



POLITECNICO DI BARI

Dipartimento di Ingegneria Elettrica e dell'Informazione- DEI
CORSO DI LAUREA MAGISTRALE IN INGEGNERIA
DELL'AUTOMAZIONE

**TESI DI LAUREA IN
ROBOTICS**

ARCHITETTURE DI FUNCTIONAL SAFETY PER MANIPOLATORI COLLABORATIVI: STRATEGIE DI CONTROLLO E DIAGNOSI DEI FAULT

Relatore:

Prof. Paolo Lino

Correlatori:

Ing. Pietro De Carlo

Ing. Michele Tomaselli

Ing. Adriano Sciusco

Laureando:

Fabio Ceglie

Anno accademico 2024-2025



Politecnico
di Bari

**LIBERATORIA ALLA CONSULTAZIONE DELLA TESI DI LAUREA DI CUI
ALL'ART.4 DEL REGOLAMENTO DI ATENEO PER LA CONSULTAZIONE
DELLE TESI DI LAUREA (D.R. n. 479 del 14/11/2016).**

Il sottoscritto FABIO CEGLIE, matricola 586799, Corso di Laurea INGEGNERIA DELL'AUTOMAZIONE – CYBER PHYSICAL SYSTEMS, autore della presente tesi di Laurea dal titolo ARCHITETTURE DI FUNCTIONAL SAFETY PER MANIPOLATORI COLLABORATIVI: STRATEGIE DI CONTROLLO E DIAGNOSI DEI FAULT
Abstract: Lavoro di ricerca sulla sicurezza funzionale in ambito robotico industriale, incentrato sulle collaborazioni uomo-macchina, analisi dei rischi, sviluppo di sistemi di controllo per l'individuazione dei malfunzionamenti e sistemi di intervento per garantire la sicurezza funzionale.

Autorizza

Non Autorizza

La consultazione della presente tesi, fatto divieto a chiunque di riprodurre

Altamura, 14/06/2025

Firma

Fabio Ceglie

Il sottoscritto,

Cognome: CEGLIE

Nome: FABIO

Matricola: 586799

Data Seduta Laurea: 25/06/2025

dichiara

*che la tesi cartacea consegnata in data odierna è conforme a quella caricata su esse3, quindi,
approvata dal Relatore Prof. PAOLO LINO*

Bari, ____ / ____ / ____

Firma

Fabio Ceglie

Indice

Prologo	6
Capitolo I – Obiettivi	8
Capitolo II - Introduzione	11
Human Robot Interaction.....	11
Functional Safety.....	14
ISO 13849.....	18
ISO 26262.....	20
ISO 10218.....	21
ISO/TS 15066.....	24
Modalità operative	27
Confronto e differenze tra i vari standard	38
Sensor Faults	42
Actuator Faults.....	51
Capitolo III – Caso di studio	52
Descrizione del caso di studio	52
Cinematica del manipolatore	55
Dinamica del manipolatore	57
Controllo del manipolatore	59
Capitolo IV – Implementazione	65
Approccio all’implementazione.....	65
Architettura multilivello	66
Cinematica inversa tramite metodo della pseudo-inversa.....	69
Implementazione dei modelli di simulazione	73
Implementazione dell’architettura a livelli	78
Implementazione del controllo PID	79
Implementazione del metodo della pseudo-inversa	81
Test del metodo della pseudo-inversa su un manipolatore planare a tre bracci.....	82
Capitolo V – Test e performance	87

Parametri di simulazione	87
Risultati simulazioni	93
Capitolo VI – Conclusioni	127
Riferimenti.....	129
Glossario figure.....	132

Prologo

Negli ultimi decenni, il settore industriale e automotive ha assistito a una crescente integrazione di sistemi robotici avanzati, guidata dalla necessità di incrementare l'efficienza produttiva, la precisione operativa e la flessibilità nei processi. Tuttavia, l'aumento della complessità dei sistemi robotici e la loro stretta interazione con operatori umani hanno sollevato nuove sfide in termini di sicurezza funzionale (*Functional Safety*). La sicurezza funzionale, infatti, è diventata un requisito imprescindibile per garantire che i sistemi complessi possano operare senza causare rischi inaccettabili per le persone, l'ambiente e le infrastrutture.

Nel contesto industriale e automotive, la sicurezza funzionale si occupa di assicurare che le funzioni di sicurezza dei sistemi robotici, quali il rilevamento di guasti, l'arresto d'emergenza e il controllo ridondante, siano progettate, implementate e mantenute in modo tale da minimizzare il rischio di incidenti. Per raggiungere tali obiettivi, si è reso necessario lo sviluppo e l'adozione di protocolli di sicurezza e standard internazionali che stabiliscano le linee guida per la progettazione, la verifica e la convalida dei sistemi.

Tra gli standard più rilevanti in questo ambito, l'ISO 26262 è considerato il punto di riferimento per la sicurezza funzionale dei sistemi elettrici ed elettronici nei veicoli stradali, fornendo un quadro normativo completo che copre l'intero ciclo di vita del prodotto. In ambito industriale, l'ISO 13849 e l'IEC 61508 sono altrettanto cruciali, definendo i requisiti per la sicurezza delle macchine e dei sistemi di controllo programmabili, mentre lo standard ISO/TS 15066 fornisce le linee guida di sicurezza per sistemi robotici come manipolatori e per l'interazione di tali con operatori umani. Questi standard hanno spianato la strada a un approccio sistematico alla sicurezza funzionale, che si traduce in processi di sviluppo più rigorosi e nell'adozione di tecniche avanzate di gestione del rischio.

Nonostante gli avanzamenti significativi nello sviluppo di standard e protocolli di sicurezza, il rapido progresso tecnologico nei settori industriale e automotive continua a introdurre nuove sfide. L'adozione diffusa di tecnologie emergenti, come l'intelligenza artificiale, la robotica collaborativa

e i veicoli autonomi, richiede un continuo aggiornamento delle normative esistenti e l'implementazione di nuovi paradigmi di sicurezza funzionale.

Il lavoro di tesi si concentra sull'analisi dei robot collaborativi, con particolare attenzione ai manipolatori industriali e all'applicazione degli standard internazionali di sicurezza come ISO 10218, ISO/TS 15066 e ISO 26262. Dopo una panoramica sullo sviluppo tecnologico dei cobot, il lavoro si propone di sviluppare un sistema di controllo avanzato che integri funzionalità di rilevamento fault e risposta intelligente, garantendo la sicurezza dell'interazione uomo-robot. La ricerca, condotta in collaborazione con Bosch e il Politecnico di Bari, mira a trasferire i principi della functional safety dal settore automotive alla robotica collaborativa. Saranno identificati task industriali reali, progettando e testando strategie di controllo sicure, adattabili e affidabili per scenari complessi.

L'approccio prevede l'integrazione di sensori e sistemi di monitoraggio in tempo reale per gestire situazioni anomale senza compromettere la produttività. Verranno proposti meccanismi dinamici di intervento proporzionale alla gravità del fault, per garantire la continuità operativa in condizioni di sicurezza. La tesi mira anche a fornire indicazioni concrete per l'evoluzione futura delle normative di settore. Il risultato atteso è un prototipo di sistema robotico collaborativo più sicuro, flessibile e pronto per applicazioni in ambienti industriali reali. Questo contributo si inserisce nella più ampia visione di una robotica sempre più autonoma, sicura e integrata nei processi produttivi.

Capitolo I – Obiettivi

Il presente lavoro di tesi si prefigge di affrontare una tematica di crescente importanza nel contesto dell'automazione industriale avanzata: l'analisi approfondita dello stato dell'arte dei robot collaborativi (cobot), con un focus specifico sui manipolatori industriali, e l'applicazione rigorosa dei dettami degli standard di sicurezza internazionali al fine di individuare e sviluppare soluzioni innovative per la gestione efficace dei fault.

Lo sviluppo dinamico del settore dei cobot è intrinsecamente legato ai significativi progressi registrati in diverse aree tecnologiche chiave. Tra queste, spiccano l'evoluzione dei sistemi di sensori, l'integrazione sempre più sofisticata dell'intelligenza artificiale e lo sviluppo di software avanzati per il controllo robotico. I cobot si distinguono per la loro capacità di operare in prossimità e in collaborazione diretta con l'essere umano, resa possibile dalla dotazione di sensori di coppia, forza e visione. Questi dispositivi sensoriali svolgono un ruolo cruciale nel rilevamento e nella risposta alla presenza dell'operatore, garantendo un'interazione fisica sicura.

La sicurezza di tale interazione è un aspetto non negoziabile, sancito da normative internazionali di riferimento quali la ISO 10218 e la ISO/TS 15066. Il rispetto di tali standard rappresenta un prerequisito fondamentale per l'implementazione sicura ed efficace dei cobot in ambienti industriali.

Parallelamente alla sicurezza, il lavoro di tesi riconosce l'importanza cruciale della flessibilità, dell'adattabilità e della modularità dei sistemi robotici collaborativi. La capacità di un cobot di eseguire una varietà di compiti differenti senza richiedere una riprogettazione completa del sistema, unitamente alla possibilità di integrare facilmente diversi accessori (come pinze, sistemi di visione artificiale e altri strumenti), ne amplifica notevolmente il potenziale applicativo in contesti produttivi dinamici e diversificati.

Le aree di applicazione dei manipolatori collaborativi sono in continua espansione e spaziano in numerosi settori industriali. Tra i principali si annoverano il settore automobilistico e dell'elettronica, dove i cobot sono impiegati in attività di assemblaggio, manipolazione e controllo qualità; il settore logistico e i magazzini automatizzati, per operazioni di picking, packing e palettizzazione; la chirurgia robotica assistita e l'assistenza agli anziani o ai disabili, in ambiti che richiedono precisione e interazione delicata, l'imballaggio e il confezionamento in svariati settori merceologici e molti altri ambiti in cui la collaborazione uomo-robot può apportare significativi benefici in termini di efficienza, ergonomia e sicurezza.

Nonostante il loro crescente successo, il campo dei cobot si trova attualmente ad affrontare alcune sfide significative. Una delle principali limitazioni riguarda la capacità di gestione di carichi pesanti e le velocità operative, che generalmente non raggiungono i livelli dei robot industriali tradizionali. Un'ulteriore area di intensa ricerca è focalizzata sul miglioramento della fluidità e della naturalezza della collaborazione uomo-robot, in particolare in ambienti di lavoro complessi e non strutturati. In questo contesto, l'intelligenza artificiale e le tecnologie di apprendimento automatico rivestono un ruolo fondamentale nello sviluppo di sistemi in grado di comprendere il contesto operativo, anticipare le intenzioni dell'operatore e reagire in modo intuitivo e sicuro.

In linea con queste sfide e opportunità, l'obiettivo primario di questo lavoro di tesi è duplice. In primo luogo, si intende analizzare criticamente lo stato attuale della tecnologia dei robot collaborativi e delle relative normative di sicurezza. In secondo luogo, il lavoro si propone di sviluppare e valutare un sistema di controllo innovativo per un manipolatore collaborativo in un contesto di interazione diretta con un operatore umano.

Tale attività di ricerca si inserisce all'interno di una più ampia iniziativa di collaborazione tra l'azienda Bosch e il Politecnico di Bari, finalizzata all'espansione e al consolidamento delle conoscenze nel campo della functional safety. Bosch, leader mondiale nel settore dell'automazione e dell'automotive, vanta una consolidata esperienza nell'applicazione della normativa ISO 26262. In questo ambito, l'azienda ha maturato competenze avanzate nella progettazione, validazione e certificazione di sistemi critici per la sicurezza, come centraline elettroniche e sistemi di assistenza alla guida (ADAS).

L'obiettivo condiviso con il Politecnico di Bari è quello di esplorare nuove frontiere per l'applicazione dei principi di sicurezza funzionale a sistemi robotici cooperativi, promuovendo lo sviluppo di architetture di controllo che integrino funzionalità di autodiagnosi, risposta intelligente ai fault e adeguamento dinamico del comportamento del robot in presenza di anomalie.

Questa tesi si configura dunque come un primo passo operativo per tradurre tale visione in una prototipazione concreta, studiando come adattare e implementare, nel dominio della robotica, gli approcci consolidati dell'ambito automotive. In questo modo si intende contribuire alla definizione di strategie di controllo sicure e intelligenti, in linea con gli standard internazionali esistenti (come la ISO 10218 e la ISO/TS 15066) e

in prospettiva compatibili con future evoluzioni normative ispirate alla ISO 26262, in risposta all'evoluzione tecnologica e all'aumento del livello di autonomia e complessità dei robot collaborativi.

Per raggiungere tale obiettivo, si prevede di:

- Identificare uno o più task specifici che possano essere eseguiti in modo collaborativo tra un manipolatore industriale e un operatore umano. La scelta dei task sarà guidata dalla necessità di evidenziare le potenzialità e le sfide della collaborazione in un contesto industriale reale.
- Sviluppare un sistema di controllo avanzato per il manipolatore, integrando le linee guida e i requisiti definiti dagli standard di sicurezza pertinenti. Un'attenzione particolare sarà posta alla progettazione di funzionalità che garantiscano la sicurezza dell'operatore e dello spazio di lavoro circostante durante l'esecuzione dei task collaborativi.
- Implementare un sistema di rilevamento dei fault in tempo reale basato sui dati forniti dai sensori del manipolatore. Questo sistema sarà in grado di monitorare costantemente lo stato del robot e dell'ambiente circostante, identificando eventuali anomalie o condizioni di fault.
- Implementare interventi di sicurezza dinamici e proporzionali in risposta ai fault rilevati. L'obiettivo è quello di applicare misure di sicurezza adeguate alla gravità del fault, minimizzando le interruzioni non necessarie del processo produttivo senza compromettere in alcun modo la sicurezza dell'operatore.

Attraverso l'analisi, la progettazione, l'implementazione e la valutazione del caso di studio, questo lavoro di tesi mira a fornire un contributo significativo alla comprensione e al miglioramento della sicurezza e dell'efficienza dei robot collaborativi nell'industria moderna.

Capitolo II - Introduzione

Human Robot Interaction

La Human Robot Interaction (HRI) [1] [2] [3] ha recentemente riscontrato un'attenzione considerevole nella comunità accademica e nel settore tecnologico. Rappresenta un campo di studio per la comprensione, lo sviluppo e la valutazione dei sistemi robotici volti all'uso o in collaborazione con l'uomo. La comunicazione tra l'uomo e il robot può avvenire in diverse modalità, ed esse sono ampiamente influenzate dalla loro prossimità fisica. La comunicazione può essere perciò divisa in due categorie generali:

- Interazione remota: l'uomo e il robot sono separati spazialmente o anche temporalmente
- Interazione in prossimità: l'uomo e il robot sono collocati nello stesso spazio operativo

In queste categorie è opportuno distinguere le applicazioni che richiedono mobilità, manipolazione fisica o interazione sociale. L'interazione remota fa riferimento solitamente ad operazioni di teleoperazione o controllo di supervisione, ad esempio operazioni di telemanipolazione per manipolatori robotici. L'interazione in prossimità con robot mobili può essere in forma di assistenza robot, oppure può prevedere e ammettere un'interazione fisica. L'interazione sociale, d'altro canto, prevede gli aspetti sociali, emotivi e cognitivi dell'interazione.

È importante definire e capire le interazioni tra uno o più umani e uno o più robot. Le interazioni tra uomo e robot sono presenti in tutte le applicazioni robotiche, anche per quelli autonomi: perciò, è fondamentale capire e valutare le capacità di uomo e robot, e sviluppare tecnologie volte a produrre le interazioni desiderate.

L'autonomia risulta essere un mezzo per supportare un'interazione produttiva tra uomo e robot, perciò la sua natura varia considerevolmente tra le diverse applicazioni. I livelli di autonomia (*Levels of Autonomy*) descrivono in che grado di autonomia i robot possono operare, ed una definizione comprensiva di tali livelli viene fornita da Tom Sheridan secondo una scala di livelli, dal più basso al più alto livello di autonomia:

1. Nessuna assistenza, l'uomo ha completo controllo;
2. Vengono fornite un set di azioni alternative all'uomo;
3. Viene effettuata una selezione delle possibilità;
4. Viene suggerita una singola azione;
5. L'azione selezionata viene eseguita sotto approvazione dell'uomo;
6. Il robot permette all'uomo di decidere in un tempo limitato prima dell'esecuzione automatica;
7. Il robot esegue automaticamente e poi informa l'uomo;
8. Il robot informa l'uomo dell'esecuzione automatica solo se egli lo richiede;
9. Il robot informa l'uomo solo se lo ritiene necessario;
10. Il robot decide autonomamente ignorando l'uomo.

Se tali livelli sono utili al comprendere il livello di autonomia di un robot, da un punto di vista dell'interazione uomo-robot, un modo complementare per considerare il concetto di autonomia è descrivere a che livello interagiscono e in che grado sia l'uomo che il robot sono autonomi.

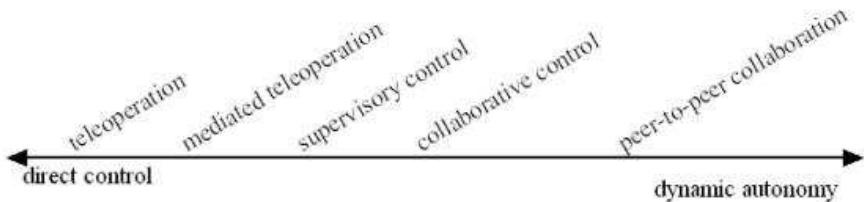


Figura 1 - Livelli di autonomia con enfasi sulle HRI

L'autonomia in un robot è implementata tramite la teoria del controllo, l'intelligenza artificiale, il processing dei segnali e la scienza cognitiva. Ad oggi, modelli di acquisizione-ragionamento-azione sono costruiti a partire da sistemi basati sul comportamento, a formare architetture ibride. In tali sistemi, la reattività a basso livello è separata dal ragionamento ad alto livello sulla pianificazione e sugli obiettivi. A complemento delle migliori negli algoritmi di controllo, ci sono stati progressi nel campo dei sensori, dell'elaborazione dei segnali e degli algoritmi di ragionamento: in particolare, gli algoritmi di localizzazione probabilistica, specialmente nella robotica mobile, sono stati utilizzati molto per la l'identificazione e mappatura degli ambienti e del robot stesso.

Un'altra componente fondamentale per rendere un'interazione benefica e sicura tra uomo e macchina è lo scambio di informazioni: le misure per valutare l'efficienza dell'interazione includono il tempo di interazione richiesto per comunicare al robot intenti o istruzioni, il carico di lavoro

mentale o cognitivo di una interazione, la quantità di percezione della situazione prodotta dall'interazione (o ridotta a causa di interruzione del robot), e la quantità di conoscenze condivise o piani comuni tra uomo e robot. Due particolari dimensioni primarie determinano il modo in cui avviene lo scambio di informazioni tra uomo e robot: il mezzo di comunicazione e la modalità di comunicazione. I mezzi primari di comunicazione sono delineati da tre dei cinque sensi: vista, udito e tatto, manifestati nelle HRI nelle seguenti modalità:

- Display visivi, tipicamente interfacce utente o interfacce di realtà aumentata;
- Gestures, che includono movimenti manuali e facciali e da segnalazioni di intenti basati sul movimento;
- Comandi vocali e linguaggio;
- Segnali acustici;
- Interazioni fisiche e aptiche.

Tali modalità di interazione variano in base al contesto e al dominio di utilizzo.

Nonostante l'adattamento e l'apprendimento dei robot è stato argomento di ricerca, l'addestramento dell'uomo ha ricevuto meno attenzioni pur ricoprendo un ruolo cruciale nella HRI. Ciò è dovuto al fatto che i robot progettati per l'interazione con l'uomo sono stati sviluppati con l'intento di non richiedere particolari addestramenti, essendo i loro domini di utilizzo particolarmente specifici e limitati temporalmente nell'interazione.

La crescente diffusione dei robot collaborativi impone una riflessione approfondita non solo sull'efficacia dell'interazione uomo-robot, ma anche sulla necessità di garantire elevati standard di sicurezza durante tale interazione. Infatti, la prossimità fisica tra operatore e robot introduce nuove sfide legate alla prevenzione di rischi e incidenti. In questo contesto, l'interfaccia intuitiva e la cooperazione fluida devono essere accompagnate da meccanismi di protezione affidabili e reattivi. È proprio qui che entra in gioco il concetto di sicurezza funzionale, elemento imprescindibile per una collaborazione efficace e sicura.

Functional Safety

Il primo passo per la comprensione del concetto di sicurezza in ambito industriale e non è quello di definire cosa si intende per ‘sicuro’. Nella prima edizione della guida ISO/IEC 51 sugli standard basilari internazionali di sicurezza, la quale propone delle linee guida introduttive sulla sicurezza, la parola ‘sicuro’ è definita come ‘nessun rischio inaccettabile’. La doppia negazione, poco chiara ai fini della comprensione, può essere tradotta come ‘libero da rischi che risultano non tollerabili’. Definiamo adesso il concetto di ‘pericoloso’, che può essere associato a quello di ‘rischio’, il quale può essere più o meno grande. Attuando delle misure contro i rischi maggiori si possono portare delle situazioni ‘pericolose’ in un range accettabile, rendendo lo stato di pericolo uno stato ‘sicuro’.

Definite le situazioni di rischio e i concetti di ‘sicuro’ e ‘pericoloso’, si possono approfondire i concetti di functional safety e intrinsic safety [4], evidenziandone le differenze. Con intrinsic safety si intende un metodo per garantire la sicurezza rimuovendo le cause di pericolo potenziale. Tramite functional safety, si riduce il rischio ad un livello accettabile per garantire la sicurezza con funzioni specifiche. La rimozione dei pericoli tramite intrinsic safety garantisce una sicurezza assoluta ma tende ad essere generalmente più costosa. D’altro canto, la functional safety permette di garantire la sicurezza a costi inferiori, ma necessita di una maggiore attenzione in fase di progettazione delle misure di sicurezza, dovendo tener conto di tutte le possibili casistiche di insuccesso o errore.

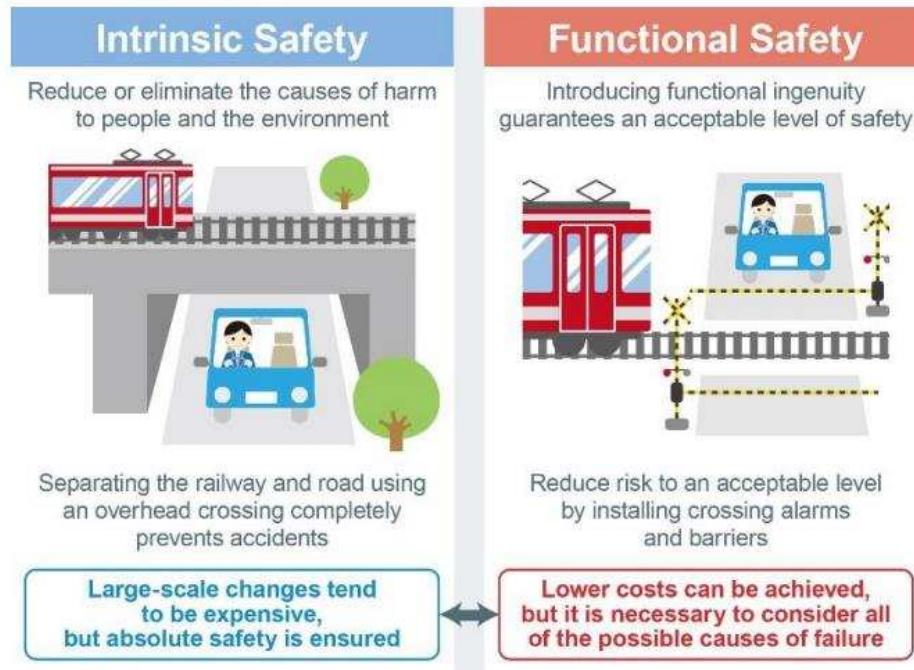


Figura 2 - Sicurezza intrinseca e sicurezza funzionale

Per ottenere una situazione sicura tramite functional safety, perciò, è necessaria una valutazione accurata di tutte le possibili cause di insuccesso in un determinato processo o situazione, specialmente valutando la possibilità di errori umani (nel caso essi siano coinvolti) o di guasti inattesi [5]. È quindi fondamentale effettuare una distinzione tra le possibili cause di fallimento o errore in due categorie: systematic failure e random failure. I systematic failure fanno riferimento a problemi creati in fase di design (comunemente chiamati bugs), evitabili utilizzando un design flow che non porti a un errore di progetto. In particolare, si inizia con la creazione di specifiche basate sui requisiti, ed ogni processo, inclusi design, verifica, prototipazione e valutazione, sono esplicate e documentate ad ogni fase di sviluppo. È inoltre importante rendere tale documentazione aggiornata e custodita accuratamente per renderla reperibile in ogni momento della progettazione. I random failures, invece, fanno riferimento a problemi o errori che avvengono dopo la fase di design, e perciò non possono essere prevenuti completamente; per tale motivo, meccanismi di sicurezza devono essere presenti per prevenire danni a persone o cose anche in caso di errore.

Nei contesti industriali in cui la sicurezza funzionale riveste un ruolo centrale, risulta fondamentale adottare metodologie sistematiche per l'analisi e la gestione dei guasti. In questo ambito si inseriscono tecniche consolidate come FMEA, FMEDA, FMECA e FTA, strumenti analitici, i quali permettono di

individuare preventivamente le modalità di guasto, valutarne le conseguenze sul sistema e progettare contromisure adeguate, contribuendo così ad aumentare l'affidabilità, la sicurezza e la robustezza dei sistemi collaborativi complessi, come i robot industriali. Le varie metodologie introdotte sono di seguito descritte ed approfondite.

FMEA

La FMEA (Failure Mode and Effect Analysis) [6] [7] è una metodologia utilizzata per analizzare le modalità di guasto o di difetto di un processo, prodotto o sistema, analizzarne le cause e valutarne gli effetti sull'intero sistema/impianto. Generalmente (ma non necessariamente) l'analisi è eseguita preventivamente; quindi, si basa su considerazioni teoriche e non sperimentali.

- “Failure Mode” o modalità di fallimento: descrive i possibili modi in cui ciascuna componente del processo potrebbe presentare un malfunzionamento. I guasti/errori/difetti possono essere potenziali o effettivi.
- “Effect Analysis” o analisi degli effetti: si riferisce all'individuazione delle potenziali conseguenze dei malfunzionamenti, sia a livello di procedure interne all'azienda che a livello di reputazione aziendale con il cliente.

I principali motivi per cui l'analisi FMEA è utilizzata sono:

- Aumento dell'efficienza aziendale;
- Riduzione dei costi di riparazione;
- Maggiore tempo di attività;
- Maggiore sicurezza per i lavoratori e gli utenti;
- Aumentare la velocità di risposta ai problemi.

Il primo passo da realizzare nella tecnica FMEA consiste nella scomposizione del processo, prodotto o sistema in esame in sottosistemi elementari. A questo punto, nell'analisi dei malfunzionamenti di ogni sottosistema, occorre elencare tutte le possibili modalità di fault, e per ciascuna elencarne tutte le possibili cause, tutti i possibili effetti e tutti i controlli in essere (a prevenzione o a rilevamento del fault). I controlli sono tutti quegli accorgimenti che, nel caso di FMEA di prodotto, prevengono o rilevano carenze progettuali che possono sfociare nel malfunzionamento anzidetto o che, nel caso di FMEA di processo, prevengono o rilevano carenze produttive che possono sfociare nello stesso fault.

Per tutte le combinazioni fault - causa, si devono valutare tre fattori:

- P = probabilità di accadimento;
- G = gravità dell'effetto;
- R = possibilità di rilevamento da parte dei controlli (rilevabilità).

Ad ognuno dei tre fattori sarà assegnato un punteggio da 1 a 10, in cui (per le voci “P” e “G”) 1 rappresenta la condizione di minimo rischio e 10 quella di massimo rischio (per la voce “R” minore è il punteggio, maggiore è la possibilità di rilevamento del malfunzionamento). I punteggi devono essere assegnati secondo scale non lineari in modo da garantire una corretta ponderazione dei tre fattori. Nella pratica sono disponibili tabelle pubblicate da AIAG, VDA, ANFIA, SAE, etc. L’analisi appena descritta permette di individuare i fault più critici mediante l’indice di Priorità del Rischio (RPN).

$$RPN = P \times G \times R$$

Le azioni di miglioramento del prodotto, processo o sistema dovranno essere orientate principalmente sui malfunzionamenti che presentano i più alti valori di RPN. La FMEA può essere poi ripetuta a seguito delle azioni migliorative, per verificare se i valori di RPN sono diminuiti.

FMEDA

La FMEDA (Failure Modes Effects and Diagnostic Analysis) viene utilizzata per calcolare i guasti casuali di un componente: si tratta di un’estensione della procedura di FMEA classica. La tecnica è stata sviluppata inizialmente per dispositivi elettronici, attualmente viene utilizzata anche per dispositivi meccanici ed elettromeccanici. I risultati della FMEDA sono i diversi tassi di guasto utilizzati nella functional safety.

FMECA

La FMECA (Failure Modes, Effects and Criticality Analysis) è un’estensione della FMEA che include un mezzo per classificare la gravità dei fault per consentire la scelta di contromisure prioritarie.

FTA

La FTA (Fault Tree Analysis) [8] è un metodo di analisi dei guasti utilizzato principalmente nell'ingegneria della sicurezza e dell'affidabilità per comprendere come i sistemi possono fallire e ridurre i rischi. Essa utilizza simboli logici per mappare le relazioni tra guasti e sottosistemi, calcolando le probabilità di guasto e migliorando il design del sistema per ridurre i rischi.

ISO 13849

La norma EN ISO 13849-1 [9] è essenziale per valutare la sicurezza dei sistemi di controllo complessi delle macchine. Questa norma internazionale stabilisce i requisiti per determinare i Performance Level (PL) necessari, identificare i componenti di controllo rilevanti per la sicurezza e implementare le funzioni di sicurezza.

Si applica a parti e componenti legati alla sicurezza, indipendentemente dalla tecnologia utilizzata (elettrica, idraulica, pneumatica, meccanica). La norma descrive i requisiti di sicurezza per la configurazione e l'integrazione di queste parti, definendo proprietà e caratteristiche come il Performance Level richiesto (PLr) per eseguire specifiche funzioni di sicurezza.

Il rischio viene classificato in cinque livelli, da PL “a” (basso) a PL “e” (alto), con requisiti più elevati per i sistemi di controllo in situazioni più pericolose.

Nel 2023, l'ISO ha pubblicato una nuova edizione della norma ISO 13849-1. Questa revisione include disposizioni dettagliate per la determinazione del Performance Level e riconosce l'importanza crescente del software.

La norma EN ISO 13849-1 si basa su un approccio probabilistico in fase di valutazione di sistemi di controllo di sicurezza, includendo requisiti uniformi a livello internazionale che si riferiscono alla valutazione del rischio, alla determinazione dei PL necessari, all'identificazione dei componenti di controllo rilevanti per la sicurezza, fino all'implementazione delle funzioni di sicurezza. L'assegnazione dei rischi ai PL richiesti viene effettuata sulla base di un grafico, oltre che della valutazione delle funzioni di sicurezza, attraverso metodi strutturali e statici.

Tramite tale grafico si analizzano e valutano la gravità di possibili lesioni, la frequenza di esposizione al rischio e l'evitabilità dei rischi. L'esito della valutazione è il Performance Level (PL) richiesto per le singole funzioni di sicurezza che hanno il compito di ridurre i rischi. Il rischio è associato ad una

lettera minuscola: ‘a’ è relativo ad un livello di rischio ridotto, ‘e’ ad un rischio elevato. Le lettere maiuscole S, F e P indicano:

- S – Gravità della lesione
 S1 = lesione lieve (solitamente reversibile)
 S2 = lesione grave, compresa la morte (solitamente irreversibile)
- F – Frequenza e/o durata dell’esposizione al pericolo
 F1 = durata da rara a frequente e/o breve
 F2 = durata da frequente a costante e/o prolungata
- P – Possibilità di evitare o ridurre il pericolo
 P1 = Possibile a determinate condizioni
 P2 = Quasi impossibile
 Inoltre, 5 fattori specificano ulteriormente tale parametro:
 1) Rapidità con cui insorge il pericolo;
 2) Opzioni per evitare il pericolo;
 3) Esperienze pratiche di sicurezza in combinazione con il processo;
 4) Operatività a cura di personale opportunamente formato o idoneo;
 5) Funzionamento con o senza sorveglianza.

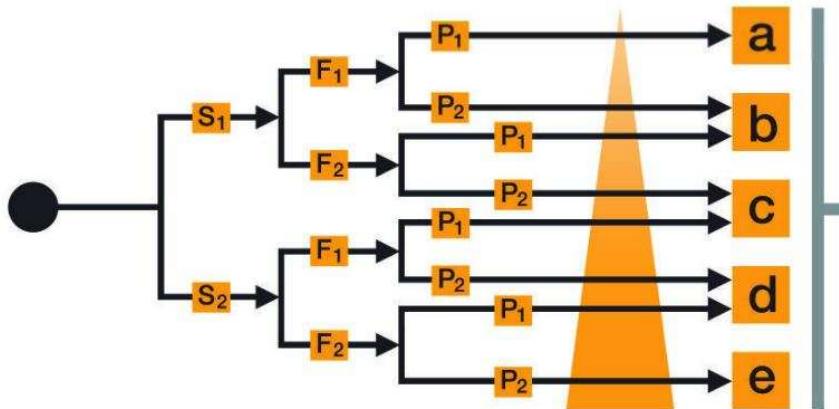


Figura 3 - Determinazione livelli di rischio

L’adozione di tecniche strutturate per l’analisi e la gestione dei guasti rappresenta un primo passo fondamentale per aumentare l’affidabilità dei sistemi collaborativi. Tuttavia, affinché tali approcci risultino efficaci e

riconosciuti a livello industriale, è necessario che siano allineati ai requisiti stabiliti dagli standard internazionali. Le normative di sicurezza, come le ISO di riferimento, forniscono infatti un quadro regolamentare preciso entro cui progettare, validare e certificare sistemi robotici sicuri. L'integrazione tra metodologie di analisi e standard normativi costituisce la base per un approccio coerente e conforme alla safety.

ISO 26262

Gli standard internazionali (IS) sono pubblicati dall'organizzazione internazionale per la standardizzazione (ISO), un'organizzazione non governativa con sede in Geneva, Svizzera. Lo standard ISO 26262 [10] è uno standard per la functional safety per veicoli stradali basata sul IEC 61508, uno standard internazionale pubblicato da IEC (International Electrotechnical Commission) per la functional safety in sistemi elettrici, sistemi elettronici, elettronica di sicurezza programmabile in tutti i tipi di industria. A partire dai concetti base del IEC 61508, lo standard ISO 26262 è stato creato come adattamento per i sistemi elettrici ed elettronici in ambito automotive.



Figura 4 - Standard functional safety

La prima versione dello standard ISO 26262 è stata pubblicata nel novembre 2011, mentre la seconda edizione, frutto di numerose revisioni, è stata rilasciata nel dicembre 2018. La prima edizione è incentrata sulle macchine

commerciali con passeggeri dal peso inferiore ai 3500kg, la seconda va ad ampliare lo spettro a veicoli come autotrasportatori, bus e motocicli.



Figura 5 - Panoramica ISO 26262

Per ottenere una certificazione ISO 26262 è necessario far testare il veicolo ad un corpo di terze parti incaricato di effettuare tutte le verifiche necessarie, che in Europa è affidata ad un'organizzazione di ispezione privata (TÜV, acronimo di *Technischer Überwachungs-Verein*), autorizzata dalla *German Technical Inspection Association*. È possibile ottenere tale certificazione senza l'ausilio di terzi, a patto di dimostrare accuratamente di essere conformi allo standard: tale procedura, spesso onerosa; rende preferibile affidarsi ad organizzazioni di terze parti.

ISO 10218

Racchiude i requisiti di sicurezza per l'integrazione dei robot in ambienti industriali; descrive le situazioni di pericolo identificate in tali sistemi, e

fornisce i requisiti necessari ad eliminare o ridurre adeguatamente i rischi associati a tali pericoli.

Poiché i sistemi robotici sono sempre integrati in una particolare applicazione, è necessaria una valutazione dei rischi per determinare le misure di riduzione del rischio per il suo intero ciclo di vita. La valutazione dei rischi comprende la determinazione dei limiti del robot, identificazione dei pericoli, stima dei rischi. Tra i limiti del robot, sono compresi i limiti di utilizzo (descrizione delle funzioni e delle diverse modalità di utilizzo, descrizione dell'interfaccia e degli strumenti), limiti spaziali (range di movimento, spazio per l'installazione e la manutenzione), limiti temporali.

Table A.1 — List of significant hazards

No.	Type or group	Example of hazards		Subclause reference
		Origin	Potential consequences	
1	Mechanical hazards	<ul style="list-style-type: none"> — movements of any part of the robot arm (including back), end-effector or mobile parts of robot cell — movements of external axis (including end-effector tool at servicing position) — movement or rotation of sharp tool on end-effector or on external axes, part being handled, and associated equipment — rotational motion of any robot axes — materials and products falling or ejection — end-effector failure (separation) — loose clothing, long hair — between robot arm and any fixed object — between end-effector and any fixed object (fence, beam, etc.) — between fixtures (falling in); between shuttles, utilities — impossibility of exiting robot cell (via cell door) for a trapped operator in automatic mode — unintended movement of jigs or gripper — unintended release of tool — unintended movement of machines or robot cell parts during handling operations — unintended motion or activation of an end-effector or associated equipment (including external axes controlled by the robot, process specific for grinding wheels, etc.) — unexpected release of potential energy from stored sources 	<ul style="list-style-type: none"> — crushing — shearing — cutting or severing — entanglement — drawing-in or trapping — impact — stabbing or puncture — friction, abrasion — high-pressure fluid/gas injection or ejection 	4.1; 4.2; 4.2 d) 6); 4.2 f); 4.3; 4.4; 4.4.1; 4.4.2 d); 4.4.2 f); 4.5; 5.2; 5.2.1; 5.2.2; 5.2.3; 5.3; 5.3.2; 5.3.6; 5.3.7; 5.3.8.2; 5.3.9; 5.3.10; 5.5.1; 5.5.2; 5.5.3; 5.5.4; 5.6.4; 5.8; 5.9; 5.10.2; 5.10.3; 5.10.6.1; 5.10.6.2; 5.10.6.4; 5.10.7; 5.11; 5.11.4; 5.11.5.4

Figura 6 - Lista dei possibili pericoli - 1

No.	Type or group	Example of hazards		Subclause reference
		Origin	Potential consequences	
7	Material/ substance hazards	<ul style="list-style-type: none"> — contact with components covered in harmful fluids — failures of mechanical and electrical components — corrosive fumes and dust 	<ul style="list-style-type: none"> — sensitization — fire — chemical burn — inhalation illnesses 	4.2, 4.3, 4.4, 4.5, 5.5.2, 5.5.3
8	Ergonomic hazards	<ul style="list-style-type: none"> — poorly designed teach pendant, HMI touch screen or operator panel (too far or high) — poorly designed loading/unloading post (e.g. long distance between components box location and loading/unloading area) — poorly designed enabling devices — inappropriate location or identification of controls (e.g. hard to reach) — inappropriate location of components that require access (troubleshooting, repair, adjustment) — obscured hazards, inadequate or blocked local lighting 	<ul style="list-style-type: none"> — unhealthy postures or excessive effort (repetitive strain) — fatigue 	4.2 d); 4.3; 4.4; 4.5; 5.3.2; 5.3.13; 5.5; 5.5.2; 5.5.3; 5.9
9	Hazards associated with environment in which the machine is used	<ul style="list-style-type: none"> — installations in earthquake zones — electromagnetic interference or surges in energy source — moisture — temperature 	<ul style="list-style-type: none"> — burn, — disease or illness — slipping, falling — respiratory damage — impact 	4.1; 4.2; 5.2; 5.3; 5.5
10	Combinations of hazards	<ul style="list-style-type: none"> — robot system directed to start by one person, but this action is not expected by another person — hazards encountered due to multiple failures/situations — misidentification of actual problem and compound problem by making incorrect or unnecessary actions — action increases severity of harm, i.e. in avoiding a sharp edge, contact is made with a hot surface instead — unintended release of holding devices allowing motion under residual forces (inertia, gravity, spring/energy storage means) — failure of a safeguarding device to function as expected 	<ul style="list-style-type: none"> — any other consequence of combinations of hazards and hazardous situations 	4.2; 4.3; 4.4; 4.5; 5.2; 5.3.10; 5.6.3.3; 5.8; 5.9; 5.9.1;

Figura 7 - Lista dei possibili pericoli - 2

No.	Type or group	Example of hazards		Subclause reference
		Origin	Potential consequences	
2	Electrical hazards	<ul style="list-style-type: none"> — contact with live parts or connections (electrical cabinet, terminal boxes, control panels at machine) — confusion of various voltages within a system, electrical cabinet and terminals, i.e. drive power, control power (24 V versus 110 V) — contact with discrete components in the electrical (electronic) circuitry, i.e. capacitors — exposure to arc flash — process using high voltage or high frequency, i.e. electrostatic painting, inductive heating — welding applications using high voltage 	<ul style="list-style-type: none"> — electrocution — shock — burn — projection of molten particles 	4.4.1; 5.3.2; 5.3.6; 5.3.7; 5.8.2; 5.10.6.1; 5.10.6.2; 5.10.7
3	Thermal hazards	<ul style="list-style-type: none"> — hot surfaces associated with the end-effector, or associated equipment or work piece (e.g. welding torches, hot materials in forging presses, injection moulding, grinding and de-burring) — cold surfaces or objects (cryogenic processes) — explosive atmosphere caused by the process, i.e. paint (atomized particles, powder painting), flammable solvents, grinding and milling dust — temperature extremes required to support the process [molten materials; ovens for cooking or heating (autoclaves); freezer or chillers, etc.] — flammable materials (inside dust collector systems, cleaning tanks, sealant applicators) 	<ul style="list-style-type: none"> — burn (hot or cold) — radiation injury 	5.3; 5.5.2; 5.5.4
4	Noise hazards	<ul style="list-style-type: none"> — specific applications which are sources of high noise (e.g. a water jet cutter, stamping presses, pumps and valving, metal removing operations) — noise level preventing hearing or understanding audible danger warning signals, including inability of persons to coordinate their actions through normal conversation 	<ul style="list-style-type: none"> — loss of hearing — loss of balance — loss of awareness, disorientation — any other (e.g. mechanical) as a consequence of ambient conditions or distraction 	Noise is excluded from the scope of this part of ISO 10218
5	Vibration hazards	<ul style="list-style-type: none"> — direct contact with the source — loosening of connections, fasteners — misalignment of components or parts 	<ul style="list-style-type: none"> — fatigue — neurological damage — vascular disorder — impact 	4.2; 4.3, 4.4, 4.5, 5.5.2, 5.5.9
6	Radiation hazards	<ul style="list-style-type: none"> — EMF interference with proper operation of the robot system — exposed to process-related radiation, i.e. arc welding, laser. 	<ul style="list-style-type: none"> — burn — damage to eyes and skin — related illnesses 	4.2, 4.3, 4.4, 4.5, 5.5.2, 5.5.9

Figura 8 - Lista dei possibili pericoli - 3

ISO/TS 15066

L’obiettivo dei robot collaborativi è quello di combinare l'affidabilità e la consistenza delle performance dei robot con le abilità individuali dell'uomo:

l'essere umano ha eccellenti capacità di problem solving, mentre il robot fornisce potenza, precisione e durata delle prestazioni. Per raggiungere una certa sicurezza, le applicazioni tradizionali prevedono l'esclusione dell'operatore dalle zone operative mentre il robot è in funzione; inoltre, molte operazioni che necessitano dell'intervento dell'uomo spesso non possono essere automatizzate tramite l'utilizzo di sistemi robotici. Lo standard ISO/TS 15066 fornisce linee guida per operazioni che includono robot collaborativi nelle quali operatori umani e sistemi robotici condividono la stessa area operativa. In tali operazioni, l'integrità del sistema di controllo di sicurezza assume maggior importanza, in particolar modo quando parametri come velocità e forza sono controllati. Una valutazione del rischio dettagliata è necessaria non solo per il robot stesso, ma anche per l'ambiente nel quale esso è locato.

Le specifiche tecniche definite dallo standard supportano gli standard di sicurezza per robot industriali definiti nelle ISO 10218-1 e 10218-2.

Per la comprensibilità del documento, vengono fornite le definizioni per alcuni termini chiave:

- Collaborative operation: stato nel quale un sistema robotico orientato ad uno scopo ed un operatore collaborano all'interno di uno spazio cooperativo;
- Power mechanical power: rateo meccanico di produzione, o quantità di energia consumata nell'unità di tempo;
- Collaborative workspace: zona all'interno dello spazio collaborativo nella quale il robot e l'uomo possono compiere delle operazioni in concomitanza;
- Quasi-static contact: contatto tra un operatore e una parte del sistema robotico, casi in cui arti dell'operatore possono essere schiacciati o bloccati tra le parti mobili del robot o parti fisse e mobili della cella robotica;
- Transient contact: contatto tra un operatore e parti del sistema robotico, situazioni nelle quali l'operatore non rimane incastrato e può recuperare o liberarsi dalle parti mobili del sistema robotico;
- Protective separation distance: la minima distanza permessa tra una qualsiasi parte del robot potenzialmente pericolosa ed una qualsiasi persona nello spazio collaborativo (può essere fissa o variabile);
- Body model: rappresentazione del corpo umano che consiste in segmenti individuali del corpo caratterizzati da proprietà biomeccaniche;

Una parte chiave nella progettazione di un sistema robotico collaborativo e del layout della cella di lavoro è l'eliminazione dei pericoli e la riduzione del rischio, e può includere o influenzare il design dell'ambiente di lavoro. I principali fattori che vanno presi in considerazione sono:

- Limiti tridimensionali stabiliti per lo spazio collaborativo;
- Accessi ed autorizzazioni allo spazio collaborativo;
- Ergonomia ed interfaccia dell'uomo con l'attrezzatura;
- Limiti d'utilizzo;
- Transizioni (limiti temporali).

È importante condurre una ricerca di tutti i possibili pericoli derivanti dal processo di collaborazione tra uomo e robot, oltre a quelli relativi al robot in sé: il processo di identificazione dei pericoli deve considerare almeno:

- Pericoli relativi al robot, tra i quali caratteristiche del robot (carico, velocità, forza, momento, coppia, potenza, geometria, materiale e forma della superficie), condizioni di quasi-static contact, locazione dell'operatore rispetto al robot;
- Pericoli relativi al sistema robotico, quali pericoli attribuiti all'end-effector, posizione e movimento dell'operatore, design delle apparecchiature e degli end effector;
- Pericoli relativi alle applicazioni, come pericoli specifici (temperature, parti espulse, schegge da saldatura), limiti causati dall'attrezzatura del personale, disattenzioni nell'ergonomia (perdita di attenzione, operazioni improprie).

Fondamentale è l'identificazione dei processi associati al sistema robotico; tutte le combinazioni di processi e pericoli devono essere previste e identificate. I processi collaborativi possono essere caratterizzati da:

- Frequenza e durate della presenza di un operatore nello spazio collaborativo con un robot movente;
- Frequenza e durata del contatto tra operatore e sistema robotico con il sistema di potenza o applicazioni relative a sorgenti attive di energia;
- Transizioni tra operazioni collaborative e non collaborative;
- Restart automatico o manuale del sistema di movimento del robot al termine dell'operazione collaborativa;
- Operazioni che comprendono più operatori;
- Ogni processo addizionale nello spazio collaborativo.

Per quanto riguarda l'eliminazione dei pericoli e la riduzione dei rischi, sono identificati in ordine di priorità:

- Eliminazione dei pericoli intrinsecamente tramite design di sicurezza o riduzione di essi;
- Misure di protezione che prevengono l'accesso del personale ad un pericolo o controllo del pericolo portandolo in uno stato sicuro prima che un operatore possa accedere o possa essere esposto ad esso;
- Provvedere a misure protettive supplementari come istruzioni all'uso, corsi di formazione, segnaletiche, attrezzature di protezione per il personale, etc.

Nel caso di robot non collaborativi, la riduzione del rischio è ottenuta tramite barriere di sicurezza che separano l'operatore dal sistema robotico.

Modalità operative

Le operazioni collaborative [11] possono includere uno o più dei seguenti metodi:

- 1) Safety-rated monitored stop;
- 2) Hand guiding;
- 3) Speed and Separation Monitoring (SSM);
- 4) Power and Force Limiting (PFL).

1. Safety-rated stop

Tale metodo permette di fermare il movimento del robot nello spazio collaborativo prima che l'operatore entri anch'egli in tale spazio per interagire col sistema robotico e completare un'operazione (come piazzare un carico sull'end effector). Se non è presente nessun operatore nello spazio collaborativo, il robot può operare in modalità non-collaborativa. Nel momento in cui l'operatore abbandona la zona cooperativa, il robot può riprendere senza ulteriori interventi il suo normale funzionamento.

Robot motion or stop function		Operator's proximity to collaborative workspace	
		Outside	Inside
Robot's proximity to collaborative workspace	Outside	Continue	Continue
	Inside and moving	Continue	Protective stop
	Inside, at Safety - Rated Monitored Stop	Continue	Continue

Figure 2 — Truth table for safety-rated monitored stop operations

Figura 9 - Tabella della verità per le operazioni di safety-rated monitored stop

Lo spazio collaborativo deve essere stabilito in accordo ai requisiti dello standard ISO 13855. Il robot deve essere equipaggiato con dispositivi di sicurezza che permettono la rilevazione di un operatore all'interno dello spazio collaborativo; anche l'accesso allo spazio collaborativo deve essere controllato in accordo alla valutazione dei rischi.

Mentre il safety-rated stop è attivo, l'operatore ha il permesso di entrare nella zona collaborativa sotto le seguenti condizioni:

- Sistema robotico o altri pericoli non presenti nello spazio collaborativo;
- Sistema robotico nello spazio collaborativo e safety-rated monitored stop attivo;
- Sistema robotico nello spazio cooperativo in stato di protective stop, in accordo con i requisiti dello standard ISO 10218-1:2011.

2. Hand Guiding

In tale metodo operativo, l'operatore utilizza un dispositivo di comando manuale per trasmettere istruzioni di movimento al sistema robotico. Prima di permettere all'operatore di poter entrare nello spazio collaborativo, il robot

deve essere nella modalità safety-rated monitored step. L’operazione si volge nelle seguenti modalità:

- Il robot è pronto all’hand guiding quando entra nello spazio collaborativo e performa un safety-rated monitored stop: a quel punto, l’operatore può entrare nello spazio collaborativo;
- Nel momento in cui l’operatore è in controllo del dispositivo di comando, il safety-rated monitored stop viene arrestato e l’operatore può completare il task;
- Al termine dell’operazione di hand guiding, viene istanziato nuovamente un safety-rated monitored stop;
- Quando l’operatore esce dallo spazio collaborativo, il robot può riprendere le operazioni non collaborative.

3. Speed and Separation Monitoring

In tale metodo operativo, il sistema robotico e l’operatore possono muoversi in concorrenza nello spazio collaborativo. La riduzione del rischio è ottenuta mantenendo almeno la distanza di separazione protettiva tra l’operatore e il robot in ogni istante. Durante il movimento del robot, il sistema robotico non si trova mai più vicino di tale distanza dall’operatore, e se la distanza di separazione scende al di sotto del valore limite, il sistema robotico viene stoppato. Quando l’operatore si allontana dalla zona collaborativa, il robot può riprendere il suo normale funzionamento; inoltre, ad una riduzione della velocità corrisponde anche una riduzione della distanza di separazione protettiva.

La massima velocità permessa e la minima distanza di separazione in un’applicazione può essere sia costante che variabile. Per valori variabili, tali possono essere tarati in modo continuo in base alle velocità relative e alle distanze tra robot e operatore. Per valori costanti, la velocità massima permessa e la distanza di separazione possono essere determinate dalla valutazione dei rischi nel peggior caso durante tutto il task. La distanza di separazione protettiva è descritta dalla formula:

$$S_p(t_0) = S_h + S_r + S_s + C + Z_d + Z_r \quad (1)$$

Dove

$S_p(t_0)$ è la distanza di separazione protettiva al tempo t_0 ;

t_0 è l’istante di tempo corrente;

S_h è il contributo attribuito al cambio di posizione dell'operatore;

S_r è il contributo attribuito al tempo di reazione del robot;

S_s è il contributo attribuito allo spazio di arresto del robot;

C è la distanza di intrusione definita nello standard ISO 13855; è la distanza che una parte del corpo può compiere all'interno della zona di monitoraggio prima di essere rilevata;

Z_d è la posizione di incertezza del collaboratore all'interno dello spazio collaborativo, misurata dal sensore di presenza e derivante dalla tolleranza del sistema di misurazione;

Z_r è la posizione di incertezza del sistema robotico, risultante dalla precisione del sistema di misurazione della posizione del robot.

La formula è applicata a tutte le combinazioni di personale all'interno dello spazio collaborativo e parti mobili del robot. Ad esempio, le parti più vicine tra una parte mobile del robot e un operatore potrebbero allontanarsi tra loro, mentre altre parti dell'operatore potrebbero avvicinarsi ad alcune parti del robot in movimento.

Il contributo S_h può essere espresso tramite la formula:

$$S_h = \int_{t_0}^{t_0 + T_r + T_s} v_h(t) dt \quad (2)$$

Dove

T_r è il tempo di reazione del sistema robotico, ed include il tempo di rilevazione della posizione dell'operatore, processing del segnale, attivazione dello stop del robot, ma escludendo il tempo di arresto del robot.

T_s è il tempo di arresto del robot, dall'attivazione del comando di stop fino al momento in cui il robot è fermo; T_s non è costante, ma funzione della configurazione del robot, del movimento pianificato, della velocità, dell'end effector e del carico;

v_h è la velocità direzionata dell'operatore nello spazio collaborativo in direzione della parte movente del robot, e può essere positiva o negativa dipendentemente dall'incremento o decremento della distanza di separazione;

t è la variabile di integrazione

Se la velocità v_h dell'operatore non è monitorata, il sistema assume un valore di riferimento pari a 1,6 m/s nella direzione che diminuisce la distanza di

separazione, oppure potrebbe variare da questo valore in base alla valutazione dei rischi. Un valore costante per S_h utilizzando la velocità dell'operatore pari a 1,6 m/s può essere stimata utilizzando la formula:

$$S_h = 1,6 \times (T_r + T_s) \quad (3)$$

Il contributo alla distanza di separazione attribuita al tempo di reazione del robot S_r è espressa dalla formula:

$$S_r = \int_{t_0}^{t_0+T_r} v_r(t) dt \quad (4)$$

Dove v_r è la velocità diretta del robot in direzione dell'operatore all'interno dello spazio collaborativo, e può essere positiva o negativa relativamente all'incremento o al decremento della distanza di separazione.

Il sistema deve essere progettato tenendo in conto che v_r può essere valutato in diverse casistiche:

- Se la velocità del robot non viene monitorata, il sistema assume v_r come la massima velocità raggiungibile dal robot;
- Se la velocità del robot viene monitorata, il sistema può utilizzare tale velocità, tenendo in conto che nel frattempo le accelerazioni del robot possono diminuire la distanza di separazione
- Se un limite di sicurezza per la velocità è già applicato, il sistema può utilizzare tale valore per il calcolo della distanza di sicurezza per la parte del robot in considerazione

Un valore costante per S_r può essere stimato utilizzando la formula:

$$S_r = v_r(t_0) \times T_r \quad (5)$$

Il contributo alla distanza di separazione dovuto allo spazio di arresto è dato dalla formula:

$$S_s = \int_{t_0+T_r}^{t_0+T_r+T_s} v_s(t) dt \quad (6)$$

Dove v_s è velocità del robot durante l'arresto, dall'attivazione del comando di stop fino al momento in cui il robot è fermo. Anche in questo caso possono verificarsi due casi:

- Se la velocità del robot non è misurata, il sistema può assumere come valore la distanza direzionale che va a diminuire di più il valore della distanza di separazione;
- Se la velocità del robot è misurata, il sistema può utilizzare quella velocità per il calcolo di S_s .

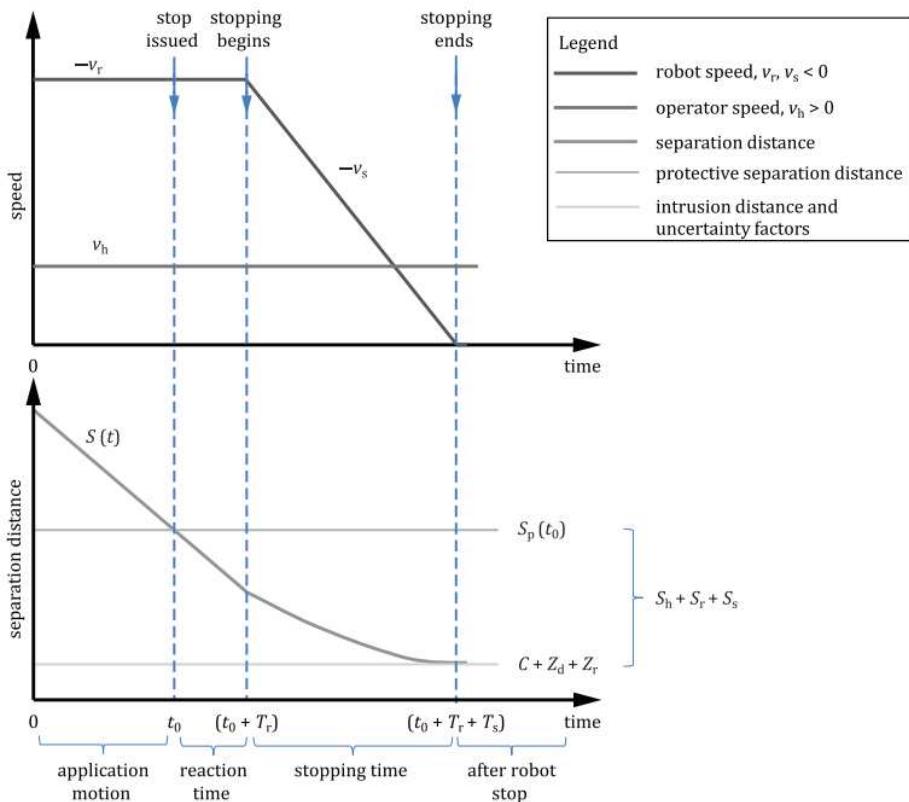


Figura 10 - Rappresentazione grafica dei contributi alla distanza di separazione protettiva tra operatore e robot

4. Power and Force Limiting

In tale metodo, il contatto fisico tra il sistema robotico e l'operatore può accadere in maniera intenzionale o non intenzionale. Le operazioni collaborative che utilizzano tale metodologia prevedono che i sistemi robotici siano appositamente sviluppati per tali task. La riduzione del rischio è ottenuta, sia tramite sicurezza intrinseca, sia tramite sistemi di controllo per la sicurezza, mantenendo i pericoli associati al sistema robotico sotto alcuni valori limite determinati durante la valutazione dei rischi.

Le situazioni di contatto possono essere di diversa matrice:

- Contatti volontari che fanno parte della sequenza applicativa;
- Situazioni di contatto incidentali, che possono essere conseguenza di non aderenza alle procedure di lavoro, ma senza un errore tecnico;
- Errori tecnici che portano a situazioni di contatto.

I tipi di contatto tra robot e operatore possono essere categorizzati in:

- Quasi-static contact, ovvero una parte del corpo dell'operatore è bloccata tra due parti mobili del robot; in tale situazione, la forza (o la pressione) applicata sulla parte bloccata del corpo dell'operatore è protesa nel tempo
- Transient contact, anche detta “impatto dinamico”, descrive una situazione nella quale una parte del corpo dell'operatore viene impattata da una parte mobile del robot, ed è possibile recuperare o liberarsi dal robot senza rimanere incastrato o intrappolato. Il transient contact è dipendente dall'inerzia del robot, da quella della parte umana interessata e dalle velocità relative dei due.

La riduzione dei rischi attribuite ai casi di quasi-static contact e transient contact possono essere passive o attive: quelle passive fanno riferimento al design meccanico del sistema robotico, mentre quelle attive fanno riferimento al design del sistema di controllo.

Le misure passive comprendono l'aumento dell'area di contratto (angoli arrotondati, superfici lisce e conformi), assorbimento dell'energia o estesa del tempo di trasferimento di essa (pad o cuscinetti di assorbimento, componenti deformabili), riduzione delle forze impattanti, e limitazione delle masse moventi.

Le misure attive comprendono la limitazione di forze e coppie, limitazione della velocità delle parti moventi, limitazione della potenza o dell'energia in funzione delle masse e delle velocità, utilizzo di funzioni di sicurezza relative alla limitazione dello spazio operativo, utilizzo del safety-rated monitored stop, utilizzo dei sensori per anticipare o prevedere una situazione di contatto.

I valori limite per i più rilevanti eventi di contatto sulle parti esposte del corpo devono essere analizzati considerando i “worst case”: le soglie per gli eventi transienti e quasi-static devono essere utilizzati nella determinazione del giusto livello di riduzione del rischio. Il design e le misure implementate devono mantenere il livello dei contatti al di sotto dei valori limite precedentemente definiti.

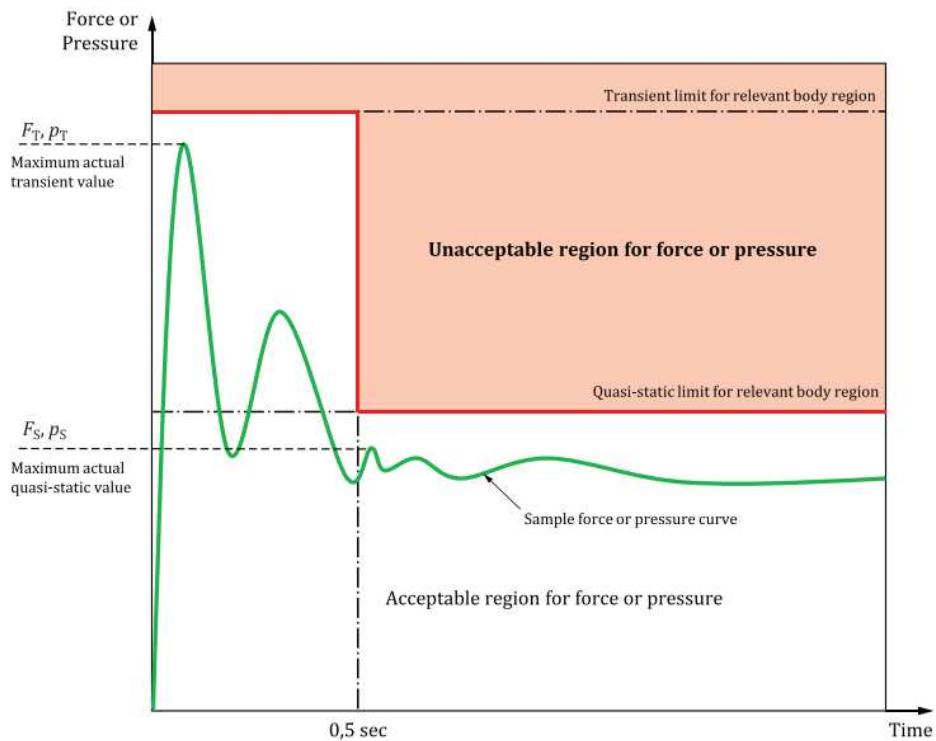


Figure 4 — Graphical representation of acceptable and unacceptable forces or pressures

Figura 11 - Rappresentazione grafica delle forze e pressioni ammissibili e non ammissibili

Di seguito vengono esplicate le metodologie per la determinazione delle soglie limite utilizzate nel power and force limiting.

Nella valutazione dei rischi bisogna tenere in conto i contatti accidentali tra alcune parti dei robot collaborativi e parti dell’operatore. Essendo le parti umane sensibili in modo differente agli urti, devono essere diverse le soglie per i massimi carichi sopportabili senza incorrere in infortuni: i contatti tra robot e uomo possono essere modellati considerando urti anelastici e considerando la capacità di carico del robot, insieme ad altri fattori inerenti alle varie parti dell’operatore in contatto. I valori di soglia sono ottenuti da vari studi sia sul livello del dolore sia per zone specifiche sia per aree più generiche, e le zone particolarmente a rischio sono contraddistinte da una sigla.

Table A.2 — Biomechanical limits

Body region	Specific body area	Quasi-static contact		Transient contact	
		Maximum permissible pressure ^a p_s N/cm ²	Maximum permissible force ^b N	Maximum permissible pressure multiplier ^c P_T	Maximum permissible force multiplier ^c F_T
<i>Skull and fore-head^d</i>	1 Middle of forehead	130	130	not applicable	not applicable
	2 Temple	110		not applicable	not applicable
<i>Face^d</i>	3 Masticatory muscle	110	65	not applicable	not applicable
	4 Neck muscle	140	150	2	2
<i>Neck</i>	5 Seventh neck muscle	210		2	
	6 Shoulder joint	160	210	2	2
<i>Back and shoulders</i>	7 Fifth lumbar vertebra	210		2	2
	8 Sternum	120	140	2	2
<i>Chest</i>	9 Pectoral muscle	170		2	
	10 Abdominal muscle	140	110	2	2
<i>Pelvis</i>	11 Pelvic bone	210	180	2	2
<i>Upper arms and elbow joints</i>	12 Deltoid muscle	190	150	2	2
	13 Humerus	220		2	
<i>Lower arms and wrist joints</i>	14 Radial bone	190	160	2	2
	15 Forearm muscle	180		2	
	16 Arm nerve	180		2	
Body region	Specific body area	Quasi-static contact		Transient contact	
		Maximum permissible pressure ^a p_s N/cm ²	Maximum permissible force ^b N	Maximum permissible pressure multiplier ^c P_T	Maximum permissible force multiplier ^c F_T
<i>Hands and fingers</i>	17 Forefinger pad D	300	140	2	2
	18 Forefinger pad ND	270		2	
	19 Forefinger end joint D	280		2	
	20 Forefinger end joint ND	220		2	
	21 Thenar eminence	200		2	
	22 Palm D	260		2	
	23 Palm ND	260		2	
	24 Back of the hand D	200		2	
	25 Back of the hand ND	190		2	
	26 Thigh muscle	250		2	
<i>Thighs and knees</i>	27 Kneecap	220	220	2	2
	28 Middle of shin	220		2	
<i>Lower legs</i>	29 Calf muscle	210	130	2	2

^a These biomechanical values are the result of the study conducted by the University of Mainz on pain onset levels. Although this research was performed using state-of-the-art testing techniques, the values shown here are the result of a single study in a subject area that has not been the basis of extensive research. There is anticipation that additional studies will be conducted in the future that could result in modification of these values. Testing was conducted using 100 healthy adult test subjects in 20 specific body areas. In each of the body areas, peak pressures were recorded for quasi-static contact were established without onset of pain thresholds. The maximum permissible pressure values shown here represent the 75th percentile of the range of recorded values for a specific body area. They are defined as the physical quantity corresponding to when pressures applied to the specific body area create a sensation corresponding to the onset of pain. Peak pressures are based on averages with a resolution size of 1 mm². The study results are based on a test apparatus using a flat (1.4 × 1.4) cm (metal) test surface with 2 mm radius on all four edges. There is a possibility that another test apparatus could yield different results. For more details of the study, see Reference [5].

^b The values for maximum permissible force have been derived from a study carried out by an independent organization (see Reference [6]), referring to 188 sources. These values refer only to the body regions, not to the more specific areas. The maximum permissible force is based on the lowest energy transfer criteria that could result in a minor injury, such as a bruise, equivalent to a severity of 1 on the Abbreviated Injury Scale (AIS) established by the Association for the Advancement of Automotive Medicine. Adherence to the limits will prevent the occurrence of skin or soft tissue penetrations that are accompanied by bloody wounds, fractures or other skeletal damage and to be below AIS 1. They will be replaced in future by values from a research more specific for collaborative robots.

^c The multiplier value for transient contact has been derived based on studies which show that transient limit values can be at least twice as great as quasi-static values for force and pressure. For study details, see References [2], [3], [4] and [2].

^d Critical zone (*italicized*)

Figura 12 - Limiti di forza e pressione biomeccanici

Allo scopo di ottenere una valutazione accurata dello scenario di un contatto durante la valutazione dei rischi, devono essere valutati sia i valori di forza che quelli di pressione. Ad esempio, nel caso in cui l'arto è bloccato tra le parti moventi del robot, una misura di pressione è più rilevante rispetto ad una di forza; perciò, verrà valutata come soglia limite quella di pressione. Al contrario, se l'impatto avviene su superfici ampia area (ad esempio l'addome) e non ci sono parti intrappolate, la misura preponderante sarà quella di forza.

Se il task collaborativo permette il contatto tra operatore e robot, è possibile effettuare una valutazione dei rischi che tiene conto di questo fattore. In particolare, se l'area di contatto e la parte del corpo sono noti, il valore di energia trasmesso può essere modificato adattando la velocità del robot nel punto di contatto. Per descrivere tale scenario, consideriamo un modello a due corpi, nel quale identifichiamo con m_R la massa del robot, la quale si muove per andare in contatto con la regione in esame del corpo m_H ad una velocità v_{rel} , attraverso una regione bidimensionale di contatto A , risultando in un urto completamente anelastico, il quale corrisponde alla situazione peggiore.

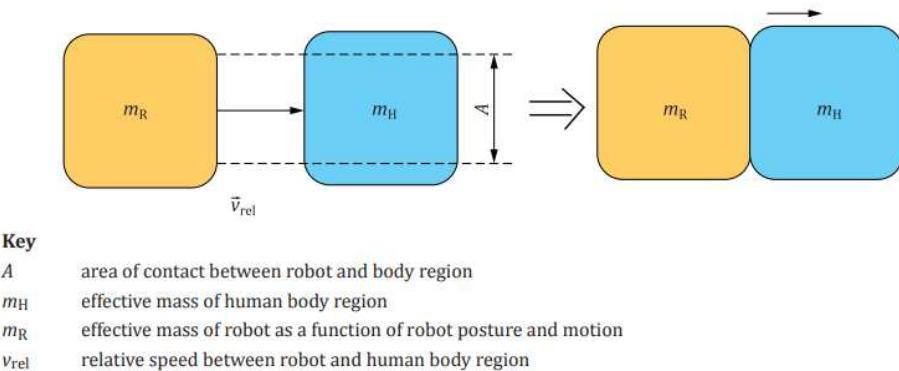


Figura 13 - Modello per contatti transienti

Body region	Effective spring constant	Effective mass
	K N/mm	m_H kg
Skull and forehead	150	4,4
Face	75	4,4
Neck	50	1,2
Back and shoulders	35	40
Chest	25	40
Abdomen	10	40
Pelvis	25	40
Upper arms and elbow joints	30	3
Lower arms and wrist joints	40	2
Hands and fingers	75	0,6
Thighs and knees	50	75
Lower legs	60	75

NOTE Mass values for thighs, knees and lower legs are set to the full body weight, since these body parts are not free to recoil or retract from impact while the operator is standing.

For each body region, the maximum permissible energy transfer can be calculated as a function of the maximum force or maximum pressure values shown in [Table A.2](#) using Formula (A.1):

Figura 14 - Masse e costanti elastiche effettive per il corpo umano

Per ogni regione del corpo, il massimo trasferimento di energia permesso può essere calcolato come funzione della forza massima o pressione massima mostrati in figura 12 utilizzando la formula:

$$E = \frac{F_{max}^2}{2k} = \frac{A^2 p_{max}^2}{2k} \quad (7)$$

Dove

E è l'energia trasferita

F_{max} è la massima forza di contatto per la specifica regione del corpo

p_{max} è la massima pressione di contatto per la specifica regione del corpo

A è l'area di contatto tra il robot e la regione del corpo

Una volta stabilito il limite di energia trasferibile durante il contatto, tale valore può essere utilizzato per identificare la velocità massima permessa al robot nello spazio collaborativo, mantenendo i valori di forza e pressione sotto ai limiti preposti in caso di contatto con l'operatore. L'assunzione che porta alla derivazione dei limiti di velocità per il contatto è quella di equiparare l'energia elastica del corpo umano alla totale energia cinetica nel centro di massa, assumendo un urto completamente anelastico. L'energia in tale modello è espressa dalla seguente formula:

$$E = \frac{F^2}{2k} = \frac{1}{2} \mu v_{rel}^2 \quad (8)$$

Dove

v_{rel} è la velocità relativa tra il robot e la regione del corpo umano in esame

μ è la massa ridotta del sistema a due corpi, espresso dalla formula

$$\mu = \left(\frac{1}{m_H} + \frac{1}{m_R} \right)^{-1} \quad (9)$$

Dove

m_H è la massa effettiva della regione del corpo in esame

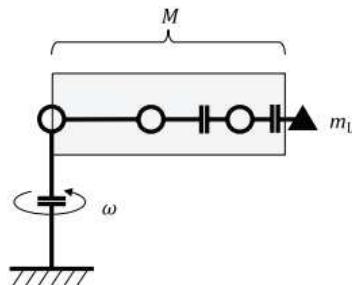
m_R è la massa effettiva del robot in funzione della postura e del suo moto, espressa dalla formula

$$m_R = \frac{M}{2} + m_L \quad (10)$$

Con

m_L è la massa effettiva del carico del sistema robotico, che include l'end effector e il pezzo di lavoro

M è la massa totale delle parti moventi del robot in esame



Key

m_L	effective payload of robot system
M	total mass of moving parts of robot
ω	rotational speed

Figure A.3 — Simplified mass distribution model

Figura 15 - Modello semplificato della distribuzione di massa

Risolvendo la formula

$$v_{rel,max} = \frac{F_{max}}{\sqrt{\mu k}} = \frac{p_{max}A}{\sqrt{\mu k}} \quad (11)$$

Confronto e differenze tra i vari standard

È necessario confrontare gli standard relativi ai settori automotive e robotico per comprendere analogie, differenze e potenziali sinergie tra normative come la ISO 26262, sviluppata per l'automotive, e le ISO 10218 e ISO/TS 15066, specifiche per la robotica industriale e collaborativa. Analizzare analogie e differenze tra tali normative consente di individuare approcci complementari e possibili sinergie, utili per trasferire buone pratiche tra settori ad alta criticità.

1. Focus e ambito degli standard

- ISO 26262: Si concentra specificamente sulla sicurezza funzionale dei sistemi elettrici/elettronici (E/E) nei veicoli stradali, con particolare

attenzione ai guasti sistematici e randomici. È altamente dettagliato per affrontare i rischi derivanti da malfunzionamenti tecnologici durante l'uso del veicolo.

- ISO 13482: Copre la sicurezza dei robot di assistenza personale, con un focus principale sui rischi derivanti dall'interazione tra il robot e gli esseri umani, come contatti accidentali o movimenti imprevisti.
- ISO 10218: È focalizzato sui robot industriali e si occupa principalmente della sicurezza durante l'interazione uomo-robot in ambienti industriali, concentrandosi su misure di progettazione, integrazione e uso sicuro.
- ISO/TS 15066: Integra l'ISO 10218 per i robot collaborativi, fornendo linee guida per valutare i limiti di forza e pressione durante le interazioni dirette tra robot e operatori umani.

2. Livello di dettaglio

- ISO 26262:
 - Altamente strutturato e dettagliato, con 12 parti che coprono l'intero ciclo di vita del prodotto, dalla concept phase alla dismissione.
 - Fornisce linee guida dettagliate per l'analisi dei rischi (Hazard Analysis and Risk Assessment, HARA) e per la determinazione dei livelli di integrità della sicurezza (Automotive Safety Integrity Levels, ASIL).
 - Include strumenti per la gestione del rischio, come la classificazione dei guasti (single-point vs. multi-point) e l'allocazione di requisiti di sicurezza ai componenti.
 - Specifica processi per garantire la verifica e la validazione approfondite, come test statici, dinamici e analisi dei guasti.
- ISO 13482, ISO 10218, ISO/TS 15066:
 - Meno dettagliati rispetto all'ISO 26262 e più orientati a fornire linee guida generali sulla progettazione sicura e sulla prevenzione dei rischi fisici.
 - Non forniscono metodologie esaustive per l'analisi dei rischi o criteri specifici per la classificazione della sicurezza.

- Spesso si limitano a stabilire requisiti base, come i limiti di forza e pressione (ISO/TS 15066) o i criteri di progettazione per evitare collisioni e malfunzionamenti (ISO 10218).

3. Approccio al rischio e alla safety

- ISO 26262:
 - Approccio basato sulla gestione dei rischi legati a malfunzionamenti tecnologici.
 - Prevede una classificazione rigorosa dei pericoli secondo l'ASIL, che considera severità, esposizione e controllabilità.
 - Promuove l'integrazione di misure di sicurezza tecniche e organizzative in tutte le fasi di sviluppo.
- ISO 13482, ISO 10218, ISO/TS 15066:
 - Focalizzati su rischi meccanici e fisici derivanti dall'interazione tra macchina e uomo.
 - Meno orientati ai guasti sistematici e casuali e più focalizzati sul design e sull'ergonomia per minimizzare il rischio di incidenti.
 - Non adottano un sistema equivalente all'ASIL, ma pongono maggiore enfasi sull'uso sicuro del prodotto attraverso istruzioni e limiti fisici.

4. Specificità delle linee guida

- ISO 26262:
 - Offre descrizioni specifiche e strumenti dettagliati per ogni fase del ciclo di vita, come modelli di sviluppo (V-model), tecniche di analisi dei guasti (FMEA, FTA) e requisiti per il software, hardware e sistemi integrati.
 - Include linee guida per i fornitori e la gestione della configurazione, evidenziando la necessità di una tracciabilità rigorosa.
 - Richiede processi documentati per dimostrare la conformità.

- ISO 13482, ISO 10218, ISO/TS 15066:
 - Forniscono linee guida più generali, ad esempio indicazioni sulla progettazione del robot per limitare i rischi di collisioni o specifiche sui limiti di forza/pressione nelle interazioni uomo-robot.
 - Non entrano nei dettagli della progettazione del software o dell'analisi di guasti elettronici, lasciando questi aspetti a standard più specifici (es. IEC 61508).

5. Conformità e implementazione

- ISO 26262:
 - La conformità richiede un'ampia documentazione e prove oggettive dell'applicazione dei requisiti durante tutte le fasi.
 - È uno standard obbligatorio di fatto nell'industria automobilistica per i sistemi E/E, dato il livello di rischio associato.
- ISO 13482, ISO 10218, ISO/TS 15066:
 - Richiedono valutazioni meno rigorose e sono orientati più alla prevenzione di comportamenti pericolosi che all'analisi dettagliata del guasto.
 - Maggiore flessibilità nella loro applicazione, con meno requisiti documentali.

In definitiva, la normativa ISO 26262 è più dettagliata e specifica rispetto agli standard ISO 13482, ISO 10218 e ISO/TS 15066. Questo perché si rivolge a un contesto ad alto rischio, dove i malfunzionamenti di sistemi complessi possono avere conseguenze gravi. Gli standard per la robotica, invece, si concentrano principalmente sulla prevenzione dei rischi fisici nelle interazioni uomo-macchina, con un approccio meno analitico e strutturato.

Sensor Faults

I sensori, ampiamente utilizzati per l'acquisizione di segnali, sono spesso posti in luoghi soggetti ad azioni atmosferiche o ambientali non ideali per le normali condizioni di funzionamento (alte temperature, applicazioni subacquee, etc.), le quali rendono tali sensori soggetti a possibili malfunzionamenti o danneggiamenti che vanno ad affliggere la precisione, la stabilità e l'affidabilità di un sistema. Nel caso di errore nel sensore, le performance del sistema possono degradare, e portare a conseguenze catastrofiche; a tal proposito, l'identificazione preventiva dei malfunzionamenti assume un importante ruolo nell'assicurare la precisione e l'affidabilità dei dati.

Un malfunzionamento del sensore [12] [13] [14] indica una parziale o totale perdita di funzionalità, e l'uso prolungato di dati incorretti può portare a seri problemi ai sistemi che si basano sull'informazione fornita da tali sensori. Di seguito sono classificati i principali malfunzionamenti legati ai sensori.

TIPOLOGIA DI MALFUNZIONAMENTO	DESCRIZIONE
Incipient Failure	Stato anormale o instabile, tale che i sensori continuano a funzionare ma il dato risulta incorretto. Il grado di errore aumenta sul lungo periodo.
Sensor Bias	Tra i più comuni malfunzionamenti relativi ai sensori, nei quali si registra un valore costante al posto del dato fornito dal sensore.
Sensor Drift	Offset tempo-variante, le performance deviano dalla formula originale di calibrazione, ed il valore di offset o di gain cambia nel tempo.
Sensor Gain Fault	Il rateo di variazione del dato misurato su un tempo esteso non rispetta le specifiche.
Abrupt Failure	Causato da danni fisici al sistema sensoristico, il quale smette di funzionare improvvisamente.
Sensor Noise	Disturbi interni, disturbi hardware, e disturbi ambientali. Alti valori di noise possono causare problemi ai segnali.
Corto circuito o circuito aperto	Contatti e connessioni approssimative causano corto circuiti, mentre disconnessioni della linea di trasmissione del segnale portano a circuiti aperti.
Random Faults	A causa di layout ambientali complessi, i sensori presentano occasionalmente dei malfunzionamenti randomici.

Tabella 1 – Tipologie di malfunzionamenti ai sensori

Negli ultimi anni lo sviluppo di nuove tecnologie di diagnosi dei malfunzionamenti ha portato all'implementazione di diverse tecniche di individuazione dei fault. Il concetto di ridondanza è uno dei più utilizzati tra i metodi di fault diagnosis: tale può essere divisa in due categorie, quali ridondanza hardware e ridondanza analitica. La prima fa riferimento all'utilizzo di più sensori per la misurazione dello stesso segnale: una combinazione lineare delle misure fornita da sensori ridondanti è utilizzata per ottenere delle stime, ed ogni misura è comparata a sua volta ad una stima per determinare un eventuale malfunzionamento. La ridondanza analitica non richiede hardware aggiuntivo ed è spesso più economica rispetto ai metodi di ridondanza hardware. I processi di diagnosi dei malfunzionamenti consistono in tre parti: rilevamento, identificazione e stima: la prima verifica che il sensore operi nei normali range di misurazione, la seconda serve a identificare la natura o la sorgente di eventuali malfunzionamenti, infine la terza indica la gravità del malfunzionamento, determinando se il sensore può continuare ad operare temporaneamente o se è necessario un intervento urgente.

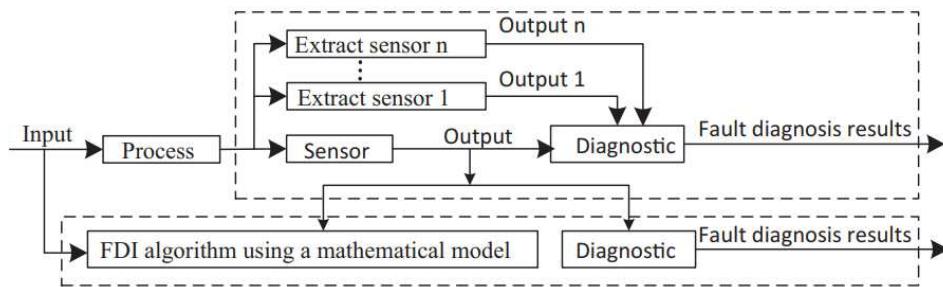


Figura 16 - Concetti di hard redundancy e analytical redundancy

Di seguito sono riportati i principali metodi di rilevazione dei malfunzionamenti:

METODOLOGIA DI RILEVAZIONE	DESCRIZIONE
Model-based	Utilizza modelli dinamici per confrontare segnali misurati e stimati, generando un residuo valutato per individuare malfunzionamenti. Alcuni approcci modellano anche non linearità, ma l'implementazione real-time è complessa.
Knowledge-based	Basato su sistemi esperti e conoscenza pregressa, senza richiedere un modello matematico. Usa dati storici e inferenze logiche per diagnosticare fault. È adattabile e tollerante ai guasti.
Ruled-based intelligent system	Si fonda su regole derivate da esperti. Intuitivo e flessibile per sistemi di piccola scala, ma poco scalabile. Non rileva guasti sconosciuti se non precedentemente documentati.
Sistemi intelligenti basati su logica fuzzy	Gestisce incertezza e inaccuratezza nei dati. Consente decisioni razionali dove la logica tradizionale fallisce. Migliora i limiti dei sistemi basati su regole esperte.
Approcci data-driven	Non richiede un modello matematico. Analizza grandi quantità di dati per rilevare pattern e anomalie. Si basa su pattern recognition e classificatori addestrati.

Reti neurali	Algoritmi che simulano il cervello umano per identificare fault tramite estrazione automatica delle feature. Adatti per sistemi non lineari e complessi.
Support Vector Machines (SVM)	Classificatore basato su campioni limitati. Rileva deviazioni dal funzionamento normale dei sensori. Offre performance superiori rispetto ai classificatori tradizionali.
Deep Learning	Variante avanzata delle reti neurali. Automatizza l'estrazione delle feature e gestisce funzioni complesse, migliorando l'accuratezza nella diagnosi dei guasti.

Tabella 2 – Metodi di rilevazione dei malfunzionamenti ai sensori

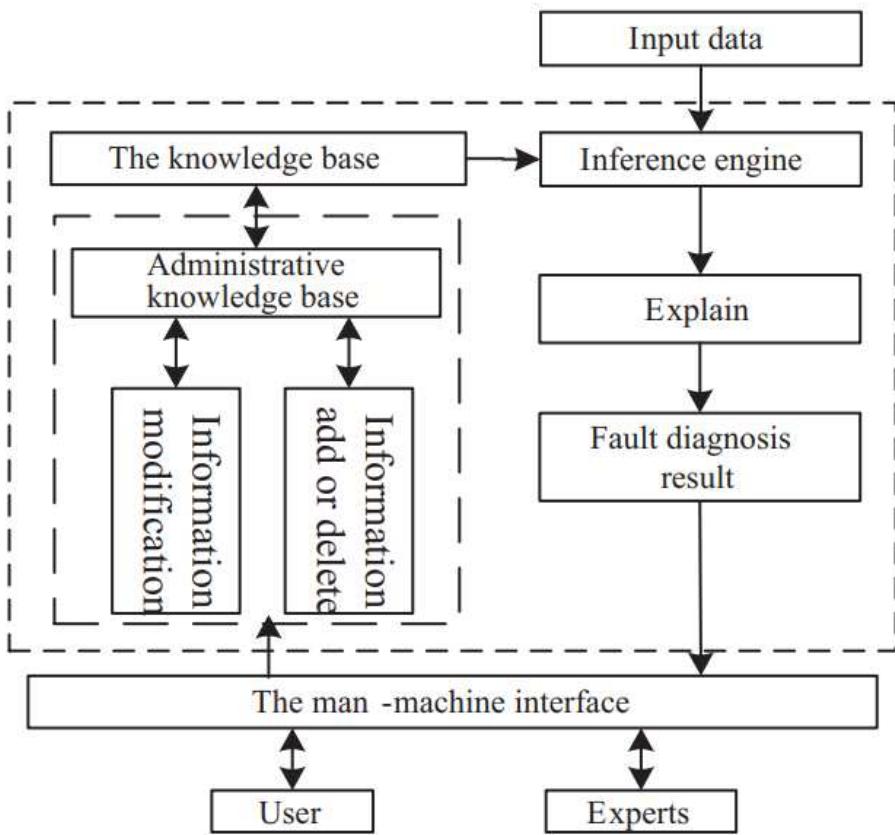


Fig. 3. The structure of expert systems for sensor fault detection.

Figura 17 - Struttura di sistemi esperti per la rilevazione dei fault ai sensori

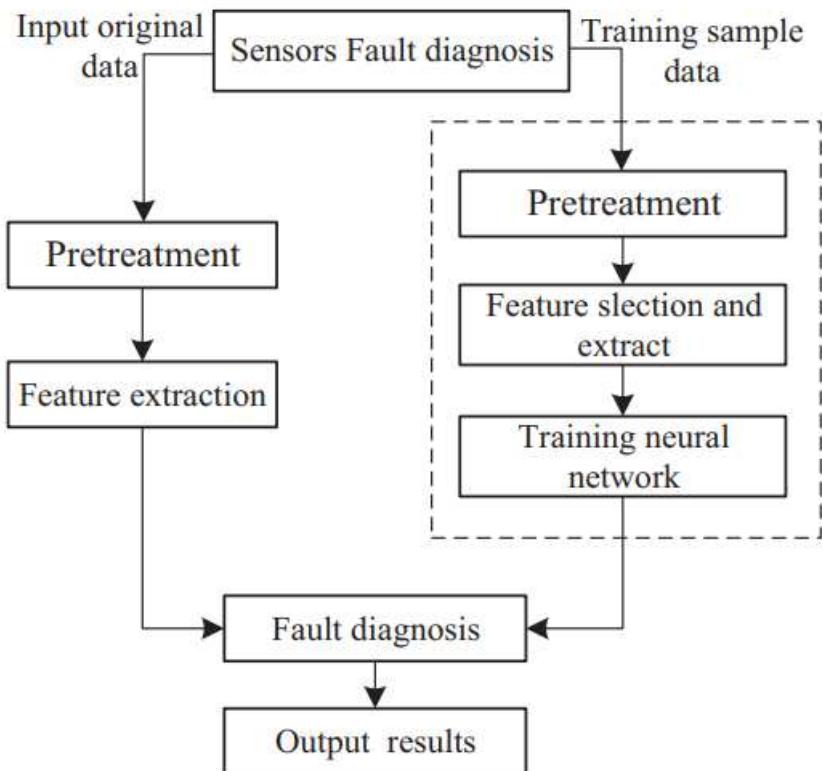


Figura 18 - Rilevazione sensor fault tramite reti neurali

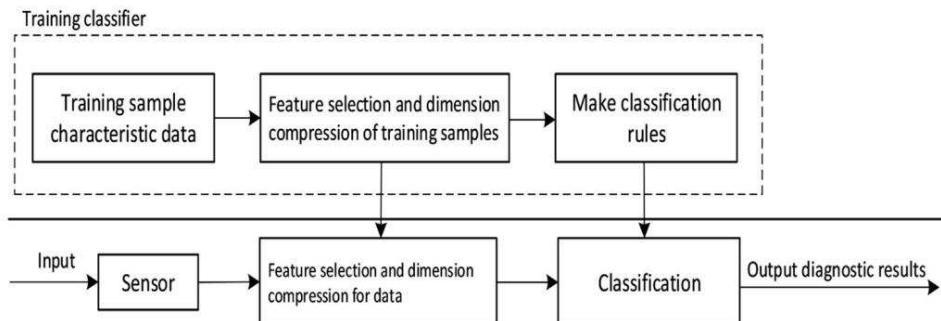


Figura 19 - Diagnosi dei fault tramite SVM

Per quanto concerne l'identificazione, essa determina la dimensione e la tempo-varianza della natura dei malfunzionamenti analizzando le caratteristiche della risposta in termini di ampiezza, fase, spettro, etc. Di seguito sono elencate le principali metodologie di identificazione del malfunzionamento:

METODOLOGIA DI IDENTIFICAZIONE	DESCRIZIONE
Principal Component Analysis (PCA)	Tecnica statistica per ridurre la dimensionalità dei dati, evidenziando le tendenze principali. Ampiamente usata per identificare pattern legati a malfunzionamenti.
Wavelet Transform	Analizza segnali nel dominio del tempo e della frequenza. Adatta a segnali non stazionari. La decomposizione wavelet permette di localizzare fault con precisione. Può essere continua (per distinguere errori/disturbi) o discreta (per analisi in frequenza).
Stima dei parametri	Utilizza modelli matematici per stimare online i parametri fisici del sensore. Il malfunzionamento è rilevato quando i parametri stimati escono da un intervallo sicuro. È meno stabile e preciso nei sistemi non lineari.
Stima dello stato	Basata su osservatori di stato (filtri). Confronta output misurati e stimati per identificare i fault. Utilizzata anche per la stima del rumore e la ricostruzione di segnali.
Approccio ibrido alla diagnosi	Combina più tecniche (identificazione, stima, rilevazione) per ottenere una diagnosi più robusta, rapida ed efficace, compensando i limiti dei singoli approcci.

Tabella 3 – Metodi di identificazione dei malfunzionamenti ai sensori

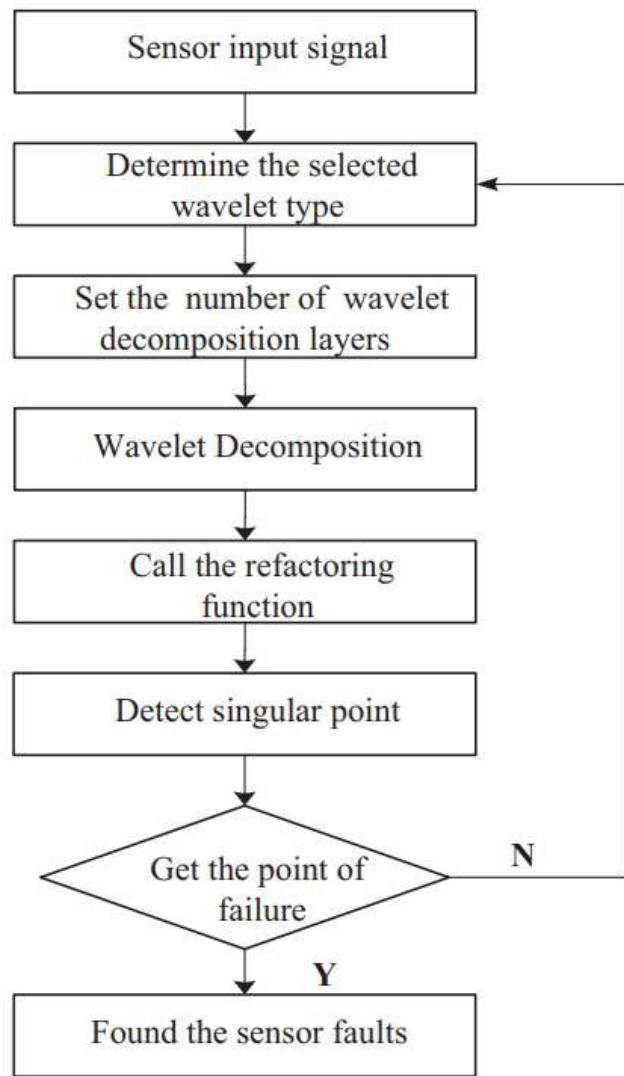


Figura 20 - Localizzazione dei fault ai sensori tramite wavelet transform

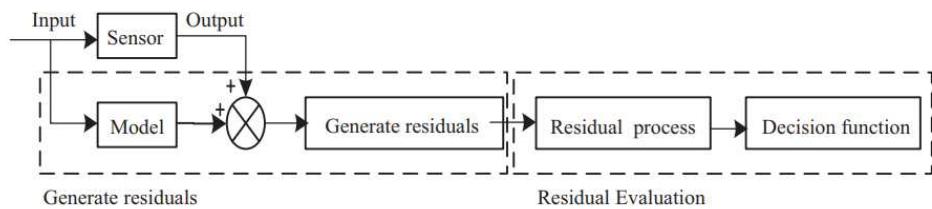


Figura 21 - Processo di stima dei fault ai sensori

Actuator Faults

Non solo i sensori possono essere soggetti a malfunzionamenti, ma anche gli attuatori [16] [17] [18]: in molte applicazioni, i requisiti di sicurezza richiedono l'uso di sensori e attuatori tolleranti ai malfunzionamenti. Per mantenere il costo totale di un sistema il più basso possibile, solo le componenti che potrebbero essere soggette a malfunzionamenti più facilmente devono essere ridondanti. A seguito di un rilevamento del guasto, è possibile eseguire una delle seguenti operazioni:

- Riconfigurazione: rappresenta la metodologia più completa da attuare in caso di fault. L'utilizzo di ridondanza analitica permette la ricostruzione di una misura di un sensore difettato attraverso un modello analitico descrittivo delle dinamiche del processo, le quali prevedono l'utilizzo di misure fornite da altri sensori funzionanti.
- Cambio operativo o riconfigurazione del controllore: il controllore può essere riconfigurato, cambiandone i parametri o la struttura, ad esempio rendendolo più robusto alle incertezze di sistema. Tale metodo non permette di gestire contemporaneamente più fault, perciò andrebbe abbinato a ridondanza analitica o hardware.
- Stop delle operazioni: se il malfunzionamento dovesse risultare troppo importante, successive operazioni potrebbero non essere possibili e il sistema deve essere fermato, poiché un proseguimento dei processi potrebbe portare a guasti permanenti.
- Riparo/manutenzione: in aggiunta o a sostituzione delle azioni precedenti, la riparazione deve essere effettuata per portare il sistema alla sua completa funzionalità.

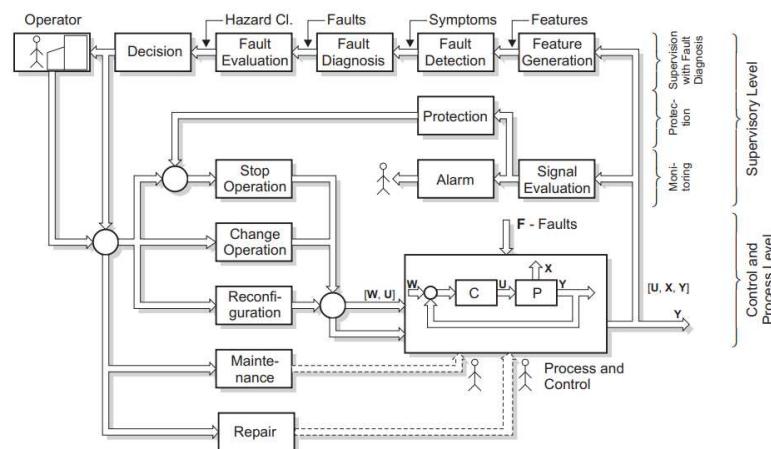


Figura 22 - Schema di sistema di gestione integrato dei fault

Capitolo III – Caso di studio

Descrizione del caso di studio

Le fasi di lavoro previste seguono una struttura metodologica ben definita. Dopo un'approfondita ricerca bibliografica sugli aspetti legati alla robotica collaborativa, alla sicurezza funzionale e alle tecniche di analisi dei guasti, si procede con l'individuazione del caso di studio, consistente in un'operazione collaborativa tra uomo e macchina da realizzare tramite inseguimento di traiettoria da parte del manipolatore. Una volta definito il compito e scelto il robot, si passa all'analisi delle possibili condizioni di fault che possono compromettere il raggiungimento dell'obiettivo o rappresentare un rischio per la sicurezza dell'operatore: ad esempio, eventuali malfunzionamenti alle componenti del sistema robotico possono portare ad urti con un operatore o con l'ambiente, rendendo le operazioni in questione non sicure. Vengono quindi individuate le componenti critiche del sistema soggette a malfunzionamenti, con particolare attenzione ai sensori, agli attuatori e alle componenti hardware e software del sistema di controllo. L'ultima fase del lavoro è dedicata allo sviluppo e alla valutazione di metodologie di rilevamento dei fault e di strategie di intervento che, in risposta a condizioni anomale, garantiscano la continuità operativa del sistema in condizioni sicure o conducano il robot in uno stato sicuro arrestando l'attività.

Il caso di studio è stato individuato con l'obiettivo di sviluppare, testare e validare un sistema di controllo avanzato, integrando le considerazioni sulla sicurezza funzionale e sull'interazione uomo-robot discusse nei paragrafi precedenti. La scelta è ricaduta sul manipolatore CRS-A255, messo a disposizione dal laboratorio di robotica del Dipartimento di Ingegneria Elettrica e dell'Informazione (DEI) del Politecnico di Bari, in quanto rappresenta una piattaforma ideale per attività sperimentali sia in ambiente reale sia in simulazione. Si tratta infatti di un robot ad architettura aperta, che consente un accesso diretto alla struttura di controllo, facilitando l'implementazione e la modifica di strategie avanzate. Inoltre, grazie alla sua configurazione e alla possibilità di montare diversi end-effector, il manipolatore si presta a simulare compiti collaborativi che coinvolgono l'interazione con un operatore umano. Un ulteriore aspetto rilevante è la possibilità di iniettare fault sui giunti e sulle componenti del sistema, rendendolo uno strumento adatto per l'analisi degli effetti dei guasti e la verifica dell'efficacia delle contromisure di sicurezza progettate.

Il manipolatore industriale a catena cinematica aperta, prodotto dalla *Thermo Scientific Catalyst Express*, è caratterizzato da un design robusto che permette un posizionamento senza errori all'interno dello spazio di lavoro. Esso presenta cinque gradi di libertà rotazionali ed altrettanti motori a corrente continua a magneti permanenti permettono il movimento dei giunti. L'accoppiamento tra motori e giunti non è diretto, ma realizzato mediante organi di trasmissione del moto quali ruote dentate e catene: tale dettaglio influisce notevolmente sulla dinamica del manipolatore, specialmente in caso in presenza di elevati rapporti di trasmissione. Sull'albero di ciascun motore sono calettati un freno elettromagnetico ed un encoder che provvede alla misura e trasduzione della posizione del giunto corrispondente. Gli organi terminali che possono essere montati sul *tool flange* di un robot industriale sono diversi tra loro e variano in base al compito che si vuole realizzare con l'ausilio del manipolatore. Nel banco utilizzato, il robot A 255 è stato dotato di un servo gripper che conferisce al manipolatore la capacità di afferrare gli oggetti. Il controllore C500 è lo strumento proposto al controllo del manipolatore ed è composto da tre parti fondamentali: il microcontrollore, i convertitori di potenza e le protezioni da sovraccorrenti.

In ambito industriale le varie parti di un controllore sono inaccessibili dall'esterno, di modo che l'unica tecnica di controllo possibile è quella implementata sul microcontrollore, che a sua volta pilota i convertitori di potenza. In questo caso si parla di controllo in architettura chiusa. Grazie alla presenza del controllore, l'utente non è tenuto ad elaborare un proprio algoritmo di controllo o di generazione puntuale della traiettoria, e questo rende l'utilizzo del robot in architettura chiusa piuttosto semplice ed immediato. Le tecniche che consentono di inviare comandi al robot, rimanendo in architettura chiusa, sono due: utilizzando il *teach pendant* o tramite un software di interfaccia installato su PC. L'interfacciamento tra il controllore e il PC è realizzato mediante una porta seriale. Ovviamente, la scelta tra questi differenti modi per utilizzare il robot è strettamente legata al tipo di applicazione che si intende realizzare. Nel primo caso si utilizza una tastiera portatile collegata al controller C500, il *teach pendant* appunto, con cui è possibile comandare al robot semplici operazioni quali movimenti dei giunti e dell'end-effector, set della velocità, ecc. Tali operazioni sono efficaci nel caso in cui si vogliano far compiere al manipolatore operazioni non particolarmente complicate.

Nel caso in cui si vogliano far compiere al manipolatore compiti più complessi, è necessario adottare una tecnica di controllo diversa che prevede

l'utilizzo di un PC. Per definire i compiti che il robot deve eseguire via PC si utilizza il software Robcomm, il quale permette di interfacciare il PC direttamente con il microcontrollore presente nel manipolatore. La programmazione del robot è realizzata ad alto livello utilizzando il linguaggio di programmazione RAPL3, orientato specificamente alla programmazione di manipolatori industriali. Il task, quindi, per essere eseguito, viene prima scomposto in una serie di operazioni elementari e successivamente viene tradotto in RAPL3. A questo punto Robcomm rende semplice ed immediata la fase di compilazione e di download del file sorgente in RAPL3 sul microcontrollore, svincolando l'utente dalla gestione dell'hardware del microcontrollore stesso.

Il controllo in architettura chiusa ha il grosso pregio di rendere piuttosto semplice l'utilizzo del robot e l'assegnazione dei movimenti al manipolatore: tuttavia, non consente di implementare un diverso algoritmo di controllo, di realizzare la pianificazione della traiettoria, di aggiungere e gestire ulteriori sensori, come ad esempio telecamere o sensori di forza.

Alla luce di tali considerazioni, è evidente come il controllo in architettura chiusa, sebbene semplice e sicuro, è in alcuni aspetti limitante. In alternativa al controllo in architettura chiusa, si può praticare un controllo in architettura aperta, il quale lascia ampio potere decisionale all'utente che può progettare il sistema di controllo e pilotare direttamente i convertitori di potenza mediante una scheda di interfacciamento per generare magari una traiettoria relativa ad un determinato task. Un grande vantaggio del controllo in architettura aperta consiste nel poter sfruttare al meglio le potenzialità del robot, migliorando il controllo implementato nel controllore, modificando gli algoritmi per l'inversione cinematica e di generazione della traiettoria. Al fine di realizzare il controllo in architettura aperta, il controllore C500 è dotato di una scheda di acquisizione prodotta dalla ditta canadese *Quanser* collegata al PC, che permette di prelevare i segnali provenienti dagli encoder ed eventualmente bypassare il controllo preesistente ed inviare, sempre via PC, i segnali di pilotaggio dei convertitori di potenza. La gestione dei segnali I/O tra scheda di acquisizione e PC è realizzata attraverso il software *WinCon*. Lo schema di controllo e la pianificazione della traiettoria sono implementati in ambiente MATLAB & Simulink, consentendo non solo di programmare ad alto livello il microcontrollore, ma anche di sfruttare tutte le potenzialità del software e dei suoi toolbox, nella definizione della parte di controllo, della gestione dei segnali provenienti dai sensori e nell'elaborazione dei dati.

Essendo i giunti rotoidali, le variabili di giunto associate sono le posizioni angolari $\theta_i(t)$ con $i = 1,2,3,4,5$ (per comodità si associa alla variabile

$\theta(t) = q(t)$) [19]. Indicando con $q_1(t), q_2(t), q_3(t), q_4(t), q_5(t)$ le posizioni angolari dei giunti, si devono rispettare i vincoli meccanici rispetto alla posizione di ready, ovvero la posizione di riferimento dei giunti:

$$-179^\circ < q_1(t) < 179^\circ$$

$$-90^\circ < q_2(t) < 20^\circ$$

$$-20^\circ < q_3(t) < 90^\circ$$

$$-90^\circ < q_4(t) < 90^\circ$$

$$-179^\circ < q_5(t) < 179^\circ$$

Cinematica del manipolatore

Al fine di calcolare l'equazione cinematica diretta per il manipolatore CRS-A255, è necessario utilizzare un metodo generale e sistematico per definire posizione ed orientamento di due bracci consecutivi. Infatti, attraverso la convenzione di Denavit-Hartenberg (DH) [20], è possibile fissare l'orientamento e la posizione dei sistemi di riferimento fissi di ciascun braccio, che costituisce la struttura del manipolatore, seguendo alcune semplici regole.

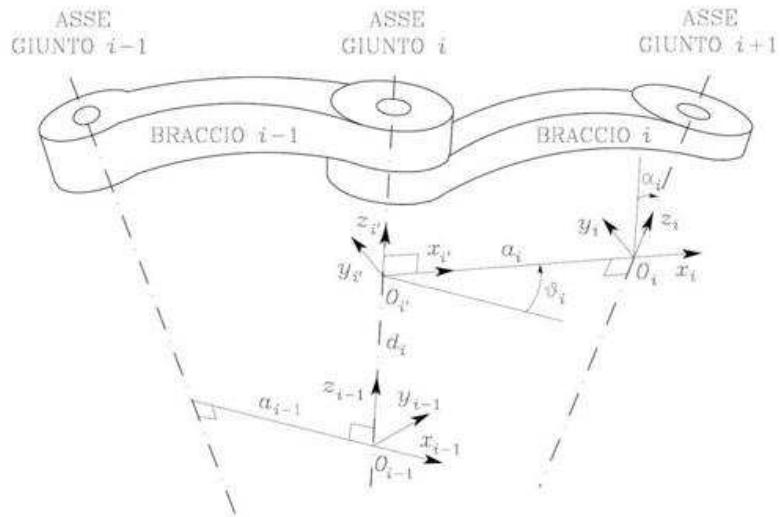


Figura 23 - Parametri cinematici di Denavit-Hartenberg

Una volta determinate le terne solidale a ciascun braccio, risulta che la posizione e l'orientamento della terna i rispetto alla terna $i - 1$ sono esprimibili in funzione dei parametri di DH.

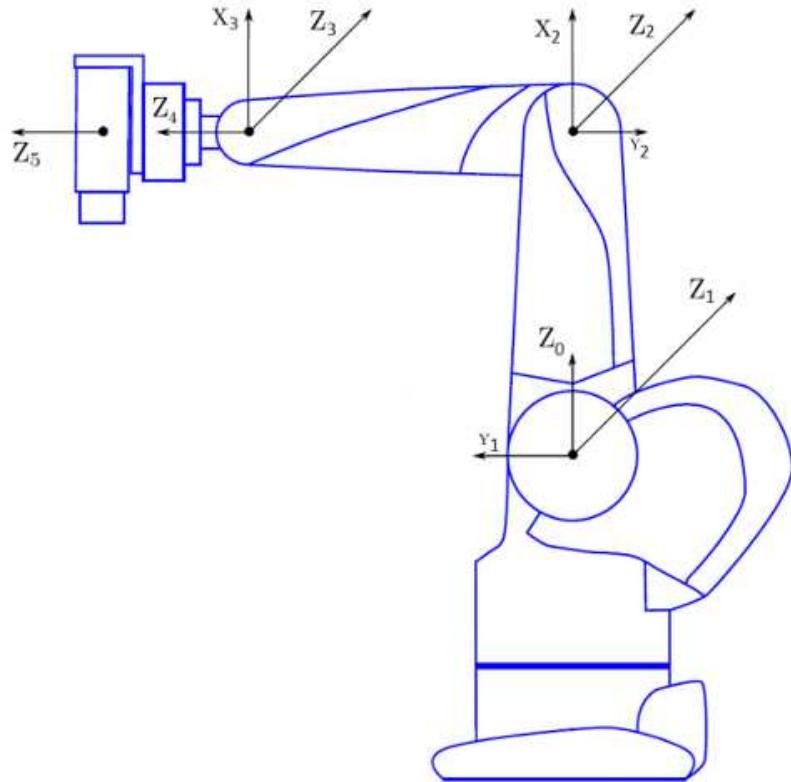


Figura 24 - Sistema di riferimento secondo la convenzione D-H

In ogni caso la convenzione DH non fornisce una definizione univoca della terna, l'indeterminazione può essere sfruttata per semplificare la procedura ricercando, ad esempio, condizioni di allineamento tra assi delle terne consecutive. A seguito della scelta della convenzione di DH, è possibile ricavare la tabella dei parametri per il manipolatore.

Braccio	a_i [mm]	α_i [rad]	d_i [mm]	θ_i [rad]
1	0	$\frac{\pi}{2}$	0	θ_1
2	255	0	0	θ_2
3	255	0	0	θ_3
4	0	$\frac{\pi}{2}$	0	θ_4
5	0	0	150	θ_5

Tabella 4 - Parametri Denavit-Hartenberg CRS A255

A questo punto si è in grado di esprimere la trasformazione di coordinate che lega la terna i alla terna $i - 1$, in funzione dei parametri di Denavit-Hartenberg; è possibile quindi ricavare la matrice di trasformazione finale che lega l'organo terminale con la terna base:

$$T_5^0(q) = A_1^0(q_1) * A_2^1(q_2) * A_3^2(q_3) * A_4^3(q_4) * A_5^4(q_5) = \\ = \begin{bmatrix} t_{11} & t_{12} & t_{13} & p_x \\ t_{21} & t_{22} & t_{23} & p_y \\ t_{31} & t_{32} & t_{33} & p_z \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

In cui gli elementi della matrice rotazionale sono:

$$\begin{aligned} t_{11} &= s_1 s_5 + c_{234} c_1 c_5 & t_{21} &= c_{234} c_5 s_1 - c_1 s_5 & t_{31} &= s_{234} c_5 \\ t_{12} &= c_5 s_1 - c_{234} c_1 c_5 & t_{22} &= -c_1 c_5 - c_{234} s_1 s_5 & t_{32} &= -s_{234} s_5 \\ t_{13} &= s_{234} c_1 & t_{23} &= s_{234} s_1 & t_{33} &= -c_{234} \end{aligned}$$

Mentre gli elementi rispetto alla traslazione sono:

$$\begin{aligned} p_x &= c_1 (a_3 c_{23} + a_2 c_2 + d_5 s_{234}) \\ p_y &= s_1 (a_3 c_{23} + a_2 c_2 + d_5 s_{234}) \\ p_z &= a_3 s_{23} + a_2 s_2 - d_5 c_{234} \end{aligned}$$

Dinamica del manipolatore

Il modello dinamico del manipolatore fornisce una descrizione delle relazioni esistenti tra le coppie di attuazione ai giunti e il moto della struttura. Determinare il modello dinamico del manipolatore è estremamente importante in quanto esso è indispensabile per la simulazione del moto,

l'analisi di strutture di manipolazione e per individuare algoritmi di controllo. Uno dei modelli utilizzati per derivare le equazioni del moto del manipolatore si basa sulla formulazione di Lagrange, che conduce alla derivazione del modello dinamico in forma chiusa. Tramite tale metodologia è possibile ricavare le equazioni del moto con un approccio indipendente dal sistema di coordinate di riferimento.

Si definisce Lagrangiana di un sistema meccanico la differenza tra l'energia cinetica T e quella potenziale U del sistema:

$$L = T - U \quad (12)$$

Stabilite le variabili di giunto, le equazioni di Lagrange possono essere espresse in questo modo:

$$\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{q}_i} \right) - \frac{\partial L}{\partial q_i} = \xi_i \quad \text{con } i = 1, 2, \dots, 5 \quad (13)$$

In cui ξ_i è la forza generalizzata associata alla coordinata generalizzata q_i . A queste forze generalizzate danno contributo le forze non conservative, ovvero le forze generate ai giunti dagli attuatori, le coppie di attrito ai giunti indotti da forze esplicate dall'organo terminale sull'ambiente in situazioni di contatto.

Note energia cinetica ed energia potenziale, è possibile ricondursi all'equazione del moto:

$$L(q, \dot{q}) = T(q, \dot{q}) - U(q) = \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n b_{ij}(q) \dot{q}_i \dot{q}_j - \sum_{i=1}^n (m_{li}[g_0]^T p_{li} + m_{mi}[g_0]^T p_{mi}) \quad (14)$$

Effettuando le operazioni di derivazione, si ottiene il nuovo sistema di equazioni:

$$\sum_{j=1}^n b_{ij}(q) \ddot{q}_j + \sum_{j=1}^n \sum_{k=1}^n h_{ijk}(q) \dot{q}_k \dot{q}_j + g_i(q) = \xi_i \quad i = 1, \dots, n \quad (15)$$

Il sistema ottenuto presenta tre differenti termini:

- Termini di accelerazione: b_{ii} contiene il momento di inerzia dall'asse del giunto i nella configurazione corrente, quando gli altri giunti sono bloccati, mentre i termini b_{ij} considerano gli effetti dell'accelerazione dei giunti j sul giunto i ;
- Termini quadrati di velocità, $h_{ijj}q_j^2$ rappresenta l'effetto centrifugo indotto al giunto i dalla velocità del giunto j . Si osservi che $h_{iii} = 0$ poiché $\frac{\partial b_{ii}}{\partial q_i} = 0$, mentre il termine $h_{iji}q_j h_{ijj} \dot{q}_k$ rappresenta l'effetto di Coriolis indotto al giunto i dalle velocità del giunto j e k ;
- Termini che dipendono dalla configurazione: $g_i(q)$ rappresenta le coppie generate all'asse del giunto i nella configurazione per l'effetto della gravità.

I termini al secondo membro sono invece le forze generalizzate associate e quindi contenenti il vettore delle coppie di attuazione ai giunti, coppie di attrito viscoso e di attrito statico e, infine, le coppie di bilanciamento causate dal contatto con l'ambiente esterno; così facendo si ottiene, riorganizzando l'equazione matematica:

$$B(q)\ddot{q} + C(q, \dot{q})\dot{q} + F_v\dot{q} + F_s sgn(\dot{q}) + g(q) = \tau - J^T(q)h_e \quad (16)$$

Controllo del manipolatore

Tra i diversi metodi di controllo di un manipolatore, è stato scelto un controllo a dinamica inversa nello spazio dei giunti; tale metodologia è particolarmente utile nel caso si voglia far inseguire al manipolatore una traiettoria prefissata, definendo anche velocità e accelerazioni nei vari punti intermedi. Questo approccio è basato sull'esatta linearizzazione del sistema attraverso un feedback non lineare del sistema.

Si considera l'equazione dinamica del sistema:

$$B(q)\ddot{q} + C(q, \dot{q})\dot{q} + F\dot{q} + g(q) = u \quad (17)$$

Definendo:

$$n(q, \dot{q}) = C(q, \dot{q})\dot{q} + F\dot{q} + g(q) \quad (18)$$

Viene scelto:

$$u = B(q)y + n(q, \dot{q}) \quad (19)$$

Sostituendo l'equazione (7) nella (5), si ottiene:

$$y = \ddot{q} \quad (20)$$

L'equazione (8) rappresenta un nuovo vettore di input per il sistema e tale schema di controllo ottenuto è equivalente ad un doppio integratore:

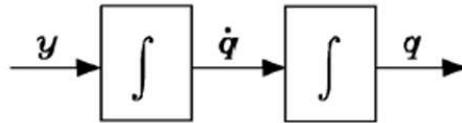


Figura 25 - Vettore di input del sistema

Scegliendo

$$y = -K_P q - K_D \dot{q} + \ddot{q}_d + K_P q_d + K_D \dot{q}_d \quad (21)$$

E definendo l'errore di posizione

$$\tilde{q} = q_d - q \quad (22)$$

Si ottiene:

$$\ddot{\tilde{q}} + K_D \dot{\tilde{q}} + K_P \tilde{q} = 0 \quad (23)$$

È stata quindi determinata la nuova equazione dinamica del sistema che descrive le dinamiche dell'errore di posizione rispetto alla traiettoria assegnata. K_D e K_P sono delle matrici diagonali determinate a partire dalle pulsazioni naturali desiderate e dai coefficienti di smorzamento:

$$K_P = \begin{bmatrix} \omega_{n1}^2 & 0 & \dots & 0 \\ 0 & \omega_{n2}^2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \omega_{nn}^2 \end{bmatrix} \quad K_D = \begin{bmatrix} 2\delta_1\omega_{n1} & 0 & \dots & 0 \\ 0 & 2\delta_2\omega_{n2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 2\delta_n\omega_{nn} \end{bmatrix}$$

Scegliendo opportunamente K_P e K_D è possibile ottenere la dinamica dell'errore del secondo ordine sottosmorzata e che tende asintoticamente a zero.

Lo schema di controllo ottenuto è di seguito riportato:

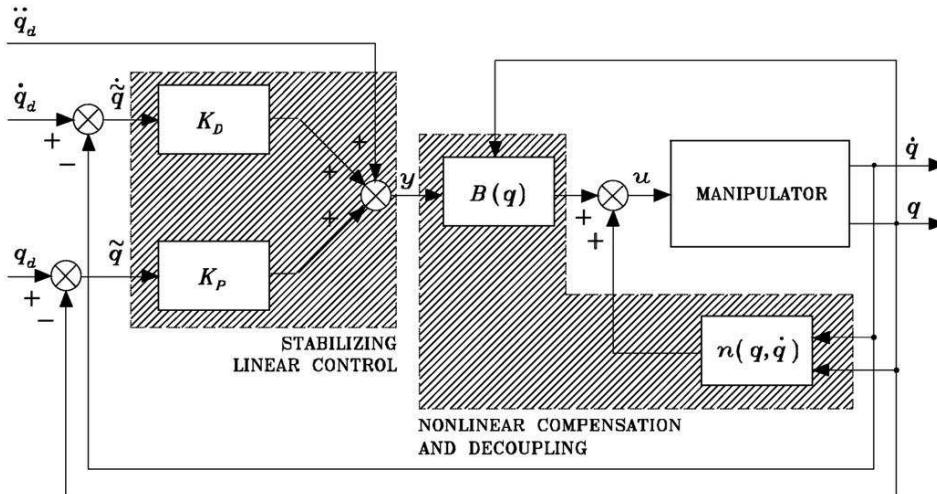


Figura 26 - Schema di controllo del manipolatore

La prima parte del diagramma a blocchi è quella che consente di stabilizzare l'azione di controllo lineare attraverso la scelta delle matrici K_P e K_D , mentre la seconda parte riguarda la compensazione non lineare ed il disaccoppiamento.

Ottenute quindi una descrizione del manipolatore, del suo modello cinematico e dinamico, e del sistema di controllo che vogliamo attuare, è necessario valutare, per il nostro caso di studio, dei possibili rischi associati ad un task collaborativo tra uomo e manipolatore, in quanto impattanti sulla sicurezza e sull'efficienza del sistema stesso, e sulle possibili metodologie per evitare o mitigare possibili danni all'uomo o alla macchina tramite interventi più o meno severi.

È possibile classificare le tipologie di fault che possono occorrere durante l'interazione uomo-manipolatore in base all'origine e all'impatto: tali possono essere:

- Meccanici (usura dei componenti come giunti, cuscinetti, trasmissioni, rotture strutturali come cedimenti di bracci o connessioni dovute a carichi eccessivi, imprecisioni cinematiche);
- Elettrici (interruzioni all'alimentazione, guasti ai sensori o agli attuatori, anomalie nei motori per via di surriscaldamenti o perdite di coppia);

- Software (bug o malfunzionamenti non previsti, errore nei modelli di calcolo per la pianificazione del movimento, problemi di comunicazione come ritardi o perdite dati tra manipolatore e sistema di controllo centrale);
- Ambientali (interferenze esterne come campi magnetici o vibrazioni che influenzano i sensori, condizioni ambientali avverse relative a temperatura, umidità, ecc.)
- Indotti dall'operatore (interazioni involontarie che causano collisioni o movimenti non sicuri, o mancate osservanze delle procedure di sicurezza).

Individuati i principali fattori di rischio, è necessario effettuare un risk assessment (analisi dei rischi), processo fondamentale per identificare, valutare e mitigare i potenziali pericoli associati ai task collaborativi. Gli standard ISO forniscono linee guida specifiche per garantire che i manipolatori collaborativi siano progettati e utilizzati in modo sicuro.

Tramite l'utilizzo di checklist e analisi storiche vengono identificati i pericoli potenziali, i quali vengono poi classificati in base alla loro origine. La valutazione dei rischi consiste invece nel determinare per primo l'impatto di un potenziale fault, stimare la probabilità di accadimento di tali fault, e infine considerare entrambi i fattori per definire il rischio totale. Nel processo di analisi dei rischi sono definite anche le modalità di mitigazione dei rischi, suddivise in misure tecniche (implementazione di sistemi di controllo ridondanti, sensori di sicurezza e algoritmi di rilevamento dei fault), misure procedurali (definizione di procedure operative standard e formazione degli operatori) e misure progettuali (ad esempio riduzione della velocità o dei carichi durante le interazioni uomo macchina).

Nel nostro caso d'esame verranno considerati dei malfunzionamenti critici in un sistema di questo tipo e che sono potenzialmente pericolosi sia per l'operatore umano che per la macchina e l'ambiente in cui lavora. In particolare, consideriamo tre tipi di malfunzionamenti:

- Fault sul segnale di controllo: il segnale di controllo nel nostro caso è costituito dai riferimenti di posizione, velocità e accelerazione, definiti lungo una traiettoria polinomiale di terzo grado polinomiale.

I fault su questo tipo di segnale possono includere disturbi o rumori, che alterano i riferimenti oppure offset e deriva dei segnali, caratterizzati da alterazioni sistematiche che portano il manipolatore fuori traiettoria. L'impatto di tali fault risulta in errori nei movimenti,

nella riduzione della precisione e in un aumento dei rischi di collisione.

- Fault sull'inverter: l'inverter si occupa di pilotare le tensioni ai motori che muovono i giunti rotoidali del manipolatore. Eventuali fault su tale componente possono includere perdita di fase (come una mancanza di alimentazione in una delle fasi), surriscaldamento (raggiungimento di temperature critiche che influenzano il normale funzionamento del componente) e guasti ai componenti elettrici (come transistor o circuiti di controllo). Tali fault possono portare ad un arresto improvviso dei motori, a movimenti non controllati e perdite di coppia.
- Fault sui sensori: essi monitorano la posizione e la corrente nei giunti. Tali fault possono includere errori di misurazione, risultanti in dati inaccurati sulla posizione dei giunti, o guasti totali, oppure rumore elevato e offset del segnale. Essi possono portare a difficoltà nel controllo di posizione e forza, con potenziali conseguenze sulla sicurezza e sulla precisione operativa.

I malfunzionamenti precedentemente evidenziati possono portare, in caso di collaborazione di un manipolatore con un operatore umano, a conseguenze più o meno gravi per l'incolumità sia del sistema sia dell'uomo. Un fault nei sensori di posizione o forza può causare un'errata percezione dello stato del robot, portando a movimenti imprevisti o a una mancata reazione in caso di contatto con l'operatore. Ad esempio, un sensore di forza difettoso potrebbe non rilevare correttamente un impatto, impedendo al sistema di attivare misure di sicurezza come l'arresto di emergenza. Guasti negli inverter dei motori, responsabili del controllo della velocità e della coppia, possono provocare accelerazioni o frenate improvvise e incontrollate, aumentando il rischio di collisioni. Inoltre, malfunzionamenti generici nel software di controllo o nelle unità di elaborazione possono portare a errori nei comandi inviati agli attuatori, causando traiettorie impreviste o perdite di controllo del manipolatore. La combinazione di questi fattori può mettere seriamente a rischio l'incolumità dell'operatore, rendendo essenziale l'implementazione di strategie di sicurezza come la ridondanza dei sensori, il monitoraggio continuo dei parametri critici e l'adozione di protocolli di arresto sicuro in caso di anomalie.

I fault che sono stati considerati per il caso di studio in questione prevedono malfunzionamenti agli inverter che pilotano le tensioni da applicare ai motori,

malfunzionamenti ai sensori di posizione dei giunti e malfunzionamenti ai segnali di trasmissione dei riferimenti al sistema di controllo. La scelta di queste tipologie di guasto è stata guidata da criteri di rilevanza e praticità: si tratta infatti di anomalie facilmente implementabili sia in ambiente simulato sia, con le dovute precauzioni, in previsione su un sistema fisico reale. Inoltre, tali fault rappresentano scenari realistici e ricorrenti nei contesti industriali, dove la continuità e l'affidabilità del controllo dipendono in larga misura dal corretto funzionamento dell'elettronica di potenza, dei sensori e della comunicazione interna.

Nel dettaglio, il malfunzionamento dell'inverter è stato modellato come un annullamento parziale o totale delle tensioni applicate ai motori, compromettendo la capacità del manipolatore di generare movimento. Il guasto ai sensori è stato rappresentato come l'introduzione di un disturbo nel segnale di posizione, che può portare a misure errate e a una conseguente errata risposta del sistema di controllo. Infine, il fault nei segnali di trasmissione dei riferimenti è stato simulato come un'amplificazione indesiderata del segnale di comando, che altera l'intensità delle azioni di controllo previste.

Malfunzionamenti di questo tipo possono compromettere in modo significativo le prestazioni del sistema di controllo, generando errori di posizionamento, instabilità o comportamenti imprevisti, e quindi rappresentano una sfida concreta nella progettazione di strategie di rilevamento e risposta sicura ai guasti.

L'obiettivo sperimentale sarà quello di valutare l'incidenza dei fault considerati al sistema robotico, sia in termini di prestazione del controllo sia sull'eventualità che tali problemi possano portare ad un'insufficiente garanzia di sicurezza per un operatore in prossimità o per l'ambiente di lavoro. Effettuate le necessarie valutazioni, l'obiettivo sarà trovare un metodo di rilevazione dei malfunzionamenti efficace e tempestivo e, infine, delle tecniche di intervento più o meno invasive per portare il sistema in uno stato sicuro, in base alla gravità del malfunzionamento.

Capitolo IV – Implementazione

Approccio all’implementazione

L’implementazione pratica del caso di studio è stata condotta mediante l’utilizzo di modelli simulativi del manipolatore CRS-A255, sviluppati appositamente per riprodurre con buona affidabilità e precisione il comportamento del sistema reale. Tali modelli, introdotti nei paragrafi successivi, sono stati realizzati in ambiente MATLAB & Simulink e includono una rappresentazione dettagliata della dinamica del robot, dei suoi attuatori e sensori, nonché delle logiche di controllo. In particolare, è stato implementato un controllo a dinamica inversa nello spazio dei giunti, descritto nel paragrafo dedicato al sistema di controllo, che consente di compensare in modo accurato le dinamiche non lineari del manipolatore e di ottenere un comportamento stabile e preciso anche in presenza di disturbi. I modelli, come approfondito nel paragrafo relativo all’iniezione dei fault, sono stati integrati con meccanismi per la simulazione di guasti intenzionali alle componenti critiche del sistema, come gli inverter, i sensori e i canali di comunicazione. Questa struttura modulare consente di testare in modo sistematico gli effetti dei fault sul comportamento del sistema e di validare le strategie di rilevamento e mitigazione sviluppate.

Al fine di garantire un monitoraggio efficace del sistema e una gestione tempestiva dei malfunzionamenti, è stata progettata un’architettura di rilevamento multilivello, in grado di operare su più piani di osservazione e controllo. Questa struttura consente di individuare diverse tipologie di fault attraverso una combinazione di strategie di monitoraggio locale e globale.

Inoltre, è stato implementato un sistema di controllo diverso da quello a cinematica inversa nello spazio dei giunti, ovvero un controllo PID indipendente dei giunti. Questo approccio, pur non tenendo conto esplicitamente del modello dinamico completo del robot, offre il vantaggio di semplificare l’architettura di controllo e garantire una buona stabilità in molte applicazioni pratiche. L’indipendenza tra i controllori consente di ridurre l’influenza dinamica reciproca tra i diversi bracci del manipolatore, limitando gli effetti delle interazioni meccaniche tra i giunti. In questo modo, è possibile ottenere un comportamento più prevedibile e localizzato, facilitando l’analisi e l’individuazione di anomalie. Inoltre, in caso di malfunzionamento localizzato su uno specifico giunto, il controllo indipendente permette di isolare il problema e attuare misure correttive mirate senza necessariamente compromettere l’intero sistema. Questa struttura risulta particolarmente utile nel contesto della rilevazione e gestione dei fault, in quanto consente di

mantenere il funzionamento residuo del robot e garantire la sicurezza operativa anche in presenza di guasti parziali.

Per questo secondo metodo di controllo, è stata prevista anche l'implementazione di un sistema di inversione cinematica online che sfrutta la ridondanza del manipolatore per effettuare delle ottimizzazioni mirate e trovare soluzioni che permettano di rispettare i vincoli imposti. L'utilizzo di tale tecnica permette di attuare un ricalcolo della traiettoria in caso di guasto ad uno dei giunti e di portare a termine il task sfruttando la funzionalità dei giunti operativi.

Architettura multilivello

La soluzione proposta per andare ad individuare i malfunzionamenti per permettere le misure correttive di protezione prevede un'architettura a livelli: tali livelli prevedono una gerarchia di importanza nella quale il livello più alto è monitorato da quello più basso per verificare il normale funzionamento. Le principali soluzioni adottate in questo tipo di architettura prevedono l'utilizzo di ridondanza, sia per quanto riguarda gli attuatori che per i sensori; ad esempio, la presenza di un segnale ridondante per la misura della posizione angolare di un giunto e di un decisore permettono di individuare eventuali malfunzionamenti in tempi rapidi, andando ad evitare problemi nell'esecuzione di un task. In tal caso, si può ipotizzare di utilizzare il livello 2 per effettuare in tempo reale un controllo delle posizioni angolari di ogni giunto e di confrontare i segnali provenienti dall'encoder: un decisore può segnalare una discrepanza tra i valori misurati dal livello 1 e quelli del segnale ridondante, definendo delle soglie massime di errore ammesse oltre le quali viene segnalato il malfunzionamento. È evidente come un approccio simile permette di raggiungere l'obiettivo minimo di progetto, ovvero quello di minimizzare i danni che eventuali malfunzionamenti possono causare nel caso di interazioni del manipolatore con un operatore umano.

Questo schema architetturale si ispira direttamente al modello multilivello proposto da Bosch nel contesto dei sistemi di guida autonoma [22]. Tale architettura si fonda su una stratificazione funzionale dei componenti del sistema, dove ciascun livello ha una responsabilità operativa ben definita e, al tempo stesso, è soggetto alla supervisione attiva da parte dei livelli inferiori. In questa visione, la ridondanza non è soltanto strutturale (sensori e attuatori replicati), ma anche logica e funzionale, in quanto ogni livello può replicare

o stimare il comportamento di quello superiore, consentendo una diagnosi più robusta e una mitigazione immediata in caso di fault.

Nel metodo Bosch, tipicamente applicato in ambito automotive secondo i dettami della ISO 26262, si distinguono tre livelli principali:

- Livello 0, responsabile dell'esecuzione diretta del task (ad esempio il controllo in retroazione dei giunti);
- Livello 1, dedicato alla supervisione del funzionamento del livello inferiore e alla raccolta di segnali diagnostici;
- Livello 2, con funzioni di monitoraggio globale, decisione e gestione delle strategie di fail-operational o fail-safe.

L'adattamento di questa filosofia al contesto robotico collaborativo risulta particolarmente promettente, poiché consente di integrare requisiti di functional safety in architetture di controllo che devono operare in ambienti dinamici e condivisi con operatori umani. Il comportamento del sistema può così essere analizzato in chiave probabilistica-statistica, stimando le coperture di fault detection e ottimizzando le politiche di intervento in funzione della gravità del malfunzionamento e del contesto operativo. Questo approccio fornisce non solo maggiore affidabilità al sistema, ma anche una base strutturata per la certificazione di robot collaborativi secondo standard di sicurezza futuri, mutuati da quelli automotive.

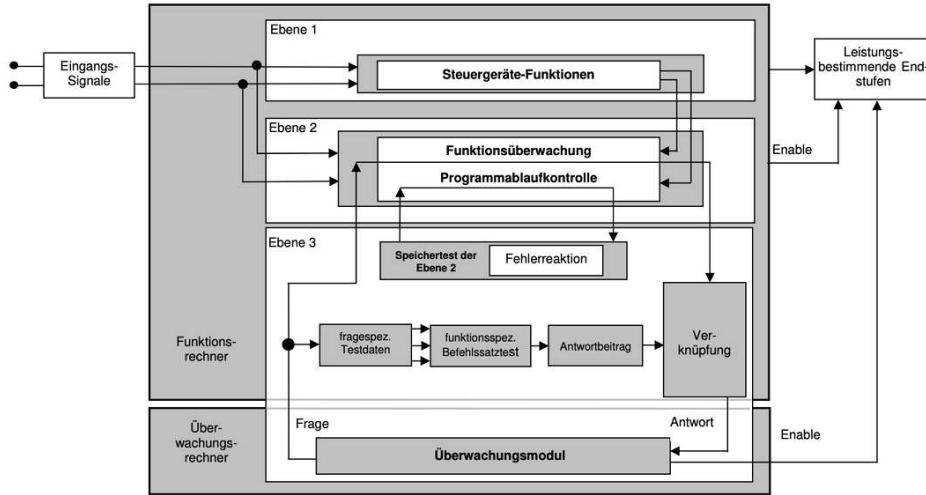


Figura 27 - Architettura EGas a tre livelli

La soluzione proposta nel nostro caso di studio prevede due livelli di esecuzione paralleli: in simulazione, nel livello 1 viene eseguito il controllo a dinamica inversa per l'inseguimento della traiettoria precalcolata come descritto precedentemente, mentre il livello 2 prevede lo stesso controllo privato di tutte le funzioni di monitoraggio non necessarie al controllo della normale esecuzione del task. Il sistema di check invece prevede di prelevare le posizioni dei giunti misurate in entrambi i livelli; tali posizioni sono confrontate ad ogni passo di discretizzazione e viene ricavato l'errore in valore assoluto tra i due vettori. Nel caso di normale funzionamento, l'errore è presumibilmente trascurabile, perciò nessun flag viene innescato durante l'intera esecuzione del task. Nel caso di malfunzionamento ad una componente del manipolatore (motore, giunto, sistema di controllo, sensore, ecc.), la posizione dei giunti del livello 1 devierà da quella attesa simulata nel livello 2, generando un errore assoluto nel sistema di check che, superato il valore di sogli impostato, segnalera un flag. Il flag può essere successivamente implementato per andare ad attuare delle misure correttive real-time, in base alle possibilità e alla gravità del fault considerato: ad esempio, un errore sull'inverter che pilota le tensioni da applicare ad ogni motore per muovere il giunto desiderato non prevede possibilità di intervento poco invasive; perciò, all'attivazione del flag è possibile fermare il manipolatore imponendo tensioni nulle ad ogni motore. Se il malfunzionamento prevede che il corretto funzionamento della maggior parte dei giunti è garantito, è possibile attuare misure di intervento meno invasive, come un ritorno alla configurazione di partenza o un ricalcolo della traiettoria.

per sfruttare la ridondanza del manipolatore e raggiungere la posa finale anche senza l'utilizzo di uno dei giunti.

Misure correttive

Sistema di check basato su due livelli:

- Primo livello: simulazione del sistema di controllo del manipolatore
- Secondo livello: monitoraggio del primo livello, simulazione degli input e degli output attesi

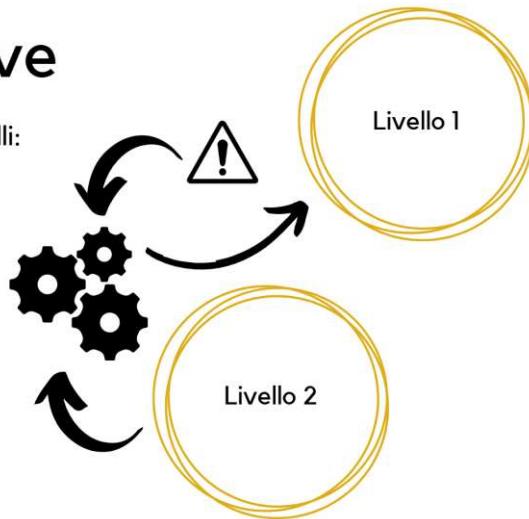


Figura 28 - Architettura di rilevazione e intervento a livelli

Cinematica inversa tramite metodo della pseudo-inversa

Nella soluzione della cinematica inversa di un manipolatore robotico, esistono due approcci principali: analitico e numerico. Il metodo analitico consiste nel ricavare una soluzione esplicita, esprimendo direttamente le variabili di giunto in funzione della posizione e orientazione desiderate. Questo approccio è estremamente efficiente in tempo reale, poiché fornisce una soluzione immediata senza la necessità di iterazioni, garantendo tempi di calcolo ridotti e maggiore stabilità. Tuttavia, è applicabile solo a manipolatori con una struttura sufficientemente semplice da permettere una risoluzione chiusa delle equazioni. Il metodo numerico, invece, utilizza algoritmi iterativi per trovare una soluzione approssimata, come il metodo di Newton-Raphson. Sebbene sia più flessibile e applicabile a qualsiasi struttura robotica, è computazionalmente più oneroso e può soffrire di problemi di convergenza o di soluzioni non univoche, rendendolo meno adatto a implementazioni real-time.

È necessario effettuare delle considerazioni sulla ridondanza del manipolatore rispetto ad un task assegnato prima di valutare le metodologie di cinematica inversa. La ridondanza di un manipolatore robotico è strettamente connessa alla natura del compito da eseguire, in particolare ai

requisiti di posizione e orientamento dell'end-effector. Un manipolatore si definisce ridondante quando dispone di un numero di gradi di libertà (DoF, *Degrees of Freedom*) superiore a quello minimo necessario per portare a termine un determinato task. Nel caso di un compito che richieda il controllo completo della posa dell'end effector nello spazio tridimensionale, ovvero tre DoF per la posizione e tre per l'orientamento, sono richiesti almeno sei gradi di libertà. Pertanto, un manipolatore a cinque DoF, come il CRS A255 utilizzato in questo lavoro, risulta non ridondante rispetto a tale compito. Tuttavia, se il task richiede solo il controllo della posizione (tre DoF) oppure un orientamento parziale, il manipolatore può essere considerato ridondante, offrendo la possibilità di ottimizzare la traiettoria, evitare ostacoli o distribuire i carichi articolari in modo più favorevole. In scenari reali, la ridondanza rappresenta un'importante risorsa anche per la gestione di malfunzionamenti: un guasto che comprometta la funzionalità di un giunto riduce il numero di DoF effettivamente disponibili, comportando una perdita della ridondanza o, nei casi più critici, l'impossibilità di completare il task. Un esempio rappresentativo è quello di un manipolatore planare a tre DoF impiegato per raggiungere posizioni sul piano X-Y: in condizioni nominali, il sistema è pienamente attuato e in grado di accedere a ogni punto all'interno del proprio workspace. Tuttavia, un malfunzionamento al primo giunto riduce i DoF a due, limitando fortemente la mobilità e rendendo irraggiungibili alcune configurazioni. Tale considerazione evidenzia come la corrispondenza tra i DoF del manipolatore e quelli richiesti dal task sia un fattore cruciale per la continuità operativa del sistema, soprattutto in presenza di fault.

Per garantire un ricalcolo della traiettoria in tempo reale in presenza di variazioni impreviste (es. guasti a un giunto o ostacoli), è possibile combinare un metodo analitico, ove disponibile, con un approccio basato sulla pseudo-inversa del Jacobiano, utilizzando una funzione costo per ottimizzare la configurazione del manipolatore. L'idea è di minimizzare una funzione obiettivo che penalizza gli scostamenti dai valori intermedi dei giunti, riducendo movimenti indesiderati e mantenendo il robot in una configurazione favorevole durante l'intero movimento. Questo permette di adattare rapidamente la traiettoria senza compromettere la stabilità del sistema, rendendo il controllo del manipolatore più robusto ed efficiente in scenari dinamici.

La cinematica inversa è il processo di determinazione dei parametri di un manipolatore (giunti prismatici, rotoidali, ecc.) data una posa desiderata per l'end effector. È possibile determinare una possibile traiettoria nello spazio dei giunti ($q(t), \dot{q}(t)$) che permetta di ottenere le velocità (lineari ed angolari) v dell'organo terminale desiderate, a partire da una posa iniziale.

$$\dot{x} = J_A(q)\dot{q} \quad (25)$$

$$v = J(q)\dot{q} \quad (26)$$

Invertendo l'equazione cinematica differenziale (J quadrata di rango pieno) è possibile determinare una traiettoria nello spazio dei giunti che riproduca la traiettoria assegnata:

$$\dot{q} = J^{-1}(q)v \quad (27)$$

$$q(t) = q(0) + \int_0^t \dot{q}(\xi)d\xi \quad (28)$$

In tempo discreto, si utilizza la regola di integrazione di Eulero

$$q(t_{k+1}) = q(t_k) + \dot{q}(t_k)\Delta t \quad (29)$$

Con:

$$\dot{q}(t_k) = J^{-1}(q(t_k))v(t_k) \quad (30)$$

Se il manipolatore risulta essere ridondante ($r < n$) con n gradi di libertà del manipolatore e r gradi di libertà del task, lo jacobiano è una matrice rettangolare bassa e si pone il problema di trovare le soluzioni all'equazione 4.2.

Le soluzioni infinite della cinematica inversa differenziale sono definite da:

$$\dot{q} = J^+v + (I - J^+J)\dot{q}_d \quad (31)$$

Il primo termine dell'equazione rappresenta la velocità di giunto in corrispondenza della quale si ha una variazione di v , mentre il secondo termine rappresenta le velocità dei giunti in corrispondenza delle quali non può esserci una variazione di v , corrispondenti quindi a moti interni che riconfigurano il manipolatore lasciando inalterata la posizione e l'orientamento dell'organo terminale. Pertanto, è possibile scegliere \dot{q}_d definendo una funzione costo $H(q)$ definita positiva da minimizzare.

$$\dot{H} = \frac{\partial H}{\partial q}\dot{q} = \frac{\partial H}{\partial q}J^+v + \frac{\partial H}{\partial q}(I - J^+J)\dot{q}_d \quad (32)$$

Si cerca una \dot{q}_d che impone $\dot{H} < 0$ per avvicinarsi ad un minimo assoluto per H . Una scelta tipica è:

$$\dot{q}_d = -K \left(\frac{\partial H}{\partial q} \right)^T \text{ con } K > 0 \quad (33)$$

La forma della funzione $H(q)$ dipende dall'obiettivo del task: possiamo individuare tre esempi di funzione $H(q)$:

- $H(q) = \min_{p,o} \|p(q) - o\|$ (34)
- p generico punto del manipolatore
- o punto su un ostacolo

Massimizzando tale funzione si aggira un ostacolo nello spazio operativo

- $H(q) = -\frac{1}{2n} \sum_{i=1}^n \left(\frac{q_i - \bar{q}_i}{q_{iM} - q_{im}} \right)$ (35)
- q_{iM} (q_{im}) massima (minima) escursione di q_i
- \bar{q}_i valore medio della corsa

Minimizzando tale funzione si può riuscire a stare lontano dai fine corsa dei giunti, cercando di rimanere il più possibile nell'intorno del punto medio della corsa del giunto

- $H(q) = \sqrt{\det(J(q)J^T(q))}$ (36)

Indice della manipolabilità, massimizzando tale funzione si cerca di allontanarsi dalle singolarità

In definitiva:

$$\dot{q} = J^+ \dot{p} + (I - J^+ J) \dot{q}_d = J^+ \dot{p} - K(I - J^+ J) \left(\frac{\partial H}{\partial q} \right)^T \quad (37)$$

Definiamo

$$\dot{p} = v - K \dot{e} \quad (38)$$

Con

$$\dot{e} = \dot{x}_d - \dot{x} \quad (39)$$

Implementazione dei modelli di simulazione

Per implementare un sistema di controllo e intervento in grado di gestire eventuali fault sul sistema, è necessario per primo un sistema sul quale effettuare i vari test e simulare in maniera sicura il comportamento del manipolatore in esame. A tal proposito, si è fatto uso di un digital twin (gemello digitale) del manipolatore CRS A255, sviluppato e implementato sul software MATLAB & Simulink [21]. Un digital twin è una rappresentazione virtuale di un'entità fisica o di un sistema con la quale scambiare dati e informazioni, sia in modalità sincrona che asincrona. Tale componente digitale può evolversi fino a diventare una vera e propria replica digitale di risorse fisiche potenziali ed effettive di processi, persone, infrastrutture, sistemi e dispositivi che possono essere utilizzati per vari scopi. In termini generali, le principali caratteristiche del gemello digitale sono:

- Insieme dei dati e delle informazioni in qualunque modo riferibili alle entità rappresentate dal digital twin;
- Connessione tra gli elementi della componente fisica con la corrispondente parte virtuale;
- Possibilità di accesso ubiquitario a dati e risorse informatiche attraverso il web, con possibilità di ricerca e analisi delle informazioni (big data, machine learning, intelligenza artificiale)
- Scambio di dati e informazioni tra la componente virtuale e quella fisica, con utilizzo di sensori e attuatori

In molti settori industriali, i digital twin sono già ampiamente utilizzati per ottimizzare il funzionamento e la manutenzione sia di beni fisici che di sistemi e processi produttivi. A nostra disposizione è presente un modello del manipolatore digitale implementato in MATLAB & Simulink, il quale, tramite funzioni della libreria Simscape, permette di simulare il comportamento del reale manipolatore con alta affidabilità ed errori contenuti. La prima operazione per iniziare a studiare ed implementare un sistema di controllo e di intervento in caso di fault è stata quella di effettuare una conversione del modello per renderlo compatibile con le nuove versioni del software MATLAB & Simulink: in particolare, la versione della libreria Simscape utilizzata nella creazione del sistema simulato risultava incompatibile con le nuove versioni del software, poiché quest'ultima è stata completamente aggiornata e rivoluzionata rispetto alle versioni precedenti alla 2019a. La conversione consiste nel modificare i blocchi Simscape della prima versione con quelli della seconda, facendo attenzione a modificare tutti i parametri necessari per garantire il funzionamento corretto della simulazione. Tramite un sistema di conversione semiautomatica, sono stati

prima rilevati tutti i blocchi che potevano essere sostituiti in modo automatico e quelli che invece necessitavano di modifiche; tra questi ultimi, è stato importante differenziare le due generazioni per i blocchi che definiscono i corpi (BODIES) con relative proprietà inerziali e terne di riferimento, i giunti (JOINTS), il frame inerziale e i rapporti degli organi di trasmissione.

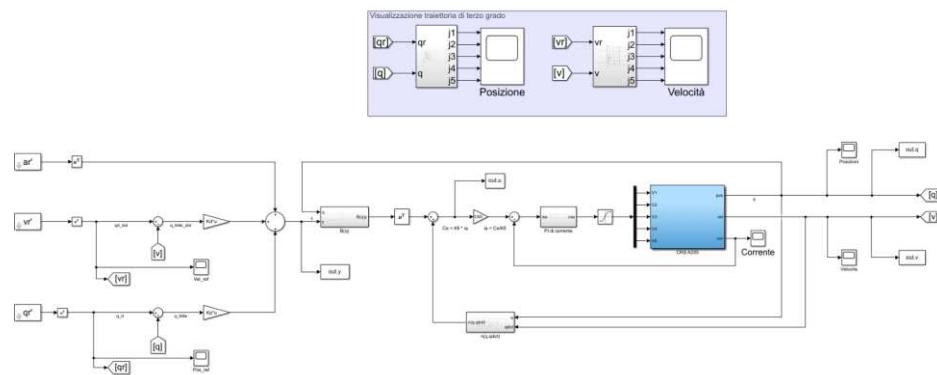


Figura 29 - Digital Twin Manipolatore CRS A255

Il sistema simulato contiene il modello dinamico dello stesso rappresentato dal blocco azzurro denominato “CRS A255”.

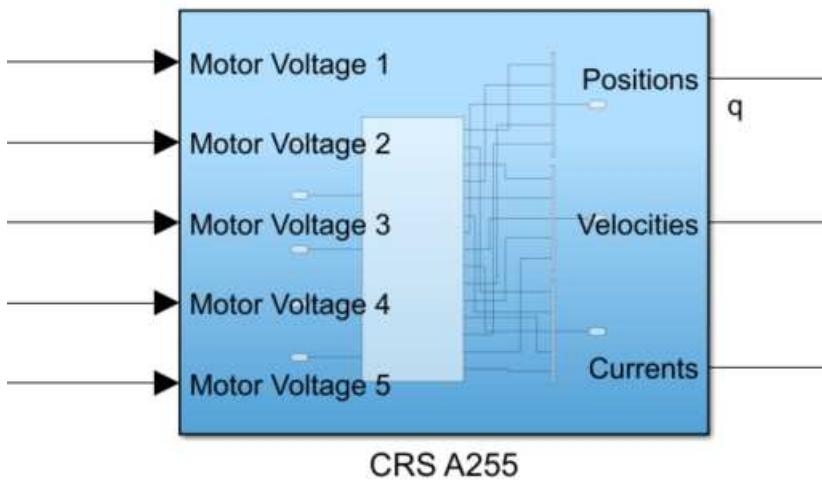


Figura 30 - Modello Simscape del Manipolatore

Tale modello dinamico consente di effettuare simulazioni sul manipolatore con un grado di accuratezza elevato. Gli input ovviamente sono rappresentati dalle cinque tensioni che, istante per istante, devono essere applicate a ciascun motore che governa ciascun giunto del manipolatore in questione. Poiché sino

ad ora è stata direttamente fornita l'azione di controllo Q rappresentante fisicamente le coppie richieste ai motori, è necessario determinare le tensioni desiderate.

Data la relazione coppia/corrente:

$$C_e = K_\phi i_a \quad (24)$$

È stato realizzato un anello interno di corrente con un PI tarato opportunamente.

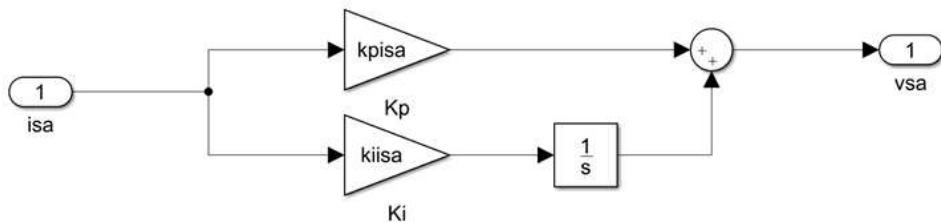


Figura 31 - PI di corrente

In particolare, i termini K_P e K_I sono stati determinati in accordo con il criterio del modulo ottimo. In uscita dal blocco regolatore di corrente è presente un saturatore che limita le tensioni applicate al motore.

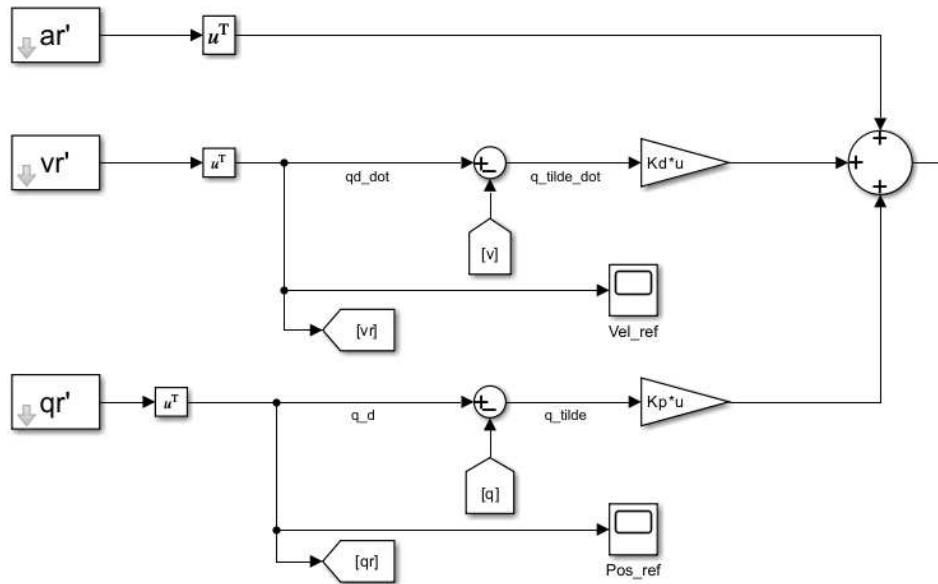


Figura 32 - Riferimenti di posizione, velocità e accelerazione

A monte del sistema di controllo sono presenti i riferimenti di posizione, velocità e accelerazione, moltiplicati per le matrici K_P e K_D , e sommati tra loro, a costituire l'azione stabilizzante di controllo lineare.

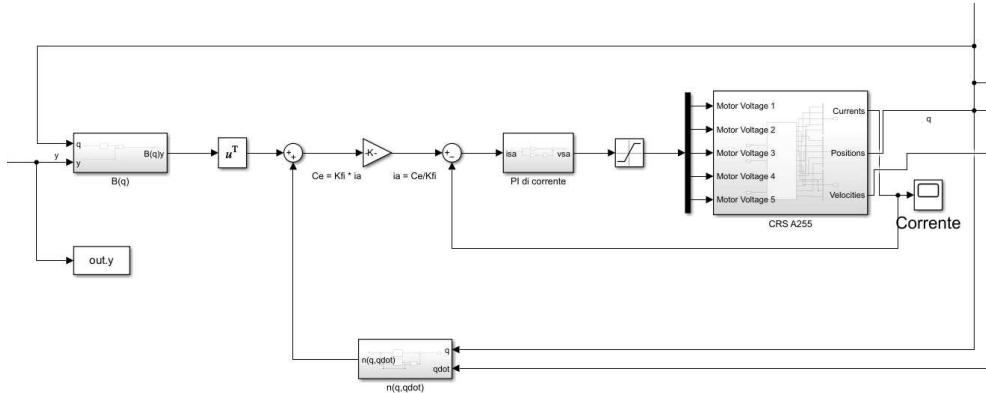


Figura 33 - Calcolo dei disaccoppiamenti e delle compensazioni in avanti

In uscita dal nodo sommatore è presente il calcolo dei termini di disaccoppiamento e la compensazione non lineare, per le quali sono necessarie le misure di posizione e velocità per ciascun giunto.

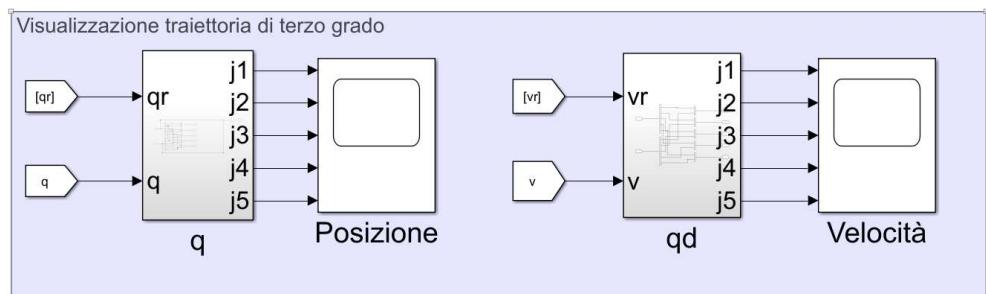


Figura 34 - Visualizzazione delle traiettorie

Sono confrontate le posizioni e velocità di riferimento e quelle misurate per avere una chiara visualizzazione delle traiettorie di terzo grado e per monitorare il corretto funzionamento del controllo.

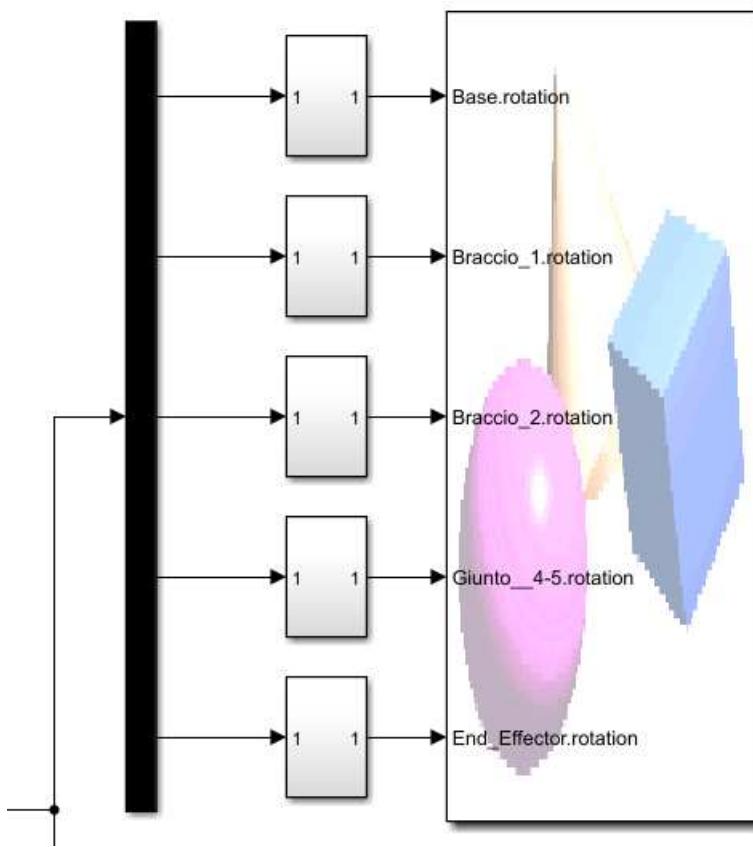


Figura 35 - Simulazione 3D del manipolatore

Una simulazione 3D permette di visualizzare graficamente il movimento del manipolatore, considerando le posizioni dei giunti misurati.

L'implementazione delle misure di sicurezza parte dal valutare le conseguenze che potenziali fault sul sistema possono innescare, e catalogarle in ordine di importanza e gravità dei danni causati da tali malfunzionamenti. Definiti quindi i fault da voler valutare, è necessario per primo analizzare i dati che si ottengono dalla simulazione prima in condizioni normali e successivamente con l'iniezione artificiale di un malfunzionamento in un determinato componente. I dati valutati ad ogni simulazione sono le posizioni, velocità, accelerazioni e coppie per ogni giunto, i riferimenti di posizione, velocità e accelerazione per ogni giunto, e le tensioni applicate ai motori da parte dell'inverter. Inizializzati i parametri utili alla simulazione, si procede a generare una traiettoria nello spazio dei giunti compatibile con i limiti strutturali del manipolatore definiti precedentemente.

Implementazione dell'architettura a livelli

Per implementare l'architettura esposta, a partire dal modello Simulink descritto precedentemente, è stato creato il primo livello, mentre una copia dello stesso è stata utilizzata per la creazione del secondo livello. Tale sottosistema è stato privato dei vari blocchi *Scope* e degli output non necessari, oltre alla parte per la visualizzazione 3D dell'animazione del manipolatore; le uniche componenti utili sono quelle relative al controllo e alla simulazione del sistema dinamico per ottenere le posizioni dei giunti stimate. Il sistema così ottenuto prevede che sia il sistema che voglio controllare che il livello 2 siano simulati: nella realtà, il livello 1 è rappresentato dalla versione fisica del manipolatore, mentre il livello 2 è rappresentato dalla versione simulata appena descritta. Essendo entrambi i livelli basati sullo stesso sistema simulato, le uniche differenze tra gli output di posizione dei giunti saranno date da eventuali delay dovuti all'esecuzione in parallelo delle simulazioni e dei fault iniettati nel sistema al livello 1. Definiti i livelli, è stato necessario implementare un sistema di rilevazione per determinare un malfunzionamento in modo tempestivo: per far ciò, sono state prelevate istante per istante le posizioni dei giunti dal livello 1 e dal livello 2; calcolato l'errore in valore assoluto, il vettore composto dagli errori viene caricato in un buffer di campioni, mentre una successiva funzione permette di verificare che se un numero superiore ad una certa quantità dei campioni di un determinato errore supera una soglia opportunamente tarata, il sistema segnala tramite un flag identificativo un eventuale malfunzionamento. L'implementazione appena descritta risulta essere un sistema digitale di antirimbalzo (*debouncing*), ovvero un sistema in grado di essere robusto al fenomeno del *flickering*, cioè la variazione di un segnale (elettrico o digitale) dallo 0 all'1 logico in maniera rapida. Il buffer risulta essere utile per determinare un'attivazione del flag con una bassa sensibilità agli errori transitori, i quali potrebbero portare ad una segnalazione di errore anche in caso di normale funzionamento. In definitiva, in uscita dal blocco funzione, si ottiene un identificativo che segnala tramite un numero univoco il malfunzionamento al giunto corrispondente.

Il sistema di check è stato quindi implementato tarando il buffer per valutare un numero di campioni (equivalenti ad un certo valore di secondi in base al tempo di campionamento considerato) relativi al valore assoluto dell'errore di posizione per ogni giunto, e segnalare tramite flag un errore nel caso in cui la media degli errori nel buffer superasse una soglia, definita come percentuale del valore finale che ogni giunto assume al termine della traiettoria, in modo tale da essere dinamico rispetto al movimento di ognuno di essi.

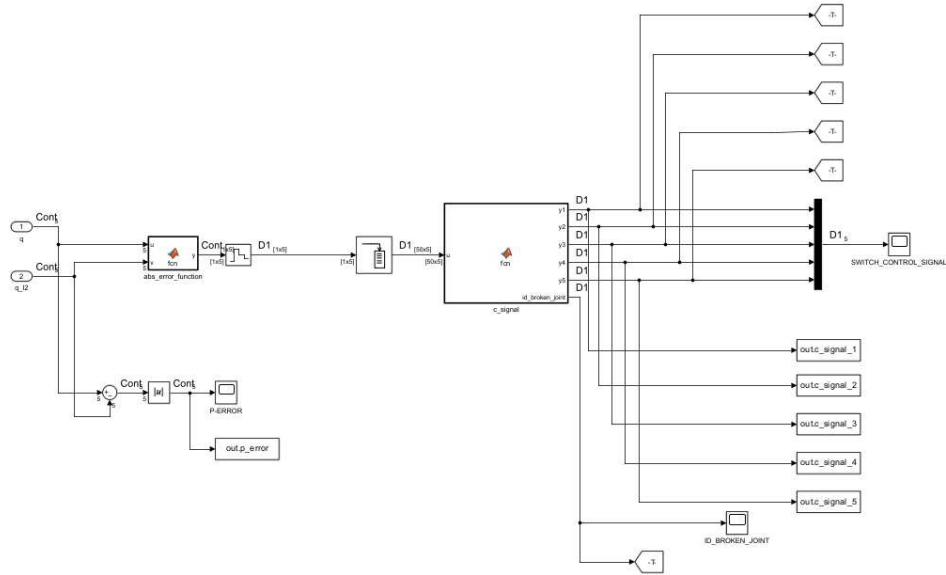


Figura 36 - Check posizioni e generazione flag

La scelta per quanto riguarda il segnale di check è ricaduta sulle posizioni dei giunti e non su altri parametri, poiché le posizioni angolari sono le componenti del sistema più sensibili ad eventuali fault su tutta la catena di controllo: difatti, un malfunzionamento al sistema di alimentazione dei motori, o agli encoder, o al microcontrollore, avrebbe una risonanza evidente nella configurazione dei giunti. Ipotizzando un sistema che implementa un tale meccanismo di sicurezza, ed un modello simulato sufficientemente accurato, una differenza nelle posizioni tra il sistema che ha subito un malfunzionamento e il suo corrispondente digitale privo di guasti è facilmente apprezzabile.

Implementazione del controllo PID

L'approccio tramite un controllo a dinamica inversa nello spazio dei giunti, descritto ed implementato precedentemente, rappresenta una soluzione efficace e accurata nel caso di normale funzionamento del manipolatore. Questo metodo consente una compensazione in tempo reale delle non linearità del sistema, garantendo un inseguimento preciso della traiettoria desiderata, a condizione che i parametri del modello siano sufficientemente noti e stabili. Tuttavia, in presenza di malfunzionamenti, tale strategia può rivelarsi inefficace o addirittura controproducente. La forte influenza dinamica che ogni giunto o braccio esercita sugli altri, infatti, complica

l'applicazione di misure di sicurezza più flessibili e meno restrittive, come ad esempio il ricalcolo dinamico della traiettoria in tempo reale o l'adattamento locale del comportamento del robot.

Per questa ragione, si è deciso di integrare al controllo a dinamica inversa un sistema basato su controllori PID indipendenti per ogni giunto. Questo approccio consente di ridurre significativamente le interazioni dinamiche tra i vari assi del manipolatore, permettendo un controllo più localizzato e modulare. Di conseguenza, in caso di malfunzionamento su un singolo giunto, è possibile isolare e gestire il problema in modo mirato, attuando misure correttive specifiche senza dover bloccare l'intero sistema o ricorrere a interventi globali e invasivi. Questa configurazione migliora la flessibilità e la sicurezza operativa del manipolatore, facilitando l'implementazione di strategie di fault-tolerant più sofisticate, che mirano a mantenere l'efficienza e la sicurezza anche in condizioni di guasto parziale.

Il seguente controllo è stato implementato andando a dare in input al sistema i riferimenti di posizioni nello spazio dei giunti, e, ottenuto l'errore di posizione, i controllori PID sono stati tarati tramite il tool *auto-tuner* di MATLAB. In uscita dai controllori sono generati i riferimenti di corrente utili all'anello di controllo interno per la generazione dei riferimenti di tensione da applicare ai motori dei giunti del manipolatore.

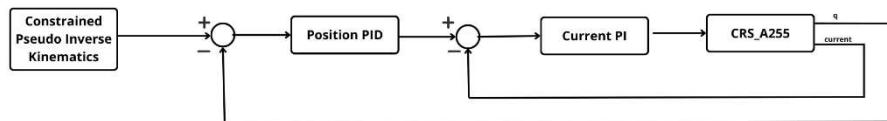


Figura 37 - Schema di controllo semplificato

In modo analogo al precedente schema di controllo, sono implementati due livelli: il primo simula il manipolatore reale, mentre il secondo rappresenta il digital twin del manipolatore. Nel primo livello saranno iniettati i fault necessari alla valutazione degli effetti e delle contromisure adottate per mitigare o eliminare i potenziali pericoli, mentre il secondo simula il sistema in caso di normale funzionamento.

Implementazione del metodo della pseudo-inversa

L'implementazione di tale metodo per il calcolo delle posizioni dei giunti che mi garantiscono l'inseguimento della traiettoria nello spazio operativo è stata eseguita in Simulink nel seguente modo:

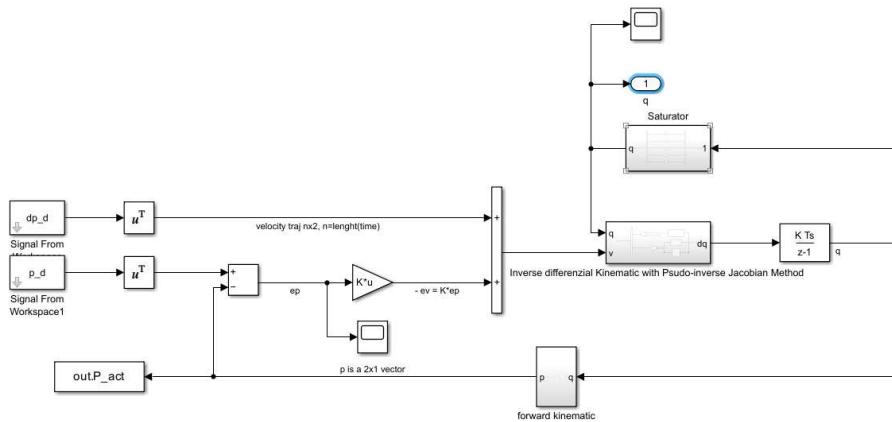


Figura 38 - Cinematica inversa tramite Pseudo-inverse dello Jacobiano e ottimizzazione delle funzioni costo

Per primo, è stato definito il nostro manipolatore tramite la libreria *Robotics Toolbox* di Peter Corke [23], in modo da poter utilizzare le funzioni per calcolare lo jacobiano e altre parti del controllo utili all'implementazione. Il sistema prende in input le traiettorie di posizione e velocità nello spazio operativo per l'end effector: la velocità è sommata all'errore di posizione moltiplicato per una costante K per ottenere il vettore \dot{p} . Tale vettore entra all'interno del subsystem che implementa il metodo della pseudo inversa per ottenere le velocità dei giunti, le quali sono integrate per ottenere le posizioni istante per istante; infine, le posizioni vengono utilizzate per calcolare, tramite cinematica diretta, le pose dell'end effector in modo da calcolare l'errore al passo successivo. All'interno dello stesso subsystem si trovano ulteriori blocchi: sono implementate le funzioni per il calcolo della pseudo inversa dello jacobiano (J^+), il kernel della matrice P ($I - J^+J$), e la funzione costo scelta per il caso applicativo.

Questo metodo viene utilizzato per generare la traiettoria nello spazio dei giunti per il manipolatore istante per istante, andando a minimizzare la funzione $H(q)$ che mi permette di mantenere i giunti il più possibile vicini ai loro valori medi. Il principale motivo per il quale è necessario implementare

tale metodo nel controllo del manipolatore è quello di trovare una soluzione analitica al problema real-time, che permetta, in caso di guasto o malfunzionamento, di cercare una traiettoria di sicurezza che preveda di non utilizzare il giunto guasto, sfruttando la ridondanza del manipolatore. Per fare ciò, è necessario modificare i valori di q_{iM} , q_{im} e \bar{q}_i , con i corrispondente al giunto malfunzionante, bloccando il valore medio uguale a quello misurato al momento del guasto e riducendo l'escursione massima per il giunto a pochi gradi. Come reazione, la funzione H aumenterà il peso corrispondente al giunto malfunzionante o guasto per privilegiare soluzioni che non prevedono movimenti di tale giunto. Per far ciò, è stata implementata una macchina a stati che modifica i valori di $qavg$ (valore medio per il giunto) e $qrange$ (range massimo di escursione del giunto) in base al valore assunto dal flag di errore identificativo del giunto guasto id_broken_joint , il quale assume valore 0 in caso di normale funzionamento e un valore da 1 a 5 nel caso di malfunzionamento associato ad uno dei giunti. In particolare, il valore di $qrange$ viene portato per il giunto corrispondente ad una escursione di due gradi, mentre il valore di $qavg$ viene settato al valore misurato della posizione corrente.

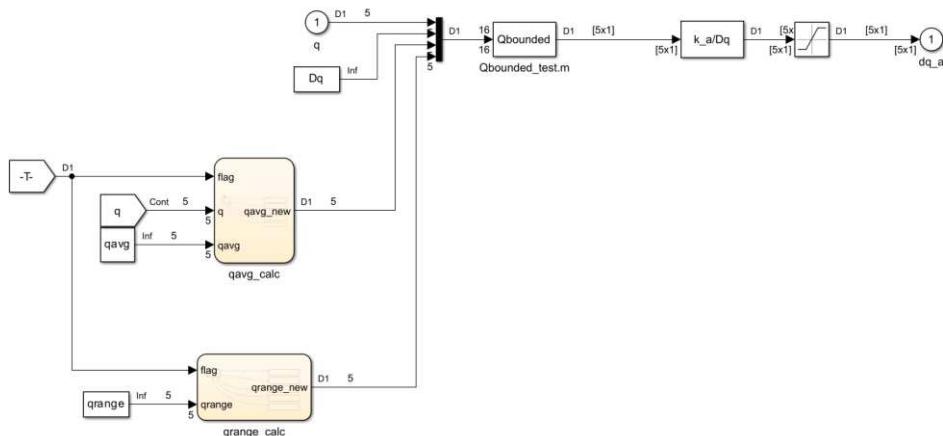


Figura 39 - Calcolo della $H(q)$ dinamico

Test del metodo della pseudo-inversa su un manipolatore planare a tre bracci

Per dimostrare l'efficacia della funzione costo nel calcolo della traiettoria real-time in caso di manipolatori ridondanti, questo approccio è stato testato su un manipolatore planare a tre bracci. I gradi di libertà del manipolatore planare a tre bracci permettono di trovare più soluzioni per l'inseguimento di

una traiettoria su un piano: i gradi di libertà r richiesti per una traiettoria sul piano x-y sono due, mentre i gradi di libertà di un manipolatore planare a tre bracci m sono tre:

$$L = m - r = 1 \quad (40)$$

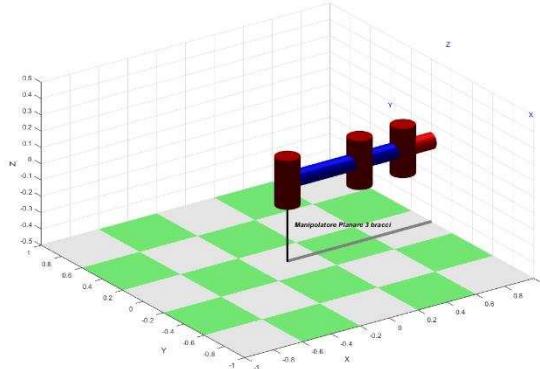


Figura 40 - Manipolatore planare a 3 bracci

Il grado di libertà in eccesso permette di utilizzare la funzione di ottimizzazione per trovare soluzioni in base alle esigenze e, nel caso particolare, di mantenere i giunti il più possibile vicini ai loro valori medi. Il seguente manipolatore planare a tre bracci è stato definito nei parametri, tramite la libreria *Robotics Toolbox* di Peter Corke, seguendo la convenzione di Denavit-Hartenberg:

Braccio	a_i [mm]	α_i [rad]	d_i [mm]	θ_i [rad]
1	500	0	0	θ_1
2	300	0	0	θ_2
3	300	0	0	θ_3

Tabella 5 - Parametri di Denavit-Hartenberg del manipolatore planare a tre bracci

È stato calcolato, tramite un algoritmo iterativo volto ad esplorare un alto numero di configurazioni, lo spazio di lavoro del manipolatore, che corrisponde all'area di un cerchio centrato in zero con raggio pari a 1.1 metri. Inoltre, tramite l'algoritmo *k-nearest neighbors* [24] sono state individuate le zone dello spazio di lavoro più popolate ed evidenziate nel grafico tramite

una scala cromatica: le zone più popolate indicano posizioni dell'end effector raggiungibili da un maggior numero di configurazioni del manipolatore.

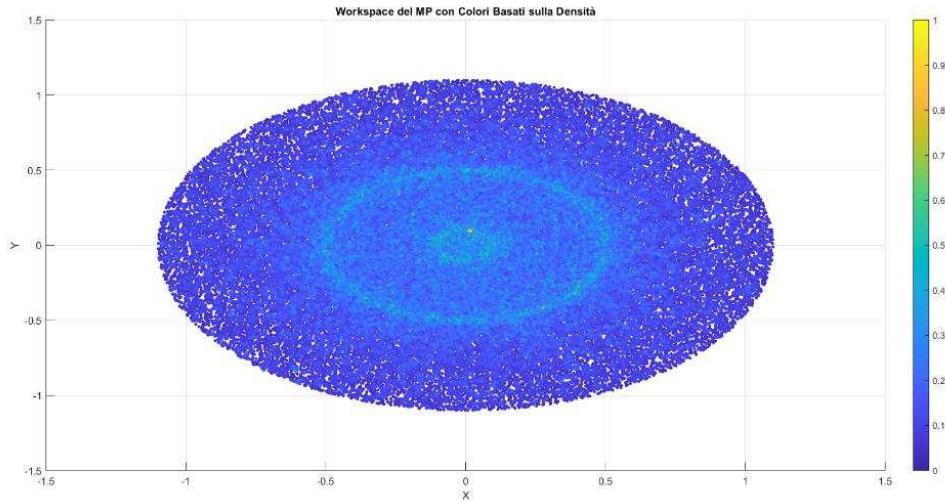


Figura 41 - Workspace del manipolatore planare

A scopo informativo, è stato valutato l'effetto che ha sullo spazio operativo del manipolatore un eventuale malfunzionamento ad uno dei giunti: a tal proposito, sono stati bloccati alla loro configurazione di partenza tutti i giunti (uno per volta) e sono state valutate le configurazioni possibili in tali situazioni. Di seguito, sono mostrati in figura gli spazi operativi nel caso, rispettivamente, di blocco alla posizione di partenza del giunto 1, del giunto 2 e del giunto 3.

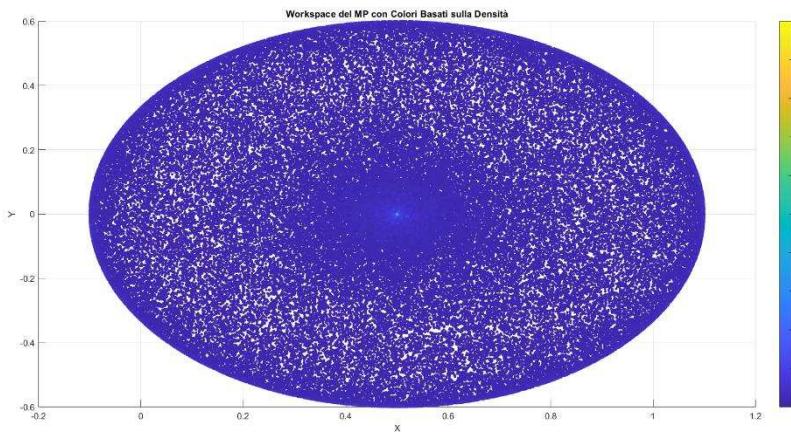


Figura 42 - Workspace manipolatore planare – 1° giunto bloccato

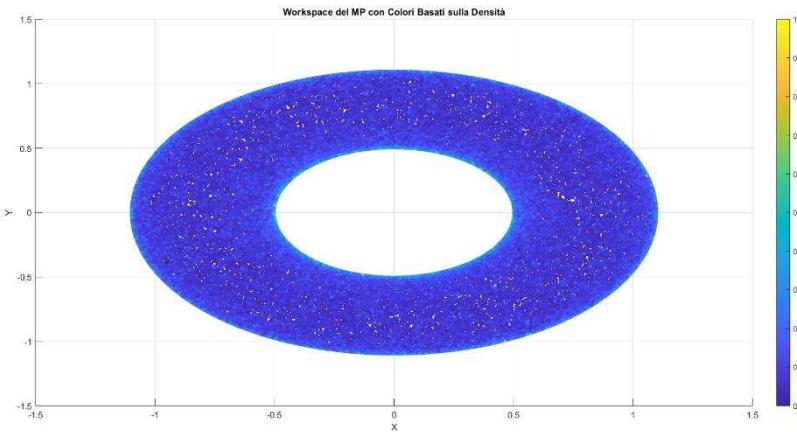


Figura 43 - Workspace manipolatore planare – 2° giunto bloccato

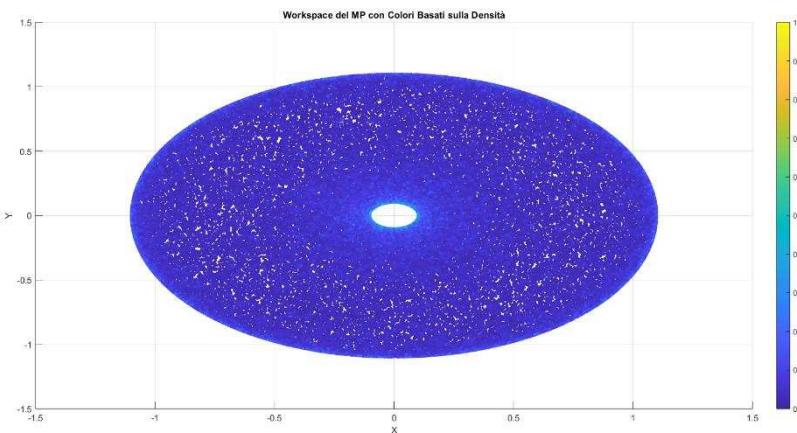


Figura 44 - Workspace manipolatore planare - 3° giunto bloccato

Definito il manipolatore, il passo successivo è quello di definire una posizione iniziale e una finale appartenenti al workspace e generare una traiettoria prima nello spazio dei giunti tramite interpolazione di punti per verificare che non si ecceda nei limiti, e successivamente nello spazio operativo. Otttenuta la traiettoria è possibile effettuare una simulazione che permette di effettuare il calcolo della cinematica inversa e quindi ottenere le posizioni angolari per ogni giunto andando a sfruttare la ridondanza e massimizzando o minimizzando le funzioni costo descritte precedentemente. Nella simulazione non è previsto un modello fisico del manipolatore planare, poiché lo scopo della simulazione è verificare l'efficacia della soluzione della cinematica inversa per manipolatori ridondanti. I risultati del test sono utili a capire se è

possibile utilizzare in tempo reale il calcolo della cinematica inversa per generare i riferimenti da applicare al sistema di controllo del manipolatore.

Capitolo V – Test e performance

Terminate la fase di ricerca e in concomitanza con la fase di implementazione tramite codice MATLAB e Simulink, sono state effettuate tutte le simulazioni dei sistemi descritti. La fase di simulazione è stata eseguita cronologicamente nel seguente ordine:

- Simulazione del sistema di controllo a dinamica inversa in autonomia, per verificare che il comportamento del sistema trasportato alla nuova versione della libreria *Simscape Multibody* sia comparabile a quello della versione precedente.
- Simulazione del controllo a dinamica inversa in presenza di malfunzionamenti totali per verificare gli effetti sulla posizione del manipolatore e sulle coppie generate.
- Simulazione in presenza di malfunzionamenti totali con il sistema di check delle posizioni ed intervento delle protezioni.
- Simulazione in presenza di malfunzionamenti parziali con il sistema di check delle posizioni e ricalcolo della traiettoria.
- Simulazione del controllo PID in assenza di malfunzionamenti.
- Simulazione del controllo PID in presenza di malfunzionamenti totali per verificare gli effetti sulla posizione del manipolatore e sulle coppie generate.
- Simulazione del controllo PID in presenza di malfunzionamenti totali con il sistema di check e intervento delle protezioni.
- Simulazione del manipolatore planare per verificare efficacia del calcolo della cinematica inversa con ottimizzazione della funzione costo per manipolatori ridondanti.
- Simulazione del controllo PID in presenza di malfunzionamenti parziali con il sistema di check delle posizioni e ricalcolo della traiettoria.

I test sono stati condotti su piattaforma Windows 11 23H2, con una CPU Ryzen 7 5700U, GPU integrata AMD Radeon, 16GB RAM DDR4-3200, su software MATLAB 2024b.

Parametri di simulazione

Per eseguire la simulazione ed ottenere i primi risultati da confrontare con quelli relativi all'esecuzione del modello del manipolatore con controllo a dinamica inversa, definito con la libreria *Simscape Multibody* di prima

generazione, è stato necessario definire in MATLAB i parametri essenziali all'esecuzione della simulazione. Inizialmente sono stati così definiti i parametri elettrici dei motori associati ai giunti del manipolatore.

Parametro	Valore [unità di misura]	Descrizione
R_a	3 [Ohm]	Resistenza elettrica di armatura
T_a	$0.4 * 10^{-3}$ [s]	Costante di tempo di armatura
K_{fi}	0.066 [Nm/A]	Costante di coppia
k_a	7 [adimensionale]	Costante di amplificazione
J_m	$1.57 * 10^{-5}$ [kg * m ²]	Inerzia di armatura
i_{an}	3.5 [A]	Corrente di armatura nominale
K_a	7 [adimensionale]	(Vedi k_a) *
J	$1.57 * 10^{-5}$ [kg * m ²]	(Vedi J_m) *

Tabella 6 - Parametri elettrici del manipolatore

* Stessi parametri già descritti ma utilizzati con nome diverso nelle diverse componenti Simulink

In seguito, sono stati definiti i parametri meccanici del manipolatore, a partire dalle masse dei bracci:

m_1	27.149655 [lb]	12.314876 [Kg]
m_2	4.1142220 [lb]	1.866180 [Kg]
m_3	4.1563835 [lb]	1.885304 [Kg]
m_4	0.59499662 [lb]	0.269886 [Kg]
m_5	0.039727640 [lb]	0.018020 [Kg]

Tabella 7 - Masse dei bracci del manipolatore

I centri di gravità per ogni braccio (in mm):

r_1	-0.0383 [mm]	$-1.7457 * 10^{-4}$ [mm]	0.2233 [mm]
r_2	0.1254 [mm]	$-3.9882 * 10^{-7}$ [mm]	$1.5014 * 10^{-4}$ [mm]
r_3	0.0914 [mm]	-0.0017 [mm]	$-2.1415 * 10^{-4}$ [mm]
r_4	$-9.6554 * 10^{-4}$ [mm]	$1.6697 * 10^{-7}$ [mm]	$-9.3276 * 10^{-4}$ [mm]
r_5	$-2.1720 * 10^{-5}$ [mm]	$-2.1624 * 10^{-5}$ [mm]	0.0374 [mm]

Tabella 8 - Centri di gravità dei bracci

Tensori di inerzia rispetto al baricentro (in lb * in²):

Link 1

$I_{xx} = 310.312220$	$I_{xy} = 1.105060$	$I_{xz} = 19.286308$
$I_{yx} = 1.105060$	$I_{yy} = 203.481030$	$I_{yz} = 26.606449$
$I_{zx} = 19.286308$	$I_{zy} = 26.606449$	$I_{zz} = 338.299350$

Tabella 9 - Tensori di inerzia rispetto al baricentro link 1

Link 2

$I_{xx} = 12.195114$	$I_{xy} = -0.091890$	$I_{xz} = 0.066511$
$I_{yx} = -0.091890$	$I_{yy} = 58.206944$	$I_{yz} = -0.023199$
$I_{zx} = 0.066511$	$I_{zy} = -0.023199$	$I_{zz} = 54.435408$

Tabella 10 - Tensori di inerzia rispetto al baricentro link 2

Link 3

$I_{xx} = 7.170433$	$I_{xy} = -0.590397$	$I_{xz} = -0.290830$
$I_{yx} = -0.590397$	$I_{yy} = 62.564072$	$I_{yz} = -0.007019$
$I_{zx} = -0.290830$	$I_{zy} = -0.007019$	$I_{zz} = 60.430655$

Tabella 11 - Tensori di inerzia rispetto al baricentro link 3

Link 4

$I_{xx} = 0.295557$	$I_{xy} = 0.000000$	$I_{xz} = 0.002961$
$I_{yx} = 0.000000$	$I_{yy} = 0.301025$	$I_{yz} = -0.000004$
$I_{zx} = 0.002961$	$I_{zy} = -0.000004$	$I_{zz} = 0.257096$

Tabella 12 - Tensori di inerzia rispetto al baricentro link 4

Link 5

$I_{xx} = 0.011029$	$I_{xy} = -0.000008$	$I_{xz} = -0.000016$
$I_{yx} = -0.000008$	$I_{yy} = 0.010930$	$I_{yz} = -0.000016$
$I_{zx} = -0.000016$	$I_{zy} = -0.000016$	$I_{zz} = 0.006095$

Tabella 13 - Tensori di inerzia rispetto al baricentro link 5

Tensori di inerzia rispetto al sistema di riferimento (in $lb * in^2$):

Link 1

$I_{xx} = 2409.049100$	$I_{xy} = 0.823974$	$I_{xz} = 378.865510$
$I_{yx} = 0.823974$	$I_{yy} = 2363.823800$	$I_{yz} = 28.247046$
$I_{zx} = 378.865510$	$I_{zy} = 28.247046$	$I_{zz} = 399.907820$

Tabella 14 - Tensori di inerzia rispetto al sistema di riferimento link 1

Link 2

$I_{xx} = 12.195258$	$I_{xy} = -0.091571$	$I_{xz} = -0.053561$
$I_{yx} = -0.091571$	$I_{yy} = 158.504410$	$I_{yz} = -0.023198$
$I_{zx} = -0.053561$	$I_{zy} = -0.023198$	$I_{zz} = 154.732730$

Tabella 15 - Tensori di inerzia rispetto al sistema di riferimento link 2

Link 3

$I_{xx} = 7.189069$	$I_{xy} = 0.403555$	$I_{xz} = -0.164676$
$I_{yx} = 0.403555$	$I_{yy} = 116.430380$	$I_{yz} = -0.009347$
$I_{zx} = -0.164676$	$I_{zy} = -0.009347$	$I_{zz} = 114.315000$

Tabella 16 - Tensori di inerzia rispetto al sistema di riferimento link 3

Link 4

$I_{xx} = 0.296359$	$I_{xy} = 0.000000$	$I_{xz} = 0.002130$
$I_{yx} = 0.000000$	$I_{yy} = 0.302687$	$I_{yz} = -0.000004$
$I_{zx} = 0.002130$	$I_{zy} = -0.000004$	$I_{zz} = 0.257956$

Tabella 17 - Tensori di inerzia rispetto al sistema di riferimento link 4

Link 5

$I_{xx} = 0.097081$	$I_{xy} = -0.000008$	$I_{xz} = 0.000034$
$I_{yx} = -0.000008$	$I_{yy} = 0.096983$	$I_{yz} = 0.000034$
$I_{zx} = 0.000034$	$I_{zy} = 0.000034$	$I_{zz} = 0.006095$

Tabella 18 - Tensori di inerzia rispetto al sistema di riferimento link 5

I rapporti di trasmissione:

$$K_r = \begin{bmatrix} 72 & 0 & 0 & 0 & 0 \\ 0 & 72 & 0 & 0 & 0 \\ 0 & 0 & 72 & 0 & 0 \\ 0 & 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 & 8 \end{bmatrix}$$

Ed i limiti delle variabili di giunto:

Giunto	Limite inferiore [rad]	Limite superiore [rad]
1	-3.05433	3.05433
2	-1.5708	0.3491
3	-0.436332	1.5708
4	-1.91986	1.91986
5	-3.1416	3.1416

Tabella 19 - Limiti delle variabili di giunto

Definiti i parametri elettrici dei motori e meccanici del manipolatore, sono stati definiti i parametri dei controllori, in particolare il regolatore PI di corrente e le matrici proporzionali e derivative per il controllo a dinamica inversa.

PI di corrente tarato secondo il metodo del modulo ottimo:

Parametro	Valore	Descrizione
t_{iisa}	$4 \cdot 10^{-4}$ [s]	Costante di tempo
K_{pisa}	$6 \cdot 10^{-4}$ [adimensionale]	Costante proporzionale
K_{iisa}	1.5	Costante derivativa

Tabella 20 - Parametri PI di corrente

Tali valori sono stati ottenuti nel seguente modo:

$$t_{iisa} = T_a \quad (41)$$

$$K_{pisa} = \frac{R_a * t_{iisa}}{2} \quad (42)$$

$$K_{iisa} = \frac{K_{pisa}}{t_{iisa}} \quad (43)$$

Mentre per il controllo a dinamica inversa:

Parametro	Valore	Descrizione
ω_{n1}	8 [rad/s]	Pulsazione naturale 1
ω_{n2}	23 [rad/s]	Pulsazione naturale 2
ω_{n3}	35 [rad/s]	Pulsazione naturale 3
ω_{n4}	10 [rad/s]	Pulsazione naturale 4
ω_{n5}	10 [rad/s]	Pulsazione naturale 5
δ	0.7071	Coefficiente di smorzamento

Tabella 21 - Parametri controllo a dinamica inversa

Le matrici proporzionali e derivative sono:

$$K_p = \begin{bmatrix} 64 & 0 & 0 & 0 & 0 \\ 0 & 529 & 0 & 0 & 0 \\ 0 & 0 & 1225 & 0 & 0 \\ 0 & 0 & 0 & 100 & 0 \\ 0 & 0 & 0 & 0 & 100 \end{bmatrix}$$

$$K_d = \begin{bmatrix} 11.3137 & 0 & 0 & 0 & 0 \\ 0 & 32.5269 & 0 & 0 & 0 \\ 0 & 0 & 49.4975 & 0 & 0 \\ 0 & 0 & 0 & 14.1421 & 0 \\ 0 & 0 & 0 & 0 & 14.1421 \end{bmatrix}$$

I valori delle matrici diagonali sono stati ottenuti nel seguente modo:

$$K_p = \omega_{n_i}^2$$

$$K_d = 2\delta\omega_{n_i}$$

Infine, sono stati definite le posizioni iniziali e finali nello spazio dei giunti ed è stata generata una traiettoria polinomiale di terzo grado per interpolare le due posizioni. La funzione utilizzata per generare la traiettoria segue le seguenti leggi:

$q(t) = a_3t^3 + a_2t^2 + a_1t + a_0$	Posizione
$\dot{q}(t) = 3a_3t^2 + 2a_2t + a_1$	Velocità
$\ddot{q}(t) = 6a_3t + 2a_2$	Accelerazione

Gli input della funzione comprendono le posizioni iniziali e finali, gli istanti di tempo iniziali e finali, il numero di campioni che costituiscono la traiettoria e, optionalmente, i valori di velocità iniziali e finali (se non specificati posti uguali a zero).

Le posizioni di partenza e arrivo (in radianti) sono le seguenti:

$$q_i = [0, 0, 0, 0, 0]$$

$$q_f = [pi, \frac{pi}{9}, \frac{pi}{2}, -\frac{pi}{2}, -pi]$$

Mentre gli istanti temporali (in secondi) passati alla funzione sono 0 per quello iniziale e 5 per quello finale.

Risultati simulazioni

Simulazione in condizioni normali

Definiti tutti i parametri, è stato possibile eseguire la simulazione della durata di cinque secondi in accordo alla durata della traiettoria definita, e sono stati plottati i grafici relativi alle posizioni e alle velocità angolari misurati dai blocchi *Joint* del modello Simscape del manipolatore, in relazione ai riferimenti.

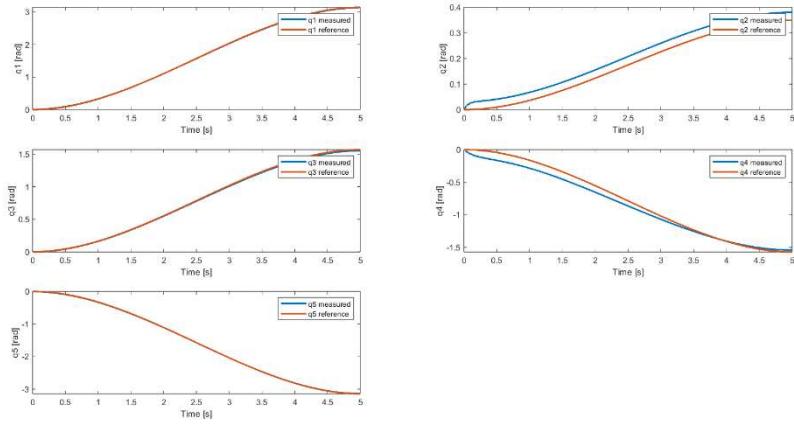


Figura 45 - Posizioni angolari misurate e di riferimento

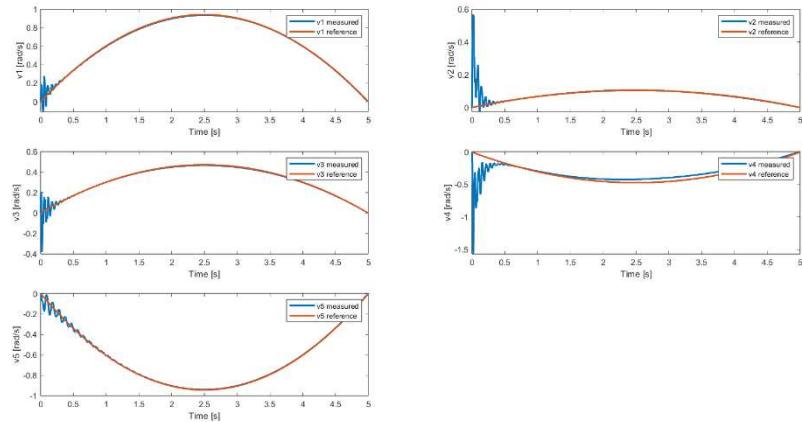


Figura 46 - Velocità angolari misurate e di riferimento

La simulazione mostra come le traiettorie di posizione e velocità sono correttamente inseguite, a meno di piccoli errori dovuti all'approssimazione dei parametri dinamici del modello, che non vanno comunque ad influire in maniera importante le prestazioni in relazione alle specifiche di progetto.

Controllo a dinamica inversa – fault all'inverter del manipolatore

A partire dalla situazione parametrica precedente, sono stati valutati gli effetti che un eventuale malfunzionamento ai diversi componenti del sistema potessero comportare all'esecuzione del task descritto. Per primo, è stato simulato un guasto totale agli inverter che pilotano le tensioni da applicare a ciascun motore: a tale scopo, è stato interposto tra il blocco PI di corrente e il

digital twin del manipolatore uno switch in grado di portare le tensioni da applicare ai motori ad un valore nullo dopo due secondi dall'inizio della simulazione.

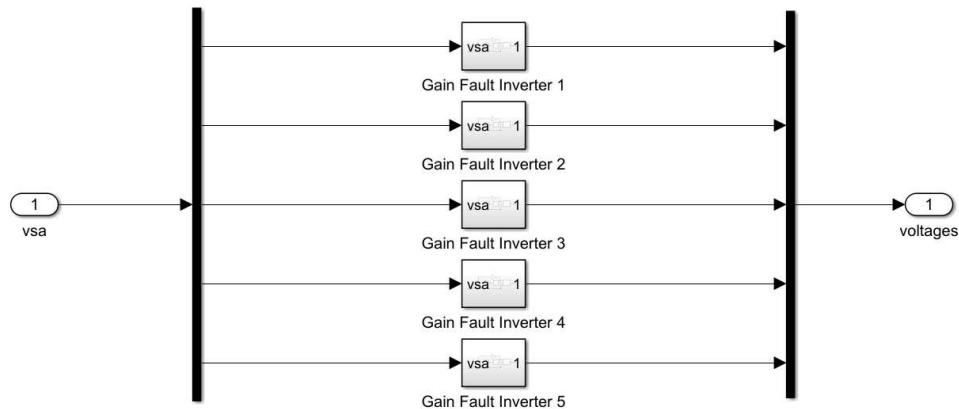


Figura 47 - Simulazione del fault totale agli inverter

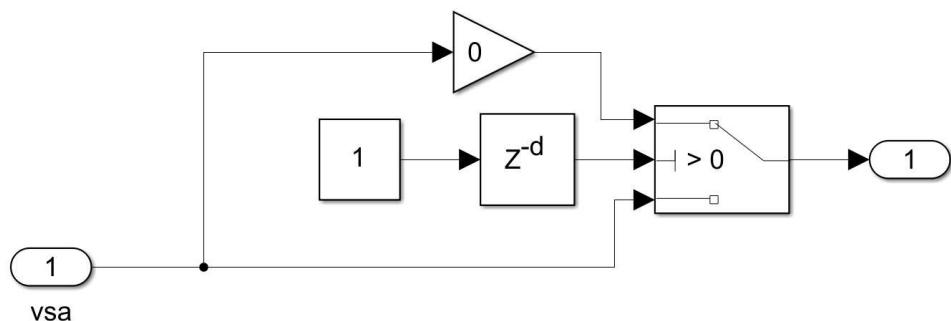


Figura 48 - Modellazione singolo fault all'inverter

Lo switch prevede che venga fornito al manipolatore il segnale generato dal Pi di corrente per i primi due secondi di simulazione, mentre per il restante tempo di simulazione la tensione in uscita sia pari a zero. I risultati della simulazione, con stessi parametri della prima a differenza dell'introduzione del malfunzionamento, sono i seguenti:

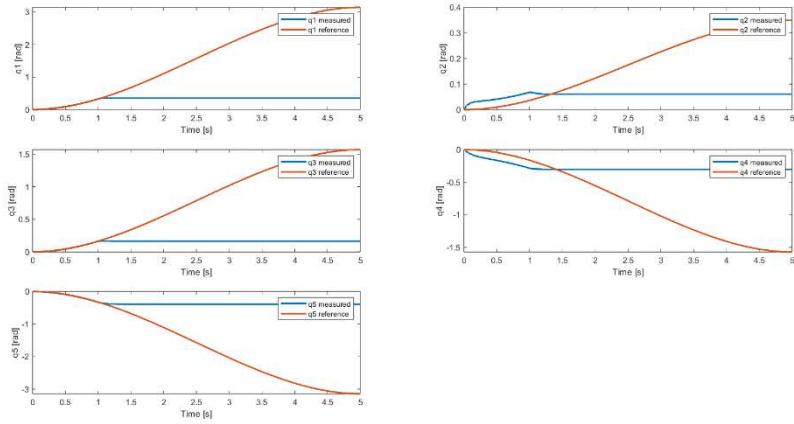


Figura 49 - Posizioni angolari misurate e di riferimento

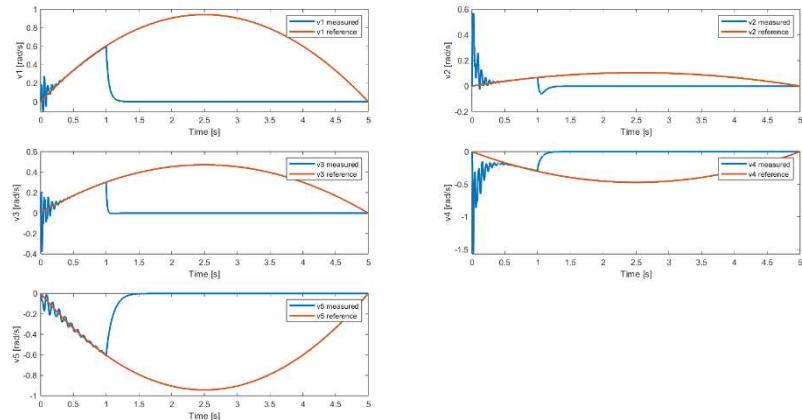


Figura 50 - Velocità angolari misurate e di riferimento

Come era facilmente ipotizzabile, un malfunzionamento di questo tipo prevede che i giunti del manipolatore restano fermi alle loro posizioni nel momento di guasto, che nel nostro caso avviene dopo due secondi dall'inizio della simulazione.

Controllo a dinamica inversa – fault ai sensori di posizione del manipolatore

Un altro caso di malfunzionamento riguarda un segnale di disturbo agli encoder che misurano la posizione angolare dei motori: in questo caso, essendo nel modello simulato i sensori simulati come se fossero posizionati direttamente sul giunto e non sul motore, il segnale nel modello simulato da

andare a modificare riguarda la posizione misurata dal digital twin del manipolatore, in particolare dal blocco *Joint* per ogni giunto. Per simulare il disturbo, è stato implementato uno switch come nel caso precedente, il quale somma un disturbo gaussiano bianco a media nulla al segnale originale dopo due secondi dall'inizio della simulazione. Nel blocco utilizzato per generare il rumore bianco viene specificata l'ampiezza della PSD (Power Spectral Density) e il tempo di campionamento.

$$\text{Noise power} = 0.001$$

$$\text{Sample time} = 0.001$$

I risultati della simulazione sono i seguenti:

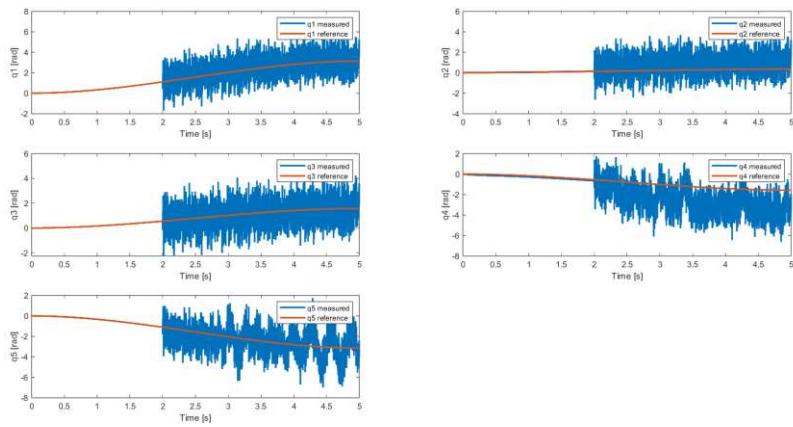


Figura 51 - Posizioni angolari misurate e di riferimento

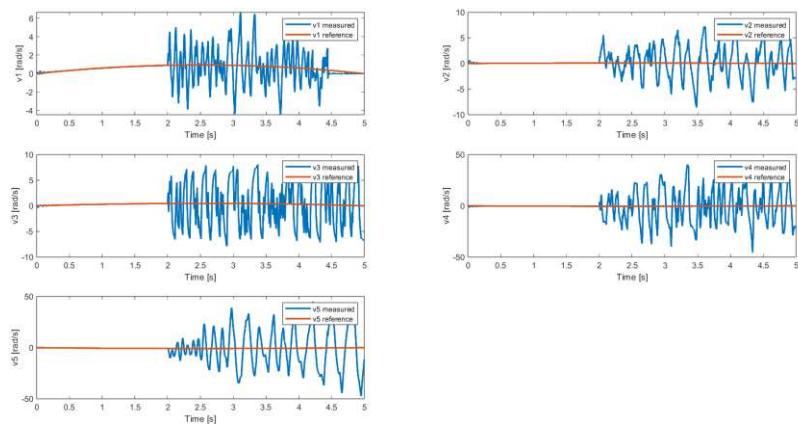


Figura 52 - Velocità angolari misurate e di riferimento

Si nota come successivamente al fault, le posizioni misurate sono affette dal disturbo e vanno ad influenzare le prestazioni del controllo in maniera importante, in quanto i valori di posizione e velocità sono posti in retroazione per il corretto calcolo dei riferimenti e delle compensazioni dinamiche.

Controllo a dinamica inversa – fault sul microcontrollore all'applicazione dei riferimenti di posizione, velocità e accelerazione

Come ultimo fault considerato, è stata ipotizzata un'amplificazione anomala dei riferimenti di posizione, velocità e accelerazione. A tal proposito, come nel caso del malfunzionamento agli inverter, tramite switch sono stati amplificati tramite blocco *Gain* i segnali di riferimento dopo due secondi dall'inizio della simulazione. I risultati sono mostrati nelle seguenti figure.

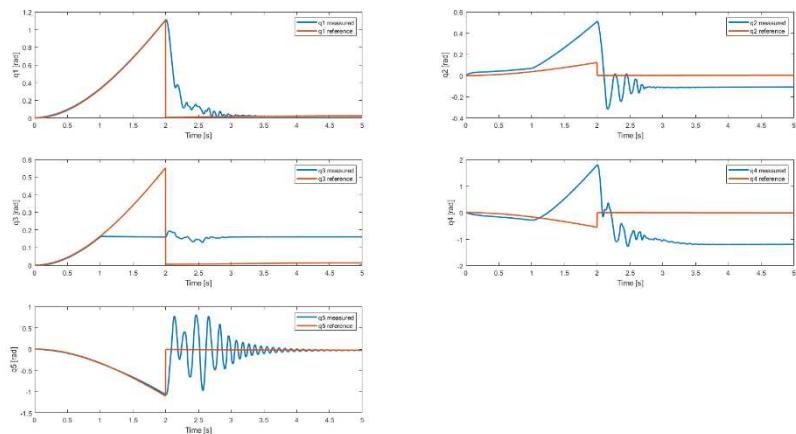


Figura 53 - Posizioni misurate e di riferimento

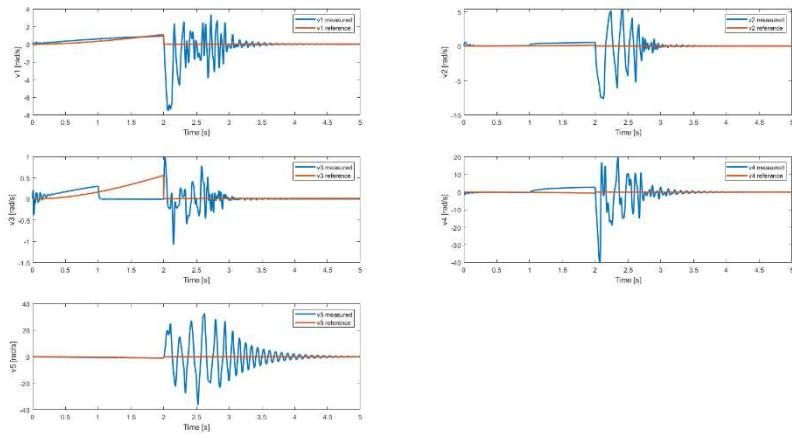


Figura 54 - Velocità misurate e di riferimento

Si nota come il cambio dei riferimenti porti il controllo a seguire le nuove traiettorie di posizione, velocità e accelerazione.

I malfunzionamenti descritti fin ora portano quindi ad una situazione di imprevedibilità del movimento del manipolatore e quindi ad un potenziale pericolo per un operatore umano o per l'ambiente di lavoro nel caso di operazioni collaborative; pertanto, le seguenti simulazioni con l'implemento del sistema di check ed intervento a livelli proposto saranno utili a verificare l'efficacia di tale meccanismo di controllo.

Controllo a dinamica inversa – test del sistema di check e intervento delle protezioni su fault all'inverter

Per testare l'efficacia del sistema di check e intervento proposto nei paragrafi precedenti, sono state simulate le situazioni di fault precedenti con l'aggiunta del blocco di checkpoint, in parallelo al sistema, e lo switch di intervento, posto tra il controllore PI di corrente e il manipolatore, così da applicare delle tensioni nulle in caso di rilevamento del fault. I risultati delle simulazioni seguenti sono stati ottenuti considerando dei valori di threshold per la rilevazione del valore medio dell'errore, su un buffer di 50 campioni, pari a:

$$\epsilon_1 = pi * 0.02;$$

$$\epsilon_2 = pi/9 * 0.02;$$

$$\epsilon_3 = pi/2 * 0.02;$$

$$\epsilon_4 = pi/2 * 0.02;$$

$$\epsilon_5 = pi * 0.02;$$

Di seguito, sono mostrati i risultati della simulazione con tali parametri; oltre ai grafici di posizione e velocità angolare dei giunti, sono mostrati il grafico dell'andamento dell'errore tra il livello 1 e il livello 2 del sistema di check e quello relativo al flag di intervento.

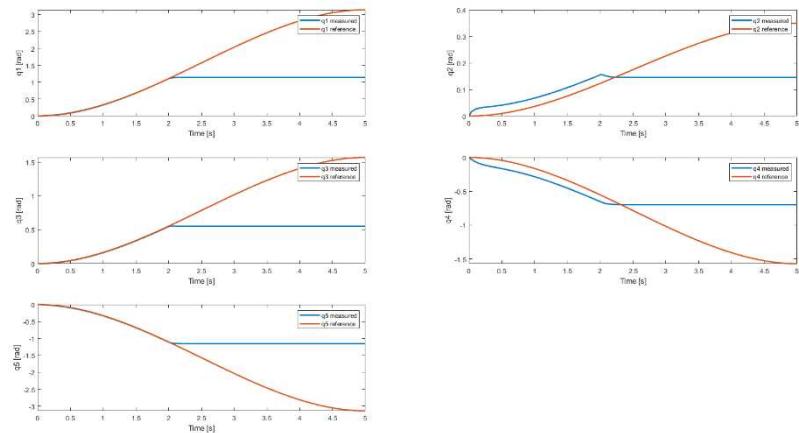


Figura 55 - Posizioni misurate e di riferimento

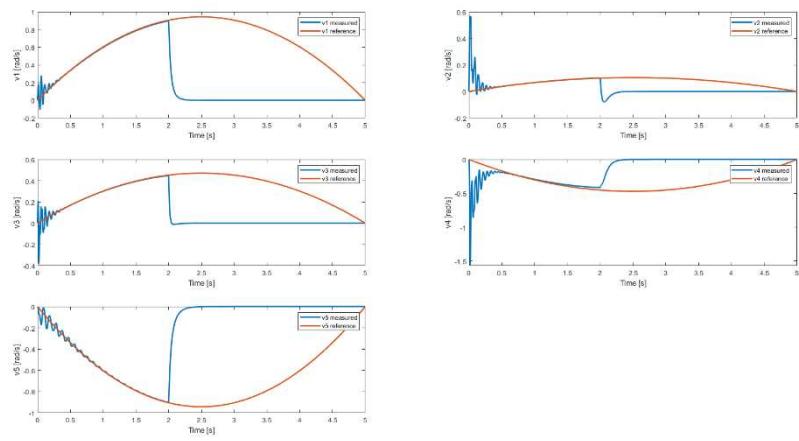


Figura 56 - Velocità misurate e di riferimento

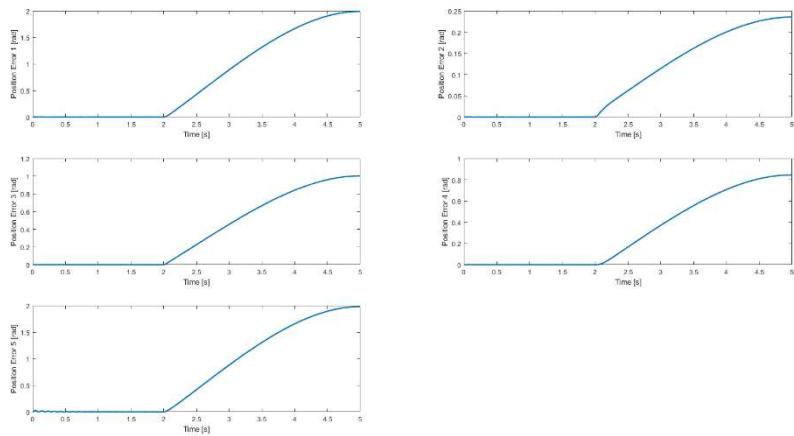


Figura 57 - Errore assoluto tra livello 1 e livello 2

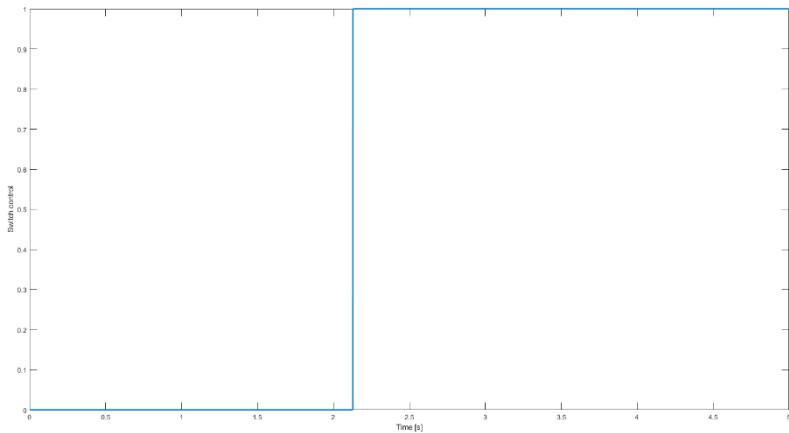


Figura 58 - Flag di intervento delle protezioni

Come è possibile notare, il malfunzionamento viene correttamente rilevato tramite il sistema a livelli: un fault all'inverter nel primo livello (che simula il sistema reale) causa una perdita dell'inseguimento delle traiettorie di posizione e velocità, mentre il livello 2, costituito dal digital twin, simula il normale funzionamento in assenza di problemi. L'errore di posizione tra i due livelli cresce nel momento in cui avviene il malfunzionamento e fa attivare il segnale di flag che impone le tensioni nulle ai motori del manipolatore. L'intervento avviene dopo circa 150ms dal fault rendendo il sistema performante in termini di responsività ed efficienza. Di seguito, il sistema sarà testato per altri tipi di malfunzionamenti gravi a tutte le componenti.

Controllo a dinamica inversa – test del sistema di check e intervento delle protezioni su fault ai sensori di posizione

Come per il caso precedente, è stato testato il sistema di check e di intervento per il fault legato ad un disturbo ai sensori. I risultati della simulazione sotto le stesse condizioni del test precedente sono i seguenti.

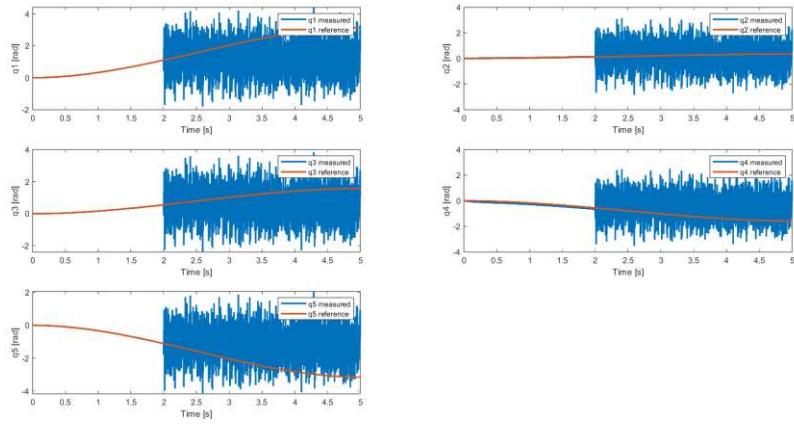


Figura 59 - Posizioni misurate e di riferimento

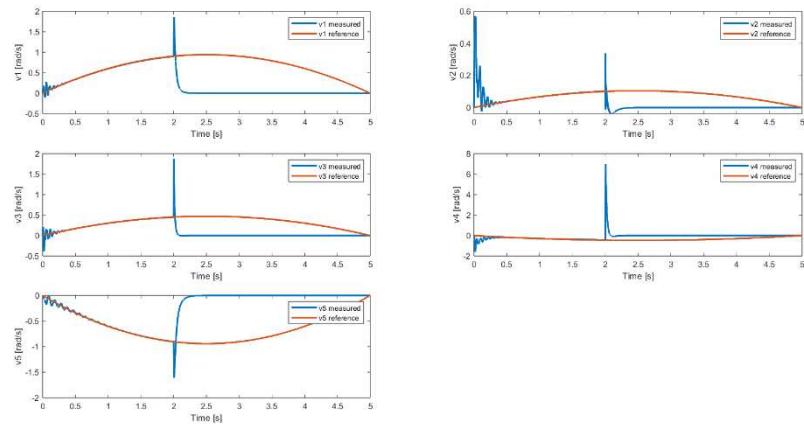


Figura 60 - Velocità misurate e di riferimento

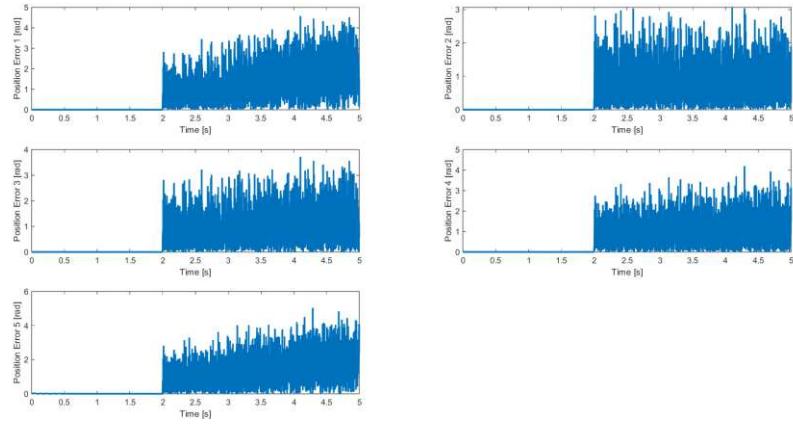


Figura 61 - Errore assoluto tra livello 1 e livello 2

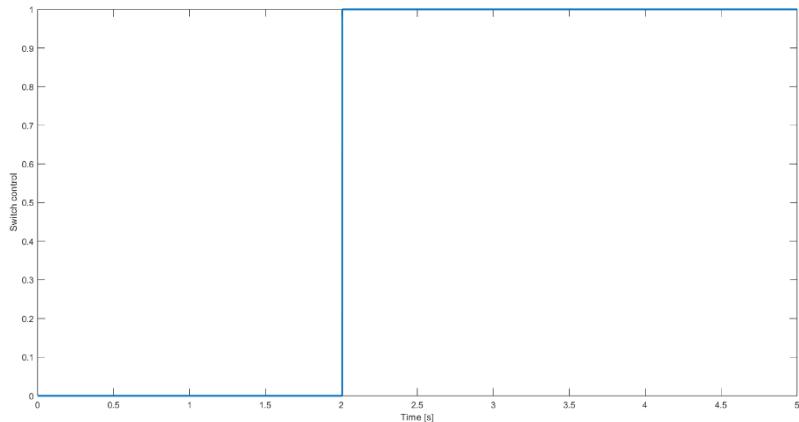


Figura 62 - Flag di intervento delle protezioni

Anche in questo caso l'intervento delle protezioni è efficace, e risulta essere anche più performante in quanto le tensioni ai motori vengono azzerati in tempi più rapidi rispetto al fault agli inverter. Ciò è dovuto all'effetto diretto che un disturbo ai sensori ha sul sistema di check, in quanto il suo funzionamento è strettamente legato alla posizioni misurate dagli encoder e quelle stimate dal digital twin.

Controllo a dinamica inversa – test del sistema di check e intervento delle protezioni su fault ai segnali di riferimento.

Infine, è stato testato il sistema nel caso di fault ai segnali di riferimento di posizione, velocità e accelerazione.

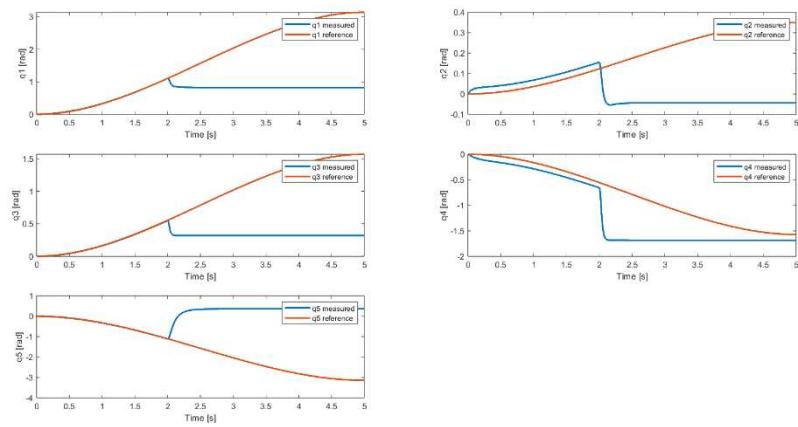


Figura 63 - Posizioni misurate e di riferimento

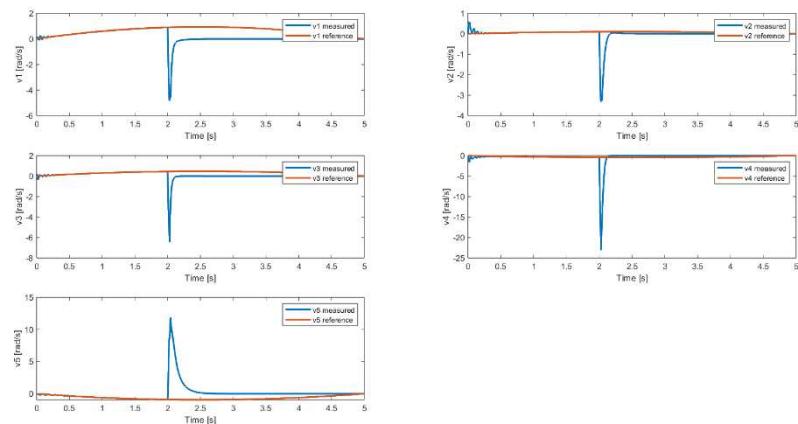


Figura 64 - Velocità misurate e di riferimento

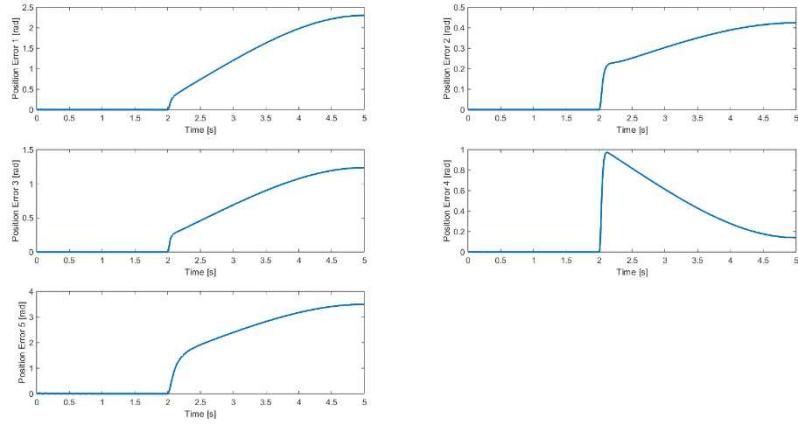


Figura 65 - Errore assoluto tra livello 1 e livello 2

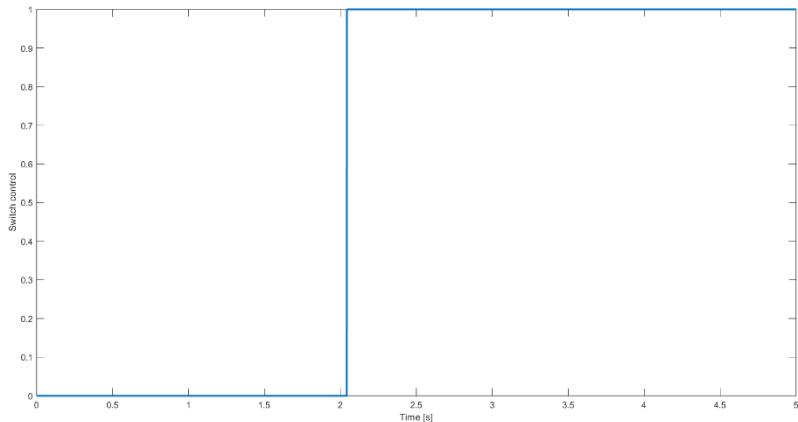


Figura 66 - Flag di intervento delle protezioni

Come è possibile notare dai grafici, anche in questo caso l'intervento delle protezioni risulta essere efficace e tempestivo. Di seguito, saranno mostrati gli effetti che un fault ad un singolo motore (inverter o sensore) hanno sul sistema e sarà testato il metodo proposto per il ricalcolo della traiettoria.

Controllo a dinamica inversa – fault al singolo inverter

Per valutare gli effetti che un malfunzionamento ad un singolo inverter ha sul sistema di controllo, sono state effettuate cinque simulazioni, una per giunto, e sono stati ricavati gli andamenti di posizione misurate e di riferimento. Di seguito, sono mostrati in figura i risultati degli scenari appena descritti.

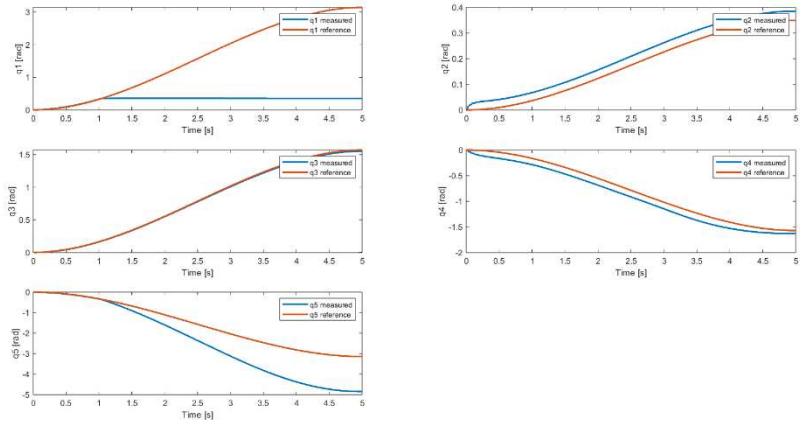


Figura 67 - Posizioni - fault giunto 1

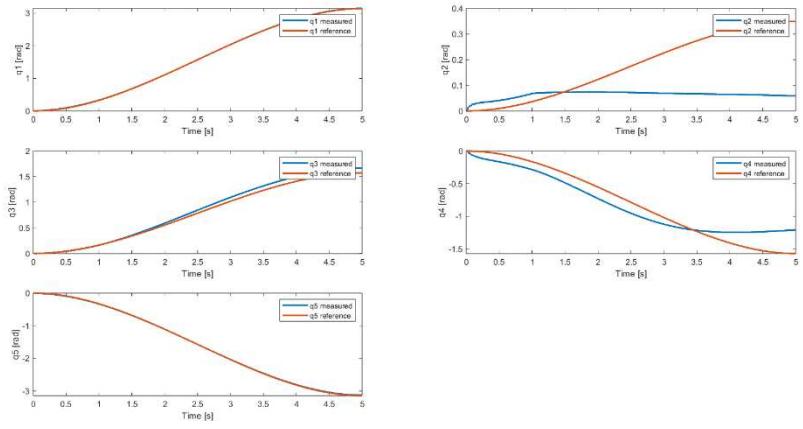


Figura 68 - Posizioni - fault giunto 2

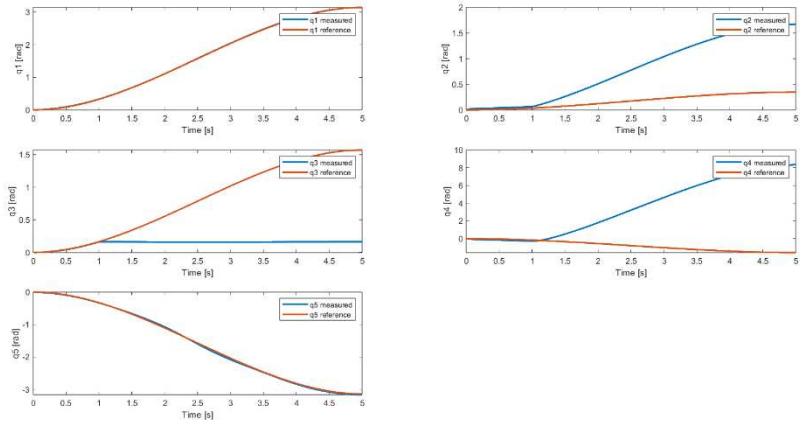


Figura 69 - Posizioni - fault giunto 3

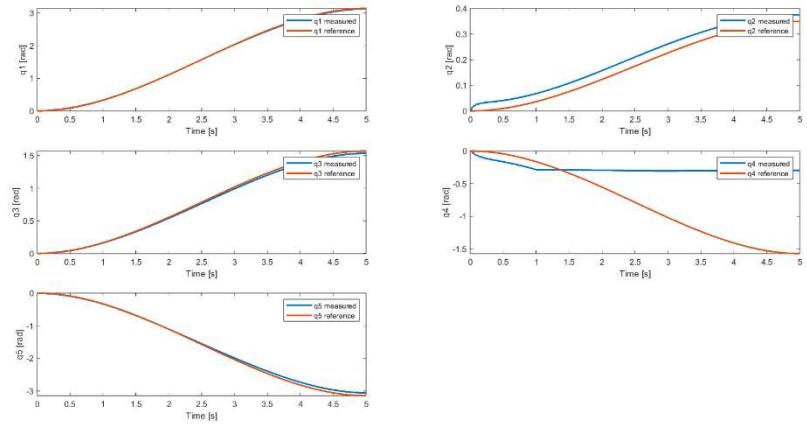


Figura 70 - Posizioni - fault giunto 4

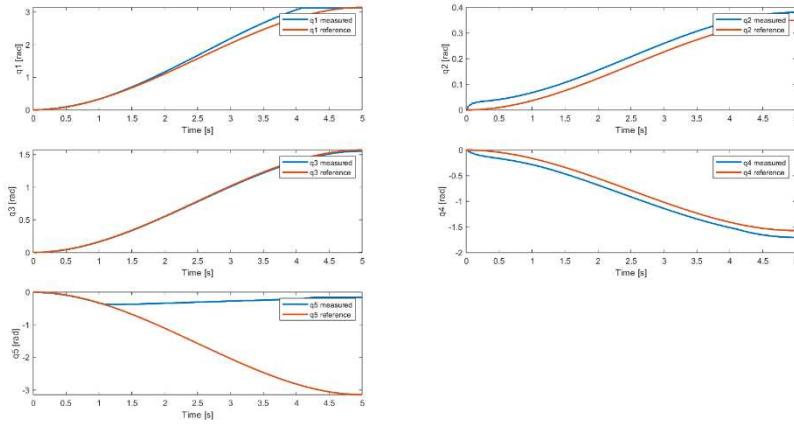


Figura 71 - Posizioni - fault giunto 5

Come è possibile notare, un malfunzionamento ad uno dei giunti influenza, per via della dinamica del sistema e del tipo di controllo utilizzato, anche altri giunti. L'intervento proposto in questo caso prevede il ricalcolo della traiettoria tramite metodo numerico proposto nel capitolo precedente.

Controllo a dinamica inversa – fault al singolo motore, sensore o riferimento e ricalcolo della traiettoria

Il metodo utilizzato per questi test prevede di ricavare un identificativo specifico per ogni giunto del manipolatore in caso di guasto, così da risalire alla componente in fault esatta per attuare misure di intervento meno restrittive. Ottenuto l'identificativo, si procede mettendo in pausa la simulazione in caso di fault, e in base all'identificativo ricalcolare la traiettoria tramite metodi numerici di cinematica inversa, considerando un manipolatore surrogato identico all'originale nel quale il giunto guasto resta bloccato alla posizione misurata al momento del malfunzionamento. Tale approccio è particolarmente utile a capire quali fossero i limiti imposti dal sistema di controllo a dinamica inversa nello spazio dei giunti, specialmente in caso di compensazioni dinamiche. Di seguito, sono mostrati i grafici in termini di posizioni angolari del manipolatore adottando il ricalcolo della traiettoria tramite metodi numerici, uno per ogni giunto guasto, ipotizzando il malfunzionamento all'inverter dei motori, in questo caso dopo un secondo dall'inizio della simulazione.

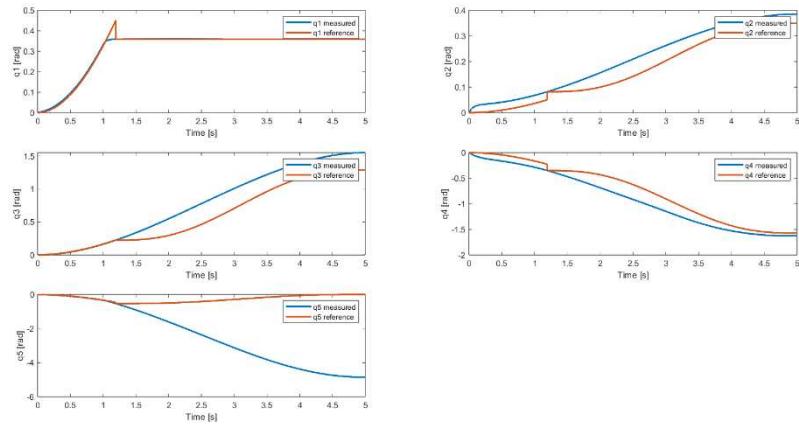


Figura 72 - Posizioni - fault giunto 1 e ricalcolo della traiettoria

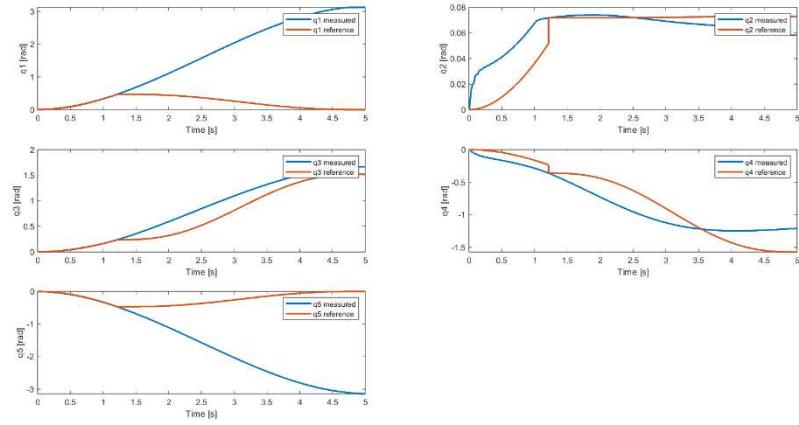


Figura 73 - Posizioni - fault giunto 2 e ricalcolo della traiettoria

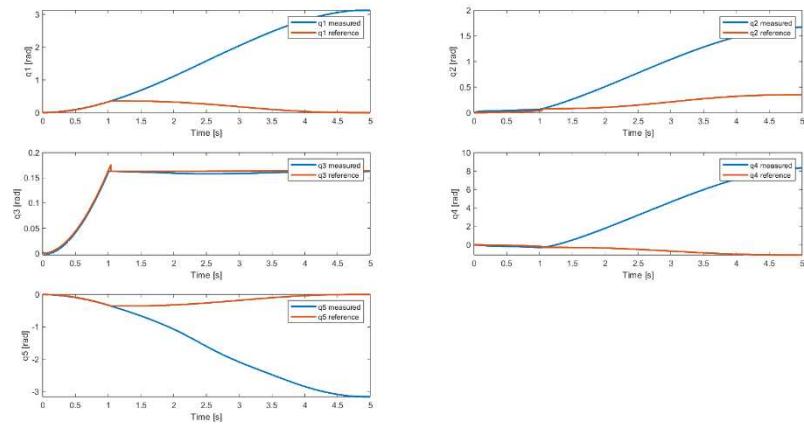


Figura 74 - Posizioni - fault giunto 3 e ricalcolo della traiettoria

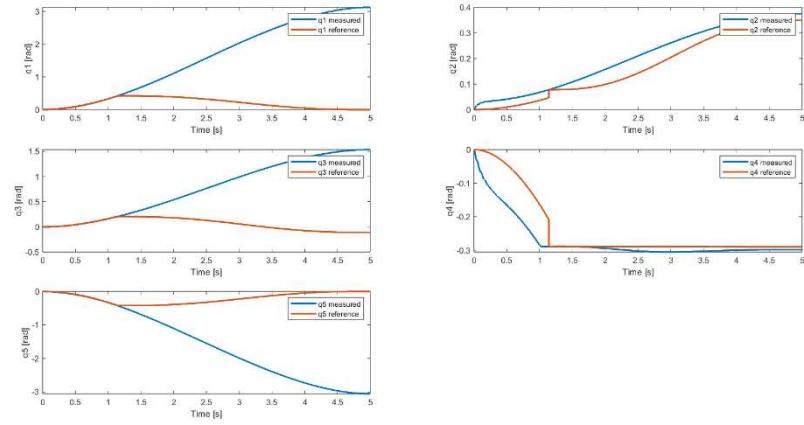


Figura 75 - Posizioni - fault giunto 4 e ricalcolo della traiettoria

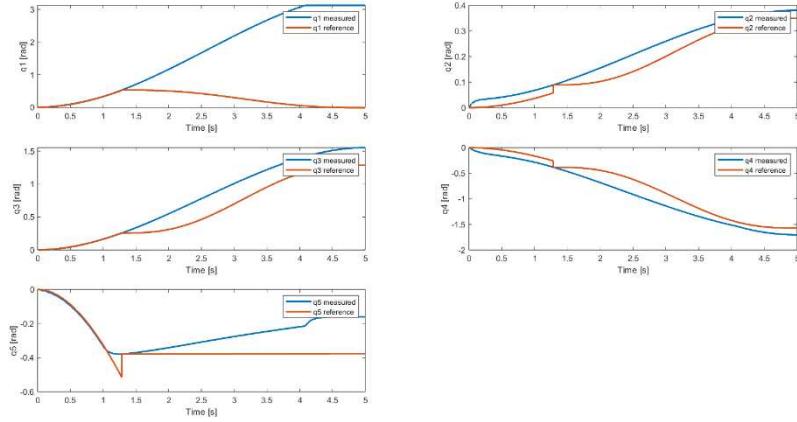


Figura 76 - Posizioni - fault giunto 5 e ricalcolo della traiettoria

È evidente come in molti casi, il ricalcolo della traiettoria risulta essere inefficace; ciò non è solamente dovuto alle influenze dinamiche discusse precedentemente, ma anche dal fatto che per ogni task, e quindi per ogni traiettoria, bisogna considerare la possibilità del manipolatore privato del giunto in fault di raggiungere la posizione finale desiderata. Ad esempio, muoversi sul piano X-Y per il manipolatore in caso di malfunzionamento del primo giunto risulta essere impossibile, poiché la zona di lavoro in quel particolare caso si riduce ad un piano nello spazio operativo individuato dalla posizione angolare del giunto al momento del malfunzionamento. In altri casi invece, come per i giunti 2, 3 e 4, esistono soluzioni alternative che permettono di sfruttare la ridondanza per il determinato task e di raggiungere la posizione finale desiderata.

Alla luce di tali considerazioni, è stato testato il controllo del manipolatore tramite regolatori PID integrato con il sistema di check a livelli discusso, implementato e testato precedentemente.

Controllo PID – simulazione in assenza di fault

Lo schema di controllo in esame discusso precedentemente prevede l'inizializzazione degli stessi parametri riguardanti il manipolatore e il controllore PI di corrente, ed in aggiunta sono stati definiti i parametri dei controllori PID di posizione e quelli relativi alla generazione delle traiettorie in tempo reale tramite metodo della pseudo-inversa per il calcolo della cinematica inversa.

I parametri definiti per questo nuovo sistema di controllo comprendono le costanti proporzionali, derivative e integrali, oltre al coefficiente di filtro per la costante derivativa, per i regolatori di posizione PID. Inoltre, sono definiti i parametri per l'inversione cinematica e, infine, le traiettorie prese in considerazione per verificare la ridondanza rispetto al task del manipolatore.

I parametri relativi al metodo della pseudo-inversa per l'inversione cinematica sono i seguenti:

Parametro	Valore	Descrizione
t_s	0.001 [s]	Tempo di campionamento
num_step	5000 [adimensionale]	Campioni totali
t_d	5 [s]	Durata simulazione
K_a	35 [adimensionale]	Guadagno funzione costo

Inoltre, viene definita una matrice di guadagno diagonale di dimensioni $r \times r$, con r grado di vincolo del task: essendo il task su tre dimensioni, la matrice sarà 3×3 .

$$K_p = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

I valori di range e medi per ogni giunto sono calcolati ed ottenuti a partire da quelli limite descritti precedentemente in radianti:

$$q_{range} = [6.1087, 1.9199, 2.0071, 3.8397, 6.2832]$$

$$q_{avg} = [0, -0.6109, 0.5672, 0, 0]$$

Sono stati valutati due possibili task da assegnare al manipolatore in termini di posizione finale da raggiungere, alla luce delle valutazioni effettuate sulla ridondanza e sulle capacità operative del manipolatore in caso di malfunzionamento di uno dei giunti. A tal proposito, a partire dalla stessa posizione di partenza nello spazio operativo, corrispondente a quella nello spazio dei giunti in caso di configurazione default, sono state definite due posizioni target nello spazio operativo: una che prevede per il manipolatore il movimento obbligatorio del primo giunto per il raggiungimento della posizione finale, mentre la seconda prevede il movimento del manipolatore sul piano verticale identificato dalla posizione di partenza del giunto 1 nello spazio dei giunti. Le posizioni iniziali e finali nello spazio operativo (in metri) sono riportate di seguito:

$$q_{i1} = [0.4050, 0, 0.255]$$

$$q_{i2} = [0.4050, 0, 0.255]$$

$$q_{f1} = [0, 0.4050, 0.255]$$

$$q_{f2} = [0.3, 0, 0.5]$$

A partire da tali valori, sono generate per interpolazione le traiettorie nello spazio dei giunti e nello spazio operativo.

I valori per le costanti proporzionali, integrali, derivative e di filtro di derivazione sono stati ottenuti tramite lo strumento *Auto-tuner*, il quale permette di effettuare una taratura dei controllori di posizione automatica, in base alle specifiche di responsività e robustezza specificate dall'utente. I valori ottenuti sono riportati nella seguente tabella:

Giunto	P	I	D	N
1	2.88	0.23	6.59	1374.23
2	3.22	0.27	6.55	1410.47
3	30.81	8.43	22.27	4908.65
4	8.00	2.30	4.86	4847.05
5	0.08	0.003	0.39	716.45

Tabella 22 - Parametri PID di posizione

Definiti tutti i parametri, è stato possibile eseguire una simulazione del sistema in assenza di malfunzionamenti per verificare il corretto funzionamento del calcolo della cinematica inversa in una situazione di normale funzionamento.

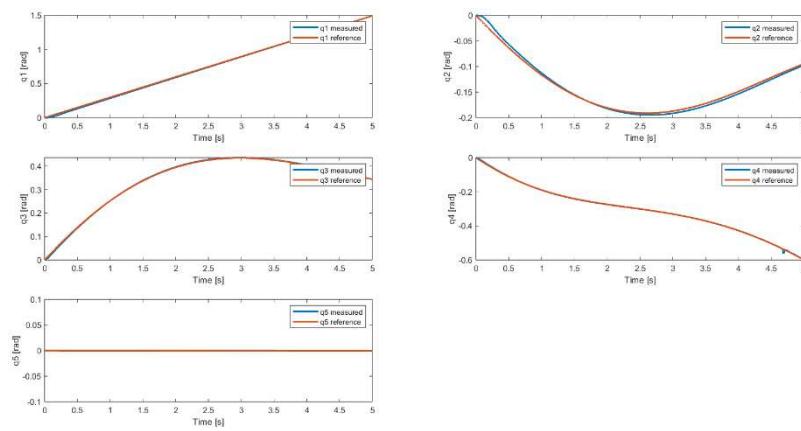


Figura 77 - Posizioni misurate e di riferimento

Metodo della pseudo-inversa su un manipolatore planare a tre bracci

Il metodo della pseudo-inversa per il calcolo della cinematica inversa volta ad ottenere istante per istante le configurazioni per i giunti del manipolatore al fine di seguire una data traiettoria nello spazio operativo è stato testato prima su un manipolatore planare, al fine di applicare poi tale metodo al caso in esame.

Definito il manipolatore tramite la libreria *Peter Corke Robotics Toolbox*, i parametri utili al calcolo tramite pseudo-inversa della cinematica inversa sono analoghi a quelli descritti precedentemente, a differenza dei valori medi e di range per i giunti:

$$q_{range} = [6.2832, 6.2832, 6.2832]$$

$$q_{avg} = [0, 0, 0]$$

Inoltre, la traiettoria planare scelta prevede tali coordinate x-y-z iniziali e finali:

$$q_i = [1.1, 0, 0]$$

$$q_f = [-0.2, -0.4, 0]$$

Con q_i coordinate dell'end effector nella posizione di partenza.

La simulazione effettuata non tiene conto della dinamica del manipolatore, ma serve esclusivamente a valutare l'efficacia del metodo basandosi sulle configurazioni ottenute dalla cinematica inversa in relazione a quelle ottenute per interpolazione, e ad analizzare l'effetto che la funzione costo ha nell'ottimizzazione nel caso di task che permettono di sfruttare la ridondanza.

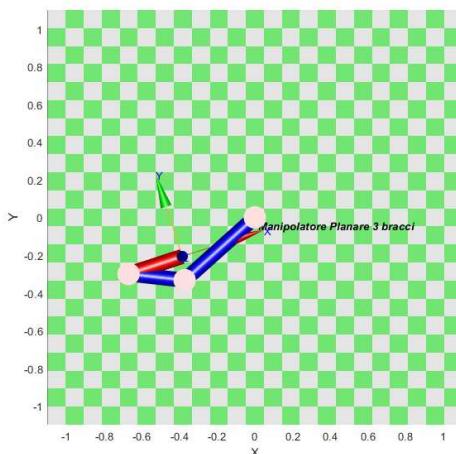


Figura 78 - Configurazione finale ottenuta per interpolazione

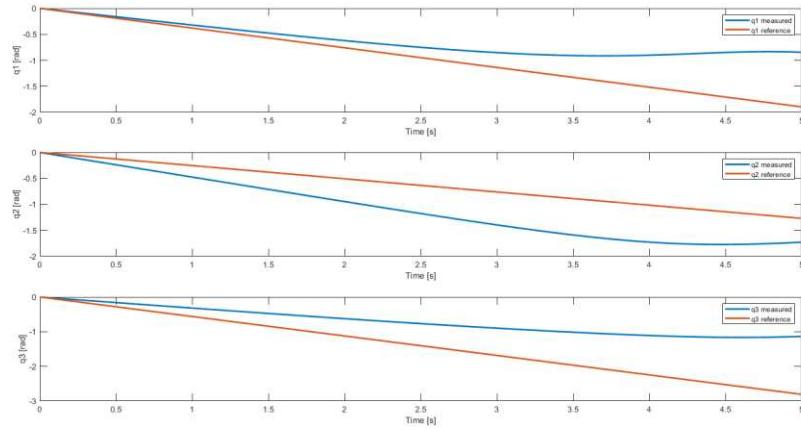


Figura 79 - Posizioni angolari interpolate e calcolate tramite cinematica inversa

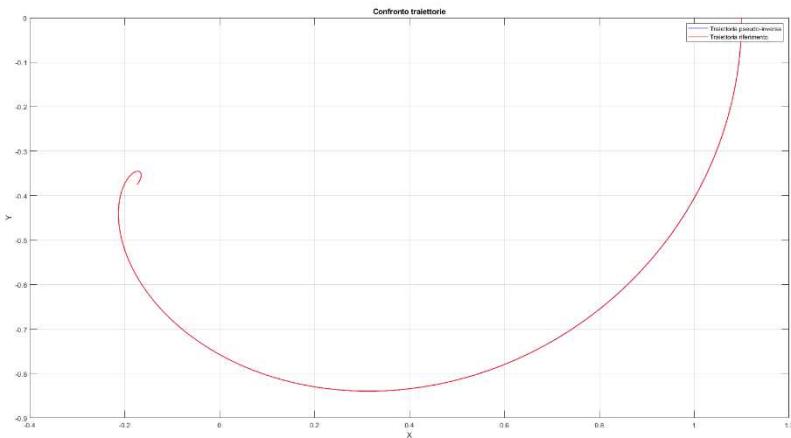


Figura 80 - Traiettoria pseudo-inversa e riferimento

Si nota come, sebbene le traiettorie dell'end effector risultino essere coincidenti, esse sono ottenute mediante configurazioni del manipolatore differenti, mostrando come la ridondanza del manipolatore permetta di ottenere traiettorie identiche con configurazioni diverse in base alle specifiche di progetto.

Controllo PID – fault ai singoli inverter e ricalcolo della traiettoria

Le successive simulazioni prevedono di testare il calcolo real-time della traiettoria tramite metodo della pseudo-inversa, tenendo in considerazione per ogni giunto tre situazioni differenti (assenza di fault, fault e ricalcolo della traiettoria 1 e fault e ricalcolo della traiettoria 2).

Fault giunto 1

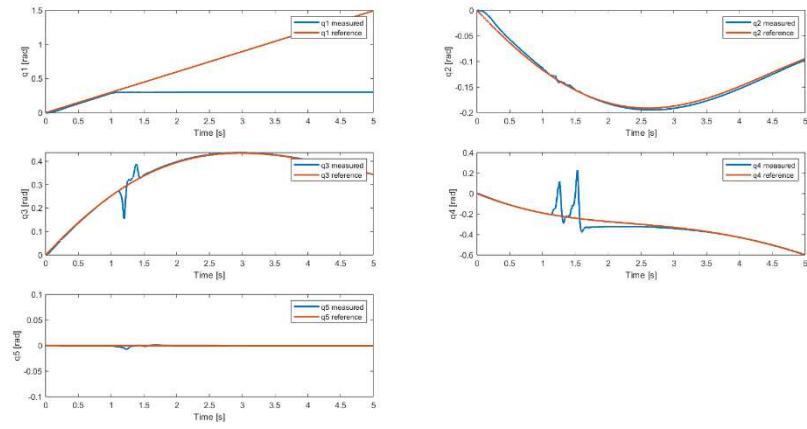


Figura 81 - Posizioni angolari - nessun intervento T1

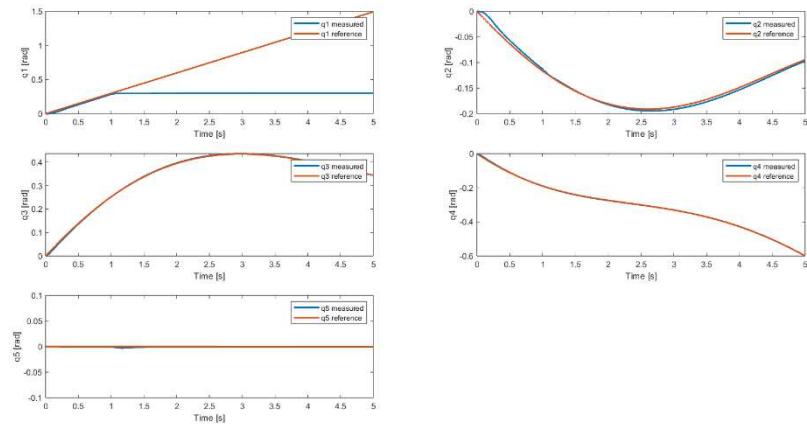


Figura 82 - Posizioni angolari - ricalcolo T1

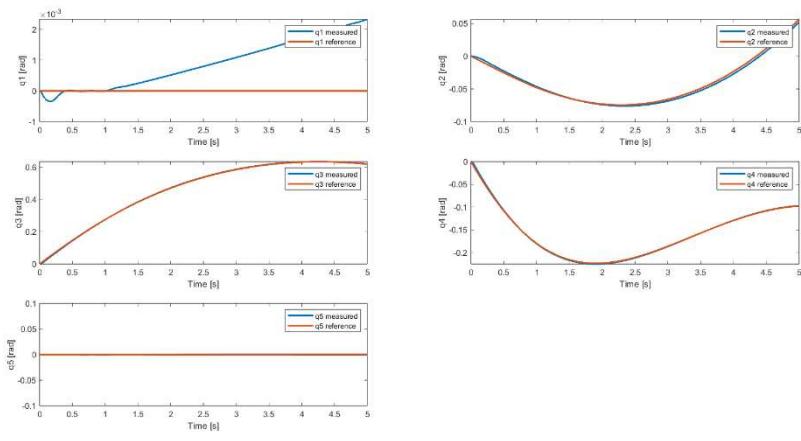


Figura 83 - Posizioni angolari - ricalcolo T2

Fault giunto 2

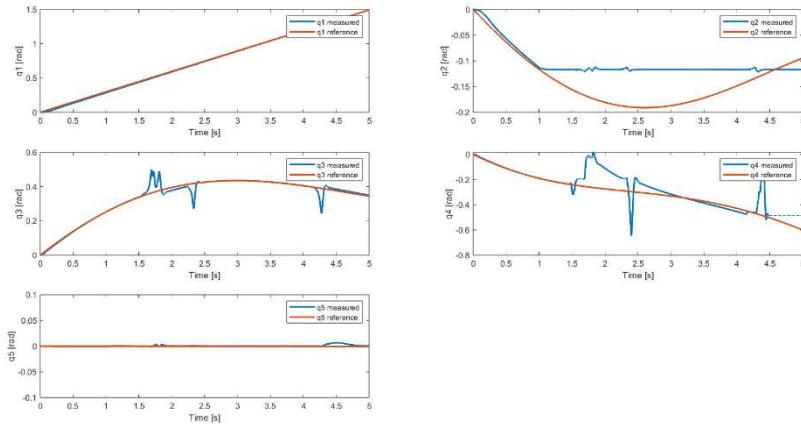


Figura 84 - Posizioni angolari - nessun intervento T1

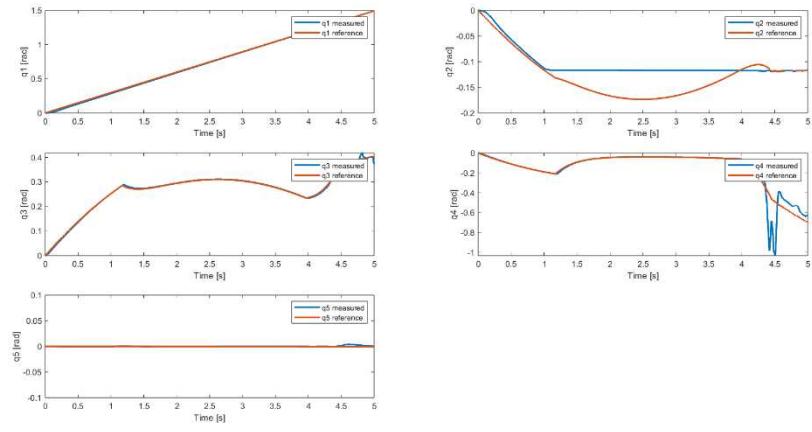


Figura 85 - Posizioni angolari - ricalcolo T1

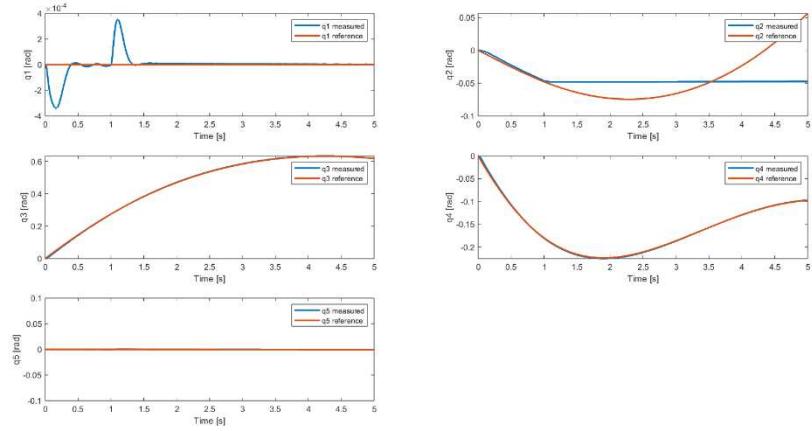


Figura 86 - Posizioni angolari - ricalcolo T2

Fault giunto 3

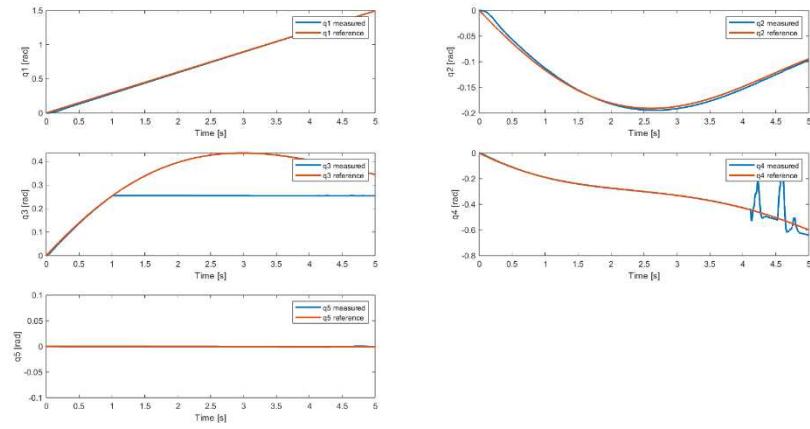


Figura 87 - Posizioni angolari - nessun intervento T1

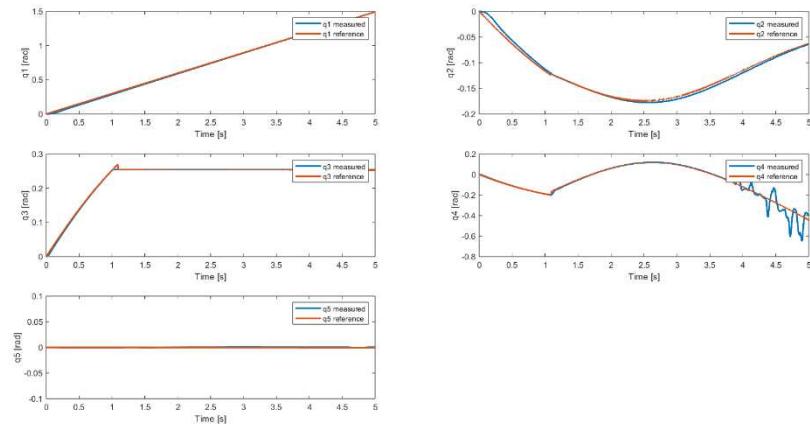


Figura 88 - Posizioni angolari - ricalcolo T1

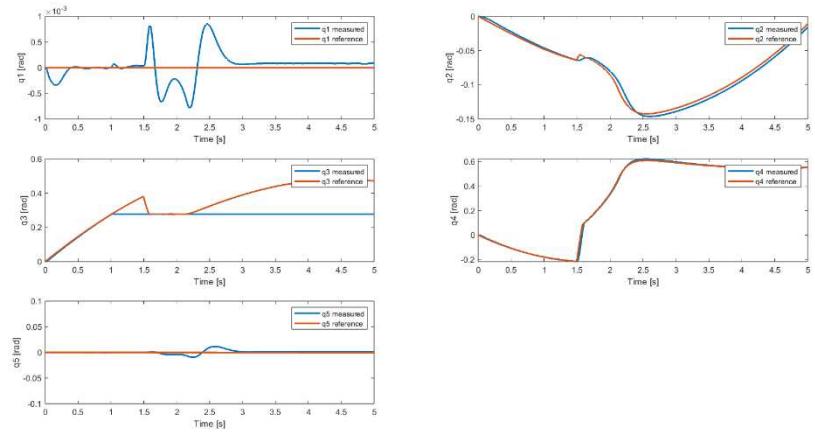


Figura 89 - Posizioni angolari - ricalcolo T2

Fault giunto 4

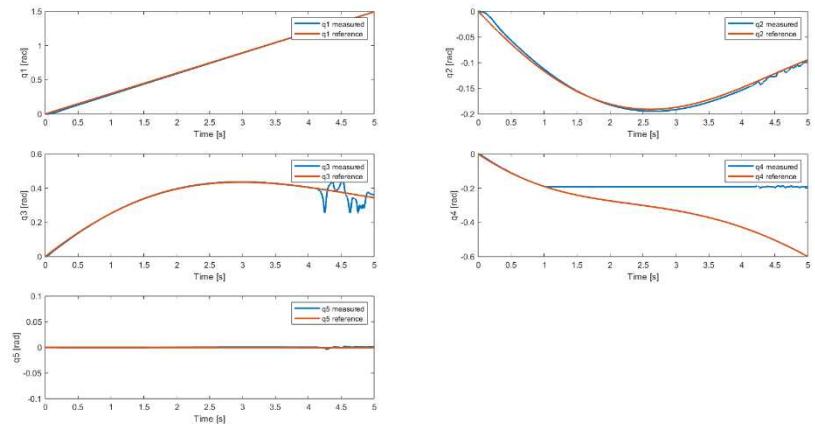


Figura 90 - Posizioni angolari - nessun intervento T1

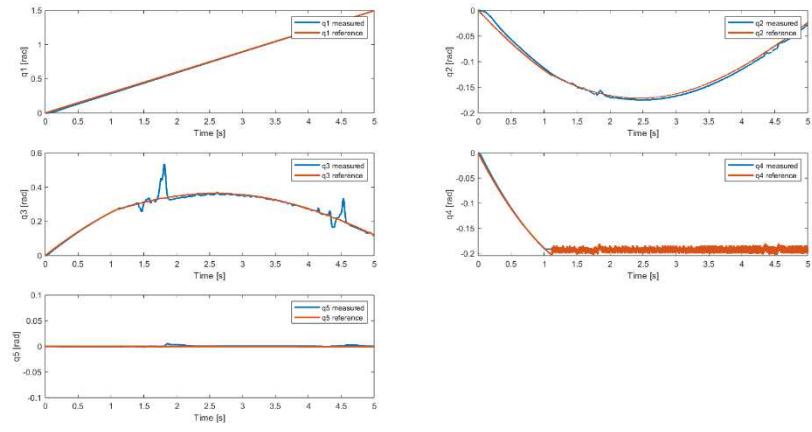


Figura 91 - Posizioni angolari - ricalcolo T1

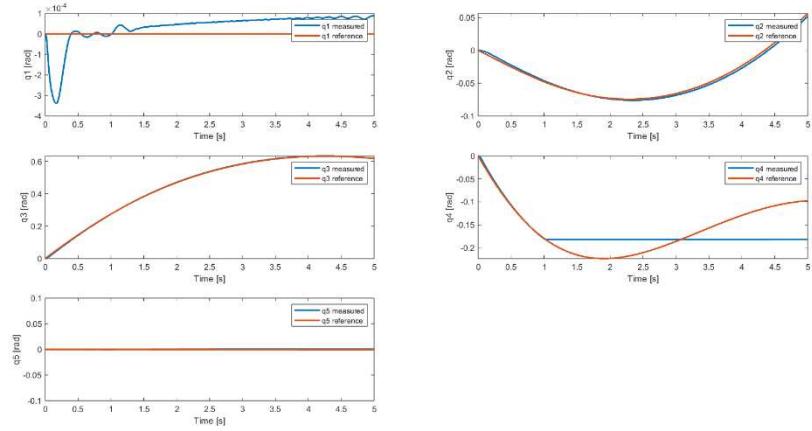


Figura 92 - Posizioni angolari - ricalcolo T2

Fault giunto 5

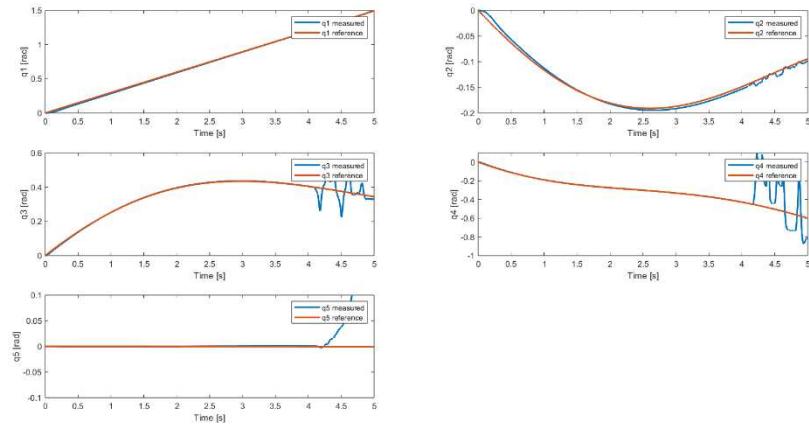


Figura 93 - Posizioni angolari - nessun intervento T1

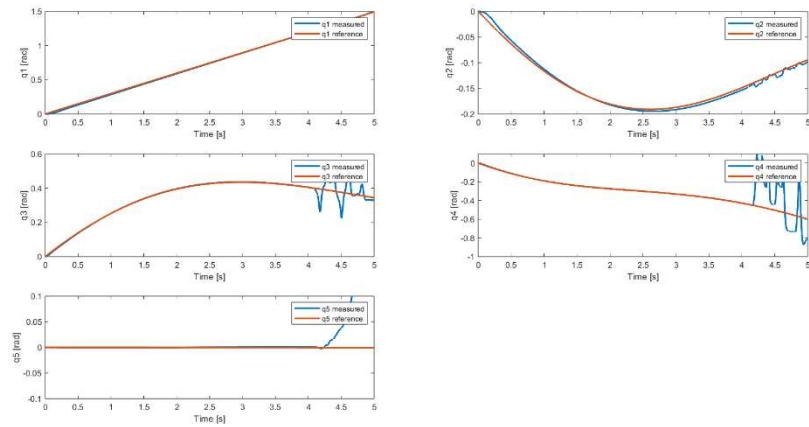


Figura 94 - Posizioni angolari - ricalcolo T1

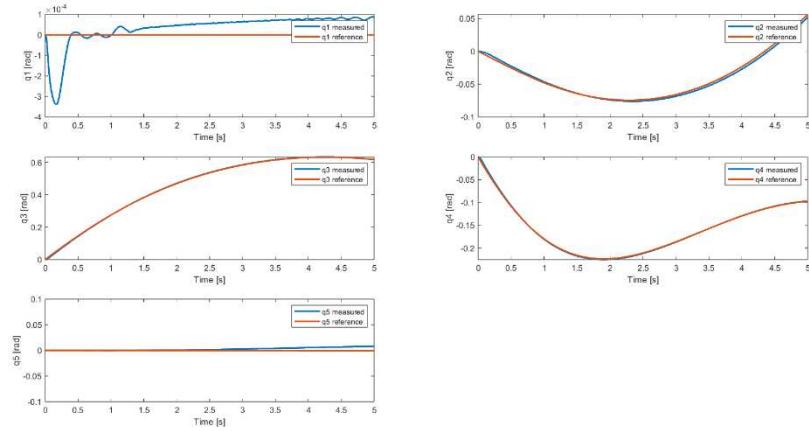


Figura 95 - Posizioni angolari - ricalcolo T2

Alla luce delle simulazioni effettuate, si nota come nel caso in cui la traiettoria rientra nello spazio operativo del manipolatore, anche in mancanza di uno dei giunti, il metodo proposto risulta essere efficace, a meno di qualche perturbazione nella risposta del sistema in vicinanza di singolarità o di mancate ottimizzazioni nel tipo di controllo. Al contrario, nel caso in cui il malfunzionamento ad un particolare giunto non permetta di raggiungere la posizione finale desiderata, il metodo proposto non risulta essere risolutivo. A tal proposito, un altro metodo prevede di portare il manipolatore ad una posizione di sicurezza nel caso in cui la posizione finale risulti essere irraggiungibile; come caso in esame, è stata presa la prima traiettoria come riferimento e un guasto al giunto 1: in tal caso, la posizione finale risulta essere irraggiungibile, perciò una nuova traiettoria viene calcolata e mandata come riferimento al sistema per portare l'end effector in una posizione sicura per eventuali operatori umani nello spazio di lavoro.

Per raggiungere questo obiettivo, è stata implementata una funzione MATLAB che interrompe la simulazione non appena viene rilevato un fault. Qualora il malfunzionamento individuato corrisponda specificamente a quello relativo al primo giunto, la funzione provvede al calcolo di una traiettoria di sicurezza che parte dal punto nello spazio operativo in cui si è verificata l'interruzione e termina in una posizione prestabilita considerata sicura. Tale traiettoria viene generata in modo da mantenere costante l'angolo del primo giunto, garantendo che tutti i punti attraversati appartengano al piano determinato dalla sua configurazione angolare al momento del fault. I risultati di tale implementazione sono mostrati di seguito, ipotizzando un fault

all'inverter che pilota il motore del primo giunto dopo un secondo dall'inizio della simulazione.

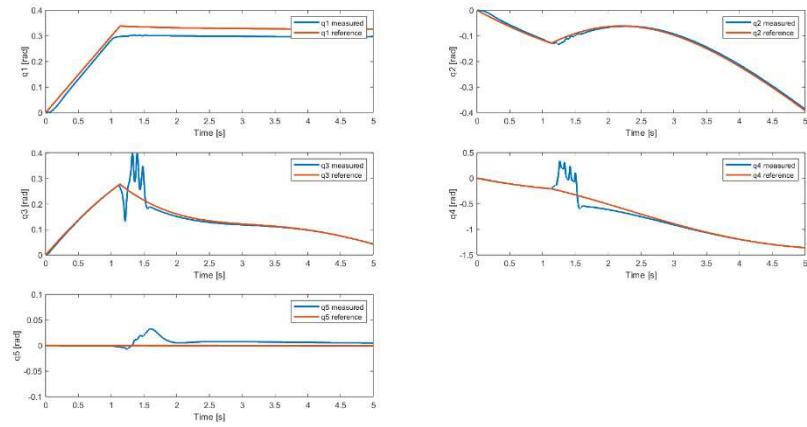


Figura 96 - Posizioni ricalcolo a configurazione sicura

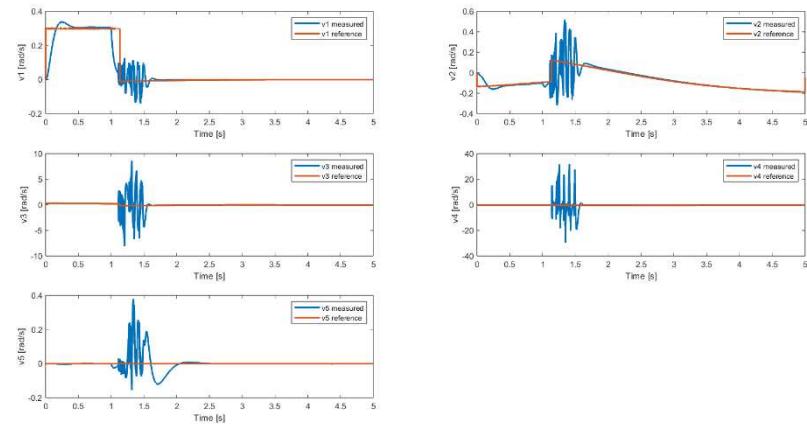


Figura 97 - Velocità ricalcolo a configurazione sicura

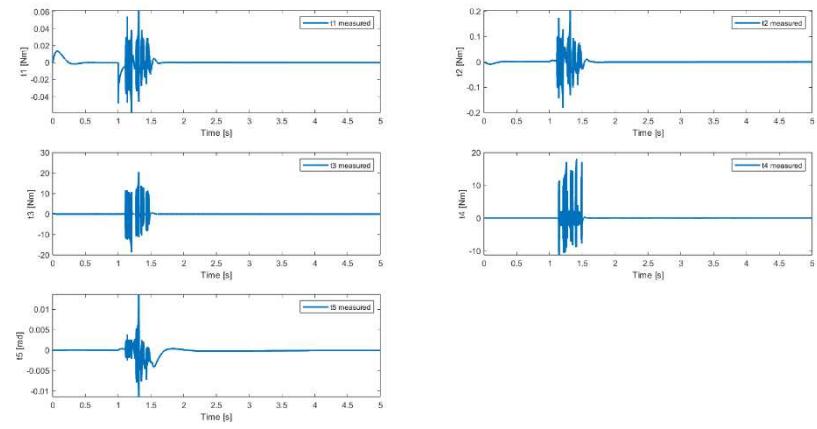


Figura 98 - Coppie ricalcolo a configurazione sicura

Capitolo VI – Conclusioni

Il presente lavoro di tesi ha affrontato un tema di crescente rilevanza nel panorama industriale moderno: la sicurezza funzionale dei robot collaborativi, con un focus specifico sui manipolatori industriali. L'analisi dello stato dell'arte ha evidenziato la centralità delle normative come pilastri fondamentali per garantire un'interazione sicura tra uomo e robot. L'esplorazione delle metodologie di risk assessment e delle tecniche di individuazione e mitigazione dei fault ha permesso di delineare un quadro completo delle sfide e delle opportunità nel campo della functional safety robotica.

L'obiettivo primario della tesi, ovvero l'applicazione dei dettami degli standard di sicurezza e l'individuazione di soluzioni innovative per la gestione dei fault nei robot collaborativi, è stato perseguito attraverso l'analisi teorica e, in modo significativo, attraverso un caso di studio pratico. L'implementazione di un sistema di controllo e l'applicazione di specifiche funzioni di sicurezza su un manipolatore industriale hanno rappresentato un banco di prova fondamentale per valutare l'efficacia delle metodologie studiate e per identificare potenziali aree di miglioramento.

La valutazione dei sistemi di sicurezza proposti e implementati ha fornito risultati preziosi in termini di prestazioni, affidabilità e capacità di risposta a scenari di fault. L'analisi dei fault legati a sensori, attuatori, o microcontrollori, unitamente alle metodologie sviluppate per la loro individuazione e mitigazione, ha dimostrato l'importanza di un approccio integrato che consideri sia gli aspetti hardware che software del sistema robotico. Le misure adottate in risposta ai malfunzionamenti considerati sono state efficaci in termini di rilevazione e gli interventi più invasivi risultano essere efficaci, mentre per le misure che permettono la continuità di esecuzione sono stati dimostrati i limiti di tale approccio, derivanti dalla configurazione utilizzata in termini di gradi di libertà e in termini di task assegnato.

Nonostante i progressi compiuti, il campo della sicurezza funzionale nei robot collaborativi è in continua evoluzione. Gli sviluppi futuri potrebbero

concentrarsi sull'integrazione di tecniche di intelligenza artificiale per una gestione dei fault più predittiva e adattiva, sull'esplorazione di nuove tipologie di sensori e attuatori con intrinseca sicurezza, e sull'affinamento delle metodologie di risk assessment per affrontare scenari di interazione uomo-robot sempre più complessi.

In conclusione, questo lavoro di tesi ha contribuito a fornire una panoramica approfondita delle sfide e delle soluzioni nel campo della sicurezza funzionale dei robot collaborativi, culminando in un'applicazione pratica che ha permesso di validare concetti teorici e di aprire nuove prospettive per la ricerca e lo sviluppo futuro. La crescente diffusione dei robot collaborativi in svariati settori industriali rende sempre più cruciale l'adozione di standard di sicurezza rigorosi e lo sviluppo di soluzioni innovative per garantire ambienti di lavoro sicuri ed efficienti.

Riferimenti

- [1] M. Goodrich e A. Schultz, «Human-Robot Interaction: A Survey», *Found. Trends Hum.-Comput. Interact.*, vol. 1, pp. 203–275, gen. 2007, doi: 10.1561/1100000005.
- [2] Canadian Centre for Occupational Health and Safety (CCOHS), «Robots and Cobots – Working Safely», 2023. [Online]. Disponibile su: https://www.ccohs.ca/oshanswers/safety_haz/robots_cobots.pdf
- [3] Workplace Safety and Health Council (Singapore), «Working Safely with Industrial Robots», 2020. [Online]. Disponibile su: <https://www.tal.sg/wshc-/media/TAL/Wshc/Resources/Publications/Others/Files/Working-Safely-with-Industrial-Robots.pdf>
- [4] «https://fscdn.rohm.com/en/products/databook/white_paper/iso26262_wp-e.pdf».
- [5] «Risk Assessment: Complex, Challenging, Absolutely Required». Disponibile su: <https://www.universal-robots.com/blog/the-risk-assessment-complex-challenging-and-absolutely-required/>
- [6] Wikipedia, *Analisi dei modi e degli effetti dei guasti — Wikipedia, L'encyclopédia libera*. 2024. [Online]. Disponibile su: http://it.wikipedia.org/w/index.php?title=Analisi_dei_modi_e_degli_effetti_dei_guasti&oldid=142583951
- [7] Headvisor, «Analisi FMEA cosa e come fare - esempi», [Online]. Disponibile su: <https://www.headvisor.it/sites/default/files/pdf/analisi-fmea-cosa-e-come-fare-esempi-headvisor.pdf>
- [8] Wikipedia contributors, *Fault tree analysis — Wikipedia, The Free Encyclopedia*. 2025. [Online]. Disponibile su: https://en.wikipedia.org/w/index.php?title=Fault_tree_analysis&oldid=1279529447
- [9] «Safety in control systems according to EN ISO 13849-1». Disponibile su: <https://search.abb.com/library/Download.aspx?DocumentID=2TLC172003B02002>
- [10] R. Co, «ISO 26262: Functional Safety Standard for Modern Road Vehicles».

- [11] A. Golshani, A. Kouhkord, A. Ghanbarzadeh, e E. Najafi, «Control Design for Safe Human-Robot Collaboration based on ISO/TS 15066 with Power and Force Limit», in *2023 11th RSI International Conference on Robotics and Mechatronics (ICRoM)*, dic. 2023, pp. 279–284. doi: 10.1109/ICRoM60803.2023.10412570.
- [12] D. Li, Y. Wang, J. Wang, C. Wang, e Y. Duan, «Recent advances in sensor fault diagnosis: A review», *Sens. Actuators Phys.*, vol. 309, p. 111990, lug. 2020, doi: 10.1016/j.sna.2020.111990.
- [13] N. Trapani e L. Longo, «Fault Detection and Diagnosis Methods for Sensors Systems: a Scientific Literature Review», *IFAC-Pap.*, vol. 56, fasc. 2, pp. 1253–1263, gen. 2023, doi: 10.1016/j.ifacol.2023.10.1749.
- [14] M. Özkan e Ç. Kasnakoglu, «Active Fault Detection in Linear Controller Hardware with Sine Signal», in *2020 7th International Conference on Electrical and Electronics Engineering (ICEEE)*, apr. 2020, pp. 90–94. doi: 10.1109/ICEEE49618.2020.9102484.
- [15] W. Wu, Y. Kang, e L. Yao, «Learning Observer Based Fault Diagnosis and Fault Tolerant Control for Manipulators with Sensor Fault», in *2019 CAA Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)*, lug. 2019, pp. 53–58. doi: 10.1109/SAFEPROCESS45799.2019.9213440.
- [16] J. Wang, X. Wang, Y. Wang, Y. Sun, e G. Sun, «Intelligent Joint Actuator Fault Diagnosis for Heavy-Duty Industrial Robots», *IEEE Sens. J.*, vol. 24, fasc. 9, pp. 15292–15301, mag. 2024, doi: 10.1109/JSEN.2024.3377234.
- [17] «Fault-tolerant actuators and drives-Structures, fault detection principles and applications», *ResearchGate*, doi: 10.1016/j.arcontrol.2009.08.002.
- [18] Z. Li, S. Dian, B. Guo, W. Cheng, L. Wang, e H. Liu, «Adaptive Observer-Based Fault Diagnosis and Model Predictive Fault-Tolerant Control for Actuator Faults in Robotic Manipulators», in *2023 China Automation Congress (CAC)*, nov. 2023, pp. 6765–6769. doi: 10.1109/CAC59555.2023.10450892.
- [19] Elviro Leo, Ignazio Olivieri, «Controllo a Dinamica Inversa Manipolatore CRS-A255». 2023.
- [20] P. Sanz, «Robotics: Modeling, Planning, and Control (Siciliano, B. et al; 2009) [On the Shelf]», *IEEE Robot. Autom. Mag.*, vol. 16, fasc. 4, pp. 101–101, dic. 2009, doi: 10.1109/MRA.2009.934833.
- [21] «Simscape Multibody Documentation». Disponibile su: <https://it.mathworks.com/help/sm/index.html>

- [22] «(PDF) A Statistical View on Automated Driving System Safety Architectures», *ResearchGate*, apr. 2025, doi: 10.1007/978-3-031-14862-0_2.
- [23] P. I. Corke, *Robotics, Vision & Control: Fundamental Algorithms in MATLAB*, Second. Springer, 2017.
- [24] Wikipedia, *K-nearest neighbors — Wikipedia, L'enciclopedia libera*. 2025. [Online]. Disponibile su: http://it.wikipedia.org/w/index.php?title=K-nearest_neighbors&oldid=144704956

Glossario figure

Figura 1 - Livelli di autonomia con enfasi sulle HRI	12
Figura 2 - Sicurezza intrinseca e sicurezza funzionale.....	15
Figura 3 - Determinazione livelli di rischio	19
Figura 4 - Standard functional safety	20
Figura 5 - Panoramica ISO 26262.....	21
Figura 6 - Lista dei possibili pericoli - 1.....	22
Figura 7 - Lista dei possibili pericoli - 2.....	23
Figura 8 - Lista dei possibili pericoli - 3.....	24
Figura 9 - Tabella della verità per le operazioni di safety-rated monitored stop	28
Figura 10 - Rappresentazione grafica dei contributi alla distanza di separazione protettiva tra operatore e robot	32
Figura 11 - Rappresentazione grafica delle forze e pressioni ammissibili e non ammissibili.....	34
Figura 12 - Limiti di forza e pressione biomeccanici.....	35
Figura 13 - Modello per contatti transienti.....	36
Figura 14 - Masse e costanti elastiche effettive per il corpo umano	36
Figura 15 - Modello semplificato della distribuzione di massa	38
Figura 16 - Concetti di hard redundancy e analytical redundancy	44
Figura 17 - Struttura di sistemi esperti per la rilevazione dei fault ai sensori..	47
Figura 18 - Rilevazione sensor fault tramite reti neurali.....	48
Figura 19 - Diagnosi dei fault tramite SVM	48
Figura 20 - Localizzazione dei fault ai sensori tramite wavelet transform	50
Figura 21 - Processo di stima dei fault ai sensori	50
Figura 22 - Schema di sistema di gestione integrato dei fault	51
Figura 23 - Parametri cinematici di Denavit-Hartenberg.....	55
Figura 24 - Sistema di riferimento secondo la convenzione D-H.....	56
Figura 25 - Vettore di input del sistema	60
Figura 26 - Schema di controllo del manipolatore	61
Figura 27 - Digital Twin Manipolatore CRS A255	74
Figura 28 - Modello Simscape del Manipolatore	74
Figura 29 - PI di corrente	75
Figura 30 - Riferimenti di posizione, velocità e accelerazione.....	75
Figura 31 - Calcolo dei disaccoppiamenti e delle compensazioni in avanti ...	76
Figura 32 - Visualizzazione delle traiettorie	76
Figura 33 - Simulazione 3D del manipolatore	77
Figura 34 - Check posizioni e generazione flag	79
Figura 35 - Schema di controllo semplificato	80
Figura 36 - Cinematica inversa tramite Pseudo-inversa dello Jacobiano e ottimizzazione delle funzioni costo.....	81

Figura 37 - Calcolo della $H(q)$ dinamico.....	82
Figura 38 - Manipolatore planare a 3 bracci.....	83
Figura 39 - Workspace del manipolatore planare	84
Figura 40 - Workspace manipolatore planare – 1° giunto bloccato	84
Figura 41 - Workspace manipolatore planare – 2° giunto bloccato	85
Figura 42 - Workspace manipolatore planare - 3° giunto bloccato	85
Figura 43 - Posizioni angolari misurate e di riferimento	94
Figura 44 - Velocità angolari misurate e di riferimento	94
Figura 45 - Simulazione del fault totale agli inverter.....	95
Figura 46 - Modellazione singolo fault all'inverter	95
Figura 47 - Posizioni angolari misurate e di riferimento	96
Figura 48 - Velocità angolari misurate e di riferimento	96
Figura 49 - Posizioni angolari misurate e di riferimento	97
Figura 50 - Velocità angolari misurate e di riferimento	97
Figura 51 - Posizioni misurate e di riferimento	98
Figura 52 - Velocità misurate e di riferimento	99
Figura 53 - Posizioni misurate e di riferimento	100
Figura 54 - Velocità misurate e di riferimento	101
Figura 55 - Errore assoluto tra livello 1 e livello 2	101
Figura 56 - Flag di intervento delle protezioni	102
Figura 57 - Posizioni misurate e di riferimento	103
Figura 58 - Velocità misurate e di riferimento	103
Figura 59 - Errore assoluto tra livello 1 e livello 2	104
Figura 60 - Flag di intervento delle protezioni	104
Figura 61 - Posizioni misurate e di riferimento	105
Figura 62 - Velocità misurate e di riferimento	105
Figura 63 - Errore assoluto tra livello 1 e livello 2	106
Figura 64 - Flag di intervento delle protezioni	106
Figura 65 - Posizioni - fault giunto 1.....	107
Figura 66 - Posizioni - fault giunto 2.....	107
Figura 67 - Posizioni - fault giunto 3.....	108
Figura 68 - Posizioni - fault giunto 4.....	108
Figura 69 - Posizioni - fault giunto 5.....	109
Figura 70 - Posizioni - fault giunto 1 e ricalcolo della traiettoria	110
Figura 71 - Posizioni - fault giunto 2 e ricalcolo della traiettoria	110
Figura 72 - Posizioni - fault giunto 3 e ricalcolo della traiettoria	111
Figura 73 - Posizioni - fault giunto 4 e ricalcolo della traiettoria	111
Figura 74 - Posizioni - fault giunto 5 e ricalcolo della traiettoria	112
Figura 75 - Posizioni misurate e di riferimento	114
Figura 76 - Configurazione finale ottenuta per interpolazione	115
Figura 77 - Posizioni angolari interpolate e calcolate tramite cinematica inversa	116

Figura 78 - Traiettoria pseudo-inversa e riferimento.....	116
Figura 79 - Posizioni angolari - nessun intervento T1	117
Figura 80 - Posizioni angolari - ricalcolo T1	117
Figura 81 - Posizioni angolari - ricalcolo T2.....	118
Figura 82 - Posizioni angolari - nessun intervento T1	118
Figura 83 - Posizioni angolari - ricalcolo T1	119
Figura 84 - Posizioni angolari - ricalcolo T2.....	119
Figura 85 - Posizioni angolari - nessun intervento T1	120
Figura 86 - Posizioni angolari - ricalcolo T1	120
Figura 87 - Posizioni angolari - ricalcolo T2.....	121
Figura 88 - Posizioni angolari - nessun intervento T1	121
Figura 89 - Posizioni angolari - ricalcolo T1	122
Figura 90 - Posizioni angolari - ricalcolo T2.....	122
Figura 91 - Posizioni angolari - nessun intervento T1	123
Figura 92 - Posizioni angolari - ricalcolo T1	123
Figura 93 - Posizioni angolari - ricalcolo T2.....	124
Figura 94 - Posizioni ricalcolo a configurazione sicura	125
Figura 95 - Velocità ricalcolo a configurazione sicura	125
Figura 96 - Copie ricalcolo a configurazione sicura.....	126