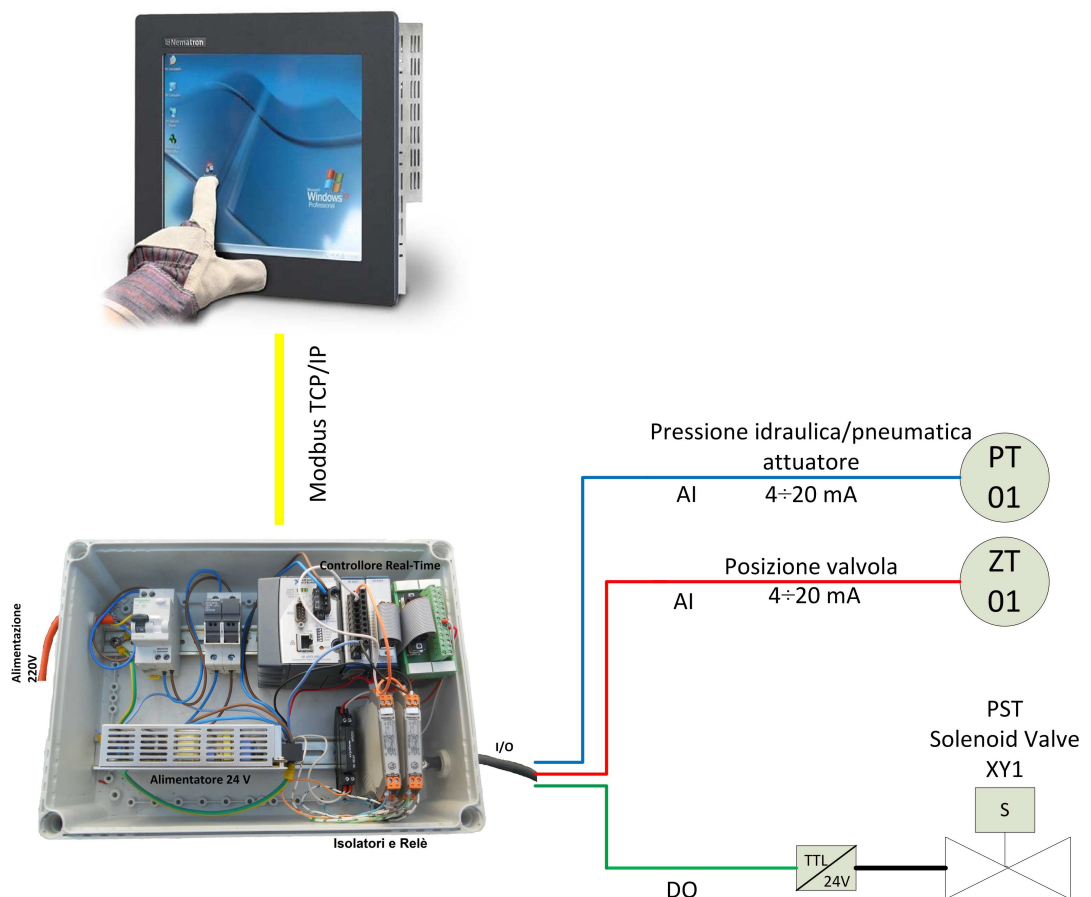


Figura 5.5: Struttura Hardware del sistema di Partial Stroke Test progettato

In figura 5.6 viene riportata la configurazione del sistema idraulico utilizzata nel progetto. La valvola solenoide in grado di eseguire il PST è quella denominata XY1 mentre le valvole XY2 e XY3 sono quelle realmente utilizzate dal SIS a se-

guito di una richiesta di chiusura dell'impianto. Tali solenoidi non possono essere utilizzate per effettuare test automatici in quanto presentano un reset manuale obbligatorio. Particolare considerato durante lo sviluppo del dispositivo è stata la configurazione di tali valvole. Infatti, nello schema si osserva che la solenoide XY1 utilizzata per effettuare il PST ha una configurazione NC (Normally Closed) e dunque la scarica di pressione del cilindro avverrà al momento di eccitazione della solenoide. Al contrario, le due valvole XY2 e XY3, usate per il Full Stroke Test, sono in configurazione NO (Normally Open) consentendo al fluido di percorrere il sistema di alimentazione solo se vengono entrambe diseccitate contemporaneamente in modo tale da entrare automaticamente in sicurezza in caso di perdita di alimentazione. La pressione operativa relativa all'attuatore utilizzato consente di lavorare tra  $130 \div 210$  bar. Nelle verifiche sperimentali verrà utilizzato il valore di 140 bar considerando però che il dispositivo funziona correttamente per tutte le pressioni operative possibili.

### 5.3 Sviluppo software dispositivo diagnostico

La realizzazione del progetto è avvenuta mediante l'utilizzo dell'ambiente di sviluppo Labview, un linguaggio di programmazione grafico sviluppato appositamente dalla National Instruments, studiato e ottimizzato per facilitare la realizzazione di applicazioni per acquisizione, analisi di segnali e controllo dati, compatibile con gran parte dell'hardware oggi disponibile per questa tipologia di applicazioni. Per il tipo di applicazione sviluppata nel progetto, si possono suddividere tre diversi moduli del programma che si differenziano tra loro per il supporto hardware a cui è destinata l'applicazione da realizzare e hanno caratteristiche differenti soprattutto per quanto riguarda le tempistiche con cui vengono eseguite le varie applicazioni e per la complessità delle librerie messe a disposizione.

#### Labview su Windows

In contrasto con i linguaggi di programmazione testuali, Lab VIEW sfrutta una programmazione grafica ad icone basata sul flusso dei dati, che permette di realizzare elaborati programmi di analisi o di controllo senza scrivere fisicamente alcuna

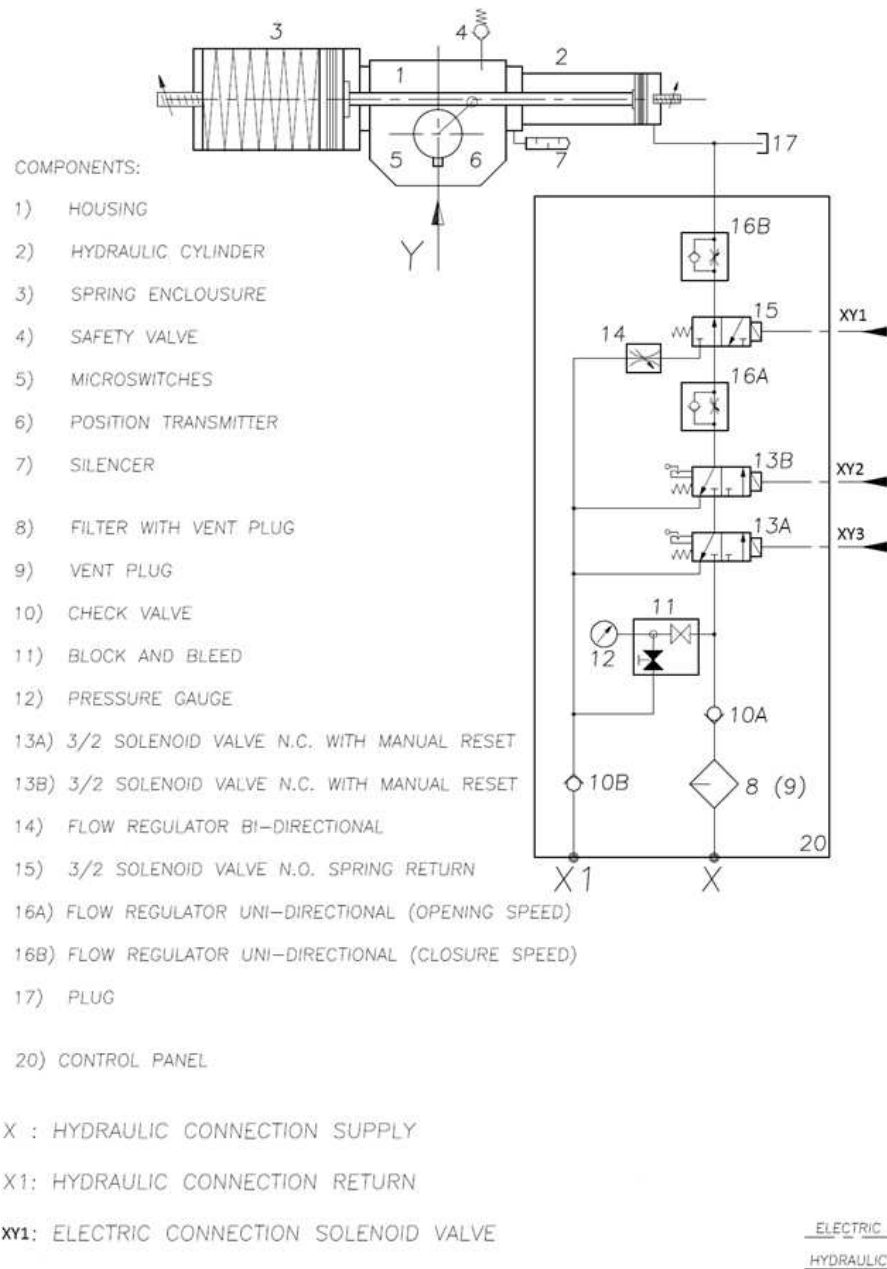


Figura 5.6: Schema del circuito idraulico utilizzato per il controllo dell'attuatore

riga di programma. Infatti i programmi realizzati con Labview, sono detti Virtual Instrument (VI) in quanto nell'aspetto fisico e nel modo di interagire riproducono strumenti reali come oscilloscopi e multimetri. L'applicazione è costituita da icone collegate tra loro da "cavi" virtuali che trasportano le informazioni che assumono una forma e un colore differente a seconda del tipo di dato trasportato. L'interfaccia utente di ogni VI è detta Front Panel in cui sono posizionati controlli e indicatori che rappresentano rispettivamente gli input e gli output interattivi. I controlli sono manopole, potenziometri, quadranti, pulsanti, interruttori, comandi scorrevoli, caselle numeriche o di testo e altri meccanismi di introduzione di dati, mentre gli indicatori sono grafici, LED, tabelle e altri componenti che consentano di visualizzare gli output acquisiti o generati dal Block Diagram. Dopo aver realizzato il pannello di controllo, è necessario implementare le funzionalità richieste dall'applicazione nello schema a blocchi, unendo ed elaborando le icone che rappresentano gli oggetti del pannello frontale. Quest'ultima parte è il corpo centrale di un VI in quanto contiene il codice grafico, sotto forma di diagramma a blocchi, che gestisce gli oggetti presenti nel pannello di controllo. Nella realizzazione del codice si possono utilizzare, oltre ai capisaldi della programmazione classica come i cicli while, for e la struttura case, gli elementi messi a disposizione dalle librerie di Labview come le strutture temporizzate che permettono di stabilire una priorità tra le varie parti del programma o funzioni già implementate, per l'acquisizione, l'analisi e l'esposizione di dati. L'enorme flessibilità di Labview risiede anche nella possibilità di stabilire una scala gerarchica e una priorità dei VI, consentendo di realizzare strutture anche molto complicate senza mai perdere di vista il quadro di insieme.

### **Labview Real Time**

L'applicazione realizzata con Labview Real Time differisce da una realizzata per Windows per il fatto che l'elaboratore RT comunica con il mondo esterno tramite un'interfaccia di rete oltre alle schede di input-output. Quindi, sfruttando questo canale di trasmissione dati, è possibile modificare tutti i parametri del sistema RT, con la necessità però di utilizzare un computer esterno, definito Host, che visualizza l'interfaccia utente, quindi aggiorna i dati in tempo reale e invia al

modulo real time le modifiche effettuate. Questo espediente consente di alleggerire il processore dal compito di visualizzare e aggiornare l'interfaccia, liberando più risorse di calcolo. In campo RT è possibile inoltre attribuire diverse priorità a ciascun VI a seconda della loro criticità temporale, cioè dell'intervallo di tempo entro i quali le applicazioni devono essere eseguite.

## FPGA

Il modulo FPGA utilizza un approccio diverso rispetto al RT, definito hard real time, in cui il programmatore è certo, a priori, che l'esecuzione del programma avvenga entro tempi prestabiliti, in quanto l'algoritmo è implementato in hardware. Il modulo FPGA mantiene la stessa facilità d'uso e intuitività dell'ambiente Labview, ma è dotato di un nuovo set di VI che consentono di realizzare applicazioni funzionanti sulla scheda utilizzata. In figura 5.7 viene riportata l'idea della FPGA che rappresenta una logica virtuale con le stesse proprietà di quella fisica. Per quanto riguarda il progetto, la componentistica relativa alla FPGA è contenuta nello chassis NI-9103.

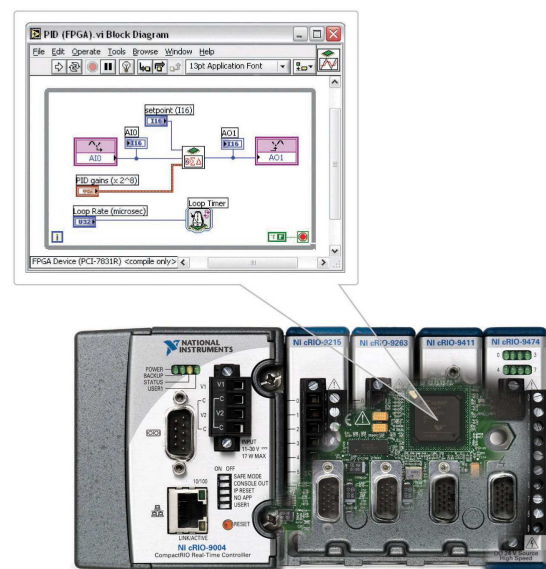


Figura 5.7: FPGA in un dispositivo cRIO

Questo dispositivo è limitato però al calcolo intero a 64 bit, quindi non è possibile implementare VI complessi. Ciò è dovuto al fatto che, per rendere il più veloce possibile l'esecuzione delle applicazioni, si è reso necessario ridurre

notevolmente la complessità dei calcoli che vengono effettuati. La realizzazione del VI per il FPGA non è molto differente da quella abituale per uno di Labview in ambiente Windows, l'unica eccezione consiste nel dover compilare tale VI nel linguaggio del FPGA e poi caricarlo nella sua memoria. Questo processo può però richiedere anche alcune ore e deve essere eseguito ogni volta che si modifichi il flusso di dati all'interno del VI. Il software del sistema di controllo gestisce la comunicazione tra i vari VI. Una parte di questa viene eseguita sull'elaboratore real time, l'altra sulla scheda del FPGA. In conclusione, è necessario definire un programma Host, che viene eseguito su un elaboratore dotato di sistema operativo e di scheda di rete, che fornisce l'interfaccia utente per la gestione del sistema RT rappresentato nel nostro caso dal controllore National Instruments cRIO, [17].

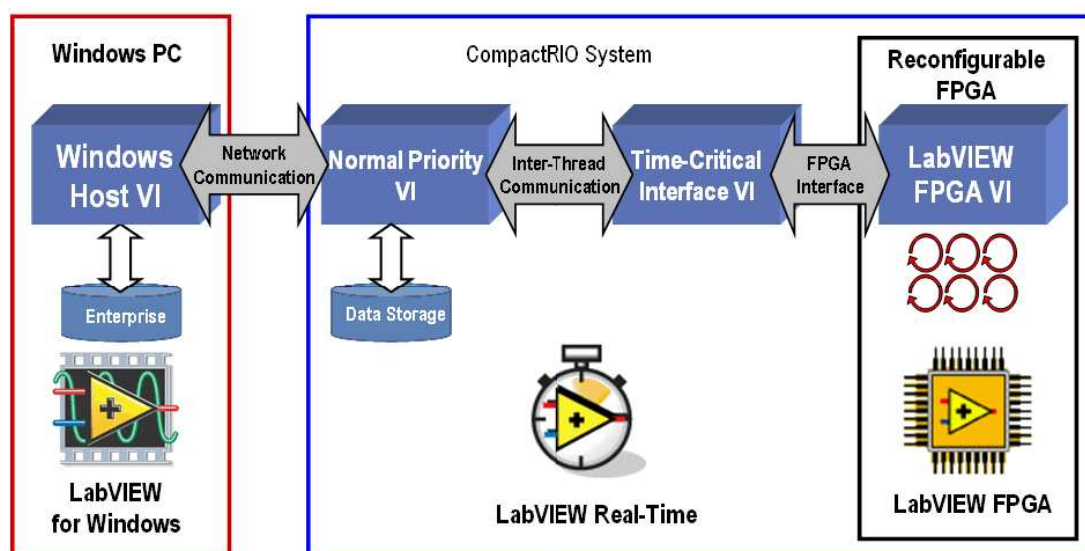


Figura 5.8: Struttura di programmazione utilizzata durante lo sviluppo dell'applicativo per il sistema diagnostico

## 5.4 HMI: Human Machine Interface

L'interfaccia tra utente e calcolatore è la sezione di programma che consente l'effettivo utilizzo del dispositivo progettato. Questa porzione di programma viene eseguita dal computer utilizzato come Host e prevede una connessione al controllore attraverso lo standard Modbus TCP/IP. La schermata principale consente di configurare e calibrare il dispositivo per renderlo operativo attraverso delle ope-



razioni prestabilite che partono dalla configurazione delle variabili necessarie per determinare le grandezze fisiche utilizzate, fino ad arrivare all'esecuzione di Partial Stroke Tests con relativa visualizzazione dei parametri utili a determinare lo stato del sistema valvola. L'HMI sviluppata è riportata in figura 5.9 ed è formata da quattro sezioni principali:

- Connessione al dispositivo Real-Time
- Visualizzazione ultimo PST eseguito
- Interazione con il dispositivo diagnostico
- Comandi di invio e risposta attraverso il canale TCP/IP e relativi errori

La prima, permette di collegarsi al fine di interagire con il dispositivo. Allo scopo deve essere inserito l'indirizzo IP del controllore cRIO e il numero di porta prevista per lo scambio dati. Una volta connesso il dispositivo viene visualizzato, se presente, l'ultimo PST eseguito sulla valvola in modo da renderne noto immediatamente il suo stato. Per quanto riguarda la sezione relativa agli errori di comunicazione presenti tra dispositivo e HMI, l'utilità è quella di riuscire ad identificare il malfunzionamento per ripristinare al meglio la connessione.

### 5.4.1 Modbus TCP/IP

Come già affermato, per la comunicazione tra PC Host e controllore Real-Time, viene utilizzato lo standard Modbus TCP/IP. Questo standard è un protocollo di comunicazione a livello applicazione basato sul principio client/server. La caratteristica che differenzia il protocollo da altri, è determinata dal frame dati detto PDU (Protocol Data Unit) che consiste solamente in due parti che sono:

- Codice Funzione: campo di 1 byte il codice del servizio richiesto tra client/server
- Dati: campo di lunghezza variabile contenente i dati necessari per finalizzare la richiesta

Per l'effettiva comunicazione sul canale di trasmissione viene inserita questa PDU nella cosiddetta Modbus TCP/IP ADU (Application Data Unit) con la struttura riportata in figura 5.10. Oltre ai campi già citati, viene aggiunto un header

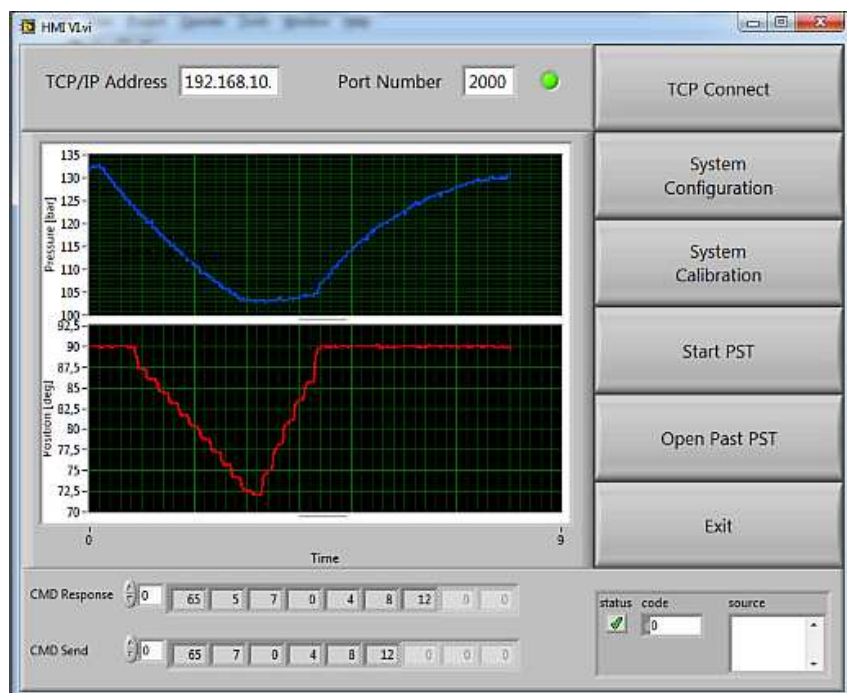


Figura 5.9: Schermata principale HMI del programma diagnostico sviluppato nel progetto di tesi

contenente le informazioni necessarie a inviare correttamente a destinazione la PDU. Dato che Modbus supporta solamente una comunicazione del tipo richiesta/risposta, l'invio di dati può solamente essere iniziato dal computer Client. Il server, identificato nel nostro caso dal controllore cRIO, non invia mai nulla senza ricevere una richiesta. Queste richieste sono determinate attraverso il campo Codice Funzione che sono per la maggior parte dei casi codici standardizzati, anche se possono essere utilizzati dei codici aperti al programmatore per implementare specifiche funzioni. Durante il progetto di tesi viene utilizzata una comunicazione Modbus principalmente utilizzando il codice 65 che ha permesso attraverso l'utilizzo di sub-code di implementare le funzionalità richieste dal dispositivo diagnostico.

#### 5.4.2 Configurazione del sistema diagnostico

Come prima operazione possibile da eseguire sul dispositivo diagnostico connesso alla HMI, vi è la configurazione del sistema. In questa sezione di programma

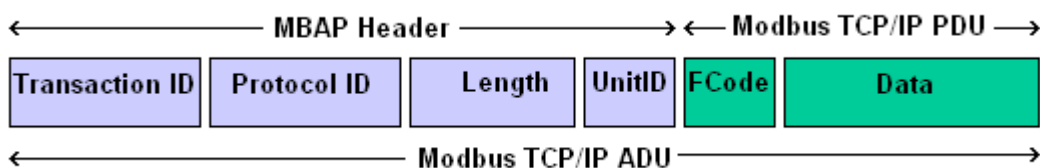
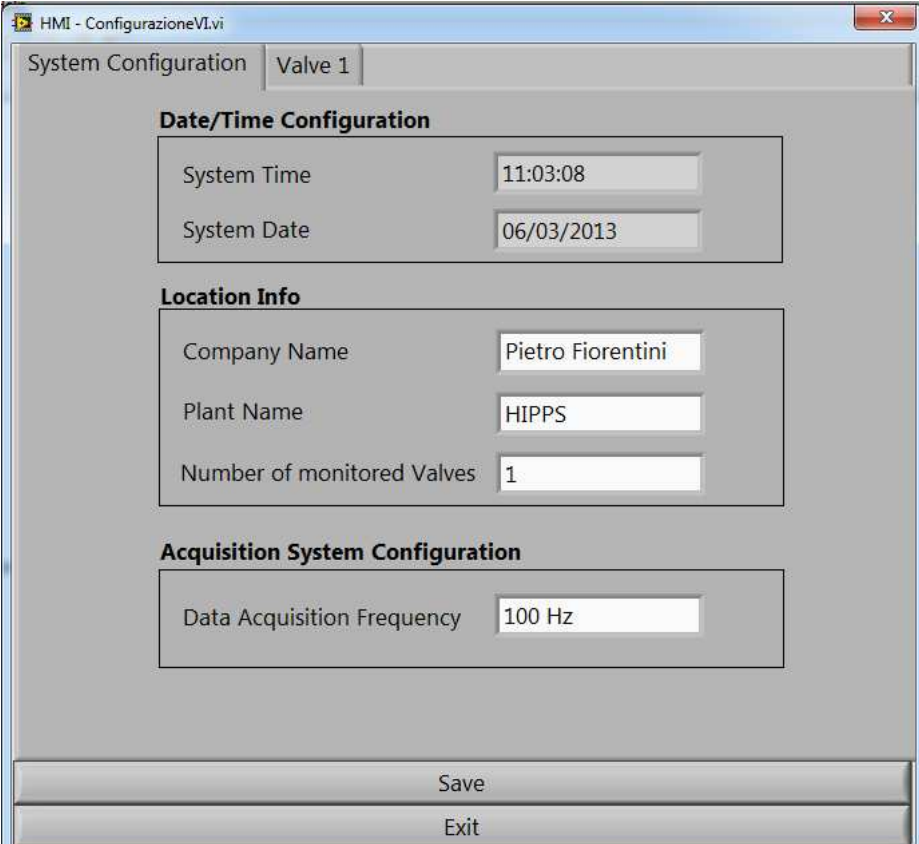


Figura 5.10: Modbus TCP/IP Application Data Unit

utente, è possibile settare tutti i parametri utili alla gestione del sistema e quelli necessari per il corretto svolgimento di un PST. Questa interfaccia, come si verifica in figura 5.11, è suddivisa in due parti principali. La prima prevede l'inserimento di dati che riguardano principalmente il dispositivo diagnostico come:

- Data/Ora: necessarie per una corretta archiviazione dei vari test eseguiti successivamente
- Posizione geografica: vengono riportate utili informazioni sulla posizione dell'impianto con relativo gestore
- Frequenza di acquisizione dati in base alle necessità dell'impianto.

La seconda sezione inserisce le informazioni relative alla valvola sottoposta al PST. Vengono infatti inseriti i dati relativi al produttore della valvola e il codice identificativo sia per il sistema nel quale viene inserita, nel nostro caso SDV100, sia il serial number che identifica univocamente la valvola tra tutte quelle prodotte. Per determinare l'escursione della valvola durante il test è possibile inserire la percentuale di chiusura voluta, in questo caso 20%, associando due variabili previste per tollerare possibili errori di offset dei trasmettitori. Infine vengono riportati i range di misura dei relativi trasmettitori di posizione e pressione allo scopo di convertire il segnale in input al controllore, da Volt alla grandezza presa in considerazione. Al termine dell'inserimento di tutti i dati è possibile, con il tasto Save, inviarli al controllore cRIO il quale provvede a creare un file testo nel quale riporta nomi e quantità inserite al fine di ottenere un sistema robusto anche nel caso di perdita di alimentazione.



HMI - ConfigurazioneVI.vi

System Configuration | Valve 1

**Date/Time Configuration**

System Time	11:03:08
System Date	06/03/2013

**Location Info**

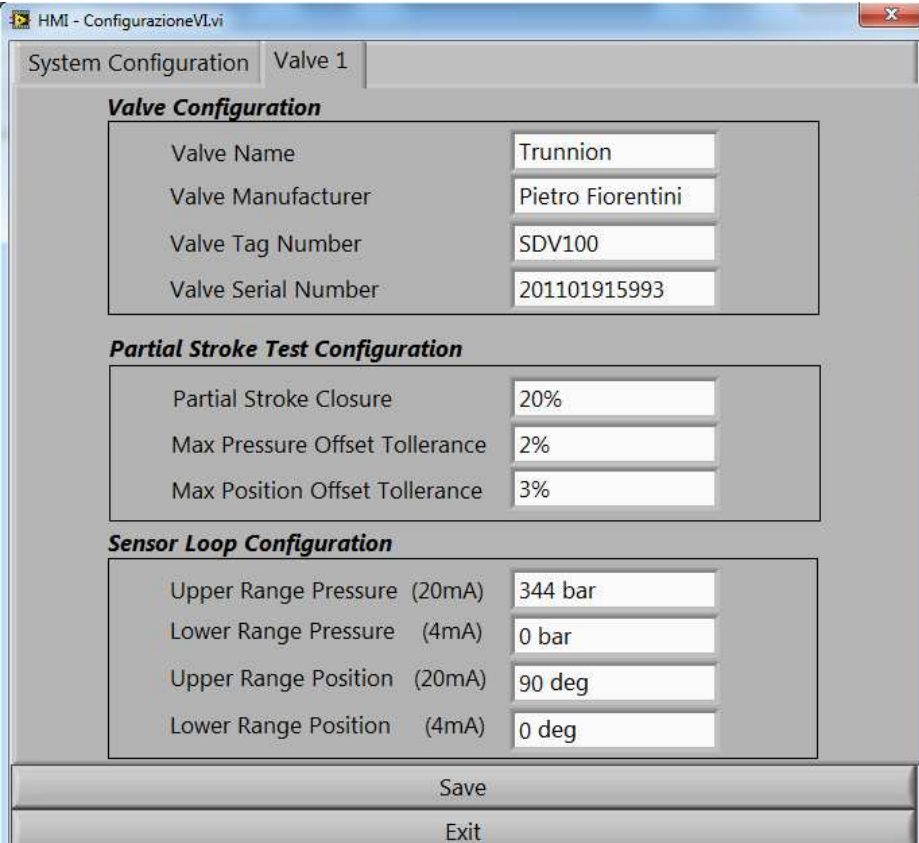
Company Name	Pietro Fiorentini
Plant Name	HIPPS
Number of monitored Valves	1

**Acquisition System Configuration**

Data Acquisition Frequency	100 Hz
----------------------------	--------

Save

Exit



HMI - ConfigurazioneVI.vi

System Configuration | Valve 1

**Valve Configuration**

Valve Name	Trunnion
Valve Manufacturer	Pietro Fiorentini
Valve Tag Number	SDV100
Valve Serial Number	201101915993

**Partial Stroke Test Configuration**

Partial Stroke Closure	20%
Max Pressure Offset Tolerance	2%
Max Position Offset Tolerance	3%

**Sensor Loop Configuration**

Upper Range Pressure (20mA)	344 bar
Lower Range Pressure (4mA)	0 bar
Upper Range Position (20mA)	90 deg
Lower Range Position (4mA)	0 deg

Save

Exit

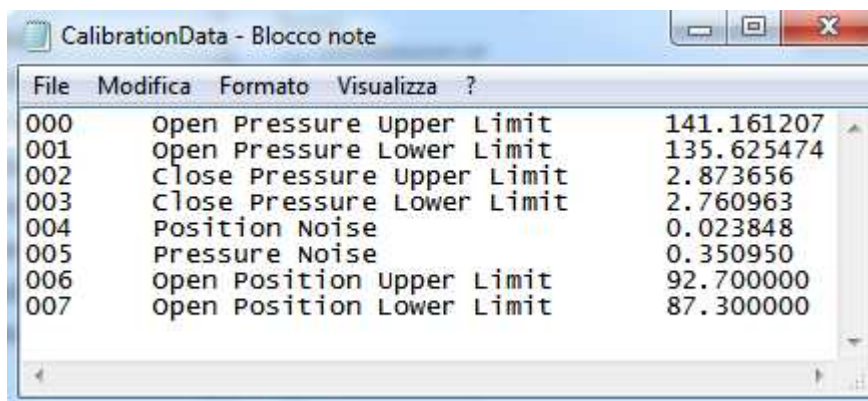
Figura 5.11: VI relativa alla configurazione del dispositivo

### 5.4.3 Calibrazione dispositivo

Durante la calibrazione automatica del dispositivo vengono determinati i parametri che caratterizzano lo stato del sistema quali:

- Rumore dei segnali di pressione e posizione
- Pressione e posizione del sistema a valvola aperta e chiusa
- Partial Stroke Test di riferimento

Si assume che la valvola sia completamente aperta, la pressione dell'attuatore sia a regime e il sistema sia in grado di operare correttamente. La prima fase della calibrazione prevede l'analisi dei segnali di pressione e posizione, verificando che la valvola sia aperta e la pressione a regime. Se le condizioni sono soddisfatte, il controllore determina il limite superiore e inferiore in cui la pressione può essere considerata quella di completa apertura. Se la variazione del segnale è troppo elevata oppure la valvola non è completamente aperta, la procedura viene interrotta avvisando l'utente finale che il sistema non è correttamente calibrato. Successivamente, la valvola viene completamente chiusa, verificando che il trasmettitore di posizione fornisca un valore prossimo a zero, contemporaneamente alla pressione dell'attuatore. In questo modo vengono determinati gli intervalli nel quale la valvola può considerarsi chiusa e l'attuatore a pressione minima. Il terzo step prevede la riapertura della valvola al fine di verificarne il corretto funzionamento sia per quanto riguarda la meccanica sia per la verifica dei range determinati precedentemente. Al termine, quando il sistema è a regime viene avviato un Partial Stroke Test di riferimento che sarà utilizzato in futuro per confrontarlo con i test eseguiti, consentendo di distinguere casi di comportamenti anomali da parte della valvola. L'esecuzione di questa fase finale è analoga a quanto avviene durante un normale PST e per questo motivo viene analizzata nella prossima sezione. Se la procedura viene terminata correttamente, viene memorizzato un file contenente le informazioni del PST di riferimento ed un file di testo contenente i parametri determinati durante la calibrazione.



ID	Parameter	Value
000	Open Pressure Upper Limit	141.161207
001	Open Pressure Lower Limit	135.625474
002	Close Pressure Upper Limit	2.873656
003	Close Pressure Lower Limit	2.760963
004	Position Noise	0.023848
005	Pressure Noise	0.350950
006	Open Position Upper Limit	92.700000
007	Open Position Lower Limit	87.300000

Figura 5.13: File di test contenente i parametri determinati in fase di calibrazione

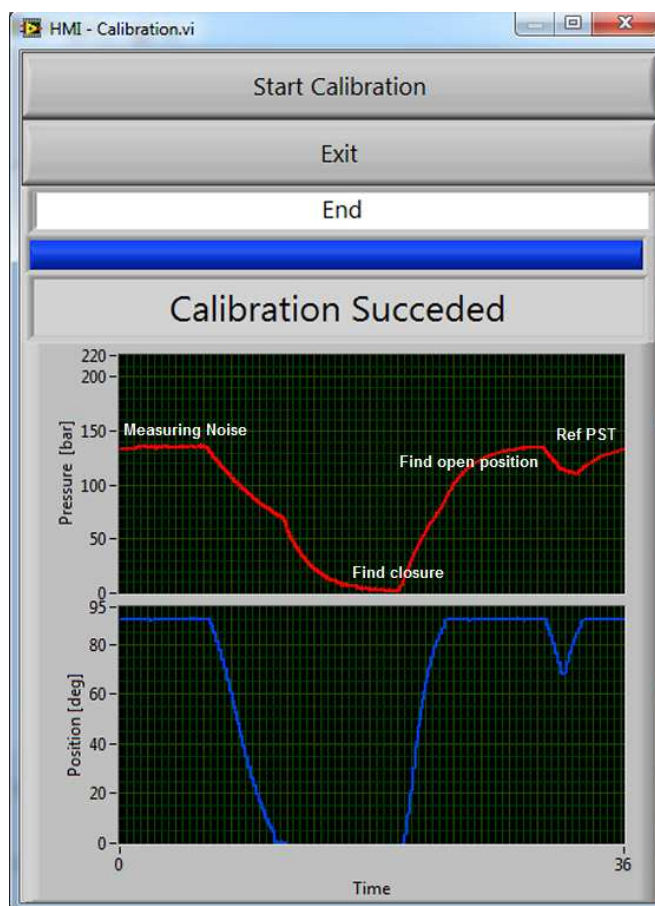


Figura 5.12: Schermata ottenuta al termine dell'esecuzione della calibrazione del dispositivo diagnostico

#### 5.4.4 Partial Stroke Test

Al termine della calibrazione automatica, il dispositivo risulta operativo ed è possibile eseguire test parziali attraverso l'apposita sezione del programma. Il test prevede una chiusura parziale della valvola durante la quale vengono analizzati i dati disponibili di pressione e posizione direttamente nel controllore Real-Time. Tale chiusura avviene comandando la valvola solenoide che prevede un azionamento del tipo on/off che consente la carica/scarica della pressione nell'attuatore idraulico. Dato che l'obiettivo è quello di verificare lo stato della valvola, non viene eseguito un controllo esclusivamente attraverso la pressione ma vi è la necessità di usufruire di tutti i possibili canali al fine di diagnosticare malfunzionamenti che si possono verificare anche durante l'esecuzione del test. Per questo motivo il controllo del movimento valvola è stato realizzato in due fasi:

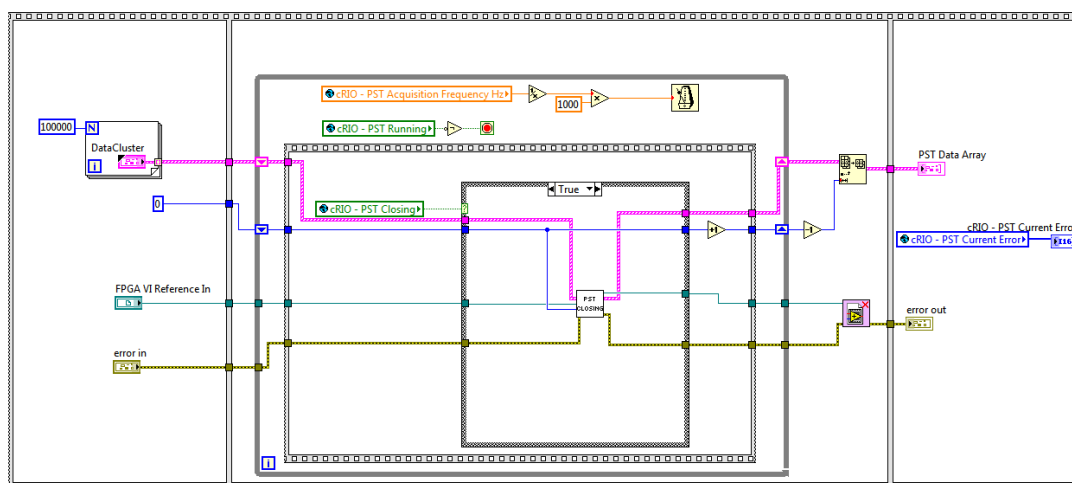
1. Eccitazione della valvola solenoide fino al raggiungimento della posizione di chiusura prestabilita in fase di configurazione
2. Diseccitazione della valvola solenoide e verifica del raggiungimento della pressione di regime nell'attuatore

In figura 5.14a è riportato il ciclo principale che controlla la valvola durante un PST. Tale ciclo è eseguito ad una frequenza pari a quella inserita durante la configurazione e le subVI PST Closing e Opening controllano la tensione fornita alla solenoide per la scarica e carica della pressione.

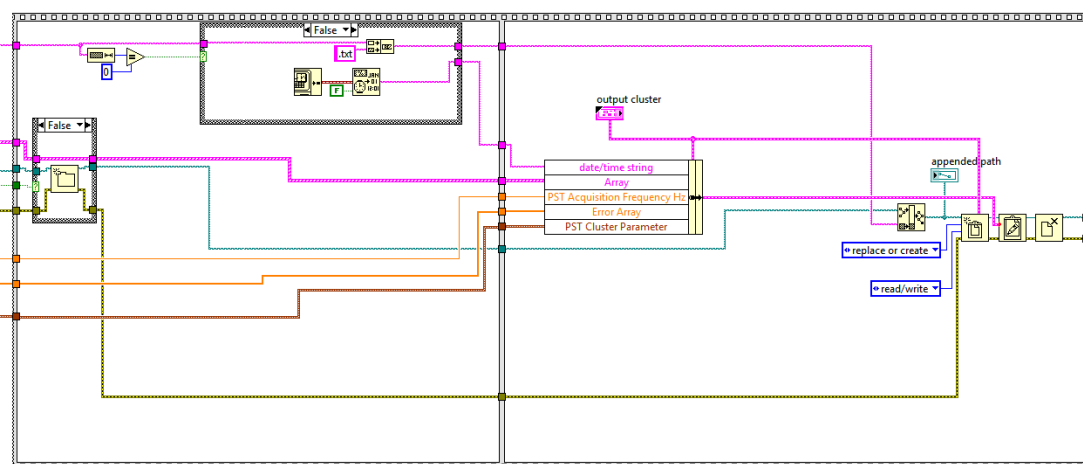
Nel momento di esecuzione del PST, il programma visualizza in tempo reale l'andamento di pressione/posizione e al termine del test fornisce immediatamente un responso positivo o negativo in base ai criteri che saranno trattati nella sezione seguente. Infine per tenere traccia dell'andamento dei vari PST nel tempo, vengono salvate tutte le informazioni necessarie per visualizzare i risultati di ogni test anche nel momento in cui viene scollegato il PC Host dal controllore industriale cRIO. In particolare vengono salvati su file:

- Data e Ora del test
- Array dati di pressione/posizione

- Frequenza di acquisizione
- Array degli errori riscontrati
- I parametri che caratterizzano l'andamento del test utilizzati per analizzare lo stato del sistema valvola



(a) Diagramma Labview per il controllo del sistema valvola-attuatore durante il PST



(b) Schema del salvataggio dei dati relativi ad un PST

Figura 5.14



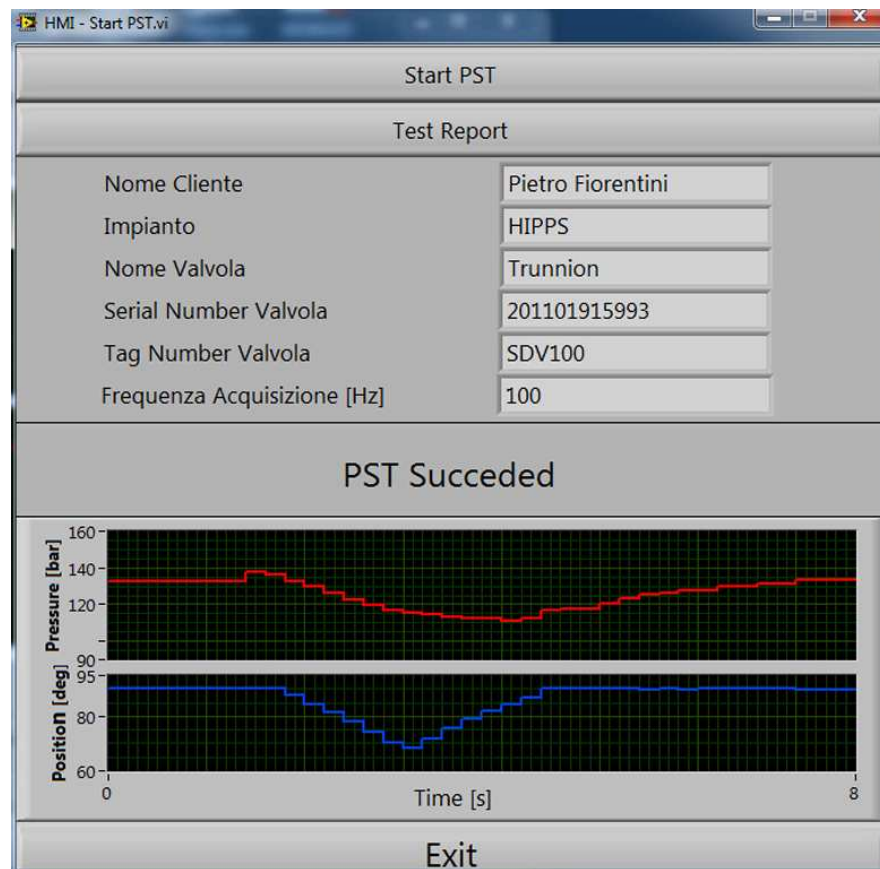


Figura 5.15: VI relativa all'esecuzione del test parziale con visualizzazione in tempo reale dell'andamento di pressione/posizione

## 5.5 Diagnosi dei guasti

L'obiettivo del progetto è quello di sviluppare un dispositivo che sia applicabile ad un range di valvole e attuatori più ampio possibile, sia per dimensione che per tipologia, rendendo necessario un approccio comparativo generale che non prevede l'utilizzo di modelli matematici, difficilmente applicabili tra sistemi diversi dato l'elevato numero di variabili necessarie alla loro modellazione. La diagnosi dei possibili malfunzionamenti del sistema, avviene attraverso lo studio del movimento parziale che solitamente non comporta disturbi al processo a valle. Allo scopo, è stata suddivisa la funzione diagnostica in due parti, una che viene svolta durante il test detta diagnosi on-line, seguita da uno studio comparativo dei valori che caratterizzano le curve di pressione e posizione, detta diagnosi off-line.

Questo permette di evitare l'incremento dell'entità dei guasti a seguito del movimento della valvola e di analizzare possibili variazioni nelle prestazioni del sistema offrendo così un'elevata copertura diagnostica.

### 5.5.1 Analisi On-Line

Data l'elevata capacità di calcolo del controllore Real-Time utilizzato, è stato possibile verificare durante l'esecuzione di un PST l'effettivo andamento delle curve di pressione e posizione. La prima verifica che viene eseguita sul sistema è quella relativa ai valori iniziali di pressione e posizione in quanto il metodo di analisi considerato è di tipo comparativo e fornirebbe valutazioni errate dello stato valvola-attuatore a seguito di escursioni troppo elevate di esse. Prima di iniziare ogni test viene verificata la pressione dell'attuatore che deve essere nel range determinato in fase di calibrazione e relativo alla posizione di completa apertura della valvola. I limiti vengono ottenuti grazie ai valori di "Max Pressure Offset Tolerance" e "Pressure Noise" come nella figura sottostante.

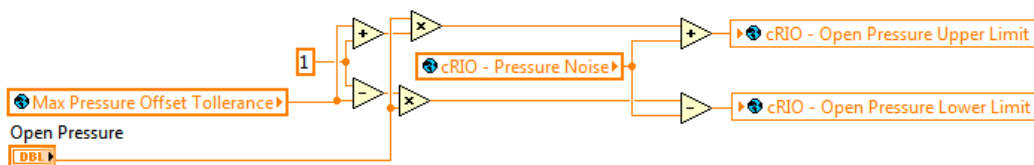


Figura 5.16: Determinazione dei limiti di pressione a valvola completamente aperta

Contemporaneamente si valuta la posizione di completa apertura della valvola con modalità analoghe a quelle utilizzate per la pressione. Se i due valori sono compatibili con quelli predeterminati in fase di calibrazione viene iniziato il test eccitando la valvola solenoide con la conseguente scarica della pressione nella camera del cilindro attuatore. Durante la chiusura della valvola, viene analizzato il tempo impiegato da essa a raggiungere la posizione di chiusura parziale prestabilita. Da parte dell'installatore del dispositivo è possibile settare un valore che identifica il massimo tempo impiegato per tale operazione in funzione delle specifiche di velocità di chiusura della valvola in caso di sovrappressioni. Se si verifica una chiusura troppo lenta si avrà un riscontro negativo per quanto riguarda

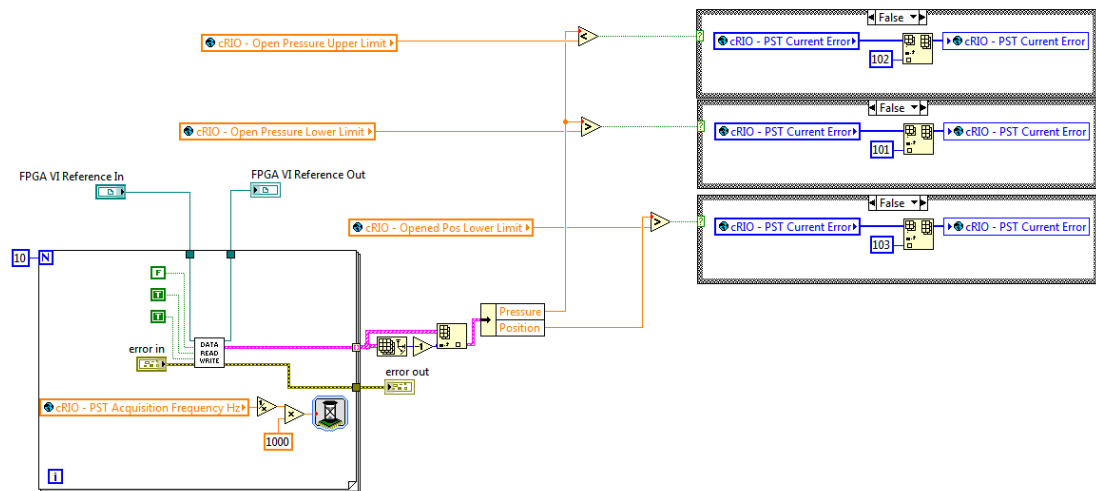


Figura 5.17: Controllo dei dati iniziali di pressione e posizione prima dell'esecuzione del PST

il risultato del test e verrà immediatamente diseccitata la valvola solenoide per non influire sull'entità del possibile danno presente. Stesse considerazioni valgono per la fase di riapertura anche se si hanno solitamente probabilità minori che ciò accada.

### 5.5.2 Analisi Off-line

Al completamento del movimento parziale viene iniziata la diagnosi off-line che necessita delle serie temporali di pressione e posizione complete. A seconda se si sono verificati o meno errori durante la diagnosi on-line, vengono eseguite operazioni differenti dato che errori di questo tipo possono determinare anche notevoli variazioni sulla risposta del sistema. Le operazioni comuni nei due casi riguardano la determinazione di punti di pressione/posizione che riescono a caratterizzare l'andamento della risposta. Questi valori vengono determinati da uno script programmato in Labview grazie alla funzione "Formula Node". Lo scopo è quello di poter confrontare automaticamente i valori con quelli di riferimento, determinati nella calibrazione, al fine di rendere semplice all'utente finale la decisione sui possibili interventi alla valvola. Questi punti caratteristici vengono individuati in:

**Start Pressure:** pressione di inizio test. Deve trovarsi tra le due soglie determi-

nate in fase di calibrazione.

**Solenoid Delay:** ritardo di attuazione della solenoide identificato del periodo che intercorre tra l'eccitazione del segnale e l'effettivo calo di pressione nell'attuatore.

**Breakaway Time:** istante nel quale si verifica il movimento dell'attuatore in fase di chiusura

**Breakaway Pressure:** pressione relativa al movimento iniziale dell'attuatore direttamente collegata alla forza elastica della molla di sicurezza.

**Maximum Closure:** massima chiusura espressa in gradi raggiunta durante il movimento parziale.

**Closing Time:** tempo in cui la valvola raggiunge la chiusura prestabilita dalla posizione di completa apertura.

**Closing Velocity:** velocità in chiusura della valvola.

**DeltaP Closing:** intervallo di pressione scaricata al fine di chiudere la valvola.

**Rise Time:** tempo di apertura della valvola.

**Actuator Fill Time:** periodo nel quale la pressione si stabilizza a seguito della completa apertura della valvola.

**Minimum Pressure Reached:** pressione minima raggiunta durante l'intero test.

**Opening Time:** tempo impiegato dal sistema per stabilizzarsi partendo dall'istante di massima chiusura.

**Opening Velocity:** velocità di apertura della valvola.

**Total Time:** tempo totale impiegato per effettuare il test.

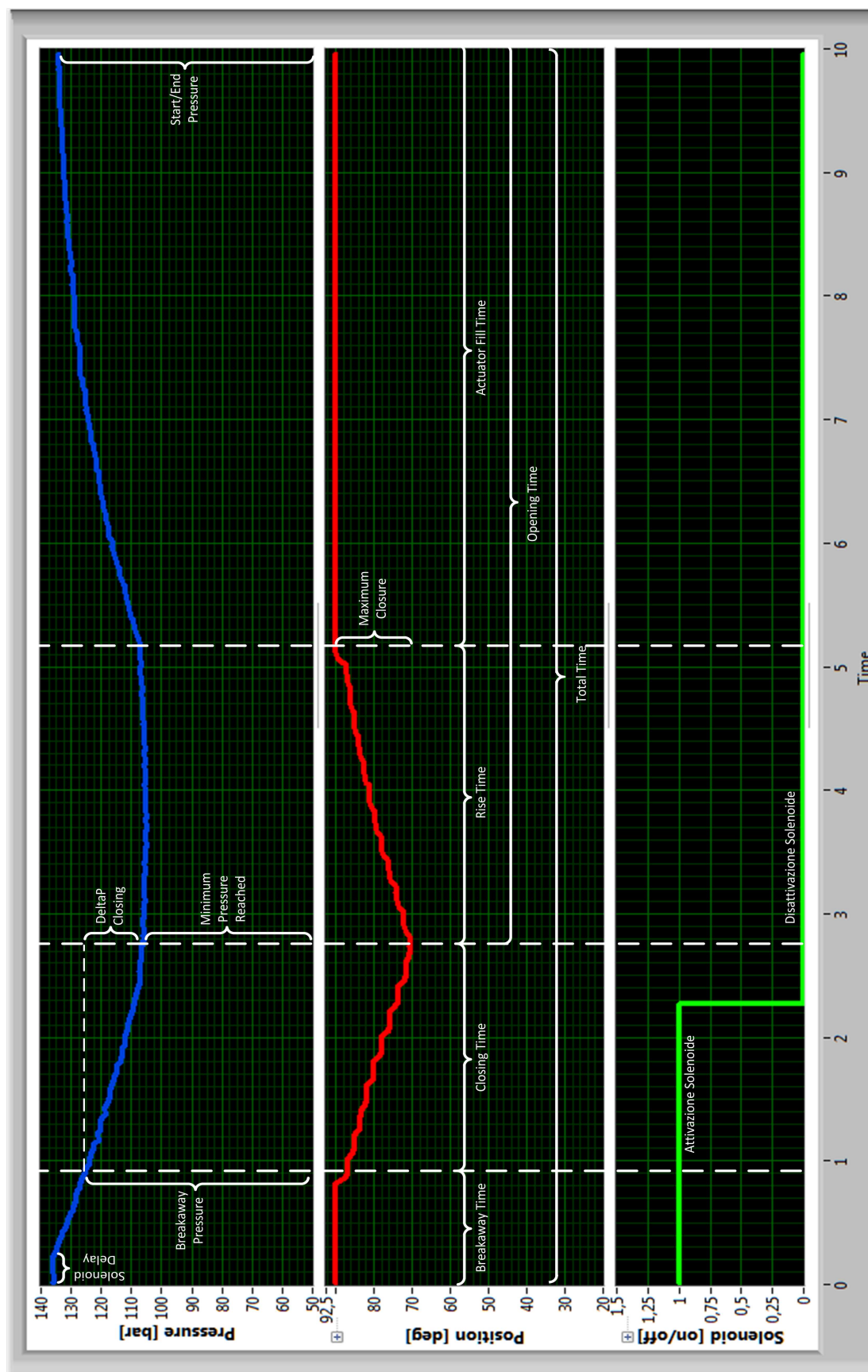


Figura 5.18: Configurazione dei punti caratteristici del Partial Stroke Test

## 5.6 Report analisi diagnostica di valvole a sfera

Quando viene terminata l'esecuzione del test si ha il responso immediato che viene visualizzato nella schermata dell'interfaccia utente come in figura 5.15. Tale schermata offre la possibilità di accedere ad una VI di report nella quale sono visualizzati i dati della diagnosi. Come si può osservare vi sono due sezioni. La prima riporta gli errori riscontrati durante il test e le possibili cause che possono determinare il comportamento ottenuto. Inoltre, viene visualizzato il PST effettuato confrontandolo graficamente con quello di riferimento per ottenere un riscontro visivo utile in casi di diagnosi comparativa portata a compimento da utenti esperti. La seconda sezione riporta tutti i valori determinati durante la diagnostica off-line e la loro deviazione percentuale rispetto ai valori di riferimento. Il LED presente in ogni punto caratteristico viene utilizzato per segnalare una deviazione maggiore di quella consentita, definita da parte dell'utente installatore. Se i valori dei parametri sono esterni a tali soglie, il PST è considerato fallito e viene allarmato l'utente di possibili malfunzionamenti al sistema. Di seguito vengono analizzati i possibili errori che si verificano durante l'analisi e le loro modalità di diagnosi.

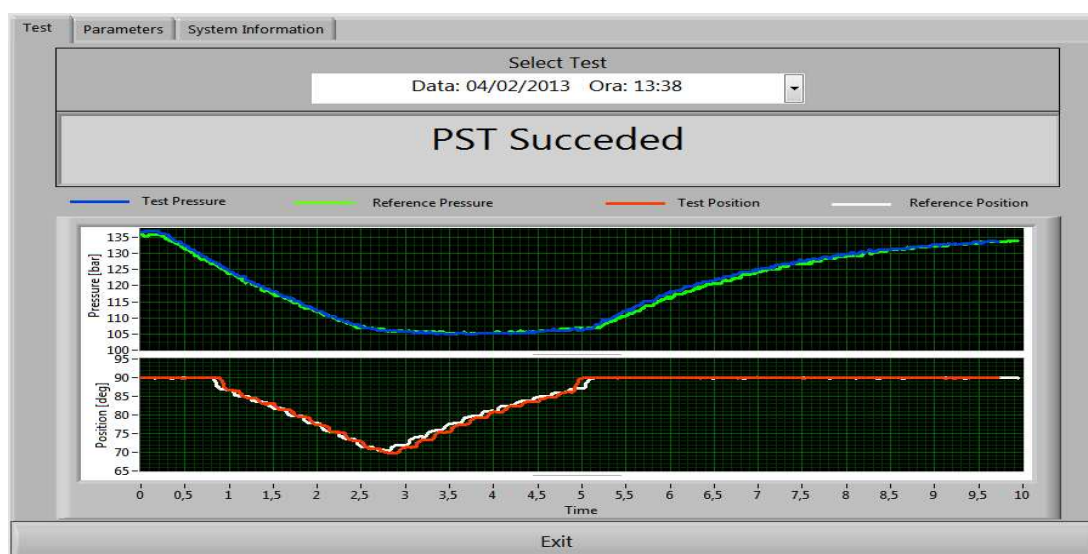


Figura 5.19: Schermata principale della VI report

	Test Parameters	Deviation From Reference
<b>Closing</b>	Start Pressure	135,36 [bar] 0,3%
	Solenoid Delay	0,34 [s] 17,24%
	Breakaway Pressure	124,19 [bar] 0%
	Maximum Closure	71,08 [deg] -0,18%
	Breakaway Time	1,02 [s] 8,51%
	Closing Time	2,33 [s] -1,27%
	Closing Velocity	8,15 [deg] 1,96%
	DeltaP Closing	20,63 [bar] 0%
<b>Opening</b>	Rise Time	2,58 [s] -5,15%
	Actuator Fill Time	4,05 [deg] 5,47%
	Minimum Pressure Reached	103,56 [bar] 0%
	Opening Time	6,63 [s] 1,07%
	Opening Velocity	7,36 [deg] 6,13%
	Total Time	9,98 [s] 1,22%

Exit

Figura 5.20: Valori dei parametri e deviazioni percentuali dal riferimento

### 5.6.1 On-line Error

Quando si verificano degli errori durante l'esecuzione del test, la risposta risultate presenta solitamente della variazioni importanti rispetto a quella di riferimento. Per questo motivo vengono determinati i punti caratteristici come nell'analisi offline sebbene siano utilizzati solamente i valori che sono robusti ad errori di questo tipo. Viene quindi disabilitata la visualizzazione di tali parametri.

#### Wrong Start Pressure: Error 101,102

Per effettuare un'analisi corretta del sistema valvola-attuatore, tutte le variabili prese in considerazione devono essere nelle condizioni di utilizzo standard cioè pressioni a regime e valvola completamente aperta. Per questo motivo, prima di iniziare il test, si verifica il valore della pressione presente nel cilindro attuatore. Se questa pressione risulta differente da quella determinata in calibrazione relativa alla pressione a regime con valvola aperta, il test viene annullato riportando l'errore di "Start Pressure too low" oppure "Start Pressure too high", rispettivamente numero 101 e 102. Cause di questo malfunzionamento possono essere: guasti al sistema di alimentazione centrale, problemi di tenuta nel cilindro attuatore oppure guasti ai trasmettitori di pressione. Per la simulazione di questa



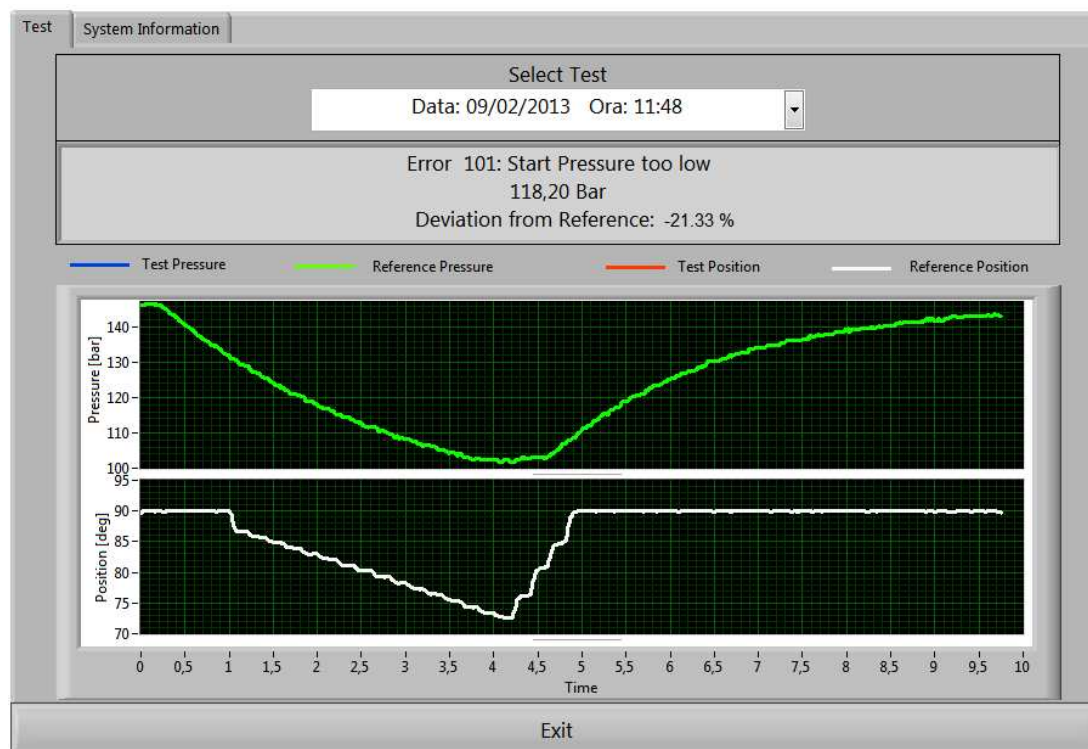


Figura 5.21: Test effettuato con pressione dell'attuatore insufficiente per garantire la riapertura della valvola

tipologia di guasti è stata variata la pressione idraulica distribuita dalla centralina lungo il circuito.

### Wrong Start Position: Error 103

Dato che il sistema diagnostico considera solamente la posizione di completa apertura per iniziare la procedura di analisi, un valore differente porterebbe un movimento minore della valvola e conseguentemente una risposta della pressione non conforme a quella di riferimento. L'intervallo utilizzato per il riscontro è determinato dal limite inferiore e superiore relativi alla posizione di valvola aperta. In questo caso, la valvola solenoide non viene eccitata e viene mostrato l'errore numero 103 nell'interfaccia utente associandolo alla posizione corrente della valvola e alla sua deviazione rispetto ai 90°. La rilevazione di questo errore potrebbe essere connessa a un problema di calibrazione del trasmettitore di posizione oppure ad una valvola effettivamente chiusa parzialmente. Dato che la posizione



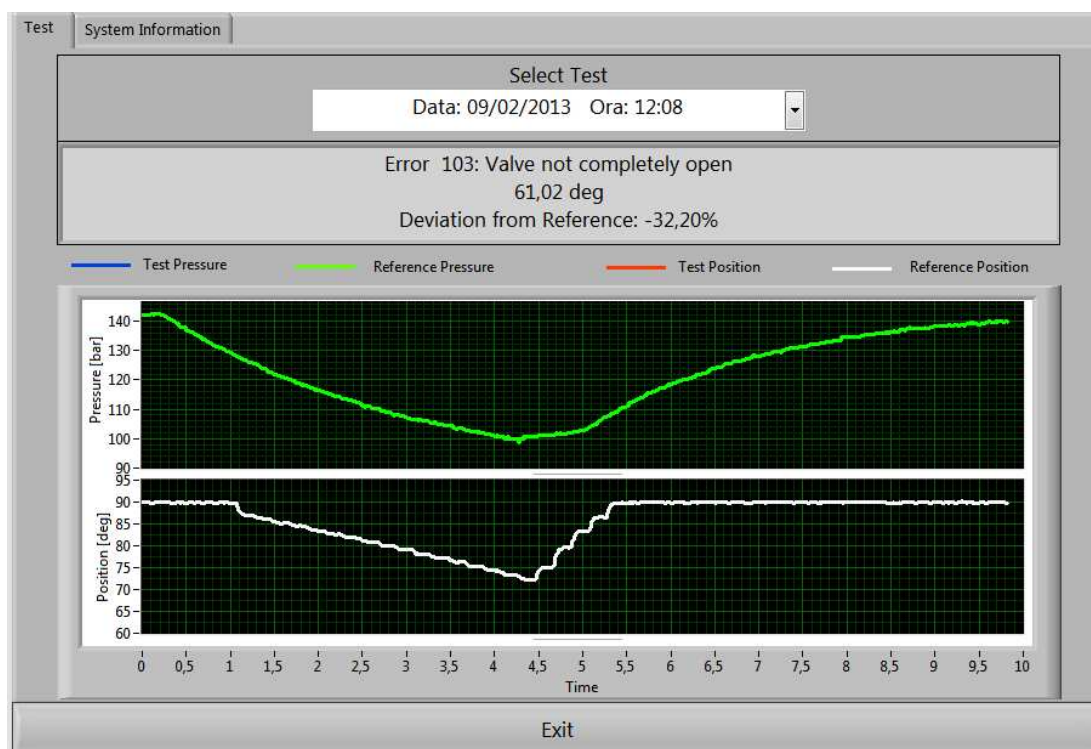


Figura 5.22: Report nel caso di valvola non completamente aperta ad inizio test

della sfera non può essere controllata, per simulare tale malfunzionamento è stato utilizzato un generatore di  $4 \div 20$  mA per fornire all'isolatore del circuito di posizione il valore voluto, bypassando così trasmettitore reale.

### Position Sensor Disconnected: Error 452

Il malfunzionamento si verifica se non si hanno variazioni di posizione durante il test. Si osserva come la variazione di pressione sia identica a quella di riferimento fino alla chiusura prestabilita dal PST e poi continua a calare con la stessa pendenza. Questo significa che non vi sono problemi riguardanti l'attuatore. Il programma di analisi verifica se la minima posizione raggiunta è all'intero della fascia che caratterizza quella di massima apertura constatando se il trasmettitore è disconnesso dall'attuatore e non fornisce l'andamento nel tempo desiderato. Analogamente al caso di posizione iniziale errata, in questo caso il generatore di  $4 \div 20$  viene mantenuto costante a 20 mA fornendo al sistema diagnostico un valore di  $90^\circ$  di apertura.

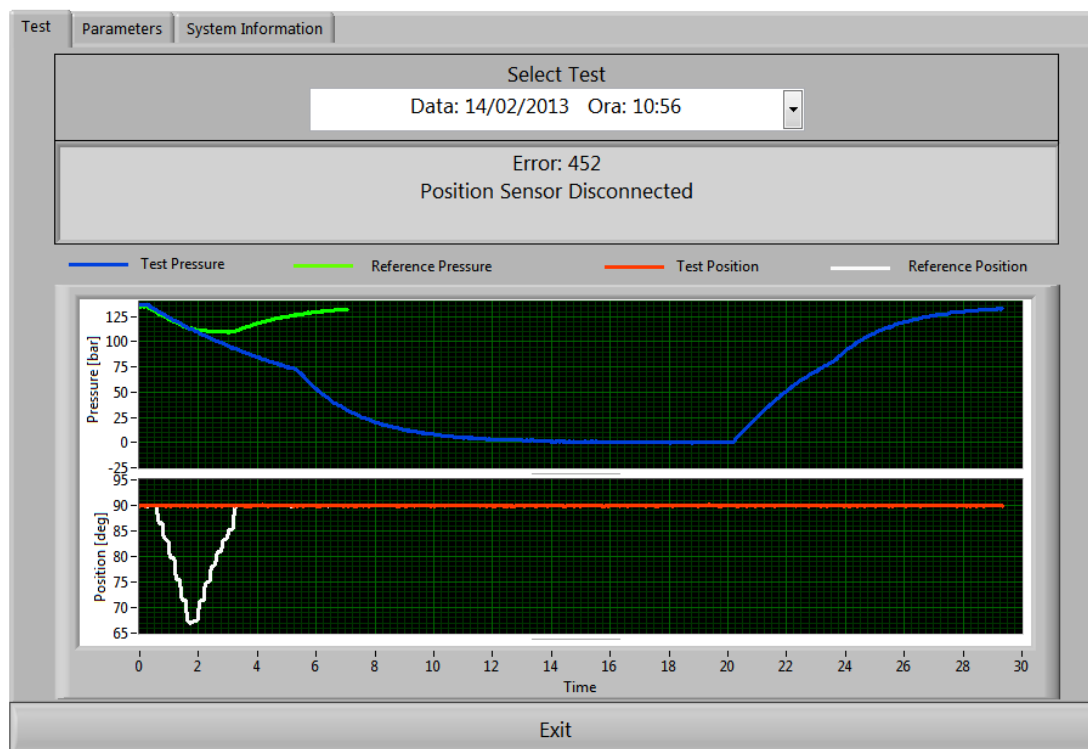


Figura 5.23: Risposta tipica nel caso di disconnessione del sensore di posizione

### Valve Stuck on Closing: Error 453

Se la valvola non è in grado di chiudersi durante l'esecuzione del test, il sistema verifica il guasto utilizzando un time-out in chiusura. Analizzando poi l'andamento della pressione del sistema è possibile determinare se la valvola è bloccata oppure se il guasto riguarda altre parti della valvola-attuatore. Si osserva infatti che in questo caso si ha un andamento diverso della pressione rispetto al riferimento anche nella prima fase, quando la valvola non si è ancora mossa. Tutti i malfunzionamenti che determinano il non raggiungimento della posizione prestabilita da parte della valvola, sono segnalati da questo errore. Questo guasto è da prendere seriamente in considerazione dato che preclude la funzione di sicurezza svolta dal sistema HIPPS e deve essere tempestivamente verificato da parte del gestore d'impianto. Tali problemi possono sorgere a causa dei fluidi che vengono gestiti dagli impianti chimici, che solitamente contengono detriti in grado di danneggiare o strozzare le valvole di sicurezza. Tali detriti possono cristallizzarsi sulla superficie o sedimentarsi nei pressi del corpo valvola creando così un aumento del-

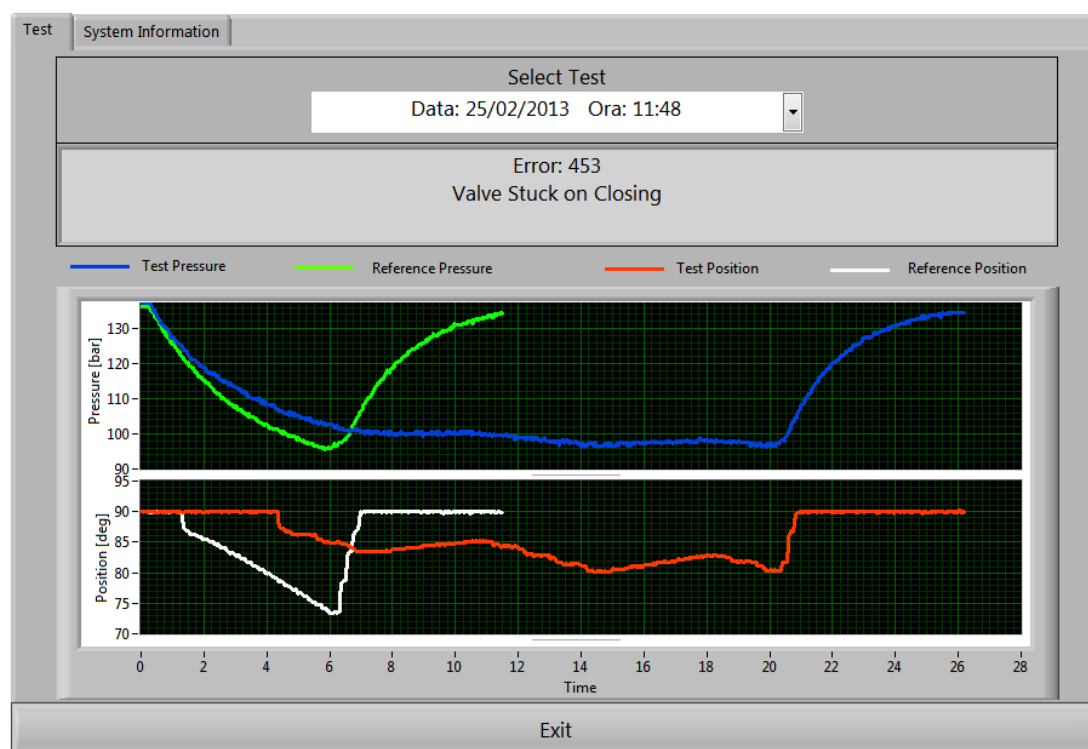


Figura 5.24: Risultato sperimentale della simulazione di valvola bloccata

la forza di attrito presente nei componenti meccanici fino al blocco della valvola. Data la notevole coppia sviluppata da parte dell'attuatore per eseguire la funzione di sicurezza di chiusura, per motivi di sicurezza non è stato possibile bloccare meccanicamente il corpo valvola. Per la simulazione del guasto è stata pulsata la solenoide simulando un movimento a scatti del sistema valvola attuatore.

### 5.6.2 Off-line Error

Nel caso in cui l'andamento del PST non presenti errori durante la sua esecuzione, il sistema analizza i punti caratteristici determinati dalla diagnosi off-line. Dato che è stata considerata una metodologia di rilevazione guasti di tipo comparativo, vengono verificate le deviazioni percentuali dei parametri caratteristici rispetto a quelli di riferimento in modo da segnalare automaticamente all'utente finale delle anomalie sul comportamento della valvola. L'utilità di questo tipo di analisi è quella di prevenire possibili futuri guasti dati principalmente dall'usura meccanica del sistema di isolamento del fluido. Inoltre, il dispositivo è in grado di analizzare

i dati e fornire una possibile causa dell'alterazione presente.

### **Degradazione del sistema**

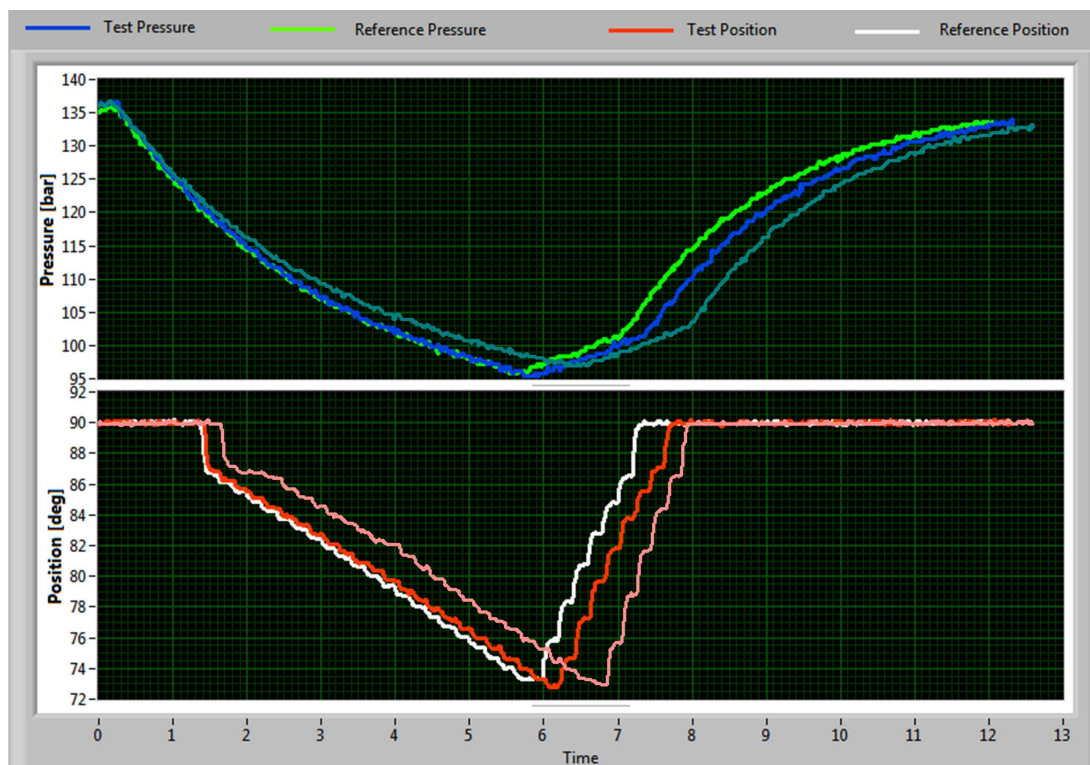
La possibile degradazione dei componenti meccanici nel tempo è segnalata unicamente nel momento in cui un parametro risulta esterno alla soglia basata sull'andamento di riferimento. Dato che i risultati che si ottengono dipendono dall'entità dell'usura e dal componente che viene preso in considerazione, durante la progettazione del dispositivo si è scelto di notificare all'utente lo stato di ogni singolo parametro in modo da poter analizzare i risultati anche da parte di un utente esperto. La degradazione considerata nel progetto è relativa ai componenti tra sfera e corpo valvola che nel tempo possono portare ad un aumento di attrito dato dalla loro usura o deformazione. Il malfunzionamento è stato simulato variando i tempi di chiusura dell'attuatore tramite dei regolatori presenti nel circuito idraulico in grado di rallentare la scarica di pressione ottenendo un comportamento simile a quello dell'aumento di attrito tra componenti. Come si può osservare in figura 5.25b, il sistema segnala i parametri fuori soglia con la relativa intensità. In questo caso gli effetti generati sulla valvola portano ad un rallentamento del tempo di chiusura e ad un istante di distacco tra sfera e corpo maggiore dato dall'aumento di forza di attrito statico. Gli errori forniti dal controllore diagnostico vengono riportati in tabella 5.1.

### **Worn Out Spring: Error 450**

La molla presente nell'attuatore è utilizzata per rendere il sistema fail-safe cioè per garantire la messa in sicurezza del sistema anche dopo la perdita di controllo dell'impianto. Tale molla deve garantire la chiusura della valvola e la classe di tenuta per cui è stato progettato il sistema di sicurezza. La degradazione della molla negli attuatori può dunque causare dei fallimenti critici del sistema. In attuatori che utilizzano più molle il guasto può non causare l'immediata rottura dell'attuatore ma viene a crearsi una notevole riduzione della spinta per il funzionamento fail-safe che può limitare le operazioni della valvola o decrementare la tenuta di fluido in caso di chiusura. Inoltre, un guasto alla singola molla può indicare che le restanti siano vicine alla rottura. Solitamente il deterioramento è dovuto a vari

Error	Description
401	Breakaway Pressure too low
402	Breakaway Pressure too high
403	Maximum Closure too low
404	Maximum Closure too high
405	Breakaway Time too low
406	Breakaway Time too high
407	Closing Time too low
408	Closing Time too high
409	Closing Velocity too low
410	Closing Velocity too high
411	DeltaP Closing too low
412	DeltaP Closing too high
413	Rise Time too low
414	Rise Time too high
415	Actuator Fill Time too low
416	Actuator Fill Time too high
417	Minimum Pressure Reached too low
418	Minimum Pressure Reached too high
419	Opening Time too low
420	Opening Time too high
421	Total Time too low
422	Total Time too high
423	Opening Velocity too low
424	Opening Velocity too high
425	Solenoid Delay too low
426	Solenoid Delay too high
450	Worn-out Actuator Spring

Tabella 5.1: Errori determinati attraverso l'analisi off-line del dispositivo diagnostico



(a) Comportamento della valvola a seguito di una variazione del regolatore della pressione di scarico dell'attua

		Test Parameters	Deviation From Reference	
<b>Closing</b>	Start Pressure	136,67 [bar]	0,33%	<input type="radio"/>
	Solenoid Delay	0,5 [s]	-1,96%	<input type="radio"/>
	Breakaway Pressure	116,44 [bar]	-8,14%	<input type="radio"/>
	Maximum Closure	73,75 [deg]	2,92%	<input type="radio"/>
	Breakaway Time	1,96 [s]	125,29%	<input checked="" type="radio"/>
	Closing Time	7,8 [s]	160%	<input checked="" type="radio"/>
	Closing Velocity	2,09 [deg]	-65,47%	<input checked="" type="radio"/>
	DeltaP Closing	24,06 [bar]	-6,65%	<input type="radio"/>
<b>Opening</b>	Rise Time	1,42 [s]	11,81%	<input type="radio"/>
	Actuator Fill Time	4,36 [deg]	-13,32%	<input type="radio"/>
	Minimum Pressure Reached	92,39 [bar]	-8,52%	<input type="radio"/>
	Opening Time	5,78 [s]	-8,25%	<input type="radio"/>
	Opening Velocity	11,49 [deg]	-19,71%	<input type="radio"/>
	Total Time	15,54 [s]	52,8%	<input checked="" type="radio"/>

Exit

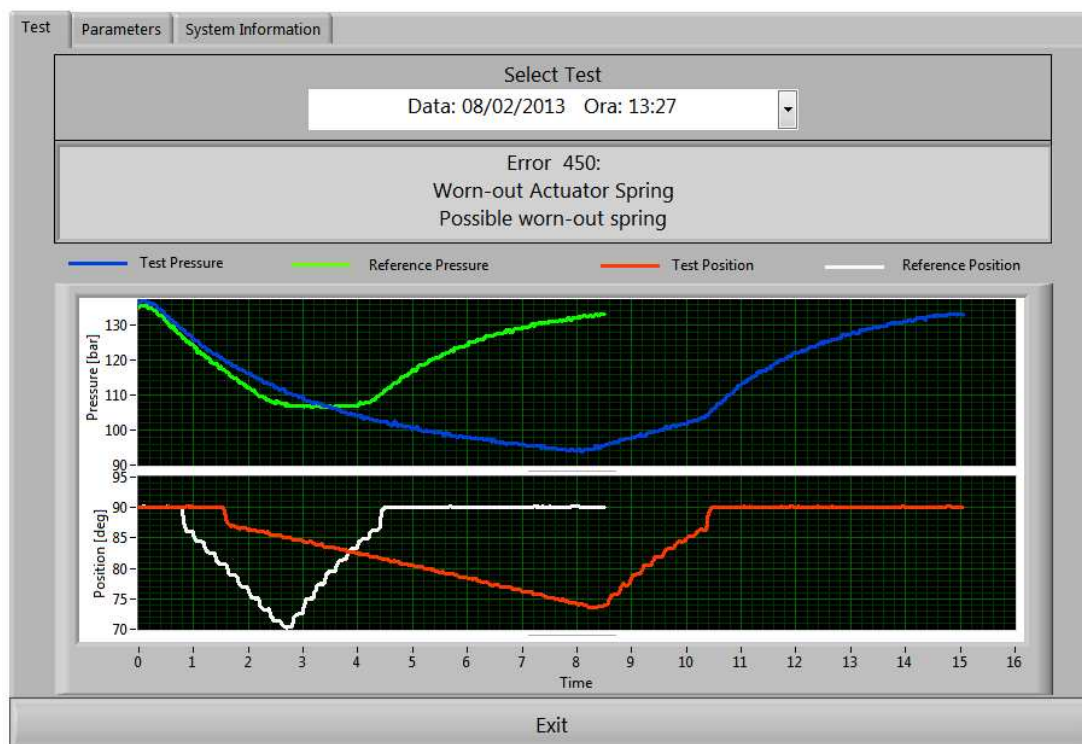
(b) Errori forniti durante la simulazione di usura dei componenti meccanici

Figura 5.25

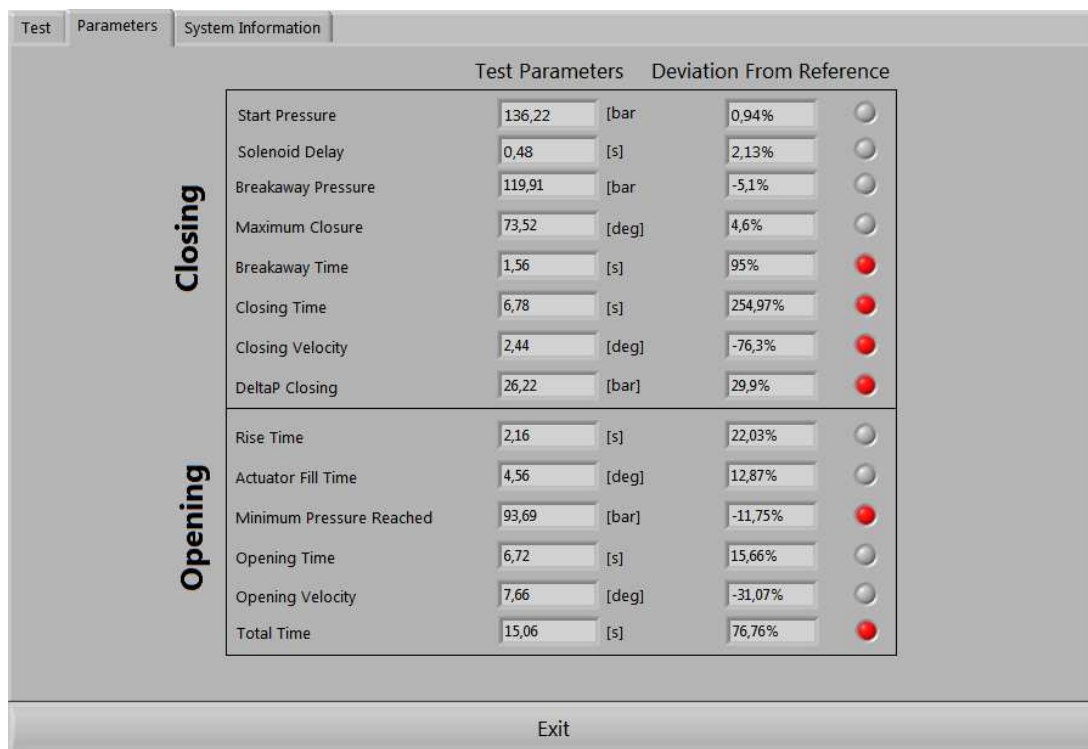
fattori quali erosione, ossidazione e collassi strutturali dovuti a fatica meccanica. Un possibile comportamento del sistema è riportato in figura 5.26a, utilizzando il sensore di posizione si osserva che lo spostamento dell'attuatore raggiunge la posizione prestabilita impiegando un tempo molto maggiore rispetto a quello nominale e la pressione raggiunge livelli inferiori a quelli in condizioni di assenza guasti. Parametro rilevante è il tempo di distacco della valvola che fornisce un'indicazione di quanto velocemente la molla riesce a scaricare la pressione all'interno dell'attuatore. In questo caso si ottiene un tempo di "breakaway" molto maggiore del normale. Quindi la diagnosi del problema da parte del dispositivo è eseguita mediante la verifica delle condizioni che più rispecchiano quelle di usura della molla che sono:

- Error 406: Breakaway Time too high
- Error 408: Closing Time too high
- Error 409: Closing Velocity too low
- Error 417: Minimum Pressure Reached too low





(a) Risposta del sistema soggetto ad un'elevata usura della molla fail-safe



(b) Parametri di risposta durante la simulazione di un sistema con molla usurata

Figura 5.26



# Conclusioni e sviluppi futuri

Nel presente lavoro di tesi è stato sviluppato un dispositivo diagnostico applicabile a valvole di processo utilizzate per l'isolamento dell'impianto a valle, inserite all'interno dei sistemi HIPPS in configurazione fail-safe. Dato che tali valvole esplicano unicamente la funzione di sicurezza, sono solitamente mantenute in posizione di completa apertura per tutta la loro vita operativa e vengono chiuse solamente su richiesta in seguito alla perdita di controllo dell'impianto. Allo scopo di determinare la probabilità di fallimento su richiesta di tali componenti è stato necessario attuare un'analisi FMEDA in grado di analizzare i principali modi di guasto e i benefici introdotti mediante l'utilizzo della procedura di PST. I risultati ottenuti forniscono una copertura diagnostica del dispositivo di PST pari al 60.64% consentendo di estendere il periodo di "proof test" dell'impianto da uno a due anni mantenendo il livello di SIL 3 prestabilito. Il progetto è stato sviluppato attraverso l'ambiente di programmazione Labview che ha consentito la progettazione di un'interfaccia lato Client, collegata attraverso Modbus TCP/IP al controllore Real-Time. Le prove sperimentali eseguite durante il progetto, garantiscono la diagnosi di malfunzionamenti sia in fase di test, con un controllo on-line, sia a test concluso attraverso l'analisi dei possibili problemi di usura cui sono soggetti questi sistemi. Data la difficoltà di diagnosi di tutte le tipologie di guasto presenti in questi dispositivi, viene fornita la possibilità ad un utente di verificare l'andamento dei test eseguiti nel tempo al fine di aumentare la capacità diagnostica. Data l'elevata potenza di calcolo del controllore Real-Time utilizzato e la possibilità di gestire contemporaneamente svariati I/O si prevede come sviluppo futuro la gestione simultanea fino ad un massimo di quattro valvole. Il sistema utilizzato per le prove sperimentali prevedeva come elementi finali valvole a

sfera rotative. Per aumentare la generalità d'impiego del dispositivo sarà necessario considerare l'introduzione della gestione anche di valvole lineari come possono essere quelle a saracinesca. Infine, per incrementare la copertura diagnostica del dispositivo a tutti i possibili guasti che possono verificarsi in sistemi composti da valvola e attuatore, dovranno essere progettati specifici test con fault insertion al fine di studiare i relativi comportamenti sviluppando nuove procedure per la diagnosi.





# Appendice A

## Specifiche tecniche controllore

---

### Specifiche cRIO-9004

#### Network

Network Interface	Modbus Ethernet
	RS 485 Modbus

#### Processor

MPC 5200 400 MHz real-time processor
--------------------------------------

#### Memory

Nonvolatile	512 MB
DRAM	64 MB

#### Power Requirements

Power Supply	18 VDC to 24 VDC
Power consumption controller only	7 W max

#### Environmental

Operating Temperature	-40°C to 70°C
Operating Humidity	10 to 90 % RH, noncondensing

#### Shock and Vibration

Operating Vibration, Random	5 g <sub>rms</sub> , 10 to 500 Hz
Operating Shock	30 g, 11 ms half sine
	50 g, 3 ms half sine
	18 shocks at 6 orientations



# Bibliografia

- [1] EinarMunkeby, “Effect of safe failures on the reliability of safety instrumented systems,” Master’s thesis, Department of Production and Quality Engineering, Norwegian University of Science and Technology, 2008.
- [2] *IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.*, International Electrotechnical Commission, Geneva Std.
- [3] *IEC 61511. Functional Safety - Safety Instrumented Systems for the Process Industry.*, International Electrotechnical Commission, Geneva Std.
- [4] M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods and Applications.* John Wiley & Sons, 2003.
- [5] P. Skousen, *Valve Handbook*, 3rd ed. McGraw Hill Professional, 2011.
- [6] B. G. Lipták, Ed., *Process Control and Optimization.* ISA - The Instrumentation, Systems, and Automation Society, 2006, vol. Second.
- [7] B. Nesbitt, *Handbook of Valves and Actuators.* Butterworth-Heinemann, 2011.
- [8] P. Beater, *Pneumatic Drives: System Design, Modelling and Control.* Springer, 2007.
- [9] C. Curran, “High integrity pressure protection systems (hipps) development for the gulf of mexico on deepstar, api 170 and industry developments,” in *OTC 19703*, 2008.

- 
- [10] W. L. Mostia, "Testing of sis valves," *www.exida.com*.
- [11] H. A. Haapanen Pentti, "Failure mode and effect analysis of software-based automation systems," *STUK-YTO-TR 190*, 2002.
- [12] H. C. William M. Goble, *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*. ISA - The Instrumentation, Systems, and Automation Society, 2005.
- [13] *OREDA: Offshore REliability DAta handbook*. OREDA Participants, 2002.
- [14] *Electrical and Mechanical Component Reliability Handbook*. EXIDA, 2008.
- [15] *IEC 60534-4, Industrial process Control Valves, Part 4: Inspection and Routine Testing*, International Electrotechnical Commission Std., 1999.
- [16] C. Tarantola, "Pfd assessment report n.278j06001/a," Tüv Nord Italia S.R.L., Tech. Rep., 2007.
- [17] M. Cangini, "Definizione delle strategie di attuazione per iniezione e accensione in un sistema di rapid control prototyping realizzato su piattaforma national instruments," Master's thesis, Università di Bologna, A.A. 2012/2013.



## Ringraziamenti

Ringrazio innanzitutto i miei genitori per il sostegno morale e materiale in questi anni di studio. Un grazie a Veronica per avermi sempre sostenuto nei momenti difficili. A tutti gli amici che hanno reso questi anni di studio piacevoli grazie alla loro compagnia. Ringrazio, in particolare, Stefano Bernardi per la sua disponibilità durante tutto il lavoro di tesi e a Alberto De Marco per la pazienza dimostratami. Un grazie al Professor Alessandro Beghi per aver reso possibile questa esperienza.