Applicazione della Normativa ISO26262 a veicoli ibridi elettrici

Tesi di Laurea Magistrale svolta presso Pure Power Control s.r.l.

Relatori: Prof. Alberto Landi
Prof. Lorenzo Pollini
Ing. Emanuele Mazzi

Candidato: Nicola Greco

Università di Pisa

Dipartimento di Ingegneria dell'Informazione

Anno Accademico 2012/2013

Indice

1 I Veicoli ibridi **1**

1.1 L'architettura dei veicoli ibridi 2

1.1.1 Architettura ibrida di tipo serie 5

1.1.2 Architettura ibrida di tipo parallelo 8

1.1.3 Architettura ibrida di tipo power split 11

2 La normativa ISO26262 **14**

2.1 Analisi e valutazione del rischio 16

2.1.1 Probabiltà di esposizione 16

2.1.2 Severità 17

2.1.3 Controllabilità 19

2.2 Determinazione degli ASIL e degli Obiettivi di Sicurezza 20

3 Strumento software per l'applicazione della normativa **21**

3.1 Gestione del database delle situazioni 22

3.2 Gestione del database di componenti e malfunzionamenti 23

3.3 Definizione del layout 24

3.4 Definizione delle situazioni operative e degli ASIL 25

4 Il modello di Powertrain **28**

4.1 Il modello della batteria 30

4.2 Il modello della macchina elettrica 34

4.3 Il modello dell'inverter 39

4.4 Il modello del motore termico 43

4.5 Il modello delle frizioni 45

4.6 Il modello della trasmissione 48

4.6.1 Il modello del cambio 48
4.6.2 Il modello dell'albero di trasmissione 49
4.7 Il modello della logica di controllo 50
4.7.1 Modalità operativa 51
4.7.2 Cambio automatico 52
4.7.3 Controllo segnali 53
4.7.4 Gestione della coppia 54
4.8 Il modello dello chassis 55

5 Il modello matematico **58**
5.1 Il modello equivalente dello chassis 58
5.2 Il modello equivalente dello stato di carica 60

6 Assegnazione degli ASIL e degli Obiettivi di Sicurezza **63**
6.1 Coppia non desiderata a veicolo fermo 65
6.2 Coppia superiore a quella richiesta 66
6.3 Coppia inferiore a quella richiesta 67
6.4 Mancata erogazione di coppia 69

7 Sistema di diagnosi e verifica dei requisiti di sicurezza **70**
7.1 Monitor di sistema 71
7.2 Diagnosi 73
7.3 Recovery 75

8 Simulazioni **77**
8.1 Coppia non desiderata a veicolo fermo 78
8.1.1 Analisi di sensitività parametrica 80
8.2 Coppia superiore a quella richiesta 81
8.3 Coppia inferiore quella richiesta 84
8.4 Coppia nulla 88

9 Automi Ibridi **91**
9.1 Definizione di Automa ibrido 93
9.2 Lo studio del Safe Set 94
9.3 Coppia non desiderata a veicolo fermo 96
9.4 Assenza di coppia dalla macchina elettrica 110

Elenco delle figure

1.1 Architettura di un veicolo ibrido serie 5
1.2 Flussi di potenza di un'architettura serie 6
1.3 Architettura di un veicolo ibrido parallelo 8
1.4 Flussi di potenza di un'architettura parallela 9
1.5 Unità di trasmissione planetaria 11
1.6 Flussi di potenza di un'architettura power split 12

3.1 Pannello di gestione del database delle situazioni operative . . . 22
3.2 Pannello di gestione del database degli oggetti e dei malfunzionamenti 23
3.3 Pannello di gestione del layout 24
3.4 Pannello creazione delle situazioni operative 25
3.5 Pannello di assegnazione delle classi di Severità e Controllabilità e degli ASIL 26
3.6 Pannello riassuntivo dell'assegnazione degli ASIL 26
3.7 Pannello opzioni per i percorsi di default 27
3.8 Pannello di opzioni per i percorsi della sessione in corso 27

4.1 Architettura di Powertrain parallelo in esame 28
4.2 Circuito equivalente della batteria 30
4.3 Modello Simulink della batteria e del bus di corrente 32
4.4 Modello Simulink della batteria a Litio e del Convertitore DC/DC 33
4.5 Interno del modello Simulink della batteria a Litio 33
4.6 Sezioni trasversali dei rotori di motori PMSM superficiali detti SPMSM (a) e interni detti IPMSM (b) 35
4.7 Andamento della coppia massima e minima della PMSM al variare dei giri al minuto 38

4.8 Modello Simulink della PMSM 38
4.9 Chopped che modella ciascun ramo dell'inverter 39
4.10 Modello Simulink dell'inverter 42
4.11 Andamento della coppia massima e minima del motore termico al variare dei giri al minuto 43
4.12 Modello Simulink del motore termico 44
4.13 Modello Simulink dei due organi frizione 47
4.14 Modello Simulink del cambio 49
4.15 Modello Simulink dell'albero di trasmissione 50
4.16 Modello Simulink della logica di controllo 51
4.17 Modello StateFlow della Modalità operativa 52
4.18 Modello StateFlow del Cambio automatico 53
4.19 Modello StateFlow della Control logic 53
4.20 Modello StateFlow della Torque management 54
4.21 Modello Simulink dello chassis e del pneumatico 56
4.22 Modello Simulink completo del Powertrain 57

5.1 Modello equivalente semplificato della batteria 60

7.1 Monitor di sistema 71
7.2 Macchina a stati interna al Monitor di sistema 72
7.3 Macchina a stati che implementa il sistema di Diagnosi 73
7.4 Macchina a stati che implementa il sistema di Recovery 75

8.1 blocco Inverter con iniezione dei segnali di guasto 77
8.2 spostamento del veicolo in seguito alla frenata da parte del guidatore 78
8.3 spostamento del veicolo in seguito all'attivazione della recovery . 79
8.4 Andamento dello spostamento al variare di t_{att} 80
8.5 Andamento della velocità del veicolo in seguito al malfunzionamento 81
8.6 Andamento della velocità del veicolo in seguito al malfunzionamento, nel caso di recovery attiva 82
8.7 Andamento dei segnali di attivazione di diagnosi e recovery, e delle coppie dei due motori 83

8.8 Andamento della velocità del veicolo in seguito al malfunzionamento . . . 84
8.9 Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery attiva . . . 85
8.10 Attivazione di diagnosi e recovery, e coppie dei due motori . . . 86
8.11 Confronto fra le velocità del veicolo con, e senza, malfunzionamento . . . 86
8.12 Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery disattiva . . . 88
8.13 Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery attiva . . . 89
8.14 Andamento dei segnali di attivazione di diagnosi e recovery, e delle coppie dei due motori . . . 90

9.1 Schema di un automa ibrido . . . 92
9.2 Esempio di rappresentazione di un automa ibrido . . . 94
9.3 Rappresentazione dell'automa ibrido in caso di coppia non desiderata a veicolo fermo . . . 97
9.4 Spazio di stato continuo in ogni stato discreto q_i . . . 100
9.5 Fase per $i = 0$ caso coppia non desiderata a veicolo fermo . . . 101
9.6 Fase per $i = 1$ caso coppia non desiderata a veicolo fermo . . . 102
9.7 Dinamica continua con il controllore massimale . . . 103
9.8 Dinamica discreta con il controllore massimale . . . 104
9.9 Andamenti delle regioni di stato per l'attivazione del controllo, al variare del tempo di ritardo . . . 105
9.10 Spazio di stato continuo in ogni stato discreto q_i caso con ritardo 105
9.11 Fase per $i = 0$ caso coppia non desiderata a veicolo fermo con ritardo . . . 106
9.12 Fase per $i = 1$ caso coppia non desiderata a veicolo fermo con ritardo . . . 107
9.13 Dinamiche continue, al variare dell'instante di apertura frizioni . 108
9.14 Dinamica discreta con il controllore sviluppato . . . 109
9.15 Manovra di sorpasso . . . 110
9.16 Rappresentazione Automa ibrido in caso di coppia inferiore o nulla a quella richiesta . . . 111

9.17 Superficie delimitante il sorpasso massimo utilizzando il solo motore elettrico 116
9.18 Superficie delimitante il sorpasso massimo utilizzando il solo motore termico 116
9.19 Spazio di stato continuo e descrizione azioni di controllo e disturbo 117
9.20 Descrizione operatori Pre_e, Pre_c e $Unavoid\_Pre$ 119
9.21 Traccia piani XY e XZ 120
9.22 Traccia piani YZ per $X = 0$ e per $X = 450m$ 120
9.23 Simulazione con e senza recovery della manovra di sorpasso . . . 121
9.24 Vista dall'alto del Safe set con relativa simulazione 122

Elenco delle tabelle

2.1 Classificazione della probabilità di esposizione 16
2.2 Classificazione della probabilità di esposizione rispetto alla frequenza della situazione 17
2.3 Classificazione della probabilità di esposizione rispetto alla durata della situazione 17
2.4 Classificazione della severità di un evento 17
2.5 Classificazione della severità di un evento in base alla scala AIS 18
2.6 Classificazione della controllabilità di un evento 19
2.7 Determinazione di un ASIL in base a Esposizione, Severità e Controllabilità di un evento 20

4.1 Valori coefficienti R_{TH} e E_{TH} 48

6.1 Assegnazione degli ASIL nel caso di movimento non desiderato . 65
6.2 Assegnazione degli ASIL nel caso di coppia superiore 66
6.3 Assegnazione degli ASIL nel caso di coppia inferiore 67
6.4 Assegnazione degli ASIL nel caso di assenza di coppia 69

Introduzione

La presenza sempre maggiore di componenti elettrici ed elettronici a bordo dei veicoli stradali destinati alla produzione in serie, unitamente al continuo sviluppo di tecnologie che permettono di affiancare alla normale propulsione termica una propulsione di tipo elettrico, rende necessario stabilire delle precise direttive che debbano essere rispettate durante l'intero processo di sviluppo.

La tesi si pone come obiettivo quello di applicare la normativa ISO26262 seguendo un nuovo approccio metodologico, di tipo model-based. È stato sviluppato un innovativo strumento di supporto all normativa, in grado di generare in modo strutturato ed esaustivo le varie situazioni operative, fornendo inoltre assistenza durante la classificazione degli scenari, e permettendo di simulare le condizioni di guasto; tale strumento permette inoltre l'interazione diretta con il modello di simulazione, al fine di verificare e validare il rispetto dei requisiti di sicurezza formulati.

È stata quindi applicata la teoria degli automi ibridi al caso di studio della normativa, validando le specifiche di sicurezza mediante la tecnica di verifica formale del Controllore Massimale.

Ringraziamenti

Ringrazio innanzitutto la mia famiglia, che mi ha dato la possibilità di raggiungere questo traguardo. Un pensiero speciale va a mio nonno, che purtroppo non potrà festeggiare con me, ma che sicuramente sarebbe fiero di questo mio obiettivo raggiunto. Ringrazio di cuore la mia fidanzata Silvia, che è riuscita a sopportarmi in questi ultimi mesi, e mi ha spronato più di ogni altro a tenere duro anche nei tanti momenti in cui pensavo proprio di non farcela. Un ringraziamento particolare va al mio collega Davide, con cui ho condiviso il percorso di tesi ed il cui aiuto è stato fondamentale, ed ai miei tutor aziendali Andrea ed Emanuele, per l'opportunità che mi hanno dato e per il supporto fornito durante tutto il lavoro di tesi.

Un sentito ringraziamento va a tutti gli amici che ho conosciuto durante il mio percorso universitario, e con i quali ho condiviso gioie e dolori: Alessio, Dario, Davide, Giulio, Massimo, Riccardo, Simone, Tommaso F. e Tommaso C. .

Ultimi ma non ultimi, i miei migliori amici Alessio e Valerio, il cui supporto morale si è rivelato fondamentale sopratutto in questo ultimo periodo: sono felice di poter condividere con voi uno dei momenti più importanti della mia vita.

Nicola

Capitolo 1

I Veicoli ibridi

Nel 2005 è entrato in vigore il protocollo di Kyoto: il trattato prevede l'obbligo di operare una riduzione delle emissioni di elementi di inquinamento (biossido di carbonio ed altri gas serra, quali metano e ossido di azoto) in una misura non inferiore all'8% rispetto alle emissioni registrate nel 1990, nel periodo 2008-2013. Tra i maggiori responsabili dell'emissione di CO_2 si trovano le automobili ed in generale qualunque mezzo di trasporto che utilizzi per la propulsione un motore a combustione interna. Negli ultimi anni si sono dunque studiati nuovi sistemi di propulsione con l'obiettivo di annullare o quantomeno ridurre significativamente sia le emissioni di anidride carbonica, sia il consumo di combustibili fossili, la cui disponibilità è destinata a calare contrariamente al loro prezzo.

I veicoli puramente elettrici sembrano essere i migliori candidati per compimento di tali obiettivi. In questa tipologia di veicoli la propulsione è ad opera di un motore elettrico alimentato da batterie di adeguata capacità: in particolare se l'energia immagazzinata nelle batteria è prodotta da fonti rinnovabili, quali il fotovoltaico o l'eolico, si ottiene il totale abbattimento di emissioni di CO_2. Lo sviluppo e la diffusione di tali veicoli è però frenato da molteplici fattori: le prestazioni e l'autonomia sono ancora molto distanti dai livelli raggiunti dai veicoli tradizionali con motore a combustione interna, inoltre il risparmio economico che si avrebbe per quanto riguarda i consumi dei combustibili non compensa ancora il costo della sostituzione delle batterie alla fine del loro ciclo di vita.

Nell'attesa di progressi e miglioramenti nella tecnologia delle batterie o più

in generale nei sistemi di immagazzinamento dell'energia, si è deciso di puntare ad un buon compromesso tra prestazioni e tutela dell'ambiente, rappresentato dai veicoli ibridi.

1.1 L'architettura dei veicoli ibridi

Si definisce veicolo ibrido (HEV, Hybrid Electric Vehicle), o veicolo a propulsione ibrida, un veicolo dotato di due o più sorgenti di potenza distinte, di cui almeno una reversibile. Nel caso specifico di automobili ibride elettriche, la sorgente principale è costituita da un classico motore a combustione interna benzina o diesel, denominato ICE (Internal Combustion Engine), mentre la sorgente secondaria e reversibile è costituita da una macchina elettrica, denominata EM (Electric Machine), alimentata da un pacco batterie.

L'uso dei due tipi differenti di propulsione permette di beneficiare dei vantaggi forniti da entrambi, e compensare i difetti delle singole architetture, cosi da avere come risultato un veicolo con efficienza superiore rispetto la soluzione a combustione tradizionale ma mantenendo la stessa potenza.

In un veicolo ibrido sono presenti due o più sistemi di potenza, che interagiscono tra di loro per mezzo di convertitori unidirezionali o bidirezionali: quindi, se in un veicolo tradizionale l'energia segue sempre un percorso diretto dal motore alle ruote, in un veicolo ibrido la bidirezionalità di alcuni dispositivi consente di gestire l'energia in modo più efficace sfruttando la possibilità di farle percorrere "strade" diverse. La modalità con cui l'energia meccanica proveniente dai due propulsori viene combinata per fornire la trazione del veicolo è determinata da un apposito processo di controllo della vettura, solitamente indicato con il nome di *Energy Management Problem*. Il sistema di controllo garantisce quindi una cooperazione delle due unità di propulsione al fine di ottenere una riduzione dei consumi globali di carburante e delle emissioni di gas inquinanti.

Le principali caratteristiche di un veicolo ibrido sono le seguenti

- un veicolo ibrido può recuperare parte dell'energia cinetica durante la frenata utilizzando la macchina elettrica come un generatore, così da ricaricare le batterie,

- un veicolo ibrido può spegnere il motore a combustione durante le fasi in cui esso viene impiegato a regime minimo, al fine di ridurre consumi ed emissioni,

- un veicolo ibrido può ottimizzare le fasi a basso rendimento del motore a combustione spostando il suo punto di funzionamento.

Il miglioramento nell'economia del carburante dipende fortemente dal tipo di veicolo, dal ciclo di guida che sta effettuando e sopratutto dal sistema di controllo delle due fonti di energia.

Il grado di ibridizzazione di un veicolo può essere determinato dalla seguente equazione

$$H = \frac{P_{EM}}{P_{EM} + P_{ICE}}$$

dove H indica il grado di ibridizzazione, P_{EM} la potenza del motore elettrico e P_{ICE} la potenza del motore termico.

I componenti che costituiscono l'architettura di un veicolo ibrido, oltre a quelli tradizionali di una normale autovettura a combustione interna, sono:

Macchina elettrica: può essere sia in corrente alternata, sia a magneti permanenti in corrente continua. Può svolgere sia le funzioni di generatore, convertendo energia meccanica in elettrica, sia come motore elettrico, convertendo l'energia elettrica in energia meccanica. Nella scelta di un motore elettrico è necessario tenere conto di importanti fattori quali il peso, l'ingombro e la tensione di alimentazione. La leggerezza è una caratteristica fondamentale per ridurre i consumi ed aumentare le prestazioni, a parità di potenza. L'ingombro risulta una caratteristica primaria, in quanto la presenza della macchina elettrica non deve andare ad intaccare notevolmente il layout del veicolo. La tensione di alimentazione dovrebbe essere la più elevata possibile, in modo da mantenere discrete potenze pur con ridotte correnti, consentendo quindi di utilizzare conduttori di sezione inferiore aumentando i rendimenti.

Accumulatori: sono unità in costante via di sviluppo e rappresentano uno dei punti cruciali di un veicolo ibrido: devono garantire buone caratteristiche funzionali, influendo il meno possibile su peso e volume occupato.

Sul mercato sono presenti diverse tipologie di accumulatori: i più economici sono quelli al piombo-acido, caratterizzati da una vita relativamente breve ed una bassa densità di corrente; un'altra tipologia è quella costituita dagli accumulatori ai nichel-metal idruri ($NiMH$), i quali sono i più diffusi per la produzione di veicoli ibridi per via della loro elevata densità di energia, il loro lungo ciclo di vita e l'ingombro contenuto; un'ultima categoria è costituita dagli accumulatori agli ioni di litio, su cui si sta concentrando notevolmente l'attività di ricerca negli ultimi anni, caratterizzati da una elevata densità di energia e di rendimento alle basse temperature, al contrario della controparte a nichel-metal idruri che raggiungono facilmente elevate temperature compromettendo il loro rendimento.

Elettronica di potenza: le macchine elettriche in corrente continua necessitano di moduli di commutazione, per controllare il flusso di corrente di ciascun avvolgimento durante la rotazione del motore. Devono poter commutare con grande rapidità correnti ad elevata intensità, e poterne controllare verso e fase.

Sistemi di raffreddamento: la presenza di accumulatori ed elettronica di potenza sviluppa una elevata quantità di calore, che deve essere prontamente smaltita: è quindi necessario creare un adeguato sistema di refrigerazione, in grado di mantenere le prestazioni e preservare i sistemi di accumulo.

Dal punto di vista funzionale, i veicoli ibridi possono essere classificati in tre categorie, caratterizzate da diverse interconnessioni fra le varie fonti di potenza

- architettura ibrida di tipo serie,
- architettura ibrida di tipo parallelo,
- architettura ibrida di tipo power split.

Nel proseguo si analizzano in dettaglio le tre diverse architetture.

1.1.1 Architettura ibrida di tipo serie

Un veicolo ibrido serie (*S-HEV*, Series Hybrid Electric Vehicle) è un veicolo dotato di due distinti Powertrain connessi in serie tra di loro: il motore elettrico rappresenta l'unico dispositivo preposto alla propulsione del mezzo. La configurazione di un veicolo di questo tipo è rappresentata in figura 1.1

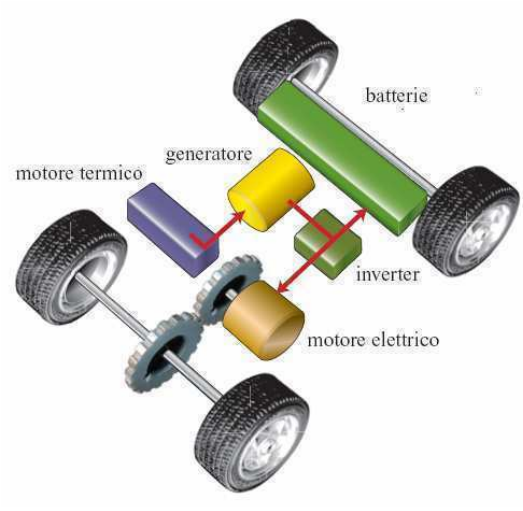

Figura 1.1: Architettura di un veicolo ibrido serie

Il motore termico genera energia meccanica, come nei veicoli tradizionali, la quale non è però direttamente impiegata per la propulsione, ma viene convertita da un generatore elettrico. I morsetti elettrici del generatore vengono allacciati ad un bus di potenza, che confluisce in un convertitore elettronico a cui è connesso anche il sistema di batterie. Per questo motivo la potenza meccanica fornita dal motore termico è convertita in energia elettrica che può andare ad alimentare direttamente il motore elettrico o essere utilizzata per ricaricare la batteria.

Le trasformazioni di energia cui è caratterizzato questo tipo di architettura sono tre: inizialmente si passa da una trasformazione chimica a una meccanica, per poi passare ad una trasformazione meccanica - elettrica e infine ad una trasformazione elettrica - meccanica. Da qui si evince la necessità di avere tre componenti minimi per la propulsione che rendano possibili le trasformazioni appena citate.

Questa configurazione porta il motore termico a non essere direttamente collegato alle richieste di potenza del veicolo, cosi da poter lavorare costantemente sul punto di lavoro ottimo per quanto riguarda efficienza e emissioni; inoltre il disaccoppiamento tra l'asse meccanico del motore e le ruote rende possibile l'eliminazione della frizione. In figura 1.2 sono evidenziati i flussi di potenza relativi a questa architettura

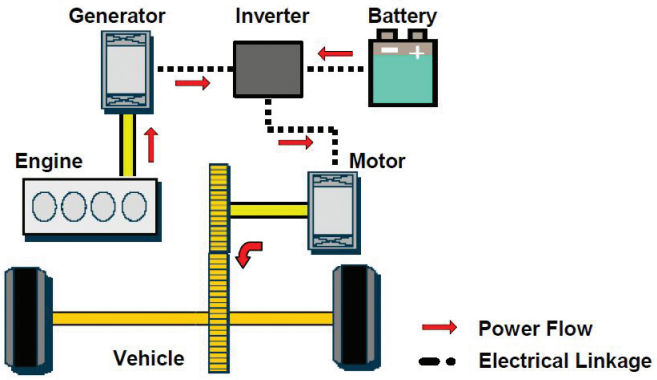

Figura 1.2: Flussi di potenza di un'architettura serie

Dal momento che la propulsione è gestita principalmente dalla macchina elettrica, il dimensionamento del motore termico è determinato dalla potenza media richiesta dal veicolo, diversamente dagli autoveicoli tradizionali nei quali il motore a combustione interna viene dimensionato in base alla massima potenza richiesta.

Questa architettura è caratterizzata dalle seguenti modalità operative

Modalita puramente elettrica: il veicolo è in moto, il motore termico è spento mentre quelle elettrico viene alimentato unicamente dalle batterie.

Modalita puramente termica: il veicolo è in moto, il motore elettrico viene alimentato dal motore termico attraverso il generatore, le batterie non scambiano potenza con il resto del sistema.

Modalità ibrida: il veicolo è in moto, l'energia per la propulsione viene fornita contemporaneamente sia dal motore termico che dalla macchina elettrica.

Trazione con ricarica: il veicolo è in moto, il motore termico fornisce contemporaneamente energia al motore elettrico, attraverso il generatore, e al convertitore elettronico per la ricarica delle batterie.

Frenata rigenerativa: il veicolo è in fase di frenata, il motore termico viene spento mentre quelle elettrico funziona da generatore, trasformando l'energia cinetica dissipata per ricaricare le batterie.

Carica batterie: il veicolo è fermo, il motore elettrico non riceve energia mentre l'energia sviluppata dal motore termico viene utilizzata per ricaricare le batterie.

I pregi di un'architettura ibrida serie sono i seguenti

- il motore a combustione interna lavora sempre nelle condizioni di massima efficienza,
- il motore a combustione interna trascina un generatore che opera sempre a rendimento massimo,
- non vi è alcun legame meccanico tra il motore a combustione e le ruote,
- il motore a combustione interna ha una potenza più bassa rispetto ad un veicolo convenzionale.

I difetti invece sono i seguenti

- sono presenti tre componenti: un motore termico, una macchina elettrica ed un generatore,
- sono richieste batterie più grandi e quindi più pesanti,
- si ha una tripla conversione di energia.

Confrontando quindi i benefici e gli aggravi legati a questa configurazione, ne deriva che l'architettura di tipo serie si dimostra inadatta ad essere adottata come soluzione alternativa ai veicoli tradizionali, poichè necessità di una struttura di dimensioni notevoli. Per questo motivo l'architettura serie viene generalmente applicata a veicoli per trasporto pubblico ed in generale agli automezzi dove le già considerevoli dimensioni non pongono particolari limiti.

1.1.2 Architettura ibrida di tipo parallelo

Un veicolo ibrido parallelo (*P_HEV*, Parallel Hybrid Electric Vehicle) è un veicolo dotato di due distinte sorgenti di potenza, connesse in parallelo tra di loro, in grado quindi di garantire in maniera indipendente l'uno dall'altro energia per la propulsione. La configurazione di un veicolo di questo tipo è rappresentata in figura 1.3

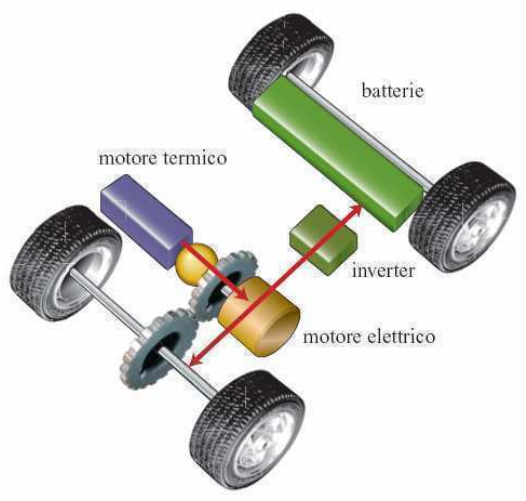

Figura 1.3: Architettura di un veicolo ibrido parallelo

In questa configurazione sia il motore termico, sia la macchina elettrica sono accoppiati meccanicamente all'albero di trasmissione, così da sommare le rispettive potenze. L' accoppiamento è garantito da un dispositivo meccanico chiamato ripartitore di coppia.

Il funzionamento di un veicolo ibrido parallelo si basa sulla possibilità dei due motori di poter fornire energia per la propulsione in modo indipendente e combinato: il motore termico converte l'energia chimica del carburante in energia meccanica, mentre la macchina elettrica scambia energia col sistema di accumulo a cui è connesso. Attraverso il ripartitore di coppia i due motori possono lavorare in parallelo o separatamente. C'è quindi un ulteriore grado di libertà disponibile per soddisfare i requisiti di potenza, che può essere usato per ottimizzare la distribuzione di potenza tra due percorsi energetici paralleli: ad esempio, quando non è richiesta potenza al canale energetico del motore

termico quest'ultimo può può essere spento, contribuendo ad un conseguente risparmio energetico.

Questa architettura è caratterizzata da due sole trasformazioni di energia, ma ne derivano un più complesso sistema di trasmissione (si veda per esempio la reintroduzione delle frizioni) ed una logica di controllo più articolata. Inoltre viene meno il vantaggio di far lavorare a punto fisso il motore termico, con conseguente aumento dei consumi e delle emissioni.

Nella figura 1.4 sono evidenziati i flussi di potenza per questa architettura

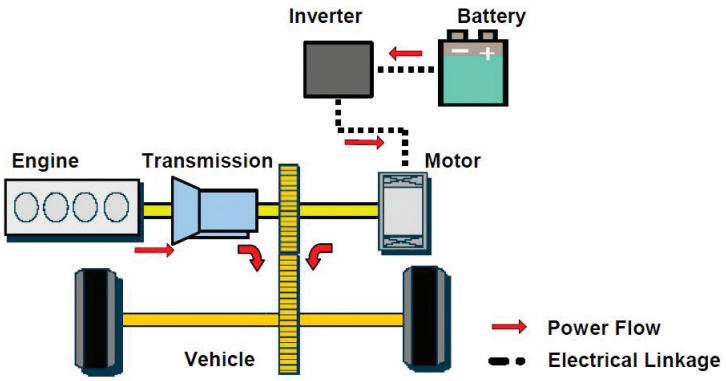

Figura 1.4: Flussi di potenza di un'architettura parallela

Lavorando in modo parallelo si sommano le coppie generate dai due motori, che quindi possono essere dimensionati tenendo conto solo una frazione della massima potenza che la macchina dovrà avere.

Le modalità operative dell'architettura serie sono le seguenti

Modalità puramente elettrica: il veicolo è in moto, il motore termico è spento mentre quelle elettrico viene alimentato unicamente dalle batterie,

Modalità puramente termica: il veicolo è in moto, l'energia necessaria per la propulsione è fornita esclusivamente dal motore termico: il veicolo in questo caso si comporta a tutti gli effetti come un veicolo tradizionale,

Modalità ibrida: il veicolo è in moto, l'energia per la propulsione viene fornita contemporaneamente sia dal motore termico che dalla macchina elettrica, e per quanto possibile il motore termico viene fatto funzionare a regimi tali da mantenere contenuti i suoi consumi,

Modalità boosting: il veicolo è in fase di accelerazione, la propulsione viene fornita contemporaneamente sia dal motore termico che dal motore elettrico, ma a differenza della modalità ibrida il motore termico è utilizzato senza alcun vincolo sul numero di giri.

Frenata rigenerativa: il veicolo è in fase di frenata, il motore termico viene spento mentre quelle elettrico funziona da generatore trasformando l'energia cinetica dissipata per ricaricare le batterie.

Nonostante la limitata capacità degli accumulatori che vengono generalmente installati a bordo dei veicoli ibridi per questioni di peso, questo tipo di architettura risulta molto interessante e conveniente. La possibilità di far funzionare l'auto esclusivamentemediante la macchina elettrica consente infatti di spegnere il motore termico, e ridurre quindi notevolmente i consumi, nei tratti caratterizzati da una bassa velocità di percorrenza e costituiti da frequenti accelerazioni e decelerazioni, come per esempio un tratto cittadino.

Di seguito si riassumono i pregi dell'architettura parallela

- a parità di prestazioni, permette l'utilizzo di un motore a combustione interna di potenza inferiore,
- il veicolo complessivamente è in grado di fornire buone prestazioni perchè entrambi i motori possono lavorare insieme,
- l'energia non deve essere convertita da meccanica ad elettrica per poi tornare nella forma meccanica.

I difetti di tale architettura sono invece i seguenti

- maggiore complessità del sistema di trazione e di trasmissione,
- il motore termico funziona a regime variabile, con conseguente riduzione del rendimento ed aumento delle emissioni.

In conclusione quindi l'architettura ibrido parallela si presta ad essere implementata efficacemente sulle auto tradizionali, dove le dimensioni contenute del veicolo non consentono l'adozione di un'architettura serie.

1.1.3 Architettura ibrida di tipo power split

La configurazione di tipo power split garantisce i vantaggi di entrambe le architetture viste in precedenza, ma necessita di un ulteriore collegamento meccanico tra motore termico e ruote (rispetto ala configurazione in serie) ed un generatore (non presente nella configurazione parallela).

Nonostante la complessità del sistema e l'incremento del costo, l'avanzamento tecnologico permette ad alcuni veicoli ibridi moderni di adottare in modo vantaggioso questa architettura.

Un componente fondamentale dell'architettura power split è la trasmissione planetaria, mostrata in figura 1.5: essa permette di dividere l'energia prodotta dal motore termico, inviandone una parte direttamente alla trasmissione e una parte al generatore (da qui il nome di questa architettura "power split").

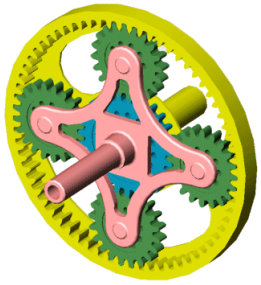

Figura 1.5: Unità di trasmissione planetaria

Per quanto concerne la parte elettrica (ibrido serie), una parte della potenza del motore termico viene consegnata al generatore che la converte in elettricità, per cui il motore elettrico riceve l'energia elettrica dalle batteria e dal generatore per generare coppia destinata alla trasmissione. Per quanto riguarda la parte meccanica (ibrido parallelo), la restante coppia generata dal motore termico viene inviata direttamente alla trasmissione senza trasformazioni di energia.

E' possibile bypassare il generatore collegato al motore termico, eliminando il collegamento serie tra il motore termico e quello elettrico, agendo sullo statore del generatore con un apposito blocco. I flussi di potenza per un'architettura power split sono riportati in figura 1.6

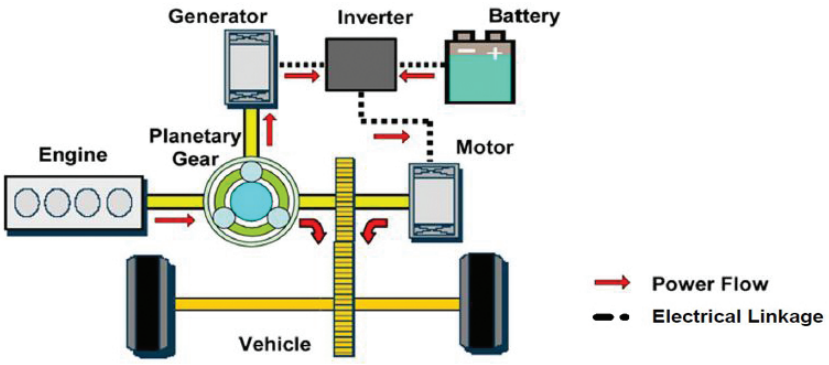

Figura 1.6: Flussi di potenza di un'architettura power split

Questa soluzione assicura una più ampia gamma di modalità operative al fine di gestire il flusso di potenza, ed essenzialmente possono essere racchiuse in due gruppi

1. Engine heavy

   startup/basso carico : il solo motore elettrico è attivo, il motore termico è spento,

   accelerazione : il motore termico e quello elettrico si dividono la potenza alle ruote,

   guida normale : il motore termico da solo fornisce potenza alle ruote, il motore elettrico è spento.

2. Electric heavy

   startup/basso carico : il solo motore elettrico è attivo, il motore termico è spento,

   accelerazione/guida normale : il motore termico e quello elettrico forniscono ciascuno parte della potenza alle ruote, in proporzione variabile a seconda delle condizioni di marcia e della politica di gestione

Le altre fasi di guida sono comuni alle due strategie

decelerazione/frenata : il motore elettrico funge da generatore e ricarica le batterie,

ricarica batterie in movimento : durante la guida, il motore termico non solo fornisce potenza alle ruote, ma anche al generatore elettrico, che ricarica le batterie grazie al convertitore di potenza,

ricarica batterie da fermo : quando il veicolo è fermo, il motore termico può essere mantenuto in funzione per fornire potenza al generatore e ricaricare le batterie.

Capitolo 2

La normativa ISO26262

La normativa ISO26262 rappresenta un nuovo standard di sicurezza, sviluppato specificatamente per l'industria automobilistica, con il compito di supportare l'intero processo di sviluppo di componenti elettrici ed elettronici presenti a bordo di veicoli stradali destinati alla produzione in serie.

La prima edizione è stata pubblicata nel Novembre 2011 dalla *International Organization for Standardization* allo scopo di rimpiazzare, in ambito automotive, il precedente standard IEC-61508: tale standard di sicurezza era stato sviluppato originariamente per l'automazione e i processi industriali, non prestandosi quindi in maniera ottimale all'applicazione nel campo automobilistico.

La normativa è applicata a ciascun componente elettrico ed elettronico presente a bordo del veicolo, definendo come debba essere sviluppato il relativo sistema di sicurezza in modo da scongiurare, o ridurre al minimo, i rischi dovuti ad un suo malfunzionamento.
Lo standard ISO26262 è costituito da 10 sezioni

1. Vocabolario
2. Gestione della sicurezza funzionale
3. Fase concettuale
4. Sviluppo del prodotto a livello di sistema
5. Sviluppo del prodotto a livello hardware

6. Sviluppo del prodotto a livello software
7. Produzione e messa in funzione
8. Processi di supporto
9. Automotive Safety Integrity Level (ASIL)
10. Linee guida sullo standard ISO26262.

In questa trattazione viene analizzata nel dettaglio la sezione 3, intitolata *fase concettuale,* i cui obiettivi sono

- definire e descrivere un oggetto elettrico o elettronico presente a bordo di un veicolo
- identificare tutti i possibili malfunzionamenti cui può essere soggetto un componente
- classificare gli scenari operativi nei quali un malfunzionamento può risultare in una condizione di rischio
- formulare dei requisiti di sicurezza in modo da scongiurare, o rendere minima, la probabilità del verificarsi di una condizione di rischio in seguito ad un malfunzionamento.

2.1 Analisi e valutazione del rischio

Per ciascun oggetto elettrico ed elettronico devono essere individuati i malfunzionamenti che possano causare una condizione di rischio; tali malfunzionamenti devono poi essere classificati, andando ad analizzare tutte le possibili condizioni operative nelle quali possono verificarsi.
La classificazione di un malfunzionamento è basata sulla valutazione di tre parametri:

1. la probabilità di esposizione alla situazione operativa,
2. la severità dei danni fisici riportati da guidatore ed eventuali altre persone coinvolte,
3. la controllabilità dell'evento.

2.1.1 Probabiltà di esposizione

La stima della probabilità di esposizione richiede la valutazione di tutti gli scenari (definiti anche *situazioni operative*) nei quali può verificarsi il malfunzionamento in esame: a tale scopo, devono essere combinate tutte le possibili categorie che possano descrivere una situazione operativa, quali le condizioni stradali, la tipologia di strada percorsa, il tipo di manovra effettuata, le condizioni ambientali etc.. .

La probabilità di esposizione rappresenta una stima della probabilità di trovarsi in una condizione operativa, in accordo ad una scala di cinque valori, come illustrato nella Tabella 2.1

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Tabella 2.1: Classificazione della probabilità di esposizione

il livello $E0$ indica una condizione operativa che probabilmente mai si verificherà, mentre il livello $E4$ indica una situazione che si verificherà qusi certamente.

La probabilità di esposizione di una situazione può essere valutata rispetto alla frequenza, oppure rispetto alla durata dell'evento, come illustrato nelle tabelle seguenti

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average

Tabella 2.2: Classificazione della probabilità di esposizione rispetto alla frequenza della situazione

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time

Tabella 2.3: Classificazione della probabilità di esposizione rispetto alla durata della situazione

Tipici esempi di situazioni operative aventi classe di esposizione $E4$ (alta probabilità) sono

1. guida in strada urbana,
2. manovra di sorpasso in strada secondaria
3. manovre di accelerazione e frenata.

2.1.2 Severità

La classe di severità rappresenta una stima dell'entità dei danni fisici riportati dal guidatore e da eventuali altri partecipanti all'evento, in una scala di quattro valori come illustrato in Tabella 2.4

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Tabella 2.4: Classificazione della severità di un evento

Statistiche sulla gravità dei danni fisici riportati in caso di incidente possono facilitare l'assegnazione della classe di severità.

La stima della classe di severità può essere altresì svolta facendo riferimento alla classificazione AIS (*Abbreviated Injury Scale*) fornita dalla *Association for the Advancement of Automotive Medicine*, la quale classifica in sette livelli l'entità dei danni fisici riportabili in un incidente

- AIS 0: nessun danno riportato,
- AIS 1: danni lievi, quali ferite superficiali e piccole contusioni,
- AIS 2: danni moderati, quali ferite profonde, traumi con incoscienza fino a 15 minuti, fratture di lieve entità,
- AIS 3: danni severi (ma non rischio di vita), quali fratture a testa, costole e dislocazioni vertebrali,
- AIS 4: danni severi (con probabile sopravvivenza), quali gravi fratture alla testa con incoscienda fino a 12 ore,
- AIS 5: danni critici(con rischio di vita), quali gravi fratture cervicali con danni alla colonna vertebrale ed incoscienza superiore alle 12 ore
- AIS 6: danni fatali, quali gravi fratture cervicali e profonde ferite ad organi vitali.

Una volta individuata la scala AIS corrispondente, è possibile valutare la relativa classe di severità in accordo alla seguente tabella

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	— AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6

Tabella 2.5: Classificazione della severità di un evento in base alla scala AIS

Esempi di incidenti con classe di severità $S3$ (grave entità) sono

- collisione frontale/posteriore a media/alta velocità
- impatto laterale con oggetti stazionari (quali alberi, lampioni etc..) a media/alta velocità
- investimento di pedoni/ciclisti

2.1.3 Controllabilità

La classe di controllabilità di un evento rappresenta una stima della probabilità che il guidatore riesca a mantenere il controllo del veicolo, in modo da scongiurare o rendere minima l'entità dei danni riportati durante l'evento in analisi, ed è classificata in una scala di quattro valori come illustrato nella seguente tabella

Class of controllability (see Table 3)			
C0	**C1**	**C2**	**C3**
Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm

Tabella 2.6: Classificazione della controllabilità di un evento

Un aiuto all'attribuzione della classe di controllabilità può essere fornito da un modello di simulazione, con cui poter valutare l'entità dell'azione di controllo necessaria a mantenere il veicolo in sicurezza, una volta introdotto il guasto.

Tipiche situazioni aventi classe di controllabilità $C3$ (difficilmente controllabili) sono

- guasto al sistema ABS durante una frenata di emergenza in strada scivolosa
- apertura involontaria dell'airbag durante una manovra
- non corretto angolo di sterzo durante una manovra.

2.2 Determinazione degli ASIL e degli Obiettivi di Sicurezza

Il passaggio successivo all'assegnazione delle classi di Esposizione, Severità e Controllabilità, è la determinazione del livello *ASIL*.
Un ASIL (*Automotive Safety Integrity Level*) definisce i requisiti di sicurezza che un componente deve soddisfare in modo che, anche in condizioni di guasto, possa essere garantito un sufficiente margine di sicurezza per il guidatore e qualunque altra persona coinvolta.

In Tabella 2.7 è illustrata la modalità di determinazione di un ASIL, sulla base dei tre parametri illustrati nel precedente paragrafo; un ASIL è classificato in una scala che va da QM (valore minimo, che non richiede alcun requisito di sicurezza) a D (valore massimo attribuibile).

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabella 2.7: Determinazione di un ASIL in base a Esposizione, Severità e Controllabilità di un evento

Per ciascuna situazione operativa avente $ASIL > QM$, devono essere formulati uno o più *obiettivi di sicurezza*: un obiettivo di sicurezza (*Safety Goal*) rappresenta un requisito che deve essere rispettato, al fine di scongiurare qualunque rischio relativo ad una situazione di pericolo. Ciascun obiettivo di sicurezza eredita il livello ASIL del corrispondente evento di rischio: se simili obiettivi di sicurezza vengono formulati per eventi diversi, essi vanno combinati in un unico obiettivo di sicurezza avente livello ASIL più alto fra quelli considerati.

Capitolo 3

Strumento software per l'applicazione della normativa

Allo stato dell'arte attuale, l'applicazione della normativa avviene mediante lavoro di gruppo, affidandosi al know-how aziendale e all'esperienza dei singoli, facendo scarso uso di strumenti di supporto: si è quindi sviluppato uno strumento innovativo, in ambiente Matlab/Simulink, in grado di fornire assistenza all'utente durante l'intera fase di applicazione della normativa. Il primo passo risulta quello di generare tutte le possibili combinazioni degli scenari in cui un malfunzionamento può verificarsi: tale operazione risulta però molto complessa dal punto di vista computazionale, in quanto il numero di combinazioni cresce esponenzialmente con l'aumentare delle tipologie di scenari: il software realizzato, per mezzo di una interfaccia grafica user-friendly, automatizza l'intero processo di creazione e gestione, fornendo istantaneamente all'utente una lista di situazioni operative (eventualmente privata di una o più classificazioni, a scelta dell'utente).

In aggiunta, il software permette di gestire le classificazioni delle situazioni operative, i malfunzionamenti di ciascun componente e l'assegnazione degli ASIL.

Grazie alla sua versatilità, è possibile effettuare modifiche in corso d'opera senza riformulare il problema dalla base, come accade attualmente facendo uso di strumenti di gestione tabellare.

3.1 Gestione del database delle situazioni

Questo pannello permette di gestire le categorie utilizzate per la descrizione di uno scenario, quali la tipologia di strada percorsa, le condizioni meteorologiche, il tipo di manovra, le condizioni del manto stradale etc...: ogni elemento appartenente ad una categoria ne descrive un possibile valore, ed è caratterizzato da una propria classe di Esposizione (illustrata nella sezione 2.1.1). In Figura 3.1 è illustrato il pannello di gestione del database delle situazioni

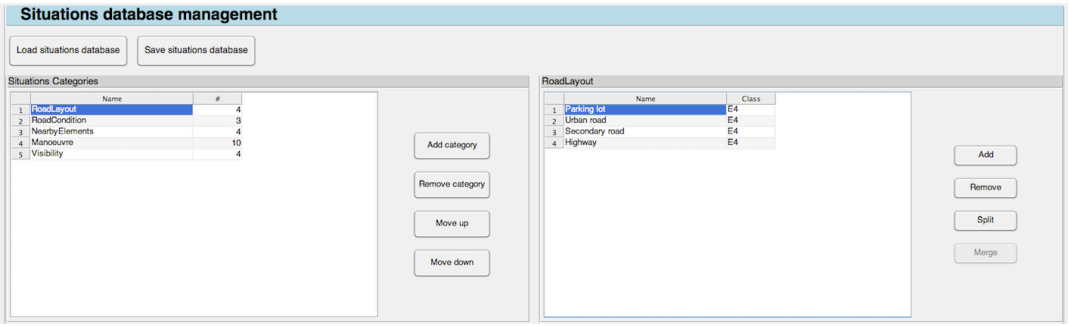

Figura 3.1: Pannello di gestione del database delle situazioni operative

tra le opzioni disponibili vi è l'opportunità di salvare un database, o di caricarne uno preesistente in memoria; su di un database, una volta caricato, possono essere effettuate varie operazioni quali

- aggiunta/rimozione di una specifica categoria
- aggiunta/rimozione di elementi appartenenti ad una categoria
- possibilità di unire più elementi di una categoria, a formare un unico elemento (la cui classe di esposizione viene valutata come combinazione dei vari elementi).

Una corretta gestione del database delle situazioni operative consentirà di produrre una lista di casi d'uso esaustiva e coerente.

3.2 Gestione del database di componenti e malfunzionamenti

Questo pannello ha lo scopo di gestire un database contenente i componenti elettrici ed elettronici, divisi per categoria, e per ciascuno di essi poter definire i malfunzionamenti cui può essere soggetto. Tale database sarà poi utilizzato nel pannello di creazione del layout, ed i relativi malfunzionamenti costituiranno la relativa analisi di rischio. Il pannello di gestione di componenti e malfunzionamenti è illustrato in Figura 3.2

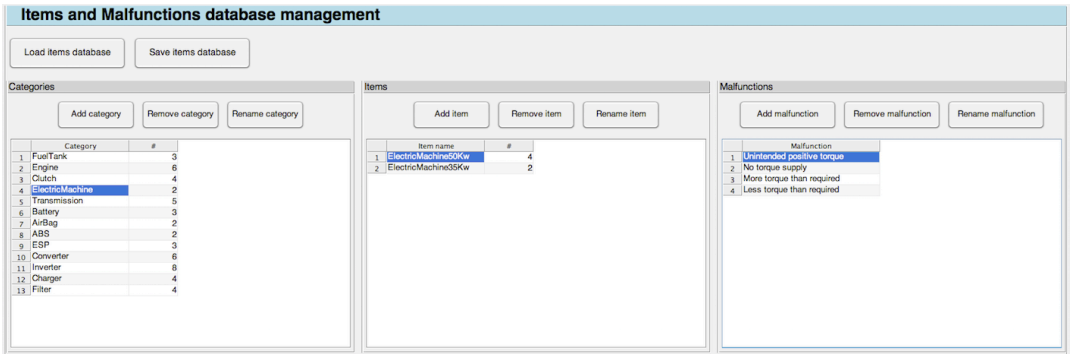

Figura 3.2: Pannello di gestione del database degli oggetti e dei malfunzionamenti

come per il caso precedente, c'è la possibilità di salvare o caricare un database preesistente; inoltre, sul database possono essere effettuate operazioni quali

- aggiunta/rimozione di una categoria di componenti
- aggiunta/rimozione di componenti appartenenti ad una categoria
- aggiunta/rimozione/rinominazione di malfunzionamenti relativi ad un componente

3.3 Definizione del layout

Questo pannello ha lo scopo di definire un layout di powertrain, fra i seguenti disponibili

- powertrain ibrido serie,
- powertrain ibrido parallelo,
- powertrin ibrido di tipo powersplit.

Una volta selezionato il tipo di powertrain, si può caricare il database dei componenti (o scegliere di utilizzarne uno di default). Per ciascun elemento appartenente al layout, viene elencata la rispettiva categoria nel database, in modo da scegliere quello corretto da aggiungere al layout; in basso a destra è rappresentato lo schema a blocchi del layout scelto. In Figura 3.3 è illustrato il pannello di definizione del layout

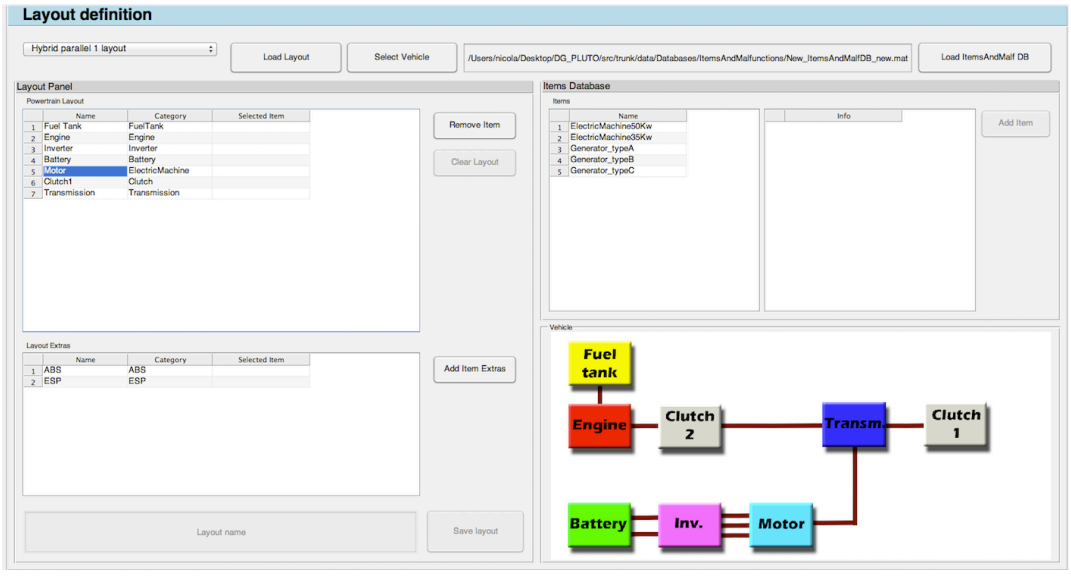

Figura 3.3: Pannello di gestione del layout

nella finestra in alto a sinistra sono elencati gli oggetti appartenenti al layout scelto; una volta aggiunti tutti gli elelemti, il layout può essere salvato ed utilizzato nella fase successiva, relativa all'analisi ASIL per i malfunzionamenti dei componenti.

3.4 Definizione delle situazioni operative e degli ASIL

Questo pannello costituisce il nucleo centrale dell'analisi.

In Figura 3.4 è illustrato il pannello mediante cui l'utente può scegliere quali elementi includere nella generazione delle situazioni operative: tale scelta è di estrema importanza, in quanto ciascun malfunzionamento avrà un diverso insieme di situazioni operative nelle quali può causare un rischio, quindi includere tutte risulterebbe sbagliato (portando inoltre alla creazione di migliaia di combinazioni); a tale scopo, il pannello permette all'utente di escludere una o più categorie, e uno o più elementi appartenenti ad una categoria, in modo da ridurre il numero di combinazioni.

Come esempio, immaginiamo di dover analizzare il malfunzionamento relativo al repentino calo di coppia fornita dalla macchina elettrica; nella realizzazione delle situazioni operative, parametri come visibilità o elementi nelle vicinanze non risultano di interesse, come manovre di parcheggio o frenata: escludendo quindi gli elementi sopracitati dalla creazione delle combinazioni, verranno generate solo situazioni operative di interesse per il malfunzionamento specifico.

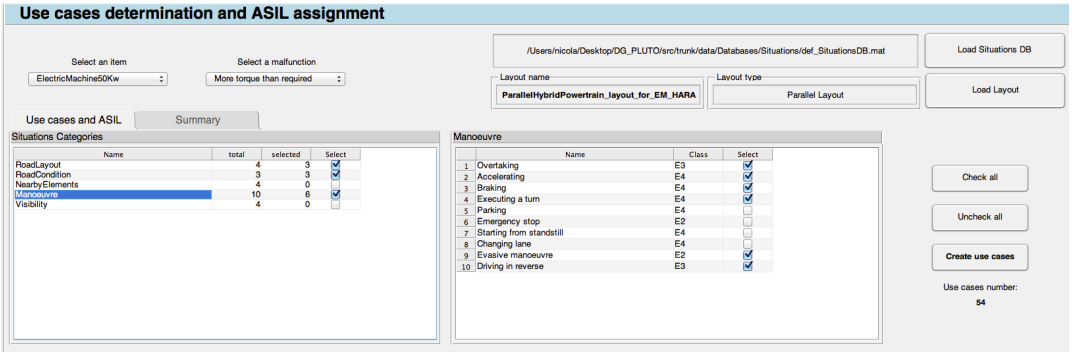

Figura 3.4: Pannello creazione delle situazioni operative

Una volta realizzate tutte le combinazioni, nel pannello inferiore l'utente avrà la possibilità di assegnare a ciascuna la rispettiva classe di Severità e Controllabilità, in accordo a quanto visto nel capitolo(INTRODUZIONE ISO), e quindi procedere all'assegnazione automatica degli ASIL come illustrato in Figura 3.5

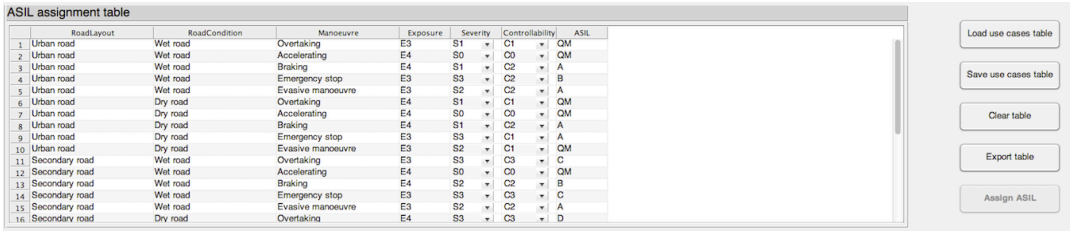

Figura 3.5: Pannello di assegnazione delle classi di Severità e Controllabilità e degli ASIL

Dal momento che la fase di assegnazione delle classi di Severità e Controllabilita potrebbe risultare molto lunga, è possibile salvare i progressi per poterli ricaricare in un secondo momento e così non perdere il lavoro svolto.

Assegnati gli ASIL, in un successivo pannello saranno riassunte le sole condizioni operative avrnti un $ASIL > QM$, come illustrato in Figura 3.6

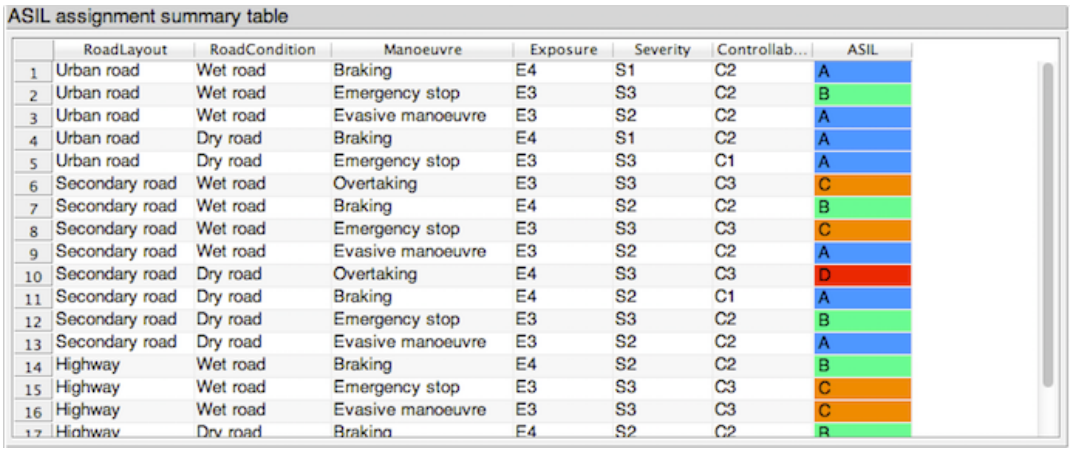

Figura 3.6: Pannello riassuntivo dell'assegnazione degli ASIL

per tali condizioni operative dovranno essere quindi stabiliti degli obiettivi di sicurezza.

Il pannello delle opzioni permette di impostare i percorsi di default in cui salvare automaticamente i database delle situazioni, dei malfunzionamenti e dei layout. I percorsi posso essere impostati sia per la sola sessione in corso, sia come default per tutte le sessioni dell'interfaccia grafica, come illustrato nelle Figure 3.7 e 3.8

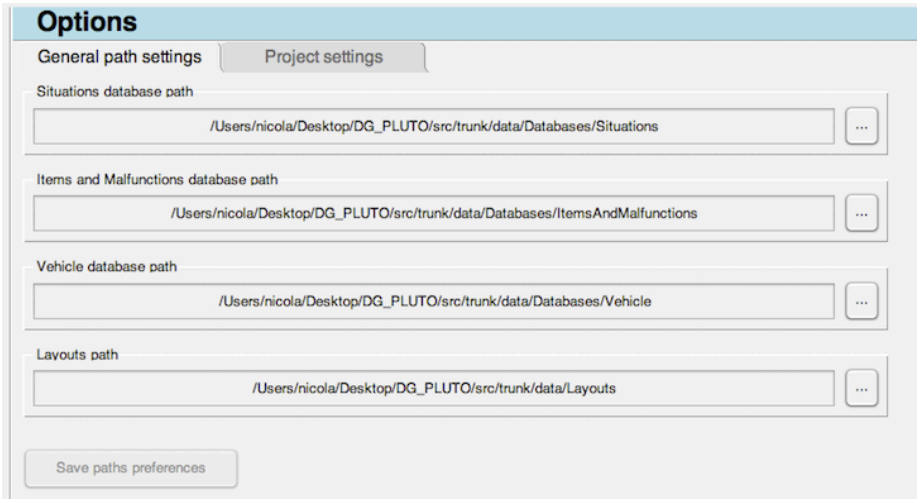

Figura 3.7: Pannello opzioni per i percorsi di default

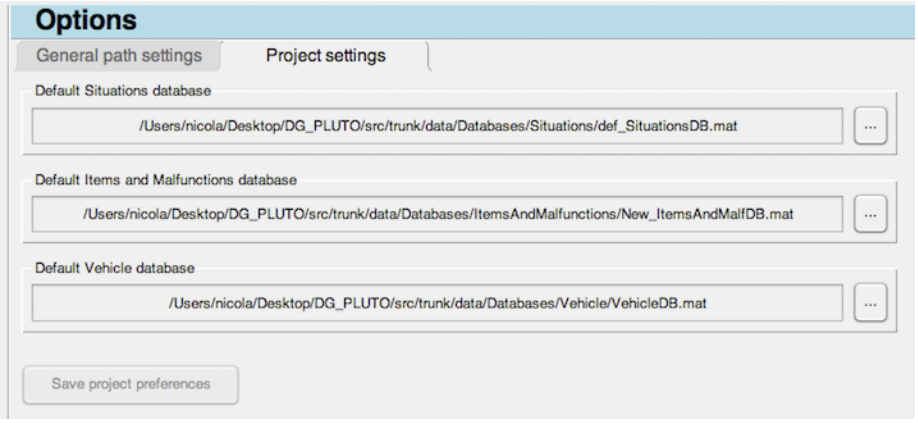

Figura 3.8: Pannello di opzioni per i percorsi della sessione in corso

Capitolo 4

Il modello di Powertrain

In questo capitolo è descritto nel dettaglio il modello di Powertrain adottato per svolgere le simulazioni.

L'architettura in esame non è di tipo parallelo standard: non è presente infatti un reale organo meccanico ripartitore di coppia, come spiegato nella sezione 1.1.2 a pagina 8, ma il motore termico e la macchina elettrica sono collegati tra loro sul medesimo interasse, che trasmette la coppia generata al cambio marcia. In questo caso il motore termico è inserito prima della macchina elettrica, che viene posizionata sull'interasse che trasmette la coppia generata dal motore termico cosi che le coppie dei due motori vengono sommate. L'architettura complessiva è rappresentata in figura 4.1

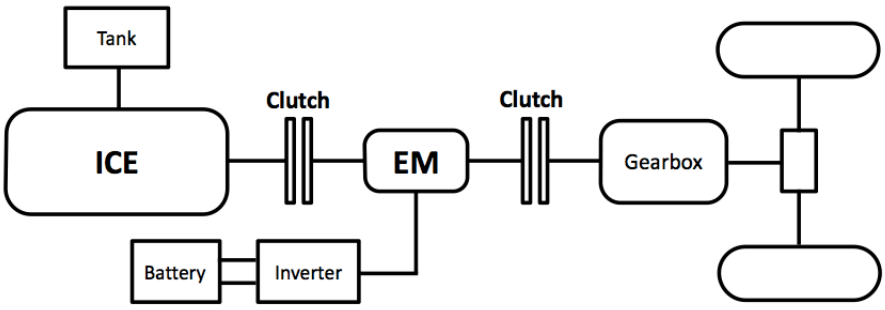

Figura 4.1: Architettura di Powertrain parallelo in esame

Si noti anche la presenza di due frizioni: la prima è posta a valle del motore termico ed ha il compito di disconnetterlo dalla trasmissione, la seconda è posta

a valle della macchina elettrica ed ha il compito di disconnettere entrambe le fonti di potenza dalla trasmissione.

I componenti presenti nel Powertrain sono i seguenti

- La batteria,
- la macchina elettrica,
- l'inverter,
- il motore termico,
- le frizioni,
- la scatola del cambio,
- l'albero di trasmissione,
- la logica di controllo.

4.1 Il modello della batteria

Il modello dinamico della batteria al litio rispetta il comportamento ingresso uscita delle batterie utilizzate nelle autovetture.

La batteria è stata modellata con un circuito equivalente che riesce a riprodurre il comportamento della tensione di batteria sulla base della corrente di carica o di scarica. Il circuito equivalente risultante è illustrato in figura 4.2.

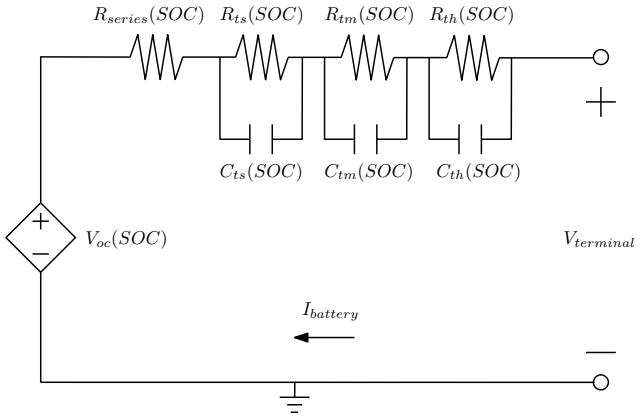

Figura 4.2: Circuito equivalente della batteria

La tensione in uscita dalla batteria risulta pari alla tensione di uscita del circuito equivalente $V_{terminal}$, in cui è presente un generatore di tensione controllato dal valore dello stato di carica (SOC) e da una serie di tre paralleli $R-C$ che riproducono il comportamento dinamico della batteria su orizzonti temporali rispettivamente dei secondi, dei minuti e delle ore. I valori di R e C variano anch'essi in base al valore dello stato di carica della batteria. Nel caso di studio sono state mantenute solamente le dinamiche dell'ordine dei minuti e delle ore.

Risulta di estrema importanza modellare la dipendenza che c'è tra la capacità effettiva della batteria e l'entità delle correnti con cui la stessa viene ricaricata o scaricata: per questo si ricava il valore dello stato di carica SOC in accordo all'equazione 4.1:

$$SOC = SOC_0 + \int_0^t f\left(i\left(t\right)\right) i\left(t\right) dt \tag{4.1}$$

dove $i\left(t\right)$ è il fattore di scarica (o carica) della batteria ed f indica una funzione peso sulla velocità di scarica (o di carica) e che può essere ricavata dal datasheet

del componente.

Affiancato alla batteria è presente un convertitore DC/DC che mantiene il livello di tensione del bus al valore prefissato.
Si passa quindi a descrivere le equazioni implementate nel modello della batteria. Partendo dall'equazione 4.1, derivando ambo i membri si ottiene

$$S\dot{O}C = -\frac{f_{influence}\left(i\left(t\right)\right)D_r}{3600} \qquad D_r = \frac{i\left(t\right)}{C_b} \tag{4.2}$$

dove $f_{influence}$ è una funzione dipendente dalla corrente che modella l'influenza della corrente nello stato di carica, mentre C_b rappresenta la capacità della batteria. La corrente nell'equazione è quella proveniente dal convertitore DC/DC ed è calcolata come segue

$$i\left(t\right) = \begin{cases} \frac{I_{less}Vdc}{V_{batt}}\eta^{-1} & \text{for } I_{less}Vdc > 0 \\ \frac{I_{less}Vdc}{V_{batt}}\eta & \text{for } I_{less}Vdc \leq 0 \end{cases} \tag{4.3}$$

dove la grandezza Vdc sta ad indicare la tensione del bus, mentre I_{less} e V_{batt} sono definite rispettivamente

$$I_{less} = \frac{P_E - P_{aux}}{Vdc} \tag{4.4}$$

$$V_{batt} = \frac{Voc - V_{transiet}}{n_{cells}} \tag{4.5}$$

P_E rappresenta la potenza della macchina elettrica, P_{aux} rappresenta invece una potenza ausiliaria che nel nostro modello è posta a zero, n_{cells} indica il numero di celle della batteria, Voc rappresenta la tensione a circuito aperto che, come illustrato nella figura 4.2, dipende dallo stato di carica SOC e si valuta come segue

$$Voc = Voc_{[1,7]}SOC^T_{[1,7]} \qquad SOC^T_{[1,7]} = \begin{bmatrix} 1 & SOC & \cdots & SOC^6 \end{bmatrix} \tag{4.6}$$

$V_{transiet}$ è una tensione che viene calcolata secondo la formula

$$V_{transiet} = \begin{cases} R_{series_c}i_{[0,\infty]} + V & \text{for } i \in [0,\infty] \\ R_{series_d}i_{[-\infty,0]} + V & \text{for } i \in [-\infty,0] \end{cases} \tag{4.7}$$

le resistenze $R_{series_{c,d}}$, dipendenti dalla variabile SOC, sono calcolate come segue

$$R_{series_i} = Voc_{[1,7]} SOC^T_{[1,7]} \tag{4.8}$$

dove $i = \{\text{charge}, \text{discharge}\}$e la matrice $SOC^T_{[1,7]}$ha lo stesso valore di quella in formula 4.6, mentre la tensione V ha il seguente valore

$$V = \int \left(b_1 i + \int (b_0 i - a_0 V) - a_1 V \right) \tag{4.9}$$

i coefficienti a_0, a_1, b_0 e b_1 hanno come espressione

$$a_0 = \frac{1}{Rtm \cdot Rth \cdot Ctm \cdot Cth} \qquad a_1 = a_0 \left(Rtm \cdot Ctm + Rth \cdot Cth \right) \tag{4.10}$$

$$b_0 = a_0 \left(Rtm + Rth \right) \qquad b_1 = \frac{1}{Ctm} + \frac{1}{Cth} \tag{4.11}$$

Rtm, Rth, Ctm eCth rappresentano rispettivamente le resistenze e le capacità illustrate nella figura 4.2 del circuito equivalente, e sono di due tipi: nel caso di carica o di scarica della batteria. Sono dipendenti dal SOC e vengono calcolati come segue

$$Rtm_i = Rtm_{i[1,7]} SOC^T_{[1,7]} \tag{4.12}$$

dove $i = \{\text{charge}, \text{discharge}\}$, identicamente anche gli altri coefficienti vengono calcolati nello stesso modo.

Il modello Simulink risultante è quello mostrato in figura 4.3, nel dettaglio è presentato il modello della batteria a Litio e del convertitore DC/DC nella figura 4.4, mentre in figura 4.5 è mostrato l'interno del blocco della batteria a Litio

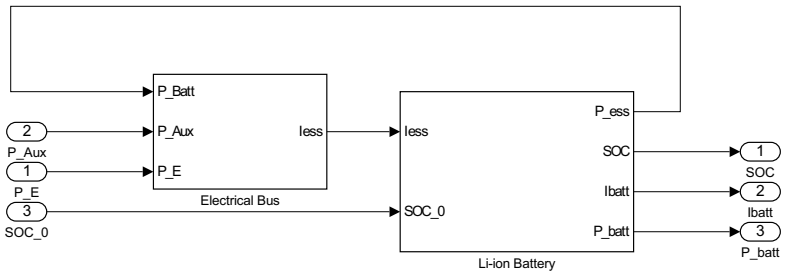

Figura 4.3: Modello Simulink della batteria e del bus di corrente

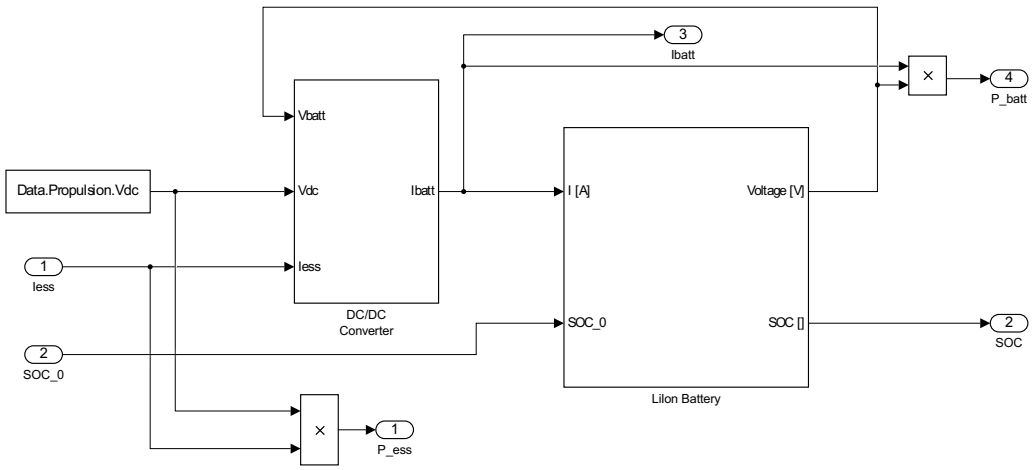

Figura 4.4: Modello Simulink della batteria a Litio e del Convertitore DC/DC

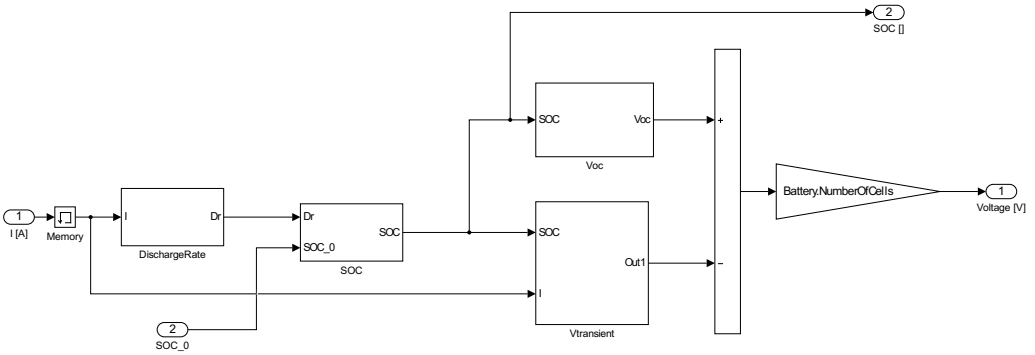

Figura 4.5: Interno del modello Simulink della batteria a Litio

4.2 Il modello della macchina elettrica

La macchina elettrica utilizzata nel modello di Powertrain è un motore sincrono a magneti permanenti, affermatosi negli ultimi anni tra le varie tipologie di motore sincrono grazie a numerosi vantaggi che questo tipo di macchina fornisce rispetto alle altre macchine in corrente alternata e in corrente continua.

Nei motori ad induzione, il vettore rotante rappresentativo della corrente statorica è composto da due componenti ortogonali: la corrente di magnetizzazione (che genera il flusso di rotore) e la corrente di coppia (che genera la coppia elettromeccanica al traferro). Nei motori sincroni a magneti permanenti l'utilizzo dei magneti, che vanno a sostituire l'avvolgimento di eccitazione delle macchine sincrone convenzionali, non rende necessaria (nelle macchine sincrone a magneti permanenti superficiali) la componente magnetizzante del vettore rappresentativo della corrente statorica nel funzionamento a flusso al traferro costante. Conseguentemente, a parità di condizioni di carico, il PMSM (*Permanent Magnet Synchronous Motors*) presenta fattori di potenza e rendimento maggiori rispetto al tradizionale motore ad induzione.

La macchina sincrona convenzionale necessita di un'alimentazione in continua dell'avvolgimento di campo, fornita mediante un sistema di spazzole ed anelli che causa perdite nel rame di rotore e richiede una continua manutenzione delle spazzole e degli anelli. L'impiego di magneti permanenti in sostituzione dell'avvolgimento di campo, dell'alimentazione in continua e del collettore consente di eliminare tutti gli svantaggi elencati precedentemente.

I motori sincroni a magneti permanenti sono realizzati in due configurazioni base, illustrate in figura 4.6:

- Motori sincroni a magneti permanenti superficiali: i magneti sono montati sulla superficie del rotore,
- Motori sincroni a magneti permanenti interni: i magneti sono allocati all'interno della struttura del rotore.

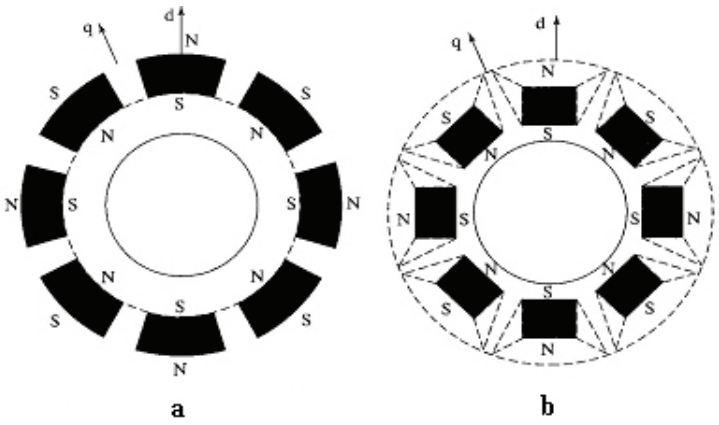

Figura 4.6: Sezioni trasversali dei rotori di motori PMSM superficiali detti SPMSM (a) e interni detti IPMSM (b)

Il motore sincrono a magneti permanenti è costituito fondamentalmente da uno statore, nelle cui cave sono disposti gli avvolgimenti trifase, costituiti da matasse deposte a 120 gradi elettrici tra loro e alimentati da tensioni sinusoidali e da un rotore nel quale i magneti permanenti producono un campo diretto lungo l'asse degli stessi. Nella derivazione delle equazioni per l'implementazione in Simulink di un PMSM si fanno le seguenti assunzioni:

- Saturazione trascurabile
- Andamento della f.c.e.m. di tipo sinusoidale
- Effetto delle correnti parassite trascurabile.

Nel caso in cui siano valide le precedenti assunzioni, le equazioni della tensione di statore del motore PMSM, nel sistema di riferimento $d-q$ di rotore risultano

$$v_d = Ri_d + \dot{\lambda}_d - \omega_r \lambda_q \tag{4.13}$$

$$v_q = Ri_d + \dot{\lambda}_q - \omega_r \lambda_d \tag{4.14}$$

dove R è la resistenza degli avvolgimenti di statore (generalmente uguali in ogni avvolgimento), ω_r è la velocità angolare di rotazione del sistema di riferimento $d-q$ rispetto allo statore e $\lambda_{d,q}$ sono i flussi concatenati che hanno l'espressione

$$\lambda_q = L_q i_q \tag{4.15}$$

$$\lambda_d = L_d i_d + \lambda_{af} \tag{4.16}$$

il flusso magnetico indotto è rappresentato dal coefficiente λ_{af} mentre $L_{d,q}$ sono le induttanze di magnetizzazione lungo gli assi $d-q$.

La coppia elettromagnetica sviluppata è pari a

$$T_{em} = \frac{3}{2} P \left[\lambda_{af} i_q + \left(L_d - L_q \right) i_d i_q \right] \tag{4.17}$$

dove P indica il numero di coppie polari. Durante il funzionamento a flusso costante, quando i_d diventa nulla, la coppia elettromotrice dell'equazione 4.17 diviene

$$T_{em} = \frac{3}{2} P \lambda_{af} i_q = K_t i_q \tag{4.18}$$

in cui K_t è la costante di coppia del motore. In forma di equazioni di stato il sistema risulta

$$\dot{i}_d = \frac{1}{L_d} \left(v_d - R i_d + \omega_r L_q i_q \right) \tag{4.19}$$

$$\dot{i}_q = \frac{1}{L_q} \left(v_q - R i_d + \omega_r L_q i_q - \omega_r \lambda_{af} \right) \tag{4.20}$$

$$\dot{\omega}_r = \frac{1}{J} \left(T_{em} - B \omega_r - T_t \right) \tag{4.21}$$

$$\dot{\theta}_r = \omega_r \tag{4.22}$$

La macchina elettrica viene controllata in coppia; il sistema di controllo invia la coppia di riferimento all'inverter che attua le correnti necessarie alla macchina elettrica per generare la coppia richiesta. Il controllo in coppia implementato è un controllo vettoriale, il quale prende in ingresso la coppia di riferimento T_{ref} e calcola direttamente la componente in quadratura (lungo l'asse q) della corrente di riferimento $i_{q_{ref}}$ come

$$i_{q_{ref}} = \frac{2}{3} \frac{T_{ref}}{\lambda_{af} P} \tag{4.23}$$

mentre il riferimento per la componente diretta è $i_{d_{ref}} = 0$.

Per mantenere gli ingressi e le uscite dell'inverter e del motore elettrico solidali a quelli reali, una volta trovata la corrente di riferimento $i_{q_{ref}}$ la si trasforma nel sistema di riferimento in fase $a-b-c$ attraverso la matrice di

Park, così definita

$$\begin{bmatrix} v_a \\ v_b \\ v_c \end{bmatrix} = \underbrace{\sqrt{\frac{2}{3}} \begin{bmatrix} \cos(\theta) & -\sin(\theta) & 1/\sqrt{2} \\ \cos(\theta - 2\pi/3) & -\sin(\theta - 2\pi/3) & 1/\sqrt{2} \\ \cos(\theta + 2\pi/3) & -\sin(\theta + 2\pi/3) & 1/\sqrt{2} \end{bmatrix}}_{\text{Matrice di Park}} \begin{bmatrix} v_q \\ v_d \\ v_0 \end{bmatrix} \tag{4.24}$$

al contrario la trasformazione inversa da coordinate $a-b-c$ a coordinate $d-q$ avviene attraverso la trasformazione inversa di Park

$$\begin{bmatrix} v_q \\ v_d \\ v_0 \end{bmatrix} = \sqrt{\frac{2}{3}} \begin{bmatrix} \cos(\theta) & \cos(\theta - 2\pi/3) & \cos(\theta + 2\pi/3) \\ -\sin(\theta) & -\sin(\theta - 2\pi/3) & -\sin(\theta + 2\pi/3) \\ 1/\sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} v_a \\ v_b \\ v_c \end{bmatrix} \tag{4.25}$$

In entrambe le trasformazioni è stato indicato con θ l'angolo di rotore.

La potenza elettrica totale entrante nella macchina elettrica, in termini delle grandezze nel sistema di riferimento $a - b - c$, è la seguente

$$P_{em} = v_a i_a + v_b i_b + v_c i_c \tag{4.26}$$

al contrario, in termini delle grandezze nel sistema di riferimento $d - q$ è la seguente

$$P_{em} = \frac{3}{2}(v_d i_d + v_q i_q) \tag{4.27}$$

come si può notare la trasformazione di Park non mantiene invariata la potenza.

Si osserva come modellare il motore PMSM nel sistema di riferimento $d - q$ di rotore porta (nelle ipotesi avanzate ad inizio paragrafo, in particolare nell'ipotesi di f.c.e.m. sinusoidale) a scrivere equazioni dinamiche relativamente semplici.

Nella figura 4.7 si mostra l'andamento della coppia massima e minima che la PMSM in esame può generare

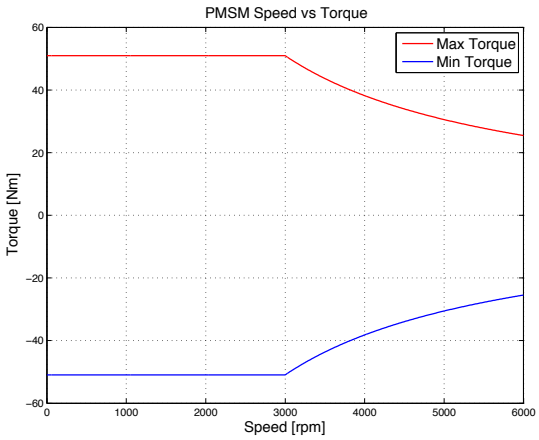

Figura 4.7: Andamento della coppia massima e minima della PMSM al variare dei giri al minuto

In figura 4.8 viene mostrata invece l'implementazione in Simulink della macchina elettrica

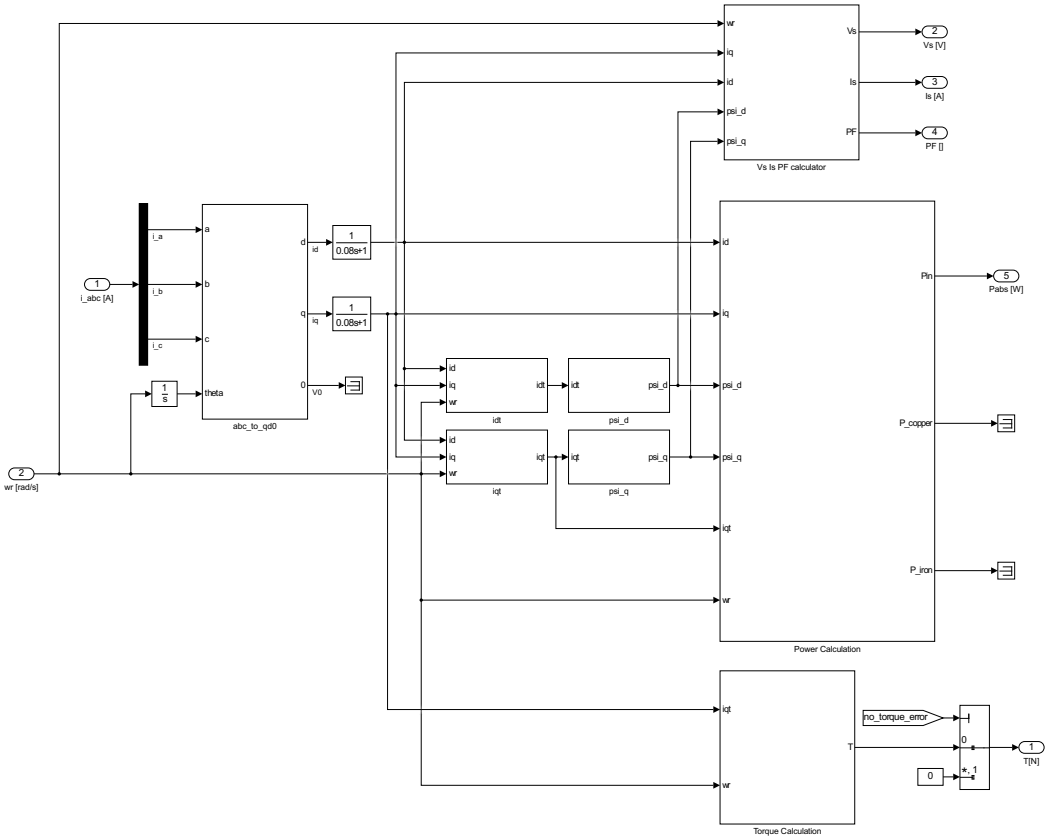

Figura 4.8: Modello Simulink della PMSM

4.3 Il modello dell'inverter

Al fine di calcolare le perdite che si verificano nell'inverter si utilizza un modello che, a partire dalle misure di corrente e tensione, fornisce le perdite sui transistor e sui diodi che compongono il convertitore. L'inverter viene quindi considerato come la composizione di tre rami, ciascuno composto da due IGBT e da due diodi di ricircolo.

Nel caso di modulazione PWM naturale si può considerare ciascun ramo dell'inverter come un chopper mostrato in figura 4.9, il cui duty cycle sia modulato in maniera sinusoidale con periodo T.

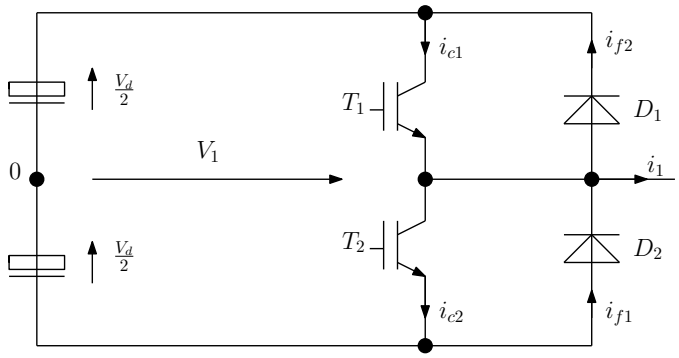

Figura 4.9: Chopped che modella ciascun ramo dell'inverter

In questo caso la corrente che attraversa ogni ramo può essere supposta anch'essa sinusoidale (di periodo T).

Durante la condizione di transizione (che si realizza nel primo semiperiodo), le perdite interessano l'IGBT T_1 (durante la conduzione) e il diodo D_2 (durante l'interdizione). Viceversa, durante la condizione di frenatura (che si realizza nel secondo semiperiodo), le perdite interessano l'IGBT T_2 (durante la conduzione) e il diodo D_1 (durante l'interdizione).

Le perdite che si sperimentano istantaneamente su ciascun dispositivo (sia esso un transistor o un diodo) si possono ottenere moltiplicando la corrente che attraversa il dispositivo per la tensione ai suoi capi.

Quando il periodo T delle grandezze sinusoidali è sufficientemente piccolo rispetto alla dinamica di variazione delle perdite che si vogliono calcolare, può essere sufficiente andare a considerare i valori medi delle perdite, anziché quelli istantanei.

Le curve che esprimono le caratteristiche tensione-corrente e le perdite energetiche di commutazione degli IGBT e dei diodi possono essere generalmente approssimate analiticamente con polinomi del 1^oe 2^o ordine

$$\begin{cases} y = A + Bx \\ y = A + Bx + Cx^2 \end{cases} \tag{4.28}$$

Le equazioni che indicano le approssimazioni analitiche delle caratteristiche tensione-corrente rispettivamente degli IGBT e dei diodi sono

$$\begin{cases} V_{ce}\left(i_c\right) = A_{fw_T} + B_{fw_T} i_c \\ V_F\left(i_d\right) = A_{fw_D} + B_{fw_D} i_f \end{cases} \tag{4.29}$$

mentre le approssimazioni analitiche delle perdite energetiche di commutazione rispettivamente per l'attivazione degli IGBT, lo spegnimento degli IGBT e lo spegnimento dei diodi hanno la forma

$$\begin{cases} E_{on_T}\left(i_c\right) = B_{on_T} i_c + C_{on_T} i_c^2 \\ E_{off_T}\left(i_c\right) = B_{off_T} i_c + C_{off_T} i_c^2 \\ E_{rec_D}\left(i_f\right) = B_{rec_D} i_f + C_{rec_D} i_f^2 \end{cases} \tag{4.30}$$

I vari coefficienti A, B e C che compaiono nelle diverse equazioni possono essere ricavati a partire dalle curve caratteristiche generalmente fornite dai costruttori dei dispositivi a semiconduttore.

Riprendiamo l'apposizione fatta, tale che la corrente sia sinusoidale

$$i = I_M \sin\left(\omega t\right) \tag{4.31}$$

si considerano ora solamente le perdite che si verificano durante la semionda positiva, visto che quelle relative alla semionda negativa sono esattamente le stesse. Si possono quindi esprimere le perdite istantanee di conduzione

nell'IGBT T_1 come

$$\begin{aligned} P_{fw_T}\left(i_c\left(t\right)\right) &= v_{ce}\left(i_c\left(t\right)\right) i_c\left(t\right) \\ &= \left[A_{fw_T} + B_{fw_T} i_c\left(t\right)\right] i_c\left(t\right) \delta\left(t\right) \\ &= I_M \left[A_{fw_T} \sin\left(\omega t\right) + B_{fw_T} I_M \sin^2\left(\omega t\right)\right] \delta\left(t\right) \end{aligned} \tag{4.32}$$

Le perdite di commutazione si possono invece esprimere rispettivamente per l'accensione e lo spegnimento come

$$\begin{aligned} P_{on_T}\left(i_c\left(t\right)\right) &= f_c \left[B_{on_T} i_c\left(t\right) + C_{on_T} i_c^2\left(t\right)\right] \\ &= f_c I_M \sin\left(\omega t\right) \left[B_{on_T} + C_{on_T} I_M \sin\left(\omega t\right)\right] \end{aligned} \tag{4.33}$$

$$\begin{aligned} P_{off_T}\left(i_c\left(t\right)\right) &= f_c \left[B_{off_T} i_c\left(t\right) + C_{off_T} i_c^2\left(t\right)\right] \\ &= f_c I_M \sin\left(\omega t\right) \left[B_{off_T} + C_{off_T} I_M \sin\left(\omega t\right)\right] \end{aligned} \tag{4.34}$$

Allo stesso modo si possono esprimere le perdite di conduzione del diodo D_2 come

$$\begin{aligned} P_{fw_D}\left(i_f\left(t\right)\right) &= v_f\left(i_f\left(t\right)\right) i_f\left(t\right) \\ &= \left[A_{fw_D} + B_{fw_D} i_f\left(t\right)\right] i_f\left(t\right) \\ &= I_M \left[A_{fw_D} \sin\left(\omega t\right) + B_{fw_D} I_M \sin^2\left(\omega t\right)\right] \left(1 - \delta\left(t\right)\right) \end{aligned} \tag{4.35}$$

in tutte le equazioni scritte si è indicato con $\delta\left(t\right)$ il duty cycle. Se si ipotizza il duty cycle modulato in modo sinusoidale questo risulterà

$$\delta\left(t\right) = \frac{1}{2} + \frac{1}{2} m \sin\left(\omega t + \phi\right) \tag{4.36}$$

Ciascun ramo dell'inverter, durante la commutazione di conduzione tra gli IGBT, necessita per funzionare correttamente di un intervallo temporale T_{dead} in cui entrambi i transistor sono aperti. Durante questo intervallo temporale conduce da subito il diodo in antiparallelo al transistor che passa dalla conduzione all'interdizione. A causa di ciò, il duty cycle espresso nell'equazione 4.36 deve essere modificato nel seguente modo

$$\delta\left(t\right) = \left(\frac{1}{2} - \frac{T_{dead}}{T_s}\right) + \frac{1}{2} m \sin\left(\omega t + \phi\right) \tag{4.37}$$

dove T_s rappresenta il periodo di commutazione.

Se si inserisce l'equazione 4.37 per il duty cycle nelle equazioni precedenti delle perdite, e se ne estrae successivamente il valor medio sul periodo T della fondamentale si ottengono, per diversi contributi di perdita

$$\begin{cases} P_{fw_T} = \left(\frac{1}{2} - \frac{T_{dead}}{T_s}\right)\left(\frac{A_{fw_T}}{\pi} I_M + \frac{B_{fw_T}}{4} I_M^2\right) + m\cos(\phi)\left(\frac{A_{fw_T}}{8} I_M + \frac{B_{fw_T}}{3\pi} I_M^2\right) \\ P_{fw_D} = \left(\frac{1}{2} + \frac{T_{dead}}{T_s}\right)\left(\frac{A_{fw_D}}{\pi} I_M + \frac{B_{fw_D}}{4} I_M^2\right) - m\cos(\phi)\left(\frac{A_{fw_D}}{8} I_M + \frac{B_{fw_D}}{3\pi} I_M^2\right) \end{cases} \tag{4.38}$$

$$\begin{cases} P_{on_T} = f_s I_M \left(\frac{B_{on_T}}{\pi} + \frac{C_{on_T}}{4} I_M\right) \\ P_{off_T} = f_s I_M \left(\frac{B_{off_T}}{\pi} + \frac{C_{off_T}}{4} I_M\right) \\ P_{rec_D} = f_s I_M \left(\frac{B_{rec_D}}{\pi} + \frac{C_{rec_D}}{4} I_M\right) \end{cases} \tag{4.39}$$

Il blocco inverter nel modello Simulink ha la forma illustrata in figura 4.10

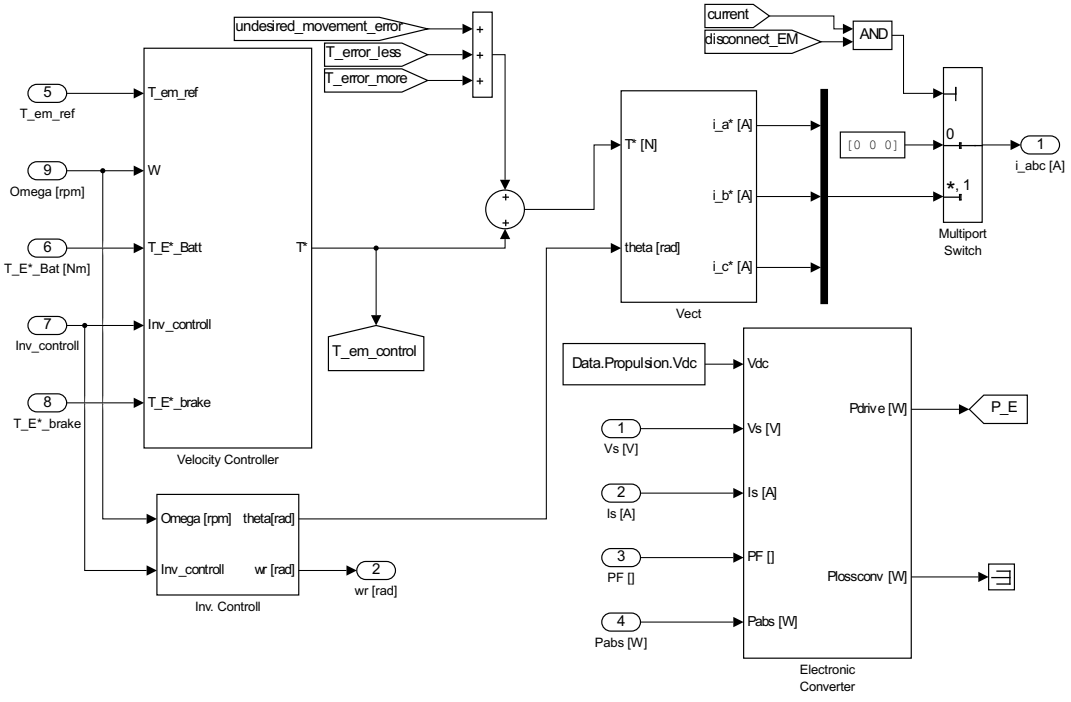

Figura 4.10: Modello Simulink dell'inverter

4.4 Il modello del motore termico

Nel modello Simulink la dinamica del motore termico è stata modellata di tipo passa basso: considerando infatti gli scopi della simulazione (la normativa ISO 26262, come già spiegato in precedenza, concentra la sua attenzione sui dispositivi elettrici ed elettronici) risulta poco utile utilizzare un modello dinamico più complesso. Per questo il modello implementato riceve la coppia di riferimento $T_{ice_{ref}}$ che viene rallentata attraverso la dinamica passa basso, e in seguito viene confrontata con la massima (o minima) coppia erogabile in accordo con i giri motore attuali. Se la coppia di riferimento è minore (o superiore) della coppia massima (o minima) erogabile ai quei determinati giri motore, allora il motore termico genera la coppia richiesta, altrimenti si satura al valore massimo (o minimo) che può attuare.

Le coppie massime e minime che il motore termico può generare in rapporto ai giri motore sono rappresentate in figura 4.11

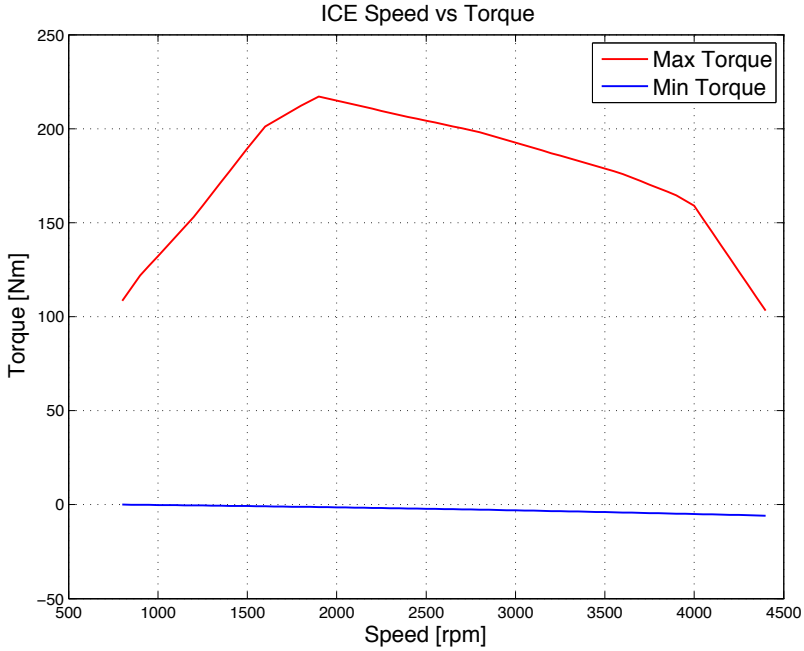

Figura 4.11: Andamento della coppia massima e minima del motore termico al variare dei giri al minuto

L'implementazione Simulink del motore termico è illustrata in figura 4.12

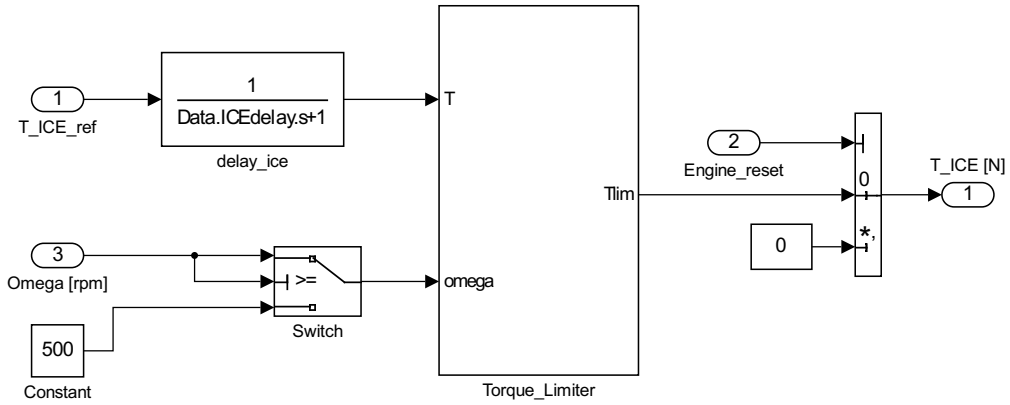

Figura 4.12: Modello Simulink del motore termico

4.5 Il modello delle frizioni

La frizione è un organo meccanico che ha la funzione di connettere a comando due alberi per permettere, ed eventualmente modulare, la trasmissione del moto rotatorio. Nel Powertrain in esame sono presenti due frizioni, ognuna delle quali agisce su un motore. La prima frizione disconnette il motore termico dalla trasmissione, mentre la seconda agisce staccando sia il motore termico che la macchina elettrica.

Essendo due le frizioni presenti ci saranno $2^2 = 4$ combinazioni di funzionamento possibili, al variare dell'apertura o della chiusura delle singole frizioni. Queste configurazioni sono

- Aperto - Aperto,
- Aperto - Chiuso,
- Chiuso - Aperto,
- Chiuso - Chiuso.

Si noti che la configurazione "Chiuso-Aperto" non verrà mai attuata: si tratterebbe di avere la prima frizione chiusa, connettendo il motore termico alla macchina elettrica, ma si scollegherebbero entrambi i motori dal Powertrain aprendo la seconda frizione.

in base alla configurazione attuata nel modello Simulink si avrà una determinata dinamica, come segue

Caso Aperto - Aperto: entrambe le frizioni sono aperte, non permettendo alla coppia generata dalle due fonti di potenza di continuare verso la trasmissione. Le equazioni dinamiche risultano

$$T_{out} = 0 \tag{4.40}$$

$$\dot{\omega}_{ice} = \frac{1}{J_{ice}} \left(T_{ice} - b_{ice}\omega_{ice} \right) \tag{4.41}$$

$$\dot{\omega}_{em} = \frac{1}{J_{em}} \left(T_{em} - b_{em}\omega_{em} \right) \tag{4.42}$$

Caso Aperto - Chiuso: in questo caso l'unica frizione ad essere chiusa è la seconda, connettendo la macchina elettrica alla trasmissione, men-

tre la frizione sul motore termico è aperta escludendo quest'ultimo dal Powertrain. Le equazioni dinamiche risultano

$$T_{out} = T_{em} \tag{4.43}$$

$$\dot{\omega}_{ice} = \frac{1}{J_{ice}} \left(T_{ice} - b_{ice}\omega_{ice} \right) \tag{4.44}$$

$$\omega_{em} = \omega_{gb} \tag{4.45}$$

dove con ω_{gb} si è indicata la velocità di rotazione della trasmissione.

Caso Chiuso - Aperto: come esposto prima, lo studio di questo caso è poco interessante ai fini del funzionamento, ma si riportano lo stesso le equazioni dinamiche

$$T_{out} = 0 \tag{4.46}$$

$$\dot{\omega}_{ice} = \dot{\omega}_{em} = \frac{1}{J_{ice} + J_{em}} \left(T_{ice} + T_{em} - b_{ice}\omega_{ice} - b_{em}\omega_{em} \right) \tag{4.47}$$

in questo caso i due motori sono collegati tra loro ma disconnessi dal Powertrain, per cui la coppia uscente è nulla e le velocità dei due motori sono identiche.

Caso Chiuso - Chiuso: in questa configurazione entrambe le fonti di potenza sono collegate alla trasmissione, permettendo il passaggio della coppia generata. Le equazioni dinamiche risultano

$$T_{out} = T_{em} + T_{ice} \tag{4.48}$$

$$\omega_{ice} = \omega_{gb} \tag{4.49}$$

$$\omega_{em} = \omega_{gb} \tag{4.50}$$

come si può notare dalle equazioni dinamiche, la coppia risultante è la somma delle due coppie generate dai due motori e la velocità angolare a cui i due motori girano è la stessa della trasmissione.

L'implementazione in Simulink delle due frizioni è rappresentato in figura 4.13

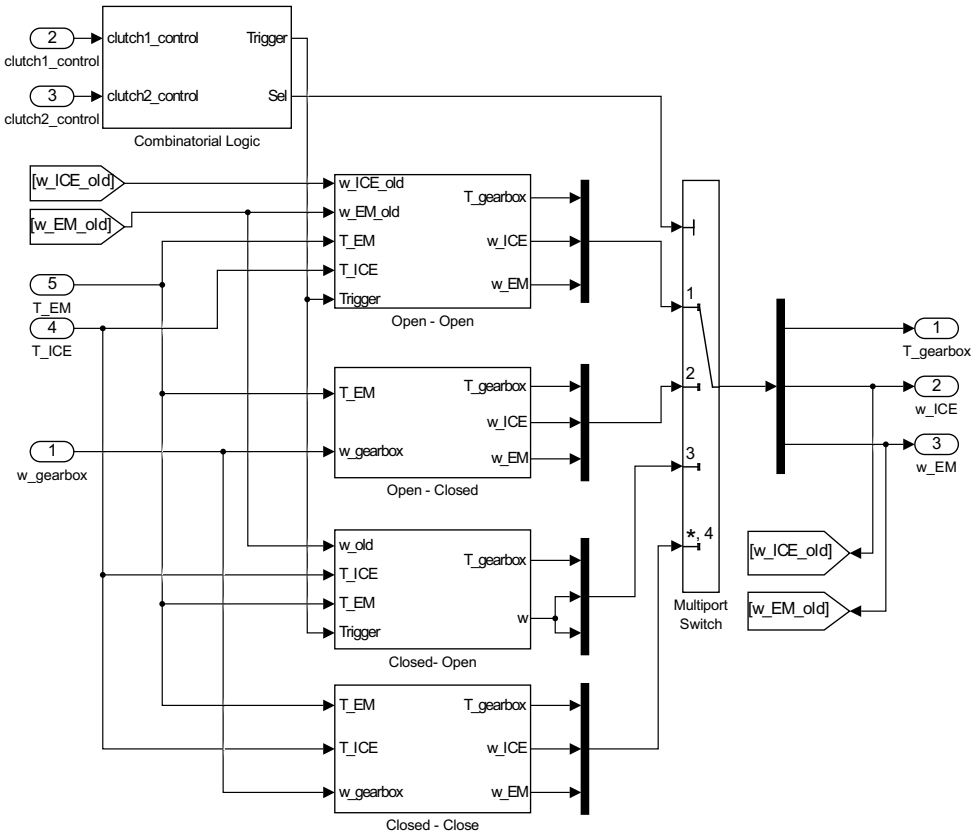

Figura 4.13: Modello Simulink dei due organi frizione

4.6 Il modello della trasmissione

Con il nome organo di trasmissione vengono raggruppati tutti i componenti del Powertrain che permettono la propagazione delle coppie generate dai due motori alle ruote del veicolo. Questi organi sono:

- Il cambio,
- L'albero di trasmissione.

4.6.1 Il modello del cambio

L'organo del cambio è un componente meccanico che ha la funzione di modificare la caratteristica della potenza in uscita da un motore. Infatti in relazione alla marcia inserita si avrà un differente rapporto di trasmissione.

Le equazioni che caratterizzano l'organo del cambio sono le seguenti

$$T_{out} = T_{in} R_{TH} E_{TH} \tag{4.51}$$

$$\omega_{in} = \omega_{out} R_{TH} \tag{4.52}$$

dove R_{TH} e E_{TH} rappresentano rispettivamente il rapporto di trasmissione e l'efficienza della marcia selezionata, entrambi funzioni dipendenti dalla marcia

$$R_{TH} = f\,(Gear) \tag{4.53}$$

$$E_{TH} = f\,(Gear) \tag{4.54}$$

Nel Powertrain questi coefficienti hanno i seguenti valori

Marcia	R_{TH}	E_{TH}
1	5.2	0.98
2	3	0.98
3	2	0.98
4	1.3	0.98
5	1	0.98

Tabella 4.1: Valori coefficienti R_{TH} e E_{TH}

Il modello Simulink del cambio è illustrato in figura 4.14

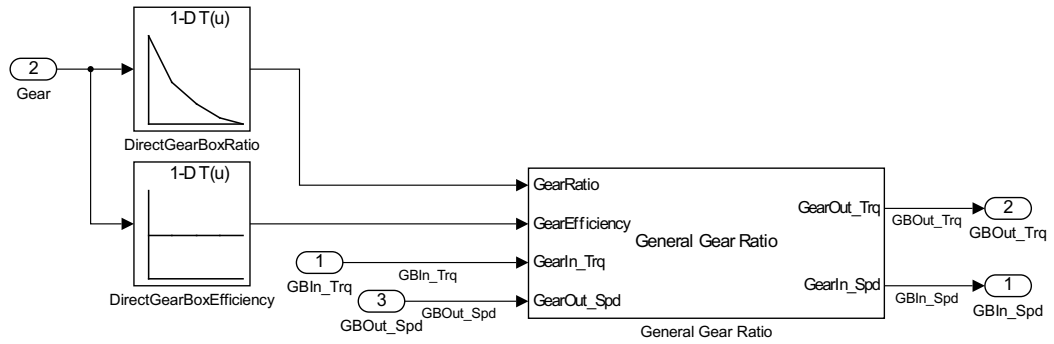

Figura 4.14: Modello Simulink del cambio

4.6.2 Il modello dell'albero di trasmissione

L'albero di trasmissione è l'ultimo organo di propagazione della coppia. Questo è collegato direttamente alle ruote della vettura, applicando ad esse la coppia generata dal Powertrain.

Come per il cambio, anche l'albero è caratterizzato da un rapporto di trasmissione, questa volta fisso e non dipendente da alcun parametro. Per questo le equazioni dinamiche sono identiche a quelle espresse nelle formule 4.51 e 4.52

$$T_{out} = T_{in} R_{TH} E_{TH} \tag{4.55}$$

$$\omega_{in} = \omega_{whl} R_{TH} \tag{4.56}$$

dove con R_{TH} e E_{TH} sono sempre indicati i rapporti di trasmissione ed efficienza, mentre la ω_{whl} è la velocità angolare delle ruote del veicolo.

Il modello Simulink dell'albero di trasmissione è rappresentato in figura 4.15

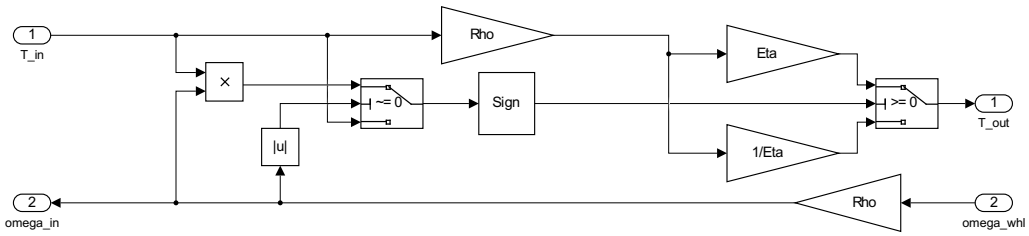

Figura 4.15: Modello Simulink dell'albero di trasmissione

4.7 Il modello della logica di controllo

La logica di controllo è rappresentata in figura 4.16; gestisce tutti i segnali, dall'apertura e chiusura delle due frizioni, alla scelta automatica della marcia da inserire fino ad arrivare alla generazione della coppia di riferimento dei due motori, per far si che il Powertrain lavori correttamente.

Essa si articola in più blocchi:

- Modalità operativa (*Mode logic*),
- Cambio automatico (*Transmission logic*),
- Controllo segnali (*Control logic*),
- Gestione della coppia (*Torque management*).

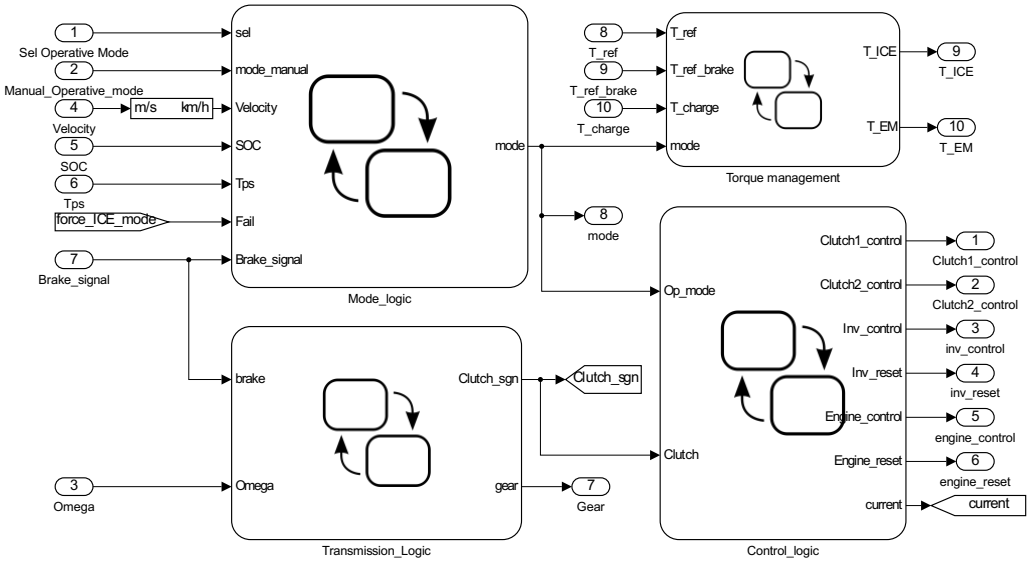

Figura 4.16: Modello Simulink della logica di controllo

Di seguito vengono analizzati nel dettaglio i compiti dei diversi blocchi di controllo.

4.7.1 Modalità operativa

Nella Modalità operativa (*Mode logic*) il sistema di controllo decide la modalità operativa da adottare. Le modalità operative sono cinque, così definite

- Modalità Fermo (*Idle*): il veicolo è fermo,
- Modalità Puramente elettrica (*Zen*): il veicolo è in movimento, il solo motore elettrico fornisce la propulsione,
- Modalità Puramente termica (*Ice*): il veicolo è in movimento, il solo motore termico fornisce la propulsione, mentre la macchina elettrica ricarica le batterie,
- Modalità Ibrida (*Hybrid*): il veicolo è in movimento e la propulsione è affidata ad entrambi i motori,
- Modalità Frenata rigenerativa (*Regenerative brake*): il veicolo è in fase di frenata, si recupera l'energia cinetica che viene trasformata in carica per la batteria dalla macchina elettrica,

- Modalità di Guasto (*Fail*): il sistema di controllo ha rilevato un malfunzionamento e forza lo spegnimento della macchina elettrica, attivando solo il motore termico.

Per le simulazioni è stato implementato un comando di selezione "manuale" della modalità operativa che si vuole attuare.

In figura 4.17 sono illustrate le varie connessioni tra le modalità operative

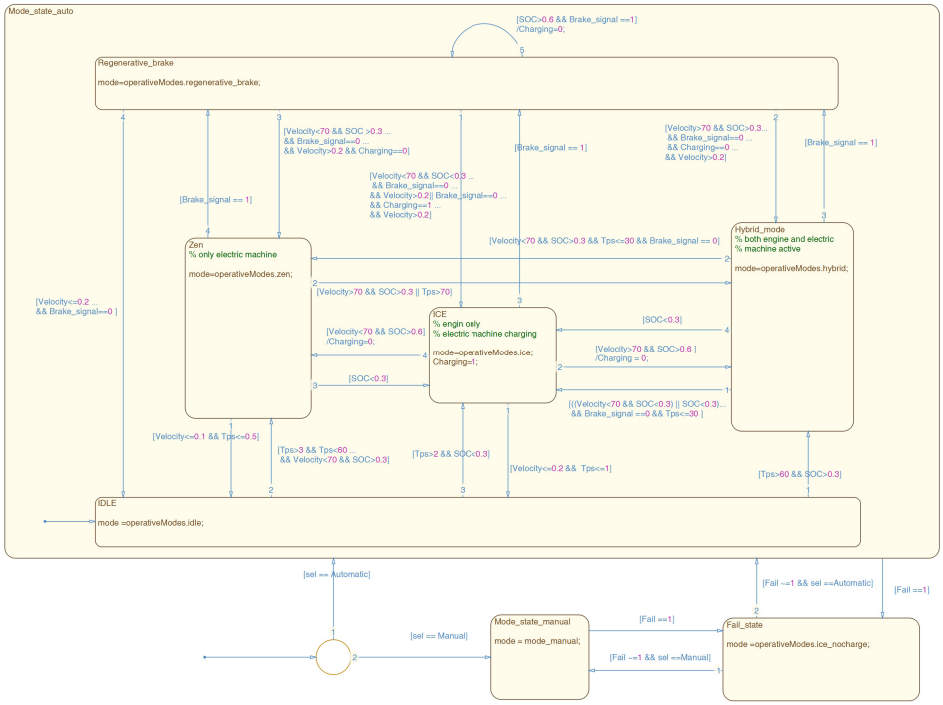

Figura 4.17: Modello StateFlow della Modalità operativa

4.7.2 Cambio automatico

Nel cambio automatico (*Transmission logic*) il controllo, in base alla velocità angolare della trasmissione, imposta la marcia da inserire e la comunica all'organo del cambio, e funziona sia in salita che in scalata di marcia.

Il tempo per il cambio marcia è impostato a 0.3 s.

L'istante di cambio è stato individuato in seguito a varie prove sul Powertrain, confrontando la velocità angolare operativa e la saturazione di velocità imposta dai rapporti del cambio e dell'albero di trasmissione.

In figura 4.18 è mostrata l'implementazione del cambio automatico

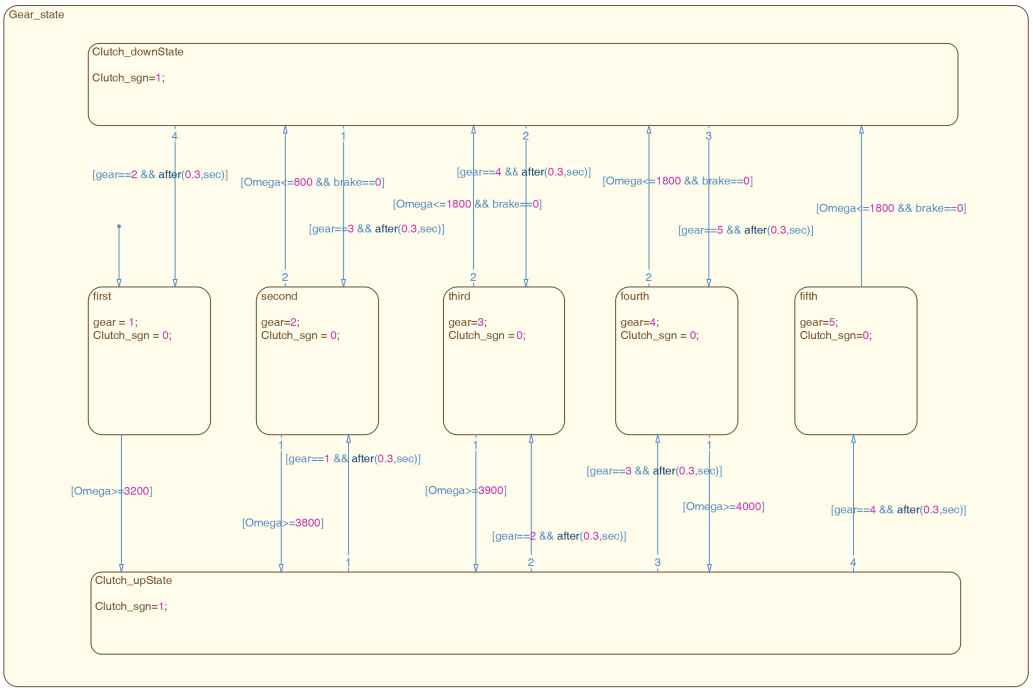

Figura 4.18: Modello StateFlow del Cambio automatico

4.7.3 Controllo segnali

Il blocco Controllo segnali (*Control logic*) riceve in ingresso la modalità operativa ed invia i segnali di controllo ai singoli componenti del Powertrain. In figura 4.19 è rappresentata l'implementazione

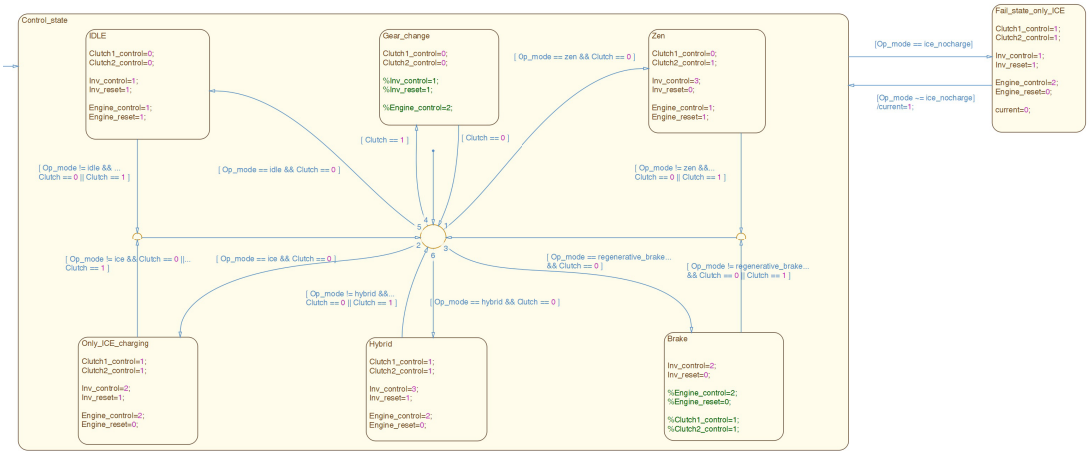

Figura 4.19: Modello StateFlow della Control logic

4.7.4 Gestione della coppia

La Gestione della coppia (*Torque management*) riceve in ingresso la coppia richiesta dal guidatore e, in base alla modalità operativa scelta, invia la coppia di riferimento da generare divisa rispettivamente in $T_{em_{ref}}$ alla macchina elettrica e $T_{ice_{ref}}$ al motore termico.

Le regole di divisione della coppia sono molto semplici e basilari, e sono legate ai limiti di performance dei vari motori: ad esempio, nel caso di modalità Ibrida (Hybrid) la coppia viene divisa equamente fra i due motori fin quando la metà della coppia da generare è inferiore alla coppia massima che può generare la macchina elettrica, altrimenti questa genera il massimo della coppia e il resto viene commissionato al motore termico. Con la stessa concezione viene gestita la coppia anche nelle altre modalità operative (per esempio nel caso Puramente elettrico (*Zen*) viene fatta generare tutta la coppia al motore elettrico e viene inviato un riferimento di coppia nullo al motore termico).

In figura 4.20 è illustrata l'implementazione del blocco di Gestione della coppia.

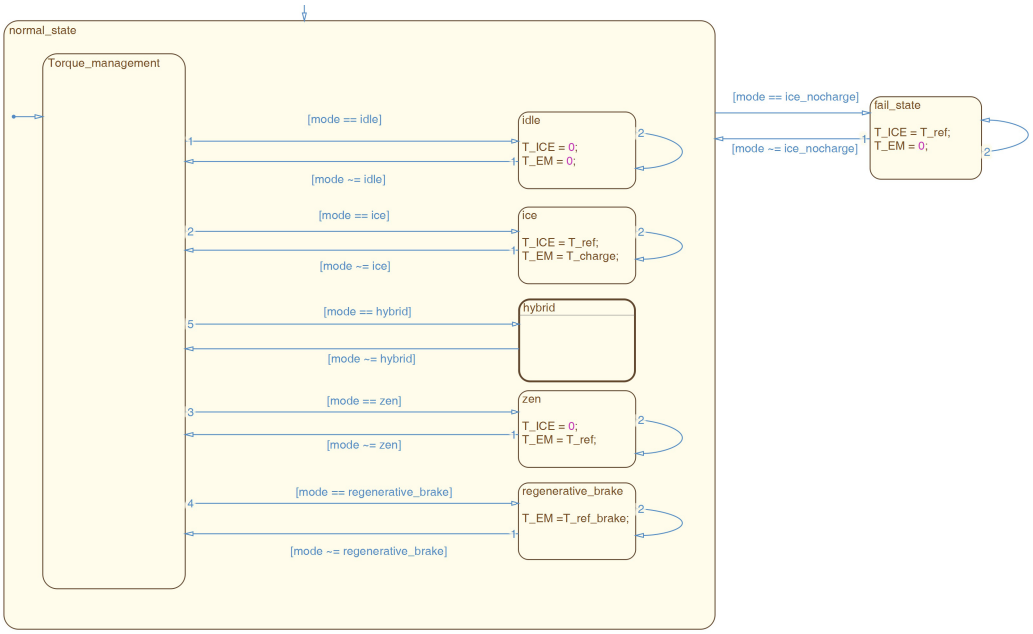

Figura 4.20: Modello StateFlow della Torque management

4.8 Il modello dello chassis

Si completa la descrizione del Powertrain implementato in Simulink con il modello dello chassis.

Questo elemento, ricevendo in ingresso la coppia dell'albero di trasmissione, restituisce la velocità relativa del veicolo su cui si suppone installato il il Powertrain in esame. Oltre alla coppia dell'albero di trasmissione, il blocco dello chassis calcola anche la forza aerodinamica e di attrito a cui è soggetto il veicolo.

Le equazioni dinamiche implementate in Simulink non hanno una elevata complessità, poichè per gli scopi di simulazione non viene richiesto un livello di dettaglio maggiore. Si parte dall'equazione basilare della accelerazione, così definita

$$a = \dot{v}_{vhl} = \frac{F_{chassis} - F_{aerodynamic}}{M} \tag{4.57}$$

in cui M è la massa totale del veicolo più il peso del passeggero $M = M_{vhl} + M_{load}$. La forza aerodinamica è calcolata come segue

$$F_{aerodynamic} = \frac{1}{2} C_x A_{front} \rho v^2 sign\,(v) \tag{4.58}$$

in cui C_x è il coefficiente di resistenza, A_{front} è l'area frontale dell'automobile e ρ è la densità dell'aria. La forza dello chassis $F_{chassis}$ è la composizione della forza frenante F_{brake} attuata dal guidatore e la forza d'attrito F_μ

$$F_{chassis} = \begin{cases} F_T - sign\,(F_T)\,(F_{brake} + F_\mu) & \text{for } (v = 0 \wedge |F_T| > F_{brake} + F_\mu) \vee \\ & (F_T sign\,(v) - F_{brake} - F_\mu > \\ & -(M_{load} + M_{vhl})\,|v|) \\ 0 & \text{for } v = 0 \wedge |F_T| < F_{brake} + F_\mu \end{cases} \tag{4.59}$$

$$F_\mu = Mg\left(\mu_{empty} + M_{load}\left(\frac{\mu_{full} - \mu_{empty}}{M_{loadMax}}\right)\right) \tag{4.60}$$

F_T è la coppia risultante alle ruote, ed è calcolata come rapporto fra la coppia

dell'albero di trasmissione e il raggio di rotolamento

$$F_T = \frac{T_{Axle}}{\text{Rolling Radius}} \tag{4.61}$$

mentre la velocità angolare delle ruote è facilmente calcolabile dalla velocità del veicolo, espressa nella formula 4.57, secondo la legge seguente

$$\omega_{whl} = \frac{60}{2\pi} \frac{v_{vhl}}{\text{Rolling Radius}} \tag{4.62}$$

Il blocco dello chassis e del pneumatico semplificato implementato in Simulink è rappresentato nella figura 4.21

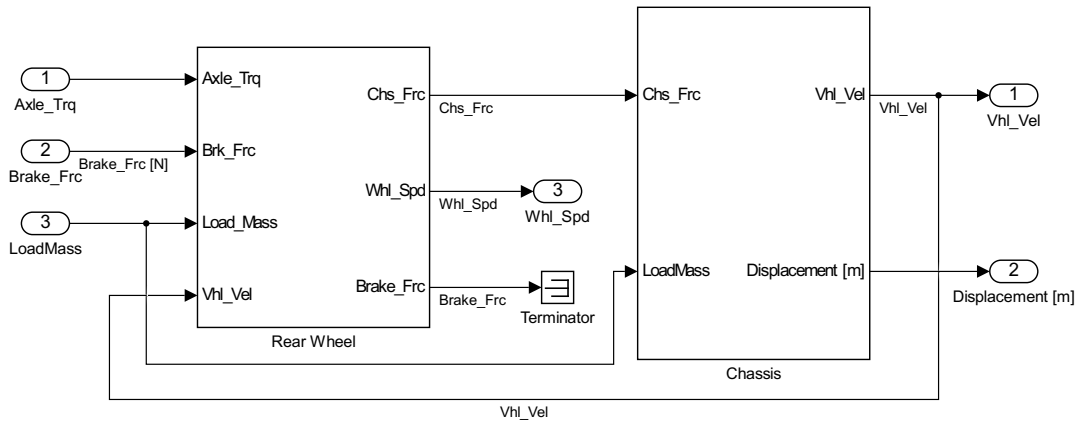

Figura 4.21: Modello Simulink dello chassis e del pneumatico

Nella pagina successiva si mostra il modello completo di Powertrain implementato in Simulink

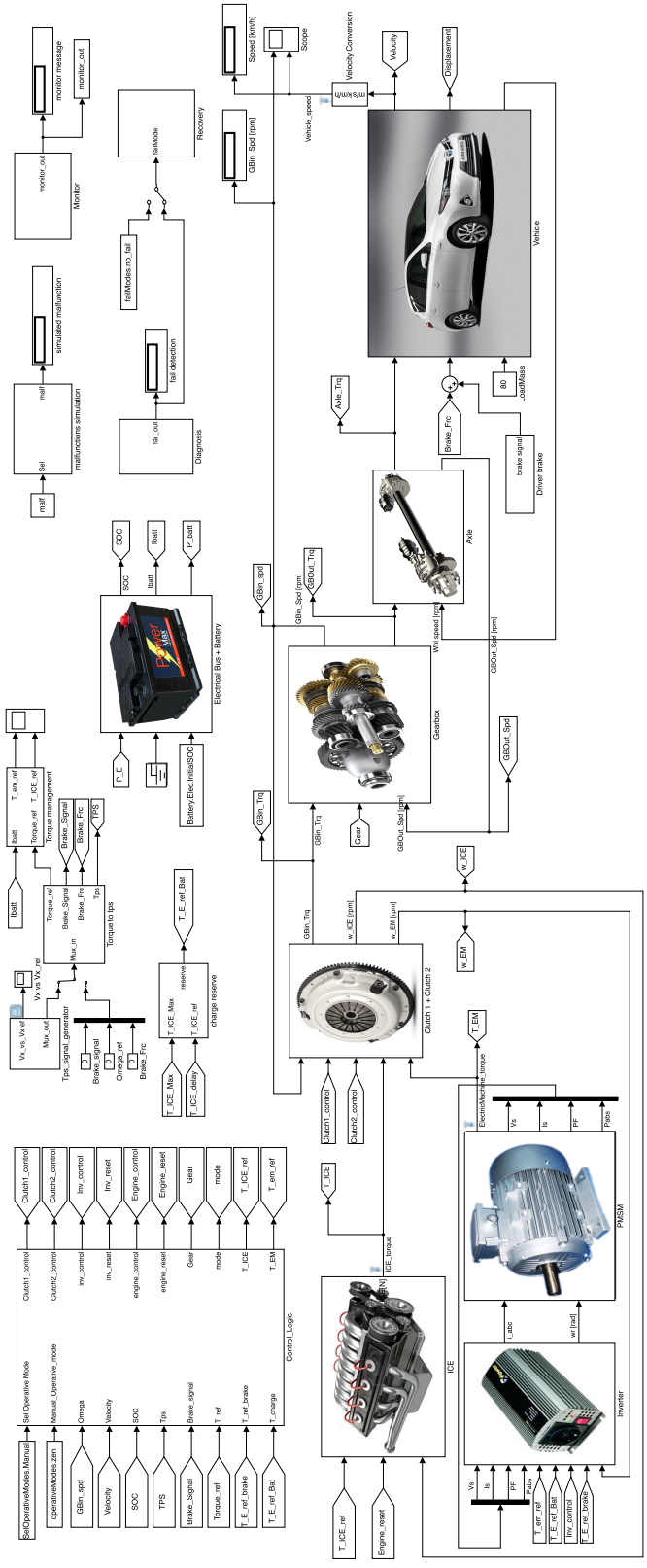

Figura 4.22: Modello Simulink completo del Powertrain

Capitolo 5

Il modello matematico

Nel capitolo 4 a pagina 28 è stato illustrato il tipo di powertrain implementato in simulazione; spesso è stato necessario ricorrere a formule complesse e non lineari per riprodurre nel miglior modo possibile il comportamento dei vari componenti:

Questo livello di dettaglio non è necessario ai fini dell'analisi che verrà svolta nel seguito, perciò si è deciso di semplificare il modello utilizzato, andandolo a sostituire con uno equivalente che permetta una semplificazione nei successivi calcoli.

Ai fini di riformulare il modello non lineare di origine, si è deciso di mantenere l'equazione differenziale 4.57 a pagina 55 rappresentante la velocità veicolo e l'equazione differenziale 4.2 a pagina 31 relativa allo stato di carica della batteria.

5.1 Il modello equivalente dello chassis

Partendo dalle equazioni introdotte nella sezione 4.8 a pagina 55 si vuole ricavare una forma semplificata dell'equazione relativa alla velocità veicolo. Si parte dalla seguente equazione

$$a = \dot{v}_{vhl} = \frac{F_{chassis} - F_{aerodynamic}}{M} \tag{5.1}$$

dove la forza dello chassis e la forza aerodinamica risultano rispettivamente

$$F_{chassis} = F_T - sign\left(F_T\right)\left(F_{brake} + F_\mu\right) \tag{5.2}$$

$$F_{aerodynamic} = \frac{1}{2} C_x A_{front} \rho v^2 sign\left(v\right) = \gamma v^2 sign\left(v\right) \tag{5.3}$$

la F_T ha l'espressione seguente

$$F_T = \frac{T_{Axle}}{\text{Rolling Radius}} = \varsigma T_{Axle} \tag{5.4}$$

mentre la F_u rimane invariata rispetto all'equazione 4.60 di origine. La coppia dell'albero di trasmissione T_{Axle} è data dalla somma delle coppie dei due motori e dei rapporti del cambio e dell'albero motore, come segue

$$\begin{aligned} F_T &= \varsigma T_{Axle} \\ &= \varsigma R_{TH_{Axle}} E_{TH_{Axle}} T_{gb} = \varsigma \beta T_{gb} \\ &= \varsigma \beta R_{TH_{gb}} E_{TH_{gb}} \left(T_{ice} + T_{em}\right) = \varsigma \beta \alpha \left(T_{ice} + T_{em}\right) \\ &= \overline{\varsigma}\left(T_{ice} + T_{em}\right) \end{aligned} \tag{5.5}$$

dove si è posto $\overline{\varsigma} = \varsigma \beta \alpha$. Per cui l'equazione 5.1 si può scrivere come

$$\begin{aligned} \dot{v}_{vhl} &= \frac{1}{M}\left[F_T - sign\left(F_T\right)\left(F_{brake} + F_\mu\right) - \gamma v^2 sign\left(v\right)\right] \\ &= \frac{1}{M}\left[\overline{\varsigma}\left(T_{ice} + T_{em}\right) - sign\left(\overline{\varsigma}\left(T_{ice} + T_{em}\right)\right)\left(F_{brake} + F_\mu\right) - \gamma \cdot v^2 sign\left(v\right)\right] \\ &= -\frac{\gamma}{M} v^2 sign\left(v\right) + \frac{\overline{\varsigma}}{M}\left(T_{ice} + T_{em}\right) - \frac{1}{M} sign\left(\overline{\varsigma}\left(T_{ice} + T_{em}\right)\right)\left(F_{brake} + F_\mu\right) \end{aligned} \tag{5.6}$$

ed una volta portata nella classica forma $\dot{x} = f\left(x, u\right)$, risulta

$$\dot{x} = -\frac{\gamma}{M} x^2 sign\left(x\right) + \frac{\overline{\varsigma}}{M}\left(u_1 + u_2\right) - \frac{1}{M} sign\left(\overline{\varsigma}\left(u_1 + u_2\right)\right)\left(F_{brake} + F_\mu\right) \tag{5.7}$$

dove si è posto $u_1 = T_{em}$ e $u_2 = T_{ice}$.

5.2 Il modello equivalente dello stato di carica

Nella figura 4.2, presente in sezione 4.1 a pagina 30, si è descritto il modello equivalente della batteria. La complessità di questo modello è dovuta ai circuiti $R-C$ presenti nel ramo principale: si è scelto quindi di adottare un modello equivalente più semplice, in cui non sono presenti i rami $R-C$. Tale circuito equivalente è illustrato in figura 5.1

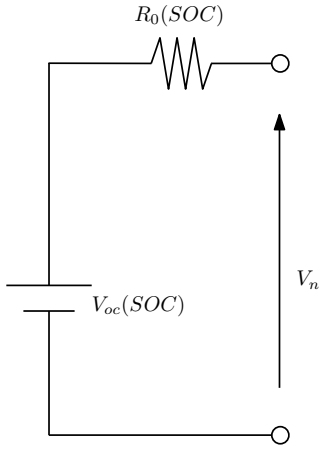

Figura 5.1: Modello equivalente semplificato della batteria

Partendo da questa rappresentazione, si esprime l'equazione che governa lo stato di carica come segue

$$S\dot{O}C\,(t) = \frac{I(t)}{Q} \tag{5.8}$$

confrontando l'equazione 5.8 con la precedente equazione 4.2 si osserva come sia stata eliminata la dipendenza della corrente.
Per quanto riguarda la tensione a circuito aperto Voc, la sua equazione diviene

$$\begin{aligned} Voc\,(SOC,T) &= Voc_0 - K_e\left(273+\bar{\theta}\right)(1-SOC) = Voc_0 - \delta\,(1-SOC) \\ &= a_0 + a_1 \cdot SOC \end{aligned} \tag{5.9}$$

dove si è indicato con T la temperatura della batteria, $\bar{\theta}$ la temperatura dell'elettrolita, Voc_0 la tensione a circuito aperto nel caso di carica completa della batteria e K_e una costante con grandezza fisica $^{V}/_{^{\circ}\mathrm{C}}$.

La resistenza R_0 ha l'espressione seguente

$$R_0\left(SOC\right) = R_{00}\left[1 + A_0\left(1 - SOC\right)\right] = b_0 + b_1 \cdot SOC \tag{5.10}$$

dove con R_{00} si è indicato la resistenza nel caso di $SOC = 1$ e con A_0 una costante adimensionale.

Una volta identificate le grandezze in gioco, si può scrivere la semplice equazione della maglia del circuito

$$Voc = R_0 I + V_n \tag{5.11}$$

immaginando quindi che ai morsetti vuoti della figura 5.1 sia collegato l'inverter, è ragionevole imporre

$$V_n I = P_e \tag{5.12}$$

dove con P_e si è indicata la potenza elettrica della macchina elettrica. Questa è anche uguale a

$$P_e = \frac{P_{em}}{\eta} \tag{5.13}$$

dove con P_{em} si indica la potenza meccanica della macchina elettrica e con η la sua efficienza. La poteza meccanica della macchina elettrica è così formulata

$$P_{em} = T_{em}\omega_{em} \tag{5.14}$$

Mettendo a sistema le equazioni 5.11 e 5.12, si ricava la corrente nel circuito

$$I_{1,2} = \frac{-Voc \pm \sqrt{Voc^2 - 4R_0{}^{P_m}/_{\eta}}}{-2R_0} \tag{5.15}$$

che, sostituita nell'equazione 5.8, porta alla seguente forma

$$\dot{SOC}\left(t\right) = \frac{1}{-2R_oQ}\left(-Voc \pm \sqrt{Voc^2 - 4R_0{}^{P_m}/_{\eta}}\right) \tag{5.16}$$

sostituite le precedenti equazioni, risulta

$$S\dot{O}C\left(t\right)=\frac{1}{-2\left(b_0+b_1SOC\right)Q}\left(a_0+a_1SOC+\right.$$
$$\left.\pm\sqrt{a_0^2+a_1^2SOC^2+2a_0a_1SOC-\frac{4}{\eta}\left(b_0+b_1SOC\right)\left(T_{em}\omega_{em}\right)}\right). \tag{5.17}$$

La velocità del motore termico ω_{em} risulta pari a

$$\begin{aligned}\omega_{em}&=\omega_{gb,in}=\omega_{gb,out}R_{TH_{Axle}}\\&=\omega_{whl}R_{TH_{Axle}}R_{TH_{gb}}=\underbrace{R_{TH_{Axle}}R_{TH_{gb}}\cdot\frac{60}{2\pi}\frac{1}{\text{Rolling Radius}}}_{\sigma}v_{vhl}=\sigma v_{vhl}\end{aligned} \tag{5.18}$$

sostituendo questa espressione nella 5.17 si avrà

$$S\dot{O}C\left(t\right)=\frac{1}{-2\left(b_0+b_1SOC\right)Q}\left(a_0+a_1SOC+\right.$$
$$\left.\pm\sqrt{a_0^2+a_1^2SOC^2+2\cdot a_0a_1SOC-\frac{4}{\eta}\left(b_0+b_1SOC\right)\left(\sigma T_{em}v_{vhl}\right)}\right) \tag{5.19}$$

che, posta nella forma $\dot{x}=f\left(x,u\right)$ risulta

$$\dot{x}=\frac{1}{-2\left(b_0+b_1x\right)Q}\left(a_0+a_1x+\right.$$
$$\left.\pm\sqrt{a_0^2+a_1^2x^2+2a_0a_1x-\frac{4}{\eta}\left(b_0+b_1x\right)\left(\sigma u_1v_{vhl}\right)}\right) \tag{5.20}$$

Capitolo 6

Assegnazione degli ASIL e degli Obiettivi di Sicurezza

Come illustrato nel capitolo 2, la normativa ISO-26262 richiede che per ogni componente elettrico o elettronico presente a bordo del veicolo in esame, sia svolta

1. l'analisi del rischio, per ciascun malfunzionamento individuato, e l'assegnazione delle classi di Esposizione, Severità e Controllabilità come descritto nella Sezione 2.1,

2. la valutazione degli ASIL, per ogni situazione operativa individuata nel punto precedente,

3. la formulazione, per ciascun evento cui è assegnato un livello $ASIL > QM$, del relativo obiettivo di sicurezza.

Sono stati individuati quattro diversi malfunzionamenti, riguardanti la macchina elettrica e la relativa elettronica di comando

- erogazione di coppia non desiderata a veicolo fermo: tale malfunzionamento può manifestarsi quando, ad esempio a causa di un guasto nel sistema di comunicazione, all'inverter arrivi un segnale di coppia positiva non direttamente richiesto dal sistema di controllo; la macchina elettrica fornirà quindi una coppia positiva che porterà ad un avanzamento longitudinale del veicolo.

- erogazione di coppia superiore a quella richiesta: tale malfunzionamento si può verificare quando il veicolo si trova in marcia, ed a una richiesta di coppia da parte del guidatore corrisponde una erogazione di coppia superiore da parte della macchina elettrica, e può essere sempre dovuto ad un errore nel canale di comunicazione.

- erogazione di coppia inferiore a quella richiesta: una smagnetizzazione dei magneti interni alla macchina elettrica, dovuta ad esempio ad una eccessiva temperatura del componente, ha come effetto quello di ridurre le prestazioni dei magneti stessi, causando un'erogazione di coppia inferiore a quella desiderata da parte della macchina elettrica.

- mancata erogazione di coppia: tale malfunzionamento può manifestarsi in seguito ad una rottura meccanica interna alla macchina elettrica, che può riguardare sia l'albero di trasmissione sia i cuscinetti stessi.

Nelle sezioni seguenti si espone, per ciascun malfunzionamento, l'analisi svolta mediante l'ausilio dell'interfaccia grafica esposta nel capitolo 3, partendo dalla valutazione delle situazioni operative nelle quali il manifestarsi del guasto risulta un pericolo fino ad arrivare alla formulazione degli obiettivi di sicurezza che possano scongiurare, o ridurre al minimo, i rischi relativi al guidatore ed ogni altro partecipante allo scenario.

6.1 Coppia non desiderata a veicolo fermo

Questo malfunzionamento si può verificare mentre il veicolo si trova in condizioni quali la sosta in coda ad altri veicoli, in prossimità di un attraversamento pedonale o fermo ad un incrocio: un' erogazione di coppia non desiderata da parte della macchina elettrica causerebbe un avanzamento longitudinale del veicolo, rischiando di dar luogo ad un impatto con il veicolo che precede o, più gravemente, all'investimento di un pedone.

L'assegnazione delle classi di Esposizione, Severità e Controllabilità (da qui in avanti, rispettivamente, E, S e C) relativamente a questo malfunzionamento risulta piuttosto semplice, in quanto poche sono le situazioni operative nelle quali può verificarsi; in Tabella 6.1 è riassunta l'analisi ASIL

situazione operativa	***E***	***S***	***C***	***ASIL***
veicolo fermo, attraversamento pedonale	E4	S3	C2	C
veicolo fermo, incrocio, strada urbana	E4	S1	C2	A
veicolo fermo, incrocio, strada extraurbana	E3	S2	C2	B

Tabella 6.1: Assegnazione degli ASIL nel caso di movimento non desiderato

si osserva come le situazione più rischiose siano

- in presenza di un attraversamento pedonale, dove vi è il rischio di investire un pedone, provocandogli seri danni fisici dovuti all'urto
- in presenza di un incrocio in strada extraurbana, dove i veicoli procedono ad elevate velocità, e l'impatto provocherebbe gravi danni fisici.

L'obiettivo di sicurezza relativo a questo malfunzionamento, valutando che uno spostamento massimo di 15 cm sia tollerabile, è così formulato

> "Impedire che l'attivazione non desiderata della macchina elettrica provochi uno spostamento del veicolo superiore a $0.15m$ (ASIL C)".

6.2 Coppia superiore a quella richiesta

Un'erogazione di coppia superiore a quella richiesta causa un'accelerazione non desiderata del veicolo, che può provocare un impatto con il veicolo che precede. Tale malfunzionamento può portare ad una situazione di pericolo anche durante manovre nelle quali si vuole rallentare il veicolo, quali una frenata o un arresto di emergenza.

Per generare le situazioni operative sono state scelte le categorie "tipologia di strada", "condizioni del manto stradale" e "tipo di manovra"; in Tabella 6.2 è riassunta l'analisi ASIL relativa al malfunzionamento

situazione operativa	***E***	***S***	***C***	***ASIL***
strada urbana, asfalto umido, manovra di frenata	E4	S3	C3	D
strada urbana, asfalto umido, frenata di emergenza	E3	S3	C2	B
strada urbana, asfalto asciutto, frenata di emergenza	E3	S3	C1	A
strada extraurbana, asfalto umido, manovra di frenata	E4	S2	C2	B
strada extraurbana, asfalto asciutto, manovra di frenata	E4	S1	C2	A
strada extraurbana, asfalto umido, manovra evasiva	E3	S3	C2	B
strada extraurbana, asfalto asciutto, manovra evasiva	E3	S3	C1	B
strada extraurbana, asfalto umido, frenata di emergenza	E3	S3	C3	C
strada extraurbana, asfalto asciutto, frenata di emergenza	E3	S3	C2	B
autostrada, asfalto umido, manovra di frenata	E3	S2	C2	B
autostrada, asfalto asciutto, manovra di frenata	E4	S2	C2	B
autostrada, asfalto umido, manovra evasiva	E3	S3	C3	C
autostrada, asfalto asciutto, manovra evasiva	E3	S3	C2	B
autostrada, asfalto umido, frenata di emergenza	E3	S3	C3	C
autostrada, asfalto asciutto, frenata di emergenza	E3	S3	C2	B

Tabella 6.2: Assegnazione degli ASIL nel caso di coppia superiore

Analizzando i risultati, si può concludere che i rischi maggiori sussistano nel caso in cui il malfunzionamento si verifichi in condizioni di

- bassa aderenza, in quanto un'accelerazione non desiderata costringerà il guidatore ad una brusca frenata, che potrebbe causare uno slittamento del veicolo dovuto all'asfalto bagnato
- in autostrada, dove la controllabilità dell'evento risulta più complessa a causa delle elevate velocità che richiedono un minor tempo di risposta

- nel caso si effettui una frenata di emergenza.

L'obiettivo di sicurezza relativo a questo malfunzionamento può così essere formulato

"Impedire che la macchina elettrica causi un aumento di prestazioni non desiderato (ASIL D)".

6.3 Coppia inferiore a quella richiesta

Un'erogazione di coppia inferiore a quella desiderata può causare un brusco calo di prestazioni, e quindi portare ad una situazione di pericolo in accordo al tipo di manovra che si sta compiendo; per l'analisi delle situazioni operative, il malfunzionamento è stato considerato sia in fase di accelerazione (la macchina elettrica non eroga la coppia desiderata), sia in fase di frenatura (la macchina elettrica non eroga la dovuta coppia di frenata).

Nella generazione delle situazioni operative sono state scelte le medesime categorie del punto precedente, e l'analisi ASIL è riassunta in Tabella 6.3

situazione operativa	***E***	***S***	***C***	***ASIL***
strada urbana, asfalto umido, manovra di frenata	E4	S1	C2	A
strada urbana, asfalto umido, frenata di emergenza	E3	S3	C2	B
strada urbana, asfalto asciutto, frenata di emergenza	E3	S3	C1	A
strada extraurbana, asfalto umido, manovra di frenata	E4	S2	C2	B
strada extraurbana, asfalto asciutto, manovra di frenata	E4	S2	C1	A
strada extraurbana, asfalto umido, manovra evasiva	E3	S2	C2	A
strada extraurbana, asfalto asciutto, manovra evasiva	E3	S2	C2	A
strada extraurbana, asfalto umido, frenata di emergenza	E3	S3	C3	C
strada extraurbana, asfalto asciutto, frenata di emergenza	E3	S3	C2	B
strada extraurbana, asfalto asciutto, sorpasso	E3	S3	C3	C
strada extraurbana, asfalto asciutto, sorpasso	E4	S3	C3	D
autostrada, asfalto umido, manovra di frenata	E3	S2	C2	B
autostrada, asfalto asciutto, manovra di frenata	E3	S2	C2	B
autostrada, asfalto umido, manovra evasiva	E3	S3	C3	C
autostrada, asfalto asciutto, manovra evasiva	E3	S3	C2	B
autostrada, asfalto umido, frenata di emergenza	E3	S3	C3	C
autostrada, asfalto asciutto, frenata di emergenza	E3	S3	C2	B

Tabella 6.3: Assegnazione degli ASIL nel caso di coppia inferiore

Diversamente dal precedente malfunzionamento, in caso di calo di prestazioni risulta di elevato rischio una manovra di sorpasso; basti immaginare che tale guasto si manifesti durante una manovra di sorpasso, in strada secondaria (quindi a velocità sostenuta): il malfunzionamento impedirebbe il completarsi della manovra, rischiando di causare l'impatto con i veicoli che provengono dalla corsia opposta. In generale poi, nelle varie manovre di frenata un calo di coppia frenante renderà necessario effettuare una frenata meccanica, con notevole ritardo rispetto a quella elettronica, e causando probabilmente uno slottamento dovuto all'asfalto scivoloso.

L'analisi porta quindi alla formulazione del seguente obiettivo di sicurezza, caratterizzaro da un requisito più stringente

"Impedire che un guasto alla macchina elettrica provochi un calo di prestazioni (ASIL D)".

6.4 Mancata erogazione di coppia

Questo tipo di malfunzionamento rappresenta un caso estremo di coppia erogata inferiore a quella richiesta, ma necessita comunque di un'apposita analisi: si avranno simili effetti, ma più gravi conseguenze in quanto stavolta la macchina elettrica non produrrà alcuna coppia.

Le situazioni operative sono le medesime del caso precedente, ma questo malfunzionamento si ripercuoterà in maniera più drastica sulla dinamica del veicolo (mentre prima la coppia, seppur inferiore a quella desiderata, veniva erogata, stavolta non viene erogata: si ha quindi un cosiddetto "buco di coppia"). In Tabella 6.4 è riassunta l'analisi ASIL su questo malfunzionamento

situazione operativa	***E***	***S***	***C***	***ASIL***
strada urbana, asfalto umido, manovra di frenata	E4	S1	C2	A
strada urbana, asfalto umido, frenata di emergenza	E3	S3	C3	C
strada urbana, asfalto asciutto, frenata di emergenza	E3	S3	C2	A
strada extraurbana, asfalto umido, manovra di frenata	E4	S2	C2	B
strada extraurbana, asfalto asciutto, manovra di frenata	E4	S2	C2	B
strada extraurbana, asfalto umido, manovra evasiva	E3	S2	C3	A
strada extraurbana, asfalto asciutto, manovra evasiva	E3	S2	C3	A
strada extraurbana, asfalto umido, frenata di emergenza	E3	S3	C3	C
strada extraurbana, asfalto asciutto, frenata di emergenza	E3	S3	C3	C
strada extraurbana, asfalto asciutto, sorpasso	E3	S3	C3	C
strada extraurbana, asfalto asciutto, sorpasso	E4	S3	C3	D
autostrada, asfalto umido, manovra di frenata	E3	S2	C3	B
autostrada, asfalto asciutto, manovra di frenata	E3	S2	C2	B
autostrada, asfalto umido, manovra evasiva	E3	S3	C3	C
autostrada, asfalto asciutto, manovra evasiva	E3	S3	C3	D
autostrada, asfalto umido, frenata di emergenza	E3	S3	C3	C
autostrada, asfalto asciutto, frenata di emergenza	E3	S3	C3	C

Tabella 6.4: Assegnazione degli ASIL nel caso di assenza di coppia

Analogamente a quanto visto in precedenza, i risultati confermano come il rischio maggiore si abbia in fase di sorpasso. L'obiettivo di sicurezza risulta il medesimo del punto precedente, necessiterà però di una manovra correttiva più rapida

"Impedire che un guasto alla macchina elettrica provochi una repentina perdita di prestazioni (ASIL D)".

Capitolo 7

Sistema di diagnosi e verifica dei requisiti di sicurezza

Unitamente al modello di simulazione, è stato implementato un sistema atto a rilevare la presenza di un malfunzionamento, ed effettuare su richiesta azioni di controllo in modo da mantenere il veicolo in condizioni di sicurezza.
Tale sistema è costituito da

- Un monitor di simulazione, avente il compito di rilevare il rispetto o meno dei requisiti di sicurezza assegnati nel capitolo 6,
- un sistema di diagnosi, avente il compito di rilevare la presenza di un malfunzionamento,
- un sitema di recovery che, attivato dalla diagnosi, compie precise azioni di controllo in modo da garantire il rispetto dei requisiti di sicurezza.

7.1 Monitor di sistema

Il monitor di sistema è illustrato in figura 7.1

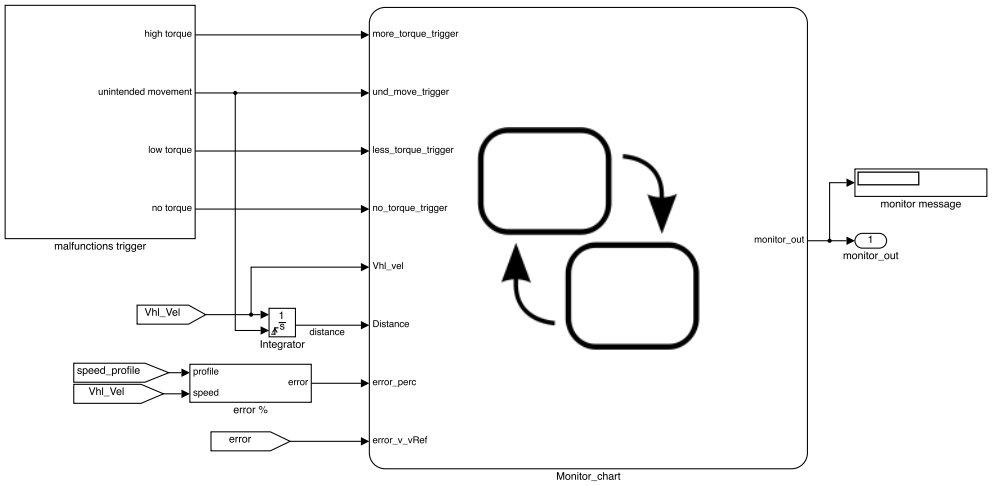

Figura 7.1: Monitor di sistema

Essendo uno strumento utilizzato esclusivamente in simulazione, ha acesso a variabili non effettivamente presenti nel sistema reale, quali

- l'istante di attivazione di uno specifico malfunzionamento
- la distanza percorsa dal veicolo, in seguito all'attivazione di un guasto
- la differenza percentuale fra il profilo di velocità desiderato e l'effettiva velocità del veicolo

Il suo compito è quello di segnalare all'utente il mancato rispetto dei requisiti di sicurezza definiti in precedenza. Tale sistema consentirà anche di valutare il corretto funzionamento di diagnosi e recovery, in quanto una loro attivazione in caso di guasto dovrà portare al rispetto degli obiettivi di sicurezza imposti.

Il nucleo del monitor di sistema è costituito da una macchina a stati, osservabile in figura 7.2. All'interno della macchina a stati sono presenti quattro sottoblocchi, ciascuno adibito a verificare il rispetto del relativo requisito di sicurezza; all'avvio della simulazione, divengono attivi gli stati iniziali dei quattro sottoblocchi: il segnale di iniezione del guasto attiverà quindi la trasizione

in uno degli di controllo, in cui vengono analizzate le varibili relative al requisito e, nel caso in cui sia rilevata una violazione, viene inviato in uscita dal monitor un messaggio di avvertimento.

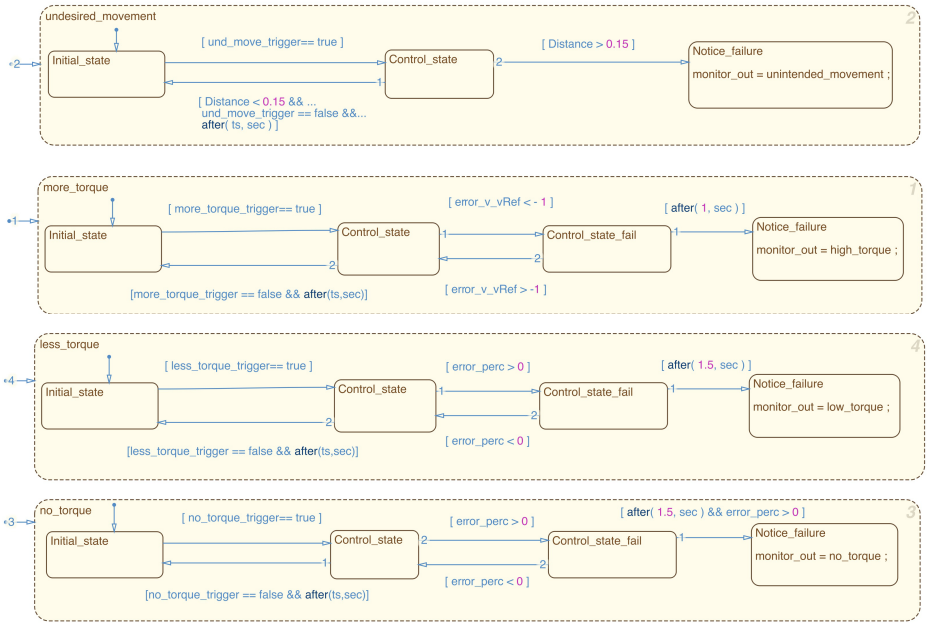

Figura 7.2: Macchina a stati interna al Monitor di sistema

I quattro sottoblocchi sono così definiti

1. blocco adibito alla verifica del requisito sullo spostamento non desiderato: nello stato di controllo, è segnalato il fallimento del requisito se viene percorsa una distanza maggiore di $0.15\,m$ in seguito all'erogazione di una coppia non desiderata,

2. blocco adibito alla verifica del requisito nel caso di coppia maggiore: nello stato di controllo, viene segnalato il fallimento se la differenza fra il profilo di velocità di riferimento e la velocità attuale supera una determinata soglia per un certo intervallo di tempo,

3. blocco adibito alla verifica del requisito nel caso di coppia minore: nello stato di controllo, viene segnalato il fallimento se la differenza fra la coppia erogata e quella richiesta supera una determinata soglia percentuale per un certo intervallo di tempo,

4. blocco adibito alla verifica del requisito nel caso di coppia nulla: stesso comportamento del precedente blocco.

7.2 Diagnosi

Durante la marcia non si è a conoscenza del preciso istante in cui si verifica un guasto: compito del sistema di diagnosi è quindi quello di identificare la presenza di un malfunzionamento, e segnalarlo tempestivamente al sistema di recovery. Come per il monitor di sistema, anche la diagnosi è costituita da una macchina a stati, osservabile in figura 7.3

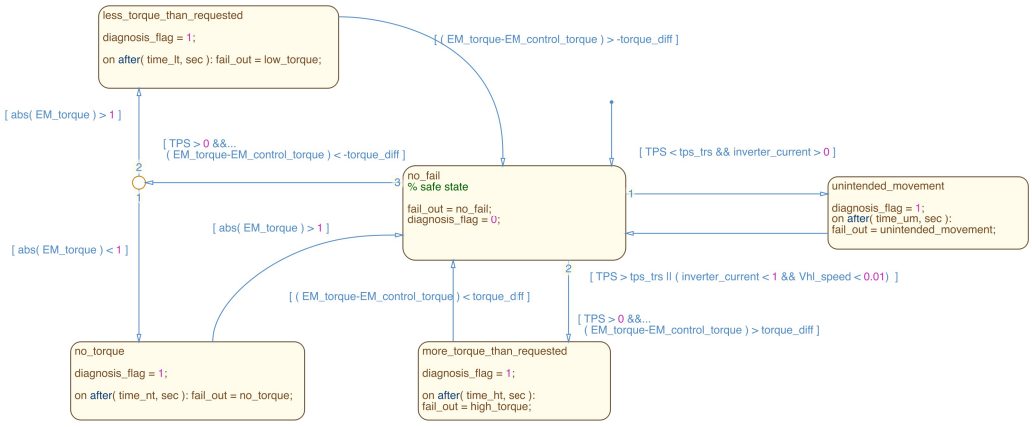

Figura 7.3: Macchina a stati che implementa il sistema di Diagnosi

L'identificazione di un malfunzionamento avviene andando a valutare l'andamento dei seguenti segnali

- la posizione pedale, segnale che può essere utlizzato per riconoscere un movimento non desiderato
- la velocità di avanzamento, che indica quando il veicolo è fermo
- le correnti in uscita dall'inverter, che consentono di stimare la coppia erogata dalla macchina elettrica
- la coppia richiesta dal controllo alla macchina elettrica.

Dallo stato iniziale, definito *stato sicuro*, si ha una transizione in uno stato di controllo se la diagnosi riscontra una variazione sui segnali compatibile con un malfunzionamento: trascorso un preciso intervallo temporale all'interno dello stato di controllo, la diagnosi invia un segnale al sistema di recovery per indicare la presenza di uno specifico guasto.

La diagnosi relativa ai quattro malfunzionamenti è stata così implementata

- blocco adibito alla diagnosi per lo spostamento non desiderato: si passa dallo stato sicuro allo stato di controllo, nel caso in cui le correnti in uscita dall'inverter producano un segnale compatibile con una richiesta di movimento della macchina elettrica, ma il guidatore non sta agendo sul pedale dell'acceleratore (che risulta, quindi, inferiore ad una determinata soglia percentuale $TPS < tps_{trs}$); trascorso un tempo $time_{um}$, viene attivato il canale di uscita per segnalare il guasto al sistema di recovery.

- blocco adibito alla diagnosi di coppia maggiore: si transisce nello stato di controllo nel caso in cui la differenza fra la coppia erogata dalla macchina elettrica e la coppia richiesta dal controllore superi una soglia $torque_{diff}$: se la macchina permane nello stato di controllo per un intervallo temporale superiore a $time_{ht}$ viene segnalato il guasto al sistema di recovery.

- blocco adibito alla diagnosi di coppia inferiore: la transizione dello stato di controllo avviene se la differenza fra la coppia erogata dalla macchina elettrica e la coppia richiesta dal controllore superi una soglia negativa $-torque_{diff}$: se la macchina permane nello stato di controllo per un intervallo temporale superiore a $time_{lt}$ viene segnalato il guasto al sistema di recovery.

- blocco adibito alla diagnosi del buco di coppia: stessa diagnosi del precedente malfunzionamento, con la differenza che si transisce nello stato di controllo se la coppia uscente dalla macchina elettrica risulta nulla.

7.3 Recovery

Una volta identificato un malfunzionamento, devono essere intraprese precise azioni di controllo allo scopo di mantenere il veicolo in sicurezza: compito del sistema di recovery è quello di attivare specifici controlli, una volta segnalata dalla diagnosi la presenza di un guasto.

Come per il monitor di sistema e la diagnosi, anche la recovery è stata implementata con una macchina a stati, osservabile in figura 7.4. Dallo stato iniziale, sicuro, si attiva una transizione in uno stato di controllo e recupero del malfunzionamento una volta attivo il rispettivo segnale di guasto da parte della diagnosi: in tale stato vengono attivati specifici controlli, in modo da isolare la fonte del guasto e mantenere il veicolo in sicurezza. Effettuate le azioni di controllo, sarà quindi nuovamente la diagnosi a rilevare che il malfunzionamento non è più presente e a riportare il sistema di recovery nello stato iniziale.

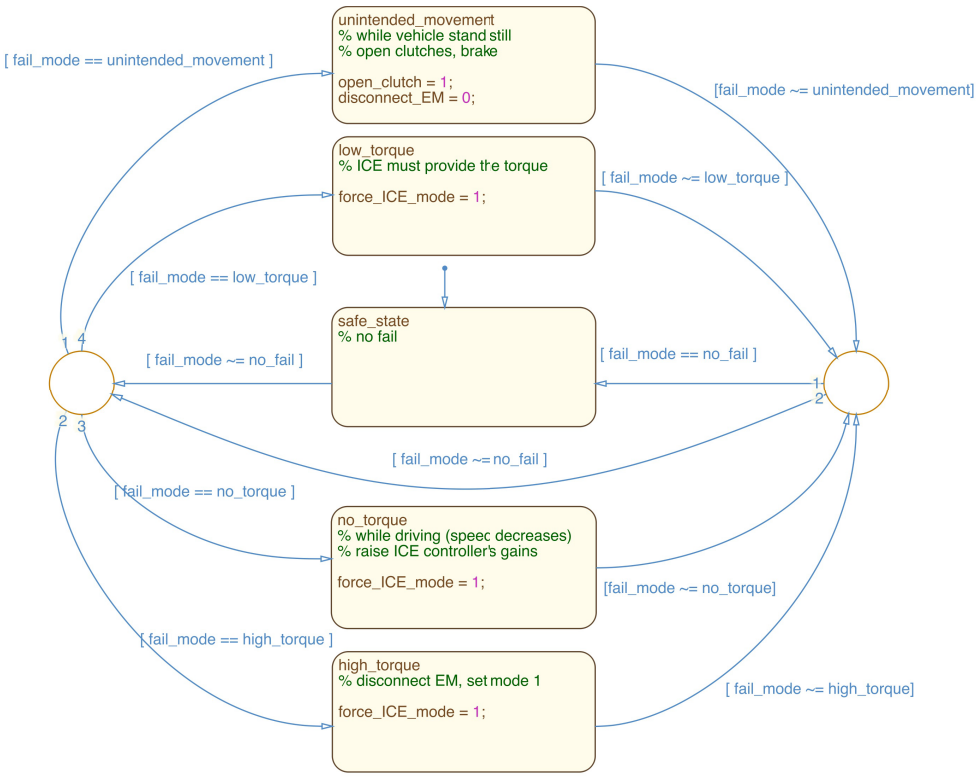

Figura 7.4: Macchina a stati che implementa il sistema di Recovery

Nello specifico, le azioni di controllo effettuate dal sistema di recovery sono le seguenti

- forzare l'attivazione della sola modalità termica: nel caso di calo/aumento di prestazioni della macchina elettrica, il sistema di recovery deve tempestivamente attivare una modalità operativa in cui sia attivo il solo motore termico, isolando e disattivando la fonte del guasto
- aprire forzatamente la frizione: nel caso in cui il veicolo si muova inavvertitamente, la frizione deve essere tempestivamente aperta in modo da interrompere la trasmissione di coppia; unitamente a ciò, la macchina elettrica deve essere disattivata in modo da evitarne un surriscaldamento.

Capitolo 8

Simulazioni

Le simulazioni sono state svolte introducendo i malfunzionamenti illustrati nel Capitolo 6, con l'obiettivo di verificare il corretto funzionamento dei sistemi di diagnosi e recovery.

Per simulare la presenza di un malfunzionamento si sono introdotti dei segnali di guasto nel canale di controllo dell'inverter, come illustrato in Figura 8.1: la macchina elettrica non riceverà quindi il solo segnale proveniente dal controllore, ma sarà presente un segnale additivo atto a modellare il guasto.

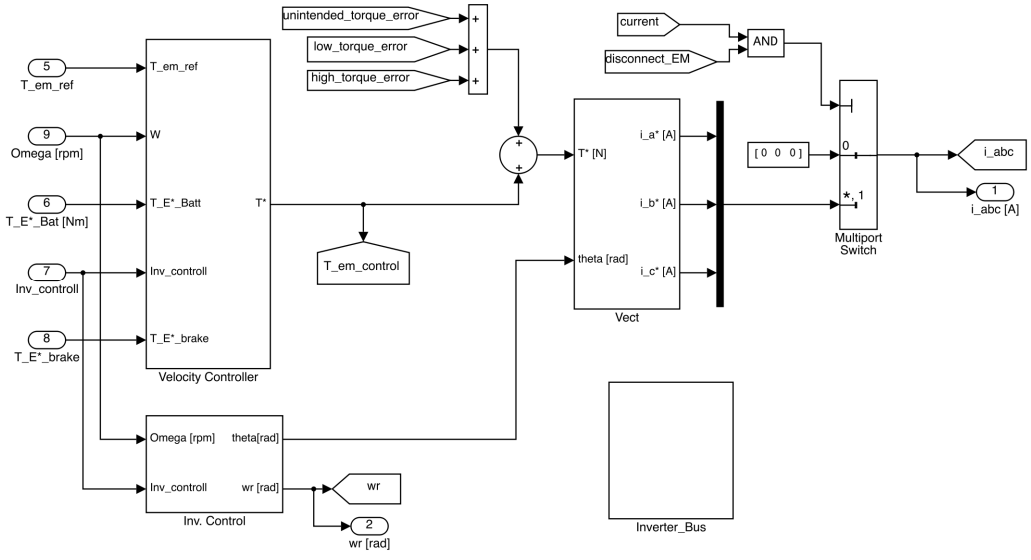

Figura 8.1: blocco Inverter con iniezione dei segnali di guasto

8.1 Coppia non desiderata a veicolo fermo

Questo tipo di malfunzionamento si può verificare mentre il veicolo si trova in condizioni quali la sosta in coda ad altri veicoli, in prossimità di un attraversamento pedonale o fermi ad un incrocio: un' erogazione di coppia non desiderata da parte della macchina elettrica causerebbe un avanzamento longitudinale del veicolo, rischiando di dar luogo ad un impatto con il veicolo che precede o, più gravemente, all'investimento di un pedone.

Una prima simulazione è stata svolta andando a disabilitare il sistema di recovery, lasciando quindi al guidatore il compito di recuperare il controllo del veicolo. I risultati ottenuti costituiranno un valido confronto fra l'azione umana e la risposta del controllo elettronico.

In Figura 8.2 si può osservare l'andamento dello spostamento del veicolo, in seguito al verificarsi del malfunzionamento, nel caso in cui il guidatore riesca a schiacciare prontamente il pedale del freno. Il tempo di risposta del guidatore è stato posto pari a $t_{risp} = 1.2s$.

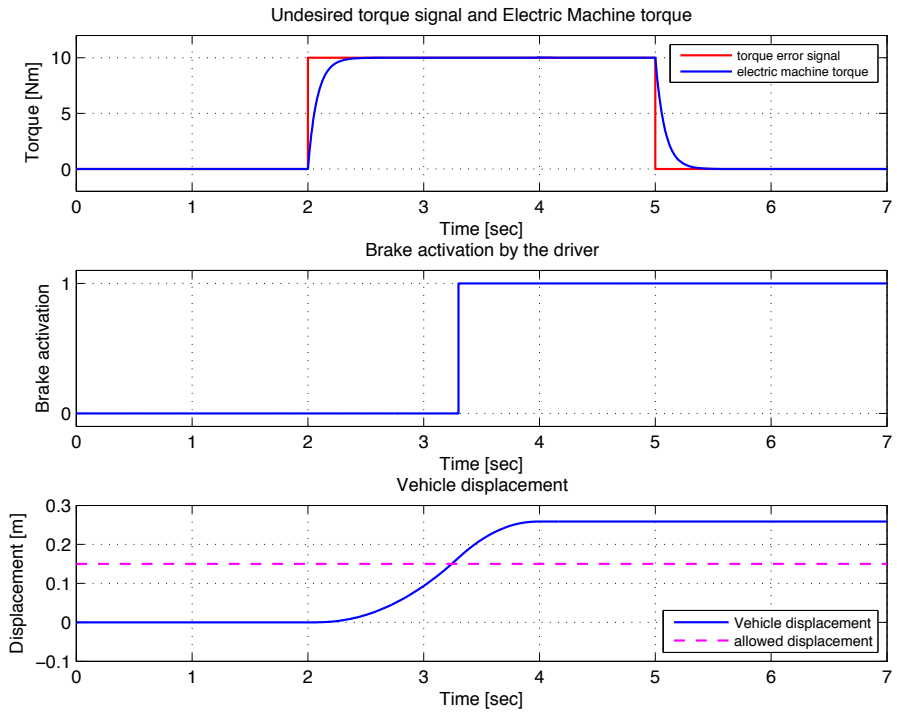

Figura 8.2: spostamento del veicolo in seguito alla frenata da parte del guidatore

si nota come il veicolo superi abbondantemente il limite di spostamento imposto, pari a $0.15\,m$, interrompendo la propria corsa a circa $0.26\,m$.

La successiva simulazione è stata svolta andando ad attivare il sistema di recovery; in Figura 8.3 si può osservare come, ora, il requisito di sicurezza sia rispettato

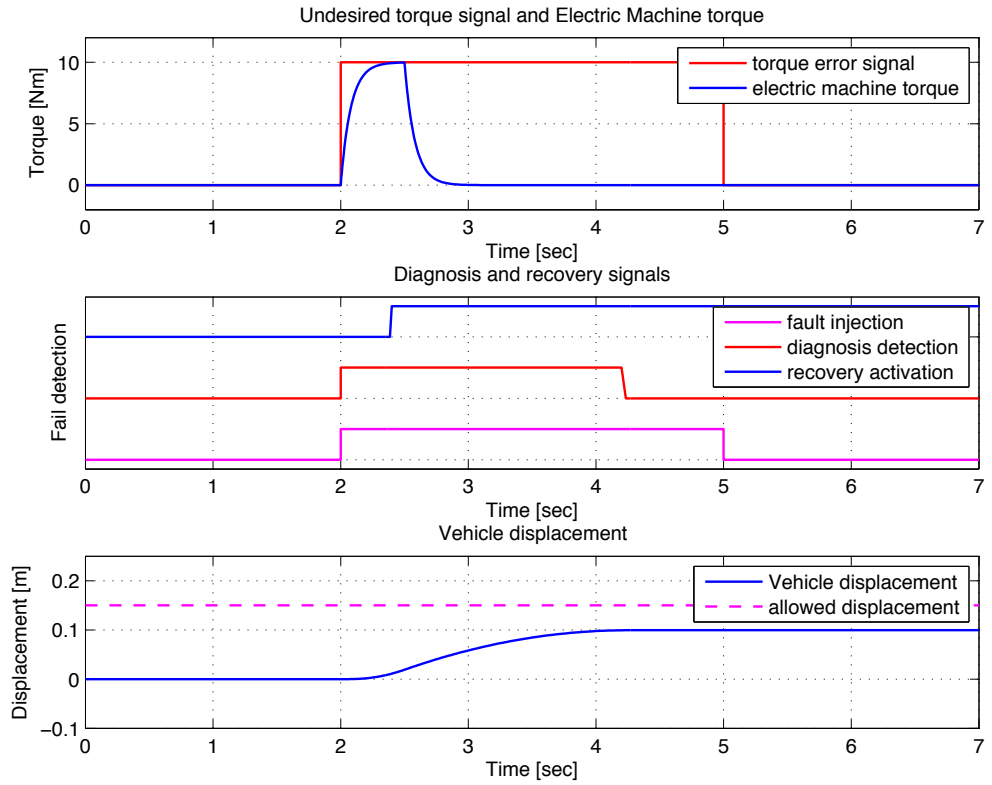

Figura 8.3: spostamento del veicolo in seguito all'attivazione della recovery

stavolta il veicolo interrompe la propria corsa in uno spazio inferiore agli $0.1\,m$; nel grafico centrale si può osservare l'andamento temporale dei segnali di iniezione del guasto, il riconoscimento da parte della diagnostica e l'attivazione del sistema di recovery (si nota come il sistema di diagnosi rilevi prontamente il malfunzionamento).

8.1.1 Analisi di sensitività parametrica

Il sistema di diagnosi segnala la presenza del malfunzionamento nel caso in cui l'inverter stia inviando una corrente non desiderata alla macchina elettrica per un intervallo di tempo superiore a t_{att}, sono quindi effettuate delle simulazioni discrete, al variare di tale soglia temporale. I risultati delle simulazioni sono illustrati in Figura 8.4

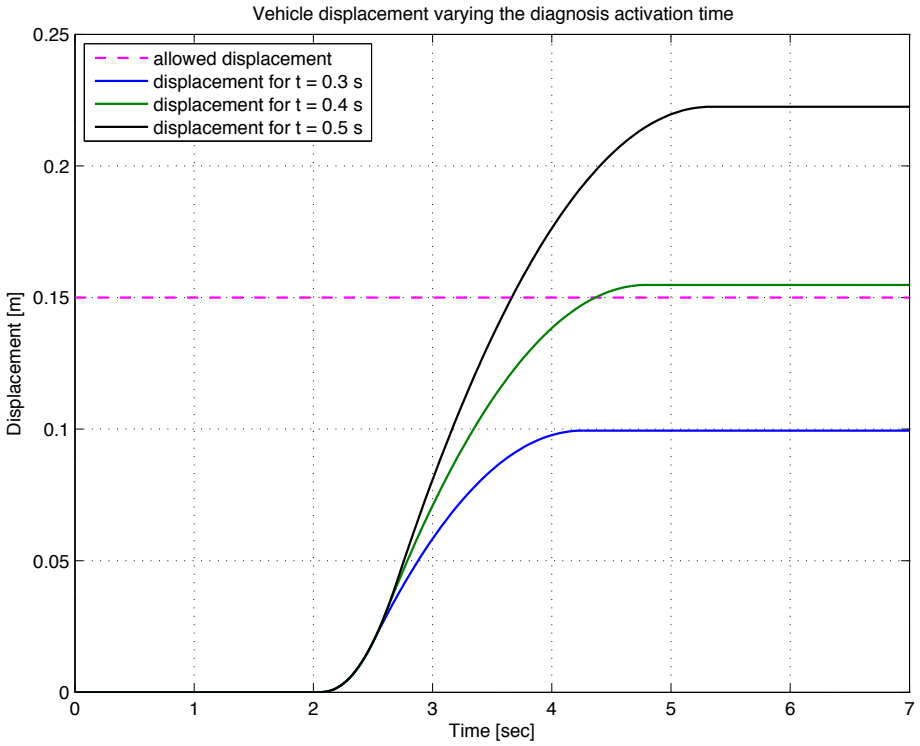

Figura 8.4: Andamento dello spostamento al variare di t_{att}

si osserva come, per valori di $t_{att} \geq 0.4s$, non sia rispettato il requisito di sicurezza sullo spostamento del veicolo.

8.2 Coppia superiore a quella richiesta

Un'erogazione di coppia superiore a quella richiesta causa un'accelerazione non desiderata del veicolo, che può provocare un impatto con il veicolo che precede.

Le simulazioni sono state svolte seguendo un profilo di strada urbana (condizioni in cui è elevata la presenza di veicoli e di pedoni nelle immediate vicinanze): in tale scenario il veicolo opera in modalità puramente elettrica, e quindi un malfunzionamento del sistema di propulsione si ripercuote significativamente sulla dinamica.

In Figura 8.5 è mostrato l'andamento della coppia della macchina elettrica e la velocità del veicolo, in seguito al verificarsi del guasto, nel caso in cui il sistema di recovery non sia attivo

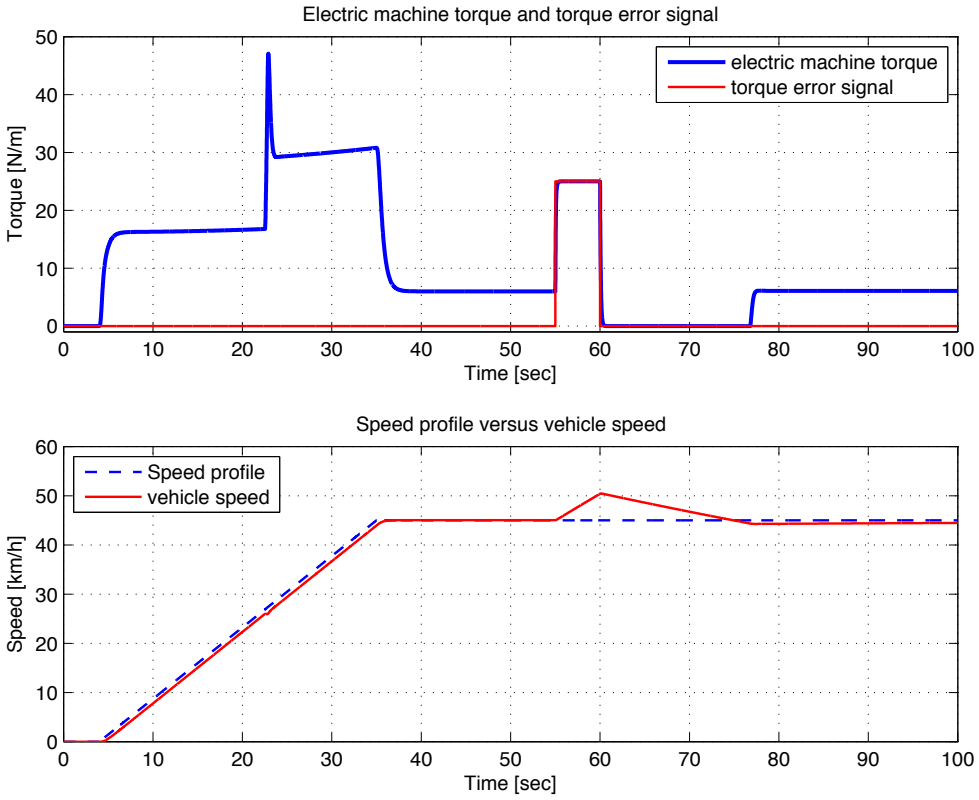

Figura 8.5: Andamento della velocità del veicolo in seguito al malfunzionamento

si può osservare come il malfunzionamento, in condizioni stazionarie, provochi un'elevata accelerazione, portando in breve tempo la velocità del veicolo oltre

il profilo desiderato: è necessario quindi che i sistemi di diagnosi e recovery intervengano tempestivamente.

Le seguenti simulazioni sono svolte andando ad attivare la modalità di recovery. L'obiettivo di sicurezza è quello di mantenere la velocità del veicolo quanto più vicina al profilo di velocità desiderato, mentre l'azione svolta dalla recovery è quella di inibire la macchina elettrica (fonte del guasto, e quindi probabilmente non più funzionante), e forzare l'attivazione del motore termico.

In Figura 8.6 è mostrato l'andamendo della coppia della macchina elettrica e la velocità del veicolo, nel caso in cui il sistema di recovery sia attivo

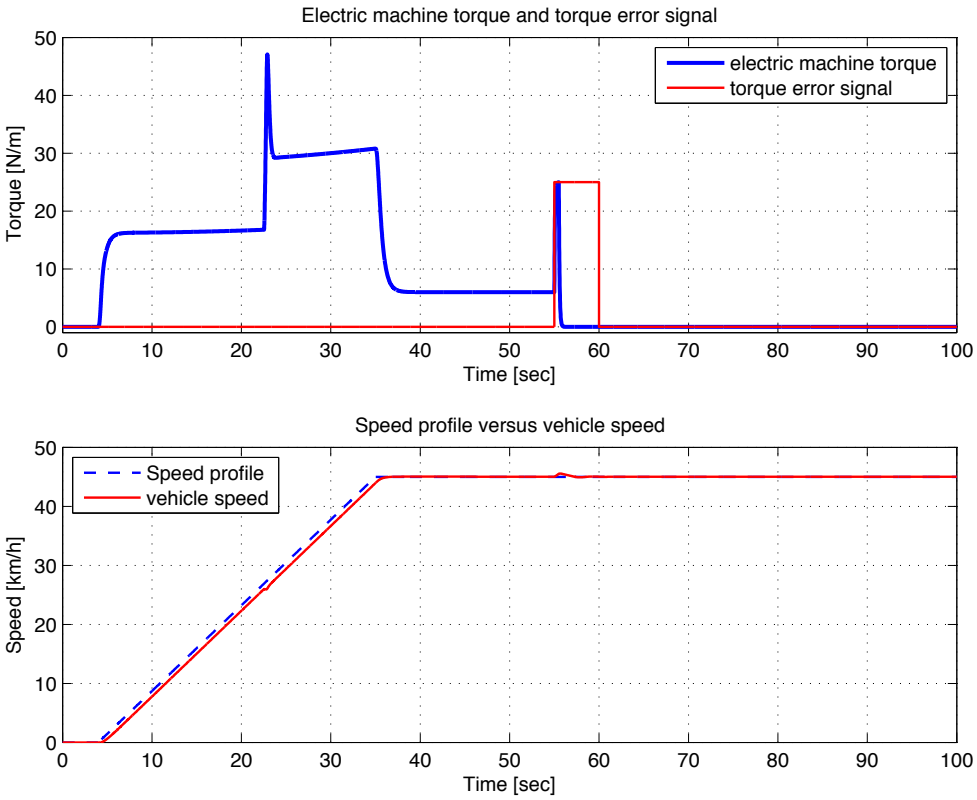

Figura 8.6: Andamento della velocità del veicolo in seguito al malfunzionamento, nel caso di recovery attiva

osservando il primo grafico, si nota come la coppia vada a zero in seguito all'attivazione del sistema di recovery, permettendo un mantenimento del profilo di velocità.

Nel dettaglio, in Figura 8.7 si osservano i segnali di attivazione della diagnosi e della recovery, oltre alle coppie del motore elettrico e del motore termico

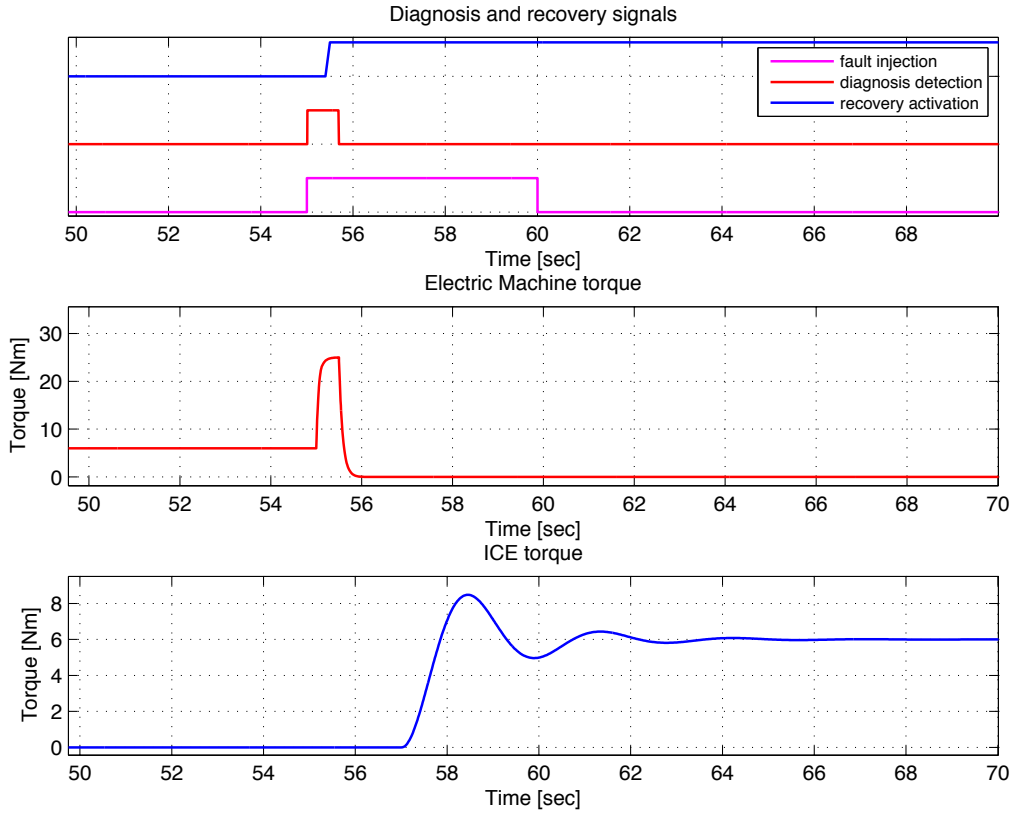

Figura 8.7: Andamento dei segnali di attivazione di diagnosi e recovery, e delle coppie dei due motori

a seguito dell'attivazione del segnale di recovery, la macchina elettrica è disattivata e diviene attivo il motore termico.

8.3 Coppia inferiore quella richiesta

Un'erogazione di coppia inferiore a quella desiderata può causare un brusco calo di prestazioni, e quindi portare ad una situazione di pericolo in accordo al tipo di manovra che si sta compiendo.

Per le simulazioni è stata considerata una manovra di sorpasso: un calo di prestazioni dovuto ad un malfunzionamento porterebbe un ritardo nel compimento della manovra, con rischio di impatto frontale con i veicoli che procedono nella corsia opposta.

In figura 8.8 si osserva come, nel caso in cui il sistema di recovery non sia attivo, il malfunzionamento causi un ritardo di circa 5 secondi nel compimento della manovra

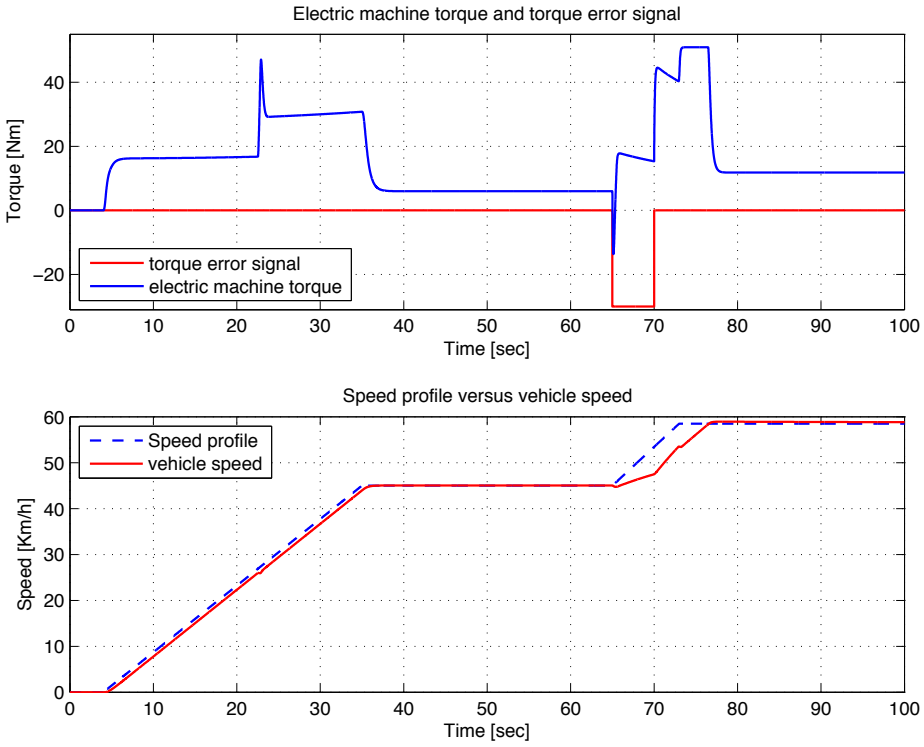

Figura 8.8: Andamento della velocità del veicolo in seguito al malfunzionamento

In Figura 8.9 si osserva invece l'andamento della velocità del veicolo, in seguito al malfunzionamento, nel caso in cui il sistema di recovery sia attivo

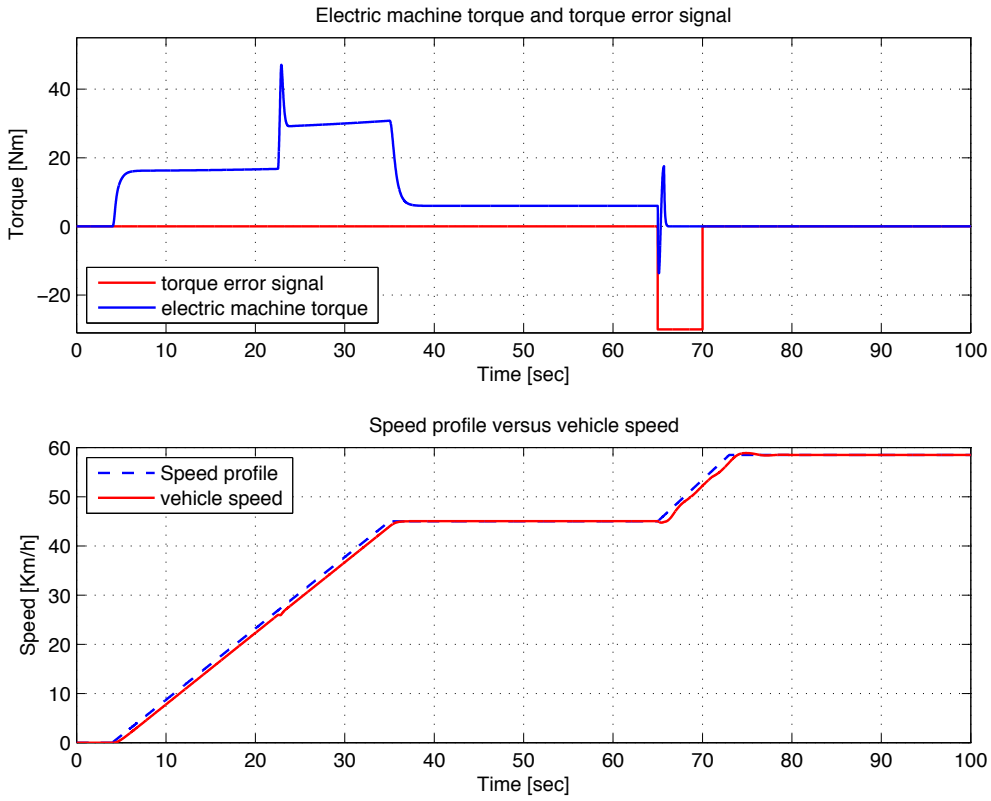

Figura 8.9: Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery attiva

in seguito all'attivazione del sistema di recovery, la macchina elettrica è disattivata e l'attivazione del motore temico porta a compimento la manovra.

Analogamente al precedente malfunzionamento, in Figura 8.10 si può osservare l'andamento dei segnali di attivazione di diagnosi e recovery, con la conseguente inibizione della macchina elettrica e l'attivazione del motore termico

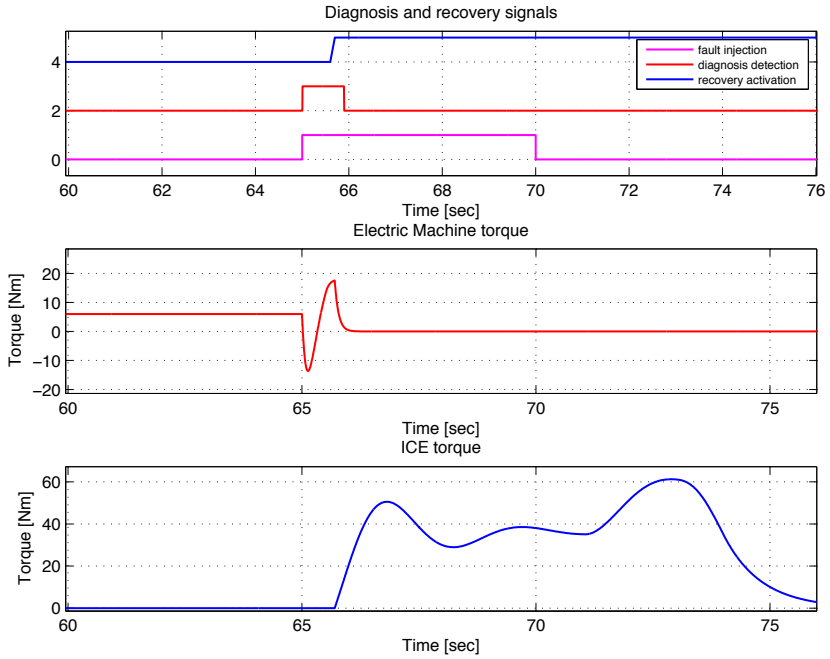

Figura 8.10: Attivazione di diagnosi e recovery, e coppie dei due motori

Risulta di interesse un contronto fra le prestazioni ottenute rispettivamente con e senza il malfunzionamento

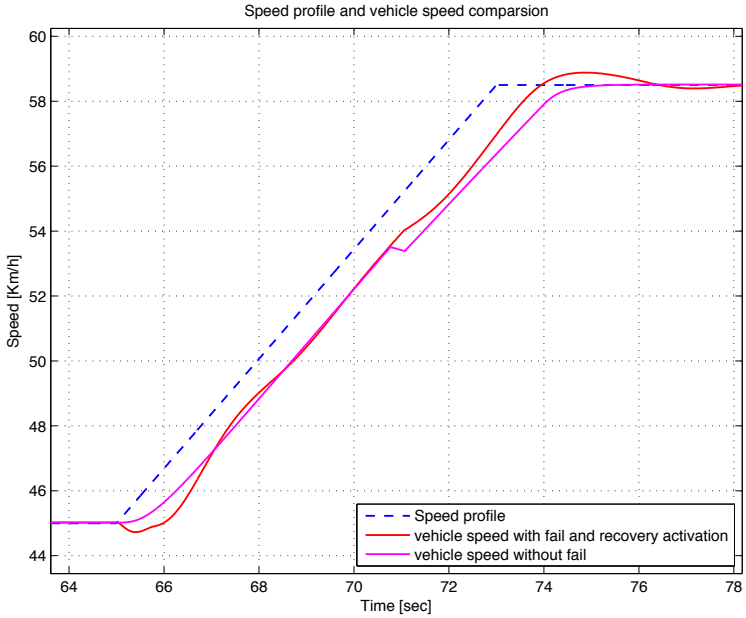

Figura 8.11: Confronto fra le velocità del veicolo con, e senza, malfunzionamento

Il profilo di velocità ottenuto in presenza del malfunzionamento risulta migliore in quanto è attivo il solo motore termico, caratterizzato da performance superiori rispetto alla macchina elettrica: tale profilo di velocità è comunque caratterizzato da un ritardo nella salita, dovuto al tempo di attivazione dei sistemi di diagnosi e recovery, ed alla più lenta dinamica del motore termico rispetto al motore elettrico.

8.4 Coppia nulla

Questo tipo di malfunzionamento rappresenta un caso estremo di coppia erogata inferiore a quella richiesta, ma necessita comunque di una diagnodi apposita, in quanto produrrà un requisito di sicurezza più stringente.

Analogamente al precedente malfunzionamento, le simulazioni sono effettuate andando a compiere una manovra di sorpasso; in Figura 8.12 si può osservare l'andamento della velocità del veicolo, nel caso in cui si verifichi assenza di coppia per un intervallo di tempo prolungato

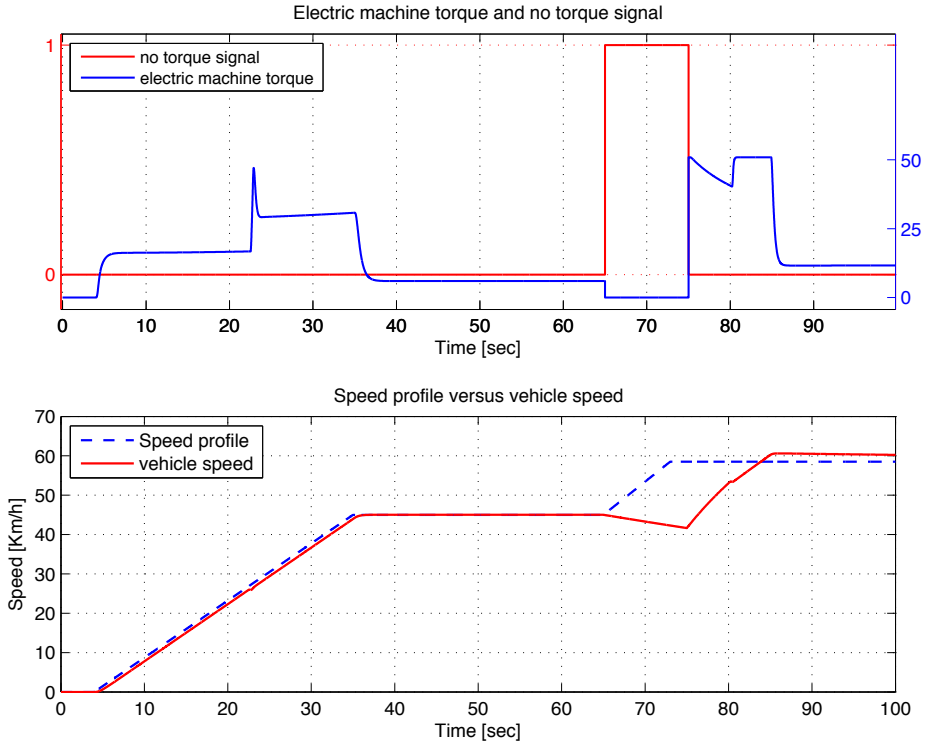

Figura 8.12: Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery disattiva

si può osservare come, nel primo grafico, la coppia della macchina elettrica si annulli in corrispondenza del verificarsi del malfunzionamento; diversamente al caso precedente, stavolta la manovra potrà essere conclusa solo al concludersi del malfunzionamento.

Nel caso in cui il sistema di recovery sia attivo, il malfunzionamento viene gestito correttamente, ed in Figura 8.13si può osservare come la manovra sia compiuta senza difficoltà

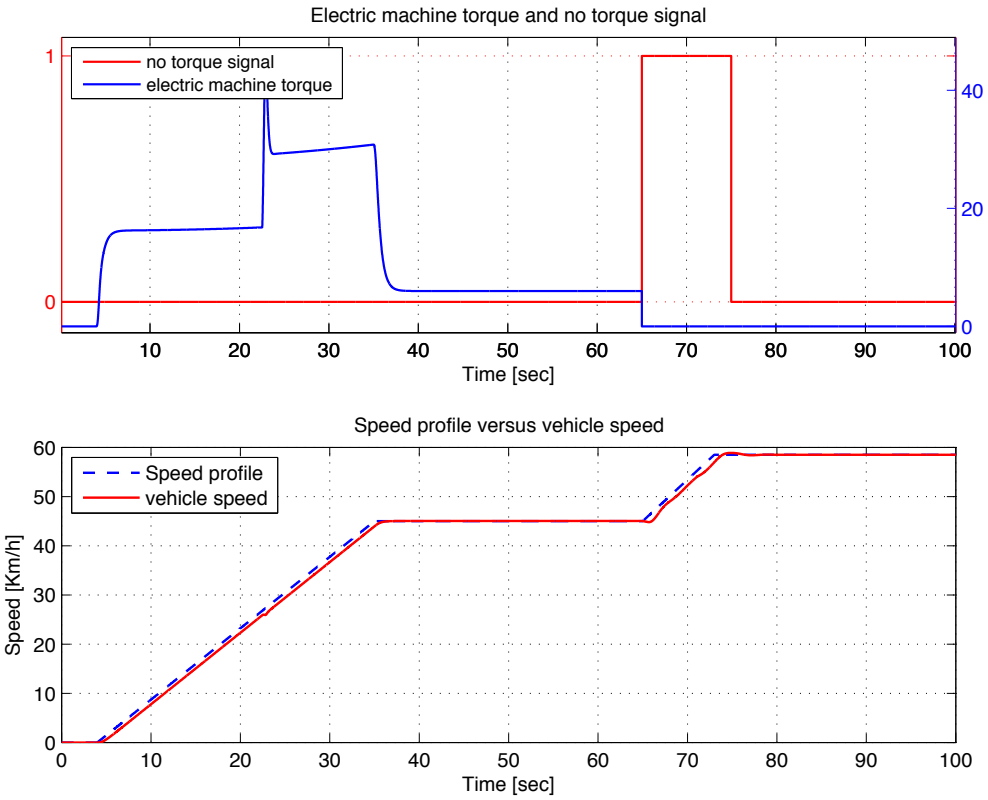

Figura 8.13: Andamento della velocità del veicolo in seguito al malfunzionamento, con recovery attiva

nel primo grafico si osserva l'andamento della coppia della macchina elettrica, che va a zero al verificarsi del malfunzionamento e vi rimane in quanto il sistema di recovery attiva forzatamente il motore termico.

Per completezza, in Figura 8.14 si osserva l'andamento dei segnali di attivazione dei sistemi di diagnosi e recovery, e le coppie erogate dai due motori

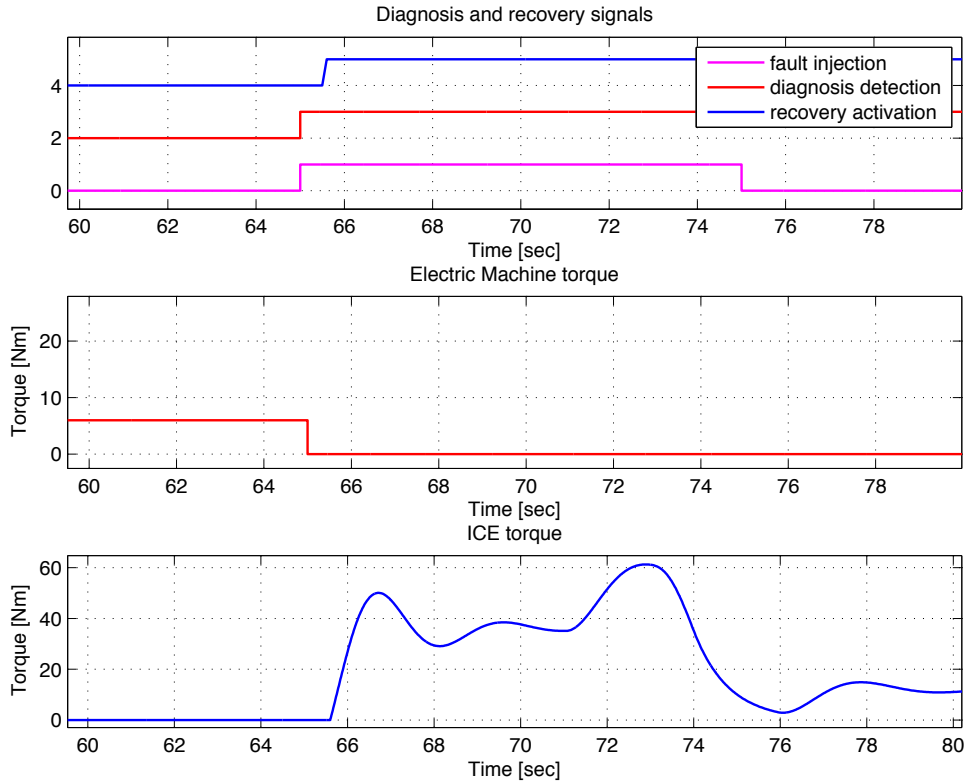

Figura 8.14: Andamento dei segnali di attivazione di diagnosi e recovery, e delle coppie dei due motori

l'attivazione del sistema di recovery inibisce la macchina elettrica, forzando l'attivazione del motore termico ed il conseguente recupero della manovra.

Capitolo 9

Automi Ibridi

L'analisi accurata di qualsiasi fenomeno o sistema fisico passa attraverso una sua descrizione mediante il linguaggio matematico. L'individuazione del sistema fisico presenta larghi margini di arbitrarietà, dal momento che che le interazioni fra le parti di un sistema possono risultare numerose, e non è detto che sia ottimale cercare di rappresentarle tutte. Inoltre, cercare di modellare tutte le dinamiche porta ad elevati livelli di complessità. Per descrivere correttamente un sistema bisogna, innanzitutto, definire gli aspetti del suo comportamento, che hanno un'importanza rilevante nell'analisi che si sta compiendo, e valutare l'equilibrio ottimale in relazione agli scopi dell'analisi, ottenendo un buon compromesso tra accuratezza della rappresentazione e semplicità di funzionamento.

Negli ultimi anni è cresciuta in molti campi di ricerca, dall'informatica, all'elettronica, fino al controllo di processi, la necessità di integrare i classici modelli matematici, in grado di descrivere le dinamiche continue dei sistemi, con componenti logici descrivibili per mezzo di macchine a stati finiti o regole "if - then - else". Tali sistemi, descritti da interconnessioni di sistemi dinamici e dispositivi logici, vengono definiti con il termine di *automi ibridi*.

Il concetto di modello di un sistema è tradizionalmente associato a equazioni differenziali, tipicamente derivate da leggi fisiche che ne governano le dinamiche: la teoria e gli strumenti di controllo per questi modelli classici sono numerosi ed esaustivi.

D'altra parte, in molte applicazioni il sistema che deve essere controllato è costituito non solo da una dinamica continua ma, molto spesso, da componenti

logici quali valvole, interruttori e selettori di velocità. Fino a poco tempo fa la progettazione del controllo era basata su regole euristiche, derivanti dalla conoscenza pratica del sistema in esame. Per ovviare a questa problematica i ricercatori hanno iniziato a trattare i sistemi ibridi, ovvero processi che evolvono secondo dinamiche continue (in genere di basso livello, come ad esempio motori) e regole logiche (di alto livello, come ad esempio dispositivi elettronici): per cui i sistemi ibridi sono sistemi in cui una parte logica discreta (generalmente un automa a stati finiti) interagisce strettamente con un sistema tempo continuo.

Gli automi ibridi sono usati come modelli matematici per molte importanti applicazioni, come sistemi di controllo del traffico aereo, sistemi manifatturieri, processi chimici e reti di comunicazione in tempo reale. In figura 9.1 è rappresentato uno schema di automa ibrido

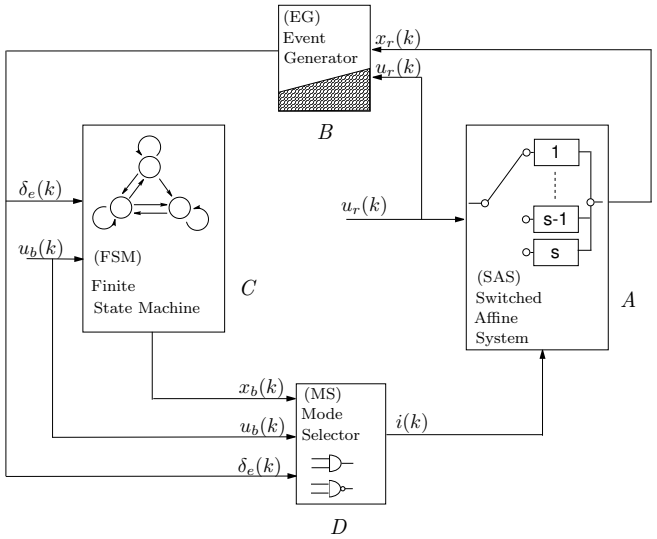

Figura 9.1: Schema di un automa ibrido

l'automa è costituito da una macchina a stati finiti che raccoglie le dinamiche discrete del sistema ibrido, con uno "switched affine system" che rappresenta la parte continua delle dinamiche ibride. L'interazione tra le due parti è affidata a due elementi di connessione: il generatore di eventi e il selettore di modo. Il primo prende i segnali tempo continui della parte continua e genera dei segnali discreti, i quali insieme ad altri ingressi discreti esterni attivano il cambiamento di stato della macchina a stati finiti. Il secondo combina tutte le

varie componenti discrete per selezionare il modo operativo, ossia le dinamiche continue del sistema switched affine.

9.1 Definizione di Automa ibrido

In letteratura sono molte le definizioni di automa ibrido, e le pubblicazioni a riguardo stanno aumentando esponenzialmente. In questo capitolo si presenta la più famosa definizione di Automa Ibrido che si è affermata in questi anni

Definizione 9.1. Un Automa ibrido H è una collezione $H = (Q, X, f, Init, Dom, E, G, R)$, dove

- $Q = \{q_1, q_2, \dots\}$ è l'insieme finito degli stati discreti,
- $X = \mathbb{R}^n$ è lo spazio di stato continuo,
- $f(\cdot, \cdot) : Q \times X$ definisce il flusso continuo in ogni stato $q \in Q$ mediante l'equazione $\dot{x} = f(q, x)$,
- $Init \subseteq Q \times X$ definisce gli stati iniziali ammissibili,
- $Dom(\cdot) : Q \to 2^X$ assegna ad ogni stato discreto $q \in Q$ un dominio per lo stato continuo: $x \in Dom(q)$,
- $E \subseteq Q \times Q$ insieme finito delle transizioni discrete,
- $G(\cdot) : E \to 2^X$ assegna condizioni di guardia ad ogni transizione discreta $e = (q, q') \in E$,
- $R(\cdot, \cdot) : E \times X \to 2^X$ assegna reset ad ogni transizione discreta $e = (q, q') \in E$ e ad ogni stato $x \in G(e)$,

Un esempio di rappresentazione di Automa Ibrido è illustrato in figura 9.2

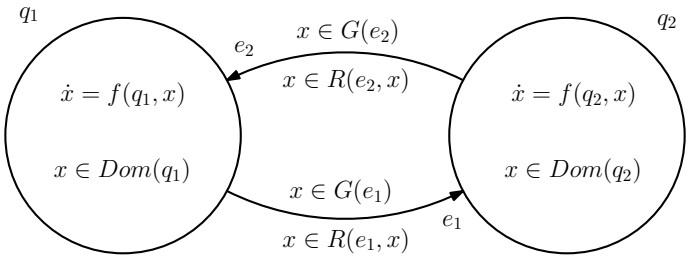

Figura 9.2: Esempio di rappresentazione di un automa ibrido

9.2 Lo studio del Safe Set

Individuate delle condizioni o proprietà di sicurezza che l'automa ibrido deve rispettare, si può identificare una regione dello spazio di stato $Q \times X$ in cui esse siano sempre verificate. Se l'evoluzione, sia continua che discreta, dell'automa ibrido rimane confinata in questa regione dello spazio di stato, allora l'automa si definisce *Safe* (sicuro).

Definizione 9.2. Lo stato (q, x) rimane sempre in un insieme di stati $F \subset Q \times X$. Nella dicitura Temporal Logic

$$\Box\,(q, x) \in F$$

Una volta enunciata la definizione di safe set, si può procedere ad un suo studio relativamente alle simulazioni dei malfunzionamenti svolte nel capitolo 8, andando stavolta ad effettuare uno studio della sicurezza mediante la teoria degli automi ibridi.
Gli obiettivi di sicurezza, determinati nel capitolo 6, possono essere associati a condizioni di Safe per l'automa ibrido. Questo permetterà quindi di svolgere un'analisi di tipo analitico, oltre che qualitativa sulle sole simulazioni.

Per attuare uno studio di questo genere si prende in esame un diverso formalismo per definire un automa ibrido, come segue

Definizione 9.3. Un Automa ibrido H è una collezione $H = ((Q, X), (\Sigma_c, U), \left(M_c^{disc}, M_c^{cts}\right), (\Sigma_e, D), \left(M_e^{disc}, M_e^{cts}\right), (\delta, f))$ dove

- Q rappresenta l'insieme finito degli stati discreti,

- $X \subseteq \mathbb{R}^n$ rappresenta lo spazio di stato continuo,
- Σ_c rappresenta l'insieme finito discreto di eventi di controllo, $\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_c^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$,
- $U \subseteq \mathbb{R}^m$ rappresenta l'insieme continuo degli ingressi di controllo tale che $\mathcal{U} = \{u(\cdot) \in PC^0 \mid u(t) \in U, \forall t\}$, $M_c^{cts} : Q \times X \to 2^U \setminus \{\}$,
- Σ_e rappresenta l'insieme finito discreto di eventi di disturbo, $\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_e^{disc} : Q \times X \to 2^{\Sigma_e^\epsilon} \setminus \{\}$,
- $D \subseteq \mathbb{R}^p$ rappresenta l'insieme continuo degli ingressi di disturbo tale che $\mathcal{D} = \{d(\cdot) \in PC^0 \mid d(t) \in U, \forall t\}$, $M_e^{cts} : Q \times X \to 2^D \setminus \{\}$,
- $\delta : Q \times X \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X} \setminus \{\}$ sono le transizioni discrete tra uno stato ed un altro, $\delta(q, x, \sigma_c, \sigma_e) = W \subseteq Q \times X$, $\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$,
- $f : Q \times X \times U \times D \to \mathbb{R}^n$ definisce il flusso continuo, $\dot{x}(t) = f_q(x(t), u(t), d(t))$ con $x(t_0) = x_0$.

Una volta definito il formalismo adottato, si procede ad enunciare l'algoritmo ricorsivo da applicare per identificare il safe set. L'algoritmo è il seguente

Algoritmo 9.1 Algoritmo Fixed Point Procedure [Tomlin, Lygeros, Sastry - HSCC98]

$W^0 := Good$
$i := -1$;
repeat{
$i := i + 1$;
$W_d^i := W^i \setminus Pre_e(W^i)$;
$W^{i+1} := W_d^i \setminus Unavoid\_Pre\left(Pre_e(W^i) \cup \overline{W^i}, Pre_c(W^i)\right)$;
}until $W^{i+1} = W^i$
$Safe := W^i$

dove Pre_e, Pre_c e $Unavoid\_Pre$ sono operatori discreti e continui che hanno la seguente espressione

$$Pre_e\left(W^i\right) = \left\{(q, x) \in Q \times X : \forall \sigma_c \in M_c^{disc}(q, x), \exists \sigma_e \in M_e^{disc}(q, x) \mid (\sigma_c, \sigma_e) \neq (\epsilon, \epsilon) \wedge \delta(q, x, \sigma_c, \sigma_d) \nsubseteq W^i\right\} \quad (9.1)$$

$$Pre_c\left(W^i\right) = \left\{(q,x) \in Q \times X : \exists \sigma_c \in M_c^{disc}\left(q,x\right), \forall \sigma_e \in M_e^{disc}\left(q,x\right) \mid \right.$$
$$\left. \left(\sigma_c, \sigma_e\right) \neq (\epsilon, \epsilon) \wedge \delta\left(q,x,\sigma_c,\sigma_d\right) \subseteq W^i \right\} \quad (9.2)$$

$$Unavoid\_Pre\left(B,E\right) = \left\{(q,\hat{x}) \in Q \times X \mid \forall u \in M_c^{cts} \exists \overline{t} > 0, \exists d \in M_e^{cts} \mid \right.$$
$$\text{such that for the trajectory } x\left(t\right) = \psi_q\left(u,d,\hat{x},t\right) \text{ we have}$$
$$\left. \forall \tau \in \left[0,\overline{t}\right)\left(q,x\left(\tau\right)\right) \in \text{Wait} \cap \overline{E} \wedge \left(q,x\left(\overline{t}\right)\right) \in B \right\} \quad (9.3)$$

Tali operatori permettono di eliminare regioni dello spazio di stato in cui l'evoluzione dell'automa ibrido porti, a causa di disturbi discreti e/o continui, a violare le condizioni si sicurezza imposte. L'algoritmo ricorsivo può anche non convergere ad un punto fisso: nel caso di convergenza, lo spazio di stato trovato costituirà lo spazio $Safe$.

Lo spazio di stato *Good* identifica un sottospazio di $Q \times X$ in cui l'automa non viola le condizioni di sicurezza. Una volta trovata la regione $Safe$, si può definire il controllo massimale (*Maximal Controller*), il quale è rappresentato dalla famiglia di tutti i controllori tali che, data una qualsiasi configurazione $(q,x) \in Safe$, l'evoluzione dell'automa ibrido resta confinata nello spazio di stato $Safe$.

9.3 Coppia non desiderata a veicolo fermo

Si analizza il caso di guasto esposto nel capitolo 6, in cui il veicolo è fermo, il guidatore non richiede nessuna coppia agendo sul pedale dell'accelerazione, ma a causa di malfunzionamento di un componente elettrico/elettronico (nel nostro caso l'inverter fornisce una corrente errata alla macchina elettrica) il veicolo avanza longitudinalmente, portando a situazioni di pericolo esposte nel capitolo precedentemente menzionato.

Innanzitutto si è studiata la dinamica del guasto, realizzando quindi un automa ibrido in grado di rappresentare fedelmente i vari scenari possibili. Si parte con uno scenario in cui la vettura non è in movimento. A causa di un guasto questa riceve una coppia non desiderata che causa uno spostamento del veicolo; se lo spostamento è maggionre della soglia di sicurezza, fissata a $0.15m$, si ha la violazione del requisito di sicurezza portando l'evoluzione

dell'automa ibrido nel *Bad State*; nel caso in cui il controllo agisca tempestivamente, aprendo le frizioni in tempo utile a non superare la soglia di sicurezza, il veicolo decelererà fino a fermarsi. Le variabili continue che modellano questa dinamica sono la velocità del veicolo x_1 e lo spostamento del veicolo x_2. L'automa ibrido risultante da questo studio della dinamica è rappresentato in figura 9.3

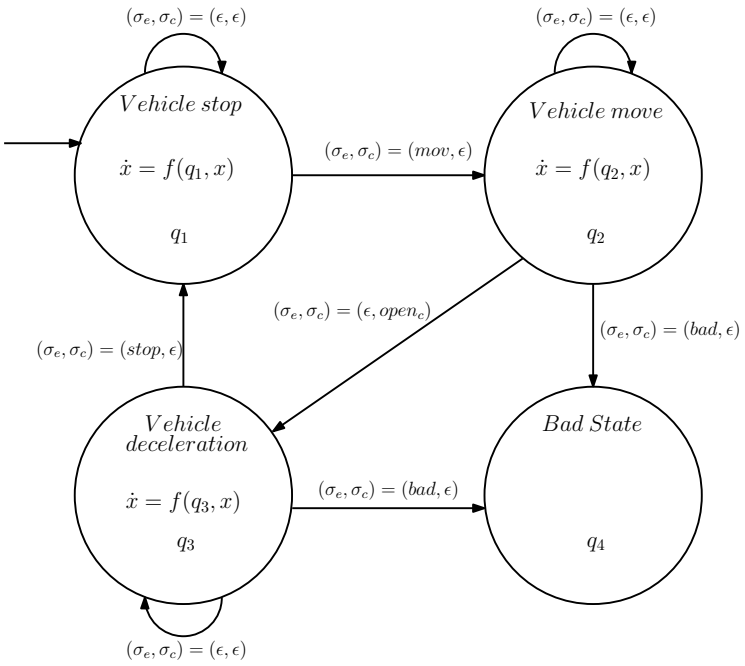

Figura 9.3: Rappresentazione dell'automa ibrido in caso di coppia non desiderata a veicolo fermo

Per rappresentare l'automa ibrido si è scelto di utilizzare la nomenclatura della definizione 9.3, che però non permette di avere transizioni fra stati discreti con condizioni sulle variabili di stato continue, per cui si è convenuto di modellare queste condizioni come se fossero disturbi discreti dati da σ_e. Per esempio il passaggio nello stato discreto *Bad State* è causato da uno spostamento dell'automobile superiore alla soglia $0.15m$, per cui quando $x_2 > 0.15m$: questa transizione è stata convertita in un disturbo discreto tale che questo valga $\sigma_e = bad$ nel caso in cui $x_2 > 0.15m$.

Per cui l'automa ibrido sarà costituito dalla collezione

$H = \left((Q, X), (\Sigma_c, U), \left(M_c^{disc}, M_c^{cts}\right), (\Sigma_e, D), \left(M_e^{disc}, M_e^{cts}\right), (\delta, f)\right)$, dove

- $Q = \{q_1, q_2, q_3, q_4\}$;,
- $X = [0, +\infty) \times [0, +\infty)$,
- $\Sigma_c = \{open\}$, $\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_c^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$,
- $U \in [0, 52]\text{Nm}, \mathcal{U} = \{u(\cdot) \in PC^0 \mid u(t) \in U, \forall t\}$, $M_c^{cts} : Q \times X \to 2^U \setminus \{\}$,
- $\Sigma_e = \{move, bad, stop\}$, $\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_e^{disc} : Q \times X \to 2^{\Sigma_e^\epsilon} \setminus \{\}$,
- $D \in [0, 52]\text{Nm}, \mathcal{D} = \{d(\cdot) \in PC^0 \mid d(t) \in U, \forall t\}$, $M_e^{cts} : Q \times X \to 2^D \setminus \{\}$,
- $\delta : Q \times X \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X} \setminus \{\}$ sono le transizioni discrete tra uno stato ed un altro, $\delta(q, x, \sigma_c, \sigma_e) = W \subseteq Q \times X$, $\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$,
- $f : Q \times X \times U \times D \to \mathbb{R}^n$ definisce il flusso continuo, $\dot{x}(t) = f_q(x(t), u(t), d(t))$ con $x(t_0) = x_0$.

Riprendendo il modello matematico semplificato esposto nel capitolo 5 a pagina 58, la velocità del veicolo sarà descritta dalla formula 5.7. Si possono effettuare ulteriori semplificazioni, infatti si sta modellando un caso in cui il veicolo è fermo o si sposta a velocità relativamente basse, per cui è possibile eliminare dall'equazione la forza aerodinamica $\frac{\gamma}{M} v^2 sign(v)$. Considerando poi che si sta analizzando un avanzamento del veicolo, non serve la dipendenza dal segno $sign(\bar{\varsigma}(u_1 + u_2)) = 1$; inoltre il guidatore non sta premendo il pedale del freno, per cui la forza frenante è nulla ($F_{brake} = 0$). Essendo il veicolo fermo, il motore termico è spento ($u_2 = 0$), e i disturbi continui modellati sono due: d_1 è il disturbo generato da una corrente errata fornita dall'inverter, mentre d_2 è un disturbo che rappresenta le perdite non modellate della macchina elettrica.

Da queste considerazioni, i flussi continui per ogni stato discreto risultano

$$f(q_1, x) = \begin{bmatrix} -0.001 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ d_1 \\ d_2 \end{bmatrix} - \begin{bmatrix} \frac{1}{M} \\ 0 \end{bmatrix} F_\mu \tag{9.4}$$

$$f(q_2, x) = \begin{bmatrix} -0.001 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ d_1 \\ d_2 \end{bmatrix} - \begin{bmatrix} \frac{1}{M} \\ 0 \end{bmatrix} F_\mu \tag{9.5}$$

$$f(q_3, x) = \begin{bmatrix} -0.001 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} - \begin{bmatrix} \frac{1}{M} \\ 0 \end{bmatrix} F_\mu \tag{9.6}$$

in cui il termine in posizione $(1, 1)$ consente di tenere conto dell' attrito dovuto dalla velocità, mentre nel caso $f(q_3, x)$ non sono presenti gli ingressi per via dell'azione del controllo che apre le frizioni non permettendo il passaggio di coppia. Le condizioni iniziali risultano

$$x_1(0) = 0 \tag{9.7}$$

$$x_2(0) = 0 \tag{9.8}$$

Per quanto riguarda gli ingressi discreti del disturbo e del controllo, essi sono così definiti: il disturbo può attuare $\Sigma_e = \{move, bad, stop\}$, rispettivamente nel caso in cui il veicolo si trova in moto ($x_1 > 0$), nel caso in cui il veicolo superi la soglia di sicurezza impostata ($x_2 > 0.15$) e nel caso in cui il veicolo sia fermo ($x_1 = 0$), mentre il controllo può attuare un unica strategia $\Sigma_c = \{open\}$, che consiste nell'apertura delle frizioni.

Definito l'automa ibrido, si applica l'algoritmo 9.1 per individuare la regione $Safe$. Lo spazio di stato continuo in ogni stato discreto q_i, con i rispettivi segnali discreti di disturbo e controllo sono rappresentati in figura 9.4

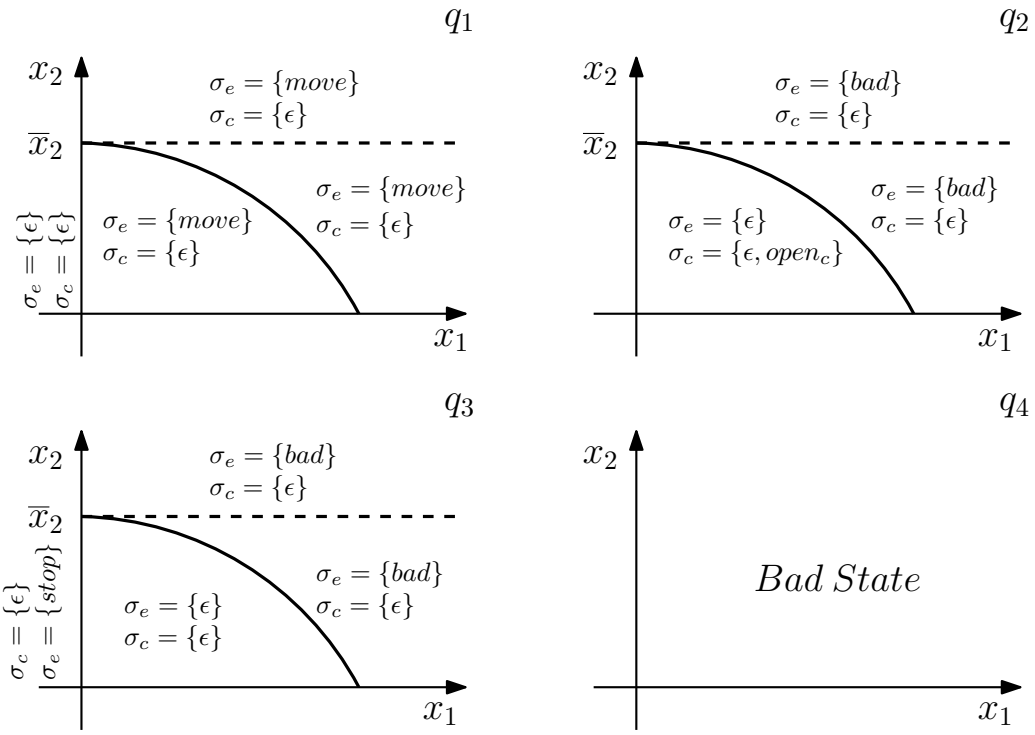

Figura 9.4: Spazio di stato continuo in ogni stato discreto q_i

I grafici dello spazio delle fasi presentano rispettivamente la velocità x_1 sulle ascisse e lo spazio percorso x_2 sulle ordinate. Con $\bar{x}_2$ è indicato lo spostamento massimo consentito alla vettura, oltre il quale si avrà violazione del requisito di sicurezza. La parabola, che divide in due regioni lo spazio di stato al di sotto della retta $x_2 = \bar{x}_2$, descrive la dinamica di decelerazione nel caso di frizioni aperte, cioè il flusso continuo $f(q_3, x)$. Ne risulta, quindi, che per fermare il veicolo nello spazio di sicurezza l'azione del controllo dovrà essere attivata nella regione interna, o al massimo sulla parabola in questione.

Si procede con l'applicazione dell'algoritmo. L'insieme W^0 è così costituito

$$W^0 = \{q_1, q_2, q_3\} \times X \tag{9.9}$$

Il primo passo dell'algoritmo porta a calcolare l'operatore $Pre_e(W^0)$: questo operatore definisce lo spazio di stato in cui, dato un qualsiasi controllo, esiste un disturbo tale che la coppia sia diversa da$\{\epsilon, \epsilon\}$ che attivi una transizione che porta l'evoluzione dell'automa ibrido in uno spazio non contenuto in W^i.

In figura 9.5 l'operatore $Pre_e\left(W^0\right)$ è rappresentato in verde, e vale

$$Pre_e\left(W^0\right) = \{q_2, q_3\} \times \{Parabola > 0\} \tag{9.10}$$

per cui la $W_d^0 = W^0 \setminus Pre_e\left(W^0\right)$. L'operatore $Pre_c\left(W^0\right)$ rappresenta lo spazio di stato in cui esiste un controllo tale che, per qualsiasi disturbo, con la coppia diversa da$\{\epsilon, \epsilon\}$, si attivi una transizione che porta l'evoluzione dell'automa in uno spazio contenuto in W^i. Questo nella figura 9.5 è rappresentato in blu, e vale

$$Pre_c\left(W^0\right) = \{q_1\} \times X \cup \{q_2\} \times \{Parabola < 0\} \cup \{q_3\} \times \{x_1 = 0\} \tag{9.11}$$

L'operatore $Unavoid\_Pre\left(B, E\right)$ in questo caso è l'insieme vuoto, non essendoci nessuna zona in cui l'evoluzione libera della variabile continua porti l'Automa ibrido in uno stato appartenente a $Pre_e\left(W^0\right) \cup \overline{W^0}$; ne risulta

$$W^1 = W_d^0 = \{q_1\} \times X \cup \{q_2\} \times \{Parabola < 0\} \cup \{q_3\} \times \{Parabola < 0 \cup x_1 = 0\} \tag{9.12}$$

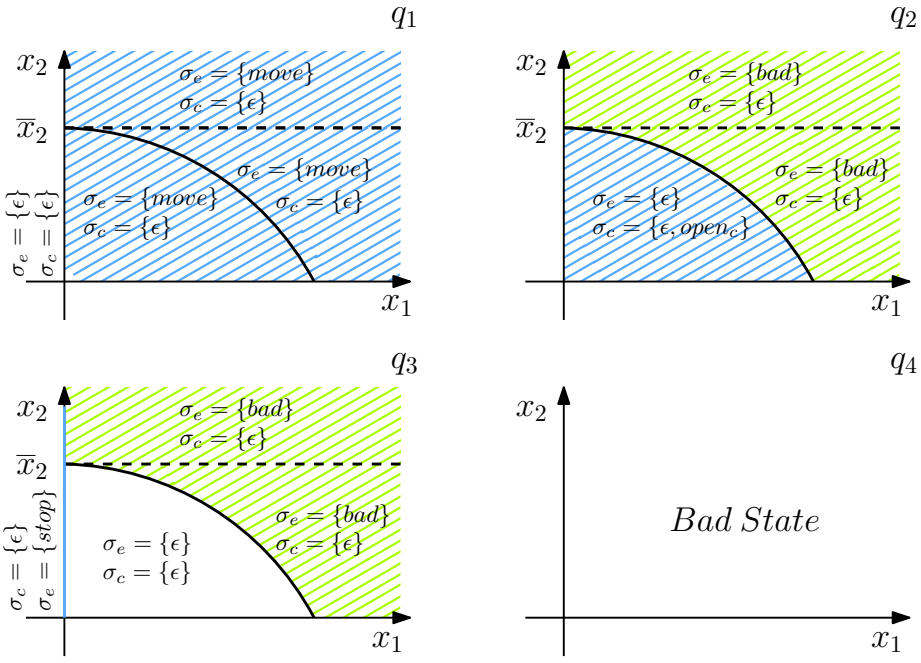

Figura 9.5: Fase per $i = 0$ caso coppia non desiderata a veicolo fermo

Partendo ora da W^1 si ricalcolano gli operatori. In precedenza in q_1 la

zona superiore la parabola veniva attribuita all'operatore Pre_c, poichè attivava una transizione appartenente a W^0. Adesso, avendo eliminato da W^0, con l'operatore Pre_e, la zona al di sopra della parabola in q_2, la stessa zona in q_1 non potrà più essere associata a Pre_c poichè ora attiva una transizione che ci porta in una regione di spazio di stato al di fuori di W^1. Per cui l'operatore Pre_e in questa fase risulta

$$Pre_e\left(W^1\right) = Pre_e\left(W^0\right) \cup \{q_1\} \times \{Parabola > 0\} \tag{9.13}$$

$Pre_e\left(W^1\right)$ è rappresentato in figura 9.6 sempre in verde. Di conseguenza ora $Pre_c\left(W^1\right)$ risulta identico a $Pre_c\left(W^0\right)$ senza la regione di spazio di stato al di sopra della parabola

$$Pre_c\left(W^1\right) = \{q_1, q_2\} \times \{Parabola < 0\} \cup \{q_3\} \times \{x_1 = 0\} \tag{9.14}$$

L'operatore $Unavoid\_Pre\left(B, E\right)$ è sempre identico all'insieme vuoto e sarà

$$W^2 = W_d^2 = \{q_1, q_2, q_3\} \times \{Parabola < 0\} \tag{9.15}$$

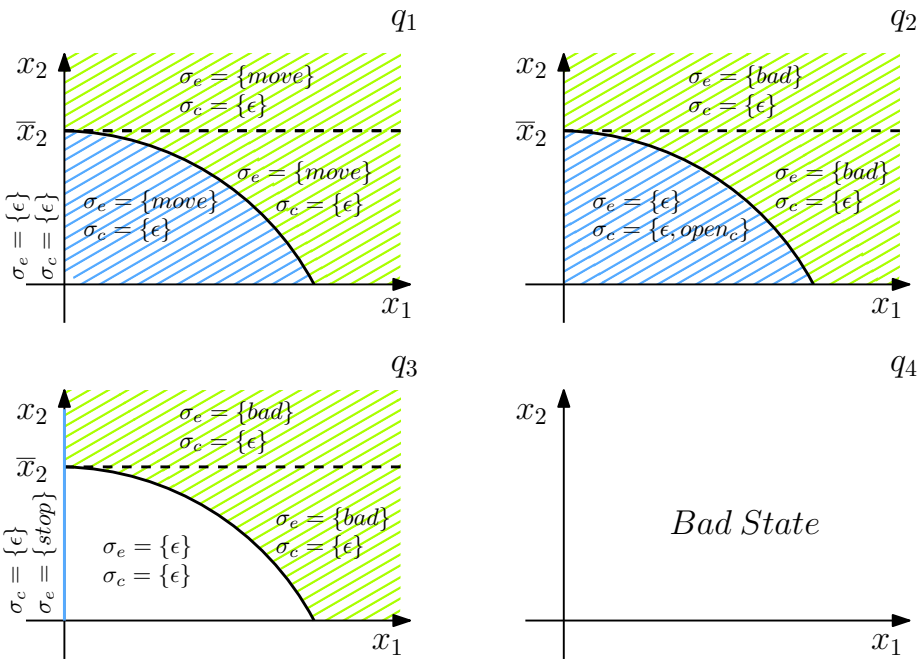

Figura 9.6: Fase per $i = 1$ caso coppia non desiderata a veicolo fermo

Nella terza iterazione dell'algoritmo, con $i = 2$, gli operatori hanno la stessa forma della fase precedente, ad eccezione dell'operatore Pre_c: infatti ora la transizione che viene attivata nello stato q_3 quando il veicolo si arresta deve essere confinata tra $x_2 \in [0, \bar{x}_2]$. Questo cambiamento però non porta ad eliminare alcuna altra regione dello spazio delle fasi, così che si arriva al punto fisso cercato. Ne risulta

$$Safe = W^3 = W^2 = \{q_1, q_3\} \times \{Parabola < 0 \cup x_1 = 0\} \cup \{q_2\} \times \{Parabola < 0\} \tag{9.16}$$

Partendo dal risultato appena trovato è possibile calcolare il controllore massimale che aziona il controllo dell'apertura dalla frizione sulla regione limite. Nel caso in studio, la dinamica $f(q_3, x)$ che genera la curva che delimita la regione $Safe$ è stata parametrizzata con la parabola

$$x_2 = -9.6090x_1^2 + 0.004x_1 + 0.15 \tag{9.17}$$

per cui il controllo attiverà il comando di apertura delle frizioni quando la coppia $(x_1, x_2) \in Parabola$. Nelle figure 9.7 e 9.8 sono rappresentate la dinamica continua e quella discreta dell'Automa ibrido con il controllore massimo sulla frontiera

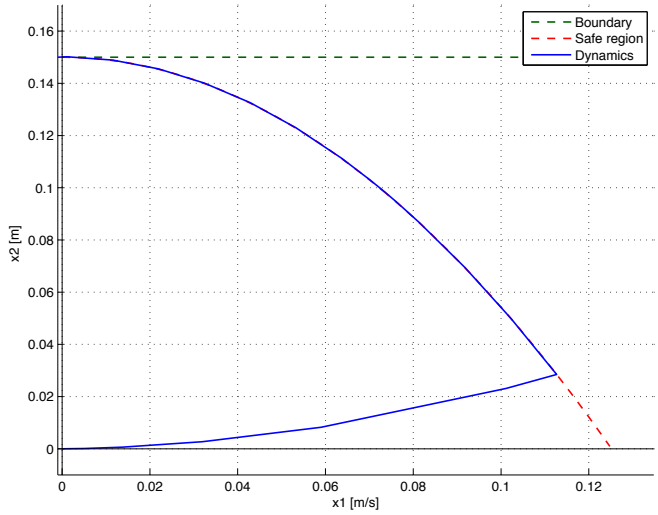

Figura 9.7: Dinamica continua con il controllore massimale

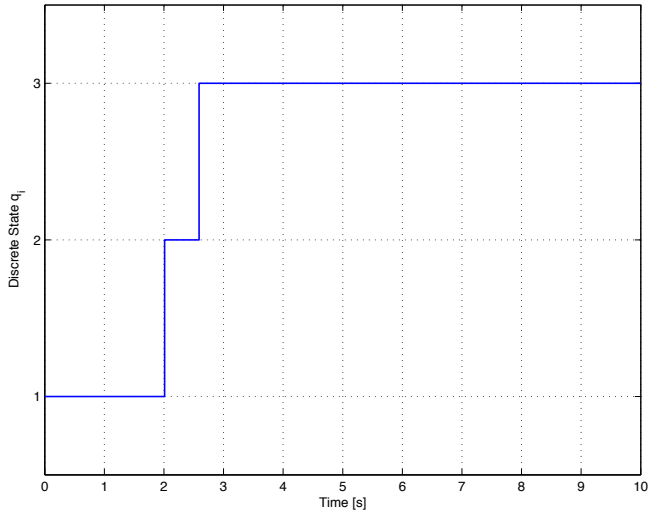

Figura 9.8: Dinamica discreta con il controllore massimale

Nel caso analizzato, il controllo invia il comando di apertura delle frizioni e queste vengono aperte istantaneamente generando la dinamica appena illustrata. Questo nella realtà non è può accadere, in quanto vi sarà un certo tempo di ritardo fra l'invio del comando e l'effettiva apertura delle frizioni: risulta quindi chiaro come, inviando un comando di apertura sulla soglia della regione Safe, la presenza del ritardo possa portare la dinamica continua a superare la regione sicura andando a violare il requisito imposto sullo spostamento del veicolo.

Questo nuovo vincolo porta all'introduzione di una ulteriore regione nello spazio di stato, definita *regione di ritardo di attivazione*: tale regione delimita lo spazio di stato massimo, all'interno del quale il comando di apertura delle frizioni deve essere attivato, in modo da mantenere la dinamica continua dell'automa ibrido all'interno della regione Safe. In figura 9.9 sono mostrate le regioni di stato limite per l'attivazione del controllo, al variare del tempo di ritardo. Dal grafico si nota come, aumentando il tempo di ritardo, il controllo abbia sempre meno spazio di stato su cui poter agire.

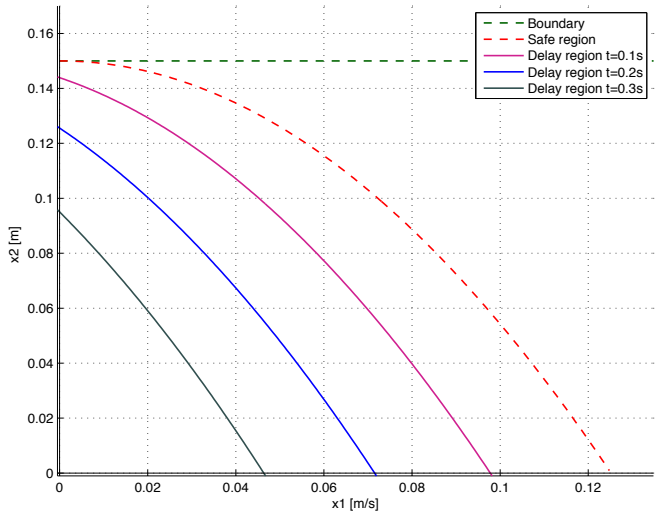

Figura 9.9: Andamenti delle regioni di stato per l'attivazione del controllo, al variare del tempo di ritardo

Nel modello esposto il tempo di ritardo è stato fissato a $0.125s$. L'introduzione del ritardo porta ad una variazione della regione Safe: sarà infatti presente una nuova delimitazione sullo spazio di stato, costituita dalla curva tratteggiata

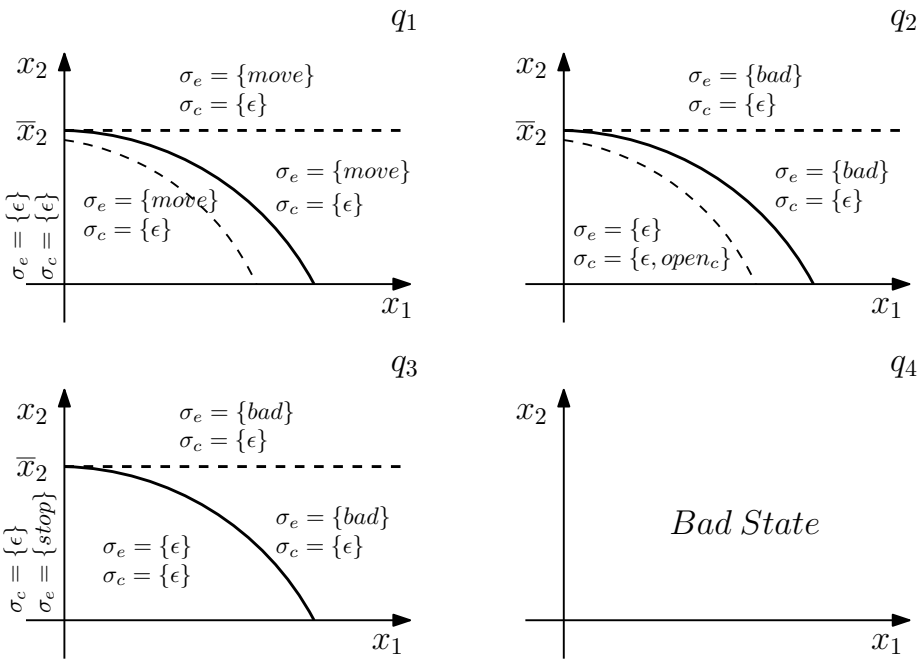

Figura 9.10: Spazio di stato continuo in ogni stato discreto q_i caso con ritardo

Un'attivazione del controllo nello spazio fra le due curve non porterebbe al rispetto del requisito imposto sullo spostamento

Procedendo con la prima fase dell'algoritmo, per $i = 0$ si avrà sempre W^0 come esposto nella formula 9.9, così come l'operatore $Pre_e\left(W^0\right)$. Gli operatori Pre_c e $Unavoid\_Pre$ risulteranno invece diversi dal caso precedente

$$Pre_c\left(W^0\right) = \{q_1\} \times X \cup \{q_2\} \times \{Parabola_{ritardo} < 0\} \cup \{q_3\} \times \{x_1 = 0\} \tag{9.18}$$

$$Unavoid\_Pre\left(B, E\right) = \{q_2\} \times \{Parabola_{ritardo} > 0 \wedge Parabola < 0\} \tag{9.19}$$

In figura 9.11, in viola, viene rappresentato l'operatore $Unavoid\_Pre$: stavolta tale operatore risulta non vuoto, in quanto nella zona viola vi sarà un disturbo continuo tale che, per qualsiasi azione di controllo continuo, porti l'evoluzione a rimanere confinata nello stato q_2 fino ad un tempo $\bar{t}$, nel quale l'evoluzione apparterà alla zona $Pre_e\left(W^0\right)$

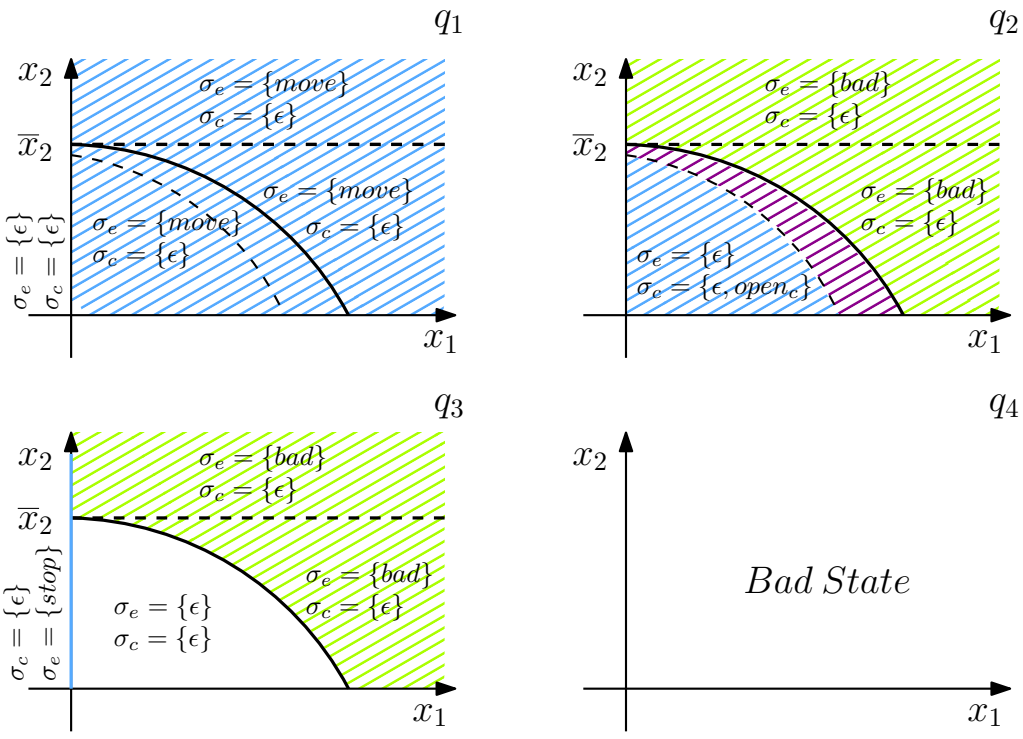

Figura 9.11: Fase per $i = 0$ caso coppia non desiderata a veicolo fermo con ritardo

$$W_d^0 = \{q_1\} \times X \cup \{q_2, q_3\} \times \{Parabola < 0\} \tag{9.20}$$

$$W^1 = W_d^0 \setminus Unavoid\_Pre\,(B, E) = \{q_1\} \times X \cup \{q_2\} \times \{Parabola_{ritardo} < 0\} \cup \{q_3\} \times \{Parabola < 0\} \tag{9.21}$$

Nella seconda fase dell'algoritmo, per $i = 1$, come visto in precedenza l'operatore Pre_e subirà una variazione. Avendo eliminato da W^1 una regione di piano in q_2 rispetto a W^0, ora l'operatore Pre_e avrà la forma

$$Pre_e\left(W^1\right) = \{q_1\} \times \{Parabola_{ritardo} > 0 \setminus x_1 = 0\} \cup \{q_2\} \times \{Parabola > 0\} \cup \{q_3\} \times \{Parabola > 0\} \tag{9.22}$$

anche l'operatore Pre_c varierà rispetto alla fase precedente diventando

$$Pre_c\left(W^1\right) = \{q_1\} \times \{Parabola_{ritardo} < 0\} \cup \{q_2\} \times \{Parabola_{ritardo} < 0\} \cup \{q_3\} \times \{x_1 = 0\} \tag{9.23}$$

l'operatore $Unavoid\_Pre$ rimane invece invariato. La rappresentazione degli operatori sarà quindi

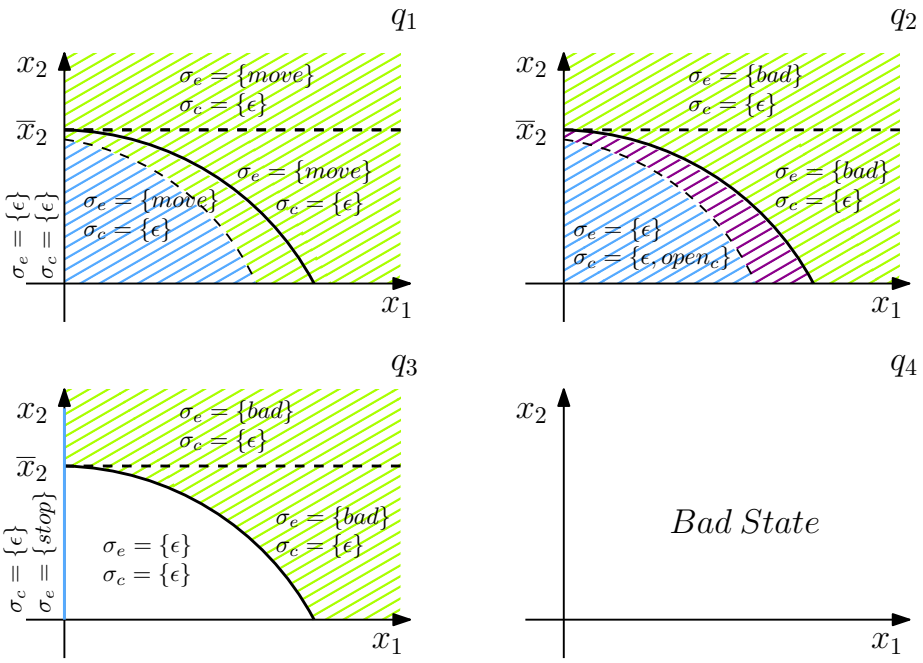

Figura 9.12: Fase per $i = 1$ caso coppia non desiderata a veicolo fermo con ritardo

Da qui sarà

$$W^2 = W_d^1 \setminus Unavoid\_Pre\,(B.E) = \{q_1\} \times \{Parabola_{ritardo} < 0 \cup x_1 = 0\} \cup \{q_2\} \times \{Parabola_{ritardo} < 0\} \cup \{q_3\} \times \{Parabola < 0 \cup x_1 = 0\} \quad (9.24)$$

Anche stavolta si raggiunge il punto fisso nella terza fase, terminando l'algoritmo con il risultato

$$Safe = W^3 = W^2 = \{q_1\} \times \{Parabola_{ritardo} < 0 \cup x_1 = 0\} \cup \{q_2\} \times \{Parabola_{ritardo} < 0\} \cup \{q_3\} \times \{Parabola < 0 \cup x_1 = 0\} \quad (9.25)$$

Procedendo alla simulazione del modello illustrato nel capitolo 4, in figura 9.13 è illustrata la dinamica dello stato nello spazio delle fasi

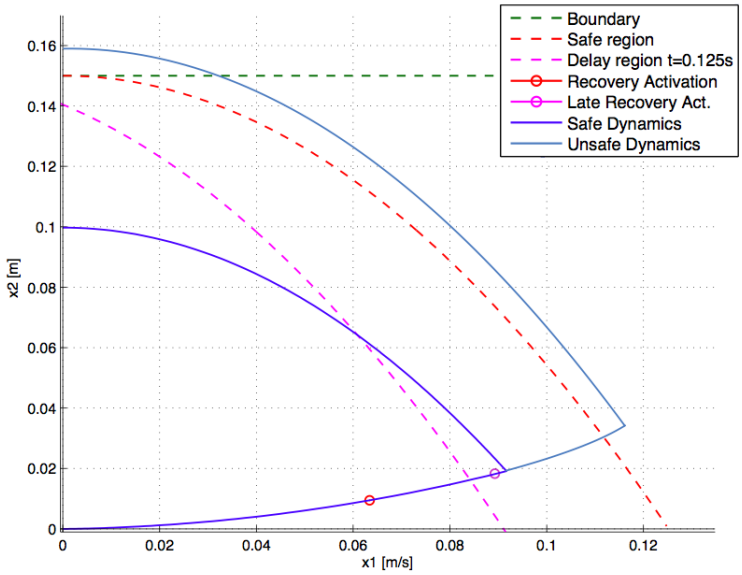

Figura 9.13: Dinamiche continue, al variare dell'instante di apertura frizioni

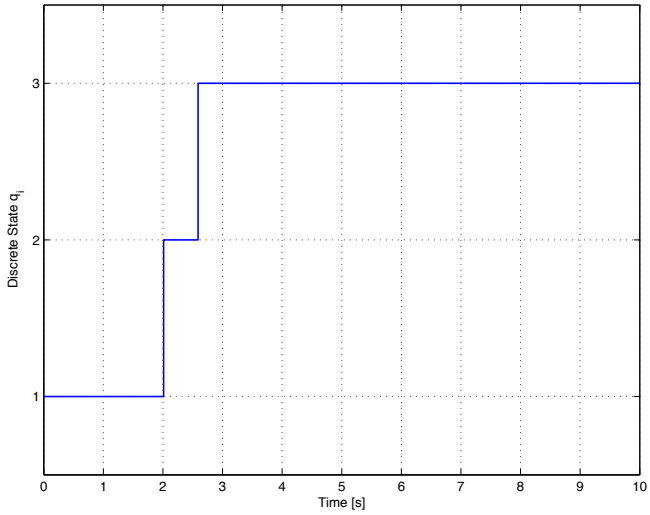

Figura 9.14: Dinamica discreta con il controllore sviluppato

Si può osservare come, in figura 9.13, l'attivazione del controllo (rappresentata da un cerchio rosso) all'interno della zona che delimita la regione del ritardo di attivazione porti al rispetto del requisito di sicurezza (la dinamica del sistema rimane quindi completamente confinata nella regione Safe); l'attivazione del controllo oltre la zona limite, invece, porta al mancato rispetto del requisito di sicurezza.

9.4 Assenza di coppia dalla macchina elettrica

Il malfunzionamento in esame provoca un brusco calo di prestazioni, che durante un sorpasso può causare un pericolo enorme per il guidatore. La manovra che più di tutte può causare una situazione di pericolo, nel caso di questo malfunzionamento, è il sorpasso su strada extraurbana, dove per superare bisogna invadere la corsia opposta in cui sono in transito veicoli con un senso di marcia opposto. Si può schematizzare la manovra attraverso la figura 9.15

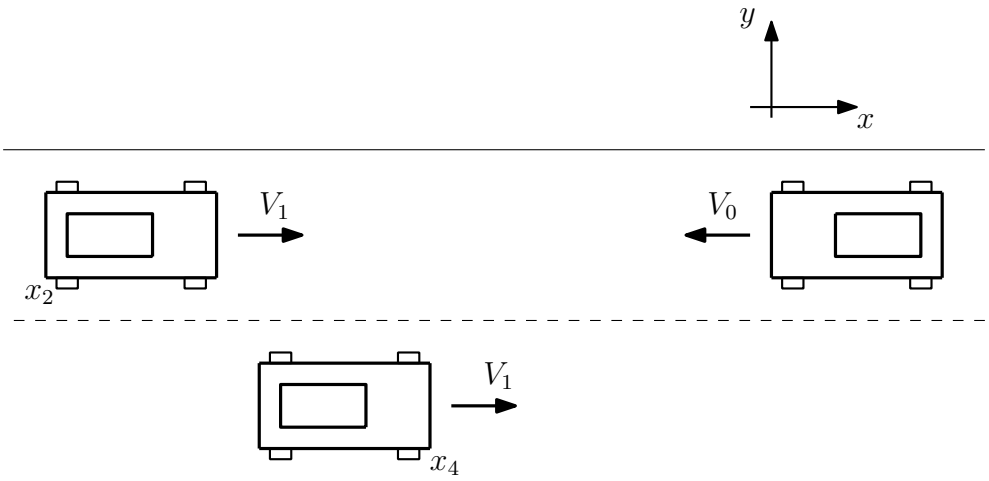

Figura 9.15: Manovra di sorpasso

nella figura sono presenti tre vetture: la prima a sinistra è la vettura che sta effettuando il sorpasso, con una velocità iniziale $V_1 = 12.5^{\mathrm{m}}/_{\mathrm{s}}$, la seconda è la macchina da sorpassare che viaggia sempre ad una velocità costante di V_1, mentre l'ultima macchina è quella proveniente dal senso opposto che viaggia anche lei ad una velocità costante $V_0 = 11.11^{\mathrm{m}}/_{\mathrm{s}}$. Con le variabili continue x_2 e x_4 si rappresentano le posizioni, rispettivamente del posteriore della macchina di sinistra e dell'anteriore della macchina centrale, che assumiamo rispetto la macchina che arriva dal senso opposto, per cui il sistema di riferimento è in movimento e solidale con la vettura di destra. L'autovettura di sinistra quindi dovrà superare la vettura di mezzo (questo accadrà quando $x_2 > x_4$) e rientrare nella propria corsia prima che si scontri con la vettura di destra che arriva dal senso opposto (lo scontro avverrà quando $x_2 \geq 0$). Un altra specifica per il sorpasso è data dalla posizione della macchina centrale, infatti la x_4 non potrà diventare positiva (indicando che la macchina centrale e la macchina di destra

sono in linea) se $x_2 < 0$ altrimenti la vettura di sinistra non potrà ritornare nella propria corsia. Tutte queste condizioni dovranno portare l'evoluzione dell'Automa nel *Bad State*, altrimenti il sorpasso sarà avvenuto con successo.

Attraverso questa analisi l'Automa ibrido risultante è il seguente

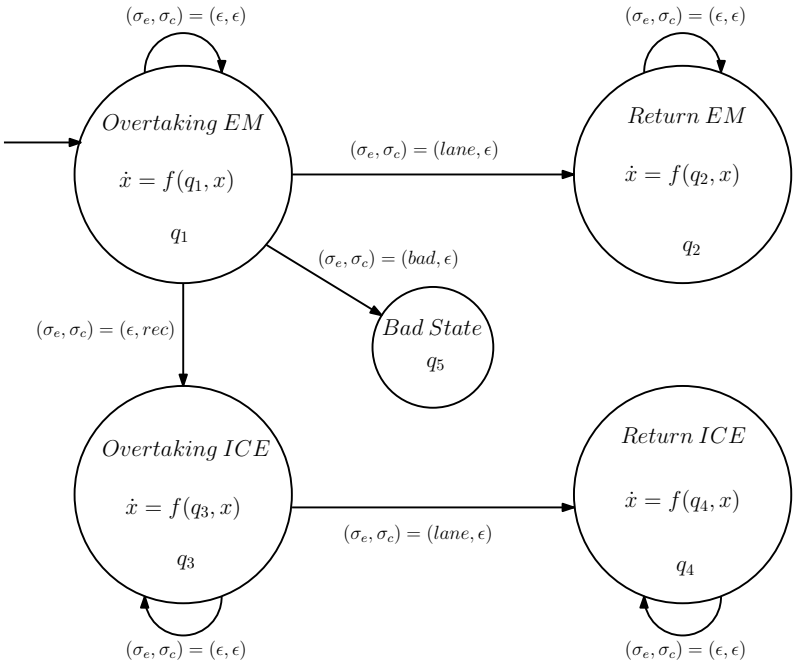

Figura 9.16: Rappresentazione Automa ibrido in caso di coppia inferiore o nulla a quella richiesta

Per eliminare la problematica del sistema di riferimento mobile si attua uno stratagemma, si suppone la macchina di destra ferma e si somma la sua velocità di crociera alle restanti due vetture tale che come velocità iniziale della vettura di sinistra si ha $V_0 + V_1 = 23.61^{\mathrm{m}}/_{\mathrm{s}}$ e la stessa velocità (questa volta costante di crociera) per la macchina centrale.

Per l'analisi di questo caso si attuano delle ipotesi di contorno sulla manovra, cosi da delimitare lo spazio di stato continuo e definire una regione chiusa su cui applicare l'algoritmo del Safe set. La prima ipotesi viene fatta sulla marcia inserita per il sorpasso: durante tutto il sorpasso viene mantenuta la terza marcia. Mentre lo spazio di stato viene delimitato attraverso delle restrizioni sulla manovra, infatti si è scelto di analizzare manovre di sorpasso in cui la macchina di sinistra ha una distanza massima dalla macchina che sta venendo nel senso opposto di $2000m$, mentre tra la macchina che compie il

sorpasso e quella che viene sorpassata la distanza massima può essere di $450m$. Altra ipotesi è data dalle velocità della macchina che sorpassa, questa è l'unica velocità che varia nel tempo e può variare da un minimo $0^{\mathrm{m}}/_{\mathrm{s}}$ (caso partenza sorpasso con velocità nulla) a un massimo dato dalla velocità di saturazione in terza marcia. Attuando queste ipotesi si ha una regione delimitata.
L'Automa ibrido rappresentato, secondo la nomenclatura usata, sarà la collezione $H = \left((Q, X), (\Sigma_c, U), \left(M_c^{disc}, M_c^{cts}\right), (\Sigma_e, D), \left(M_e^{disc}, M_e^{cts}\right), (\delta, f)\right)$ dove

- $Q = \{q_1, q_2, q_3, q_4, q_5\}$;
- $X = [0, 450] \times [0, 2000] \times [11.11, 60]$;
- $\Sigma_c = \{rec\}$, $\Sigma_c^\epsilon = \Sigma_c \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_c^{disc} : Q \times X \to 2^{\Sigma_c^\epsilon} \setminus \{\}$;
- $U \in [0, 240]\mathrm{Nm}$, $\mathcal{U} = \{u(\cdot) \in PC^0 \mid u(t) \in U, \forall t\}$, $M_c^{cts} : Q \times X \to 2^U \setminus \{\}$;
- $\Sigma_e = \{lane, bad\}$, $\Sigma_e^\epsilon = \Sigma_e \cup \{\epsilon\}$ dove ϵ è il silent mode, $M_e^{disc} : Q \times X \to 2^{\Sigma_e^\epsilon} \setminus \{\}$;
- $D \in [-52, 0]\mathrm{Nm}$, $\mathcal{D} = \{d(\cdot) \in PC^0 \mid d(t) \in U, \forall t\}$, $M_e^{cts} : Q \times X \to 2^D \setminus \{\}$;
- $\delta : Q \times X \times \Sigma_c^\epsilon \times \Sigma_e^\epsilon \to 2^{Q \times X} \setminus \{\}$ sono le transizioni discrete tra uno stato ed un altro, $\delta(q, x, \sigma_c, \sigma_e) = W \subseteq Q \times X$, $\delta(q, x, \epsilon, \epsilon) = \{(q, x)\}$;
- $f : Q \times X \times U \times D \to \mathbb{R}^n$ definisce il flusso continuo, $\dot{x}(t) = f_q(x(t), u(t), d(t))$ con $x(t_0) = x_0$.

Le variabili continue x_2 e x_4 dell'Automa ibrido sono le posizioni delle autovetture a sinistra e nel centro, mentre le altre due variabili x_1 e x_3 sono le velocità rispettivamente della macchina che compie il sorpasso e della macchina sorpassata. Da ipotesi l'auto che viene sorpassata va ad una velocità costante per cui $x_3 = V_1$ e $\dot{x}_3 = 0$, mentre la velocità della prima vettura è descritta dall'equazione 5.7, in cui $sign(\overline{\varsigma}(u_1 + u_2)) = 1$ perché ci si muove in avanti. Negli stati q_1 e q_2 è attivo il solo motore elettrico per cui $u_2 = 0$, al contrario negli stati q_3 e q_4 è attivo il solo motore termico cosicché $u_1 = 0$ e

non sono presenti disturbi (essendo i disturbi modellati dovuti dall'inverter e dalla macchina elettrica che nello stato q_3 e q_4 sono bypassati dal controllo).

Il flusso continuo per i vari stati è il seguente

$$f(q_1, x) = \begin{bmatrix} -0.001 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ d_1 \\ d_2 \end{bmatrix} - \begin{bmatrix} \frac{1}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} F_\mu - \begin{bmatrix} \frac{\gamma}{M} x_1^2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{9.26}$$

$$f(q_2, x) = \begin{bmatrix} -0.001 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} & \frac{\bar{\varsigma}}{M} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ d_1 \\ d_2 \end{bmatrix} - \begin{bmatrix} \frac{1}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} F_\mu - \begin{bmatrix} \frac{\gamma}{M} x_1^2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{9.27}$$

$$f(q_3, x) = \begin{bmatrix} -0.001 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} u_2 - \begin{bmatrix} \frac{1}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} F_\mu - \begin{bmatrix} \frac{\gamma}{M} x_1^2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{9.28}$$

$$f(q_4, x) = \begin{bmatrix} -0.001 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} \frac{\bar{\varsigma}}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} u_2 - \begin{bmatrix} \frac{1}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix} F_\mu - \begin{bmatrix} \frac{\gamma}{M} x_1^2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{9.29}$$

mentre le condizioni iniziali dell'Automa ibrido sono dati da

$$x_1(0) = V_0 + V_1 \tag{9.30}$$

$$x_2(0) = x_{20} \tag{9.31}$$

$$x_3(0) = V_0 + V_1 \tag{9.32}$$

$$x_4(0) = x_{40} \tag{9.33}$$

Si passa ad analizzare gli ingressi discreti. Il controllo ha sempre una sola possibilità (oltre al silent mode) $\Sigma_c = \{rec\}$, quindi la diagnostica e la recovery attuano il comando rec forzando la vettura ibrida a procedere in modalità pu-

ramente termica spegnendo il motore elettrico fonte del guasto. Al contrario il disturbo discreto, che nella aiuta a modellare anche le condizioni di transizione sulle variabili continue, avrà i seguenti segnali $\Sigma_e = \{lane, bad\}$ che saranno attivati quando

Lane = se la $x_2 > x_4$,ma sarà ancora $x_2 < 0$, allora il sorpasso sarà andato a buon fine senza pericoli ed è possibile rientrare nella propria corsia. Oppure se la distanza dalla macchina che viene dal senso opposto sarà minore di $l_m + \lambda$, dove con l_m è indicata la lunghezza della vettura e con λ una distanza di sicurezza minima, si dovrà rientrare obbligatoriamente per evitare lo scontro frontale;

Bad = se il sorpasso non avviene, per cui se $x_4 > 0$ e $x_2 < 0$, oppure nello stato di rientro se $x_2 < x_4$ per cui si avrà una collisione durante il rientro in corsia.

Nell'esempio la lunghezza della macchina l_m è stata posta pari a $3.5m$, mentre la distanza di sicurezza minima λ è di $2m$.

Una volta definite tutte le ipotesi e i vincoli, si devono delimitare tutte le varie regioni di spazio di stato nel cubo scelto. Le variabili che definiscono il cubo sono:

- Sull'asse X si avrà la distanza tra la vettura che attua il sorpasso e la vettura che viene sorpassata, cioè $x_4 - x_2$;
- Sull'asse Y si avrà la distanza tra la vettura che sta effettuando il sorpasso e la vettura che sta arrivando dal senso di marcia opposto, cioè x_2;
- Sull'asse Z si avrà la velocità delle due vetture in $^{m}/_{s}$.

Dalle ipotesi fatte, il sorpasso limite è quello secondo il quale la macchina che sta sorpassando riesce a completare la manovra rientrando nella propria corsia esattamente alla distanza limite con la macchina che arriva dal senso di marcia opposto, cioè $l_m + \lambda$. La velocità di fine sorpasso si suppone sia compresa tra la velocità della macchina da sorpassare (è ragionevole pensare che per superare una vettura si debba avere almeno una velocità pari a questa) e la velocità massima attuabile. Per cui è possibile integrale all'indietro le equazioni differenziali del sistema partendo da queste condizioni limite trovando così

tutte le traiettorie massime possibili per effettuare il sorpasso sia in caso di modalità puramente elettrica che termica.

Essendo le traiettorie massime, queste sono state generate supponendo che i due motori forniscano la massima coppia possibile ai giri motore attuali, secondo gli andamenti esposti in figura 4.7 a pagina 38 e in figura **??** a pagina ??.

Avendo posto come ipotesi la marcia fissa durante il sorpasso, si avrà una velocità di saturazione per il veicolo che effettua il sorpasso, cioè si avrà che $\dot{x}_1 = 0$. Questo accade quando il carico e la forza di trazione del veicolo sono uguali infatti

$$\dot{x}_1 = -\frac{\gamma}{M}x^2 + \frac{\overline{\varsigma}}{M}u_{max} - \frac{1}{M}F_\mu = 0 \tag{9.34}$$

da cui

$$x_{1_{max}} = \sqrt{\frac{\overline{\varsigma}u_{max} - F_\mu}{\gamma}} \tag{9.35}$$

Tutte queste analisi portano a definire, sia nel caso di trazione puramente elettrica che nel caso puramente termico, delle superfici che danno il limite secondo il quale si può o non si può compiere il sorpasso. Nel caso puramente elettrico la superficie risultante sarà:

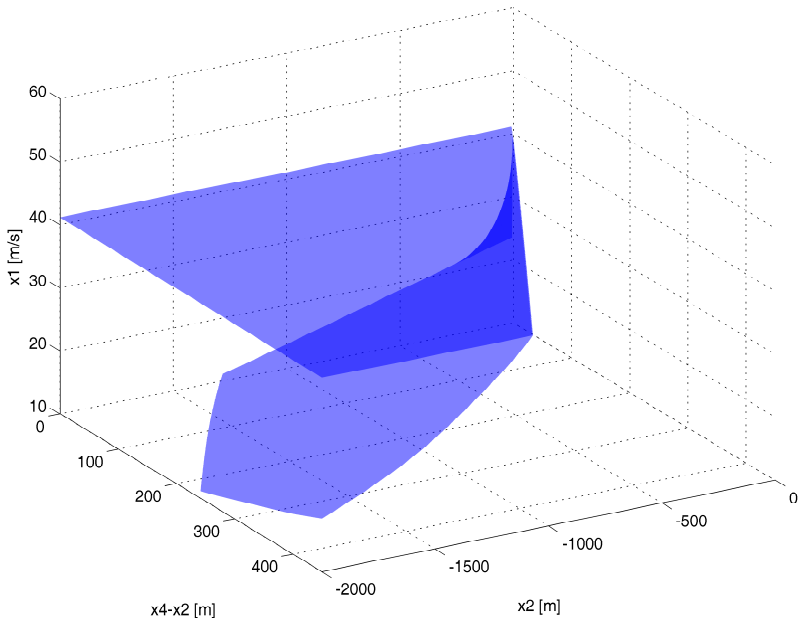

Figura 9.17: Superficie delimitante il sorpasso massimo utilizzando il solo motore elettrico

nel caso puramente termico invece avrà la seguente forma

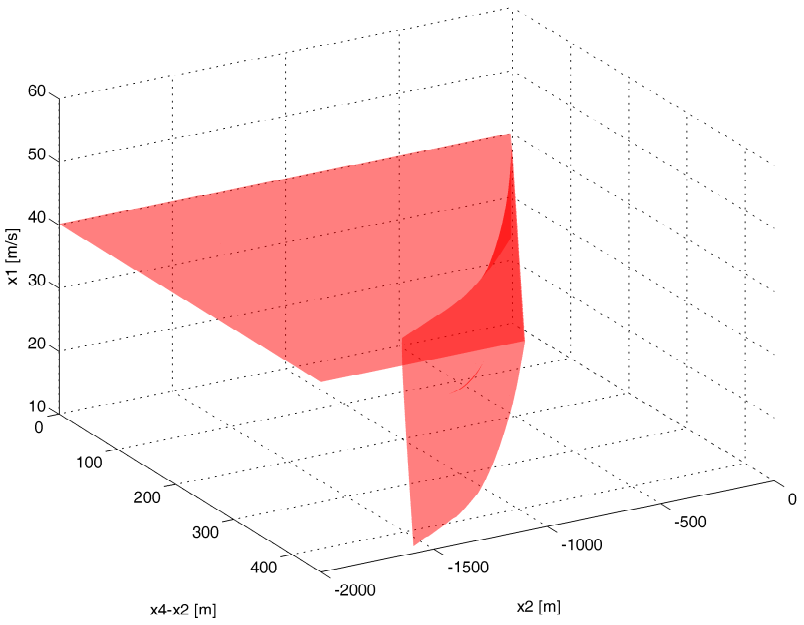

Figura 9.18: Superficie delimitante il sorpasso massimo utilizzando il solo motore termico

Si noti che la velocità massima che si raggiunge con il motore elettrico sia leggermente maggiore a quella possibile nella solo modalità termica, questo perché la saturazione della coppia massima erogabile dal motore termico avviene a giri più bassi rispetto all'elettrico. Ma le superfici rispecchiano anche la potenza dei due motori, infatti con l'elettrico è possibile iniziare il sorpasso da fermi solo se si è ad una elevata distanza dal veicolo che arriva dal senso opposto, poiché il motore elettrico ha una dinamica più lenta e una coppia massima erogabile minore rispetto al motore termico.

Per cui, se l'evoluzione continua dell'automa ibrido rimane all'interno di queste superfici, a seconda se si è in termico o in elettrico, il sorpasso avverrà sicuramente.

Una volta definite le superfici massimali, si può procedere con l'algoritmo per trovare il Safe set. Lo spazio di stato completo delle due superfici e delle azioni del disturbo e del controllo sono le seguenti

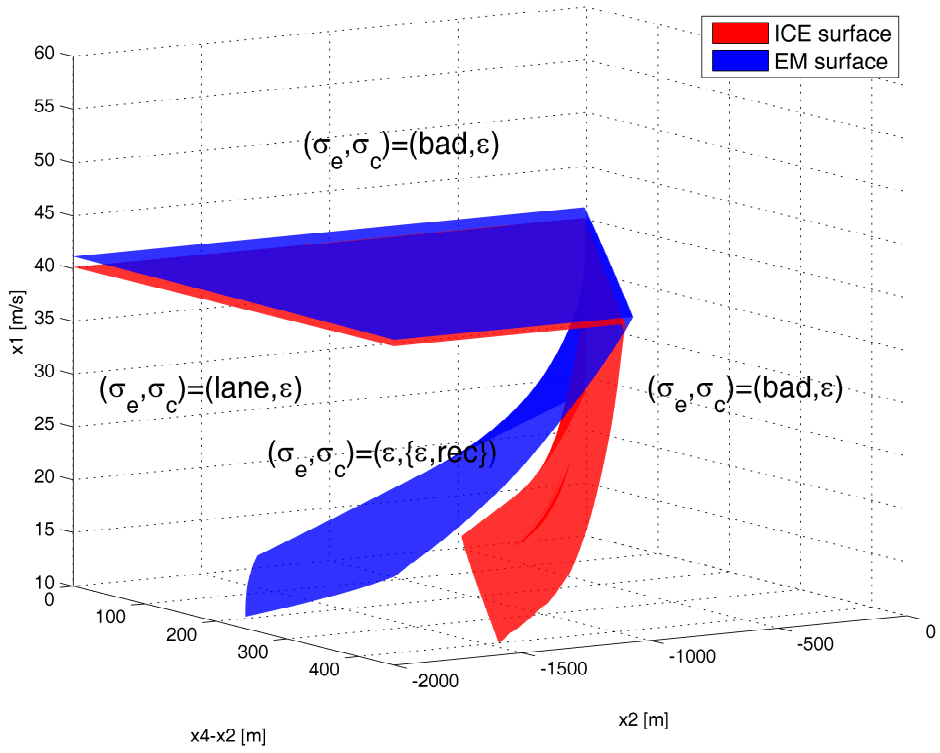

Figura 9.19: Spazio di stato continuo e descrizione azioni di controllo e disturbo

Come si nota dalla figura 9.19 la modalità *rec* può essere attivata solamente

quando l'evoluzione è all'interno della superficie rossa. Il sorpasso avviene, per cui si attiva la transizione *lane*, quando l'evoluzione continua tocca il piano YZ con $X = 0$. Al di fuori delle due superfici, sia rossa che blu, non ci sarà nessuna coppia fornita dal termico o dall'elettrico che permette di effettuare il sorpasso, per cui se l'evoluzione cade in quella zona di spazio di stato l'Automa ibrido andrà a finire nello stato *Bad*.

Prima fase $i = 0$

Si procede con il primo step dell'algoritmo. L'insieme W^0 sarà

$$W^0 = \{q_1, q_2, q_3, q_4\} \times X \tag{9.36}$$

Il primo passo dell'algoritmo porta a calcolare l'operatore $Pre_e\,(W^0)$. Questo operatore definisce lo spazio di stato nel quale per qualsiasi controllo esiste un disturbo, tale che la coppia sia diversa da $\{\epsilon, \epsilon\}$,che attivi una transizione che porta l'evoluzione dell'Automa ibrido in uno spazio non contenuto in W^i. Questo rappresenta tutto lo spazio di stato al di fuori delle due superfici, nello specifico al di fuori della superficie rossa per la parte in basso e al di fuori della superficie blu nella parte in alto.

Per cui la $W_d^0 = W^0 \setminus Pre_e\,(W^0)$. L'operatore $Pre_c\,(W^0)$ rappresenta lo spazio di stato in cui esiste un controllo tale che per qualsiasi disturbo, con la coppia diversa da $\{\epsilon, \epsilon\}$, si attivi una transizione che porta l'evoluzione dell'Automa in uno spazio contenuto in W^i. In questo caso l'operatore viene rappresentato da tutta la zona all'interno della superficie rossa, dove può essere attivata la recovery.

L'operatore $Unavoid\_Pre\,(B, E)$ rappresenta lo spazio di stato in cui l'evoluzione continua, affetta da un disturbo continuo, partendo da un punto all'interno di W^i viene portata in $\overline{W^i}$. Nel caso in esame è presente una zona di spazio di stato nella quale l'evoluzione, affetta da disturbo, evolve fino a raggiungere $\overline{W^0}$. Questa è rappresentata dalla zona in cui si incrociano le due superfici nello spigolo, nel quale la superficie blu supera la superficie rossa, per cui non può essere attivata la recovery, ma si è ancora all'interno della superficie blu, cosicché se non fosse presente il disturbo con una coppia massima del motore elettrico il sorpasso potrebbe avvenire. Ma essendo presente questo

disturbo, il motore elettrico non può fornire la coppia massima desiderata e l'evoluzione uscirà dalla zona W^0 andando a raggiungere $\overline{W^0}$.

Si mostrano i vari operatori nella figura 9.20. In verde è rappresentato Pre_e, in azzurro Pre_c e in viola $Unavoid\_Pre$

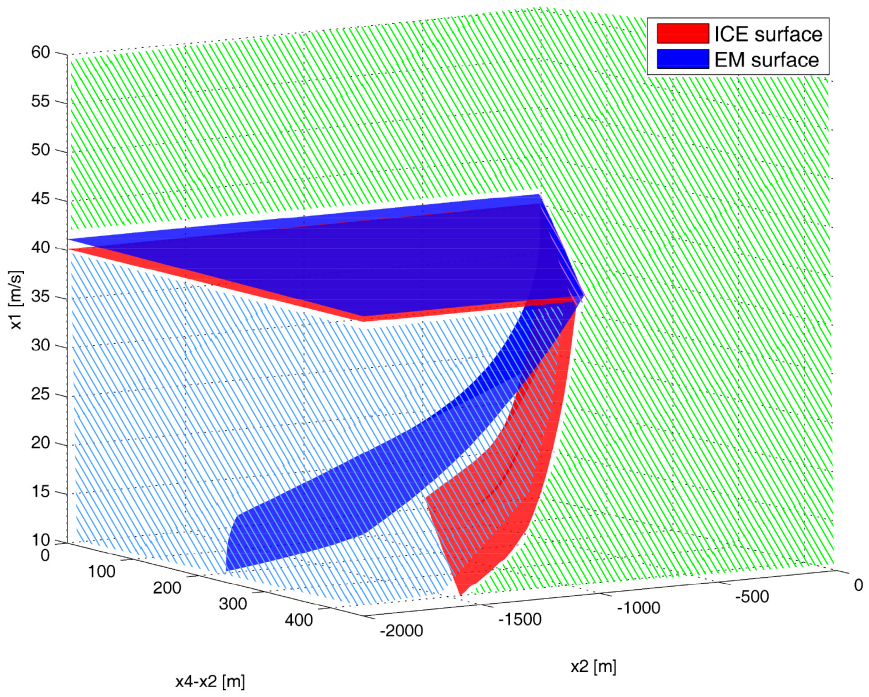

Figura 9.20: Descrizione operatori Pre_e, Pre_c e $Unavoid\_Pre$

Da qui si può definire la W^1 come la regione di spazio di stato

$$W^1 = W_d^0 \setminus Unavoid\_Pre\,(B, E) \tag{9.37}$$

cioè la zona all'interno della superficie rossa, tra la superficie rossa e quella blu in alto escludendo la zona nello spigolo in cui si intersecano le superfici.

Seconda fase $i = 1$

Iterando di nuovo l'algoritmo gli operatori Pre_e, Pre_c e $Unavoid\_Pre$ rimangono immutati rispetto la fase precedente per cui

$$W^2 = W^1 \tag{9.38}$$

raggiungendo il punto fisso cercato.

Si mostrano ora in figura 9.21 e 9.22 le tracce dei piani sulle varie facce del cubo dello spazio di stato per una migliore lettura del Safe set.

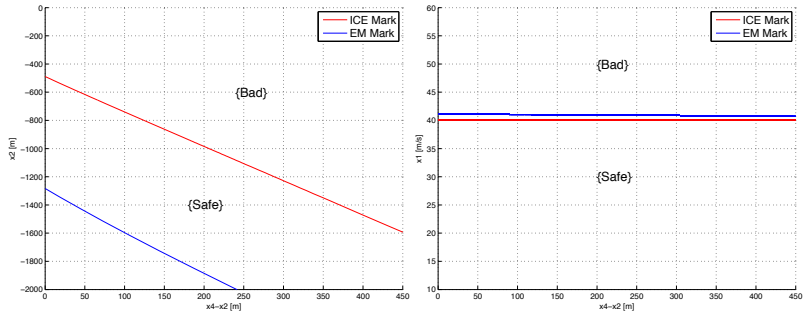

Figura 9.21: Traccia piani XY e XZ

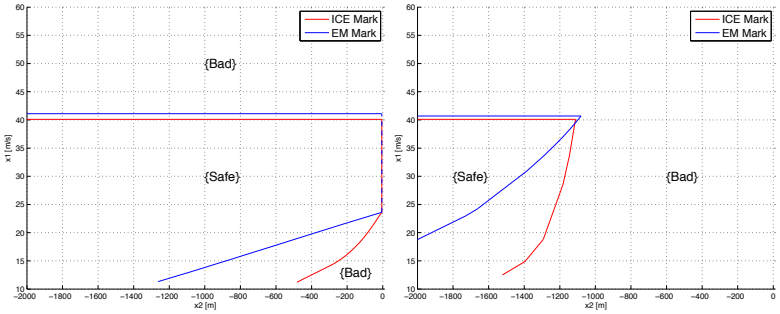

Figura 9.22: Traccia piani YZ per $X = 0$ e per $X = 450m$

Nelle figure sono state evidenziate le zone $Safe$ e le zone Bad. Nella traccia del piano YZ per $X = 450$ è facile notare il triangolo di zona $Unavoid\_Pre$.

Vengono infine presentati i risultati di simulazione, con e senza l'azione della recovery, per mostrare che il controllo rispetta la regione del Safe set trovata con l'algoritmo. Le dinamiche della simulazione sono le stesse esposte nell'argomentazione appena svolta:

- Velocità iniziale $V_1 = 12.5^{\mathrm{m}}/_{\mathrm{s}}$ per la vettura che sta sorpassando e quella che viene sorpassata (che mantiene questa velocità);
- Velocità costante di $V_0 = 11.11^{\mathrm{m}}/_{\mathrm{s}}$ per la vettura che viaggia nella corsia opposta;

- Il veicolo che sorpassa parte da una distanza $x_2 = -700m$ dal riferimento, mentre la macchina da superare è ad una distanza di $x_4 = -600m$ dal riferimento quindi $x_4 - x_2 = 100m$;
- Il disturbo viene innestato nei primi secondi di simulazione durante l'inizio della manovra di sorpasso, generando un guasto di coppia inferiore alla richiesta del guidatore.

In figura 9.23 viene mostrato l'andamento delle simulazioni, con la curva tratteggiata è descritto il caso senza recovery, mentre la linea continua rappresenta l'andamento in caso di recovery. Come si nota nel caso senza recovery, la traiettoria esce dalla zona $Safe$, infatti il sorpasso non viene compiuto provocando la collisione durante il rientro forzato in corsia. Nel caso con recovery, il guasto viene individuato e la recovery forza il passaggio alla modalità puramente termica che permette di completare la manovra di sorpasso, non uscendo dalla regione $Safe$.

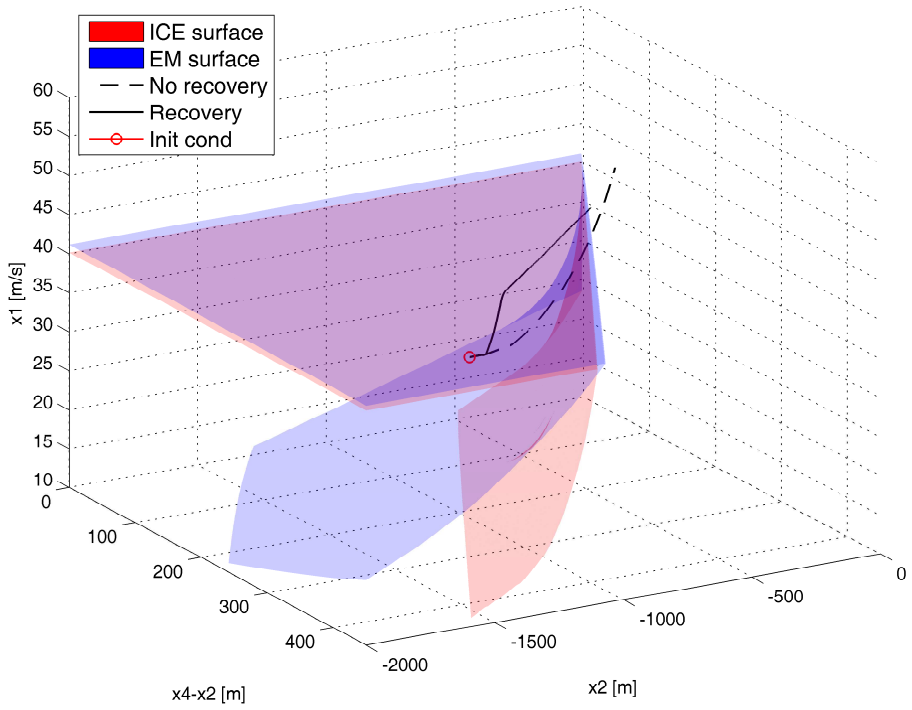

Figura 9.23: Simulazione con e senza recovery della manovra di sorpasso

E' utile porre una visione dall'alto sul piano XY della stessa immagine cosi da poter osservare meglio come la traiettoria tratteggiata nel caso senza recovery

esca fuori dal Safe set, al contrario della traiettoria in cui è attiva la recovery che rimane sempre nel Safe set raggiungendo il piano YZ per $X = 0$ completando il sorpasso. Da questa angolazione è facile anche vedere il momento dell'attivazione della recovery che spegne il motore elettrico e attiva il motore termico.

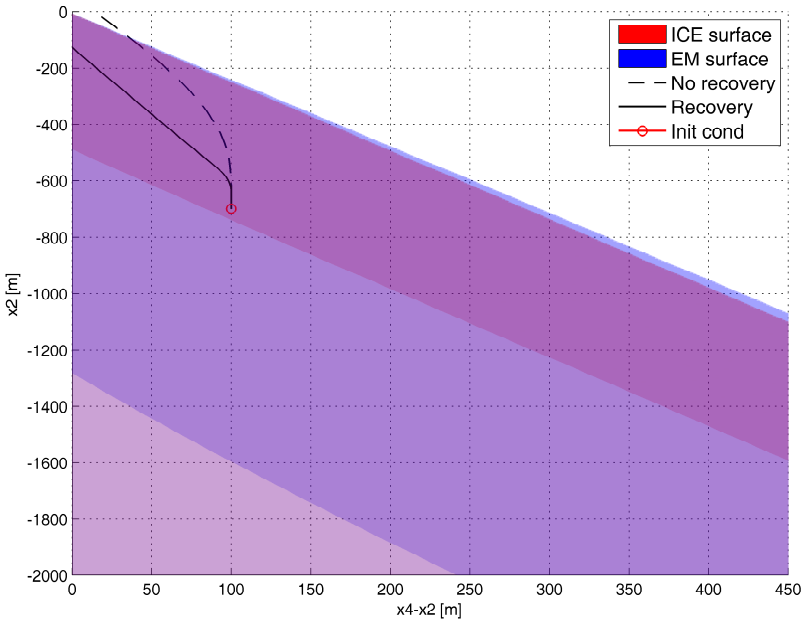

Figura 9.24: Vista dall'alto del Safe set con relativa simulazione

Si può notare che l'attivazione del controllo avviene all'interno dello spazio di stato racchiuso dalla superficie rossa, rispettando le specifiche.

Conclusioni

A colclusione del lavoro di tesi, si riassumono brevemente gli argomenti trattati

- è stato implementato un innovativo strumento di gestione ed applicazione della normativa ISO26262, che assista l'utente e permetta di automattizzare tutte le varie fasi,
- è stata applicata la teoria degli automi ibridi al caso di studio della normativa ISO26262, e per mezzo della teoria del controllore massimale è stata effettuata una validazione degli obiettivi di sicurezza imposti

Un possibile sviluppo futuro è rappresentato dall'integrazione degli strumenti di verifica formale nel software di gestione della normativa, in modo che anche il processo di validazione dei requisiti di sicurezza sia automatizzato.

Bibliografia

[1] ISO/IEC. ISO 26262:2011: Road vehicles – functional safety. Published, International Organization for Standardization, Geneva, Switzerland., 2011.

[2] A Case Study of Hybrid Controller Synthesis of a Heating System: A. Balluchi, L. Benvenuti, T.Villa, H. Wong Toiy and A.L. Sangiovanni-Vincentelli, European Control Conference ECC 31 August - 3 September 1999, Karlsruhe, Germany

[3] Hybrid Systems: Modeling, Analysis and Control: John Lygeros, Claire Tomlin, and Shankar Sastry

[4] Modellizzazione e Controllo Predittivo Ibrido di un Motore ad Iniezione Diretta a Carica Stratificata, G. Ripaccioli, Università degli Studi di Siena

[5] Sistemi Ibridi: stabilità e applicazioni al controllo, G. Iacobelli, Università degli Studi di Roma Tor Vergata

[6] E. Fornasini, G. Marchesini: Appunti di Teoria dei Sistemi, Ed. Libreria Progetto (Padova)

[7] Veicoli a propulsione elettrica e ibrida: M. Ceraolo, Università di Pisa

[8] Hands on the ISO26262 Standard: Dependable Technologies for Critical Systems : C. Esposito, Università di Napoli Federico II

[9] Hazard identification and safety goals on power electronics in hybrid vehicles, Fredrik Walderyd, Department of Energy and Environment, Chalmers University

[10] Development of an ISO 26262 ASIL D compliant verification system, Daniel Carllson, Institutionen för datavetenskap Linköpings universitet

[11] Functional Safety with ISO 26262 - Principles and Practice, Dr. Christof Ebert, Jonas Wolf , Vector Consulting Services

[12] Brake By Wire Functional Safety Concept Design for ISO/DIS 26262, J.S. Cheon, J.S. Kim, J.H. Jeon, S.M. Lee, SAE International

[13] Experience with ISO 26262 ASIL Decomposition, Andrea Piovesan and John Favaro, Automotive Spin, Milano 17 February 2011