Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Aerospaziale
A.A. 2022/2023
Tesi di Laurea Magistrale
Sessione di Laurea di Ottobre 2023 (25 Ottobre 2023)

STUDIO DEI VINCOLI NORMATIVI PER LA DEFINIZIONE DELLE ARCHITETTURE DEI SISTEMI DI BORDO

Relatori:
Prof. Marco Fioriti
Prof. Paolo Maggiore

Candidati:
Fixherald Shahini
s303616

INDICE

LISTA DELLE FIGURE

ACRONIMI E ABBREVIAZIONI

CS = Certification Specifications
AMC = Accetable Means of Compliance
ADO = Progettazione e ottimizzazione dell'architettura
ADSG = Architecture Design Space Graph
DLR = Centro aerospaziale tedesco
MBSE = Ingegneria dei sistemi basata su modelli
MDAO = Analisi e ottimizzazione della progettazione multidisciplinare
RFLP = Requisiti-Funzionali-Logici-Fisici
XDSM = Extended Design Structure Matrix
APU = Auxiliary Power Unit
EHA = Electro-Hydrostatic Actuator
EMA = Electro-machanic Actuator
OBS = On-Board Systems
PTU = Power Transfer Unit
RAT = Ram Air Turbine
RBD = Reliability Block Diagram

1. INTRODUZIONE

Per iniziare la Tesi è opportuno incominciare con un'introduzione al lavoro di Tesi svolto presso il Dipartimento di Ingegneria Meccanica e aerospaziale del Politecnico di Torino e quali sono gli obiettivi di questa che questa tesi si prefigge e in quali ambiti opera, lo stato dell'arte e altro.

1.1 OBIETTIVO DELLA TESI

La parola che riassume l'ambito di Tesi e il lavoro conseguente è una sola, Certificazione. La certificazione è di importanza assoluta in ogni campo industriale, non solo quello aeronautico. Ogni realtà industriale e ogni azienda che produce qualcosa deve essere in grado di fabbricare qualcosa di certificabile. Ogni prodotto, qualunque esso sia, ha bisogno di una certificazione, cioè, deve essere costruito secondo dettami di legge vigenti in quel paese o realtà sovranazionale o in altri paesi in cui si intende vendere il prodotto. La certificazione serve per fare automobili, macchinari, navi, strutture, case, telefoni, computer, aeromobili, satelliti e tanto altro. Ogni prodotto ha la sua certificazione, che può essere di tanti tipi e con obiettivi diversi. Nessun prodotto industriale, quale esso che sia, può essere prodotto in serie, e far produrre profitti all'azienda (*che è l'obiettivo di ogni azienda al mondo*), senza certificazione. Questo è semplicemente impossibile. Visto che questa Tesi opera nel campo aeronautico, si addentrerà solo nel processo di certificazione per aeromobili. Certificare un aeromobile vuol dire semplicemente progettare un velivolo a norma di legge, sicuro per i passeggeri e sicuro per l'ambiente circonstante. Questa sola definizione però racchiude un mondo complissimo, intricato, costosissimo e lunghissimo, che impiega tempo, denaro e risorse umane. Il primo capitolo sarà fondamentale per comprendere come funziona l'intero processo certificativo, e vedere come esso non sia qualcosa di lineare e completamente programmato, ma frutto di iterazioni, decisioni, durante l'intero processo di progettazione di ogni aeromobile aeronautico. Certificare un aeromobile è dura, e può durare anche 5 anni, se non di più, e per questo che vengono utilizzati degli '*appoggi*' normativi legislativi che aiutano i vari progettisti a costruire il velivolo, nei limiti legislativi vigenti, anche all'occorrenza modificando e aggiungendo nuove norme per andare al passo con i tempi e l'evoluzione tecnologica. Il problema è che la maggior parte delle volte non è così semplice ed immediato comprendere alcuni elementi normativi. Non è facile interpretare frasi o norme presenti nelle varie normative che sono state elencate. Questo perché, il linguaggio normativo è un linguaggio molto burocratico, proprio perché ha l'obiettivo di certificare, in tutti gli ambiti, un elemento aerospaziale. E le certificazioni passano per lo 'spazio' legislativo burocratico. Un campo, questo, che non è così familiare all'ingegnere 'tradizionale'. E quindi l'ingegnere si ritrova a dover leggere documenti che hanno sì elementi tecnici, come calcoli di velocità, o diagrammi di manovra o altro, ma molte volte scritte in maniera molto astrusa e incomprensibile, anche per un ingegnere esperto in quel campo specifico. Un linguaggio, appunto, più familiare agli avvocati o perlomeno nell'ambito legislativo. Ma è di fondamentale importanza che esistano figure di ingegneri che conoscano, non solo la tecnica aeronautica, ma riescano a familiarizzare e a comprendere il linguaggio normativo, perché nessuno può produrre in serie in bel prototipo senza certificazione di tipo e di aeronavigabilità. E questi certificati passano per una comprensione piena e totale del linguaggio normativo legislativo. Leggendo le varie normative alcuni ambiti tecnici, come strutture, manovre, velocità e altro, sono più semplici da interpretare perché hanno al loro interno un range di misura, limiti tecnici numerici e altri aspetti tecnici meno astrusi e poco dediti a mal interpretazione. Mentre sono presenti altrettanti e molto importanti elementi che invece hanno meno aspetti prettamente numerici, ma sono ad esempio di aspetto probabilistico, interpretativo e logico, il che può creare confusione e mal interpretazione. Questi elementi sono gli equipment e i sistemi di bordo, la safety legata alla loro architettura, alla loro funzione, alla loro installazione, i pericoli e le failure che nascono in questi sistemi così fondamentali per il velivolo. Ormai al giorno d'oggi '*tutto è sistemi'* e quindi questo aspetto è legato all'intero velivolo in maniera veramente critica. Quindi una mal interpretazione e confusione può provocare errori di progettazione e architettura dei sistemi veramente critici e pericolosi per la sicurezza dei membri dell'equipaggio e dei passeggeri. L'obiettivo di questo lavoro di Tesi è quello di andare ad analizzare alcune normative vigenti (*aggiornate al 2023*) per andare a cercare i vincoli normativi per la progettazione dell'architettura dei sistemi di bordo. Interpretare quindi le frasi e i sensi logici per trovare il vincolo tecnico logico per l'architettura dei sistemi. Se per aspetti, di strutture o motori o manovre, questi vincoli sono più

individuabili grazie a numeri, range tecnici, per quanto riguarda i sistemi, questi vincoli possono essere presenti in frasi burocratiche da interpretare, ma è fondamentale individuarli per riuscire a progettare l'architettura dei vari sistemi di bordo al meglio per la sicurezza. Si andranno ad analizzare le probabilità di failure per un sistema, le tipologie di failure che possono intercorre (i guasti), come le failure possono interagire, come riconoscerli e bloccarli. Trovati questi vincoli e suddivisi per importanza, si andrà poi a elaborare, grazie alla lettura e documentazione di queste normative, un'architettura esempio utilizzando un software apposito sviluppato dalla Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR) (*German Aerospace Center-DLR*), Institute of System Architectures in Aeronautics | Aircraft Design & System Integration, chiamato ADORE. Questo è un software che permette di definire il '*design space'* di un sottosistema e da lì ottenere poi diverse architetture sia convenzionali che innovative (*verrà spiegato meglio il suo funzionamento in un capitolo successivo dedicato*). Una volta creato un'architettura di un sistema esempio verrà effettuato il "pre-check certificativo" utilizzando un tool apposta in fase di sviluppo, chiamato ACOBS. Questo tool utilizzerà i vincoli architettonici di sistema individuati e catalogati nella fase di studio ed interpretazione delle varie normative. Questo lavoro quindi si pone l'obiettivo di studiare le normative e rilevare i vari vincoli architettonici di sicurezza dei sistemi bordo per poterli implementare in un tool che aiuti successivamente il processo certificativo dei sistemi. Per tutti gli altri elementi, il tempo che servirebbe sarebbe troppo per una tesi di laurea. Vista la difficoltà di interpretazione logica-filosofica che sta dietro i vincoli normativi dei sistemi, questo lavoro si pone l'obiettivo di cercare di trovare anche una chiave di lettura che aiuti quindi il processo di analisi delle norme, e sarà d'aiuto per migliorare e velocizzare il processo certificativo. Serve avere ingegneri che abbiamo esperienza e lavoro nel processo certificativo e questa tesi vuole inserirsi nel campo complesso dell'aiuto all'interpretazione delle normative sui sistemi, perché, come detto, è essenziale per l'intero processo certificativo e la produzione e la sicurezza del velivolo. Questo lavoro utilizzerà solo alcune delle normative (*che saranno presentate nel primo capitolo sulla certificazione*), la CS-25 per velivoli ad ala fissa di grosse dimensioni, la SAE ARP 4754 e 4761. Sulla CS-25 si andrà ad analizzare completamente ed approfonditamente il capitolo principale sui sistemi, il capitolo 25.1309 e il corrispettivo AMC 25.1309. È il capitolo in cui sono contenuti i maggiori vincoli architettonici e logici dei sistemi. Ma non è l'unico, verranno studiati altri capitoli, sempre all'interno della CS-25. Verrà utilizzata anche la SAE ARP 4754 che contiene al suo interno altri vincoli che saranno utilizzati nel lavoro. Ed infine verrà studiata la SAE ARP 4761 soprattutto perché contiene un esempio dettagliato di studio di sicurezza di un sistema generico, nello specifico il sistema frenate di un aereo commerciale. Questo sistema sarà utilizzato nel software ADORE per la costruzione dell'architettura, utilizzando le indicazioni presenti nella ARP 4761. Questo è un lavoro che a primo impatto per un ingegnere *'tradizionale'* potrebbe sembrare noioso, poco stimolante, e addirittura troppo difficile per via dello studio dettagliato dell'aspetto legislativo dei vari sistemi di un aeromobile, ma è essenziale che venga svolto nel migliore dei modi e con la giusta motivazione, passione e pazienza. L'obiettivo finale è quello di provare a dimostrare che è possibile inserire l'aspetto certificativo già all'interno del progetto dei sistemi di bordo. Cioè, cercare di mostrare che è possibile progettare delle architetture di sistema che siano già certificabili per l'aspetto dei requisiti minimi di safety, inseriti nelle normative. Come si vedrà nei capitoli successivi si può dire che l'obiettivo sia quello di unire il lato sinistro con il lato destro della V-model dei sistemi di bordo. Si può poi ampliare il processo anche ad altri elementi industriali. L'ingegnere per essere completo non solo deve essere capace di maneggiare la tecnica aeronautica in un settore specifico, ma deve anche essere pratico degli aspetti ed elementi normativi e legislativi e di sicurezza, che non sono assolutamente semplici e di immediata comprensione, ma essenziali, perché senza questi aspetti così importanti nessun aeromobile potrebbe mai vedere la luce.

2. LA CERTIFICAZIONE

2.1 IL PROCESSO CERTIFCATIVO

Descritto nell'introduzione l'obiettivo della Tesi, il primo capitolo andrà a sviscerare e descrivere nel dettaglio l'aspetto certificativo e il lavoro dell'ingegnere che prima è stato citato, l'ingegnere certificatore. Nell'industria aeronautica, elicotteristica e spaziale un aspetto fondamentale ed essenziale per la riuscita finale del progetto è il processo di certificazione, per ottenere un certificato di omologazione (*type certificate*). La certificazione è un processo fondamentale che permette all'azienda che ha progettato il velivolo di produrre in serie il proprio prodotto e di poterlo vendere ai futuri clienti. Tuttavia, questo processo di certificazione, che deve essere fatto in accordo con l'ente certificatore (*EASA per l'Europa, FAA per gli Stati Uniti*) non è semplice, banale e immediato, richiede anni di test e un ingente spesa di denaro. Per questo le aziende quando progettano i propri velivoli lo fanno seguendo linee guida, normative, regole, scritte ed elaborate proprio dagli enti certificatori di cui sopra. Inoltre ogni azienda ha al suo interno un intero dipartimento di ingegneri certificatori che hanno il compito di leggere, comprendere ed interpretare le varie normative (*ci sono normative differenti in base alla tipologia di velivolo e al suo peso)* e seguire il progetto e il lavoro del velivolo in modo da permettere un processo di certificazione più veloce e facilitato ed evitare che il prodotto finito non abbia nessun tipo di problema di certificazione, perché questo causerebbe una modifica dell'intero velivolo, e si andrebbe a ritardare l'intero progetto finale e a spendere ulteriore soldi, che potrebbero, nel peggiore dei casi, rovinare l'azienda stessa. L'ingegnere certificatore dell'azienda impedisce che tutto questo accada seguendo e controllando che il progetto segua le direttive e le regole descritte nelle varie normative. Una volta che i prototipi sono stati ultimati e consegnati all'ente certificatore per la valutazione finale, se progettati seguendo le regole, allora saranno più facilmente e velocemente certificabili. È utile ai fini del lavoro spendere, in questa introduzione, alcune parole sul processo tecnico di certificazione con l'ente certificatore e sulle diverse tipologie di normative. Prima che un modello di aeromobile di nuova concezione entri in funzione, deve ottenere un certificato di omologazione dall'autorità di regolamentazione dell'aviazione responsabile. Dal 2003 l'EASA è responsabile della certificazione degli aeromobili nell'UE e per alcuni Paesi europei extra UE, mentre per quanto riguarda gli Stati Uniti l'ente è FAA. Questo certificato attesta che il tipo di aeromobile soddisfa i requisiti di sicurezza stabiliti dall'Unione Europea o dall'America.
Il processo di certificazione è suddiviso in 4 fasi:

1. *Technical Familiarisation and Certification Basis*

Il costruttore di aeromobili e velivoli presenta il progetto all'EASA quando ritiene che abbia raggiunto un grado sufficiente di maturità, anche in base al lavoro degli ingegneri certificatori presso l'azienda stessa. La squadra di certificazione EASA e l'insieme di regole che si applicheranno per la certificazione di questo specifico tipo di aeromobile sono definite (*base di certificazione*).

2. *Establishment of the Certification Programme*

L'EASA e il costruttore devono definire e concordare i mezzi per dimostrare la conformità del velivolo per ciascun requisito della base di certificazione. Ciò va di pari passo con l'identificazione del "livello di coinvolgimento" dell'EASA durante il processo di certificazione.

3. *Compliance demonstration*

L'azienda deve dimostrare la conformità del suo prodotto ai requisiti normativi, la struttura, i motori, i sistemi di controllo, i sistemi elettrici e le prestazioni di volo vengono analizzati rispetto alla base di certificazione e le direttive scritte. La dimostrazione di conformità viene effettuata tramite analisi sviluppati e raccolti mediante i test a terra ma anche mediante test durante il volo. Gli esperti dell'EASA effettuano un esame dettagliato della conformità dei test effettuati, mediante revisioni dei documenti nei loro uffici di Colonia e partecipando ad alcune di queste dimostrazioni di conformità (*test witnessing*). Questa è la fase più lunga del processo di certificazione del tipo, può durare anni, anche se il progetto è stato portato avanti seguendo le direttive normate. Nel caso di aeromobili di grandi dimensioni, il periodo per completare la dimostrazione di conformità arriva a cinque anni, ma può essere prorogato, in caso emergano problemi.

4. *Technical closure and issue of approval*

Se si è tecnicamente soddisfatti dei risultati di conformità da parte dell'azienda, l'EASA chiude l'intero processo e rilascia il certificato.

Un aspetto importante è il rilascio del certificato per velivoli convalidati da altri enti certificatori. L'EASA rilascia la certificazione primaria per i modelli di aeromobili europei che vengono convalidati in parallelo da autorità straniere per operare nei loro spazi aerei, FAA per gli Stati Uniti o il TCCA per il Canada. Al contrario, l'EASA convaliderà la certificazione FAA dei modelli di aeromobili statunitensi (*o la certificazione TCCA dei modelli canadesi)* in base agli accordi bilaterali sulla sicurezza aerea applicabili tra l'UE e il paese terzo interessato. In passato un paese terzo che EASA certificava era la Russia, ma ora, al 2023, L'EASA ha sospeso i certificati di omologazione per i produttori russi in risposta all'invasione militare russa dell'Ucraina. La certificazione può sembrare un processo tutto sommato abbastanza standard e lineare. Questa definizione non può essere più lontana dalla realtà. Il processo certificativo è un processo molto complesso, che presenta molte fasi e passaggi versante complessi e va quindi spiegato nella maniera più comprensiva possibile, perché per un '*non addetto'* può essere veramente confusionario ed impossibile da comprendere al meglio. È per questo che verrà spiegato nei dettagli, oltre a quello che è già stato detto (*preso dall'EASA*), grazie alla SAE ARP 4754 (*verrà spiegata successivamente che documento è*) che descrive al meglio l'intero processo certificativo e la scelta di architettura, che sarà utilizzata enormemente in questo lavoro di Tesi. L'obiettivo del processo di certificazione è dimostrare che il velivolo e i suoi sistemi complessi siano conformi ai requisiti di aeronavigabilità applicabili, a norma di legge. Nella maggior parte dei casi la certificazione dell'aeromobile è ottenuta attraverso la conformità a una serie di piani di certificazione dei vari sistemi. Un elemento fondamentale è la comunicazione, e questa si ottiene tramite la pianificazione ed il coordinamento. La pianificazione e il coordinamento sono elementi fondamentali per stabilire una comunicazione efficace tra il richiedente e l'autorità di certificazione (*EASA o FAA),* e questa comunicazione è fondamentale per raggiungere un accordo sui piani di certificazione dei sistemi, che riesca anche ad accorciare i tempi e costi dell'intero processo, e raggiungere un accordo sui mezzi previsti per dimostrare che l'aeromobile e i suoi sistemi sono conformi ai requisiti di aeronavigabilità. Tutto questo è fondamentale per via dei sistemi che oggigiorno sono ad un livello veramente complesso ed articolato. Una delle caratteristiche dei sistemi altamente integrati e complessi è la necessità di trovare e utilizzare metodi di garanzia dello sviluppo come parte delle prove a sostegno della certificazione dell'intero sistema. È di vitale importanza coordinarsi su una scelta accurata delle varie architetture. Un'accurata attenzione all'architettura del sistema, all'architettura degli elementi e alla selezione dei componenti può semplificare, anche di molto, i metodi di garanzia dello sviluppo e limitare le prove a sostegno della certificazione del sistema, aiutando quindi l'intero processo e l'azienda progettista richiedente. Potendo anche limitare la gamma di sistemi o elementi a cui si applica questa strategia di certificazione. Gli aeromobili del passato, ma soprattutto odierni, tendono ad avere un alto grado di variazione sia nella complessità del sistema che nella loro integrazione nel velivolo. Il processo di certificazione, pertanto, deve essere flessibile, sempre ai limiti delle leggi vigenti (*nei prossimi paragrafi verrà affrontato il problema delle nuove tecnologie e l'effetto sulle normative*). La flessibilità è ottenuta dalle aziende richiedenti tramite la pianificazione della certificazione. Esso garantisce al tempo stesso al richiedente e all'autorità di certificazione un elevato livello di fiducia nell'approccio di certificazione. La pianificazione del processo di certificazione permette di separare in piccoli compiti gestibili gli aspetti normativi del processo di sviluppo complessivo, che altrimenti sarebbero troppo ingestibili, che possono essere portati a termine in modo logico e sequenziale, permettendo di individuare più facilmente gli errori durante la via della certificazione. Un piano di primo livello descrive la base della certificazione (*regolamenti applicabili e condizioni speciali*) e delinea i mezzi e le tecniche con cui l'azienda richiedente prevede di dimostrare la conformità alle varie leggi. Questa aspetto organizzativo è vitale perché una pianificazione precoce della certificazione può ridurre al minimo gli effetti di mal interpretazioni dei regolamenti e del materiale consultivo, questo è anche il compito di un ingegnere certificatore, impedire una interpretazione errata che porterebbe problemi su problemi. Il piano di certificazione per un sistema complesso e altamente integrato permette di definire l'intero prodotto e l'installazione da certificare, delinea le modalità di certificazione del sistema e l'intero impianto da certificare, delinea i processi di sviluppo del prodotto da utilizzare per la garanzia dello sviluppo e identifica i mezzi e le tecniche proposte per la conformità ai regolamenti. Poiché molte delle attività di garanzia dello sviluppo avvengono ben prima che

sia disponibile un'implementazione, il coordinamento precoce con le autorità di certificazione è fondamentale per evitare che arrivati all'inizio del processo questo non risulti pieno di problemi e siano stato utilizzate tecniche sbagliate e che quindi si rischi di tornare indietro perdendo sia tempo che risorse. Una cosa che bisogna sottolineare è che un piano di certificazione iniziale può mancare di dettagli significativi, rendendo necessari, quindi, aggiornamenti successivi per integrare sviluppi e nuovi dettagli. Veniamo al momento di richiesta, infatti l'azienda richiedente propone un metodo di conformità che definisca come lo sviluppo del sistema e dell'apparecchiatura software e hardware soddisferà la base di certificazione. L'azienda presenta quindi i suoi piani di certificazione all'autorità di certificazione corrispondente per la revisione prima che si verifichino le attività di sviluppo. Se vengono richiesti ulteriori dati relativi ai piani e ai mezzi di conformità che vanno a giustificare varie modifiche di qualunque natura, devono essere presentati in tempo utile per consentire una revisione significativa e risolvere le questioni identificate dall'autorità di certificazione in merito ai mezzi con cui il sistema sarà conforme ai requisiti di aeronavigabilità. Fatto questo bisogna quindi ottenere l'accordo con l'autorità di certificazione sui piani modificati. Importanti sono i dati di certificazione. I dati di certificazione sono la prova che il sistema soddisfa i vari requisiti di aeronavigabilità a norma di legge. L'autorità di certificazione determina l'adeguatezza dei dati per dimostrare la conformità normativa. Il richiedente deve sviluppare una sorta di sommario, un riassunto, di certificazione per descrivere come è stato determinato che il sistema e la sua installazione sull'aeromobile, soddisfano entrambi i requisiti di aeronavigabilità, sia quindi conforme ai vincoli legislativi. Il riepilogo della certificazione fornisce una descrizione dei risultati delle attività stabilite nel piano di certificazione. Qualsiasi deviazione dal piano concordato con l'agenzia certificatrice deve essere descritta insieme alla giustificazione sul perché è stato necessario fare quella deviazione. Oltre a trattare ciascuno dei contenuti del piano di certificazione, il riepilogo di certificazione deve includere:
-Una dichiarazione di conformità ai requisiti di aeronavigabilità.
-Una descrizione di tutti i rapporti sui problemi aperti che hanno un impatto sulla funzionalità o sulla sicurezza dell'aeromobile e dei suoi sistemi.
Il piano di certificazione per un sistema altamente integrato e complesso deve rappresentare nel migliore dei modi e con un livello di dettaglio elevato sia il sistema complessivo che l'ambiente aeronautico in cui il sistema stesso opererà e sarà utilizzato. Questo rappresenta il fulcro della certificazione, cioè il rispetto delle norme del sistema interno e dell'ambiente operativo. La quantità di dettagli contenuti nel piano può variare a seconda della classificazione dei rischi associati all'aeromobile, secondo anche la matrice dei rischi. (figura 1), soprattutto se si tratta di sistemi di bordo.

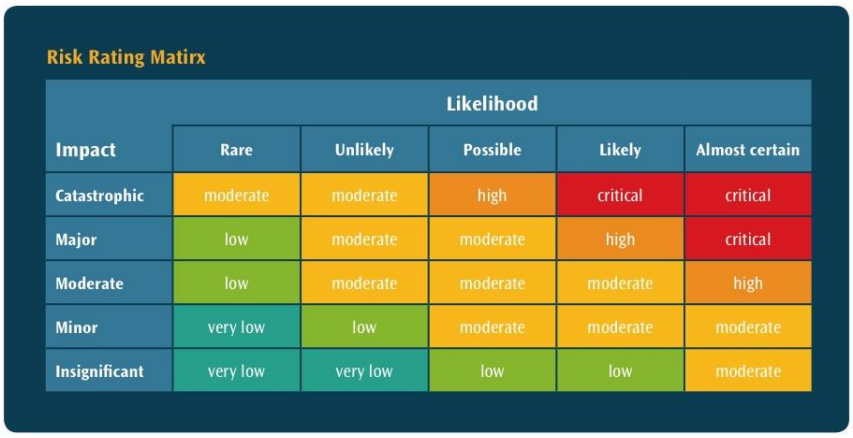


FIGURA 1

Ogni piano di certificazione deve quindi includere degli elementi ben precisi:
- Una descrizione funzionale e operativa del sistema e dell'aeromobile su cui il sistema sarà installato.
- Una descrizione devi vari elementi di cui è costituito il sistema, compresi hardware e software. Questa descrizione deve stabilire le relazioni funzionali, fisiche e informative tra il sistema e gli altri sistemi e funzioni dell'aeromobile.
- Una dichiarazione della relazione di questo piano di certificazione con qualsiasi altro piano di certificazione del sistema utilizzato.

- Una sintesi della valutazione dei rischi funzionali (*rischi dell'aeromobile, condizioni di guasto e classificazione dei rischi, tassi di rischio, etc.)*
- Una sintesi della valutazione preliminare della sicurezza del sistema (*obiettivi di sicurezza del sistema e livelli preliminari di garanzia dello sviluppo del sistema*).
- Una descrizione di tutte le caratteristiche di progettazione nuove e/o uniche che si prevede di utilizzare per raggiungere tutti i vari obiettivi di sicurezza. Bisogna descrivere se i requisiti di sicurezza sono ottenuti con elementi dello stato dell'arte e da elementi nuovi.
- Descrizione delle nuove tecnologie o delle nuove applicazioni tecnologiche da implementare (*questo aspetto delle nuove tecnologie e del ruolo normativo sarà trattato in maniera dettagliata successivamente*)
- La base di certificazione del sistema, comprese eventuali condizioni speciali, se per caso non si seguono le norme ufficiali degli enti certificatori ma si utilizzano norme di altro genere che comunque devono garantire lo stesso livello di sicurezza adeguato.
- I metodi proposti per dimostrare la conformità con la base di certificazione ufficiale (*ad esempio la FAR 25.1309 o CS 25.1309*), compresi i vari processi di garanzia dello sviluppo previsti dalla normativa vigente (*valutazione della sicurezza, convalida, verifica, gestione della configurazione e garanzia del processo*).
- Un elenco dei dati da presentare e dei dati da conservare sotto controllo di configurazione, insieme ad una descrizione dei suddetti dati e a un campione dei formati dei dati.
- La sequenza temporale e il calendario approssimativo di tutti i test di certificazione, possono comunque subire modifiche in base agli eventuali problemi che potrebbero emergere nel corso dei test.
- Identificazione del personale e successivamente dell'organizzazione specifica responsabile del coordinamento della certificazione.

Oltre al piano presentato, un elemento importante è l'indice di configurazione del sistema. Questo indice identifica tutti gli elementi fisici che insieme costituiscono il sistema nel suo complesso. Inoltre, l'indice di configurazione identifica tutte le procedure e tutte limitazioni che sono parte integrante della sicurezza del sistema. Inoltre, devono essere identificate qualsiasi caratteristica o capacità di progettazione del sistema o di capacità superiori a quelle richieste per stabilire la sicurezza del sistema ai sensi delle normative di legge vigenti.

Un tipico indice di configurazione del sistema deve includere le seguenti informazioni:
- Identificazione della configurazione di ciascun elemento del sistema
- Software dell'elemento associato
- Interconnessione degli elementi
- Interfacce richieste con altri sistemi
- Procedure e limitazioni operative o di manutenzione legate alla sicurezza del sistema

In aggiunta, se applicabile, devono essere incluse informazioni che descrivano l'intercambiabilità consentita di elementi alternativi all'interno del sistema, la cosiddetta ridondanza funzionale. Nonostante tutto, non esiste un processo specifico unico raccomandato per lo sviluppo dei sistemi, ce ne possono essere di tanti tipi, in base al sistema e alla sua complessità o in base ad altri fattori esterni o interni al sistema. Visto che non esiste un processo unico, il processo di sviluppo specifico scelto deve essere descritto in modo sufficientemente dettagliato per ottenere una comprensione reciproca degli elementi chiave e delle loro relazioni, in modo da facilitare il processo di certificazione evitando problemi e poter comprendere meglio le reali capacità di quel processo e se può essere utile migliorarlo o no in futuro in vista di nuovi sistemi. Il piano di sviluppo prevede alcuni elementi di spicco, deve identificare i processi di primo livello che si prevede di utilizzare, gli eventi chiave che scandiscono il ciclo di sviluppo previsto e i processi di sviluppo che segnano il ciclo di sviluppo pianificato, nonché la struttura organizzativa e le responsabilità individuali chiave che supportano lo sviluppo. Questo ultimo punto è importante per organizzare il lavoro ed eventualmente capire, se ci sono stati errori, di chi sia la colpa in un eventuale indagine, tecnica e giuridica. I processi e gli eventi devono essere descritti in modo sufficiente per stabilire la loro importanza relativa per lo sviluppo del sistema, i tempi e le interdipendenze, e la natura dei risultati attesi al completamento dell'evento o del processo. L'elemento fondamentale per un sistema, per garantire le sue funzioni e la sua sicurezza, è la sua architettura. La descrizione dell'architettura e della progettazione è fondamentale nel processo di certificazione e deve basarsi su una comprensione comune di funzionalità prevista a livello di aeromobile fornita o supportata dal sistema, l'ambiente operativo previsto per il sistema e le capacità specifiche del sistema installato sull'aeromobile. Devono essere forniti sufficienti dettagli architettonici e di progettazione del sistema per stabilire come il sistema raggiungerà la funzionalità prevista. La descrizione deve anche

identificare i mezzi primari di contenimento dei guasti o delle avarie, per evitare il proliferarsi di failure che possono portare a failure condition ed eventi catastrofici. Gli elementi di progettazione vecchi, nuovi o inediti, nonché le caratteristiche architettoniche specifiche e gli elementi di progettazione svolgono un ruolo specifico e di vitale importanza nella creazione o nel mantenimento della sicurezza del sistema.

2.2 LE NORMATIVE

Per aiutare e omologare tutti i progetti di aeromobili delle varie aziende europee e no, ma che si rifanno all'EASA, sono state prodotte normative e direttive per il progetto di ogni tipo di velivolo. Queste normative sono chiamate:
-*Certification Specifications (CS, including the general AMC-20)*
-*Acceptable Means of Compliance (AMC) & Guidance Material (GM) to a rule*
L'insieme delle documentazioni EASA per la certificazione è denominata Agency Rules.
Dall'istituzione dell'ICAO e dall'inizio della regolamentazione per la sicurezza dell'aviazione civile, la complessità e la densità delle operazioni aeree non hanno cessato di aumentare ad un livello incredibile, insieme all'enorme gamma di scelte tecnologiche disponibili, come verrà spiegato meglio successivamente. La complessità dell'aviazione rende impossibile regolamentare l'intero settore senza disporre di diversi livelli di normative. Mentre in alcuni casi è opportuno, e persino necessario e obbligatorio, utilizzare norme vincolanti (*regolamenti*), in altri casi è necessario prevedere una certa flessibilità da parte del sistema normativo, attraverso l'uso di norme, quindi, non vincolanti (*soft law*). Questa necessità di avere un approccio equilibrato della regolamentazione è stata universalmente riconosciuta ed è stata attuata da tutte le organizzazioni internazionali e dalle autorità nazionali di regolamentazione.

Nel sistema EASA esistono tre livelli principali di materiale normativo:

- Il regolamento di base stesso, adottato dal Parlamento europeo e dal Consiglio europeo (*sede degli stati membri dell'Unione Europea*), è vincolante in tutti i suoi elementi.
- Le modalità di attuazione del regolamento di base, adottate dalla Commissione europea;
- Certification specification (CS), Acceptable Means of Compliance (AMC) and Guidance Material (GM), adottate dall'Agenzia.

Viene presentata nell'Appendice A una panoramica delle diverse tipologie di normative introdotte da EASA. Questa suddivisione è presa direttamente dal sito ufficiale di EASA, aggiornato al 2023 [1]. Come è possibile notare dall'Appendice A il campo più corposo è rappresentato dalla Initial Airworthiness, cioè dalla certificazione iniziale di aeronavigabilità, è la parte più critica perché deve regolare ogni tipo di aeromobile per la certificazione iniziale e il seguente inizio di produzione industriale. Insieme a queste certification specifications, per migliorare la comprensione e l'interpretazione delle varie direttive, l'EASA ha elaborato varie AMC e Guidance Material (GM) con l'obiettivo di aiutare le varie aziende nel percorso delle varie norme, che dono ufficiali dell'EASA. Esistono dal lato americano della FAA e delle FAR (*l'equivalente statunitense dell'EASA e delle CS europee)* anche degli aiuti alla comprensione delle normative e dei regolamenti, queste si chiamano AC-Advisor Circular. Per anni anche l'EASA e l'Europa, data la vicinanza socio-politico-economica con l'America, ha utilizzato le AC per interpretare e spiegare le proprie normative e regolamenti, questo perché le CS e le normative europee sono la 'copia esatta', con solamente differenze linguistiche e di sintassi, delle FAR americane, la sostanza era identica e non è mai cambiata, neanche ora al 2023. Le AMC sono norme non vincolanti adottate dall'EASA per illustrare i mezzi per stabilire la conformità al regolamento di base e alle relative norme attuative, le normative, dei vari aeromobili. Gli AMC emessi dall'EASA non sono di natura legislativa. Non creano quindi obblighi aggiuntivi per gli ingegneri certificatori, che possono decidere di dimostrare la conformità ai requisiti applicabili ai velivoli utilizzando altri mezzi. Tuttavia, poiché i vari legislatori desideravano che tale materiale garantisse la certezza del diritto e contribuisse a uniformare l'attuazione dei vari requisiti, hanno conferito all'AMC adottata dall'EASA una de facto conformità alle norme, in modo da impegnare le autorità competenti a riconoscere gli ingegneri certificatori che rispettano l'AMC dell'EASA come conformi alla legge. È riportato integralmente

nell'Appendice A la suddivisione delle varie AMC e GM, preso dal sito ufficiale di EASA, aggiornato al 2023. [2] Anche il campo della AMC & GM è vastissimo e variegato proprio perché i campi e gli ambiti dell'aeronavigabilità sono molto estesi e non di facile comprensione ed interpretazione, e quindi si necessitano di aiuti per evitare interpretazioni errate. Ma non sono gli unici documenti disponibili, sono i più usati e *de facto* gli ufficiali, o ufficiosi. Poiché le AMC non sono vincolanti, gli ingegneri certificatori possono scegliere mezzi e documenti alternativi per conformarsi alla regolamentazione ufficiale, che comunque sono in linea con gli standard vigenti. Ma niente è senza conseguenze, perché in questo caso, tuttavia, viene a mancare la conformità fornita dagli AMC ufficiali dell'EASA e bisogna, quindi, dimostrare alle autorità competenti di aver rispettato le leggi. Questi documenti alternativi vengono chiamati AltMoC, Alternative Means of Compliance. Le norme di attuazione per le licenze degli equipaggi, le operazioni aeree, gli aeroporti e le licenze dei controllori del traffico aereo descrivono il processo che deve essere per forza utilizzato dagli ingegneri certificatori e dalle autorità competenti quando intendono utilizzare un AltMoC, invece degli AMC, per conformarsi alle regole e alle leggi. Le norme di attuazione vigenti stabiliscono che l'attuazione delle AltMoC da parte delle organizzazioni e aziende produttrici e di progettazione è soggetta all'approvazione preventiva da parte dell'autorità competente e viene sempre indicata cosa deve essere fatto per ottenere l'approvazione finale. Le norme attuative stabiliscono inoltre gli obblighi che le autorità competenti hanno quando danno l'approvazione preventiva a un'organizzazione e azienda e quando queste adottano un AltMoC che può quindi essere utilizzato dalle organizzazioni regolamentate sotto la loro supervisione. [9] Però, ed è cosa fondamentale, uno degli obblighi previsti dalle norme attuative è quello di notificare all'EASA che tipo di AltMoC viene utilizzato e cosa contiene, cioè, spiegare dettagliatamente il AltMoC utilizzato. Le autorità competenti sono quindi invitate (*ma possiamo dire obbligate se vogliono ottenere la certificazione)* a utilizzare il modulo di notifica AltMoC preparato dall'EASA per notificare sia gli AltMoC proposti dalle organizzazioni che quelli effettivamente utilizzati. Si vede quindi che le AMC non sono obbligatori e che si possono utilizzare altri documenti per progettare e certificare, da parte delle aziende, i nuovi aeromobili, ma se vengono utilizzati documenti alternativi il processo è più lungo e dispendioso, con notevole aumento di tempo e costi, perché l'EASA deve comprendere totalmente che tipo di alternative sono state utilizzate e se queste ultime sono valide per garantire la sicurezza del velivolo come è standard. Per questo che le aziende europee ed extra-europee, che vogliono ottenere la certificazione, è meglio che utilizzino le normative *de facto* ufficiali e che quindi richiedano ingegneri certificatore esperti e competenti nel settore certificativo, perché questo potrà permettere di risparmiare tempo e costi, che sono fondamentali in qualunque azienda, soprattutto quelle aerospaziali. Questa Tesi andrà a lavorare su alcune normative della Initial Airworthiness, studiando e valutando le CS (*certification specifications*) e gli AMC & GM relativi. Più in dettaglio saranno utilizzati e valutati la CS-25 per i grandi aeromobili. La CS-25 è una normativa e certification specification creata da EASA e inserita nella parte di Initial Airworthiness e si applica per la progettazione dei grandi aeromobili a turbina. Non è specificata, però, una limitazione esplicita della massa dell'aeromobile (CS 25.1). Gli aerei commerciali con un peso superior a 5700 kg (12 500 lb) sono certificati come 'grandi aeromobili' e quindi rientrano nella categoria della CS-25 (*FAR-25 per gli Stati Uniti)* [4]. Gli aerei di minor peso sono classificati come aerei utility di piccole dimensioni e sono certificati utilizzando la CS-23. Oltre a queste due CS, ci sono la CS-27 e la CS-29, che rappresentano il corrispettivo per gli elicotteri. Anche qui c'è la divisione in base al peso dell'elicottero. Gli elicotteri con un peso massimo e minore di 3 175 kg (*7 000 lbs)* e un numero di passeggeri massimo o minore di 9 [3]. Per gli elicotteri che superano queste limitazioni c'è la CS-29. Queste quattro CS rappresentano la certificazione di aerei ed elicotteri nel loro intero, ma esistono CS anche per le certificazioni di parti di aeromobili. Ci sono la CS-E, per l'engine (motore), la CS-P per il propeller e la CS-APU per l'APU. Insieme alla CS, si utilizzeranno anche le relative AMC & GM. Per il lavoro e l'obiettivo di questo lavoro, che poi sarà spiegato in dettaglio, verranno utilizzati anche altri tipi di materiali, in particolare le SAE ARP 4654 e SAE ARP 4761. Questi due documenti rappresentano delle linee guida per la progettazione dei sistemi di un aeromobile in base a vari requisiti, e queste linee guida utilizzano tecniche per calcolare e valutare i rischi e la safety dei vari sistemi. Non fanno parte di EASA, perché sono state create e appartengono a organizzazioni indipendenti, ma vengono utilizzati per interpretare al meglio alcuni requisiti e norme delle CS europee e FAR americane. Quindi vengono ormai utilizzante da tutte le aziende aeronautiche e aerospaziali per la progettazione e la certificazione dei vari aeromobili. Come per le normative ufficiali, esistono varie ARP per diversi elementi. Saranno però studiati, ai fini del lavoro due ARP, la 4754 e la 4761. In particolare, la SAE ARP 4754 discute e delinea lo sviluppo di sistemi aeronautici tenendo conto dell'ambiente operativo e delle funzioni generali

dell'aeromobile. Sono inclusi la convalida dei requisiti e la verifica dell'implementazione del progetto per la certificazione e la garanzia del prodotto. Questa SAE ARP fornisce le pratiche per dimostrare la conformità alle normative e serve ad assistere un'azienda nello sviluppo e nel rispetto dei propri standard interni considerando le linee guida qui contenute. Le linee guida presenti nel suddetto documento sono state sviluppate nel contesto del Titolo 14 Code of Federal Regulations (14CFR) Part 25 e della European Aviation Safety Agency (EASA) Certification Specification (CS) CS-25. Può essere applicabile ad altri regolamenti, come le part 23, 27, 29, 33 e 35 (*CS-23, CS-27, CS-29, CS-E, CS-P*). La SAE ARP 4754 affronta il ciclo di sviluppo per aeromobili e sistemi che implementano funzioni aeronautiche. Però non copre tutte le caratteristiche. Viene utilizzata insieme ad altri documenti altrettanto importanti e complementari, che verranno elencati successivamente. Infatti, non include una copertura specifica dello sviluppo dettagliato di software o hardware elettronico, e dei processi di valutazione della sicurezza, delle attività di sicurezza in servizio, dello sviluppo strutturale degli aeromobili, né riguarda lo sviluppo dell'elenco delle apparecchiature minime principali (MMEL) o dell'elenco delle deviazioni di configurazione (CDL). Una copertura più dettagliata degli aspetti software dello sviluppo si trova nel documento RTCA DO-178B, "*Software Considerations in Airborne Systems and Equipment Certification*" e nella sua controparte EUROCAE, ED-12B. La copertura degli aspetti hardware elettronici dello sviluppo si trova nel documento RTCA DO-254 / EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware". Le linee guida di progettazione e le considerazioni sulla certificazione per l'avionica modulare integrata si trovano nel documento RTCA/EUROCAE DO-297/ED-124. Le metodologie per i processi di valutazione della sicurezza sono delineate nel documento SAE ARP4761, *"Linee guida e metodi per condurre il processo di valutazione della sicurezza su sistemi e apparecchiature aeree civili*". I dettagli per la valutazione della sicurezza in servizio si trovano nella SAE ARP 5150, "Safety Assessment of Transport Airplanes In Commercial Service" e nella SAE ARP 5151 Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service. Le attività successive alla certificazione (*modifica di un prodotto certificato*) sono trattate nella sezione 6 del presente documento. I regolamenti e i processi utilizzati per sviluppare e approvare il MMEL variano in tutto il mondo. La guida per lo sviluppo del MMEL dovrebbe essere richiesta all'autorità locale di aeronavigabilità [5]. Come visto è insieme di documenti ufficiali che aiutano a interpretare e a seguire il giusto processo per la progettazione di prodotti aeronautici. Come detto, vediamo in dettaglio cosa contiene l'altra ARP importante per questo lavoro di tesi, la ARP 4761. La SAE ARP 4761 è un documento, complementare alla ARP 4754, che descrive le linee guida e i metodi per eseguire la valutazione della sicurezza per la certificazione degli aeromobili civili. Come per la 4754, anche questo documento è associato principalmente alla dimostrazione della conformità con FAR / JAR 25.1309. I metodi qui descritti identificano un mezzo sistematico, ma non l'unico, per dimostrare la conformità dei sistemi di un aeromobile. Non rappresenta però l'unica fonte di interpretazione delle norme 25.1309, ce ne possono essere altri, ma da anni questo è *de facto* quello più utilizzato. Un sottoinsieme di questo materiale può essere applicabile ad apparecchiature non relative alla norma 25.1309. Viene introdotto il concetto di valutazione della sicurezza a livello di aeromobile e vengono delineati gli strumenti per svolgere questo compito. Viene considerato l'ambiente operativo generale dell'aeromobile. I processi descritti nel documento in questione sono generalmente applicabili solo ai nuovi progetti o ai progetti esistenti interessati dalle modifiche di qualunque tipo dei vari sistemi dell'aeromobile. Nel caso dell'implementazione di disegni e modelli esistenti in una nuova derivazione, possono essere utilizzati mezzi alternativi come, ad esempio, l'esperienza di servizio di piloti ed ingegneri e manutentori per dimostrare la conformità. [6] A volte il processo di definizione dei requisiti non avviene tramite l'utilizzo delle CS o altri documenti ufficiali che conosciamo, ma tramite altri documenti di diversa estrazione e provenienza, ma che lo stesso garantiscono il rispetto della safety e dei requisiti. In questo caso allora viene compiuto un processo che si chiama '*Equivalent findings'*. Questo processo permette di certificare un velivolo che è stato progettato utilizzando norme e documenti diversi da quelli de facto utilizzati da tutti, ma che comunque permettono di rispettare tutti i requisiti di sicurezza imposti dalla safety e presenti nei documenti de facto ufficiali. Una cosa che bisogna però dire, ed è importantissimo soffermarsi su questo aspetto, è l'avvento delle nuove tecnologie. La tecnologia evolve in maniera veramente straordinaria, a livelli davvero impressionanti, si veda ad esempio l'enorme successo e progresso che sta avendo l'intelligenza artificiale (AI), che è qualcosa di veramente impressionante e al limite dell'inquietante. Ebbene, le varie normative quando vengono scritte non possono certo immaginare che nel futuro verranno fuori nuovi motori o nuovi sistemi o nuove armi o nuove tecnologie in generali che saranno sicuramente al di fuori degli standard dell'epoca. Le varie normative

cercano di essere il più generali e precise allo stesso tempo per permettere una certificazione di tecnologie simili o al più della stessa epoca (*se vogliamo essere esagerati ma non troppo diremmo 'era'*). Quindi quando si certifica un velivolo, un sistema, un componete, lo si fa per le tecnologie vigenti all'epoca o al massimo con alcune migliorie ristrette e localizzate. Questo le normative vigenti lo permettono senza nessun tipo di modifica sostanziale. Ma tutto cambia quando si utilizzano tecnologie rivoluzionarie, come ad esempio l'idrogeno come combustibile per diminuire o azzerare l'emissione di anidride carbonica nell'atmosfera, o altre tecnologie, magari, di armamenti ipersonici mai visti fino ad oggi, da montare su aerei. In questo caso cosa bisogna fare, è chiaro ed evidente che le normative vigenti non potranno mai certificare strumenti di questo genere; quindi, o si buttano le nuove tecnologie e continuare ad utilizzare quelle certificabili, oppure si deve procedere in un altro modo. Si deve procedere in altro modo, mai eliminare e distruggere il progresso, solo per aspetti burocratici e legislativi. Si crea quindi una nuova certificazione ad hoc, tramite studi e test, che permetta di eliminare questo problema e certificare le nuove tecnologie. Si definiscono delle 'special condition', condizioni specifiche che sanano un buco di requisiti con una certificazione ad hoc. All'inizio queste certificazioni sono speciali ed eccezionali e create ad hoc, ma con il tempo e con l'aumento e le migliorie delle nuove tecnologie (*che allo stato iniziale possono essere grezze e comunque poco pratiche*), diventeranno standard e saranno integrate nella certificazione ordinaria delle varie CS o altri documenti utilizzati. Questo è importante sottolinearlo, perché l'ambite aeronautico, come qualsiasi altro ambiente ingegneristico, è soggetto a cambiamenti per nuove tecnologie anche rivoluzionarie, e il processo di certificazione, essenziale per garantire la safety adeguata all'utilizzo di tutti i giorni, deve poter andare di pari passo e aggiornarsi sempre, per permettere, quindi, a tutta la popolazione mondiale (*al 2023 arrivata alla straordinaria quota di 8 miliardi di persone)* di poterne usufruire per migliore la vita delle persone e del nostro bellissimo pianeta. Si è visto come la certificazione e la progettazione siano processi complessi e che devono essere sempre al passo coi tempi. È quindi necessario cercare di creare elementi e modelli che aiutino questi due processi complessi. Il modello più utilizzato dagli ingegneri di sistema è il modello a V.

2.3 IL V-MODEL E LA CERTIFICAZIONE

Il processo certificativo è un elemento fondamentale nella vita di un ingegnere sistemista, sia aeronautico che di produzione che meccanico o meccatronico o di altri campi. Oltre alla classificazione del processo di certificazione e ai tipi di normative che vengono utilizzate in questo molto complesso processo iterativo, un altro altrettanto elemento di progettazione e anche di certificazione, che è fondamentale nella vita dei system engineering è lo schema a V, o internazionalmente detta V-model. Oggi la V dell'ingegneria dei sistemi è onnipresente in quasi tutti gli ambienti di sviluppo dei sistemi. Ha uno status iconico. Il modello a V, o V-model, enfatizza un approccio piuttosto naturale alla risoluzione dei problemi. Partendo da un livello grezzo e complesso iniziale il problema viene suddiviso in parti che possono più facilmente gestibili. Ogni livello è integrato con l'altro, da quello finale a quello iniziale. A ogni livello, è possibile confrontare la soluzione o parte di essa con il problema o con la relativa parte a quel problema. [7] Questo permette al modello di essere sempre, o quasi, al passo con i tempi e con le nuove tecnologie, come è stato detto precedentemente, che crescono e progrediscono in maniera superlativa. E quindi permette di avvicinare la progettazione e la certificazione all'uso di queste nuove tecnologie che si stanno affacciando al nostro tempo. La semplicità di questo modello consente varie proiezioni e dà luogo a molte interpretazioni. Il modello a V è quindi una rappresentazione grafica del ciclo di vita dello sviluppo di un sistema. Viene utilizzato principalmente per produrre modelli rigorosi del ciclo di vita dello sviluppo e modelli di gestione dei progetti dei sistemi complessi. Descrive le attività da svolgere e i risultati che devono essere prodotti durante lo sviluppo del prodotto. Come riportato in figura, il modello a V è diviso in due parti (*come una normale lettera V dell'alfabeto latino*). (figura 2 e figura 3)

Il lato sinistro della "V" rappresenta la scomposizione dei requisiti e la creazione di specifiche di sistema. Il lato destro della "V" rappresenta l'integrazione delle parti e la loro verifica e convalida. Non è però corretto al 100% dire che solo nella parte destra c'è la convalida. Infatti, i requisiti devono essere convalidati prima rispetto ai requisiti di livello superiore o alle esigenze degli utenti. Inoltre, c'è anche un ulteriore elemento come la convalida dei modelli di sistema. Questo può essere fatto parzialmente anche sul lato sinistro. Il modo più semplice è dire che la verifica è sempre per i requisiti (*termini tecnici*) e la convalida sempre per il mondo reale o le esigenze dell'utente. Lo standard aerospaziale RTCA DO-178B afferma che i requisiti sono convalidati, confermati come veri, e il prodotto finale viene verificato per garantire che soddisfi tali requisiti. Si può spiegare meglio la distinzione tra convalida e verifica con delle domande. La convalida può essere espressa dalla domanda "Stai costruendo la cosa giusta?" e la verifica da "La stai costruendo bene?". Ma per essere più tecnici e precisi la guida PMBOK, adottata anche dall'IEEE come standard li definisce come segue nella sua 4° edizione: [8]

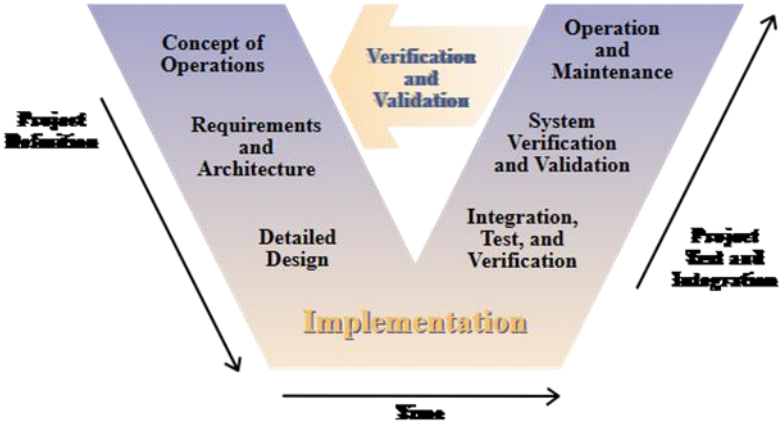


FIGURA 2

"*Convalida: La garanzia che un prodotto, un servizio o un sistema soddisfi le esigenze del cliente e di altre parti interessate e identificate. Spesso comporta l'accettazione e l'idoneità con i clienti esterni. Si frappone in contrasto con la verifica."*
"Verifica: La valutazione della conformità o meno di un prodotto, servizio o sistema a una normativa, un requisito, una specifica o una condizione imposta. Spesso è un processo interno al progetto. Si frappone in contrasto con la convalida."

Il modello V non è unico, ne esistono di diversi tipi e rappresentazioni, ma si possono definire tre grandi categorie, il V-Modell tedesco, un modello di test generale e lo standard del governo degli Stati Uniti.

Il V-model nasce e fornisce indicazioni per la pianificazione e la realizzazione dei progetti principalmente complessi. Permette di raggiungere i seguenti obiettivi nella progettazione di un sistema:

- Minimizzazione dei rischi del progetto: il modello a V migliora la trasparenza e il controllo del progetto specificando approcci che sono standardizzati e descrivendo i risultati corrispondenti e i ruoli responsabili. Consente poi un riconoscimento delle deviazioni e dei rischi di pianificazione nella fase iniziale del progetto e migliora la gestione dei processi, riducendo così il rischio che può sorgere successivamente.
- Miglioramento e garanzia della qualità: essendo un modello con dei processi standardizzati, il modello V assicura che i risultati che devono essere raggiunti siano completi e abbiano la qualità desiderata. I risultati provvisori definiti possono essere verificati in una fase iniziale. Dei contenuti uniformi dei prodotti potranno migliorare la leggibilità, la comprensibilità e la verificabilità.
- Riduzione dei costi totali durante l'intero ciclo di vita del progetto e del sistema: lo sforzo e i costi per lo sviluppo, la produzione, il funzionamento e la manutenzione di un sistema può essere

calcolato, stimato e controllato in modo trasparente applicando un modello di processo standardizzato. I risultati ottenuti saranno uniformi e facilmente rintracciabili. Ciò potrà ridurre la dipendenza dell'acquirente dal fornitore e lo sforzo per le attività e i progetti successivi.

- Miglioramento della comunicazione tra tutte le parti interessate: la descrizione e l'aspetto standardizzato e uniforme di tutti gli elementi e termini rilevanti è la base per permettere una comprensione reciproca tra tutte le parti interessate. Pertanto, la perdita di risposta e di comunicazione corretta tra utente, acquirente, fornitore e sviluppatore è ridotta.

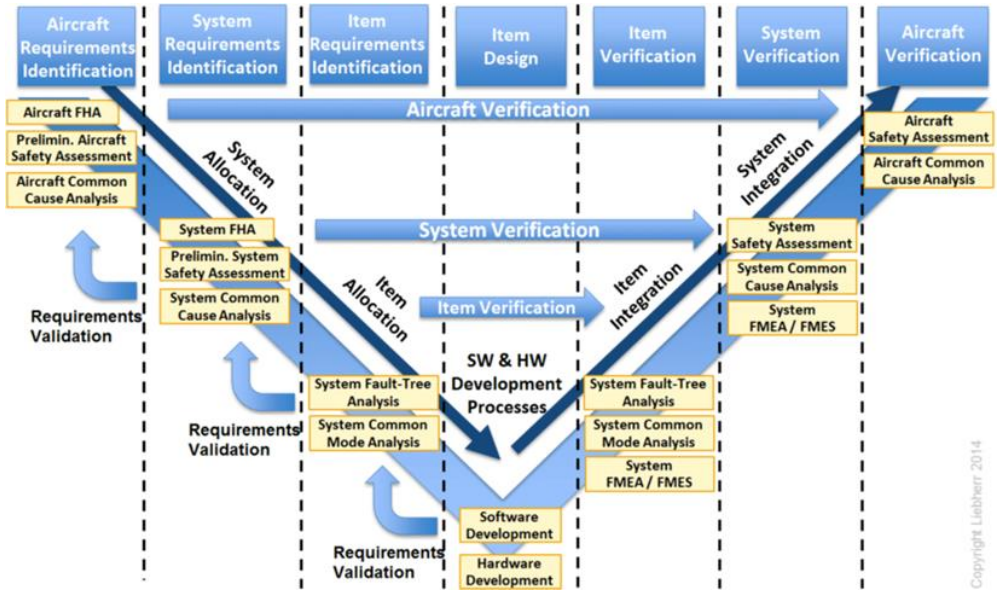


FIGURA 3

Come si è visto, i vantaggi che il V-model offre rispetto ad altri modelli di sviluppo dei sistemi è notevole e sono:

- Il V-model fornisce un'assistenza concreta su come implementare un'attività e le sue fasi di lavoro, definendo esplicitamente e in maniera trasparente gli eventi necessari per completare una fase di lavoro: ogni schema di attività contiene istruzioni, raccomandazioni e spiegazioni dettagliate dell'attività.
- Gli utenti del V-model partecipano attivamente allo sviluppo e alla manutenzione del V-model.

Però nonostante tutto, non esiste niente di perfetto a questo mondo, e anche i sistemi e modelli così ottimi e performanti hanno dei limiti e delle imperfezioni. Per alcuni aspetti il modello a V deve essere regolato o adottato o modificato di conseguenza

- L'inoltro dei contratti per servizi non è regolamentato dal modello.
- L'organizzazione e l'esecuzione del funzionamento, la manutenzione, la riparazione e lo smaltimento del sistema non sono coperti dal modello V. Tuttavia, la pianificazione e la preparazione di un concetto per questi compiti sono regolate nel modello V.
- Il modello V riguarda lo sviluppo del software all'interno di un progetto piuttosto che di un'intera organizzazione.

Comunque, il modello a V è veramente un modello che aiuta gli ingegneri di sistema e i certificatori a progettare e regolare un sistema complesso, quali sono quelli dei giorni attuali e le nuove sfide ingegneristiche che sono all'orizzonte. Il modello V è emerso probabilmente negli anni '60, anche se non sembrano esserci citazioni pubbliche disponibili. Nel 1979, Barry W. Boehm pubblicò un articolo che si basava sul modello a V. Utilizzò la V nel contesto dell'ingegneria del software per sottolineare l'importanza della verifica e della convalida. Boehm, all'epoca, fece una distinzione tra una parte superiore della V per la convalida e una parte inferiore della Vee per la verifica e la validazione e ha collegato questi processi rispettivamente ai requisiti e alle specifiche. (figura 3). La natura multilivello dei sistemi dei sistemi

rappresentati nella V non è stata poi ulteriormente rielaborata. Boehm ha attribuito la "V-Chart", alla comunicazione personale di J.B. Munson, System Development Corporation nel 1977. In un contesto sistemistico, la "V-Chart" è stata presentata alla prima conferenza annuale di NCOSE nel 1991. Nel 1992, poi, la Germania ha pubblicato uno standard per i progetti di carattere governativo. A quanto pare, lo standard ha avuto origine dal Ministero della Difesa ed è stato stabilito nei primissimi anni '90 o anche prima. Questo standard, nella sua versione completa, è una descrizione del processo, denominata "V-Modell®". La V, nonostante una prima impressione sulla effettiva figura, non sta per la rappresentazione grafica del modello di processo, ma è un'abbreviazione del termine tedesco "Vorgehensmodell", che potrebbe essere tradotto come "modello di processo". Ma, ironicamente, i processi descritti sono rappresentati con una forma a V. L'edizione del 1992 riguardava solo lo sviluppo di software. È stata resa disponibile al pubblico da Bröhl e Dröschel in "Das V-Modell" nel 1993. Un'ulteriore edizione sviluppata del "V-Modell®", pubblicata nel 1997, comprendeva aspetti di sistema con riferimenti alla definizione di sistema della norma ISO 12207.Lo standard, poi, si è evoluto ed è diventato il "V-Modell® XT", con la sigla XT che sta per estensibile oppure anche per estrema personalizzazione. Al Simposio internazionale INCOSE 2013, Dieter Scheithauer e Kevin Forsberg hanno presentato il documento "V-Model Views". Questo documento raccoglie le esperienze e i miglioramenti dei due decenni precedenti. Gli autori estendono l'ambito del Modello V dal processo di sviluppo al ciclo di vita del prodotto e del sistema, passando dai bisogni ed esigenze delle parti interessate fino alla loro soddisfazione. Rispetto al 1991, questa versione suddivide la visione complessiva in quattro viste distinte: Base-V, Sviluppo-V, Garanzia-V e Dinamica-V. Trasforma, inoltre, la dimensione orizzontale da una sequenza temporale o di maturità del progetto a una sequenza logica. Scheithauer e Forsberg enfatizzano la progettazione del lato sinistro della V in opposizione alla decomposizione imposta da una cascata. E infine mostrano come la validazione non si applica solo al sistema finale ma anche ad ogni elemento lungo il ciclo di vita del sistema. Ovvero, i requisiti delle parti interessate, i requisiti di sistema, l'architettura a ogni livello e integrati nell'intera architettura del sistema e nel sistema operativo devono essere convalidati e verificati per la loro idoneità allo scopo. Viene affermato che il modello V è stato introdotto due volte, negli anni '80 dalla NASA e con il documento di Forsberg e Mooz nel 1991. Come è stato ampiamente descritto, quindi, il processo di certificazione si inserisce nel processo di ‘verifica’ del modello a V. Siamo tecnicamente, e ufficialmente, nella parte destra del diagramma, della V, ma come è stato detto e dimostrato anche nella parte sinistra si fanno check di verifica, per dimostrare che i requisiti allocati e i design rispettino le norme previste dalla legge. Inoltre, l’integrazione, non solo nella parte destra, ma anche in parte e in contemporanea nella parte sinistra, durante la progettazione, della verifica e del processo di certificazione, permette di velocizzare l’intero processo, abbassando i tempi e soprattutto i costi. L’intero processo certificativo è un processo molto complesso e lungo e, come è stato descritto nei capitoli precedenti, bisogna integrare bene il processo di verifica delle norme e dei requisiti durante la progettazione utilizzando normative e documenti ufficiali e ufficiosi, appositi, che permettono una migliore via di certificazione. Questo lo sia fa anche utilizzando vari modelli di sviluppo di progetti appropriati, come ad esempio il modello a V. Questi capitoli, così abbastanza dettagliati, sul processo certificativo, sulle varie normative utilizzate, sul modello di sviluppo più utilizzato, servono a comprendere al meglio l’obiettivo primario di questo lavoro di tesi, che proprio si basa su questo processo e sulla comprensione di alcune normative e requisiti, che sarà spiegato nel dettaglio nel capitolo successivo.

3. I VINCOLI E LE NORMATIVE

Nei precedenti capitoli sono stati spiegati dettagliatamente il processo certificativo e le sue normative e l'obiettivo del lavoro di Tesi. Bisogna ora andare a sviluppare il concetto di vincolo normativo e studiare quindi le normative per andare ad individuare, nell'ambito dei sistemi di bordo, quali possono essere i vincoli. Quando si progetta un sistema aeronautico bisogna tenere in conto diversi fattori, di ogni genere e appartenenza, missione, task, ambiente operativo, prospettive economiche e industriali, costi e vincoli normativi. I vari vincoli che sono individuati all'interno della CS-25 [16], cioè delle normative ufficiali e anche attraverso le normative ufficiose di EASA, saranno scritti in corsivo e grassetto all'interno del testo della Tesi, in modo da essere facilmente riconoscibili. Il vincolo normativo è un aspetto che indica all'ingegnere dei limiti da imporre al proprio sistema. Non si parla di vincolo meccanico, ma prendiamo in esame l'aspetto legislativo e di diritto, anche se i due ambiti si equivalgono. Prendendo come riferimento il vocabolario ufficiale Treccani, con il termine vincolo normativo si intende:

- "vincolo che impone limitazioni alle posizioni o alle configurazioni possibili di un sistema";
- "obbligo di rispettare determinati equilibri o di restare all'interno di limiti quantitativi ben individuati";
- "Nel linguaggio giuridico, la soggezione ad un obbligo o la limitazione di un diritto".

Il vincolo, quindi, pone dei limiti e degli obblighi legislativi al progetto del sistema in generale. Si può decidere di non seguire questi obblighi, ma poi quando arriverà il momento della certificazione, il sistema progettato non sarà in linea con le leggi vigenti e quindi verrà scartata una sua possibile messa in produzione e utilizzo in ambiente aeronautico. Quindi i vincoli hanno diverse funzioni, tutte volte a creare un sistema che sia il migliore e sicuro per le persone che dovranno usufruirne. I vincoli delimitano la progettazione e l'operatività dei vari sistemi all'interno di aree di sicurezza legislativa, appositamente studiate, valutate e collaudate. Questi vincoli si trovano nelle normative, che sono state ampiamente descritte nel capitolo precedente. I vincoli possono essere di tanti tipi, in base all'elemento che va a vincolare, in base alle caratteristiche che va a controllare. Esistono i vincoli architettonici, che limitano aspetti legati all'architettura di un sistema e al suo funzionamento. Ci sono i vincoli di installazioni, che vanno a limitare e controllare le caratteristiche relative alle installazioni dei vari sistemi nella struttura principale dell'aereo e come essi interagiscono con il sistema principale. I vincoli delle funzioni controllano e limitano le caratteristiche delle funzioni che i vari sistemi devono essere in grado di effettuare durante il loro ciclo di vita. Ci sono i vincoli del controllo qualità e ce ne sono di tanti altri tipi, e ognuno di questi va a individuare una caratteristica che deve osservare e limitare in base alle leggi vigenti e permettere al sistema di operare correttamente. Per quanto riguarda i vincoli di installazione bisogna controllare che le installazioni non provochino failure a cascata, oppure bisogna studiare la cosiddetta ZSA, 'zonal safety analysis' che vuole controllare i sistemi divisi in zone di installazione. Naturalmente i vincoli di installazione non si concludono qui, ma delimitano ancora tante altre cose. I vincoli che analizziamo in questa Tesi sono quelli relativi ai sistemi di bordo, che sono di tanti tipi e diversi tra loro, ma hanno il minimo comune denominatore di essere delimitati da stessi vincoli così particolari. Particolare è la parola corretta perché i vincoli normativi dei sistemi si differenziano molto dai vincoli di altri elementi dell'aereo, come i comandi di volo o le strutture. In questi casi i vincoli sono di facile comprensione per via del fatto che la loro dicitura è abbastanza semplice perché sono elencati range numerici in cui far rientrare le varie caratteristiche che si vogliono implementare e che le strutture e i comandi di volo devono avere. Naturalmente con la parola 'abbastanza semplice' si intende rispetto ai vincoli dei sistemi di bordo, a volte anche i vincoli con i range numerici o formule ben descritte non sono di facile interpretazione per via di alcune variabili difficili e aspetti non sempre chiari. I vincoli che verranno analizzati in questa Tesi sono ancora più complessi da capire ed interpretare. Ci sono ben 2 livelli di comprensione dei vincoli dei sistemi di bordo. Il primo livello riguarda il capire se quello che stiamo leggendo è veramente un vincolo oppure no. A differenza dei vincoli delle strutture o dei comandi volo, i vincoli dei sistemi non hanno quasi mai, o ne hanno poche, di range numerici che possono permettere facilmente di individuare il vincolo stesso. La maggior parte delle volte sono frasi di difficile comprensione, con pochi numeri e molte parole difficili e quindi non sempre si riescono ad individuare al primo colpo questi vincoli. Bisogna leggere con attenzione tutta la normativa e capire se la frase che stiamo leggendo possa essere effettivamente un vincolo di sistema. Si tratta a volte di frasi che potremmo definire filosofiche. Una volta individuato che quella frase rappresenta effettivamente un vincolo sui sistemi di bordo si passa al secondo livello, capire quali sono effettivamente i limiti e gli obblighi che quel vincolo fornisce e definisce. A differenza dei vincoli su altri elementi dell'aereo, quali strutture e comandi di volo e altri, in cui sono

presenti range e valori numerici, quindi di quasi immediata interpretazione, i vincoli sui sistemi sono di difficile comprensione. È ostico comprendere in pieno cosa quella frase voglia effettivamente dire e come quella frase può essere tradotta in un vincolo e in un numero da utilizzare nella progettazione del sistema. Per fare un esempio iniziale (*poi si andranno a vedere nello specifico tutti i vincoli che si è riusciti ad individuare nelle normative con la loro interpretazione*): "*il sistema dei serbatoi deve essere progettato in modo che un singolo guasto non porti ad un evento catastrofico"*. Questa frase, che rappresenta un vincolo architettonico del sistema dei serbatoi, può voler dire tutto e niente e molti vincoli dei sistemi sono rappresentati e scritti in questo modo. Cosa vuol dire che bisogna progettare il sistema in modo che un singolo guasto non porti ad un evento catastrofico? Come si traduce questo in un valore numerico che può essere utilizzato nell'effettiva progettazione del sistema? È facile dire che un guasto non porta a nessun evento catastrofico, ma come lo si dimostra? Cosa vuol dire evento catastrofico? Cos'è un singolo guasto? Come si vede da queste e altre domande che possono essere per questa frase, bisogna saper interpretare al meglio il vincolo in modo da tradurlo dal linguaggio legislativo, di diritto, al linguaggio ingegneristico. A questo servono gli ingegneri certificatori. Il compito di questa tesi è proprio quello di individuare questi vincoli dei sistemi di bordo all'interno della normativa e cercare di tradurli in qualcosa che possano al meglio essere usati nella progettazione e nella verifica dei vari sistemi. Verrà utilizzata in maniera dettagliata e spiegata una matrice molto importante che traduce 'eventi catastrofici' o 'eventi pericolosi' in numeri e range da utilizzare nella progettazione dei sistemi, questa è la matrice di rischio. (figura 4 e figura 5)

Rischio [R]	**Improbabile** [P1]	**Poco probabile** [P2]	**Probabile** [P3]	**Molto probabile** [P4]
Danno lieve [E1]	**Rischio basso** [P1]X[E1]=1	**Rischio basso** [P2]X[E1]=2	**Rischio moderato** [P3]X[E1]=3	**Rischio moderato** [P4]X[E1]=4
Danno significativo [E2]	**Rischio basso** [P1]X[E2]=2	**Rischio moderato** [P2]X[E2]=4	**Rischio medio** [P3]X[E2]=6	**Rischio rilevante** [P4]X[E2]=8
Danno grave [E3]	**Rischio moderato** [P1]X[E3]=3	**Rischio medio** [P2]X[E3]=6	**Rischio rilevante** [P3]X[E3]=9	**Rischio alto** [P4]X[E3]=12
Danno gravissimo [E4]	**Rischio moderato** [P1]X[E4]=4	**Rischio rilevante** [P2]X[E4]=8	**Rischio alto** [P3]X[E4]=12	**Rischio alto** [P4]X[E4]=16

FIGURA 4

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	**Catastrophic (1)**	**Critical (2)**	**Marginal (3)**	**Negligible (4)**
Frequent (A)	**High**	**High**	**Serious**	**Medium**
Probable (B)	**High**	**High**	**Serious**	**Medium**
Occasional (C)	**High**	**Serious**	**Medium**	**Low**
Remote (D)	**Serious**	**Medium**	**Medium**	**Low**
Improbable (E)	**Medium**	**Medium**	**Medium**	**Low**
Eliminated (F)	**Eliminated**			

FIGURA 5

La matrice di rischio (figura 4-5) è costruita tenendo in considerazioni due elementi fondamentali delle failure, probabilità e rischio. Si costruisce la matrice incrociando le possibili combinazioni tra la gravità di un danno e la probabilità che accada. Più un danno è grave e probabile più la progettazione deve essere in grado di evitarlo il più possibile. Nella CS-25, alla pagina 779 del capitolo 25.1309, è presente una matrice simile a quelle presentate sopra, che però indica una cosa molto importante, dove è ammissibile e accettabile una possibile failure nel sistema progettato. Si sa, il rischio zero non esiste, solo se non si vola allora ci sono zero rischi che un aereo cada e i passeggeri muoiano detta in maniera cruda, ma se vogliamo viaggiare e raggiungere parti distanti del mondo dobbiamo considerare un rischio nel nostro sistema e nella nostra progettazione. I vincoli normativi obbligano di mantenere le caratteristiche entro un certo range proprio per permettere di avere un rischio accettabile delle possibili failure. La matrice di rischio ci indica in maniera plastica dove questo rischio è accettabile e dove non lo è. (figura 6) [16]

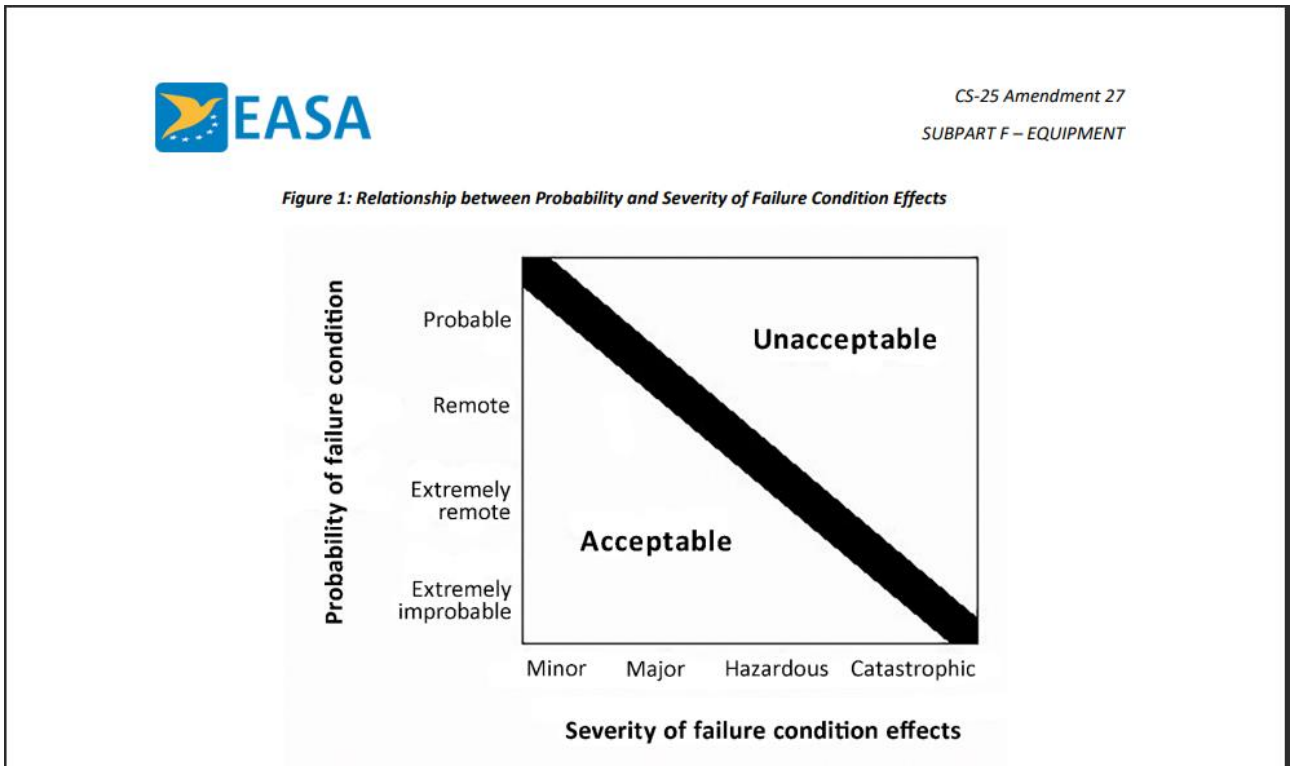


FIGURA 6

La differenza con le precedenti matrici sta solo dove si posizionano gli assi, se in alto o in basso. (figura 6) Comunque, è possibile vedere come i vincoli normativi permettano di accettare un rischio di failure che sia al massimo probabile ma con pochissima gravità o altrimenti estremamente improbabile ma con elevata gravità. Oltre a questa combinazione ogni rischio di failure è inaccettabile e un sistema che possa anche solo eventualmente presentare una possibilità iniziale di rischio di failure di entità elevata non sarà mai presa in considerazione e non sarà mai certificata. Si sa che purtroppo anche i migliori sistemi hanno presentato nel corso della loro vita operativa failure di entità elevata, questo nessuno può prevederlo, nemmeno i migliori vincoli normativi, ma comunque il sistema deve essere progettato per impedire questi eventi. Un elemento fondamentale di questi rischi è capire come valutare che un sistema rispetti i rischi accettabili. Si possono fare ben complessi, ma impossibili da capire oppure semplici ma non robusti. Serve un valore che ci indichi, durante le prove, i test, che il sistema rispetti le considerazioni che la matrice di rischio rileva. I vincoli sui sistemi sono molto labili e poco precisi, e queste diciture 'catastrofico, hazardous, major, probabile o estremamente improbabile' ne sono l'esempio. Quand'è che una failure è catastrofica? E quand'è che è hazardous? E Major? E quand'è che è estremamente improbabile? La normativa ci permette di risolvere questi dubbi sui vincoli dando un significato ben preciso e un range di probabilità. Vediamo innanzitutto cosa è una failure e una failure conditions. Ogni classificazione nella CS-25 è riferita alle failure conditions, alle loro probabilità e alle loro gravità. Dalla CS-25 AMC 25.1309: "*Failure. An occurrence, which affects*

the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: Errors may cause Failures but are not considered to be Failures. Failure Condition. A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events."
La failure è quindi un evento che influisce sul funzionamento di un componente, o una parte di esso, in modo tale che non possa più funzionare come previsto (*questo include sia la perdita di funzione che il malfunzionamento).* Una failure consitions è invece il manifestarsi di una failure. Le failure non sempre si manifestano, possono accadere ma non se ne accorge. La si vede solo tramite le spie nella cabina di pilotaggio e tramite ispezione. Quando i passeggeri e il volo sono compromessi, quindi le failure si sono manifestati agli occhi delle 'persone normali', allora si parla di failure condition. Ogni failure condition può essere classificata in base alla sua severità e insieme alla probabilità viene a crearsi la matrice di rischio. Questa classifica è così composta (*dall'AMC 25.1309 pag 777*):
"(1) No Safety Effect: Failure conditions that would have no effect on safety; for example, failure conditions that would not affect the operational capability of the aeroplane or increase crew workload.
(2) Minor: Failure conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
(3) Major: Failure conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
(4) Hazardous: Failure conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating, conditions to the extent that there would be:
(i) A large reduction in safety margins or functional capabilities;
(ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
(iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
(5) Catastrophic: Failure conditions, which would result in multiple fatalities, usually with the loss of the aeroplane".
Come è possibile notare dalle descrizioni delle gravità delle failure, non sempre i confini tra uno stato di gravità e il successivo sono così ben definiti. Certo, il confine tra l'hazardous e il catastrofico è più marcato, mentre è più labile il confine tra Major e Hazardous. Visto che è fondamentale comprendere quanto grave una failure sia per procedere alla progettazione e alla certificazione, è di fondamentale importanza capire dove si pongono i confini tra una definizione di gravità e l'altra. A volte, come è anche indicato nella normativa, se il confine non è coì ben definito o non è possibile stabilire al 100% se una failure sia Major o Hazardous, spetta all'esperienza e alla conoscenza degli ingegneri stabilire quale sia questo confine e posizionare una failure in quella o quell'altra categoria. L'ingegnere e altri esperti riescono a capire se si tratta di una o l'altra categoria di failure, conducendo ulteriori test o comprendendo meglio le conseguenze reali di quell'eventuale failure nel resto dei sistemi e nel velivolo. La normativa CS-25, oltre a spiegare con la sua scrittura a volte non ben comprensibile, le caratteristiche della gravità delle varie failure, mostra anche la tipologia di probabilità che una failure accada. Sono classificate come segue:
"(1) Probable failure conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane.
(2) Remote failure conditions are those unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type.
(3) Extremely remote failure conditions are those not anticipated to occur to each

aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type.
(4) Extremely improbable failure conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type".

Come per le definizioni delle gravità, anche le definizioni delle probabilità non sempre sono ben definiti. Anche in questo caso può e deve servire e subentrare il fattore umano degli ingegneri che possano meglio comprendere quando una failure è 'remota' o 'estremamente remota'. Le normative dei sistemi di bordo, come è stato descritto nei capitoli precedenti, necessitano sempre di ingegneri esperti nel linguaggio legislativo proprio non ci sono calcoli o numeri o definizioni ben precise. Si parla molto di come l'intelligenza artificiale, che si sta sviluppando in maniera massiccia, possa aiutare o addirittura sostituire vari lavori, in quanto più rapida e precisa della mente umana, ma in questo caso non sarebbe possibile perché serve sempre una mente umana che possa ben comprendere dove e come posizionare i confini tra una categoria e l'altra perché l'AI potrebbe erroneamente sottovalutare o sopravvalutare una possibile failure complicando e danneggiando l'intero progetto. Non dico che l'intelligenza umana sia infallibile e quindi ogni sua decisione di collocare la failure in quella o quell'altra categoria sia perfetta, ma la creatività e l'esperienza umana aiutano dove a volte la rigidezza delle macchine fallisce. Anche un umano può sottovalutare o sopravvalutare una possibile failure, ma 'giocando' sulle probabilità è più probabile che la conoscenza umana riesca a trovare la giusta soluzione o una soluzione accettabile. Ricordiamo sempre che è stata l'intelligenza umana a creare l'intelligenza artificiale e non viceversa. Ma non possiamo solamente fidarci di conoscenze o altro anche perché sia una intelligenza che l'altra hanno bisogno di esperienza e lavoro per maneggiare bene i vincoli e i confini labili tra una categoria di gravità-probabilità e l'altra, quindi per fare esperienza c'è bisogno di lavoro che però porti sempre ad un risultato ottimo o comunque accettabile ed è per questo che per progettare e soprattutto certificare abbiamo bisogno di test e dati oggettivi che dimostrino che un sistema è sicuro. Questi risultati li si dimostrano con dei numeri e quindi la normativa si propone di vincolare le varie categorie con dei range numerici di probabilità, derivati da calcoli. Quindi durante la certificazione, per comprendere sei un sistema è sicuro, in base alla sua categoria di gravità-probabilità, si fa riferimento a dei range ben precisi. Questi dati di probabilità vengono definiti come 'Average probability per flight hour'. La CS-25 descrive questa definizione come: *"Average Probability Per Flight Hour. For the purpose of this AMC, is a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all aeroplanes of the type divided by the anticipated total operating hours of all aeroplanes of that type (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a Failure Condition occurring during a typical flight of mean duration divided by that mean duration)".* Cioè, questi dati di probabilità sono presi in esame dalla predizione che le failure conditions possano accadere durante l'intera vita operativa di quel tipo di aereo preso in esame e questa probabilità viene poi divisa per le ore totali operative di quello stesso tipo di aereo. La probabilità media per ora di volo è normalmente calcolata come la probabilità che si verifichi una condizione di guasto durante un volo tipico di durata media divisa per quella durata media. I dati di probabilità vincolati dalla normativa sono i seguenti:

"(i) Probable failure conditions are those having average probability per flight hour greater than of the order of 1 × 10-5
(ii) Remote failure conditions are those having an average probability per flight hour of the order of 1 × 10-5 or less, but greater than of the order of 1 × 10-7
(iii) Extremely remote failure conditions are those having an average probability per flight hour of the order of 1 × 10-7 or less, but greater than of the order of 1 × 10-9
(iv) Extremely improbable failure conditions are those having an average probability per flight hour of the order of 1 × 10-9 or less".

Si vede come il minino da ottenere per le failure conditions, partendo da quelle probabili, sia 10E-5, fino ad arrivare a quelle estremamente improbabili che devono avere valore di 10E-9. Il range delle failure deve essere per forza questo. Essendo questi dati presi dalla CS-25, per gli aerei di grandi dimensioni, ci sono delle differenze per quanto riguarda gli aerei di piccole dimensioni, i cui dati sono nella CS-23. In quel caso si parte da un valore di 10E-4 per le failure probabili e si arriva a 10E-7 per le failure estremamente improbabili. Quindi si possono avere differenze, non così marcate. Bisogna sempre garantire la sicurezza che è tipica del viaggio aereo. E questa sicurezza deriva proprio dai vincoli così restrittivi nella progettazione e

nella successiva certificazione. Con questi dati è più immediato arrivare a conclusione se un sistema è sicuro o no, dopotutto anche se i vincoli sui sistemi hanno un linguaggio molto 'burocratico' hanno sempre dei numeri precisi su cui fare affidamento e lo si vedrà anche per altri vincoli sui sistemi di bordo, così come lo sono i vincoli di altri elementi, come le strutture o i comandi di volo. Come si può Vedere nella prima delle due figure di seguito (*preso dall'AMC della CS-25.1309) (la figura e la relativa tabella 2a)* gli effetti delle failure conditions sono catalogate e classificate in base alla loro gravità. Gli effetti sono raggruppati in tre gruppi, effetti sul velivolo, effetti sui passeggeri escluso l'equipaggio ed effetti sull'equipaggio. In questi tre gruppi (*aereo, passeggeri ed equipaggio*) ci sono gli effetti che le failure conditions possono provocare e vengono quindi classificate e indicate in base alla gravità di ognuno degli avvenimenti. Quindi ad esempio per il velivolo, una failure che porti una significativa riduzione delle capacità funzionali e del saftey margins viene classificato come 'Major'. Mentre sui passeggeri, una failure che comporti una seria o fatale ferita ad un piccolo numero di passeggeri o ai piloti è indicata come 'Hazardous'. Per quanto riguarda il solo equipaggio, una failure che comporti un aumento anche piccolo di carico di lavoro è classificata come 'Minor'. Nella seconda delle due figure (con la tabella 2b, presente anche nella prima figura) sono presenti i range di probabilità di ogni tipo di classificazione delle failure conditions. Indica quale valore numerico viene inserita una failure catalogata come 'Hazardous' o 'Catastrophic'. Questo è molto importante perché nel corso dell'intera normativa sui sistemi di bordo e i relativi vincoli sono presenti solo la classificazione in parole e grazie a questa tabella è possibile comprendere a che valore corrispondono le varie descrizioni delle failure. (figura 7 e figura 8) [16]

b. The classification of the failure conditions associated with the severity of their effects are described in Figure 2a.

The safety objectives associated with failure conditions are described in Figure 2b.

Figure 2a: Relationship Between Severity of the Effects and Classification of Failure Conditions

Severity of the Effects						
	Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
	Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
	Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of Failure Conditions		No Safety Effect	Minor	Major	Hazardous	Catastrophic

Figure 2b: Relationship Between Classification of Failure Conditions and Probability

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Qualitative Probability	No Probability Requirement	<-Probable->	<--Remote-->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability:	No Probability Requirement	<----------> $<10^{-3}$	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$

Annex to ED Decision 2021/015/R *Page 779 of 1389*

FIGURA 7

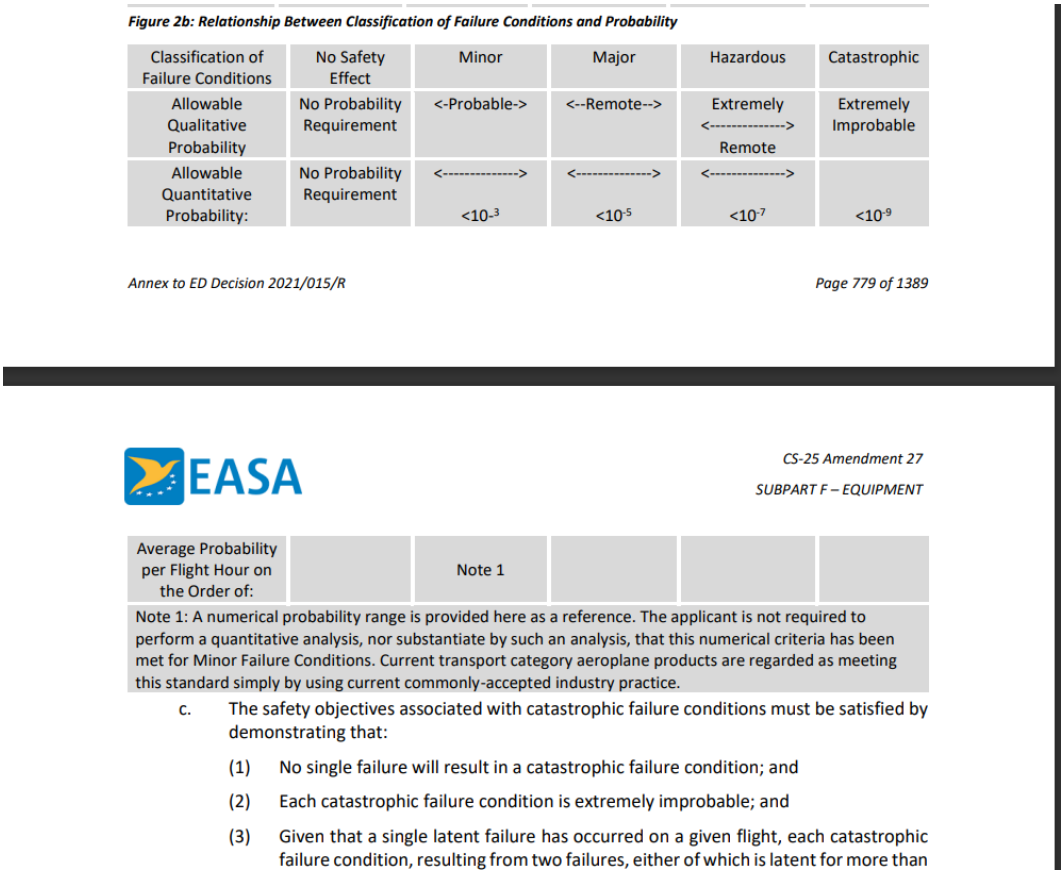


Figure 2b: Relationship Between Classification of Failure Conditions and Probability

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Qualitative Probability	No Probability Requirement	<-Probable->	<--Remote-->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability:	No Probability Requirement	<----------> $<10^{-3}$	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$

Annex to ED Decision 2021/015/R *Page 779 of 1389*

EASA

CS-25 Amendment 27

SUBPART F – EQUIPMENT

Average Probability per Flight Hour on the Order of:		Note 1			

Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

c. The safety objectives associated with catastrophic failure conditions must be satisfied by demonstrating that:

(1) No single failure will result in a catastrophic failure condition; and

(2) Each catastrophic failure condition is extremely improbable; and

(3) Given that a single latent failure has occurred on a given flight, each catastrophic failure condition, resulting from two failures, either of which is latent for more than

FIGURA 8

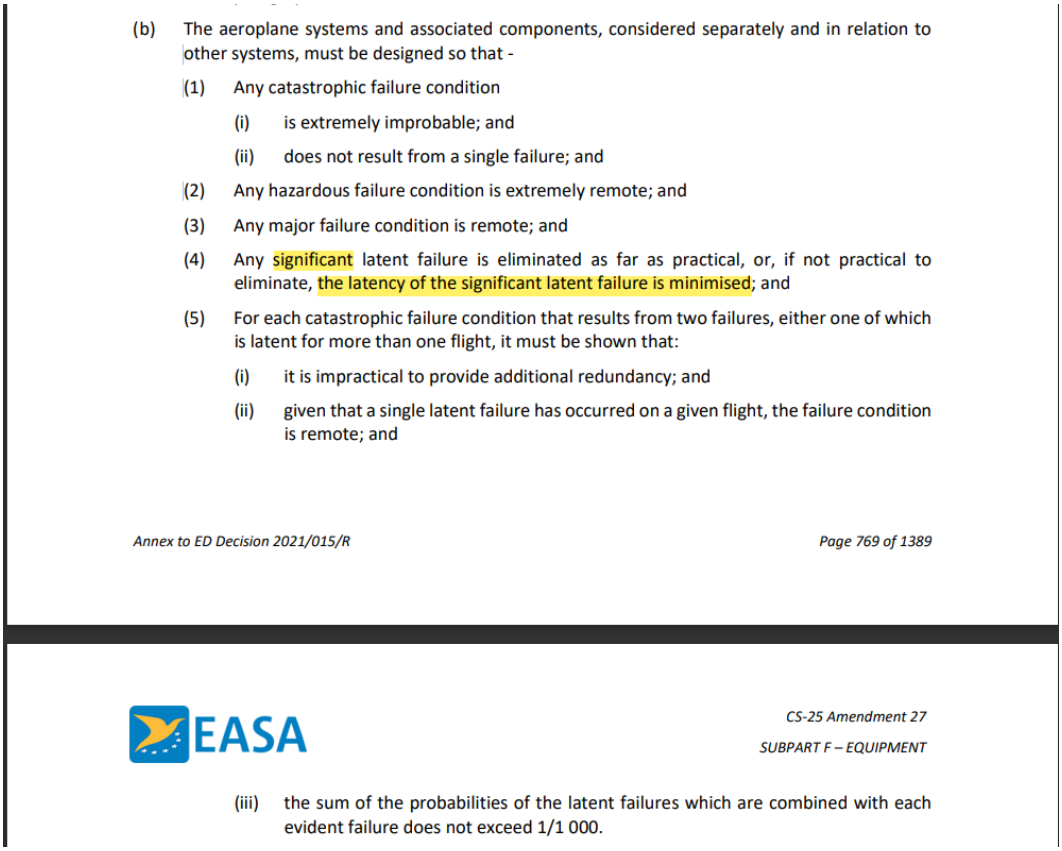
Come si può vedere dalle figure 7-8 i gradi di probabilità vengono indicati come una probabilità media per ora di volo, che devono essere in valori e range molto specifici e molto restrittivi. Questo è anche uno dei tanti elementi che rendono il trasporto aereo uno dei più sicuri al mondo, proprio per la ristrettezza e le limitazioni imposte dalle normative, che garantiscono una operabilità eccellente con pochissimi incidenti. Il massimo consentito di probabilità e guasti è un numero molto particolare e anche abbastanza controverso, cioè 10E-9. Questo è un valore che è stato preso in base ad alcune considerazioni importanti che è utile fare. Bisogna capire come si è arrivati a quel valore, che rappresenta il simbolo della sicurezza dei sistemi di bordo. *"No transportation system has figured out a way of becoming even safer than 10E-7"* (Sidney Dekker, 2005). Dekker è un grande esperto che agli inizi del millennio affermava questa importante concezione e cioè che non si può arrivare oltre il 10E-7, perché è praticamente impossibile. Allora come mai EASA e FAA, le due grandi agenzie certificatrici, pretendono un numero così elevato? La CS-25 [16] recita così per quanto riguarda i valori numerici di probabilità delle failure conditions: "*In assessing the acceptability of a design it was recognised that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 % of the total were attributed to failure conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1 × 10-7 per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason, it was assumed, arbitrarily, that there are about one hundred potential failure conditions in an aeroplane, which could be catastrophic. The target allowable average probability per flight hour of 1 × 10-7 was thus apportioned equally among these failure conditions, resulting in an allocation of not greater than 1 × 10-9 to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1 × 10-9, which establishes an*

approximate probability value for the term 'extremely improbable'. Failure conditions having less severe effects could be relatively more likely to occur".
La safety, a differenza di altri vincoli strutturali, non si misura con un numero, ma con una procedura di mitigazione del rischio. Con i numeri si vanno a rappresentare la probabilità di accadimento di eventi. Il requisito della CS-25.1309 non mostra in modo esplicito il valore di 10E-9, ma compare solo quando parliamo di eventi catastrofici. Non potendo arrivare a 10E-7, bisogna ipotizzare di avere 10E-6. L'ingegnere progettista crea un progetto garantendo un prodotto che garantisca una probabilità di failure condition catastrofiche di 10E-6. Il progetto, la produzione, le operazioni, la manutenzione, e molte altre operazioni del velivolo sono svolte da umani. Possono compiere errori e indurre incidenti. Solo il 10% degli errori catastrofici, che portano quindi ad aventi catastrofici e mortali, sono dovute a problemi puramente tecnici, il resto delle volte è dovuto ad errori umani. Il pilota è una barriera di sicurezza, perché, grazie alla sua esperienza e capacità, può salvare la situazione quando la tecnologia fallisce. Per questo è ancora di fondamentale importanza addestrare i piloti, anche se la tecnologia continua a migliorare, bisogna sempre avere una barriera che provi ad impedire eventi catastrofici tecnici. In caso di failure del sistema che porterebbe a una failure condition, con probabilità di 10E-4, introduco una procedura di emergenza che il pilota deve applicare in condizioni anomale. Deve esserci comunque un certo tempo concesso al pilota, in cui lui sia in grado di riconoscere il problema ed agire per contrastare il problema. In fase di TO/LND ho tempi per agire di circa 3s, mentre in volo 10s, in quanto in fasi di ascesa e discesa ho maggiore rischio di incidenti per la vicinanza al suolo. In un velivolo abbiamo di solito 100 failure condition catastrofiche, quindi passo da 10E-9 fino a 10E-7. Considerando il tasso di guasto di 10E-1 dei sistemi, arriviamo a 10E-6. In velivoli di categorie minori possiamo accontentarci di probabilità di evento catastrofico maggiore, sull'ordine di 10E-4. Più dell'80% degli incidenti è causato dall'errore umano, ed è per questo che si cerca di fare il possibile per migliorare il sistema e l'addestramento dei piloti. In questa Tesi si andranno a sviluppare ed individuare i vincoli normativi dei sistemi di bordo relativi all'architettura in generale. Quali devono essere i limiti e gli obblighi dell'architettura. Da questo tipo di ricerca poi possono nascere lavori futuri relativi ad altre tipologie di vincoli, che si potranno accennare nel capitolo conclusivo sui lavori futuri.

3.1 CS-25.1309 E I VINCOLI NORMATIVI DEI SISTEMI DI BORDO

Nel paragrafo precedente si è visto come una delle normative centrali e più importanti da cui ricavare i vari vincoli architettonici normativi è la CS-25 (*di cui si è parlato nel capitolo delle normative)*. Nella CS-25, alcuni sono i capitoli importanti in cui sono inseriti i vari vincoli normativi dei sistemi di bordo. Il più importante di questi è senza dubbio il 25.1309 e il suo corrispettivo AMC 25.1309. alcuni vincoli sono stati mostrati nel paragrafo precedente per poter comprendere al meglio alcuni elementi dei vincoli stessi e comprendere come essi non siano sempre di facile interpretazione. In questo paragrafo si andranno ad elencare tutti i vari vincoli normativi trovati all'interno del 1309. Se saranno presenti vincoli architettonici dei sistemi di bordo anche da altri capitoli, verranno adeguatamente inseriti con i propri riferimenti. L'intero capitolo della CS-25.1309 è diviso in due parti, il capitolo effettivo e il relativo AMC (*come spiegato nel capitolo dedicato*). Il capitolo effettivo è lungo circa una pagina, in cui sono presenti i vincoli effettivi e rischisti dall'EASA per la certificazione. Mentre l'AMC, lunga circa 30 pagine, presenta la spiegazione dei vincoli ufficiali, insieme ad altri vincoli propedeutici a quelli ufficiali. I vincoli ufficiali non sono tanti, ma sono veramente poco comprensibili e abbastanza vaghi. I vincoli e le spiegazioni dell'AMC servono a comprendere meglio i vincoli ufficiali e migliorare il sistema con altri vincoli. I vincoli dei sistemi di bordo dell'effettivo capitolo CS-25.1309 sono i seguenti (*come mostrato anche nella figura 9*) [16]:
"(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -
(1) Any catastrophic failure condition
(i) is extremely improbable; and
(ii) does not result from a single failure; and
(2) Any hazardous failure condition is extremely remote; and
(3) Any major failure condition is remote; and

(4) Any significant latent failure is eliminated as far as practical, or, if not practical to eliminate, the latency of the significant latent failure is minimised; and
(5) For each catastrophic failure condition that results from two failures, either one of which is latent for more than one flight, it must be shown that:
(i) it is impractical to provide additional redundancy; and
(ii) given that a single latent failure has occurred on a given flight, the failure condition is remote; and
(iii) the sum of the probabilities of the latent failures which are combined with each evident failure does not exceed 1/1 000."



(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote; and

(4) Any significant latent failure is eliminated as far as practical, or, if not practical to eliminate, the latency of the significant latent failure is minimised; and

(5) For each catastrophic failure condition that results from two failures, either one of which is latent for more than one flight, it must be shown that:

(i) it is impractical to provide additional redundancy; and

(ii) given that a single latent failure has occurred on a given flight, the failure condition is remote; and

Annex to ED Decision 2021/015/R *Page 769 of 1389*

EASA

CS-25 Amendment 27

SUBPART F – EQUIPMENT

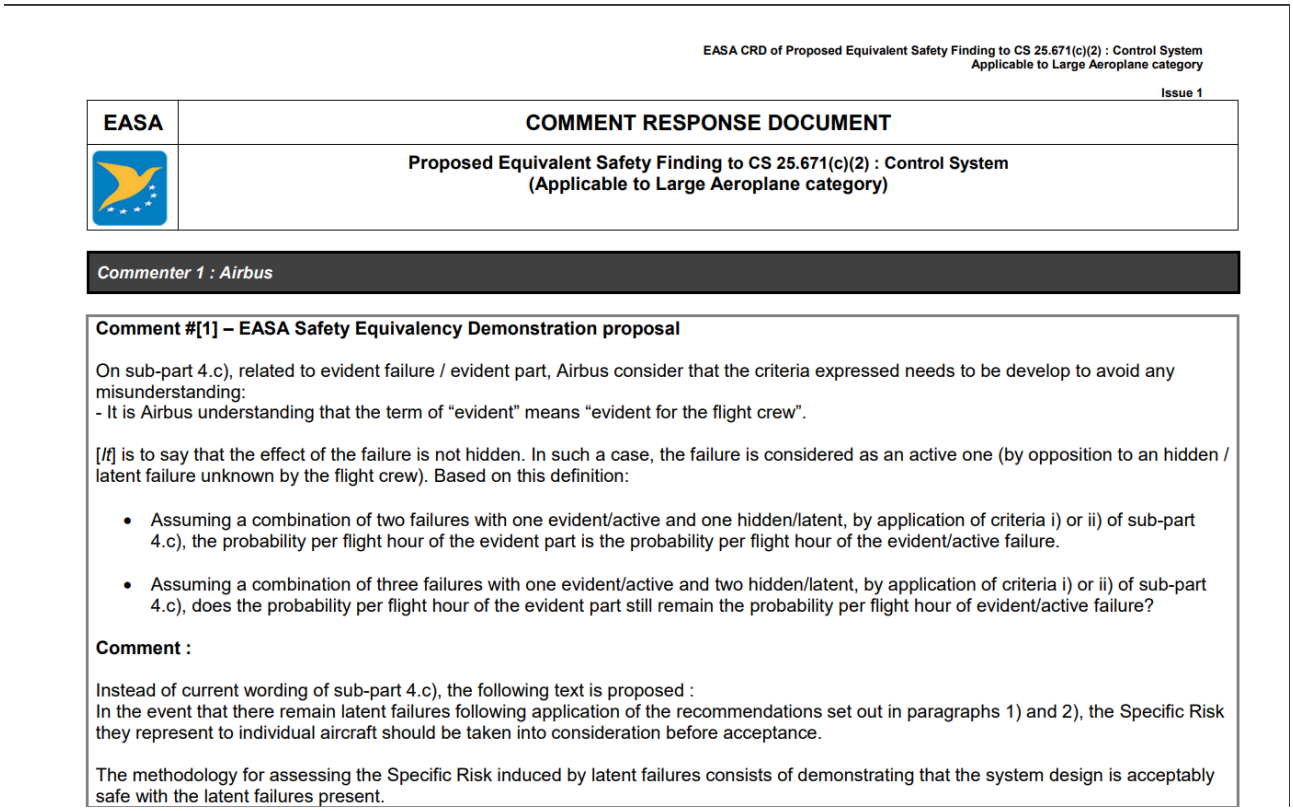
(iii) the sum of the probabilities of the latent failures which are combined with each evident failure does not exceed 1/1 000.

FIGURA 9

Iniziando dal punto (b). Questi rappresentano i vincoli principali per i sistemi di bordo della CS-25. In dettaglio si parte con una dicitura molto generale in cui si citano i sistemi dell'aereo e i suoi componenti che devono essere considerati in maniera separata e in relazione con gli altri sistemi. Oggigiorno i sistemi non sono più progettati, inseriti e non lavorano più separatamente ('*in dei silos separati nell'aereo', come diceva un esperto aeronautico anni fa*) ma lavorano in maniera sinergica con tutti gli altri sistemi dell'aereo, in un'ottica sempre più elettrica e meno idraulica. Quindi ogni sistema deve sempre essere considerato in maniera singola per progettarlo nel migliore dei modi e allo stesso tempo inserito nel grande sistema dell'aereo per comprendere meglio il suo funzionamento nel velivolo e capire come eventuali failure del sistema o di altri sistemi interagiscono e propagano. Andando al punto (1). Questi sistemi, con tutte le considerazioni fatte, devono essere progettati in modo che un evento catastrofico sia un evento estremamente improbabile e non sia il risultato di un singolo guasto. Con il termine estremamente improbabile si indica un evento alla 10E-9, come ampiamente detto descritto. Con la dicitura 'non risultante da un singolo guasto' sta a significare che: "*The potential hazards to the aeroplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions*"; cioè che un evento catastrofico deve essere il risultato di più guasti di più sistemi. Bisogna progettare i sistemi in modo che I guasti di un solo sistema non porti a nessun evento catastrofico e che nemmeno nessun guasto deve portare ad una failure

conditions catastrofica. Dai punti (2) e (3) si spiega come ogni evento di tipo 'hazardous' deve essere estremamente remoto, cioè, 10E-7, mentre gli eventi di tipo 'Major' devono essere di tipo remoto, cioè, 10E-5. A differenza delle failure conditions catastrofiche che non devono scaturire da un singolo guasto, questa cosa non viene specificata per gli hazardous e i major; quindi, in linea di massima potrebbero scaturire da un singolo guasto. L'obiettivo comunque è quello di creare un sistema che in nessun modo da un singolo guasto questi provochi failure conditions visibili. Il punto (4) introduce il concetto di latent failure, hidden failure. Queste failure sono abbastanza particolari e di enorme interesse e attenzione. Per spiegare questo vincolo bisogna cercare di capire cosa sono le hidden failue o latent failure. La CS-25 da una definizione di queste failure: "*Latent Failure. A failure is latent until it is made known to the flight crew or maintenance* personnel". Un'altra definizione dice: "*Significant Latent Failure. A latent failure that would, in combination with one or more specific failure(s) or event(s), result in a hazardous or catastrophic failure condition".* Una latent failure è un guasto che non risulta conosciuto dai membri dell'equipaggio o dal personale della manutenzione. Finché una failure non è conosciuta allora si dice latente. Una '*significante latent failure'* è invece una latent failure che non è isolata ma può creare in combinazione con altre failure, evidenti o no, o altre cause, può portare a failure conditions hazardous o catastrofiche. Il vincolo in questione, quindi, pone un bivio sulle latent failure, o eliminarle del tutto oppure, se non è possibile, cercare di minimizzare le loro possibili combinazioni con altre failure. Più avanti si cercherà di comprendere meglio le latent failure. Nel punto (5) si ha l'ultimo vincolo ufficiale della 25.1309. questo vincolo spiega come per ogni failure condition di tipo catastrofico, 10E-9, che però scaturisce da due guasti, di cui uno di tipo latent, allora bisogna mostrare alcune caratteristiche. La prima è che impraticabile inserire ulteriori ridondanze. La CS-25 definisce così le ridondanze: "*Redundancy. The presence of more than one independent means for accomplishing a given function or flight operation*". Una ridondanza è l'inserimento di un Sistema indipendente che svolga la stessa funzione del sistema principale. Ci possono essere ridondanze di vario genere, attive, passive, funzionali. Tutte hanno in comune la creazione di più sistemi che possano svolgere la funzione nel caso il sistema principale non sia più in grado di farlo. Questo aumenta molto l'affidabilità del velivolo e permette di diminuire la probabilità che una failure conditions avvenga, permettendo di arrivare a quel valore di normativa. Il problema è che non si può riempire l'aereo di ridondanze perché aumenterebbero i costi e il peso e il lavoro di manutenzione. Quindi bisogna stare molto attenti nel capire quante ridondanze inserire per ogni sistema. Il vincolo (5.i) dice questo e cioè che non è praticabile inserire troppe ridondanze nel caso una laten failure si combini con altre failure e porti ad un evento catastrofico. Il (5.ii) impone che un singolo guasto latent che porti ad una failure condition sia remota, quindi 10E-5. L'ultimo vincolo (5.iii) impone di considerare la somma probabilistica di una latent failure con una evident failure non superiore a 1/1000. Quindi bisogna considerare le combinazioni di failure per quel dato sistema e confermare che la somma tra una latent ed una evident non superi 1/1000. Questi rappresentano i vincoli principali della CS-25.1309, quelli che un progettista deve obbligatoriamente considerare nel suo sistema e che il certificatore deve accertarsi. Ma l'AMC corrispondente mostra altri vincoli più piccoli e meno articolati, ma anche di più difficile comprensione. Ma prima di vedere i vincoli architettonici dell'AMC è giusto soffermarsi su cosa siano effettivamente le latent failure e le evident failure. La CS lo spiega non in maniera completa, perciò, dopo le sollecitazioni di aziende aeronautiche, l'EASA ha rilasciato una risposta sulle latent failure, che sono le figure di seguito. Le failure evident sono quelle failure evidenti, conosciuto all'equipaggio e agli addetti della manutenzione. Mentre le hidden failure sono quelle failure nascoste, di cui non si conoscono i connotati ma che possono essere presenti e avvenire in un sistema, e quindi sconosciuti all'equipaggio e agli operatori di manutenzione. A volte non è facile definire in maniera univoca cosa sia o no le latent failure (*nota. La CS-25 afferma che latent e hidden hanno lo stesso significato e quindi possono essere usati in maniera uguale, ma per i sistemi di bordo utilizza il termine latent*). Quindi bisogna cercare sempre di mettere in considerazione una failure la cui natura non è pienamente compresa. Un elemento di enorme rileva sulla progettazione e sulla certificazione è capire come interpretare le probabilità di failure consition per quanto riguarda le combinazioni tra latent failure ed evident failure. Ci sono vincoli che trattano questo, ed è giusto cercare di comprendere e spiegare cosa comporta nella sicurezza queste tipo di combinazioni delle laten failure. Ce ne sono varie e la normativa, tramite le leggi ma anche tramite sessioni di domanda e risposta tra le aziende aeronautiche e l'EASA, cerca di darne sempre una rappresentazione, potremmo dire chiara, ma non è sempre così. I comment response document delle figure di seguito mostrano una serie di interazioni tra Airbus e Boeing proprio sul concetto delle latent failure e le loro combinazioni, nel caso dei sistemi, sia quelli di bordo che quelli di controllo [10]. Vengono indicate le combinazioni e le loro probabilità. Viene

indicato che, per quanto riguarda le failure combinate di cui una o entrambe sono latent che portano a eventi catastrofici devono essere eliminati dal design del sistema (*note. In questa sessione di domande e risposte l'EASA ha accettato di rimuovere il termine 'entrambe' per evitare ulteriori confusioni. Tutto questo a riprova di come i vincoli dei sistemi siano molte volte confusionari e di difficile interpretazione*). Bisogna vedere e comprendere i var vincoli relativi alle latent failure che andremo a vedere ed individuare, sia tramite la normativa ufficiale CS-25 che tramite normative al di fuori di quelle propriamente ufficiali. Tutto quello prodotto da EASA serve a migliorare l'interpretazione di vincoli abbastanza confusionari. (figure 10-11-12-13-14) [10]



EASA CRD of Proposed Equivalent Safety Finding to CS 25.671(c)(2) : Control System
Applicable to Large Aeroplane category

Issue 1

EASA	COMMENT RESPONSE DOCUMENT
	Proposed Equivalent Safety Finding to CS 25.671(c)(2) : Control System (Applicable to Large Aeroplane category)

Commenter 1 : Airbus

Comment #[1] – EASA Safety Equivalency Demonstration proposal

On sub-part 4.c), related to evident failure / evident part, Airbus consider that the criteria expressed needs to be develop to avoid any misunderstanding:
- It is Airbus understanding that the term of "evident" means "evident for the flight crew".

[*It*] is to say that the effect of the failure is not hidden. In such a case, the failure is considered as an active one (by opposition to an hidden / latent failure unknown by the flight crew). Based on this definition:

- Assuming a combination of two failures with one evident/active and one hidden/latent, by application of criteria i) or ii) of sub-part 4.c), the probability per flight hour of the evident part is the probability per flight hour of the evident/active failure.
- Assuming a combination of three failures with one evident/active and two hidden/latent, by application of criteria i) or ii) of sub-part 4.c), does the probability per flight hour of the evident part still remain the probability per flight hour of evident/active failure?

Comment :

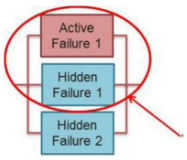
Instead of current wording of sub-part 4.c), the following text is proposed :
In the event that there remain latent failures following application of the recommendations set out in paragraphs 1) and 2), the Specific Risk they represent to individual aircraft should be taken into consideration before acceptance.

The methodology for assessing the Specific Risk induced by latent failures consists of demonstrating that the system design is acceptably safe with the latent failures present.

FIGURA 10

One method of demonstrating that the design is acceptably safe is to assume that any individual failure which is not Extremely Remote (≤ 10^{-7}/fh) and is known to be latent and not detected at each flight or during daily check, has occurred prior to a given flight. During that flight, each Failure Condition which is Catastrophic and which involves that individual failure should be shown to occur at a rate less than or equal to 10^{-6} /Fh.
In addition, when one active failure is combined with two hidden ones, if advantage is taken from one latent failure to show compliance with this 10^{-6} objective, the cases for which the failure rate of the active part is higher than 10^{-4} per flight hour will be identified to the Authorities. Similarly, each Failure Condition which is Hazardous and which involves that individual failure should be shown to occur at a rate less than or equal to 10^{-4} /fh.

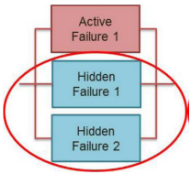
See example :



Assessment of any individual failure not Extremely Remote (≤ 10^{-7}/fh) and known to be hidden and not detected at each flight or during daily check, has occurred prior to a given flight.
Hidden Failure 2 is the individual failure :

- **(A1, H1) ≤ 10^{-6} /fh (CAT) / 10^{-4} /fh (HAZ)**

In the same way, sub-paragraph 4.d) could be illustrated as followed:



To be considered if A1 is the active failure:
- **P(H1, H2) ≤ 10^{-3}**

EASA response:
Noted - request for definition of "Evident". "Latent" is defined in AMC 25.1309 and in the ESF itself. Evident is the opposite.

FIGURA 11

In the sentence "Double failures, with either one or both latent, that can lead to a Catastrophic Failure Condition shall be avoided in system design.", propose to remove the words "or both", as this is confusing.

Proposal is PARTIALLY ACCEPTED - We believe that the proposed wording from Airbus has the same result as the existing Generic ESF, but EASA prefer to keep the existing wording. Airbus could propose to use the above wording for such an ESF on a specific project in the future.
The exception to this is that the exception for Latent failures <1E-07 is not acceptable. The criteria is also to be applied to combinations involving an Extremely Remote individual Latent Failure.

Comment #[2] – EASA Safety Equivalency Demonstration proposal

The term of "*active*" failure is used in the sub-part 4.d).

Comment
Should "*active*" and "*evident*" have the same meaning, Airbus recommend to use uniform term.

EASA response: Agreed
Need to be consistent. Evident is the same as Active, in the context of this ESF. Term "Evident" to be applied consistently.

Commenter 2 : Boeing Commercial Airplanes

Comment #[1} – Statement of issue

Part of the justification for ASAWG ARAC was to harmonize the specific risk related requirements in a way to make them consistent and to reduce the proliferation of inconsistent criteria. This ESF contradicts the criteria developed by the ASAWG ARAC (proposed in NPA 2014-02) and the spirit with which it was developed.

Comment :
The proposed generic ESF to CS 25.671(c)(2) includes additional, new specific quantitative and qualitative 25.671(c)(2) compliance criteria that go significantly beyond the current and draft harmonized 25.671 and 25.1309 rules and advisory material.
These additional criteria have been developed by EASA outside of the Aviation Rulemaking Advisory Committee covering flight control systems and other established rulemaking processes. Therefore, EASA is requested to submit any proposed generic ESF to CS 25.671(c)(2) to the ARAC covering flight control systems for review and development in accordance with established rulemaking processes.

EASA response: Disagreed

FIGURA 12

However, it is not evident that this is sufficient to provide an ESF to the existing CS25.671(c)(2). Therefore, EASA proposes the following approach and additional criteria:

1) *Double failures, with either one or both latent, that can lead to a Catastrophic Failure Condition shall be avoided in system design.*
2) *Latent failures contributing to Hazardous or Catastrophic repercussions should be avoided in system design.*
3) *The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications", as per AMC 25.1309 9.c.6.*
4) *It is recognised that, on occasion, there may be no possibility to comply with the above criteria 1) and 2). In such cases:*
   a) *The deviation shall be recorded and justified in the PSSA/SSA and reviewed during the design review process for acceptance,*
   b) *Acceptance should be based on both previous experience and sound engineering judgement and shall assess:*
      i) *the failure rates and service history of each component,*
      ii) *the inspection type and interval for any component whose failure would be latent, and*
      iii) *any possible common cause of cascading failure modes.*
   c) *The integrity of the evident part of the significant failure condition shall meet a minimum standard:*
      i) *For Catastrophic failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-5}/Fh, and*
      ii) *For Hazardous failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-4}/Fh.*
   d) *In addition, a Specific Risk calculation should be considered in accepting the presence of a latent failure. For each combination composed of one active failure and latent failures and leading to a Catastrophic Failure Condition:*

FIGURA 13

c) *The integrity of the evident part of the significant failure condition shall meet a minimum standard:*
   i) *For Catastrophic failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-5}/Fh, and*
   ii) *For Hazardous failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10^{-4}/Fh.*
d) *In addition, a Specific Risk calculation should be considered in accepting the presence of a latent failure. For each combination composed of one active failure and latent failures and leading to a Catastrophic Failure Condition:*

FIGURA 14

Questa figura rappresenta un vincolo architettonico dei sistemi di bordo riguardante la figura delle latent failure e delle loro combinazioni che possono causare degli eventi catastrofici o hazardous. (figure 13-14)
"A latent failure is one which is inherently undetected when it occurs". [10]
Questa definizione di 'latent failure' è presa dall'AC 25.1309 americano. Le AC sono le advisor circular che spiegano le normative delle FAR americane. Per anni, e bisogna dire, anche oggigiorno l'Europa utilizza molto le AC, come ad esempio l'azienda multinazionale e colosso italiano LEONARDO. I suoi ingegneri, per la certificazione, utilizzano molto le AC, a volte più delle AMC europee. Bisogna dire, per onestà intellettuale, che le AMC europee sono praticamente copiate dalle AC americane; quindi, non ci sono problemi di interpretazione o altro.
"***A significant latent failure is one which would, in combination with one or more other specific failures or events, result in a hazardous failure condition. Because the frequency at which a device is checked directly affects the probability that any latent failure of that device exists."***
Questa definizione, sempre presa dalla AC 25.1309 spiega cosa siano le '*significant latent failure*'. Rappresentano, cioè, la combinazione con altre failure che porta a situazioni di failure conditions hazardous e catastrofiche. Le AMC europee danno una definizione identica. Un'altra spiegazione ancora più accurata delle latent failure e active failure è presa dal paper "ACTIVE AND LATENT FAILURES IN AIRCRAFT GROUND DAMAGE INCIDENTS" di C. Wenner and C. G. Drury della State University of New York at Buffalo, Department of Industrial Engineering, Buffalo, NY 14260: [21]

"The failures caused by those in direct contact with the system, i.e. the mechanics who are working on the aircraft, are considered to be active failures. These failures are errors or violations that have a direct and immediate effect on the system. Generally, the consequences of these active failures are caught by the mechanic himself, or by the defenses, barriers and safeguards built into the maintenance system. Thus, the system must rarely deal with the consequences of active failures. However, when an active failure occurs in conjunction with a breach in the defenses, a more serious incident occurs (Maurino, Reason, Johnston and Lee, 1995)." In campo manutentivo una failure attiva è quella failure che è stata causata da un lavoro diretto sul velivolo e sul sistema. [21]
"Latent failures are those failures which derive from decisions made by supervisors and managers who are separated in both time and space from the physical system. For example, technical writers may write procedures for a task with which they are not totally familiar. If the procedure has even one mistake in it, the mechanic using the procedure will be encouraged to commit an error. The latent failures can often be attributed to the absence or weaknesses of defenses, barriers, and safeguards in the system. Fox (1992) defines latent failures as those decisions made in the organization which may create poor conditions, result in less than adequate training, poor supervision, etc. which may lie dormant for some time, but which have the potential to predispose active failures". In manutenzione una latent failure è quindi quel tipo di failure che non è causato su un lavoro diretto sul sistema, ma è stato causato da inadempienze di diverso tipo all'interno del progetto del sistema, all'interno dell'azienda. Quindi l'origine è lontana nel tempo e nello spazio dal sistema che si guasta. Sono le failure peggiori proprio perché non si conosce la causa vera, l'origine, e possono essere anche delle failure comuni a sistemi progettati nella stessa azienda e con lo stesso metodo. Perciò quando si progetta un sistema di bordo bisogna tenere conto delle possibili failure e lavorare ed elaborare un sistema nel modo più sicuro possibile, non solo con strumenti corretti e buone tecnologie sia dello stato dell'arte sia nuove, ma bisogna anche scrivere nel modo più semplice possibile le procedure tecniche per qualunque evenienza del sistema in modo che sia facilmente comprensibile e non nasca nessun tipo di incomprensione. (figura 15 e figura 16)

Table 1. GDI Hazard Patterns

Hazard Pattern	Number of Incidents			% of Total
Aircraft is Parked at the Hangar/ Gate/ Tarmac	81			62.3
1 Equipment Strikes Aircraft		51		
Tools/Materials Contact Aircraft			4	
Workstand Contacts Aircraft			23	
Ground Equipment is Driven into Aircraft			13	
Unmanned Equipment Rolls into Aircraft			6	
Hangar Doors Closed Onto Aircraft			5	
Aircraft (or Aircraft Part) Moves to Contact Object		30		
Position of Aircraft Components Changes			15	
Center of Gravity Shifts			9	
Aircraft Rolls Forward/Backward			6	
2 Aircraft is Being Towed	49			37.7
Towing Vehicle Strikes Aircraft		5		
Aircraft is Not Properly Configured for Towing		2		
Aircraft Contacts Fixed Object/ Equipment		42		
Aircraft Contacts Fixed Object/ Equipment			13	
Aircraft Contacts Moveable Object/ Equipment			29	
Totals	130	130	130	100%

Table 2. Incidence of Latent Failures

Latent Failure ID	Description of Latent Failure	Number of Incidents
A	**Poor Communication**	**29**
A1	Poor Communication: Between Crew	24
A2	Poor Communication: Between Shifts	5
B	**Poor Equipment**	**72**
B1	Poor Equipment: Inappropriate for Task	39
B2	Poor Equipment: Mechanical Problem	33
C	**Correct Number of Personnel Not Used**	**36**
D	**Inadequate Space**	**30**
D1	Inadequate Space: Congested Area	22
D2	Inadequate Space: Ill-suited for Task	8
E	**Problems With Painted Guide Lines**	**21**
E1	Guide Lines: Do Not Exist	7
E2	Guide Lines: Do Not Extend Out of Hangar	4
E3	Guide Lines: Not Suitable for Aircraft	10
F	**Personnel Unaware of Concurrent Work**	**8**
G	**Pressures to Maintain On-Time Departures**	**19**
H	**Lack of Awareness of Risks/Hazards**	**34**
I	**Pushback Policies Not Enforced**	**16**
	TOTAL	**265**

Note: Totals exceed the number of incidents due to multiple latent failures per incident.

FIGURA 15

Table 3. Latent Failures By Hazard Pattern

Failure / Patterns	A	A1	A2	B	B1	B2	C	D	D1	D2	E	E1	E2	E3	F	G	H	I	Totals
1	17	13	4	53	33	20	22	12	8	4	8	2	1	5	8	11	22	4	157
1.1	5	2	3	47	30	17	17	11	8	3	7	1	1	5	1	6	10	2	106
1.1.1	3	1	2	3	1	2	0	1	0	1	0	0	0	0	0	0	2	0	9
1.1.2	1	1	0	29	25	4	6	0	0	0	1	0	0	1	1	4	2	1	45
1.1.3	0	0	0	7	4	3	9	7	7	0	1	0	0	1	0	2	0	1	27
1.1.4	0	0	0	8	0	8	2	0	0	0	0	0	0	0	0	0	4	0	14
1.1.5	1	0	1	0	0	0	0	3	1	2	5	1	1	3	0	0	2	0	11
1.2	12	11	1	6	3	3	5	1	0	1	1	1	0	0	7	5	12	2	51
1.2.1	8	7	1	1	1	0	5	0	0	0	0	0	0	0	2	3	5	0	24
1.2.2	2	2	0	3	2	1	0	0	0	0	1	1	0	0	5	1	5	1	18
1.2.3	2	2	0	2	0	2	0	1	0	1	0	0	0	0	0	1	2	1	9
2	12	11	1	19	6	13	14	18	14	4	13	5	3	5	0	8	12	12	108
2.1	0	0	0	8	3	5	2	0	0	0	0	0	0	0	0	0	3	0	13
2.2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	4
2.3	10	9	1	11	3	8	12	18	14	4	13	5	3	5	0	7	9	11	91
2.3.1	2	1	1	4	1	3	2	8	4	4	5	1	1	3	0	1	3	4	29
2.3.2	8	8	0	7	2	5	10	10	10	0	8	4	2	2	0	6	6	7	62
Totals	29	24	5	72	39	33	36	30	22	8	21	7	4	10	8	19	34	16	265

FIGURA 16

La figura 15-16 riassume l'incidenza delle latent failure all'interno dei modelli di rischio. La figura illustra le latent failure più comuni che contribuiscono a specifici modelli di rischio. È importante ricordare che ciascuna latent failure non contribuisce a ciascun incidente all'interno di un modello di pericolo, ma è semplicemente una latent che ha provocato un incidente di questo tipo in passato. Dalla figura si può vedere che le latent failure che si verificano più frequentemente sono problemi con i sistemi e l'attrezzatura, l'utilizzo di un numero improprio di personale e la mancanza di consapevolezza dei rischi e dei pericoli. Quest'ultima latent failure è una categoria ampia, che comprende fallimenti come una formazione inadeguata e il presupposto che esista un'autorizzazione adeguata senza controlli. Tuttavia, non è possibile eliminare completamente nessuno di questi fallimenti latenti utilizzando solo la tecnica tradizionale di rimproverare, motivare e formare. Si possono minimizzare, come vuole la normativa 25.1309. ci sono altri vincoli sulle latent failure.

i) *The probability of the latent part of the combination (e.g. "Sum of the products of the failure rates multiplied by the exposure time" of any latent failure) must be equal or less than $1x10^{-3}$ (=1/1000) on average.*

e) *The periodic maintenance checks, which may result from the compliance to this Specific Risk criterion (d), will be considered as CMR candidates, in addition to the CMR Candidates already selected for compliance to CS 25.1309.*

is proposed to be amended as followed :

However, it is not evident that this is sufficient to provide an ESF to the existing CS25.671(c)(2). Therefore, EASA proposes the following approach and ***basic objectives*** ~~*additional criteria*~~*: 4) It is recognised that, on occasion, there may be no possibility to* ***avoid the conditions described in*** ~~*comply with the above criteria*~~ *1) and 2). In such cases:*

a) *The deviation latent failures shall be recorded and justified in the PSSA/SSA and reviewed during the design review process for acceptance,*

b) *Acceptance should be based on both previous experience and sound engineering judgment and shall assess:*

i) *the failure rates and service history of each component,*

ii) *the inspection type and interval for any component whose failure would be latent, and*

iii) *any possible common cause of cascading failure modes.*

~~*c) The integrity of the evident part of the significant failure condition shall meet a minimum standard:*~~
~~*i) For Catastrophic failure combinations comprising only one evident failure, the probability per flight hour of the evident part should be <= 10-5/Fh, and*~~
~~*ii) For Hazardous failure combinations comprising only one evident failure, the probability per flight hour of the evidentpart should be <= 10-4/Fh.*~~
~~*d) In addition, a Specific Risk calculation should be considered in accepting the presence of a latent failure. For each combination composed of one active failure and latent failures and leading to a Catastrophic Failure Condition:*~~
~~*i) The probability of the latent part of the combination (e.g. "Sum of the products of the failure rates multiplied by the exposure time" of any latent failure) must be equal or less than 1x10-3 (=1/1000) on average.*~~

e) *The periodic maintenance checks, which may result from the compliance to CS 25.671(c)this Specific Risk criterion (d), will be considered as CMR candidates, in addition to the CMR Candidates already selected for compliance to CS 25.1309.*

FIGURA 17

EASA response:

(1) Partially Agree, as per previous comment: neither "basic objectives" nor "additional criteria" will be used.
(2) Partially Agree – "avoid the conditions described in ~~*comply with the above criteria*~~***" will be amended to "Meet 1) and 2)".***
(3) Agree "deviation" is wrong word. "Remaining latent failures" is proposed instead.
(4) Disagree for 4c to 4e. At this stage the approach is applied only to the Flight Control Systems (FCS), this being the subject of 25.671 and the ESF. EASA position is that a specific approach is needed for the FCS, given the exceptional criticality of this system. Again, it is to be noted that this approach has already been successfully applied to a number of programmes.

FIGURA 18

"***When a catastrophic failure condition involves two failures, either one of which is latent for more than one flight, and cannot reasonably be eliminated, compliance with CS 25.1309(b)(5) is required".***
"Following the proper application of CS 25.1309(b)(4), the failure conditions involving multiple significant latent failures are expected to be sufficiently unlikely such that the dual-failure situations addressed in CS 25.1309(b)(5) are the only remaining significant latent failures of concern".
Le latent failure che portano ad eventi hazardous o catastrofici devono essere eliminati dal design del sistema. (figure 17-18) Come dice sempre la normativa questi ultimi due elementi che ho indicato possono non essere sempre rispettati e i sistemi possono comunque essere certificati, solo però se sono passati verso un accurato controllo PSSA e SSA e una dettagliata revisione di tutti i test. La normativa dice che per le failure conditions catastrofiche risultate da una combinazione di cui solo una evidente la probabilità dovrà essere almeno 10E-5/Fh, mentre per le failure conditions hazardous risultate da una combinazione di cui sono una evidente la probabilità dovrà essere almeno di 10E-4/Fh. Il secondo vincolo [10]
"***Given that a single latent failure has occurred on a given flight, each catastrophic failure condition, resulting from two failures, either of which is latent for more than one flight, is remote".***

Questo è il vincolo preciso che è riportato nella CS-25.1309, AMC 25.1309 sulle latent failure. Il vincolo ufficiale mostra solo la caratteristica di failure condition catastrofica, mentre gli approfondimenti e le sessioni spiegano anche l'aspetto hazardous. La normativa introduce una cosidetta 'Specific Risk calculation' in cui considera accettabile la presenza delle latent failure.

"Limit latency is intended to limit the time of operating with one evident failure away from a catastrophic failure condition. This is achieved by requiring that the sum of the probabilities of the latent failures, which are combined with each evident failure, does not exceed 1/1 000. Taking one catastrophic failure condition at a time,

— in case an evident failure is combined only once in a dual failure combination of concern, the probability of the individual latent failure needs to comply with the 1/1 000 criterion;

— in case an evident failure is combined in multiple dual failure combinations of concern, the combined probabilities of the latent failures need to comply with the 1/1 000 criterion".

La latenza limite ha quindi lo scopo di limitare il tempo di funzionamento di un sistema con un guasto evidente lontano da però da una condizione di guasto catastrofico. Per permettere la latenza limite si applica la somma delle probabilità dei guasti latenti, che combinate con ogni evident failure, non superi 1/1 000, 10E-3. Per quanto concerne le failure condition catastrofiche ci possono essere due tipi di combinazioni delle latent failure. Nel caso in cui una evident failure sia combinata una sola volta in una doppia combinazione di guasto di preoccupazione, la probabilità del singolo latent failure deve soddisfare il criterio 1/1 000, cioè 10E-3. Nel caso in cui una evident failure sia combinata in più combinazioni di guasti duali, allora a differenza della precedente saranno le probabilità combinate delle latent failure a rispettare il criterio di 1/1 000, 10E-3. Dice, quindi, la normativa che per ogni combinazione composta da una active failure e da più latent failures che porti ad una failure conditions catastrofica, allora la probabilità della parte latente della combinazione, cioè la somma dei prodotti dei tassi di failure moltiplicati dal tempo operativo in cui operano le latent failure, dovrà essere uguale o minore di 10E-3, cioè 1/1000. Un altro vincolo delle latent failure riguarda la dimostrazione che il design è accettabilmente sicuro. Questa dimostrazione mostra come ogni individual failure che non sia estremamente remoto (10E-7) e sapendo che è latente e non individuato in nessun volo o durante il check quotidiano, e che porti ad un evento catastrofico, allora deve avere un tasso di probabilità di 10E-6. Se un active failure è combinato con due latent failure e una latent failure prende il vantaggio sulla combinazione, cioè, è determinante alla causa della failure condition risultante, allora dovrà avere una probabilità di accadimento non superiore a 10E-6 per gli eventi catastrofici e 10E-4 per gli eventi hazardous. Airbus e Boeing hanno provato a far emendare questa parte di normativa togliendo la parte riguardante le combinazioni delle latent failure con le evident failure, ma la risposta di EASA è stata un secco no. Secondo EASA, questo approccio molto critico è necessario perché si sta parlando ed esaminando sistemi estremamente critici per l'aereo (in questo caso il FCS) e quindi è opportuno progettare e certificare con la massima cura e rigore ed essere il più sicuri possibili. Aggiunge EASA che questo tipo di approccio, cioè i ristretti limiti imposti alle combinazioni delle latent failures, è stato applicato con successo a diversi programmi di progettazione e certificazione di sistemi critici e che ha dato ottimo risultati in fatto di sicurezza. Come si vede la questione delle latent failure è molto critica e ingarbugliata, tanto che anche le aziende hanno cercato di ammorbidire la normativa, al momento senza successo. La sfida continua e per il momento è aggiornata al 2023. [16] [10]

"Limit residual probability is intended to limit the average probability per flight hour of the failure condition given the presence of a single latent failure. This is achieved by defining the residual probability to be 'remote'. Residual probability is the combined average probability per flight hour of all the single active failures that result in the catastrophic failure condition assuming one single latent failure has occurred".

Questo vincolo pone l'accento sulla probabilità residua limite che ha l'obiettivo di limitare la probabilità media per ora di volo della condizione di guasto in presenza di un singolo latent failure. Questa probabilità deve essere considerata remota, cioè tra 10E-5. La probabilità residua è la probabilità media combinata per ora di volo di tutti i singoli evident failure che danno luogo alla condizione di guasto catastrofica supponendo che sia avvenuto un singolo latent failure.

"***When dealing with constant failure rates, the probability of the latent failure should be computed as the product of the maximum time during which the failure may be present and its failure rate, if this probability is less than or equal to 0.1".***

Questo vincolo spiega al progettista e al certificatore come dovrebbe essere calcolato la probabilità del latent failure nel caso di tassi di guasto costanti. La probabilità delle latent failure è calcolata come il prodotto del tempo massimo durante il quale il guasto può essere presente e il suo tasso di guasto, se tale probabilità è inferiore o uguale a 0,1. Inoltre, come afferma la normativa nella spiegazione di questo vincolo, per rispettare il criterio 1/1 000, la probabilità delle latent failure di preoccupazione dovrebbe essere calcolata considerando il caso del volo peggiore, vale a dire la probabilità in cui l'evident failure si possa verificare nell'ultimo volo prima dell'ispezione di manutenzione programmata, mentre la latent failure può essersi verificata in qualsiasi volo tra due ispezioni consecutive di manutenzione programmata. In questo caso, quindi, bisogna considerare gli aspetti manutentivi, che però esulano nel lavoro di questa Tesi, che però potranno essere usati per lavori futuri. Nell'appendice 5 della CS-25 sono spiegati bene come i metodi delle latenze e residuali possono essere applicati, ma anche in questo caso esula da questo lavoro. Non è sempre facile comprendere anche le formule spiegate.

"If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation should consider the relevant exposure time".

Questo vincolo impone di considerare la failure, qualunque essa sia, se per molteplici voli, per il tempo di esposizione che questa ha nei confronti dell'aereo e dei suoi sistemi.

"For each significant latent failure which cannot reasonably be eliminated, the applicant must minimize the exposure time".

Se non è possibile eliminare la latent failure, allora bisogna minimizzare il tempo di esposizione di quest'ultima nei confronti dell'aereo e dei suoi sistemi durante il volo.

Tutti questi elementi rappresentano i vincoli riguardanti le '*laten failure'*. Continuiamo con il capitolo della CS-25.1309 e a vedere i vincoli normativi successivi che appaiano e a cercare di dispiegarli e comprenderli, e come si è appena visto non è per niente una cosa semplice. Potrebbe capitare che possano essere stati saltati alcuni vincoli che non sono stati compresi o individuati, visto l'enorme difficoltà nel comprenderli. In quel caso sarà premura di lavori successivi che vadano ad individuare i vincoli rimasti e ad aggiungere vincoli nel caso la normativa si aggiorni nel tempo. Viste le latent failure, la cs25.1309 possiede vincoli per tutte le failure.

" No single failure will result in a catastrophic failure condition; and
-(2) Each catastrophic failure condition is extremely improbable; and
-(3) Given that a single latent failure has occurred on a given flight, each catastrophic
failure condition, resulting from two failures, either of which is latent for more than one flight, is remote. It is reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1 × 10-7 per flight hour for a newly designed aeroplane.
A single failure includes any set of failures, which cannot be shown to be independent from each other
g. In general, a failure condition resulting from a single failure mode of
a device cannot be accepted as being extremely improbable."

Questo vincolo impone che nessun singolo guasto porti ad un evento catastrofico. Un evento catastrofico, se accade, deve accadere come risultato di più guasti, di più failure, mai da una single failure. Le single failure vengono anche considerate quelle che non possono essere indipendenti dalle altre failure.

"Single failures, which, in combination with operational or environmental conditions, lead to catastrophic failure conditions, are, in general, not acceptable".

Le single failure che in combinazione con condizioni ambientali avverse portino ad eventi catastrofici sono non accettabili, nemmeno improbabili o di più. Sono inaccettabili.

"The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1 × 10-9 , which establishes an approximate probability value for the term 'extremely improbable'".

Questo è l'evento catastrofico che bisogna impedire, arrivare sempre a 10e-9.

"When a system provides protection from events its reliability should be compatible with the safety objectives necessary for the failure condition associated with the failure of the protection system and the probability of such events"

La reliability di un sistema deve sempre essere coerente con il suo grado di pericolosità e probabilità di accadimento di una failure e che failure condition provocherà.

"Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure conditions".

Bisogna progettare un Sistema che riesca a contenere l'effetto delle failure e delle single failure che potrebbero portare ad un evento catastrofico.

"An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel."

Questo vincolo sarà espresso molto bene nella SAE arp 4754 sull'aspetto dei sistemi ridondanti che devono essere progettati che i vari canali ridonandoti siano tra loro separati.

"When combining the probability of such a random condition with that of a system failure, care should be taken to ensure that the condition and the system failure are independent of one another, or that any dependencies are properly accounted for".

"If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant 'at risk' time for the 'Average Flight'."

Questo è un vincolo di calcolo che indica come una failure che è rilevante solo in determinati fasi del volo devono essere calcolate in base al tempo di rischio che questa failure può avere in quel tempo. Dalla AMC 25.1309 sono presenti questi vincoli.

"(1) The following basic objectives pertaining to failures apply:
(i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.
(ii) Subsequent failures of related systems during the same flight, whether detected or latent, and combinations thereof, should also be considered
-(ii) Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.
(iii) Isolation and/or Segregation of Systems, Components, and Elements so that the failure of one does not cause the failure of another.
(iv) Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.

Questo vincolo è molto corposo che ha un elemento in comune, considerare sempre una failure, nonostante la sua probabilità va sempre considerato, sia se è singolo o in combinazione., sia che sia latente o attivo. Bisogna sempre considerare un sistema ridondato, come mostrerà la SAE 4754. Bisogna progettare anche un sistema di isolamento della failure, che mostrerà sempre la SAE 4754.

"An analysis should always consider the application of the fail-safe design concept described in paragraph 6.b, and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions"

Per avere un design fail-safe bisogna considerare tutte le conseguenze delle failure, single o in combinazione. Bisogna considerare anche gli effetti su tutti i sistemi ridondati, non solo su quello principale ma anche su quelli secondari.

"Particular attention should be given to the placement of switches or other control devices, relative to one another, so as to minimise the potential for inadvertent incorrect crew action, especially during emergencies or periods of high workload."

Questo requisite impone di prestare particolare attenzione alla progettazione dei sistemi di switch o altri sistemi di controllo che aiutano ad individuare le failure, e per impedire che l'equipaggio non compia una mossa sbagliata traviato da una failure nei sistemi di switch e di controllo.

"The overall effect on the aeroplane of a combination of individual system failure conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, failure conditions classified as minor or major by themselves may have hazardous effects at an aeroplane level, when considered in combination."

Bisogna sempre stare attenti alla progettazione del sistema e dei componenti, e non sottovalutare un basso tasso di guasto di un componente, perché anche se da solo è basso, in combinazione risulterà moltiplicato.

"According to the requirements of CS 25.1309(b)(1)(ii), a catastrophic failure condition must not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure

conditions. In addition, there must be no common-cause failure, which could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures, which cannot be shown to be independent from each other. Common-cause failures (including common mode failures) and cascading failures should be evaluated as dependent failures from the point of the root cause or the initiator."

Questo requisite spiega bene il senso del no al singolo guasto e gli effetti, e le possibili cause comuni. Questo AMC è utilizzato per interpretare al meglio il vincolo iniziale 25.1309.

"Where it is not possible to fully justify the adequacy of the safety analysis and where data or assumptions are critical to the acceptability of the Failure Condition, extra conservatism should be built into either the analysis or the design".

Questo vincolo impone che, quando non si riesca a giustificare al meglio un adeguato tasso di rischio e probabilità, o il valore della failure condition oscilla tra due range, allora bisognerà sempre impostare un 'extra conservatorismo' nell'inserire il valore e giustificare il tasso di guasto. Cioè, essere più severi per essere sicuri del sistema e della sicurezza. La sicurezza non è mai troppa e alcuni eventi oggigiorno ci mostrano come una leggerezza nella sicurezza è fatale, la gente muore. Altri vincoli presi dalla AC-25,1309

"a. The following basic objectives pertaining to failures apply:
(2) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable."

I guasti successivi, sia che questi siano latenti che no, e le loro combinazioni devono essere estremamente improbabili, con i valori spiegati. Questa AC 25.1309 mostra alcuni tipi di common cause failure: *"(3) Some examples of such potential common-cause failures or other events would include rapid release of energy from concentrated sources such as uncontained failures of rotating parti or pressure vessels, pressure differentials, non catastrophic structural failures, loss of environmental conditioning, disconnection of more than one subsystem or component by overtemperature protection devices, contamination by fluids, damage from localized fires, loss of power, excessive voltage, physical or environmental interactions among parts, use of incorrect, faulty, or bogus parts, human or machine errors, and foreseeable adverse operational conditions, environmental conditions, or events external to the system or to the airplane."*

3.2 I Vincoli nei capitoli della CS-25

I vincoli architettonici dei sistemi non compaiono solamente nel capitolo 25.1309 e AMC associato, ma sono presenti anche in altri capitoli, che si andrà ad analizzare. [16]

CAPITOLO 25.671, Subpart D-Design and Construction. Questo capitolo è relativo ai sistemi di controllo.

"-The aeroplane must be shown by analysis, test, or both, to be capable of continued safe flight and landing after any of the following failures or jams in the flight control system within the normal flight envelope. In addition, it must be shown that the pilot can readily counteract the effects of any probable failure.
-Any single failure, excluding failures of the type defined in CS 25.671(c)(3);
-(2) Any combination of failures not shown to be extremely improbable, excluding failures of the type defined in CS 25.671(c)(3)."

Questo è un vincolo molto lungo, e molto simile a quelli del capitolo 25.1309. In pratica viene detto che, a parte le failure di jam che esulano da questo lavoro di Tesi, le failure e le loro possibili combinazioni devono essere improbabili, con i valori descritti precedentemente. Inoltre, l'aeroplano deve essere progettato in modo da poter continuare a volare ed atterrare in sicurezza per qualunque tipo di failure. Deve essere in grado di continuare il volo ed atterrare nell'aeroporto più vicino per ogni tipo d failure. Il pilota deve inoltre essere in grado di reagire a qualunque failure. I sistemi devono quindi essere in grado di permettere al pilota e copilota di trovare una risposta immediata alle failure.

"The aeroplane must be designed so that, if all engines fail at any time of the flight:
(1) it is controllable in flight;
(2) an approach can be made;

(3) a flare to a landing, and a flare to a ditching can be achieved; and
(4) during the ground phase, the aeroplane can be stopped.
Compliance with CS 25.671(d) effectively requires that the aeroplane is equipped with a source(s) of emergency power, such as an air-driven generator, windmilling engines, batteries, or other power source, capable of providing adequate power to the systems that are necessary to control the aeroplane".
Questo vincolo specifica che deve essere presente almeno un sistema di back-up per garantire il corretto funzionamento del sistema di controllo di volo e del carrello di atterraggio in caso di perdita di tutti i motori. Questo lo si garantisce, per gli aeromobili esistenti, aggiungendo un'unità di potenza ausiliaria (APU) o una connessione con turbina ad aria compressa (RAT) ai sistemi specificati. Ma sono possibili anche altre soluzioni con altre fonti di energia ridondanti non dipendenti dal motore.
"CS 25.671(c)(1) requires the evaluation of any single failure, excluding the types of jams addressed in subparagraph CS 25.671(c)(3). CS 25.671(c)(1) requires to consider any single failure, suggesting that an alternative means of controlling the aeroplane or an alternative load path is provided in the case of a single failure. All single failures must be considered, even if they are shown to be extremely improbable".
Questo vincolo afferma che tutte le failure, a parte quelle del jam, devono essere considerate e devono essere estremamente improbabili, con il valore che è stato descritto precedentemente. Inoltre, ci deve sempre essere un'alternativa di sistema per permettere di controllare l'aeromobile.
"CS 25.671(c)(2) requires the evaluation of any combination of failures not shown to be extremely improbable, excluding the types of jams addressed in CS 25.671(c)(3)."
Il vincolo afferma del livello di probabilità che le combinazioni di failure, escluse il jam, devono avere per essere certificabili.
"Some combinations of failures, such as dual electrical system or dual hydraulic system failures, or any single failure in combination with any probable electrical or hydraulic system failure, are normally not demonstrated as being extremely improbable".
Questo vincolo mostra alcuni tipi di combinazioni di failure, come ad esempio quello dei sistemi elettrici o idraulici, e mostra anche che un singolo failure in combinazione con failure dei sistemi appena citati deve essere estremamente improbabile.
"Any runaway of a flight control to an adverse position must be accounted for, as per
CS 25.671(c)(1) and (c)(2), if such a runaway is due to:
— a single failure; or
— a combination of failures which are not shown to be extremely improbable.
The following should be considered when evaluating compliance with CS 25.671(c)(2):

(1) The flight control system should continue to provide its intended function, regardless of any malfunction from sources in the integrated systems environment of the aeroplane"

Questi vincoli ci spiegano come il sistema deve riuscire a garantire operabilità, almeno per atterrare, e manovrare l'aereo in emergenza in caso di failure.
"If the aeroplane is equipped with a conventional flight control system, the transmission of command signals to the primary and secondary flight control surfaces is made through conventional mechanical and hydromechanical means.
However, when the aeroplane is equipped with flight control systems using the fly-by-wire technology, incorporating digital devices and software, experience from electronic digital transmission lines shows that the perturbation of signals from internal and external sources is not unlikely"
Questo è un vincolo che spiega le differenze di architettura e componenti tra un sistema convenzionale ed un sistema fly-by-wire.
CAPITOLO 25.672, Stability augmentation and automatic and power-operated systems ***"(c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system:***

(1) The aeroplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved operating limitations that is critical for the type of failure being considered"

Questo vincolo mostra come per lo stability augmentation e anche per tutti gli altri sistemi operativi che richiedono potenza devono permettere una manovrabilità sicura del velivolo in caso di failure. Bisogna inserire ridondanze o isolamenti.
CAPITOLO 25.729

Il capitolo 25.729 è sul meccanismo di estrazione e ritrazione del carrello deve avere un sistema di emergenza che permetta di operare nel caso di guasto dei sistemi elettrici o idraulici o di altro genere di potenza. Ad esempio, è inserito, e anche nel sistema progettato in questa tesi, un meccanismo di estrazione per gravità.

"(c) Emergency operation. There must be an emergency means for extending the landing gear in the event of –

(1) any reasonably probable failure in the normal extension and retraction systems; or

(2) the failure of any single source of hydraulic, electric, or equivalent energy supply."

CAPITOLO 25.735

"(b) Brake system capability. The brake system, associated systems and components must be designed and constructed so that:

(1) If any electrical, pneumatic, hydraulic, or mechanical connecting or transmitting element fails, or if any single source of hydraulic or other brake operating energy supply is lost, it is possible to bring the aeroplane to rest with a braked roll stopping distance of not more than two times that obtained in determining the landing distance as prescribed in CS 25.125.

Il Sistema frenante deve essere progettato per operare in sicurezza anche nel caso di failure dei sistemi di alimentazione, sistemi elettrici, idraulici o meccanici. Inoltre bisogna permettere all'aereo di frenare e fermarsi ad una distanza di arresto del rollio frenato non superiore a due volte quella ottenuta nel determinare la distanza di atterraggio come prescritto nella CS 25.125. si possono inserire più linee di alimentazione e delle linee alternative.

"Ref. CS 25.735(b) Brake System Capability

(1) The system should be designed so that no single failure of the system degrades the aeroplane stopping performance beyond doubling the braked roll stopping distance (refer to CS 25.735(b)(1))."

Il vincolo mostra come il sistema freante deve riuscire ad operare in caso di avaria e failure. Per completezza viene mostrato interamente i tipi di failure che possono capitare. Preso dall'AMC 25.735.

"Failures are considered to be fracture, leakage, or jamming of a component in the system, or loss of an energy source. Components of the system include all parts that contribute to transmitting the pilot's braking command to the actual generation of braking force. Multiple failures resulting from a single cause should be considered a single failure (e.g., fracture of two or more hydraulic lines as a result of a single tyre failure). Sub-components within the brake assembly, such as brake discs and actuators (or their equivalents), should be considered as connecting or transmitting elements, unless it is shown that leakage of hydraulic fluid resulting from failure of the sealing elements in these subcomponents within the brake assembly would not reduce the braking effectiveness below that specified in CS 25.735(b)(1)."

"(a) In order to meet the stopping distance requirements of CS 25.735(b)(1) in the event of failure of the normal brake system, it is common practice to provide an alternate brake system. The normal and alternate braking systems should be independent, being supplied by separate power sources. Following a failure of the normal system, the changeover to a second system."

Questo vincolo ci mostra una regola di architettura del sistema frenante, e cioè avere sempre un sistema alternativo che permetta al sistema di operare in caso di failure del sistema principale.

"(b) The brake systems and components should be separated or appropriately shielded so that complete failure of the braking system(s) as a result of a single cause is minimised."

Le failure che sono causate da una singola causa devono essere minimizzate

"Ref. CS 25.735(e) Anti-skid System

(1) If an anti-skid system is installed (refer to CS 25.735(e)), then no single failure in the antiskid system should result in the brakes being applied, unless braking is being commanded by the pilot. In the event of an anti-skid system failure, means should be available to allow continued braking without anti-skid. These means may be automatic, pilot controlled, or both"

Se l'anti-skid non è disponibile o ha una failure allora il sistema frenante deve comunque operare.

CAPITOLO 25.745

"(c) Under failure conditions the system must comply with CS 25.1309(b) and (c). The arrangement of the system must be such that no single failure will result in a nose-wheel position, which will lead to a Hazardous Effect. Where reliance is placed on nose-wheel steering in showing compliance with CS 25.233, the nose-wheel steering system must be shown to comply with CS 25.1309. (See AMC 25.745(c).)"
Il carrellino davanti deve essere progettato per impedire qualunque tipo di single failure che porti ad eventi hazardous. Inoltre, questo sistema deve rispettare i vincoli della 25.1309. nel carrellino davanti non è inserito il freno.
CAPITOLO 25.901
"(c) The powerplant installation must comply with CS 25.1309, except that the effects of the following need not comply with CS 25.1309(b):
(1) Engine case burn through or rupture;
(2) Uncontained engine rotor failure; and
(3) Propeller debris release"
L'installazione del Sistema di potenza deve rispettare i vincoli della 25.1309. Inoltre, deve essere progettato in modo che possa contenere la failure dei rotori del motore e il rilascio dei detriti della pala. [15]
"(ii) If an estimate of the IFSD rate is required for a specific turbine engine installation, any one of the following methods is suitable for the purposes of complying with CS 25.901(c)/ CS 25.1309(b):
(C) Use a conservative value of 1x10-4 per flight hour.
(2) Multiple Engine IFSD. Typical engine IFSD rates may not meet the AC 25.1309-1B guidance that calls for 1 x 10-9 per hour for a catastrophic multiple engine IFSD.
-(ii) Nevertheless, some combinations of failures within aircraft systems common to multiple engines may cause a catastrophic multiple engine thrust loss. These should be assessed to ensure that they meet the extremely improbable criteria. Systems to be considered include:
— fuel system,
— air data system,
— electrical power system,
— throttle assembly,
— engine indication systems, etc"
Questo vincolo mostra alcuni valori di calcolo che deve avere il tasso IFSD (*in flight shtudown, cioè lo spegnimento in volo).* bisogna valutare se il guasto è multiplo o singolo. Inoltre, vengono mostrate alcuni sistemi in cui possono accadere anche combinazione di failure che portano ad eventi estremamente improbabili, e che devono essere evitati.
CAPITOLO 25.903
"The powerplants must be arranged and isolated from each other to allow operation, in at least one configuration, so that the failure or malfunction of any engine, or of any system that can affect the engine, will not –
(1) Prevent the continued safe operation of the remaining engines;
- For turbine engine installations –
(1) Design precautions must be taken to minimise the hazards to the aeroplane in the event of an engine rotor failure or of a fire originating within the engine which burns through the engine case. (See AMC 25.903(d)(1) and AMC 20-128A.)
(2) The powerplant systems associated with engine control devices, systems, and instrumentation, must be designed to give reasonable assurance that those engine operating limitations that adversely affect turbine rotor structural integrity will not be exceeded in service"
il sistema di potenza deve essere progettato in modo da permettere l'isolamento delle parti guaste e deve avere più configurazioni in modo che almeno una configurazione sia attiva e funzioni in caso di failure. Il motore 'sano' deve continuare ad operare in caso di avaria, cioè non deve avvenire nessun tipo di 'common cause failure' o 'failure a cascata'. Inoltre, il design deve essere progettato in modo da minimizzare i casi di guasto al rotore del motore. I sistemi associati al sistema motore e la loro architettura devono essere progettati in modo da fornire una ragionevole garanzia che le limitazioni operative del motore che

influiscono negativamente sull'integrità strutturale del rotore della turbina non verranno superate durante il servizio.

CAPITOLO 25.905

"(d) Design precautions must be taken to minimise the hazards to the aeroplane in the event a propeller blade fails or is released by a hub failure. The hazards which must be considered include damage to structure and critical systems due to impact of a failed or released blade and the unbalance created by such failure or release. (See AMC 25.905(d).)"

Il criterio di questo vincolo è sempre lo stesso, creare ridondanze in modo da permettere al sistema di funzionare in caso di failure delle pale. Inoltre, viene considerato hazardous le failure che danneggiano la struttura e rendono critico il sistema.

CAPITOLO 25.933

"(a) For turbojet reversing systems:
(1) Each system intended for ground operation only must be designed so that either:
(i) The aeroplane can be shown to be capable of continued safe flight and landing during and after any thrust reversal in flight; or
(ii) It can be demonstrated that any in-flight thrust reversal complies with CS 25.1309(b).
-(2) Each system intended for inflight use must be designed so that no unsafe condition will result during normal operation of the system, or from any failure (or reasonably likely combination of failures) of the reversing system, under any anticipated condition of operation of the aeroplane including ground operation
For reversing systems intended for operation in flight, the reverser system must be designed to adequately protect against unwanted in-flight thrust reversal"

Il vincolo riguardante il sistema dell'inversori di spinta, uno dei tre impianti frenanti. Questo vincolo mostra come il progetto dell'inversore di spinta deve essere fatto in modo da garantire un volo sicuro e atterraggio sicuro. Inoltre, viene citato 'ground operation'. Altri vincoli parleranno di 'in-flight operation', cioè, bisogna progettare il sistema in modo che non si attivi in volo, a meno che non lo si desideri. Infatti, il (2) spiega proprio questo. Il sistema inflight deve essere progettato in modo che risulti sicuro durante il volo e non causi failure di nessun genere.

"(b) For propeller reversing systems:
(1) Each system intended for ground operation only must be designed so that no single failure (or reasonably likely combination of failures) or malfunction of the system will result in unwanted reverse thrust under any expected operating condition. Failure of structural elements need not be considered if this kind of failure is extremely remote."

Il vincolo precedente riguardava il jet engine thrust revers, ma sono presenti anche i propeller thrust revers. Questo vincolo è il corrispettivo del propeller del precedente. Nel sistema progettato per questo lavoro di tesi sono state inserite le scelte di che tipo di thrust revers utilizzare.

"Obviously, for unwanted in-flight thrust reversals less probable than 1x10- 9/fh, certification may be based on reliability alone, as described in Section 8 («RELIABILITY OPTION») of this AMC. Furthermore, for any failure conditions where unwanted in-flight thrust reversal would impact safety, the aeroplane must meet the safety/reliability criteria delineated in CS 25.1309.
7.c.(2) Probability of unwanted in-flight thrust reversal greater than 1x10-7/fh: Full performance accountability must be provided for the more critical of a regular engine failure and an unwanted in-flight thrust reversal
7.c.(3) Probability of unwanted in-flight thrust reversal equal to or less than 1x10-7/fh, but greater than 1x10-9/fh: With the exception of the takeoff phase of flight, which needs not account for unwanted in-flight thrust reversal, the same criteria should be applied as in Section 7.c.(2), above, for the purposes of providing advisory data and procedures to the flight crew.
The unwanted in-flight thrust reversal should not result in any of the following:
degradation of flying qualities assessed as greater than Major for unwanted inflight thrust reversal more probable than 1x10-7/fh; or assessed as greater than

Hazardous for failures with a probability equal to or less than 1x10-7/fh, but greater 1x10-9/fh -7.d.(3) Probability of in-flight thrust reversal less than 1x10-9/fh:
-8.b.(1) The thrust reverser system should be designed so that any in-flight thrust reversal that is not shown to be controllable in accordance with Section 7,above, is extremely improbable (i.e., average probability per hour of flight of the order of 1x10-9/fh. or less) and does not result from a single failure or malfunction. And
8.b.(2) For configurations in which combinations of two-failure situations (ref. Section 5, above) result in in-flight thrust reversal, the following apply:
Neither failure may be pre-existing (i.e., neither failure situation can be undetected or exist for more than one flight); the means of failure detection must be appropriate in consideration of the monitoring device reliability, inspection intervals, and procedures.
8.b.(3) For configurations in which combinations of three or more failure situations result in in-flight thrust reversal, the following applies:
In order to limit the exposure to pre-existing failure situations, the maximum time each pre-existing failure situation is expected to be present should be related to the frequency with which the failure situation is anticipated to occur, such that their product is 1×10-3 or less."
Questo grande vincolo mostra tutto l'aspetto del sistema 'in-flight thrust revers'. Questo sistema non è vietato ma deve essere progettato in maniera che nessuna failure sia di tipo improbabile o estremamente improbabile, quindi si parla di 10e-7 e 10e-9. Inoltre, gli eventi catastrofici o altro non devono avvenire nel caso di singolo guasto. Viene trattato anche l'aspetto delle combinazioni di failure e all'aspetto delle failure preesistenti. Le failure preesistenti sono quelle failure che non sono state individuate o esistono da più voli. Bisogna quindi tenere conto di questi fattori. Molto simile alle latent failure. Le latent possono esistere e manifestarsi senza la presa visione dell'equipaggio, mentre le failure preesistenti sono accadute ed esistono nel sistema da tempo e su più di un volo. bisogna stare molto attenti nel progettare questo tipo di sistema. Il sistema 'in-flight' del thrust revers viene usato principalmente nei velivoli militari ad alte prestazioni, tipo i caccia. Mai sui velivoli di linea. L'unico velivolo di linea è il velivolo militare C-5 Galaxy.
CAPITOLO 25.953
"Each fuel system must meet the requirements of CS 25.903(b) by –
(a) Allowing the supply of fuel to each engine through a system independent of each part of the system supplying fuel to any other engine"
Un vincolo molto importante che dice di avere i sistemi di supply fuel, cioè di carburante, indipendenti per ogni sistema che alimenta, oltre al motore.
CAPITOLO 25.991
"There must be emergency pumps or another main pump to feed each engine immediately after failure of any main pump"
Bisogna progettare una pompa di emergenza che alimenti ognuno dei motori appena dopo la failure delle pompe principali. Anche qui il vincolo di ridondanza.
CAPITOLO 25.1011
"(a) Each engine must have an independent oil system that can supply it with an appropriate quantity of oil at a temperature not above that safe for continuous operation."
Un vincolo molto importante che riguarda l'indipedneza dei sistemi di alimentazione dei motori.
CAPITOLO 25.1143
"(a) There must be a separate power or thrust control for each engine.
(b) Power and thrust controls must be arranged to allow –
(1) Separate control of each engine; and
(2) Simultaneous control of all engines."
I sistemi di controllo della potenza e della spinta dei motori devono essere separati e devono essere capaci di controllare i motori sia separatamente sia simultaneamente.
CAPITOLO 25.1165
"(a) Each battery ignition system must be supplemented by a generator that is automatically available as an alternate source of electrical energy to allow continued engine operation if any battery becomes depleted."

Questo vincolo impone che il sistema di accensione a batteria deve essere integrato da un generatore che sia automaticamente disponibile come fonte alternativa di energia elettrica per consentire il funzionamento continuo del motore se una batteria si scarica.

"(c) The design of the engine ignition system must account for –
(1) The condition of an inoperative generator;
(2) The condition of a completely depleted battery with the generator running at its normal operating speed; and
(3) The condition of a completely depleted battery with the generator operating at idling speed, if there is only one battery."

La progettazione del Sistema di accensione a batteria deve tener conto dei possibili effetti di inoperatività dei generatori, della batteria e di altre failure che possono accadere.

"(f) Each ignition system must be independent of any electrical circuit not used for assisting, controlling, or analysing the operation of that system."

Anche questo è un vincolo di indipendenza architettonica che dice che il sistema deve essere indipendente da qualsiasi circuito elettrico non utilizzato per assistere, controllare o analizzare il funzionamento di tale sistema.

CAPITOLO 25.1307

"The following is required miscellaneous equipment:
(b) Two or more independent sources of electrical energy."

Vincolo importantissimo che indica che ogni sistema deve avere almeno 2 o anche più sorgenti indipendenti di energia. Uno dei vincoli di ridondanza più importanti.

CAPITOLO 25.1351

"The required generating capacity, and number and kinds of power sources must –
(1) Be determined by an electrical load analysis; and
(2) Meet the requirements of CS 25.1309.
It must be designed so that –
(1) Power sources function properly when independent and when connected in combination;
(2) No failure or malfunction of any power source can create a hazard or impair the ability of remaining sources to supply essential loads; -Operation without normal electrical power. (See AMC 25.1351(d).) The following apply:
(1) Unless it can be shown that the loss of the normal electrical power generating system(s) is Extremely Improbable, alternate high integrity electrical power system(s), independent of the normal electrical power generating system(s), must be provided to power those services necessary to complete a flight and make a safe landing"

Questo vincolo sul Sistema elettrico e tutte gli equipaggiamenti che usufruiscono del sistema elettrico dice che le sorgenti di potenza devono rispettare i carichi elettrici e i requisiti della 25.1309. Inoltre, i sistemi elettrici devono essere progettati in modo da funzionare correttamente quando indipendenti e connessi in combinazione. Nessuna failure deve creare condizioni hazardous o perdita di potenza prolungata. Questi vincoli sono molto importante nella progettazione dei sistemi per via del fatto che ora quasi tutto è collegato e deve avere una sorgente elettrica e funzionare elettricamente.

"The services to be powered must include –Those required for continued controlled flight; and
(iii) Those required for descent, approach and landing.
(3) Failures, including junction box, control panel or wire bundle fires, which would result in the loss of the normal and alternate systems must be shown to be Extremely Improbable.
-It may not be necessary to provide disconnection controls for all power sources, for example RAT generators or engine control dedicated generators. Where it is necessary to isolate the alternate power source when normal generator power is restored, such isolation should be possible.
-Provision should be made to ensure adequate electrical supplies to those services, which are necessary to complete the flight and make a safe landing in the event of a failure of all normal generated electrical power. All components and wiring of the alternate supplies should be physically and electrically segregated from the normal system and be such that no single failure, will affect both normal and alternate supplies."

I sistemi devono alimentare l'aereo per un continuo controllo di volo, tra cui la salita, l'approach e l'atterraggio. Alcuni tipi di guasto devono essere estremamente improbabili, come alla junction box, o al pannello di controllo. Tutti i componenti e il cablaggio delle alimentazioni alternative dovrebbero essere fisicamente ed elettricamente segregati dal normale sistema ed essere tali che nessun singolo guasto, influenzerà sia le forniture normali che quelle alternative.

CAPITOLO 25.1355

"(c) If two independent sources of electrical power for particular equipment or systems are required for certification, or by operating rules, in the event of the failure of one power source for such equipment or system, another power source (including its separate feeder) must be automatically provided or be manually selectable to maintain equipment or system operation.

A suitable supply must be provided to those services, which are required, in order that emergency procedures may be carried out, after an emergency landing or ditching"

Questo vincolo impone di avere una seconda sorgente di potenza sempre disponibile e che questa, in caso di guasto della sorgente principale, debba essere automaticamente o manualmente selezionabile per mantenere attivi i sistemi. Una sorgente di potenza secondaria deve sempre essere garantita per le procedure di emergenze.

CAPITOLO 25J953

"Each fuel system must allow the supply of fuel to the APU:

(a) Through a system independent of each part of the system supplying fuel to the main engines"

3.3 SAE ARP 4754 e i vincoli normativi

Un altro importantissimo documento in cui poter trovare vincoli architettonici dei sistemi di bordo, oltre alla CS e alla FAR, sono le SAE ARP. Nel capitolo iniziale è stato spiegato cosa sono le SAE. La SAE che verrà utilizzata è la SAE ARP 4754, spiegata anch'essa nel capitolo inziale. Verrà utilizzato lo stesso metodo utilizzato prima per descrivere i vincoli. Per iniziare è giusto spiegare cosa intende la sae 4754 con vincoli architettonici. La sae li chiama '*Safety Requirements'*. "*The safety requirements for aircraft and system-level functions include minimum performance constraints for both availability (continuity of function) and integrity (correctness of behavior) of the function. Safety requirements for aircraft and system functions are determined by identifying and classifying associated functional failure conditions. All functions have associated failure modes and associated aircraft effects, even if the classification is "No safety effect." Safety related functional failure modes may have either contributory or direct effects upon aircraft safety. Requirements that are defined to prevent failure conditions or to provide safety related functions should be traceable through the levels of development at least to the point of allocation to hardware and software. This will ensure visibility of the safety requirements at the software and hardware design level."* Questa è la definizione di safety requirements presente nella SAE 4754. Questi requisiti servono per garantire la sicurezza dei sistemi e del sistema aereo. Vengono dati dalle normative e dalla legge e includono le minime costrizioni di performance che i sistemi e l'aereo devono poter garantire. Esistono altri requisiti che la 4654 mostra e spiega ma questi esulano dal lavoro della tesi. Sono requisiti funzionali, del cliente, ambientali e altro. Esistono anche i requisiti derivati che rappresentano sia dei requisiti di sicurezza che altro. Sono delle derivazioni degli altri requisiti e rappresentano anch'essi dei vincoli architettonici. [5]

"At each phase of the development activity, decisions are made as to how particular requirements or groups of requirements are to be met. The consequences of these design choices become requirements for the next phase of the development. Since these requirements result from the design process itself, they may not be uniquely related to a higher-level requirement and are referred to as derived requirements.

Derived requirements should be examined to determine which aircraft-level function (or functions) they support so that the appropriate failure condition classification can be assigned and the requirement validated. While most such requirements will not impact the higher-level requirements, some may have implications at higher levels. Derived requirements should be reviewed at progressively higher system levels until it is determined that no further impact is propagated". Queste rappresentano i requisiti derivati impattano enormemente sulla scelta del design del sistema dell'aereo.

"Derived requirements may result from the decision to select a separate power supply for equipment performing a specific function. The requirements for the power supply, including the safety requirements, are derived requirements. The hazard resulting from the fault or failure of the function supported by the power supply determines the necessary development assurance level.
-Derived requirements may also result from architecture choices. For example, selecting a triplex architecture for achieving a high integrity functional objective would have different consequences and different derived requirements from selection of a dual monitored architecture for achievement of the same objective." [5]
In questi requisite e vincoli viene per esempio indicato che bisogna avere una sorgente di potenza separata per ogni sistema, come indicato anche nelle CS. L'altro vincolo indica un'architettura di ridondanza tripla per garantire la sicurezza dei sistemi 'high integrety functional objective'.
*"**System architectural features, such as redundancy, monitoring, or partitioning, may be used to eliminate or contain the degree to which an item contributes to a specific failure condition.** System architecture may reduce the complexity of the various items and their interfaces and thereby allow simplification or reduction of the necessary assurance activity."*
In questo requisite vengono fornite alcune tipe di scelte architetturali, quali ridondanza, monitoraggio e partizione, che aiutano a minimizzare le failure.
"If architectural means are employed in a manner that permits a lower assurance level for an item within the architecture, substantiation of that architecture design should be carried out at the assurance level appropriate to the top-level hazard"
"Redundancy is a technique for providing multiple implementations of a function either as multiple items, or multiple lanes within an item. It is a design technique based on the
assumption that a given set of faults with the same system effect will not occur simultaneously in two or more independent elements. Redundancy is required to provide fail-safe design protection from catastrophic failure conditions and may be necessary to meet the requirements associated with the more severe failure condition classifications. The redundant elements may be parallel or backup, and their designs may be similar or dissimilar". Questo requisite mostra cosa significhi ridondanza e perché sia una delle scelte migliori per quanto concerne i vincoli architettonici e la sicurezza. "*An architectural strategy incorporating dissimilarity can be a powerful means of reducing the potential for errors in requirements or in design implementation to cause serious effects. When dissimilarity is used as a means of design error containment, the degree of credit should be related to the type and scope of design errors shown to be covered by the dissimilarity method used. For example, dissimilar design implementations of the same function can provide containment coverage for some types of implementation errors but not for function requirements errors".*
Viene indicato dalla 4754 il concetto di dissimilarità e come questo possa essere un aiuto nelle scelte architettoniche. Ad esempio, implementazione di progettazione diverse della stessa funzione possono fornire copertura di contenimento per alcuni tipi di errori di implementazione ma non per errori relativi ai requisiti della funzione. Cioè, più componenti che svolgono quella funzione che funzionano diversamente. La sae 4754 presenta una serie di architetture di esempio e illustra l'effetto che tali architetture potrebbero avere sul livello di garanzia dello sviluppo dell'articolo. I sistemi aeronautici reali possono comportare combinazioni di queste architetture o architetture alternative che non sono conformi a nessuno di questi esempi. Se l'architettura viene utilizzata come mezzo per far fronte a generici errori di progettazione, sarà necessario integrare le valutazioni quantitative dell'architettura con valutazioni qualitative. Le questioni relative alla comunanza delle fonti di informazione di progettazione, alla comunanza della metodologia di progettazione, alla maturità della tecnologia e alla comprensione dell'applicazione, tra le altre, sono spesso affrontate qualitativamente. La prima di queste architetture è la partizione. "***Where an item contributes to aircraft functions of different criticality, a partition can be used to limit the cross-functional effect of system design errors in separate parts of the item.***
Partitioning is a design technique for providing isolation to contain and/or isolate faults and to potentially reduce the effort necessary for the system verification processes. Where an item contributes to aircraft functions of different criticality, a partition can be used to limit the cross-functional effect of system design errors in separate parts of the item. The design that provides the partition should be developed at the development assurance level corresponding to the highest applicable function failure condition classification. The design within a partitioned portion can be developed to the development assurance level corresponding to the most severe failure condition classification for that portion."

In questo vincolo, viene introdotto il concetto di partizione e spiegato nei dettagli. Il partizionamento, in pratica, è una tecnica di progettazione per fornire isolamento per contenere e/o isolare i guasti e ridurre potenzialmente lo sforzo necessario per la verifica del sistema processi. [5]

SAE ARP4754

TABLE 3 - System Development Assurance Level Assignment

Failure Condition Classification	System Development Assurance Level
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

FIGURA 19

La figura 19 mostra l'assegnazione dei DAL, dei livelli di rischio, per i sistemi, o i componenti, in base alla classificazione delle failure condition che le failure di questi sistemi possono provocare. "***Dissimilar, Independent Designs Implementing An Aircraft-Level Function: A parallel, dissimilar, multiple channel architecture may provide protection from both random physical failures and anomalies due to design errors. In these cases, it may be possible for the development assurance levels for the individual channels to be selected below that associated with the top-level failure condition classification. An analysis should substantiate the dissimilarity and independence of: implementation, requirements, algorithms, data, environment, and other potential sources of design error"***
Questa architettura composta da sistemi paralleli ed indipendenti che svolgono la stessa funzione. Creare un'architettura con multipli canali può portare ad una protezione da random failure.
"Systems guidance in DO-178B recommends that for parallel architectures at least one software component must have the software level associated with the most severe failure condition classification for the system function. Such an architecture would fall into the category described in 5.4.1.3. In ARP4754 parallel architectures are further subdivided by noting that there are some system architectures where the dissimilarly and independence of subsystems may be sufficiently clear as to warrant a reduction in level for each subsystem". Un vincolo di probabilità di failure importantissimo è dato dalla DO-178 e SAE 4754, in cui si dice che nelle architetture parallele almeno un sistema deve essere progettato con il livello più severo e conservativo possibile. Anche se i due sistemi sono simili e tecnicamente possono avere lo stesso livello di severità, comunque uno di questi sistemi dovrà avere il livello DAL più severo. La terza architettura che la 4754 presenta come esempio di sicurezza è la Dissimilar Designs Implementing an Aircraft Level Function.
"***If multiple portions cannot be shown to be dissimilar under 5.4.1.2, then the primary portion should be developed to the development assurance level associated with the most severe failure condition classification of the function. In this case, the secondary portion(s) provides the function after a random hardware failure of the primary portion. Both primary and secondary portions can execute full time, or the secondary portion can be a "hot spare" that is reverted to after failure of the primary portion. The secondary portion(s) can be assigned a development assurance level one below that of the primary portion, but not less than Level C, if:***
a. The primary portion has a random hardware failure rate for loss of function less than 1.0x10-5 for catastrophic failure conditions, or less than 1.0x10-4 for hazardous failure conditions; and
b. The primary portion is always used unless it has failed; and
c. The secondary portion does not contribute to fault detection, and can not cause the primary portion to fail."
La successiva architettura della 4754 è Active-Monitor Parallel Design:

"The active-monitor parallel architecture represents the situation where both the active and monitor portions are necessary to meet the integrity requirements. This architecture provides detection of random physical failures and with sufficient independence may detect anomalies due to design error. The most severe failure condition classification establishes the development assurance level necessary for at least one channel and the channel independence. The other channel may have a lower level of development assurance, as necessary to meet availability requirements."

In questa architettura parallela a monitor attivo, sia la parte attiva che quella di monitoraggio sono necessarie per soddisfare i requisiti di integrità. Questa architettura fornisce il rilevamento di guasti fisici casuali e con sufficiente indipendenza può rilevare anomalie dovute a errori di progettazione. La classificazione delle condizioni di guasto più grave stabilisce il livello di garanzia dello sviluppo necessario per almeno un canale e l'indipendenza del canale. L'altro canale potrebbe avere un livello inferiore di garanzia dello sviluppo, se necessario per soddisfare i requisiti di disponibilità. L'ultima architettura di esempio che la 4754 ci mostra è Backup Parallel Design:

"There may be items in a system that function as a backup to other items. That is, they are required to operate only after the other system items have failed. If the primary system satisfies the integrity requirements without the backup and the probability of the random failure rate for loss of function of the primary items is very low (1.0x10-7, if the failure condition is catastrophic, or 1.0x10-5, if the failure condition is hazardous), then the development assurance level of the backup may be assigned up to two levels below that of the top-level hazard, but not less than level D. This assignment is subject to the agreement of the certification authority. Development assurance of the system architecture leading to the determination of the availability requirement of the backup should be at the level of the most critical system failure condition".

Questa architettura rappresenta e implementa il concetto di ridondanza funzionale, cioè un componente che all'occorrenza può svolgere altre funzioni diverse da quelle che abitualmente opera. Potrebbero esserci elementi in un sistema che funzionano come backup per altri elementi. Cioè, devono funzionare solo dopo che gli altri elementi del sistema hanno fallito. Se il sistema primario soddisfa i requisiti di integrità senza il backup e la probabilità del tasso di guasto casuale per la perdita di funzionalità degli elementi primari è molto bassa (*1.0x10-7, se la condizione di guasto è catastrofica, o 1.0x10-5, se la condizione di guasto è pericolosa*), il livello di garanzia dello sviluppo del backup può essere assegnato fino a due livelli inferiori a quello del pericolo di livello superiore, ma non inferiore al livello D. Questa assegnazione è soggetta all'accordo dell'autorità di certificazione. La garanzia dello sviluppo dell'architettura del sistema che porta alla determinazione del requisito di disponibilità del backup dovrebbe essere al livello della condizione di guasto del sistema più critica. La figura della SAE 4754 mostra i livelli di classificazione del rischio per ogni architettura presentata. (figura 20 e figura 21)

TABLE 4 - Examples of Architecturally Derived Assurance Levels and Constraints

	Architecture (see note 1)	Failure Condition Classification Catastrophic	Failure Condition Classification - Severe-Major/Hazardous
1	Partitioned Design (Multiple Failure Categories)	Level A for the system including establishment of the partition	Level B for the system including establishment of the partition
	Within each partitioned portion	Level corresponding to the most severe failure condition classification within that partitioned portion	Level corresponding to the most severe failure condition classification within that partitioned portion
2	Dissimilar, Independent Designs Implementing an Aircraft-Level Function (notes 2 and 3)	Level A for the system including establishment of dissimilarity and independence	Level B for the system including establishment of dissimilarity and independence
	Portions (note 4)	Level B (note 5 and 5.4.1.2)	Level C (note 5 and 5.4.1.2)
3	Dissimilar Designs Implementing an Aircraft Level Function (note 2)	Level A for the system including establishment of partition between the portions	Level B for the system including establishment of partition between the portions
	Primary Portion	Level A	Level B
	Secondary Portion	Level B (note 5 and 5.4.1.3)	Level C (note 5 and 5.4.1.3)
4	Active/Monitor Parallel Design (note 2)	Level A for the system	Level B for the system
	Active and Monitor Portions	At least one portion to Level A; the other portion to at least Level C (notes 5 and 6)	At least one portion to Level B; the other portion to at least Level C (notes 5 and 6)
5	Backup Parallel Design (note 2)	Level A for the system	Level B for the system
	Primary Portion	Level A	Level B
	Backup Portion	Level C (note 5)	Level D (note 5)

FIGURA 20

Note 1: These architectures illustrate specific development assurance situations; practical systems may employ a wide range of alternative architectures.
Note 2: The logic to determine switching/voting/fault detection between elements should be developed to the highest level applicable.
Note 3: It is especially important to obtain the agreement of the certification authority as outlined in 4.1 before adopting this method.
Note 4: Portions can refer to an item, a group of items or an entire subsystem in this case.
Note 5: Availability requirements must be satisfied and the constraints of the applicable paragraph followed.
Note 6: The development assurance level is dependent on the classification of any failure condition not constrained by the monitor.

No shade: applies to the system as a whole.
Shaded: applies to portions of the system, where system architecture permits

FIGURA 21

"***Calculating the event probability of a failure condition should include the time during which a latent failure can persist. The time exposure during which backups and/or protective mechanisms could fail and/or remain failed prior to repair should be considered. In many cases, the failures are detected by normal flight crew observation, or during periodic power-up or self test routines. In some cases, the detection of latent failures is associated with the interval between equipment shop tests or specific aircraft***

maintenance tests". Questo requisite porta all'attenzione il problema delle latent failure e i loro effetti. Infatti, dice che, quando si calcola la probabilità di una failure condition bisogna considerare il tempo in cui una laten failure persiste.

"The need to provide a fail-safe design will serve to separate a function from its applicable backups and/or protective mechanisms or may separate redundant backups and/or protective mechanisms from each other. Once the applicable separation and isolation requirements have been identified, the common cause analysis should proceed to address the common cause fault potential across each boundary, and should identify the fault containment strategies to be used, along with the rationale supporting the fault coverage provided."

Questa è l'ultima considerazione sulla sicurezza delle architetture e del fail-safe design che riassume tutto quello già detto e spiegato. Le attività di valutazione della sicurezza e i relativi obiettivi per ciascuna classificazione delle condizioni di guasto sono descritti nelle sezioni successive di questo documento come riportato nella figura 22. (*Nota: i requisiti relativi alla sicurezza a livello di elemento vengono derivati durante il processo PSSA*). Linee guida e metodi dettagliati per condurre le varie valutazioni sono descritte in ARP4761. Dalla SAE ARP 4761 [6] non sono stati inseriti vincoli perché in quella SAE vengono spiegati i metodi di verifica, come funzionano e come usarli con esempi, quindi non aveva senso inseirli in questo lavoro di Tesi, perché si sta parlando di generalità. Un elemento però va inserito. Alla fine, nella SAE 4761 viene fatto un esempio di studio di affidabilità e certificazione per un sistema frenante di una ereo fittizio di grosse dimensioni. Questo sistema è stato preso in esame e ampliato agli spoiler e agli inverosri di spinta per costruire il design space del sistema su ADORE, come si vedrà nei prossimi capitoli. L'unico elemento di safety generale è il seguente: "*An operational objective of a normal braking system with a failure rate no greater than 1E-4 per flight is imposed. Discussions with potential BSCU vendors reveal that a 6.6E-6 per hour failure rate is not feasible with a single item. A decision is made to require two BSCUs".* Questo vincolo standard generlae dice che per avere un'architettura del sistema certificabile allora devo per forza almeno due unità BSCU distinte. Questo sarà utilizzato nei successivi capitoli sul check certificativo. [6]

SAE ARP4754

TABLE 5

Derived from FHA (see 6.1) Failure Condition Classification	Derived from FHA (see 6.1) Development Assurance Level	Safety Objectives Fail-Safe	Safety Objectives Quantitative Requirement (Note 1)	Safety Analyses PSSA	Safety Analyses SSA	Safety Analyses Common Cause
Catastrophic	A	Required, {5.4}	P $<10^{-9}$	{6.2, 6.5}	{6.3, 6.5}	{6.4}
Hazardous/ Severe-Major	B	May be needed, {5.4}	P $<10^{-7}$	{6.2, 6.5}	{6.3, 6.5}	{6.4}
Major	C	May be needed, {5.4}	P $<10^{-5}$	{6.2}	{6.3}	May be needed, {6.4}
Minor	D	No	None	(Note 2)	(Note 2)	None
No Safety Effect	E	No	None	(Note 3)	None	None

Paragraph references shown in { }.
Note 1: According to AC/AMJ 25.1309; rate shown per flight hour
Note 2: According to AC/AMJ 25.1309 par 8.2 ... an analysis of physical and functional isolation from other functions and systems may be required.
Note 3: Required to the level necessary to establish that no safety effect exists.

FIGURA 22

3.4 I Vincoli nei capitoli della CS-23

I vincoli presentati nei paragrafi precedenti si basano sulle normative relative ai grandi aerei, ma anche i piccoli aerei, monomotori o piccoli bimotori, hanno i loro vincoli sui sistemi di bordo. Questi vincoli si trovano nella normativa 'gemella' della CS-25, la CS-23. C'è un piccolo particolare sulla CS-23, diversa dalla CS-25. La CS-23 ha subito una riscrittura che ne ha modificato la struttura interna, in maniera pesante. Questo ha portato a riscrivere o togliere alcuni elementi, dando alle aziende manufatturiere i vincoli e le parti tolte. E quindi giusto che in questo paragrafo vengano inserite sia i vincoli della CS-23 emendamento 4, prima della riscrittura, e i vincoli della CS-23 emendamento 5, dopo la riscrittura. I capitoli e la struttura della CS-23 prima della riscrittura sono identici alla CS-25, dopo la riscrittura cambia la struttura, ma non la sostanza. [17] [18]

CAPITOLO 23.672

"(b) The design of the stability augmentation system or of any other automatic or power-operated system must permit initial counteraction of failures without requiring exceptional pilot skill or strength, by either the deactivation of the system, or a failed portion thereof, or by overriding the failure by movement of the flight controls in the normal sense.

(c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system –

(1) The aeroplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved operating limitations that is critical for the type of failure being considered;"

Un vincolo sui Stability augmentation and automatic and power operated systems molto simile a quello della CS-25.

CAPITOLO 23.677

"(b) Trimming devices must be designed so that, when any one connecting or transmitting element in the primary flight control system fails, adequate control for safe flight and landing is available with –

(1) For single-engine aeroplanes, the longitudinal trimming devices; or

(2) For twin-engine aeroplanes, the longitudinal and directional trimming devices."

In questo vincolo sul sistema del trim si vede come ci sia una distizione tra aereo monomotore e bimotore. Questa differenza si vedrà anche per altri vincoli sui sistemi.

CAPITOLO 23.701

"(a) The main wing flaps and related movable surfaces as a system must

(2) Be designed so that the occurrence of any failure of the flap system that would result in an unsafe flight characteristic of the aeroplane is extremely improbable;"

CAPITOLO 23.729

"(c) Emergency operation. For a landplane having retractable landing gear that cannot be extended manually, there must be means to extend the landing gear in the event of either –

(1) Any reasonably probable failure in the normal landing gear operation system; or

(2) Any reasonably probable failure in a power source that would prevent the operation of the normal landing gear operation system."

Questo vincolo è molto simile a quello relativo alla CS-25, con l'aggiunta che in questo c'è specificato che il carrello sia retrattile. Per il resto è uguale, non deve verificarsi un guasto che comprometta l'atterraggio.

CAPITOLO 23.735

"(d) If anti-skid devices are installed, the devices and associated systems must be designed so that no single probable malfunction or failure will result in a hazardous loss of braking ability or directional control of the aeroplane."

Il vincolo sul Sistema di frenata delle ruote è meno complesso della CS-25, per via della semplicità dell'aereo. Sull'anti-skid il vincolo è uguale, bisogna che il suo guasto non sia un single failure.

CAPITOLO 23.745

"(a) If nose/tail-wheel steering is installed, it must be demonstrated that its use does not require exceptional pilot skill during take-off and landing, in cross-winds and in the event of an engine failure or its use must be limited to low speed manoeuvring".

Vincolo normative sul carrellino anteriore, simile alla CS-25.

CAPITOLO 23.901

(a) For the purpose of CS-23, the aeroplane powerplant installation includes each component that –

(1) Is necessary for propulsion; and

(2) Affects the safety of the major propulsive units."
Vincolo sull'importanza dell'alimentazione da parte dei motori e del fatto che deve garantire sicurezza ai sistemi alimentati.
CAPITOLO 23.903
"(b) Turbine engine installations. For turbine engine installations –
(1) Design precautions must be taken to minimise the hazards to the aeroplane in the event of an engine rotor failure or of a fire originating inside the engine which burns through the engine case. (See AMC 20-128A)
(2) The powerplant systems associated with engine control devices, systems and instrumentation must be designed to give reasonable assurance that those operating limitations that adversely affect turbine rotor structural integrity will not be exceeded in service."
Vincolo della CS-23 che indica come bisogna minimizzare le failure dei motori e che questi non portino ad eventi catastrofici nel sistema alimentati da essi.
"(c) Engine isolation. The powerplants must be arranged and isolated from each other to allow operation, in at least one configuration, so that the failure or malfunction of any engine, or the failure or malfunction (including destruction by fire in the engine compartment) of any system that can affect an engine will not –
(1) Prevent the continued safe operation of the remaining engines; or
(2) Require immediate action by any crew member for continued safe operation of the remaining engine".
In questo vincolo, sia di architettura che di installazione, il motore non deve essere single failure per i sistemi alimentati e non la sua installazione non deve portare a guasti catastrofici. È un vincolo importante perché a differenza dei grandi aerei i motori dei piccoli aerei non sono sempre installati sollo le ali, ma possono avere vari posti diversi.
CAPITOLO 23.904
"If installed, an automatic power reserve (APR) system that automatically advances the power or thrust on the operating engine, when either engine fails during take-off, must comply with Appendix H of CS 23"
Vincolo che si complete con i vincoli di reliability di seguito.
CAPITOLI H23.2, H23.3, H23.5
"Automatic power reserve system means the entire automatic system used only during take-off, including all devices both mechanical and electrical that sense engine failure, transmit signals, actuate the fuel control or the power lever on the operating engine, including power sources, to achieve the scheduled power increase and furnish cockpit information on system operation."
Questa è la definizione del APR, automatic power reserve, per dare energia in caso di failure dei sistemi di potenza, da inserire nelle architetture dei sistemi come back-up energetico.
"(a) It must be shown that, during the critical time interval, an APR failure that increases or does not affect power on either engine will not create a hazard to the aeroplane, or it must be shown that such failures are improbable.
(b) It must be shown that, during the critical time interval, there are no failure modes of the APR system that would result in a failure that will decrease the power on either engine or it must be shown that such failures are extremely improbable.
(c) It must be shown that, during the critical time interval, there will be no failure of the APR system in combination with an engine failure or it must be shown that such failures are extremely improbable"
Questo vincolo rappresenta le condizioni di affidabilità, di reliability, del sistema APR. Il grado di classificazione è improbabile. I valori di guasto sono quelli della CS-25. Per la CS-23, quasi mai si raggiunge il caso dell'estremamente improbabile, per via della semplicità dei sistemi.
"(a) In addition to the requirements of CS 23.1141, no single failure or malfunction (or probable combination thereof) of the APR, including associated systems, may cause the failure of any powerplant function necessary for safety."
CAPITOLO 23.933
"(a) For turbojet and turbofan reversing systems –

(1) Each system intended for ground operation only must be designed so that during any reversal in flight the engine will produce no more than flight idle thrust. In addition, it must be shown by analysis or test, or both, that –

(i) Each operable reverser can be restored to the forward thrust position; or

(ii) The aeroplane is capable of continued safe flight and landing under any possible position of the thrust reverser.

(2) Each system intended for in-flight use must be designed so that no unsafe condition will result during normal operation of the system, or from any failure (or likely combination of failures) of the reversing system, under any operating condition including ground operation.

(b) For propeller reversing systems –

(1) Each system must be designed so that no single failure (or reasonably likely combination of failures) or malfunction of the system will result in unwanted reverse thrust under any expected operating condition. Failure of structural elements need not be considered if this kind of failure is extremely remote"

Vincolo sul Sistema degli inversori, sia per motori a getto, che per quelli con le pale. Il vincolo ricalca quello della CS-25. Anche per quanto riguarda il sistema di uso in volo.

CAPITOLO 23.953

"(a) Each fuel system for a twin-engine aeroplane must be arranged so that, in at least one system configuration, the failure of any one component will not result in the loss of power of more than one engine or require immediate action by the pilot to prevent the loss of power of more than one engine"

Questo vincolo impone la ridondanza e l'indipendenza per un bimotore dei sistemi di alimentazione carburante.

CAPITOLO 23.991

"(2) For turbine engine installations, each fuel pump required for proper engine operation, or required to meet the fuel system requirements of this subpart (other than those in subparagraph (b)), is a main pump. In addition –

(i) There must be at least one main pump for each turbine engine;

(ii) The power supply for the main pump for each engine must be independent of the power supply for each main pump for any other engine;"

il vincolo impone il minimo numero di pompe per motore e l'indipendenza delle linee di alimentazione.

"(b) Emergency pumps. There must be an emergency pump immediately available to supply fuel to the engine if any main pump (other than a fuel injection pump approved as part of an engine) fails. The power supply for each emergency pump must be independent of the power supply for each corresponding main pump".

Vincolo sulle pompe di emergenza da inserire nell'architettura. Simile alla CS-25.

CAPITOLO 23.1141

"(e) For turbine engine-powered aeroplanes, no single failure or malfunction, or probable combination thereof, in any powerplant control system may cause the failure of any powerplant function necessary for safety."

il vincolo che mostra come non sono ammissibili single failure per I sistemi di controllo del powerplant.

CAPITOLO 23.1143

"(a) There must be a separate power or thrust control for each engine and a separate control for each supercharger that requires a control.

(b) Power, thrust and supercharger controls must be arranged to allow –

(1) Separate control of each engine and each supercharger; and

(2) Simultaneous control of all engines and all superchargers.

(d) The power, thrust or supercharger controls for each engine or supercharger must be independent of those for every other engine or supercharger."

Il vincolo è simile a quello della CS-25 sul controllo del motore e della spinta.

(g) For reciprocating single-engine aeroplanes, each power or thrust control must be designed so that if the control separates at the engine fuel metering device, the aeroplane is capable of continuing safe flight."

Questo vincolo è diverso dalla CS-25, perché si parla di aerei monomotori.

CAPITOLO 23.1309

"(a) Each item of equipment, each system, and each installation –
(1) When performing its intended function, may not adversely affect the response, operation, or accuracy of any –
(i) Equipment essential to safe operation; or
(ii) Other equipment unless there is a means to inform the pilot of the effect.
(2) In a single-engine aeroplane, must be designed to minimise hazards to the aeroplane in the event of a probable malfunction or failure.
(3) In a twin-engine aeroplane, must be designed to prevent hazards to the aeroplane in the event of a probable malfunction or failure.
(4) In a commuter category aeroplane, must be designed to safeguard against hazards to the aeroplane in the event of their malfunction or failure."
Il vincolo 'specchio' 23.1309 della CS-25 è leggermente differente. Infatti pone l'accento sulla distinzione del tipo di aereo, monomotore, bimotore, commuter. Per ognuno i sistemi devono cercare di minimizzare o salvaguardare contro gli hazards.
"(1) It must perform its intended function under any foreseeable operating condition.
(2) When systems and associated components are considered separately and in relation to other systems –
(i) The occurrence of any failure condition that would prevent the continued safe flight and landing of the aeroplane must be extremely improbable; and
(ii) The occurrence of any other failure condition that would significantly reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions must be improbable".
Il vincolo della probabilità di accadimento di una failure. Come nella CS-25 il sistema deve essere considerato separato in relazione agli altri sistemi. Le failure devono essere improbabili.
"(c) Each item of equipment, each system, and each installation whose functioning is required for certification and that requires a power supply, is an "essential load" on the power supply. The power sources and the system must be able to supply the following power loads in probable operating combinations and for probable durations:
(1) Loads connected to the power distribution system with the system functioning normally.
(2) Essential loads after failure of –
(i) Any one engine on two-engine aeroplanes; or
(ii) Any power converter or energy storage device.
(3) Essential loads for which an alternate source of power is required by the operating rules, after any failure or malfunction in any one power supply system, distribution system, or other utilisation system."
Questo vincolo, che rappresenta il vincolo sulle sorgenti di potenza della CS-25 è inserito nella 1309. Pone l'accento sulle power supply e sulla failure di un motore in un bimotore. Serve sempre una sorgente di potenza alternativa.
CAPITOLO 23.1321
"(b) For each twin-engined aeroplane, identical powerplant instruments must be located so as to prevent confusion as to which engine each instrument relates."
Vincolo sui sistemi degli strumenti di bordo per un bimotore.
CAPITOLO 23.1331
"(b) The installation and power supply systems must be designed so that-
(1) The failure of one instrument will not interfere with the proper supply of energy to the remaining instrument; and
(2) The failure of the energy supply from one source will not interfere with the proper supply of energy from any other source.
(c) There must be at least two independent sources of power (not driven by the same engine on twin-engine aeroplanes), and a manual or an automatic means to select each power source"
Vincolo sulle sorgenti di potenza, sull'indipendenza delle linee di potenza e sul fatto che nessuna failure non interferisca sulle restanti linee di alimentazione. Poi sui bimotori ogni motore deve avere due sistemi di potenza indipendenti e un controllo automatico e manuale.
CAPITOLO 23.1351

"(3) No failure or malfunction of any electric power source may impair the ability of any remaining source to supply load circuits essential for safe operation."
"(5) In addition, for commuter category aeroplanes, the following apply
(iv) If two independent sources of electrical power for particular equipment or systems are required, their electrical energy supply must be ensured by means such asduplicate electrical equipment, throwover switching, or multi-channel or loop circuits separately routed;"
"(c) Generating system. There must be at least one generator/alternator if the electrical system supplies power to load circuits essential for safe operation."
CAPITOLO 1437
"For twin-engine aeroplanes, engine-driven accessories essential to safe operation must be distributed among the two engines so that the failure of any one engine will not impair safe operation through the malfunctioning of these accessories."
CAPITOLO 23.2305 EMENDAMENTO 6 [17]
"(c) For aeroplanes that have a system that actuates the landing gear, there is:
(1) a positive means to keep the landing gear in the landing position; and
(2) an alternative means available to bring the landing gear in the landing position when a non-deployed system position would be a hazard"
I vincoli nella CS-23 riscritta. Ci sono cose leggermente differenti, ma la sostanza non cambia. Il vincolo è per gli aerei che hanno un sistema di retrazione del carrello.
CAPITOLO 23.2405
"(b) Any single failure or likely combination of failures of a power or thrust control system must not prevent continued safe flight and landing of the aeroplane.
(d) Unless the failure of an automatic power or thrust control system is 'extremely remote', the system must:"
CAPITOLO 23.2410
"The applicant must assess each installation separately and in relation to other aeroplane systems and installations to show that any hazard resulting from the likely failure of any system component or accessory will not:
(a) prevent continued safe flight and landing or, if continued safe flight and landing cannot be ensured, the hazards have been minimised;
(b) cause serious injury that may be avoided;"
Il vincolo riguarda l'installazione, ma è utile anche per l'architettura del sistema powerplant e dei sistemi che si avvalgono della sorgente di potenza.
CAPITOLO 23.2430
"(a) Each system must:
(1) Be designed to provide independence between multiple energy storage and supply systems so that a failure of any one component in one system will not result in the loss of energy storage or supply of another system."
Vincolo sui sistemi di supply energy. Una failure di un componente di energy supply non compromette l'energia del sistema.
CAPITOLO 23.2435
"(h) Any likely single failures of powerplant installation support systems that result in a critical loss of thrust are mitigated."
Mitigazione delle single failure che porti alla perdita di spinta.
CAPITOLO 23.2500
"(b) Equipment and systems required to comply with type certification requirements, airspace requirements or operating rules, or whose improper functioning would lead to a hazard, must be designed and installed so that they perform their intended function throughout the operating and environmental limits for which the aeroplane is certified."
CAPITOLO 23.2505
"(b) On multi-engine aeroplanes, engine-driven accessories essential to safe operation must be distributed among multiple engines."
CAPITOLO 23.2510

"(a) The equipment and systems identified in CS 23.2500, considered separately and in relation to other systems, must be designed and installed such that:
(1) each catastrophic failure condition is extremely improbable; and
(2) each hazardous failure condition is extremely remote; and
(3) each major failure condition is remote.
(b) The operation of equipment and systems not covered by CS 23.2500 does not cause a hazard to the aeroplane or its occupants throughout the operating and environmental limits for which the aeroplane is certified."
Questo è il vincolo rispettivo della 1309. Sono affermate le stesse cose della 23.1309.
CAPITOLO 23.2525
"The power generation, storage, and distribution for any system must be designed and installed to:
(b) ensure no single failure or malfunction will prevent the system from supplying the essential loads required for continued safe flight and landing.
Il vincolo delle sorgenti di potenza. Nessuna single failure preclude un atterraggio sicuro.
Questi sono i vincoli della CS-23, sia quelli pre-riscrittura, sia quelli post-riscrittura. Bisogna dire una cosa. L'emendamento 4 e l'emendamento 5-6 sono collegati, infatti, le AMC2 di ogni capitolo della CS-23 emendamento 5-6 rimanda ai rispettivi capitoli di interesse della CS-23 emendamento 4. Quindi aver inserito in questo lavoro di tesi sia i vincoli dell'emendamento 4 sia quello dell'emendamento 6 è corretto e appropriato per comprendere i vincoli dei sistemi di bordo. A volte questi vincoli sono relativi all'installazione o altro, ma possono essere sfruttati nella progettazione delle architetture dei rispettivi sistemi di brodo. Questa ultima considerazione è la stessa per la i vincoli della CS-25.

4. DESIGN SPACE E ADORE

I sistemi complessi soddisfano le esigenze degli stakeholder e forniscono valore? Si integrano facilmente, evolvono in modo flessibile e funzionano in modo semplice e affidabile? I sistemi ben architettati lo fanno!

Il mondo oggigiorno è un mondo sempre più interconnesso e complesso, si costruiscono sistemi sempre più complessi, perché un solo sistema deve essere in grado di adempiere a diverse missioni. Un tempo le missioni erano minori e i sistemi erano più isolati e semplici. Oggi i sistemi sono interconnessi come non mai e svolgono sempre più ruoli aumentando la loro complessità. Questa interconnessione non vale solo per gli stessi ambiti, ma si sta sviluppando anche tra ambiti veramente diversi tra loro. Tutto questo è l'emblema del sistema più complesso che esista, che non è artificiale, è naturale: il nostro Mondo, la Terra. Oggi il mondo e la società sono sempre più interconnessi, grazie o a causa della globalizzazione e quindi anche i sistemi artificiali devono diventare complessi come questo nuovo mondo, come questa nuova società che vuole sempre di più con meno. L'obiettivo dei sistemisti e dei certificatori è proprio quello di creare sistemi sempre più 'omnirole' e certificare sempre più sistemi diversi e complessi. Per comprendere meglio tutto questo cito un episodio che accadde poco tempo fa in un'università americana. In una delle più prestigiose università americane avvenne un incontro tra le facoltà del dipartimento di ingegneria e di cardiologia per esplorare le opportunità di interconnessione tra sistemi così diversi tra loro, l0ingegenria e il corpo umano. Avendo deciso di concentrarsi sulla costruzione di un cuore umano meccanico che fosse praticabile, il primario di cardiologia ha iniziato la sua presentazione con una descrizione delle proprietà del cuore umano. Quasi subito un ingegnere lo interruppe, chiedendo: "Deve essere per forza nel nostro petto? Potrebbe essere, ad esempio, nella coscia, dove sarebbe più facile da raggiungere?". Nessuno in sala aveva mai considerato questa possibilità. E nessuno disse niente. Ciononostante, la presentazione continuò. Ben presto si verificò un'altra interruzione; questa volta fu un altro ingegnere a chiedere: "Invece di un solo cuore, si potrebbero avere tre o quattro piccoli cuori integrati in un sistema distribuito?". Nessuno aveva pensato a questo. E ancora nessuno disse niente. L'architettura di sistema consiste nel porre e rispondere proprio a queste domande. La branca dell'ingegneria di sistema, la System engineering, pone come obiettivo quello di creare sistemi nuovi che permettano funzioni nuove e migliorate, non solo in campo aerospaziale, ma come ho appena descritto, ma anche in campi che vanno dall'ingegneria all'economia fino governo e alla geopolitica. Insomma, un mondo interconnesso e pieno di opportunità. Il certificatore dovrà poi certificare tutti questi nuovi sistemi, in modi diversi per ognuno dei campi. Per poter costruire questi sistemi così complessi e certificarli servono nuovi approcci e nuove figure che sono già nate, ma che hanno bisogno di un boost per poter soddisfare queste esigenze. Le informazioni trattate nel seguente capitolo sull'argomento design space e architetture dei sistemi sono presi da due autorevoli fonti, il libro 'System Architecture, Strategy and Product Development for Complex Systems' di Edward Crawley, Bruce Cameron, Daniel Selva, Foreword by Norman R. Augustine, editato da Global edition. [14] Questo libro riassume vari corsi dell'architettura dei sistemi tenuti al MIT. In questo caso i sistemi sono considerati i sistemi complessi in generale, non solo aeronautici. La seconda fonte è il paper 'System Architecture Design Space Exploration: An Approach to Modeling and Optimization' di J.H. Bussemaker, P.D. Ciampa, B. Nagel, nell'università DLR (German Aerospace Center), Institute of System Architectures in Aeronautics, Hamburg, Germany. La definizione di "sistema" si è evoluta negli anni. Si tratta di "due o più elementi che interagiscono tra loro". Un sistema è un insieme di entità e delle loro relazioni, la cui funzionalità è maggiore della somma delle singole entità che la compongono. Un sistema complesso ha molti elementi o entità che sono altamente interrelati, interconnessi o intrecciati. La complessità viene introdotta nei sistemi che "chiedono loro di più": più funzioni, più prestazioni, più robustezza e più flessibilità. I sistemi complessi, di qualunque genere, richiedono una grande quantità di informazioni da specificare e descrivere. Pertanto, alcune misure di complessità si basano sul contenuto informativo della descrizione del sistema. Altre misure di complessità si basano sul tentativo di categorizzare ciò che il sistema fa; si tratta di un approccio alla complessità basato sulle funzioni. I sistemi moderni possono sembrare così semplici nel concetto, però la complessità della maggior parte dei sistemi del mondo reale è enorme. Infatti, l'equazione che descrive il numero di stati possibili di un sistema composto da diversi elementi (*che interagiscono nel modo più semplice possibile*) chiamata "equazione di stato", viene giustamente chiamata "*il mostro*" [14]. E quando un sistema include gli esseri umani, come molti sistemi odierni, la sfida dell'architettura del sistema diventa ancora più immensa a causa della presenza dell'imprevedibilità dell'uomo. Ma questi sono i tipi di sistemi che si incontrano e bisogna comprendere come decostruirli e affrontarli. Nel caso ad esempio navale e aeronautico, come portaerei, petroliere e altro,

sono diversi gli elementi che devono interfacciarsi tra loro: navi da carico, aerei di vario tipo, strutture di stoccaggio, comunicazioni e, alla base di tutte le decisioni, c'era il problema della sicurezza, il pericolo sempre presente che nell'architettura si insinuino modalità di guasto singolo, come le normative e i loro vincoli (spiegate nel capitolo precedente) mostrano in maniera pesante. Un esempio di campo non aeronautico in cui operano i sistemi complessi è il mondo degli affari. Nel mondo degli affari uno dei problemi più complessi è capire come tutte le parti principali di diciassette aziende diverse potessero essere combinate per creare una sola azienda, la Lockheed Martin Corporation. Ognuno degli "elementi" in questione, delle aziende da fondere, aveva i suoi punti di forza e le sue debolezze; ognuno di essi coinvolgeva un gran numero di persone, ognuna con i propri obiettivi, le proprie capacità e i propri limiti e, cosa fondamentale per la decisione, l'insieme doveva avere una funzionalità significativamente superiore alla somma delle parti. Se non fosse stato così, non ci sarebbe motivo di pagare il premio finanziario che è implicito nella maggior parte delle fusioni e delle acquisizioni. Purtroppo, quando si affrontano questioni complesse di questo tipo, non esiste una semplice formula matematica che riveli la risposta "giusta". Una formula può dare un contributo alla risoluzione, ma poi è la creatività dell'uomo che riesce a mettere insieme i pezzi e a trovare la soluzione, anche attraverso dei compromessi, ed è per questo che l'intelligenza artificiale non potrà sostituire la creatività umana nella sistemistica. La disciplina del pensiero sistemico si dimostra uno strumento inestimabile per valutare l'esposizione, le opportunità, le sensibilità parametriche e altro ancora. Nel caso della Lockheed Martin Corporation la maggior parte delle persone giudica che la risposta sia stata "giusta", il che, per inciso, contrasta con quasi l'80% delle imprese simili. Il processo di definizione dell'architettura dei sistemi è sia una scienza che un'arte. [14] Ma in questa arte ingegneristica c'è un fenomeno darwiniano per cui i sistemi che incarnano gli errori del passato non sopravvivono; mentre quelli che incarnano architetture solide in genere sopravvivono e addirittura prosperano. Tutti pensano che I sistemi siano Freddi e rigidi, invece sorprenderà sapere che è un'arte elaborare questi intricati sistemi e fare in modo che essi svolgano tutte le funzioni. Questo è quel che rappresenta l'architettura dei sistemi complessi. La nozione più semplice di architettura è che l'architettura è una descrizione astratta delle entità di un sistema e delle relazioni tra queste entità. Nei sistemi costruiti dall'uomo, questa architettura può essere rappresentata come un insieme di decisioni. Ogni sistema costruito dall'uomo ha un'architettura. Prodotti come il software dei telefoni cellulari o smartphone, automobili e i semiconduttori (*fondamentali in questa fase della storia)* sono definiti da alcune decisioni chiave che vengono prese all'inizio del ciclo di vita del programma. Nella progettazione di sistemi complessi, molte di queste decisioni architettoniche iniziali vengono prese senza conoscere appieno la portata finale del sistema, senza sapere cosa effettivamente diventeranno. Queste prime decisioni hanno un enorme impatto sul progetto finale. Limitano l'ambito delle prestazioni, limitano i potenziali siti di produzione, rendono possibile o impossibile per i fornitori acquisire quote di fatturato post-vendita e così via. La sistemistica ha impatti non solo nella progettazione, ma nella politica, nell'economia e nella gestione e nella finanza. Dai siti dove costruire e quindi conoscere gli Stati o dove vendere e come vendere il prodotto, tutto ha a che fare con la sistemistica. Questa focalizzazione sulle decisioni consente agli architetti di sistema di scambiare direttamente le scelte per ogni decisione, piuttosto che i progetti sottostanti che rappresentano, incoraggiando così una valutazione più ampia dei concetti. Allo stesso tempo, questo linguaggio decisionale consente agli architetti di sistema di ordinare le decisioni in base all'influenza che hanno sulle prestazioni del sistema, riconoscendo che le architetture del sistema raramente vengono scelte in un colpo solo, al primo tentativo; piuttosto, sono definite in modo iterativo da una serie di scelte. L'architettura del sistema è l'incarnazione del concetto, l'assegnazione della funzione fisica/informativa agli elementi della forma e la definizione delle relazioni tra gli elementi e con il contesto circostante. Quindi per cercare di trovare la giusta forma, la giusta sequenza e la giusta soluzione vengono applicati diversi metodi di modellazione. Si cerca di ottimizzare le scelte. Questa Tesi verterà su un nuovo approccio di modellazione dell'architettura dei sistemi, il modello del design space e sull'uso del software sviluppato per questo design space, ADORE.

4.1 L'Architecture Design Space Graph (ADSG)

Il design space permette di creare un insieme di sottosistemi e da lì ottenere diverse architetture sia convenzionali che innovative, in base alle scelte, all'ottimizzazione. I nuovi approcci della sistemistica sono i modelli basati sul design space, le figure sono gli architetti di sistema. Viene presentato un metodo per modellare gli spazi di progettazione dell'architettura di sistema. Descrivo un riassunto delle funzioni del design space, che poi verranno spiegate in maniera dettagliata nel corso del paragrafo. Le informazioni del

paragrafo sono prese dal paper J.H. Bussemaker, P.D. Ciampa, B. Nagel, “System Architecture Design Space Exploration: An Approach to Modeling and Optimization”, DLR (German Aerospace Center), Institute of System Architectures in Aeronautics, Hamburg, Germany [11]. Questo metodo aiuta a consentire la possibilità di un'esplorazione sistematica degli spazi di progettazione dell'architettura, che richiede una definizione formalizzata delle decisioni architettoniche non possibili con le attuali tecniche di ingegneria dei sistemi basate su modelli. L'esplorazione sistematica dello spazio di progettazione è necessaria per ridurre i pregiudizi degli esperti e per trovare le migliori architetture possibili in ampi spazi di progettazione. Viene utilizzato un approccio basato sulla scomposizione delle funzioni per consentire la tracciabilità ai requisiti di sistema, consentendo la compatibilità con i metodi di ingegneria dei sistemi in generale e prevenendo il bias di soluzione. ***L'Architecture Design Space Graph (ADSG)*** viene utilizzato per modellare gli spazi di progettazione dell'architettura di sistema. I nodi del grafico rappresentano funzioni, componenti, scomposizioni di funzioni, concetti, istanze di componenti, attributi e porte. I legami diretti tra i nodi indicano che il nodo di origine deriva l'esistenza del nodo di destinazione. I legami tra funzioni e componenti possono inoltre essere interpretati come una mappatura, cioè, vuole stare a significare che questo componente svolge quella funzione e induce funzioni aggiuntive. I legami di incompatibilità possono essere utilizzati per modellare situazioni in cui due elementi non possono esistere insieme in un'architettura. Due tipi di nodi decisionali vengono inseriti automaticamente in base alla struttura del grafico: decisioni di opzione che si escludono a vicenda (*esecuzione di funzioni*) e decisioni di permutazione (*connessioni di porte*). Questo metodo consente la derivazione automatizzata delle decisioni architettoniche, tenendo conto delle relazioni gerarchiche tra le decisioni, e rappresenta le architetture di sistema in modo semantico. L'ADSG può essere utilizzato per formulare tre tipi di problemi di ottimizzazione gerarchici, interi misti e multi-obiettivo, in cui le variabili di progettazione sono mappate alle decisioni architettoniche e gli obiettivi e i vincoli, tra i quali quelli normativi, sono costruiti dalle metriche delle prestazioni. A causa della natura dei problemi di ottimizzazione dell'architettura, non è possibile utilizzare algoritmi di ottimizzazione basati sul gradiente e gli algoritmi di ottimizzazione dovrebbero essere in grado di risolvere problemi multi-obiettivo e gestire le implicazioni delle variabili di progettazione gerarchica. Il modello del design space, dello spazio di progettazione dell'architettura, offre una visione dettagliata del comportamento interdipendente delle decisioni architettoniche. Rispetto alla matrice morfologica, lo schema di codifica delle variabili di progetto si traduce in uno spazio progettuale (*di grandi combinazioni*) apparente ridotto. La fase di generazione dell'architettura può essere integrata con successo tra l'algoritmo di esplorazione dello spazio di progettazione e il modello di analisi dell'architettura. Vediamo in maniera dettagliata questo design space e tutto il sistema di modellazione dei sistemi, i problemi, le soluzioni, le ottimizzazioni, le caratteristiche, con lo sguardo sempre rivolto ai vincoli normativi e alla certificazione. La modellazione sistematica degli spazi di progettazione dell'architettura è necessaria quando si progettano sistemi complessi, come descritto pocanzi, per supportare gli esperti del settore nel prendere decisioni le più utili possibili e per formulare il problema di ottimizzazione necessario per esplorare l'ampio spazio di progettazione combinatoria. I metodi esistenti, però, non offrono sufficiente compatibilità con gli approcci MBSE (Model-Based Systems Engineering), non possono modellare tutti gli scenari possibili di progettazione necessari o non sono sufficientemente flessibili quando si tratta di valutare l'architettura. I sistemi complessi hanno diverse possibilità e bisognerebbe vagliarle tutte, o almeno il più alto numero possibile di scelte per ogni evenienza e funzione. Quindi bisogna trovare dei metodi che permettano di vagliate tutte le possibilità e costruire tutte le possibili architetture per soddisfare tutte le funzioni che servono e che serviranno in futuro. Viene usato, quindi, un nuovo metodo che fornisce una rappresentazione semantica dello spazio di progettazione dell'architettura, modellato come ***Architecture Design Space Graph (ADSG).*** L'ADSG rappresenta tre tipi di decisioni architetturali: mappatura funzione-componente, caratterizzazione componente e connessione componente. Il componente è alla base delle decisioni da prendere. L'ADSG è costruito da una definizione dello spazio di progettazione e decisioni architettoniche discrete che vengono inserite automaticamente in base a regole specificate. Definite le decisioni e le metriche, è possibile formulare il problema di ottimizzazione gerarchico, misto-intero e multi-obiettivo: le decisioni vengono mappate per progettare le variabili e le metriche delle prestazioni sono mappate su obiettivi o vincoli. Le prime fasi della progettazione dei sistemi complessi, viene definita l'architettura del sistema. Le decisioni prese durante questa fase sono cruciali e hanno un impatto maggiore sull'esecuzione del progetto definitivo rispetto alle decisioni prese in una fase successiva, ad esempio durante la progettazione preliminare o esecutiva. Quindi, a causa dell'importanza di queste decisioni, è necessario disporre di una buona stima dell'impatto delle diverse

decisioni per assicurarsi che venga identificata e selezionata la migliore architettura possibile, che rispetti i compromessi e le funzioni desiderate. Tuttavia, per prodotti e sistemi complessi, lo spazio di progettazione dell'architettura può essere troppo ampio per essere esplorato in modo esaustivo a causa delle enormi combinazioni di alternative. In passato, questo problema di combinazioni è stato risolto integrando il giudizio di esperti e/o utilizzando risultati storici, database, di progetti simili per prevedere l'impatto di decisioni diverse. Questi metodi, tuttavia, possono risentire del pregiudizio degli esperti, della soggettività, del conservatorismo o dell'eccessiva sicurezza, e portare a risultati erronei. Per mitigare questo, è necessario un passaggio alla valutazione quantitativa basata sulla fisica nella fase di architettura del sistema. Le tecniche sistemistiche di esplorazione dello spazio di progettazione, come l'ottimizzazione, possono essere impiegate per trovare le migliori architetture tra le molte diverse possibilità e candidati. Nell'ingegneria dei sistemi, il passaggio agli approcci basati su modelli (MBSE) permette la modellazione semantica dei sistemi. Questo ragionamento semantico è necessario per consentire l'esplorazione sistematica dello spazio di progettazione, ma non sempre offre la formalizzazione richiesta per generare, valutare ed esplorare automaticamente le architetture di sistema, come è richiesto per affrontare il problema dello spazio di progettazione. Come si vede, con l'ingegneria dei sistemi si crea un approccio a volte poco ingegneristico-tecnico, ma quasi filosofico-letterario del problema. Bisogna cercare anche di approcciarsi in maniera diversa. Approcci più formalizzati e relativamente nuovi includono metodi basati sulla matrice morfologica, l'Architecture Decision Graph e la mappatura funzione-forma. Caratteristiche importanti per consentire l'esplorazione sistematica sono l'identificazione esplicita delle funzioni e componenti e il monitoraggio delle decisioni di architettura e l'abilitazione dell'analisi quantitativa automatizzata dei candidati all'architettura. I recenti sviluppi si stanno muovendo verso nuovi modi, tra cui la considerazione anche delle connessioni tra i componenti dell'architettura nell'esplorazione dello spazio di progettazione. Il metodo del design space è un modo nuovo di intendere e lavorare con l'architettura dei sistemi. Il design space crea un nuovo metodo per modellare lo spazio di progettazione dell'architettura di sistema in modo da produrre una rappresentazione semantica e, oltre a mappare la forma con la funzione, tiene conto delle decisioni relative alla struttura dei componenti. Rispetto ai metodi di architettura MBSE convenzionali, il design space offre la formalizzazione necessaria per arrivare ad un problema di ottimizzazione. Una sfida particolare in questo tipo di formulazione è rappresentata dalla gerarchia decisionale: le decisioni architetturali possono essere attive o passive in base ai risultati di altre decisioni. Decisioni prese per uno specifico componente può portare automaticamente ad un tipo di decisione rispetto ad un altro, questo vuol dire passivo. La generazione dell'architettura viene inserita tra l'algoritmo di esplorazione dello spazio di progettazione e il modello di analisi per permettere di gestire la gerarchia decisionale e assicurarsi che l'analisi delle architetture candidate possibili vengano eseguite solo per architetture che siano internamente coerenti a tutte le funzioni volute. Come è stato detto, all'inizio di questo capitolo, l'architettura di sistema è una delle fasi del processo di ingegneria dei sistemi. Nell'ingegneria dei sistemi, il prodotto da sviluppare è trattato come un sistema: un insieme di componenti interconnessi, che insieme svolgono funzioni che non possono fornire semplicemente unendo le capacità dei singoli componenti (*cioè, il sistema è più della somma dei suoi componenti).* [11] Il sistema nel suo insieme amplifica le funzioni della somma dei suoi componenti. Quando si progetta un sistema, si fa attenzione che ciò che fa il sistema (*le sue funzioni*) sia definito prima di come lo fa il sistema (*la sua forma*). Questi due elementi sono la base del sistema, le funzioni e la forma. La forma è ciò che è il sistema, cioè ciò che viene implementato nel sistema fisico; la forma esiste. Gli elementi della forma vengono indicati come i componenti del sistema. La funzione è ciò che fa il sistema e la ragione per cui il sistema esiste poiché le funzioni del sistema servono a soddisfare le esigenze delle parti interessate. La funzione è svolta dalla forma. Si è sviluppato un approccio che porta a più modi di scomporre i progetti: ad esempio fisico, disciplinare o ibrido. Tuttavia, la scomposizione funzionale è vantaggiosa perché fornisce una scomposizione generica per qualsiasi architettura alternativa, non suggerisce un concetto di architettura (*cioè, è priva di bias di soluzione*) e le funzioni suggeriscono tipi di soluzioni fisiche piuttosto che tecnologie specifiche. Le tecnologie saranno poi inserite nella scelta dei componenti per andare ad ampliare la scelta dell'architettura. La scomposizione funzionale offre quindi un buon modo di scomporre il problema di progettazione per specificare come vengono soddisfatti i requisiti; consentire la compatibilità con i metodi di ingegneria dei sistemi in generale; fornire un framework per la definizione di nuove architetture prive di bias di soluzione. Un modo per strutturare un sistema, il suo design space ed infine la sua architettura è utilizzare l'approccio RFLP. Questo approccio è l'approccio del design space ed è lo schema logico del funzionamento del software ADORE (*di cui si parlerà nel paragrafo successivo*). Dopo che sono stati definiti i requisiti

degli stakeholder, dei clienti, vengono definite le funzioni che il sistema dovrebbe svolgere per soddisfare i requisiti. Poi, i componenti (*o, come sono stati definiti, gli elementi della forma*) vengono assegnati alle funzioni, producendo l'architettura logica, che viene estesa all'architettura fisica definendo l'interconnessione degli elementi. L'architettura logica definisce come le funzioni vengono soddisfatte assegnando i componenti alle funzioni, in base alla conoscenza disponibile su quali componenti siano in grado di soddisfare quali funzioni. Nuove tecnologie o nuovi progetti possono poi andare a rimpolpare le funzioni con nuovi componenti. I componenti stessi possono indurre a svolgere funzioni aggiuntive per svolgere la loro funzione principale. La definizione dell'architettura logica è quindi una procedura iterativa, come tutto l'aspetto dell'ingegneria dei sistemi e della certificazione, che si completa solo quando tutte le funzioni, sia primarie che indotte, secondarie, sono soddisfatte da un componente. L'architettura fisica elabora l'architettura logica fornendo maggiori informazioni su come l'architettura può essere implementata nel sistema finale. L'architettura del sistema finalizzato è quindi la combinazione dell'allocazione della funzione alla forma e delle relazioni tra gli elementi della forma. Lo sviluppo di sistemi complessi moderni deve tenere conto di un numero sempre maggiore di capacità da fornire al sistema, nonché dei limiti organizzativi, delle sfide di integrazione e comunicazione e dei vincoli derivanti da tutte le fasi di sviluppo del life cycle, come è stato detto, all'inizio di questo capitolo, un mondo sempre più interconnesso e in cui sempre meno sistemi svolgono sempre più funzioni, il concetto dell''omnirole'. Il concetto dell'omnirole è stato introdotto nei sistemi militari, nei caccia di nuova generazione, soprattutto dalla 4th generazione in poi. Dal greco 'omni', tutto, sta a significare un sistema, un velivolo, che compie ogni ruolo, ogni missione, attacco, ricognizione, pattugliamento, notturno, ad ogni condizione atmosferica. Se durante la Seconda Guerra Mondiale e all'inizio della Guerra Fredda, durante la Guerra di Corea e del Vietnam, si utilizzavano sistemi e velivoli diversi per ogni missione, verso la metà della Guerra fredda e la sua fine si è capiti che più vantaggioso inglobare diverse funzioni nello stesso sistema. Quindi tutti i sistemi di oggi dovranno essere in grado di svolgere tutti i ruoli e le missioni. Con il design space si cerca proprio di avere tutte le funzioni in un unico posto, in modo da decidere l'architettura che svolge tutti i ruoli. È un processo, come detto, logico, che coinvolge tutte le conoscenze dei componenti e delle funzioni. Idealmente ogni decisione presa in ogni fase dello sviluppo dovrebbe essere valutata lungo l'intero ciclo di vita. La gestione di tale complessità di sviluppo porta necessariamente a sviluppare un nuovo paradigma di sviluppo del sistema. Qui si sviluppa il design space, sviluppato dal DLR "*Institute of Systems Architecture in Aeronautics*". Questo si basa su un framework concettuale basato su modelli per l'architettura, la progettazione e l'ottimizzazione di sistemi aeronautici complessi. Questo approccio e metodo avrà un impatto enorme sul ciclo di vita del prodotto, cioè una drastica riduzione dei tempi e dei costi associati allo sviluppo, attraverso una maggiore trasparenza, efficienza e tracciabilità dei processi di progettazione e decisionali. Il framework concettuale estende l'ambito dei metodi di progettazione e ottimizzazione a tutte le fasi del ciclo di vita dello sviluppo di sistemi complessi. Questo metodo, da un lato, tende ad accelerare le fasi di architettura a monte, compreso il trade-off degli obiettivi, la definizione degli scenari e i requisiti tenendo conto di tutti gli stakeholder coinvolti, la progettazione e l'ottimizzazione dell'architettura del sistema di interesse (*ad esempio un velivolo),* o Sistema di Sistema, in fase di sviluppo. Dall'altro lato, tende ad accelerare le fasi di progettazione del prodotto a valle, compresa la selezione delle capacità necessarie per ogni fase di progettazione (*concettuale, preliminare, dettagliata),* l'integrazione nei processi di progettazione e l'implementazione di sistemi di progettazione (*ambienti computazionali*), per l'esplorazione dello spazio progettuale e la scelta della soluzione ottimale. L' architettura del framework concettuale ha una struttura a strati. I cinque strati identificano i livelli principali e le principali attività all'interno di ogni livello sono: [11]

1)*Livello aziendale*: modellazione e ottimizzazione di obiettivi e processi decisionali orientati al compromesso tra le politiche da parte dell'impresa e le richieste del cliente.

2) *Livello System of Systems*: architettura e progettazione di scenari complessi per un determinato insieme di funzionalità, consentendo un compromesso tra il concetto di operazioni.

3) *Livello di sistema complesso*: progettazione e ottimizzazione dell'architettura (ADO) di un sistema complesso di interesse per un dato insieme dei requisiti e del concetto di operazioni, consentendo il compromesso tra le varie architetture candidate.

4) *Livello del sistema di sviluppo:* implementazione e funzionamento di un sistema e processi di sviluppo (processo MDAO) per la progettazione e l'ottimizzazione del sistema di interesse, per una data architettura e progettazione per la strategia X (costi minimi) e per la dimensione dello spazio progettuale.

5) *Livello di competenza*: fornire capacità eterogenee (analisi disciplinare) e servizi disponibili, consentendo la progettazione e l'ottimizzazione del sistema.
L'implementazione del concetto del design space è supportata dallo sviluppo di nuovi metodi e approcci di progettazione, sfruttando l'ingegneria del design digitale e le tecnologie di modellazione. Tutto il modello del design space si base, quindi su 3 passaggi:
1) *Definizione dello spazio progettuale dell'architettura:* lo spazio progettuale definisce le possibili componenti e le loro connessioni. Tale approccio dovrebbe garantire che l'ingegnere possa avere una visione d'insieme su quali sono le diverse decisioni architettoniche e quali istanze architettoniche sono contenute nello spazio di progettazione.
2) *Interpretazione dello spazio progettuale e costruzione del cosiddetto Architecture Design Space Graph (ADSG):* gli elementi dello spazio progettuale sono integrati nell'ADSG,
3)*Derivazione delle decisioni progettuali*: le decisioni progettuali dell'architettura vengono inserite automaticamente nell'ADSG in base a regole definite dalla metodologia. Una volta completati questi passaggi, l'ADSG può essere utilizzato per generare istanze di architettura e formulare problemi di ottimizzazioni.
Il design space, quindi, inserisce in un'unica 'grande architettura logica' tutte le possibili scelte, componenti, funzioni che possono servire per il funzionamento del sistema, in base alle esigenze dei clienti. Una volta creato questo grande schema architettonico logico si andranno a fare le scelte dei vari componenti, tecnologie inseriti per individuare l'architettura migliore, che rispetta le esigenze del cliente, i vincoli normativi e altri parametri scelti dall'azienda. Questa architettura può essere convenzionale, se si vogliono utilizzare componenti dello stato dell'arte, oppure innovativa, se invece si inseriscono componenti di nuova generazione. La definizione dello spazio di progettazione contiene le informazioni necessarie per costruire il grafico dello spazio di progettazione dell'architettura. Definisce quali funzioni e componenti fanno parte del design space e come sono collegati tra loro. Si presume che le decisioni coinvolte nella decisione sull'architettura di un sistema possano essere assegnate a tre categorie: decidere quali componenti svolgono quali funzioni, caratterizzare i componenti e collegare i componenti. Per lo sviluppo del design space, cioè del nuovo metodo di modellazione dello spazio di progettazione dell'architettura si fanno i seguenti presupposti e passi di progettazione:

- Gli stakeholder e le loro esigenze sono identificati, e da ciò sono definiti i requisiti. Si assume che il processo di definizione dei requisiti avvenga prima del processo di architettura. Quando il processo di architettura del sistema viene avviato, si iniziano a definire le funzioni principali del sistema. Ci possono essere interazioni tra la definizione dei requisiti e le fasi di progettazione, ma ci sarà almeno un punto di partenza su cui basare lo spazio di progettazione dell'architettura.
- Le scelte progettuali nell'architettura di sistema sono sufficientemente rappresentate da decisioni relative all'adempimento delle funzioni, alla caratterizzazione dei componenti e alle connessioni dei componenti. Queste tre categorie di decisioni coprono tutte le scelte progettuali generali dei problemi di progettazione dell'architettura di sistema.
- Ogni funzione è soddisfatta ed eseguita, da un componente: se ci sono modi diversi di svolgere una funzione, deve essere presa una scelta progettuale le cui opzioni si escludono a vicenda. Alcuni approcci di architettura di sistema consentono a più componenti di svolgere una funzione. Tuttavia, è possibile definire esplicitamente le opzioni che non si escludono a vicenda come opzione aggiuntiva che si escludono a vicenda.
- I componenti possono derivare, e indurre, funzioni aggiuntive: questo porta a un processo a zig-zag, e il processo di architettura può continuare solo una volta che tutte le funzioni sono state soddisfatte.
- La connessione dei componenti viene effettuata dopo aver mappato i componenti alle funzioni. La necessità di una connessione tra i componenti non può quindi essere utilizzata per includere questi componenti nell'architettura, solo la necessità di soddisfare le funzioni può farlo.
- È possibile valutare quantitativamente le prestazioni delle architetture. Questo consente l'uso di tecniche sistematiche di esplorazione dello spazio di progettazione come un Design of Experiments o l'ottimizzazione per trovare la migliore architettura per risolvere il problema in questione.

Spiegato cosa sia il design space e come funziona la logica dietro il suo utilizzo per la scelta dell'architettura migliore, bisogna descrivere gli elementi che compongono elementi dello spazio di progettazione, il design space. [11]

1. Funzioni

Le funzioni specificano cosa deve fare il sistema. Possono essere definiti come neutrali o specifici della soluzione. Si può affermare che una funzione sia neutrale rispetto alla soluzione quando non induce alcun pregiudizio verso qualche soluzione per soddisfare la suddetta funzione. Le funzioni che rappresentano il valore del sistema al contesto del sistema stesso, cioè tutto ciò con cui il sistema interagisce ma non è parte del sistema stesso, sono definite funzioni di contorno. Il progettista sceglie le funzioni al contorno quando definisce lo spazio di progettazione, sulla base delle esigenze e dei requisiti degli stakeholder identificati. Queste funzioni saranno sempre presenti. Le scelte architettoniche alla fine definiscono come queste funzioni vengono soddisfatte. Spesso le funzioni al contorno sono anche funzioni neutrali rispetto alla soluzione.

2. Mappatura dei componenti alle funzioni

I componenti svolgono funzioni e sono inclusi in un'architettura solo se sono necessari per svolgere una funzione. Ogni componente descritto nel design space definisce le funzioni che adempie e le funzioni di cui ha bisogno, che induce, per adempiere alle sue funzioni. In un'architettura di sistema, solo un componente può svolgere una funzione. Ciò significa che, se sono presenti più componenti che possono svolgere una funzione, è necessario effettuare una scelta progettuale, cominciando a creare l'architettura desiderata. La mappatura dei componenti alle funzioni è il primo passo nel processo di architettura e queste decisioni sono quindi anche le prime decisioni da prendere. È possibile definire scomposizioni di funzioni, che mappano semplicemente una funzione su una o più altre funzioni. Le scomposizioni di funzioni possono essere utili per gestire la complessità. Una decomposizione che mappa una funzione su più altre funzioni, in effetti significa che la funzione di origine si comporta come la combinazione delle funzioni di destinazione. La funzione di origine emerge dalle funzioni di destinazione. Il passaggio dalla funzione di origine alle funzioni di destinazione può essere visto come funzione zoom, poiché la funzione emersa è rappresentata da delle funzioni più dettagliate. Componenti, concetti e scomposizioni di funzioni sono tutti trattati come elementi di mappatura di funzioni. Nessun tipo ha priorità su un altro.

3 Caratterizzazione dei componenti

Una volta che i componenti sono stati mappati alle funzioni, il passo successivo nel processo di architettura è la caratterizzazione dei componenti. I componenti possono essere caratterizzati in due modi:

- Caratterizzazione per numero di istanze. I componenti hanno istanze di componenti e possono esistere più istanze di componenti e la quantità di istanze può essere una decisione di progettazione. Questo può ad esempio essere utilizzato per modellare la distribuzione o la ridondanza dei componenti.
- Caratterizzazione per attributi. Componenti o istanze di componenti possono avere attributi e la selezione di valori per gli attributi è una decisione di progettazione. La selezione dei valori degli attributi è modellata utilizzando lo stesso meccanismo delle porte, tale che sono possibili schemi decisionali più complicati rispetto alle sole opzioni che si escludono a vicenda.

4 Collegamento dei componenti

Le connessioni tra componenti sono modellate utilizzando le porte. Le relazioni formali possono rappresentare qualsiasi cosa, dalle relazioni spaziali, ai flussi di massa/energia/informazione e alle relazioni immateriali come l'appartenenza e la sequenza. Nessuna restrizione verrà fatta sul tipo di connessione; questo dipenderà interamente dall'interpretazione delle connessioni dei componenti durante la valutazione delle prestazioni delle architetture generate. Le connessioni vengono effettuate da una sorgente a una destinazione e per le porte si tratta rispettivamente di porte di uscita e di ingresso. Le porte rappresentano le interfacce delle istanze dei componenti e sono caratterizzate da un Identificatore, per cui le connessioni sono possibili solo tra porte con lo stesso identificatore; dal numero di istanze, che può essere una decisione di progettazione; da connessioni o no tra porte dello stesso componente; da connessioni ripetute; dalla specifica del grado di connessione, in cui si specifica il numero di connessioni per istanza di porta, che può essere specificato come numero esatto, un intervallo o un limite inferiore; dalla rilevanza della sequenza di connessione, per cui se è rilevante, il problema di connessione si trasforma in un problema di permutazione, altrimenti in un problema di selezione. Questi tipi di caratterizzazioni consentono di specificare problemi di connessione complessi, con molte possibili sequenze di connessione possibili. Questo tipo di problemi di connessione sono un importante contributo al possibile enorme numero di alternative. Se per un determinato problema di connessione della porta non è possibile effettuare le connessioni (*ad esempio se ci sono due porte che emettono una connessione ciascuna, ma c'è solo una porta di ingresso a cui connettersi*), significa che l'architettura non è fattibile.

5 Vincoli di incompatibilità

L'esistenza di elementi di architettura nelle istanze di architettura si basa sulle scelte effettuate su quali elementi di forma utilizzare per adempiere alle funzioni. Attraverso il meccanismo di adempimento di funzioni e derivazione di funzioni aggiuntive, la compatibilità dei componenti può essere stabilita implicitamente. Inoltre, le connessioni delle porte possono naturalmente essere utilizzate per modellare le connessioni richieste tra i componenti e quindi forzare l'esistenza di un componente se esiste anche l'altro. Queste opzioni consentono all'ingegnere di sistema di modellare complicate logiche di (in)compatibilità. Tuttavia, per evitare di dover utilizzare le porte per modellare implicitamente i vincoli di (in)compatibilità, viene messa a disposizione dell'ingegnere di sistema un'opzione aggiuntiva, più esplicita, e cioè il vincolo di incompatibilità. Tale vincolo può essere specificato tra qualsiasi funzione, componente, concetto o scomposizione ed è bidirezionale: se in uno degli elementi connessi dall'incompatibilità esiste in un'istanza dell'architettura, l'altro elemento non può esistere. I vincoli di incompatibilità non sono transitivi: se esiste un vincolo di incompatibilità tra gli elementi A e B, e tra gli elementi B e C, gli elementi A e C possono ancora esistere insieme in una possibile architettura.

6 Metriche delle prestazioni

Le metriche delle prestazioni registrano prestazioni quantificabili dell'architettura nel suo complesso oppure la registrano per un singolo elemento e specificano come le diverse istanze dell'architettura possono essere confrontate tra loro. Possono essere interpretati come obiettivi o vincoli nel contesto di un problema di ottimizzazione. Le metriche delle prestazioni possono essere associate a funzioni, componenti o istanze di componenti.

7. Variabili di progettazione aggiuntive

Ulteriori variabili di progettazione possono essere definite per le funzioni, i componenti o per le istanze di componenti.

Come detto, all'inizio del capitolo, il design space è rappresentato utilizzando l'Architecture Design Space Graph (ADSG). L'ADSG è un grafico dove i nodi rappresentano alcuni elementi dell'architettura, come funzioni, componenti e porte. Un'istanza di architettura viene creata dallo spazio di progettazione dell'architettura, prendendo le decisioni architettoniche. Prima vengono prese le decisioni di opzione, poi le decisioni di permutazione. Le decisioni di opzione vengono prese per prime, perché determinano quali nodi sono presenti nel grafo. Una volta che tutte le decisioni di opzione sono state selezionate, vengono prese le decisioni di permutazione, creando connessioni tra i corrispondenti nodi di origine e di destinazione. Questo è il processo decisionale del design space. Processo che sta ad indicare la trasformazione di un ADSG che rappresenta l'intero spazio di progettazione dell'architettura in uno che rappresenta un'istanza specifica dell'architettura. Questo viene fatto esaminando le decisioni e per ognuna di esse scegliendo quale opzione prendere. Va comunque detto che il ragionamento su quale opzione prendere proviene da fonti esterne, tra i quali processi di ottimizzazione oppure esplorazione di funzioni migliori e dati in possesso dell'azienda e dell'ingegnere. È giusto vedere in dettaglio il processo decisionale, come prendere le decisioni nella creazione di un'architettura specifica del design spcae. Le decisioni di opzione sono decisioni con opzioni multiple che si escludono a vicenda. Una volta selezionata una delle opzioni, il nodo di decisione viene rimosso dal grafico, il nodo di origine viene connesso al nodo di opzione e le opzioni rimanenti e i relativi nodi derivati vengono rimossi dal grafico. Tutti i nodi che derivano direttamente (*cioè, non attraverso un nodo di decisione)* [11] dalle funzioni al contorno sono considerati esistere incondizionatamente. Tutti gli altri nodi esistono in modo condizionale e possono essere confermati dopo essere stati selezionati in una decisione di opzione o rimossi dal grafico. Le decisioni di opzione non sono definite esplicitamente nella definizione del design space. Piuttosto, viene inserita automaticamente un'opzione-decisione per diversi schemi grafici. I nodi decisionali possono esistere in modo condizionale, nel senso che possono essere rimossi in base a qualche altra decisione. Questa dipendenza gerarchica tra decisioni viene affrontata nell'ordine in cui vengono prese le decisioni. Vengono prese solo decisioni provenienti da nodi decisionali che sono stati confermati. Il problema dell'architettura si traduce approssimativamente in un problema di assegnazione; tuttavia, sono presenti regole comportamentali aggiuntive. Ogni sorgente e destinazione, chiamata slot di connessione, è caratterizzata dal fatto che sono consentite connessioni ripetute e dal numero di connessioni provenienti o dirette allo slot. Il numero di connessioni può essere un elenco di connessioni consentite (*un numero o un intervallo)* o un numero minimo di connessioni (*con un numero massimo illimitato*). Tutti i possibili insiemi di connessione vengono quindi determinati dagli insiemi di nodi di origine e di destinazione e da un elenco facoltativo di connessioni escluse. Tutto questo porta processi

decisionali complessi e grafici sempre più ingarbugliati. L'unico modo per trovare la migliore architettura in uno spazio di progettazione afflitto da un numero macroscopico di combinazioni di alternative, è utilizzare tecniche sistematiche di esplorazione del design space. Per consentire ciò, lo spazio di progettazione deve essere ben definito in termini di un insieme di variabili di progettazione. Si possono utilizzare vari elementi. In questo momento entrano in gioco l'esperienza e la creatività umana e l'intelligenza artificiale. Un algoritmo di esplorazione dello spazio di progettazione, come un ottimizzatore, può essere utilizzato per generare punti nello spazio di progettazione e chiedere a un modello di analisi di valutare le prestazioni dei punti di progettazione. I risultati delle valutazioni vengono espressi quantitativamente in termini di obiettivi e vincoli, tra cui quelli normativi, e vengono utilizzati dall'algoritmo di esplorazione per generare nuovi punti di progettazione per la successiva iterazione, fino a quando non viene soddisfatto un criterio di arresto. L'ADSG può essere interpretato come un problema di ottimizzazione, con variabili di progettazione, obiettivi e vincoli. Bisogna riuscire a creare un modello che possa permettere la creazione, tramite decisione, della migliore architettura. Questo processo decisionale viene effettuato dal cosiddetto generatore di architetture in-the-loop. Le variabili di progettazione derivano dalle decisioni architettoniche e dalle variabili di progettazione aggiuntive nell'ADSG. Le decisioni sono codificate come variabili di progettazione discrete, con diversi indici mappati alle diverse opzioni. Le decisioni di permutazione sono anche codificate come semplici variabili di progettazione discrete per mantenere la compatibilità con i framework di ottimizzazione che possono gestire solo variabili di progettazione continue e intere. Le decisioni sono ordinate in base al loro tipo e gerarchia, assicurando che le decisioni di opzione vengano prese prima delle decisioni di permutazione e le decisioni condizionalmente esistenti vengano prese dopo le loro decisioni di conferma. Ulteriori variabili di progettazione definite nello spazio di progettazione vengono visualizzate alla fine del vettore di progettazione. Ciò garantisce che dall'inizio alla fine del processo il potenziale impatto delle variabili di progettazione sulle architetture diminuisca considerevolmente. C'è da considerare che in questi problemi di ottimizzazione le variabili di progetto possono essere attive in base ad altre variabili di progetto: sono di natura gerarchica. Ci sono tre modi per affrontare questo, ignorare gli effetti, l'imputazione o la considerazione esplicita. Ignorare gli effetti confonderebbe l'algoritmo di ottimizzazione, poiché è possibile che più vettori di progettazione diversi vengano mappati alle stesse istanze dell'architettura. La considerazione esplicita degli effetti della gerarchia richiede la modifica dell'algoritmo di ottimizzazione. Pertanto, come modalità predefinita per gestire l'effetto gerarchia, viene scelta l'imputazione. Con l'assegnazione, le variabili di progetto inattive sono impostate su un valore predefinito, 0 per le variabili di progetto discrete e il centro del dominio per le variabili di progetto continue. Bisogna comunque considerare che a causa di questo effetto, ci può essere una differenza tra lo spazio di progettazione apparente e lo spazio di progettazione fattibile. [11] Lo spazio di progettazione apparente considera tutte le combinazioni di tutte le variabili di progettazione, senza distinzione di fattibilità e realtà, mentre lo spazio di progettazione fattibile elimina combinazioni di variabili di progettazione che portano ad architetture irrealizzabili, per vari motivi o includono variabili di progettazione inattive non sui loro valori di imputazione. Durante un ciclo di esplorazione dello spazio di progettazione, i vettori di progettazione che specificano un punto di progettazione al di fuori dello spazio di progettazione fattibile vengono automaticamente spostati dal software al punto di progettazione più vicino nello spazio di progettazione fattibile. Questa logica è implementata nella fase di generazione dell'architettura, e quindi è necessario un meccanismo di feedback per notificare all'algoritmo di ottimizzazione il vettore di progetto modificato. Una volta visto come generare architetture e il processo decisionale, bisogna andare a studiare quali possono essere gli obiettivi per andare a scegliere un'architettura rispetto ad un'altra. Questi obiettivi vengono considerati come metriche delle prestazioni. Le metriche delle prestazioni sono interpretate come obiettivi (*minimizzare o massimizzare questo valore*) o vincoli (*il valore dovrebbe essere almeno o al massimo un valore target*) nel problema di ottimizzazione. [11] I vincoli possono essere anche quelli normativi che sono stati visti nel capitolo precedente e saranno usati come metrica delle prestazioni per quanto concerne il lavoro di questa Tesi. Tutto sarà visto nei prossimi capitoli. Una metrica delle prestazioni è definita da due proprietà, una direzione e, facoltativamente, un valore di riferimento. La direzione specifica cosa è preferibile, un valore inferiore o superiore. Il modo in cui una metrica può essere interpretata dipende da alcuni fattori. Una metrica delle prestazioni può essere utilizzata come obiettivo se esiste incondizionatamente, perché un obiettivo serve come modo per confrontare diverse architetture in termini di quale sia migliore in base alla metrica scelta; quindi, dovrebbe esistere in tutte le possibili architetture. Una metrica delle prestazioni può essere utilizzata come vincolo se ha un valore di riferimento, necessario per determinare se il vincolo venga violato o meno,

quello che rappresentano i vincoli normativi e la futura certificazione. Un sistema deve essere certificabile in base al fatto che non violi i vincoli legislativi, poi il cliente vede se quel sistema ha delle caratteristiche allettanti per comprarlo, quindi capire quale architettura, tra quelle che rispettano i vincoli, sia la migliore in termini di vita operativa, funzioni e costi. Queste due metriche non devono sempre essere prese separatamente, ma possono essere interpretate in entrambi i modi. Se questo è il caso, comunque deve essere specificata un'interpretazione preferita. Si noti che è possibile definire più di un obiettivo, poiché in genere ci sono compromessi contrastanti da effettuare quando si ha a che fare con più parti interessate nella progettazione di sistemi complessi. Le metriche senza un valore di riferimento possono essere utilizzate come obiettivo solo se esistono incondizionatamente e le metriche con un valore di riferimento possono sempre essere utilizzate come vincoli. I problemi con variabili di progetto condizionali sono problemi di ottimizzazione gerarchica in cui è possibile definire più di un obiettivo e nessuna ponderazione oggettiva a priori è esplicitamente considerata, e le variabili possono essere sia discrete che continue. [11] In generale il problema dell'ottimizzazione dell'architettura può essere di tre tipi, gerarchico, misto-intero e multi-obiettivo. Il problema di ottimizzazione può essere espresso come in figura 23 seguente.

$$
\begin{array}{lll}
\textit{minimize} & f_m(\boldsymbol{x},\boldsymbol{y}), & m = 1,2,\ldots,\mathcal{M} \\
\textit{where} & x_i \in \mathbb{R} & i = 1,2,\ldots,n \\
 & y_j \in \mathbb{Z} & j = 1,2,\ldots,\mathcal{J} \\
\textit{w.r.t.} & g_k(\boldsymbol{x},\boldsymbol{y}) \leq 0, & k = 1,2,\ldots,\mathcal{K} \\
 & x_i^{(L)} \leq x_i \leq x_i^{(U)} &
\end{array}
$$

FIGURA 23

X e Y sono i vettori delle variabili di progetto continue e discrete, e f e g sono le funzioni obiettivo e di vincolo. Il problema di ottimizzazione ha M obiettivi, n variabili di progetto continuo, J progetti discreti (L) e x (U) per le variabili inferiore e superiore e K rappresenta i vincoli. L'implicazione principale della natura del problema di ottimizzazione è che non è possibile utilizzare metodi basati sul gradiente per risolvere il problema e gli algoritmi di ottimizzazione dovrebbero essere in grado di risolvere problemi di ottimizzazione di tipo multi-obiettivo. Inoltre, gli algoritmi di ottimizzazione dovrebbero essere in grado di gestire le implicazioni delle variabili di progettazione gerarchiche, oppure accettare che il motore di generazione dell'architettura modifichi il vettore di progettazione in base a questa gerarchia. Gli algoritmi candidati in grado di gestire tali problemi sono gli algoritmi evolutivi multi-obiettivo (MOEA), come NSGA-II o SPEA2.

4.2 Software ADORE

Per sviluppare il design space appena descritto dettagliatamente, è stato sviluppato dalla DLR (German Aerospace Center), Institute of System Architectures in Aeronautics, Hamburg, Germany un software che funziona proprio per costruire il design space di qualunque sistema. Il suo funzionamento ricalca per filo e per segno il funzionamento del design space. [12] [13] Questo software si chiama ADORE. Il software permette di inserire tutti gli elementi caratteristici del design space, funzioni, componenti, concetti, istanze, attributi e altro. Tramite l'uso di immagini prese dal 'Tutorial: Architecture Design Space Modeling using ADORE. MBSE Development System' verrà mostrato il funzionamento di ADORE, con incluso l'immagine di un intero design space di esempio. Il sistema che è stato creato per questa tesi, tramite ADORE, sarà spiegato nel successivo capitolo. [12] [13] In questo paragrafo si andrà a vedere come modellare lo spazio di progettazione dell'architettura del sistema utilizzando ADORE. Il modello può essere utilizzato per identificare le decisioni architettoniche e per formulare problemi di ottimizzazione dell'architettura. Tutto con l'ausilio di immagini prese dal tutorial. Nella prima immagine di questo paragrafo si vede come gli elementi fondamentali di un design space e di ADORE sono le funzioni e i componenti. All'inizio si inserisce una funzione di qualunque tipo, una funzione madre da cui creare tutto il design space. Ogni funzione è attuata da un componente. Un componente a sua volta necessita di una funzione, che sarà inserita di conseguenza. Una funzione può essere attuata da più componenti, e qui nasce il processo decisionale. Durante la creazione dell'architettura si andrà a sceglie quale componente svolge meglio quella funzione, o quale componente è il compromesso migliore per quella funzione. Questo significa creare più architetture,

ogni volta scegliendo il componete, tra quelli inseriti, che migliore per ogni esigenza. Ogni componente può essere strutturate internamente inserendo gli attributi, come il tipo di carburante, o le varie configurazioni di quel componete, così per ogni scelta e architettura si andrà anche a scegliere la configurazione del componente migliore per ogni esigenza. I componenti possono poi essere collegati tramite le 'porte'. Le funzioni possono essere 'fullfiled' da componenti, concetti o decomposizioni. Le decomposizioni sono usate per mostrare che una funzione può essere scomposta in più funzioni, di cui ognuna attuata da uno o più componenti. Il software, evidenziando l'elemento con il verde mostra se un collegamento è possibile con quell'elemento. Se si effettua un collegamento ma non appare l'evidenza in verde allora quel collegamento non è possibile. Alcuni esempi di collegamenti impossibili sono tra funzioni e funzioni o tra componenti e componenti. Ci deve sempre essere una funzione e un componente per il collegamento. Se si vuole invece collegare una funzione con due o più componenti senza dover effettuare successivamente la scelta architettonica, cioè si vuole includere entrambi i componenti nella funzione allora si utilizza l'elemento 'multi-fulfillement', mentre se si vuole indicare che quella funzione non è attuata da nessun componente si utilizza l'elemento 'non-fulfillment'. Si utilizza il collegamento rosso tra due componenti se si vuole indicare che quei due componenti non possono esistere nella stessa architettura. [12]

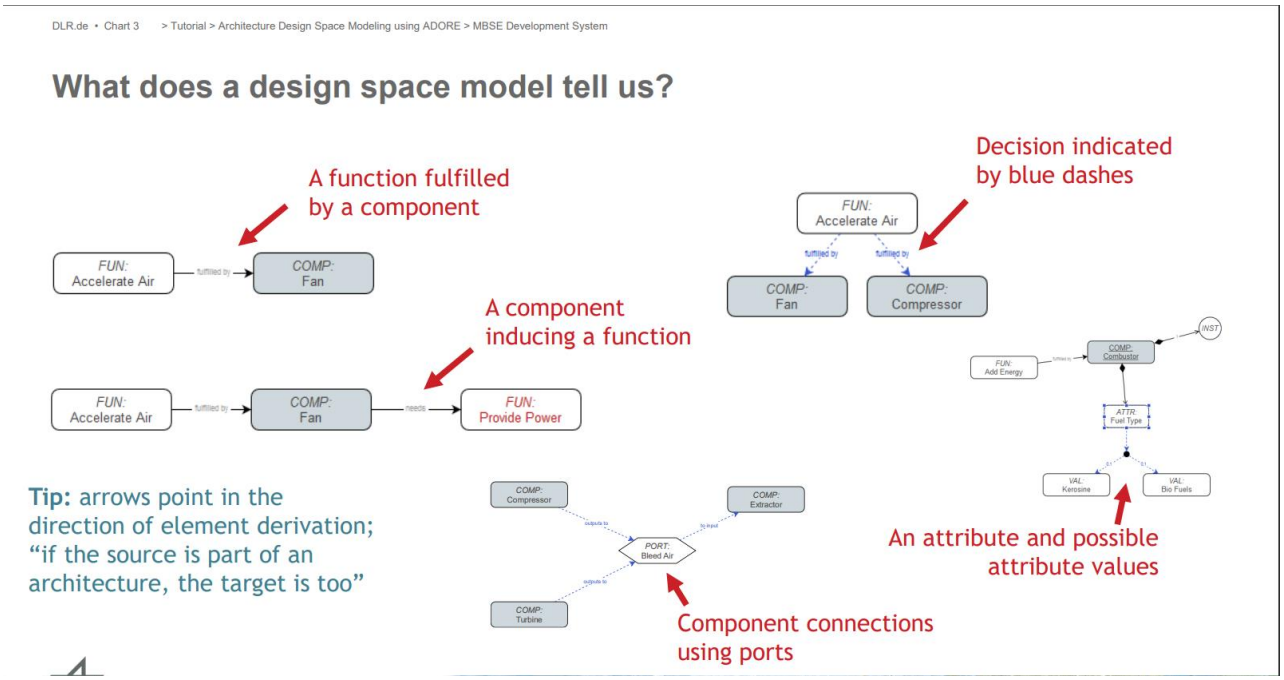


FIGURA 24

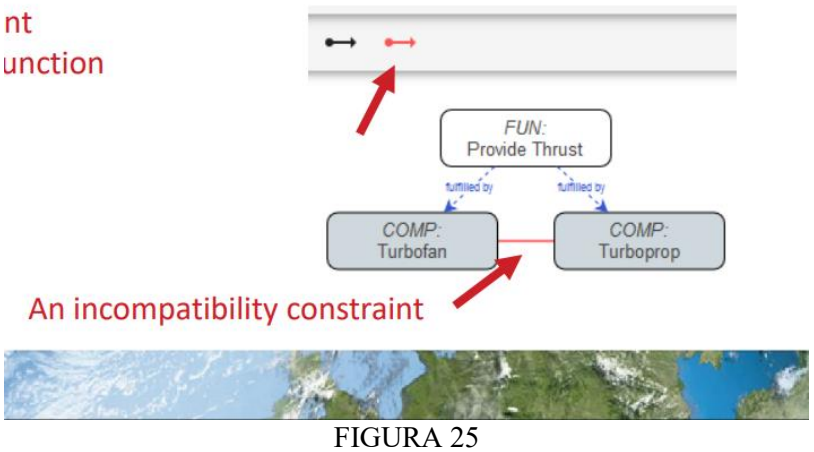


FIGURA 25

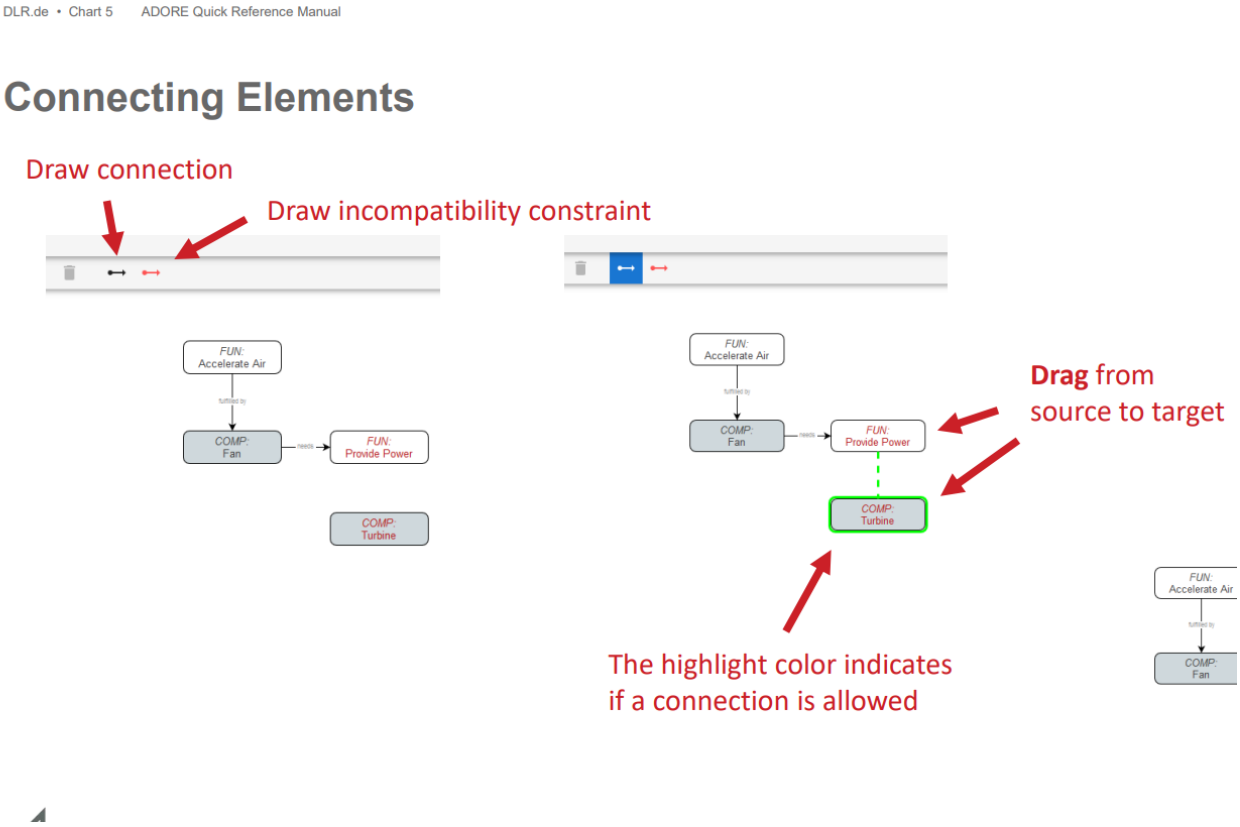


FIGURA 26

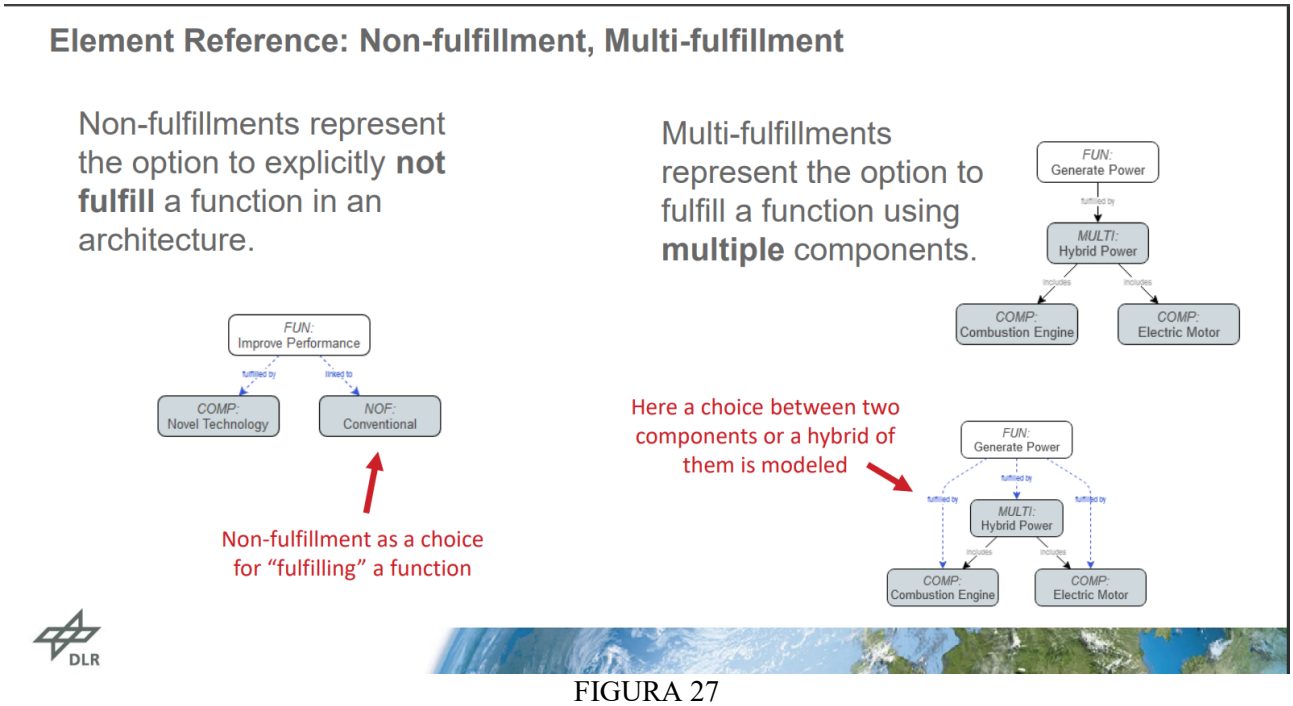


FIGURA 27

Le figure 24-25-26-27 mostra un aspetto molto importante dei componenti. Con il software ADORE si può lavorare all'interno del componente cliccando sul pulsante 'open component view'. In questa pagina si lavora solo sul componente, permettendo di inserire, come detto, possibili configurazioni e attributi. Un altro elemento importante sono le istanze. Le istanze rappresentano le scelte sulla quantità dei componenti. Inserendo un numero nella casella delle istanze si indica la quantità del componente. Però si può fare anche

cosa molto particolare e propria del design space, cioè, inserire più numeri intervallati da una virgola, nella foto esempio del componente della turbina sono indicati ‘1,2’. Questa è una scelta che bisognerà fare e significa che sono possibili o uno o due turbine. Quindi non si impone una sola quantità del componente, ma si da la scelta di decidere in base alle esigenze e alle varie funzioni di decidere se usare una sola turbina oppure due turbine. Questo vale per tutti i componenti. Si può inserire solo un numero e quindi dire che ci saranno solo *n* quantità di quel componente, oppure inserire ‘*n,m’* quindi decidere se usare *n* o *m* quantità di quel componente. Si vede nella figura 28

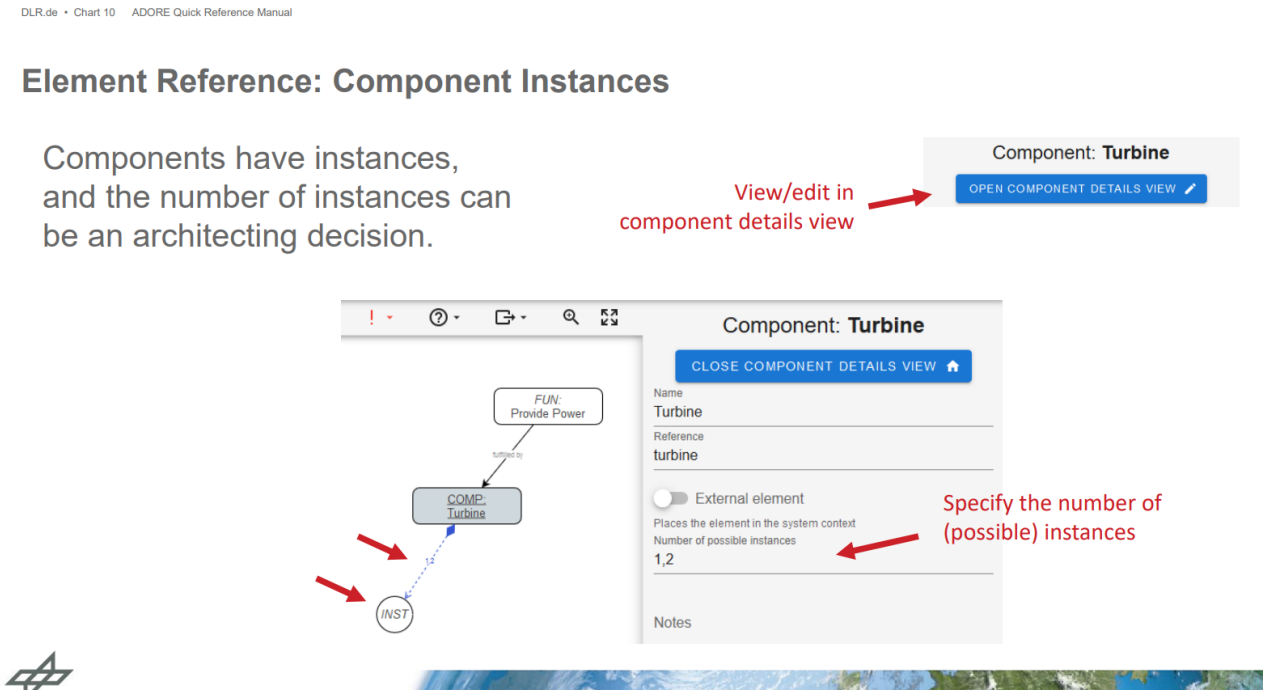


FIGURA 28

Poi ogni istanza, cioè ogni n o m quantità di quel componente possono essere diversi, cioè, avere diversi attributi, cioè non tutte le istanze, o le quantità, di quel componente saranno uguali. Un esempio è dato dalla figura in cui si vede come il componente ‘turbofan’, ha 4 istanza, cioè in quell’architettura ci saranno 4 motori turbofan, ma i pezzi non sono uguali; infatti, due motori avranno gli inversori di spinta, mentre gli altri due no. Questo è l’esempio dell’aereo Airbus A380, quadrimotore. La capacità di frenatura è sufficiente da permettere l'installazione degli inversori di spinta solo sui motori interni alle ali, mentre i motori esterni non ne sono equipaggiati. Questo permette la riduzione della quantità di detriti sollevati durante l'atterraggio. Gli inversori sono azionati elettricamente per risparmiare sul peso totale dell’aeromobile e per avere una maggiore affidabilità rispetto agli equivalenti pneumatici o idraulici. Si vede nella figura 29. [11] [12]

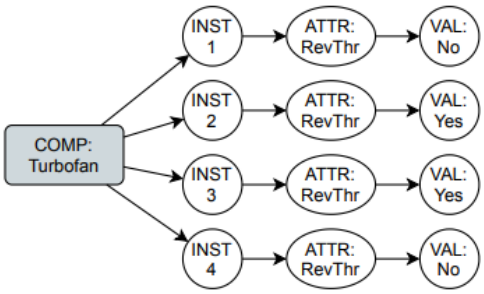


Figure 3 Component (COM) characterization: by number of instances (INST), and by attributes. Attributes are represented by attribute nodes (ATTR) pointing to attribute value nodes (VAL). Shown is a turbofan with four instances, where two have reverse thrust (RevThr) capabilities, and two have not (e.g. Airbus A380).

FIGURA 29

La figura 30 mostra come inserire le possibili caratteristiche di un componente, cioè le sue possibili configurazioni o altre scelte sul componente singolo, come detto in precedenza.

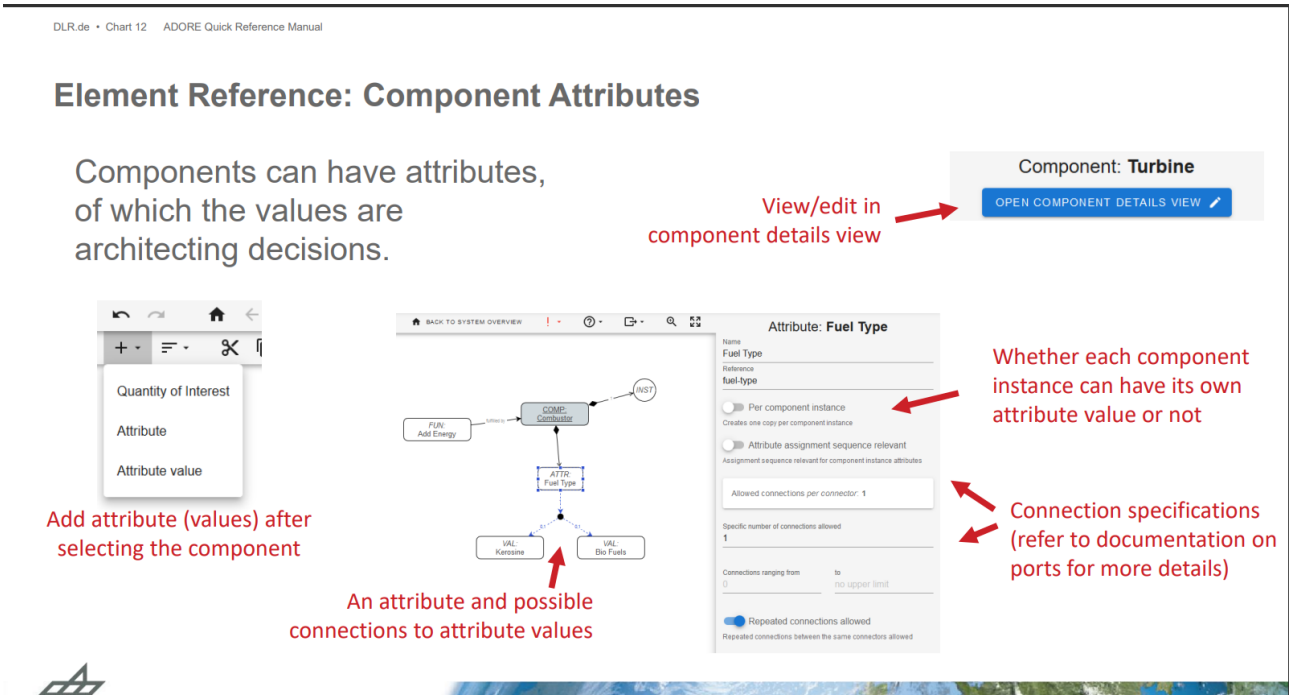


FIGURA 30

La successiva figura 31 mostra il processo decisionale dell'architettura, dopo aver costruito il design space con ADORE. Il design space permette di descrivere con un modello tutte le possibili architetture. Il design space contiene la decisione da effettuare per portare ad architetture.

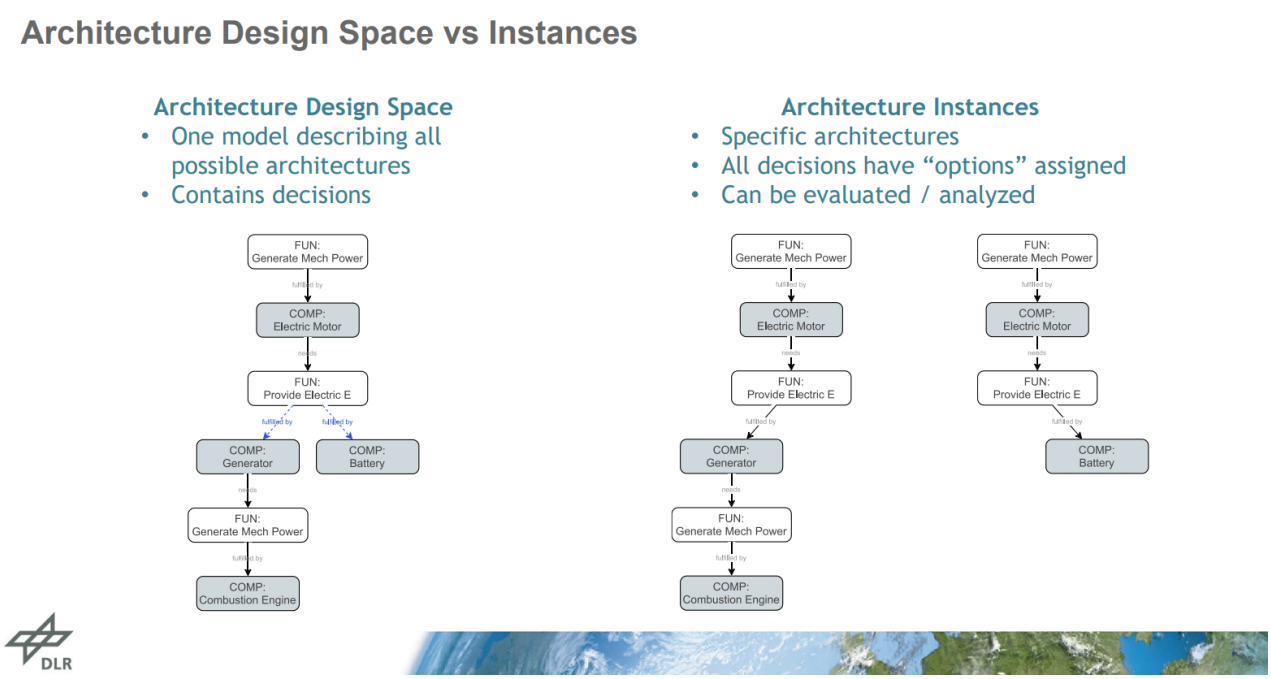


FIGURA 31

Le figure 32 di seguito mostrano l'interfaccia di ADORE, con i pulsanti da utilizzare per aggiungere elementi del design space e altro. Aggiungi il titolo del progetto, aggiungi gli elementi. Poi puoi salvare il progetto o aprirne di vecchi. Piccola avvertenza, ogni salvataggio comporta il download del file salvato. Sono comunque pochi kb di memoria, ma comunque ogni volta che salvi si scarica il file. Così potrai aprire tutti i salvataggi effettuati.

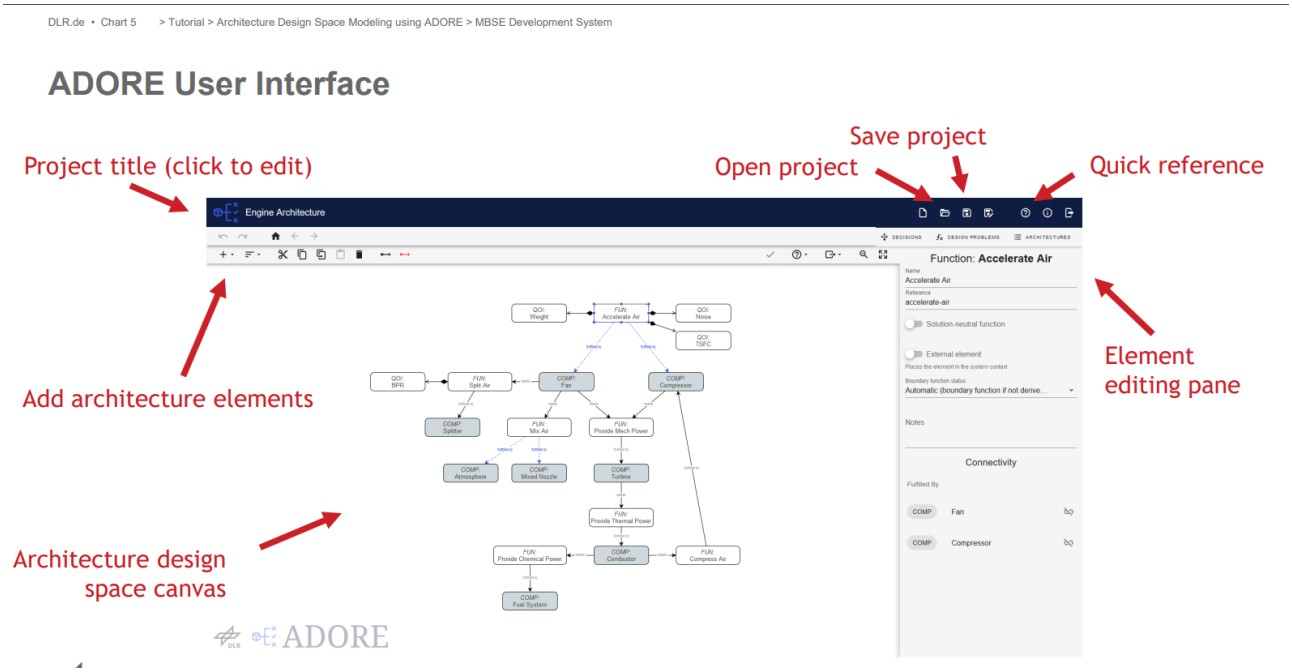


FIGURA 32

Il '*model status indicator*' indica se c'è qualche problema con il design space, se manca qualche collegamento, o delle funzioni o componenti non sono collegati. In questo modo si può vedere se il progetto sta funzionando e ha senso. (figura 33) Un elemento importante di funzionamento del software è che si può

scorrere lo schermo cliccando il pulsante destro del mouse, non quello sinistro come per tutti gli altri programmi del computer. Ogni volta che si inserisce un elemento nuovo bisogna nominarlo. Una funziona la si chiama come '*move air' o 'provide power*' o altro ancora, mentre il componente lo si nomina con il nome del componente, come '*system' o 'engine' o 'structure'*. Il multi fulfillment lo si può nominare come '*redundancy*', per indicare la ridondanza di più elementi che svolgono quella funzione.

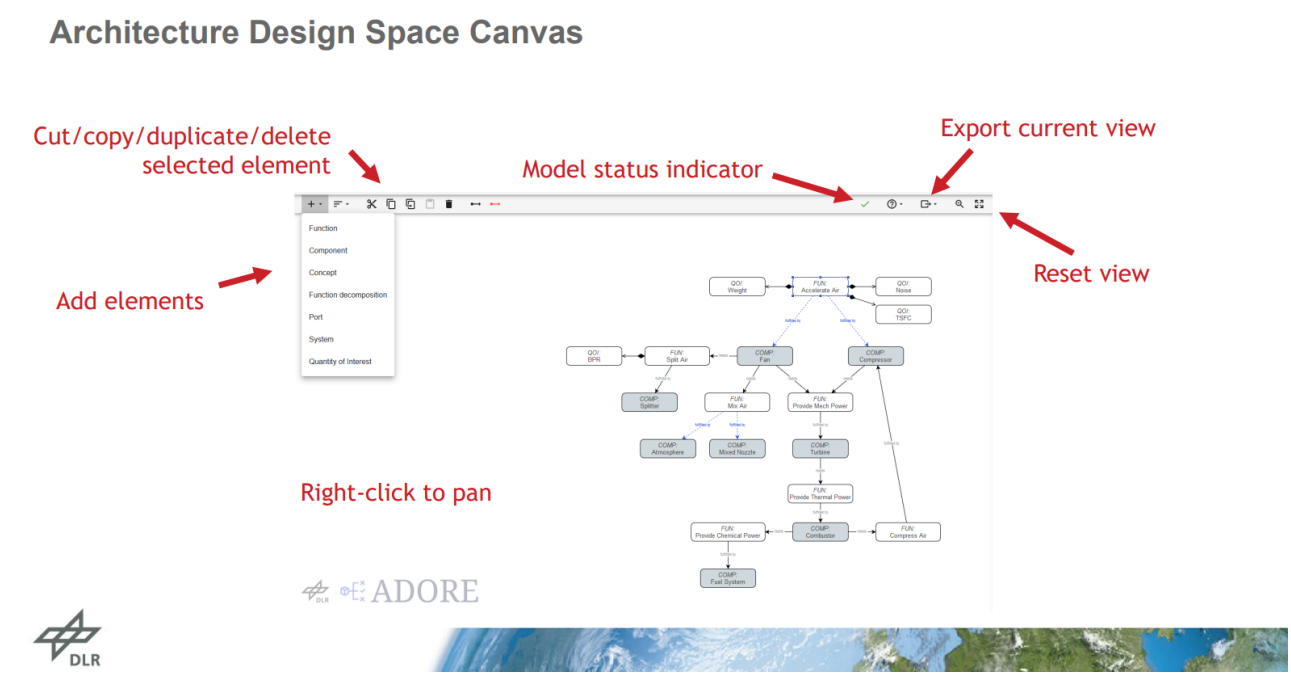


FIGURA 33

La figura 34 di seguito mostra l'elemento '*ports*'. I componenti possono poi essere connessi tra di loro per mezzo delle '*ports*'. Questo permette di allargare ulteriormente lo spazio di decisione e le possibili architetture.

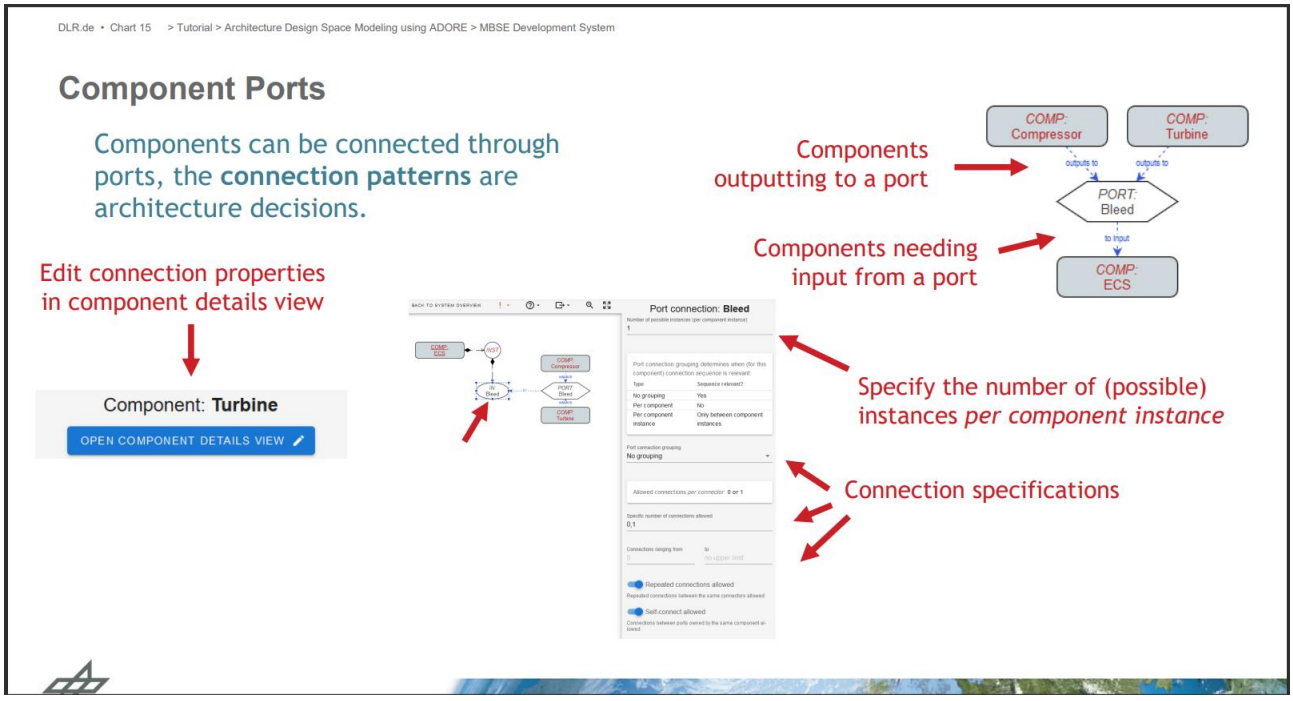


FIGURA 34

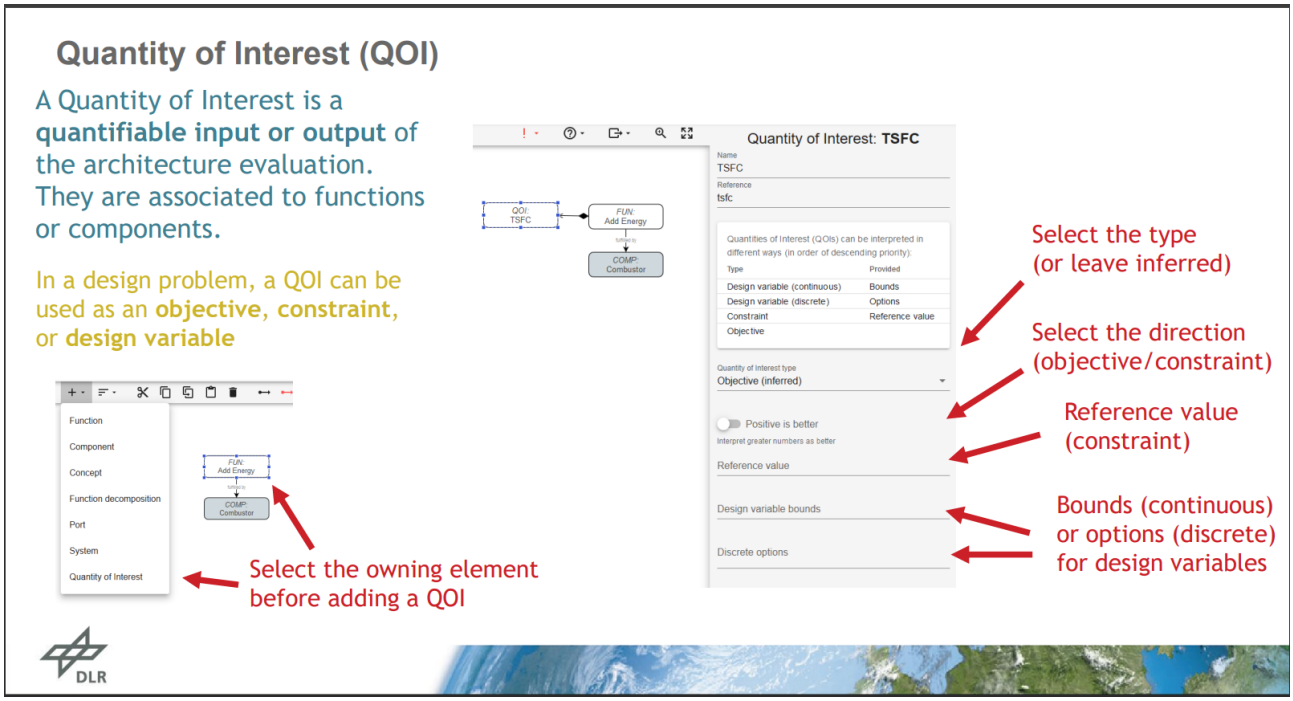


FIGURA 35

Infine, come la figura 35 di sopra ci mostra, è possibile inserire un cosiddetto '*quantity of interest (QOI)'*, cioè un input o output quantificabile che indica quale sia l'obiettivo di quella funzione o di quell'elemento in particolare (*ad esempio 'aumentare l'efficienza' o 'diminuire il peso' o 'aumentare l'affidabilità' e altro*). Queste '*quantity*' sono importanti perché esprimono un ulteriore scelta di architettura. Conclusi questi passaggi si è creato il design space del proprio sistema. Mancano ancora due cose. Definire un '*desgin* problem' e costruire manualmente le architetture. (figura 36) [12]

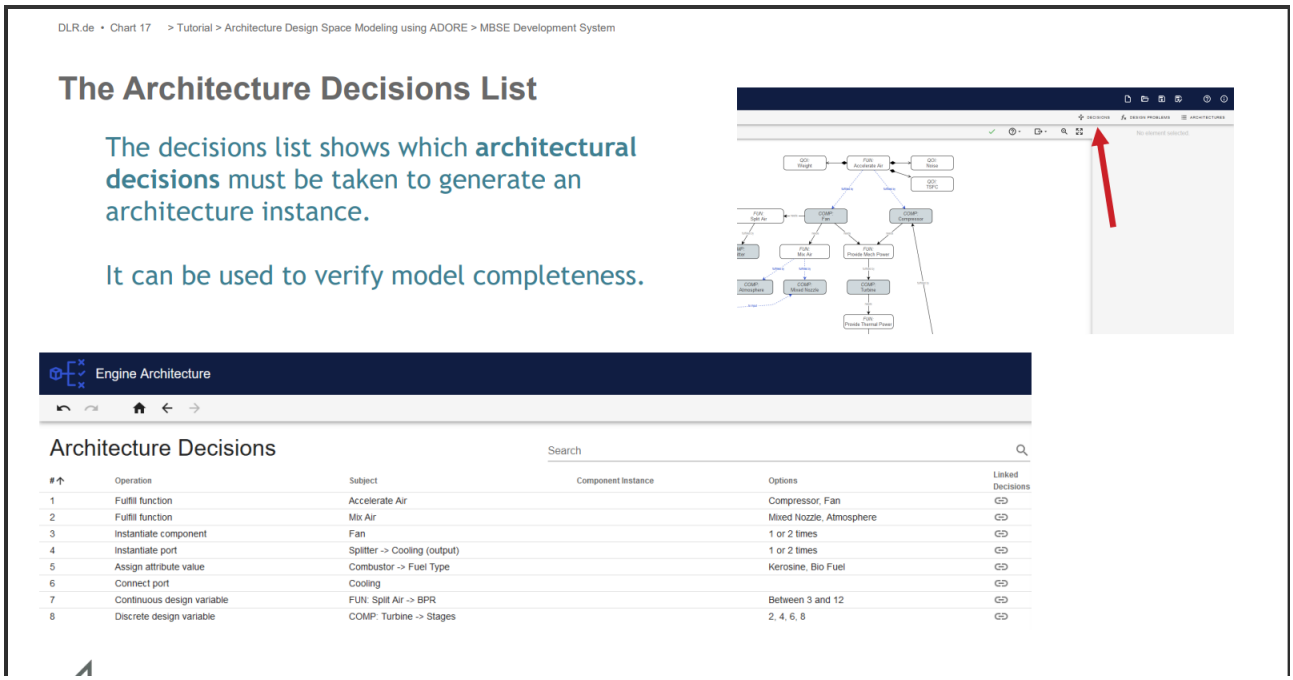


FIGURA 36

In questa pagina, come visto dalla figura sopra, è possibile vedere tutte le decisioni create nel design space, numerarle e sceglierle.

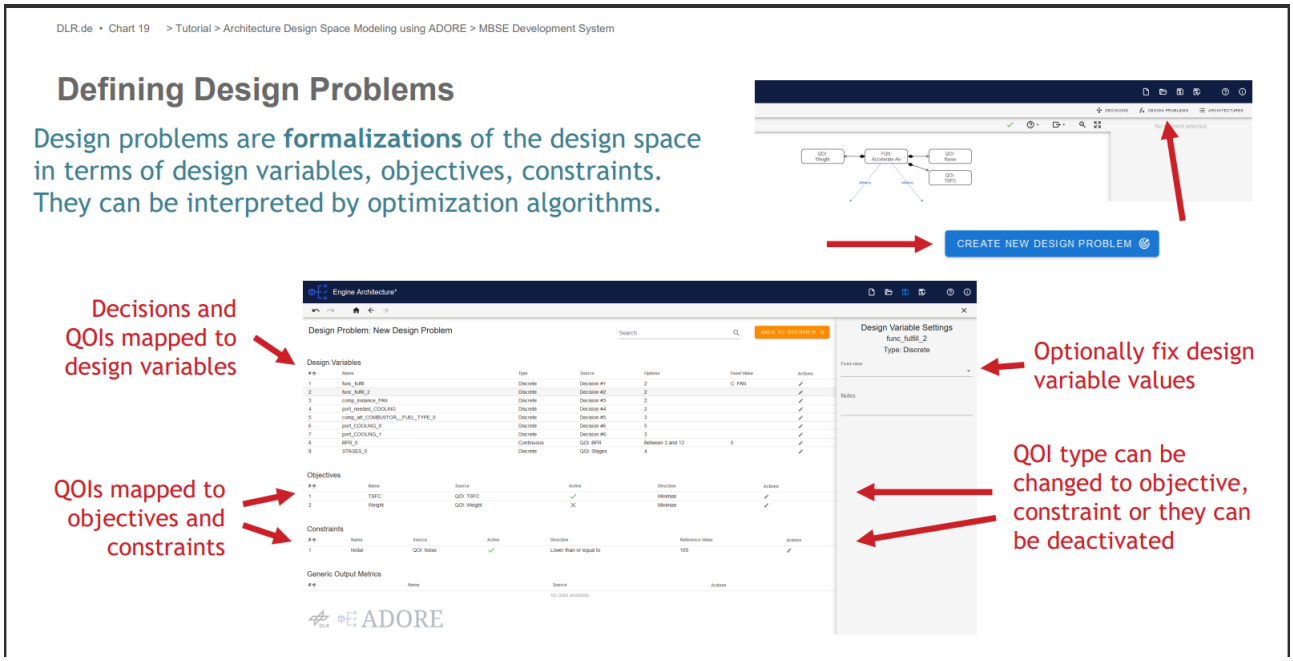


FIGURA 37

Dalla pagina delle decisioni si arriva al cosiddetto 'design problem', cioè formalizzazioni dello spazio di progettazione in termini di variabili di progettazione, obiettivi, vincoli. Possono essere interpretati da algoritmi di ottimizzazione. Quindi si può operare sia manualmente sia tramite altri software di ottimizzazione. (figura 37)

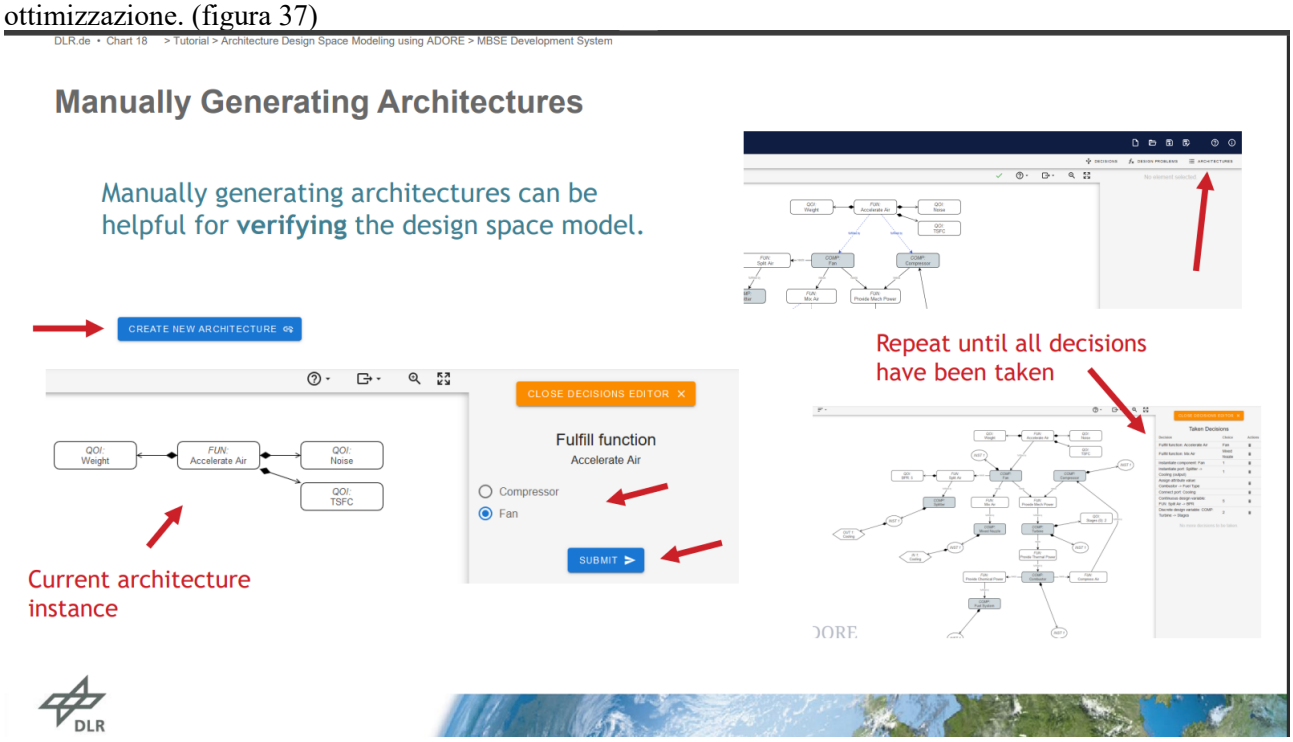


FIGURA 38

Questa figura 38, la, mostra l'ultimo aspetto del software ADORE, cioè, costruire le architetture manualmente. Lo si può fare dalla pagina 'crea l'architettura, e il software mostrerà tutte le scelte fatte nel design space e quindi si possono fare le varie scelte e costruire tutte le possibili architetture relative a quel design space. Va da sé che tutte le possibili combinazioni e architetture possono essere enormi e possono volerci anche anni a vedere tutte le opzioni; quindi, manualmente si possono costruire solo un paio di queste architetture e possibili combinazioni. L'ultima considerazione è che questo è un software in pieno sviluppo e

per ricerca aziendale, è quindi normale che ogni tanto capitino delle problematiche. Con il software ADORE, nella maniera appena spiegata, si è creato il sistema per validare i requisiti e i vincoli spiegati nei capitoli precedenti. Il sistema creato è l'intero sistema frenante di un velivolo ad ala fissa, come spiegato nel capitolo successivo.

5. Il Sistema progettato

Uno degli obiettivi di questo lavoro di Tesi, dopo la ricerca dei vincoli architettonici fondamentali per la certificazione, è quella di creare un sistema e utilizzare un tool specifico per certificarlo, inserendo i vincoli normativi trovati e spiegati nei capitoli precedenti. Quindi andare nella pratica di tutto quello detto nei precedenti capitoli. Per creare questo sistema verrà utilizzato il software ADORE, e quindi non verrà creato una singola architettura di un sistema, ma come ampiamente spiegato, verrà progettato un design space di un sistema con diverse scelte per la creazione di più architetture in base alle esigenze. Per quanto riguarda il check certificativo e l'utilizzo dei vincoli per la certificazione del sistema, verrà spiegato nel capitolo successivo. Il sistema che è stato creato è quello del sistema frenante di un velivolo aereo ad ala fissa. Si è deciso di creare questo sistema per alcuni motivi. La SAE ARP 4761 [6] mostra l'esempio dettagliato di un safaety assessament di un sistema frenate di un aereo fittizio, e quindi si è preferito utilizzare lo stesso sistema per la creazione di questo design space. Un altro motivo è che il sistema frenante è un sistema abbastanza complesso da utilizzare tutti i possibili vincoli architettonici e regole normative, ma al tempo stesso non complesso come quello idraulico od elettrico, che sarebbero troppo onerosi per un semplice lavoro di tesi. Quei sistemi si fanno in azienda quando si ha tempo e risorse molto più ampie di quelle di una Tesi magistrale. Si è utilizzati anche un altro documento, oltre alla SAE 4761, la SAE AIR 6110, che spiega alcuni elementi del sistema frenante mostrato nella SAE 4761. [6] [19] Il sistema che siamo si è andati a creare con il design space non è però solamente il sistema frenante delle ruote di un velivolo ad ala fissa, come mostrato nei due documenti appena citati, ma si è allargato il concetto di sistema frenante a tutti i tipi di freni di un aereo; quindi, il design space sarà del sistema frenante di un velivolo ad ala fissa nella sua interezza, includendo anche gli aspetti delle ali e del profilo alare e dei motori e degli inversori di spinta. Per costruire il design space sono stati studiati tutte le architetture già in uso sui velivoli ad ala fissa di molti tipi, in più sono stati visionati studi su sistemi focalizzati sulla filosofia 'more electric'. [20] Come prima cosa si è inseriti una funzione origine da cui far partire tutto il sistema. La funzione origine è '*provide stopping force',* cioè un sistema che crei una forza di frenata, sia tramite le ruote, sia tramite la portanza o la resistenza aerodinamica e sia tramite i motori. Da questa funzione si è decomposta in tre funzioni distinte, '*frenata aerodinamica, frenata delle ruote e frenata dei motori.'* L'intero sistema frenante dell'aereo è svolto da tre impianti frenanti distinti, con ognuno lo stesso obiettivo, cioè quello di rallentare e frenare l'aereo. (figura 39)

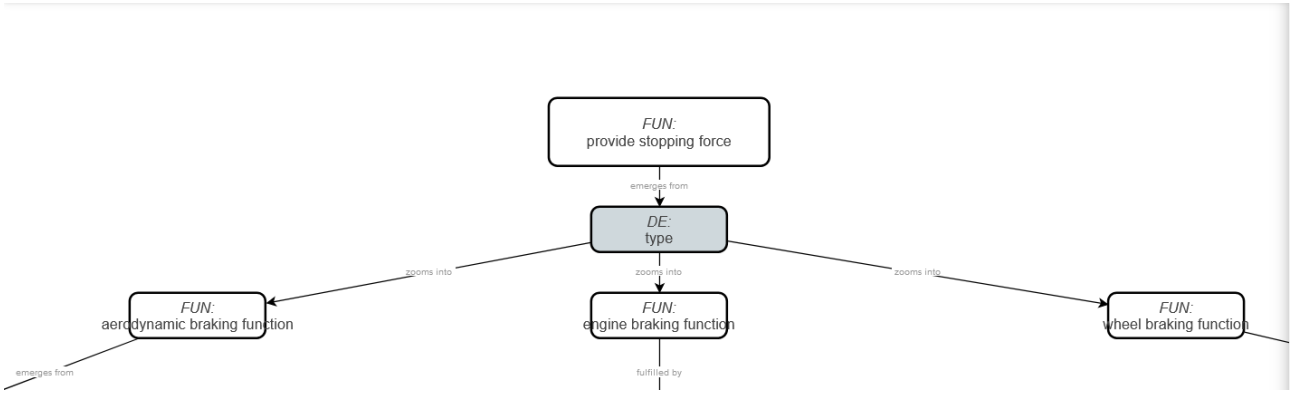


FIGURA 39

Una volta diviso i tre tipi di frenata si è andati ad espandere ognuno delle funzioni madri. Iniziamo dal sistema del freno aerodinamico. La funzione '*freno aerodinamico'* è stata decomposta in '*aumento della resistenza'* e '*riduzione della portanza'*. La funzione '*riduzione della portanza'* è svolta dal componente '*lift dumper'*, che ha bisogno della funzione di controllo, che può essere svolta da una scelta tra due componenti, '*controlli reversibili' e controlli' potenziati'*. I controlli potenziati hanno bisogno di energia che è prodotta da un servo-motore, il quale ha bisogno di due funzioni di trasmissione, 'trasmissione di potenza' e '*trasmissione di segnale'*. La trasmissione disegnale può essere di tre tipi, '*elettrica*', svolta dal componente '*fly-by-wire'*; '*meccanica*', svolta da due componenti, '*metal rods' o 'metal ropes'*; '*ottica*', svolta dal componente '*flight-by-light'*. La trasmissione di potenza è adempiuta da una scelta di tre componenti,

'sistema idraulico', '*sistema elettrico'*, oppure un multi-adempimento con entrambi i due sistemi. La funzione '*aumento della resistenza'* viene svolta da una scelta di tre componenti, '*air brake*' o '*spoiler*', oppure con un componente multi-fullfilment che utilizza entrambi i componenti. Quindi si farà la scelta se utilizzare un solo componente per questa funzione, oppure utilizzarli entrambi con l'elemento multi-fullfilment. Come la normativa esige e ogni sistema vuole, serve una sorgente di potenza, che dia energia ai sistemi. Quindi sono stati selezionati degli elementi per dare energia ai due sistemi. Il sistema idraulico è alimentato o da un '*engine pump'* o da un '*electric pump'*. A loro volta queste pompe hanno bisogno di potenza e questa potenza è data dai motori oppure da un motore elettrico o da un RAT. È possibile selezionare solo una sorgente di potenza oppure tutte, per avere ridondanza. Stessa cosa per le pompe, o una o entrambe per avere ridondanza. Le figure 40-41-42 mostrano il design space del sistema della frenatura aerodinamica.

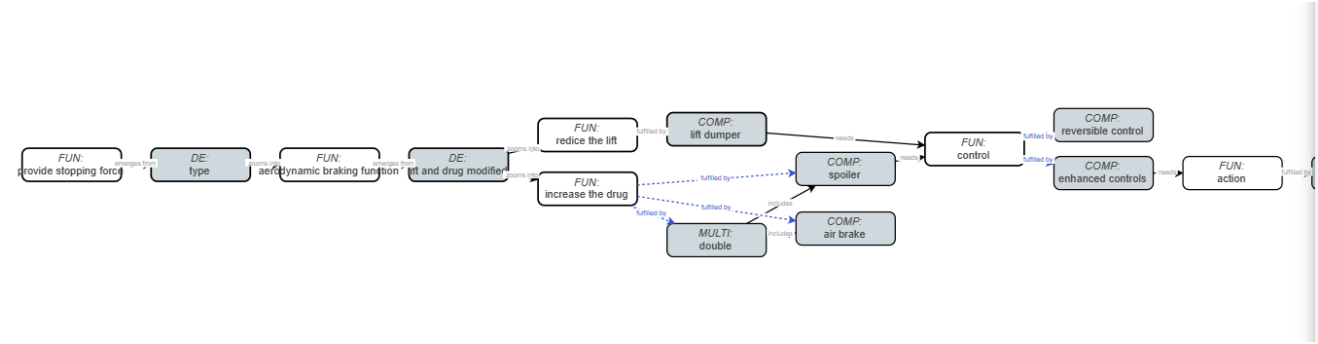


FIGURA 40

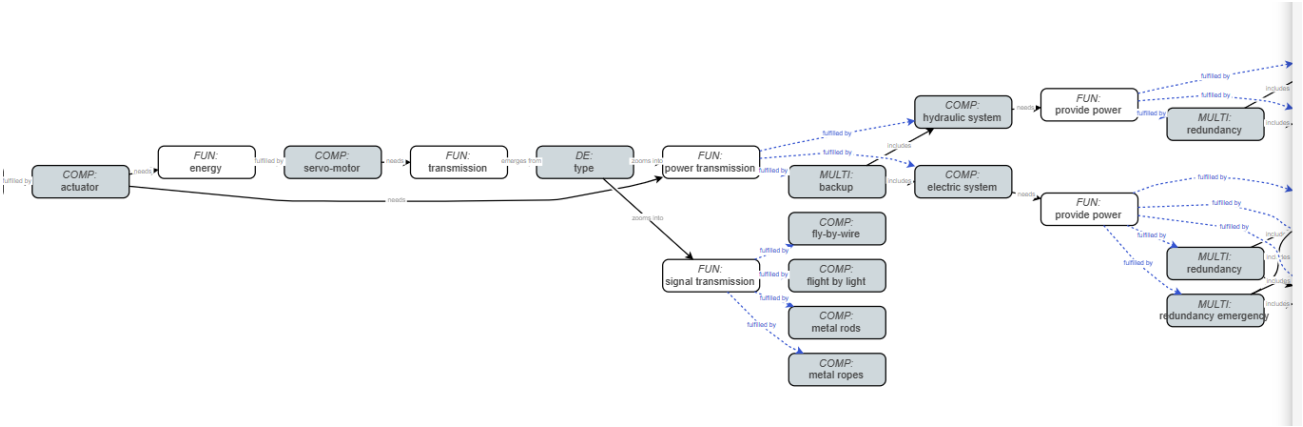


FIGURA 41

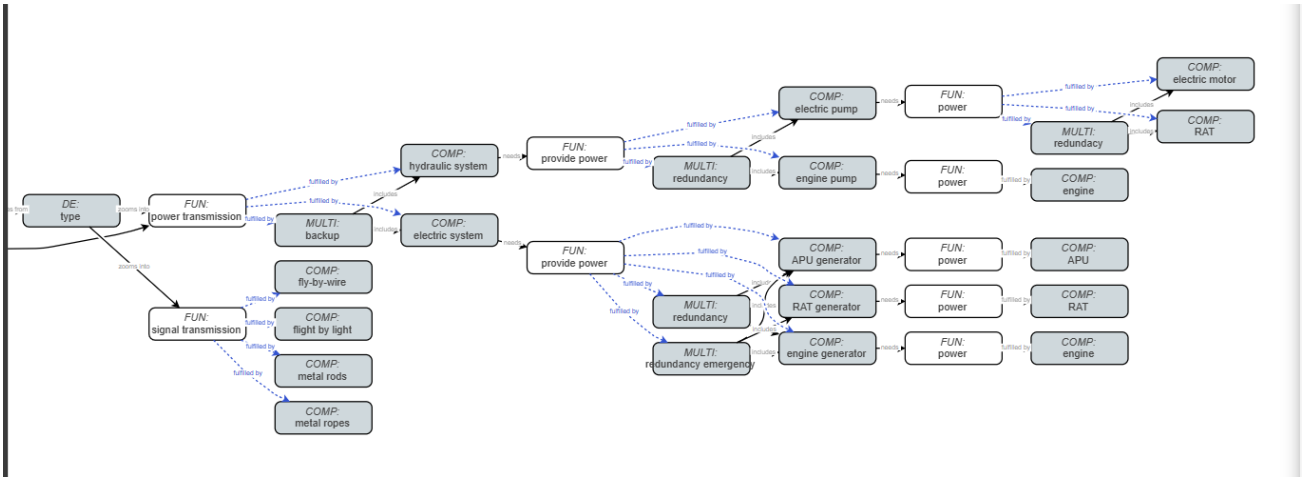


FIGURA 42

La seconda parte del sistema frenante è quella relativa ai motori, cioè all'inversore di spinta. Le figure 43-44 mostrano due spaccati del design space, per vedere meglio gli elementi.

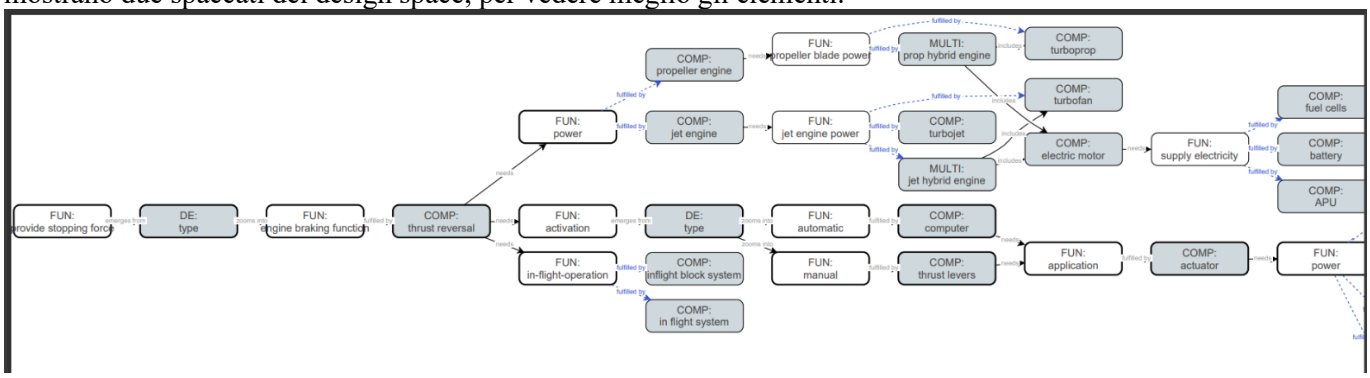


FIGURA 43

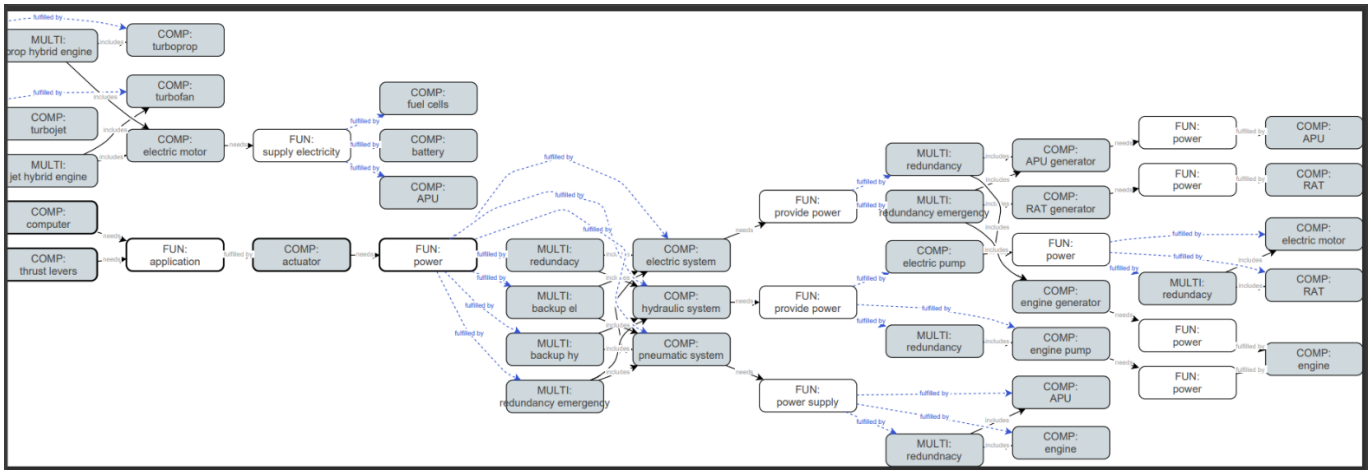


FIGURA 44

La funzione '*frenata dei motori'* è svolta dagli '*inversori di spina'*. È stato inserito una decisione riguardante il numero degli inversori di spinta che possono in numero 1 o 2 o 3 o 4, cioè non tutti i motori possono essere dotati di inversori di spinta, l'A380 ne ha solo due, nonostante sia un quadrimotore; quindi, in base alle esigenze si decide quanti inversori di spinta inserire. Gli inversori di spinta hanno bisogno di potenza, che può essere di due tipi, o potenza da jet o potenza da pale, cioè gli inversori di spinta possono essere inseriti in motori turbojet/turbofan oppure in motori turboprop. Infatti, le funzioni di potenza sono attuate dai tipi di motori citati, con una variante. Si è inserito anche il modello ibrido, cioè, sia motore tradizionale turbofan o turboprop insieme ad un motore elettrico. Questo lo si è progettato inserendo l'elemento multi-fullfilment con i motori tradizionali a kerosene insieme al motore elettrico. Si sta andando verso una concezione '*more electric'* quindi è giusto inserire nel design space la scelta tra motori tradizionali e motori ibridi. Il componente '*electric motor'* necessita di elettricità per funzionare, la quale è prodotta da due componenti, o le *batterie o le fuel cells*. Si decide quale componente utilizzare e quale sia migliore per la certificazione. Il componente *'inversori di spinta'* necessità anche di attivazione, svolta in due maniere, o *manuale*, tramite i *'thust levers* (*la manetta*); o *automatica*, svolta tramite un *computer*. Questi due componenti necessitano di una applicazione del comando ricevuto e questo è svolto dagli attuatori, che a loro volta hanno bisogno di potenza. La potenza è data dal sistema elettrico o dal sistema idraulico, oppure da entrambi utilizzando l'elemento multi-fullfilment. Si è poi inserito lo stesso procedimento dell'impianto spoiler per quanto riguarda le sorgenti di potenza dei sistemi. Quindi si sono inseriti le pompe, idrauliche ed elettriche, e i generatori, le APU e le RAT. Infine, l'ultima funzione degli inversori di spinta è quella relativa alle

operazioni in volo. Alcuni aerei, principalmente aerei russi e sovietici, sono in grado di utilizzare in sicurezza gli inversori di spinta in volo. Gli aerei commerciali moderni, tuttavia, non possono. L'uso in volo degli inversori di spinta presenta diversi vantaggi. Consente una rapida decelerazione, consentendo rapidi cambi di velocità. Previene anche l'accumulo di velocità normalmente associato alle immersioni ripide, consentendo una rapida perdita di quota, che può essere particolarmente utile in ambienti ostili come le zone di combattimento e quando si effettuano approcci ripidi alla terraferma. Quindi nel design space si è inserito la funzione 'in-flight operation', che può essere svolta da due componenti opposti, o un sistema che permetta l'utilizzo in sicurezza delle operazioni volo, oppure di un sistema di bloccaggio che impedisca l'utilizzo degli inversori di spinta in volo. si decide quale sia migliore per le varie esigenze e per la certificazione. Per concludere all'interno del componente si è sviluppato una scelta della configurazione e delle tipologie di inversori di spinta, in modo da aumentare le scelte possibili per migliorare le architetture e la certificazione. La figura mostra le possibili scelte di configurazione inseriti per gli inversori di spinta. Le possibili configurazioni possono essere, '*target system', 'clam-shell system', 'cold steam system' o 'change the pitch of propeller blades'*. L'ultima si riferisce agli inversori di spinta inseriti per i turboprop, che modificano il pitch delle pale dell'elica. Le altre configurazioni sono relative ai turbofan. (figura 45)

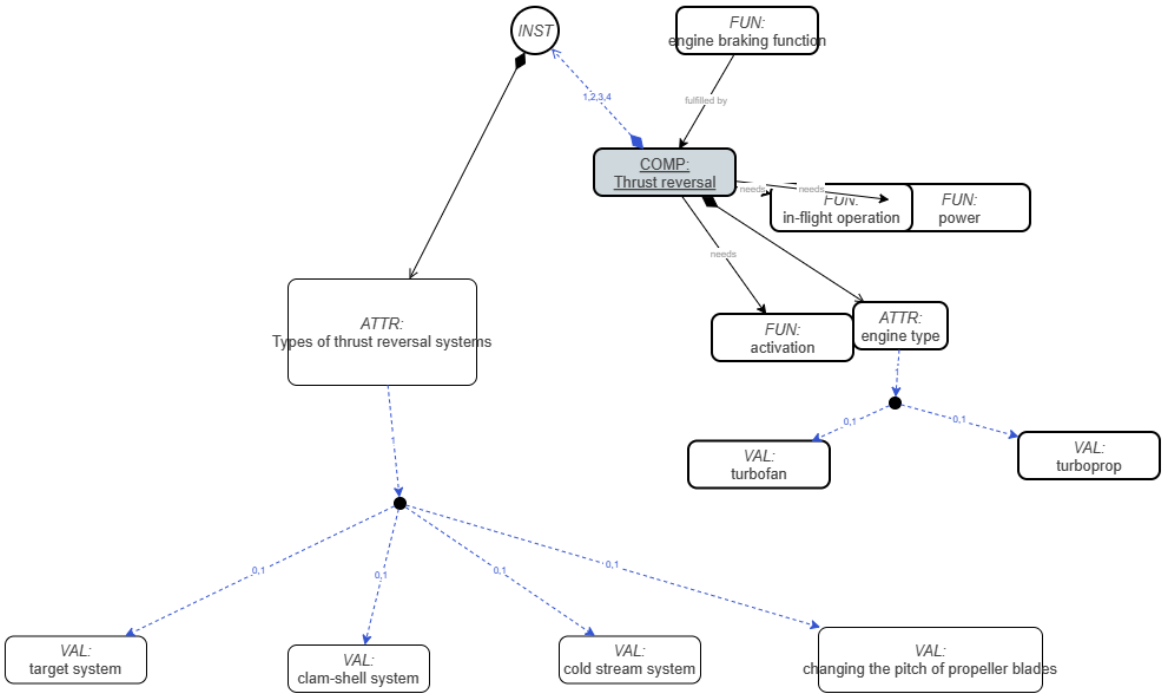


FIGURA 45

L'ultima parte del sistema progettato e dell'impianto frenante e parte più importante è il sistema dei freni delle ruote (*un aereo di piccole dimensioni può non avere gli spoiler o gli inversori di spinta ma i freni delle ruote si, anche nei grandi aerei gli spoiler e gli inversori aiutano la frenata che è principalmente svolta dai freni*). Il sistema dei freni, come di può vedere, è molto più intricato e complesso, visto che è un sistema delicato. Come si vede dalla figura il compito di frenare è compito dal componente 'wheel brake', i freni delle ruote. Questi freni hanno bisogno di varie funzioni. I freni sono composti dai dischi, che servono a trasferire i momenti torcenti alle ruote. I dischi possono essere o multidisco, o singolo disco (per i piccoli aerei) e a ganascia. Poi ci sono le pastiglie dei freni che aumentano l'attrito tra disco e ruota e costituiscono l'azione frenante. I freni devono avere un contenitore per funzionare e questo sono le ruote. Il freno poi ha bisogno di un'azione e questa la possono dare o le pinze (per i piccoli aerei, come nelle macchine) o i pistoncini, che servono anche a stringere i dischi tra di loro e azionare la forza frenante. Nei piccoli aerei i

freni sono molto simili a quelli delle automobili che tutti conoscono. Le ruote hanno poi bisogno di trasferire l'attrito al suolo per aiutare l'azione frenante e questo lo fanno gli pneumatici. Sempre le ruote hanno bisogno di una struttura che è il carrello principale, quello grande, nella zona centrale della fusoliera di sotto. Il carrellino anteriore non possiede i freni e quindi non è preso in considerazione. Gli aerei quando atterrano, lo fanno toccando il suolo prima con il carrello principale per azionare i freni e poi con il carrellino anteriore. Un'altra funzione delle ruote è l'antiscivolamento e questo lo compie il sistema anti-skid. Il sistema frenante è azionato in due modi, manualmente, dai pedali del pilota e del copilota, o automaticamente dal sistema autobrake. Il sistema frenante può funzionare anche in maniera differenziata, cioè solo per il carrello sinistro o per il destro e questo aiuta le sterzate ed è svolto dal wheel brake block, che blocca una parte del sistema. Le pastiglie hanno bisogno di un sistema di controllo usura per capire quando venire cambiate, come le auto, e questo è svolto dal wear indicatori pin. Infine, i freni hanno bisogno di raffreddamento per abbassare l'enorme temperatura creata con l'azione frenante e questo è svolto da un cooling system. (figura 46)

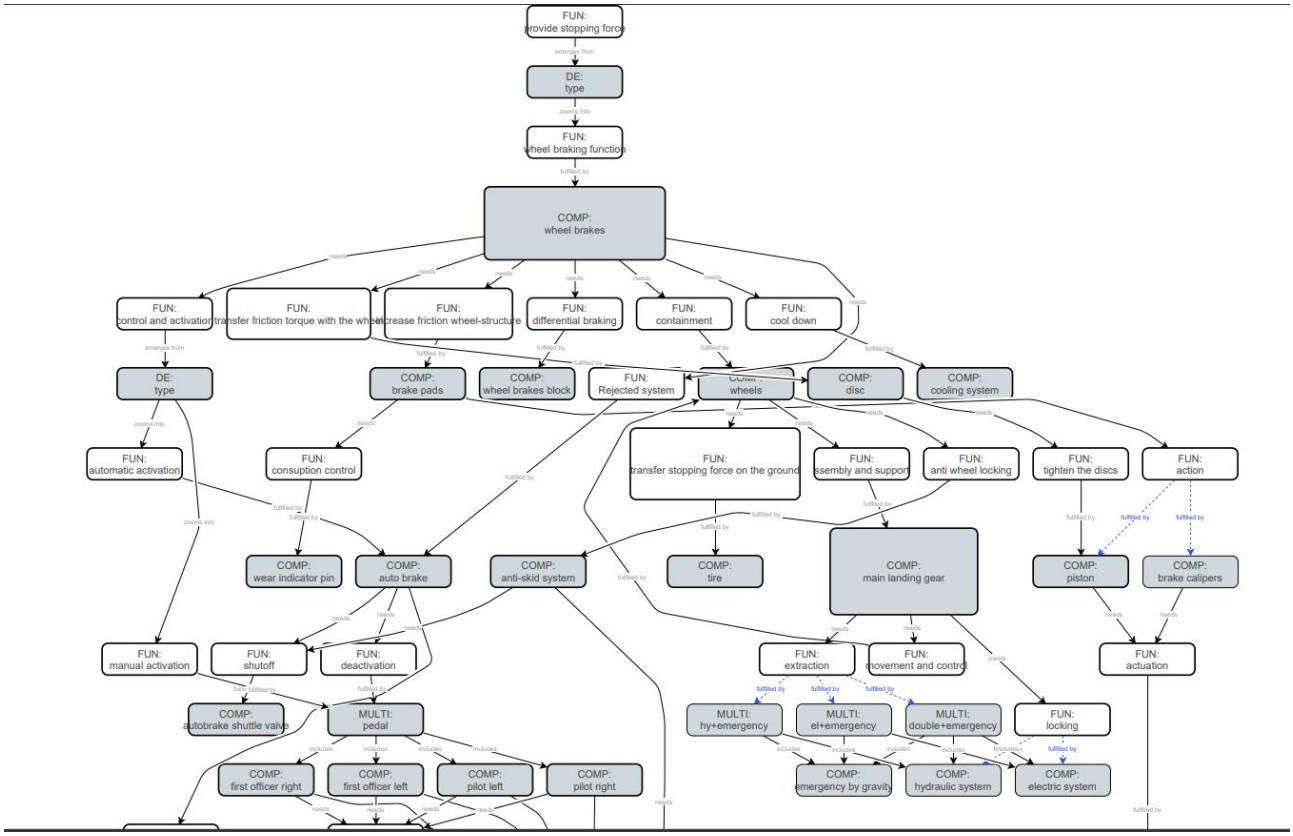


FIGURA 46

Il carrello principale ha bisogno di movimento e controllo e questo è svolto dalle ruote. Poi ha bisogno di un sistema di estrazione (anche retrazione, ma non è stato inserito perché non c'entra con la frenata). L'estrazione è svolta da tre sistemi, elettrico, idraulico e uno di emergenza. Possono esserci tutti e tre o solo due, ma l'emergenza ci deve essere sempre. Questo sistema di emergenza serve a fare estrarre il carrello quando i sistemi non funzionano e lo fa per gravità. L'anti-skid e l'autobrake hanno bisogno di un sistema shutoff e questo la svolge lo shuttle valve. L'autobrake è possibile disattivarlo con i pedali del freno. I pistoncini e la pinza hanno bisogno di attuatori per funzionare e questi attuatori possono essere idraulici, o EMA o EHA o EBHA. Gli attuatori hanno bisogno di controllo e azione, svolta dall'actuator controller e da un controllore di potenza. Una volta premuto il pedale l'azione frenante è passata alle servo-valvole o meter valve che aiutano l'azione frenante, quando l'essere umano non può farlo con la propria forza fisica. Gli attuatori e le meter valve hanno bisogno di un sistema di potenza per funzionare e questo è svolto da tre tipi di circuiti, il circuito principale il verde, il circuito alternativo il blu e il circuito di emergenza. I primi due circuiti di potenza possono essere o idraulici o elettrici o meccanici. Il circuito di emergenza può essere

idraulico o meccanico. È stato inserito una quarta linea di potenza anche generatrice, il brake accumulator, l'accumulatore, che ha bisogno dell'isolation valve per impedire che il flusso percorra la direzione inversa a quella che dovrebbe fare. I tre circuiti hanno poi bisogno di potenza e questa potenza è sviluppata nello stesso modo dei sistemi degli spoiler e degli inversori di spinta. Ci sono quindi le RAT, APU ed engine. Poi ci sono le pompe dei motori ed elettrici ed i generatori. Quando si fanno le scelte architettoniche bisogna scegliere il sistema di generazione di energia attinente alla scelta del tipo di sistema del circuito. (figure 47-48)

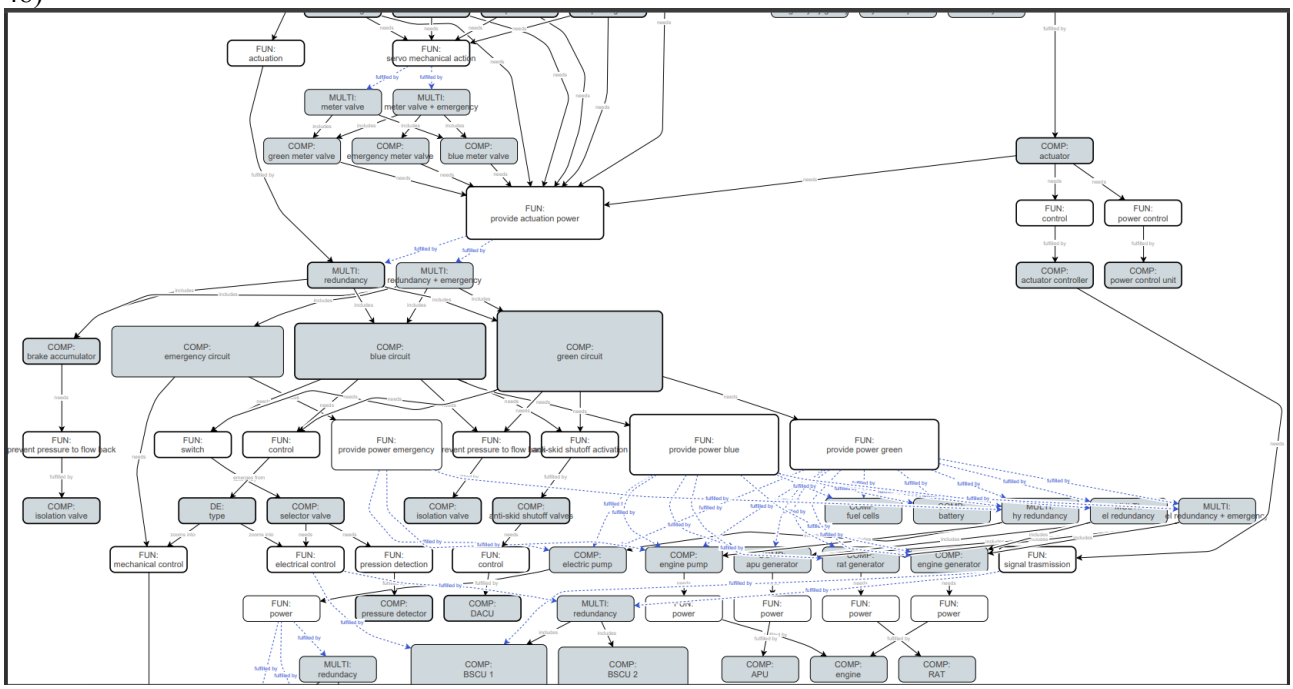


FIGURA 47

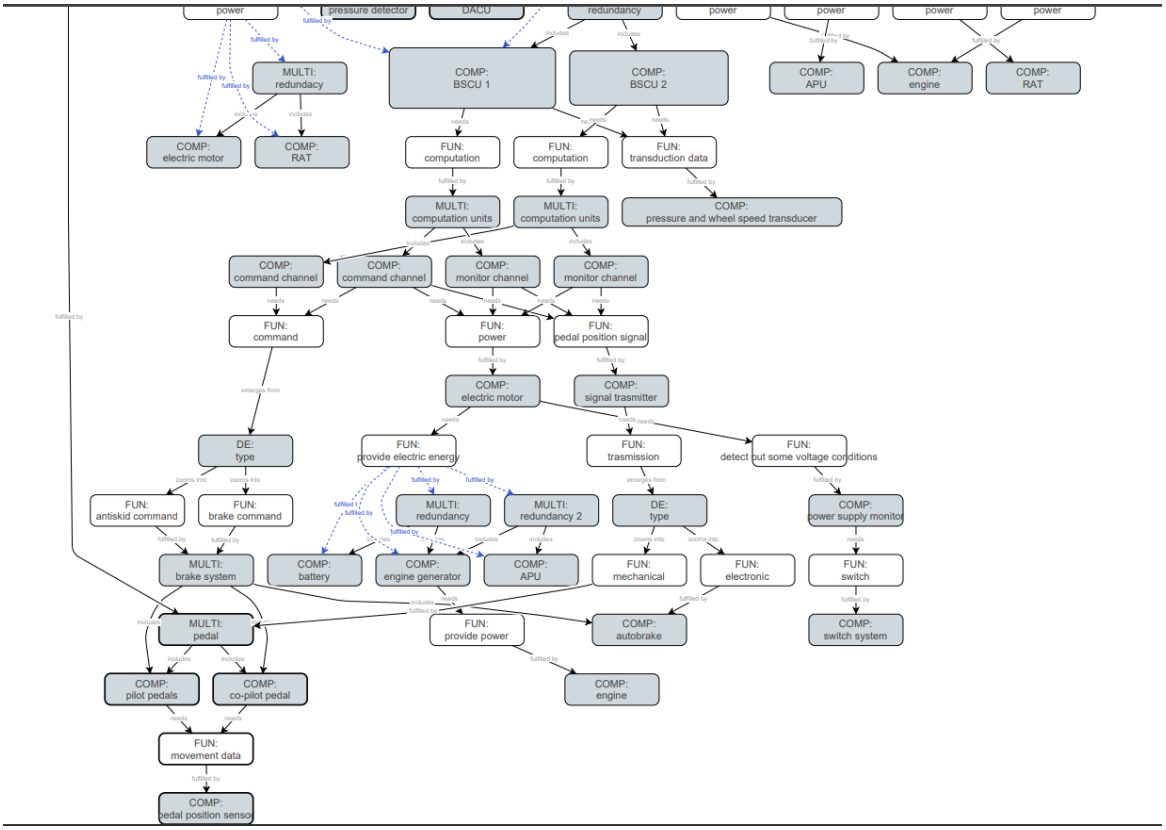


FIGURA 48

I circuiti hanno poi bisogno di altre funzioni oltre alla potenza e l'energia. Necessitano della isolation valve come il brake accumulator. È presente un sistema di switch per passare da un circuito ad un altro nel caso il principale non funzioni si passa all'alternativo ed è svolto da un selector valve che individua la pressione, tramite un pressure detector, e vede se la pressione di un sistema varia troppo rispetto al suo valore ottimale. Questo è un sistema soprattutto idraulico. I circuiti hanno un anti-skid shutoff valve che è controllato da un computer detto DACU. I circuiti sono controllati o meccanicamente, tramite i pedali, oppure, ma anche insieme, elettronicamente da due sistemi computer particolari detti BSCU. Dalla SAE ARP 4761 si vede come, per ridondanza e per arrivare al risultato di 10e-7 di guasto, bisogna provvedere ad avere due BSCU separati, con tutti i componenti interni separati. Le due BSCU sono identiche e sono costituite da due unità di computazione, che a loro volta contengono un canale di comando e un canale di monitoraggio. Questi canali hanno bisogno di tre funzioni, potenza, svolto da un motore elettrico che a sua volta ha bisogno dell'energia e di un power supply monitor per monitorare l'energia. La seconda funzione è il segnale della posizione pedale per capire se sta avvenendo la frenata e questo è svolto da un signal trasmitter che può avere segnali meccanici, cioè fisici della pedaliera o elettronici dell'autobrake. La terza funzione dei canali del BSCU è il comando della frenata che è svolto dall'autobrake e dalla pedaliera. Infine, i due BSCU necessitano di un trasduttore per tradurre i dati di pressione e velocità delle ruote per comprendere quando comando frenante dare ai freni. (figura 49 e figura 50). Le figure 51 e 52 mostrano il design space di tutto il sistema frenante nella sua globalità, unendo quindi i tre impianti dei freni, degli spoiler e degli inversori di spinta.

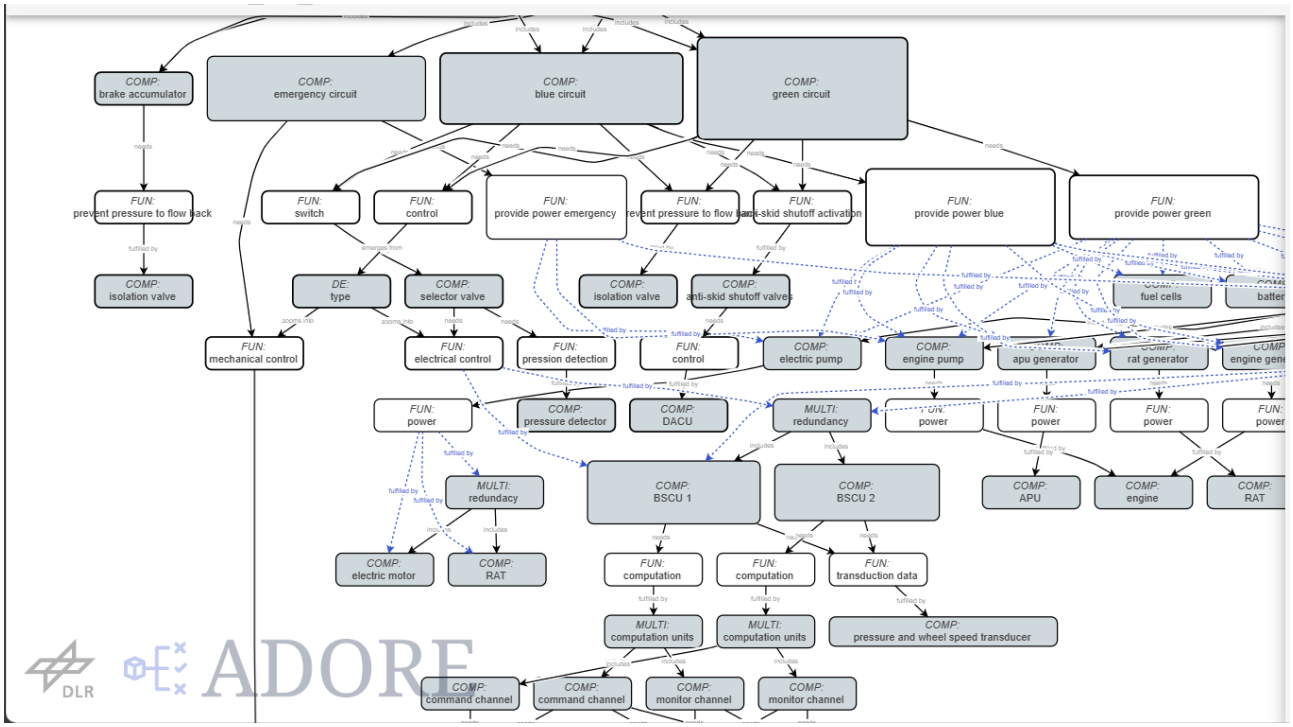


FIGURA 49

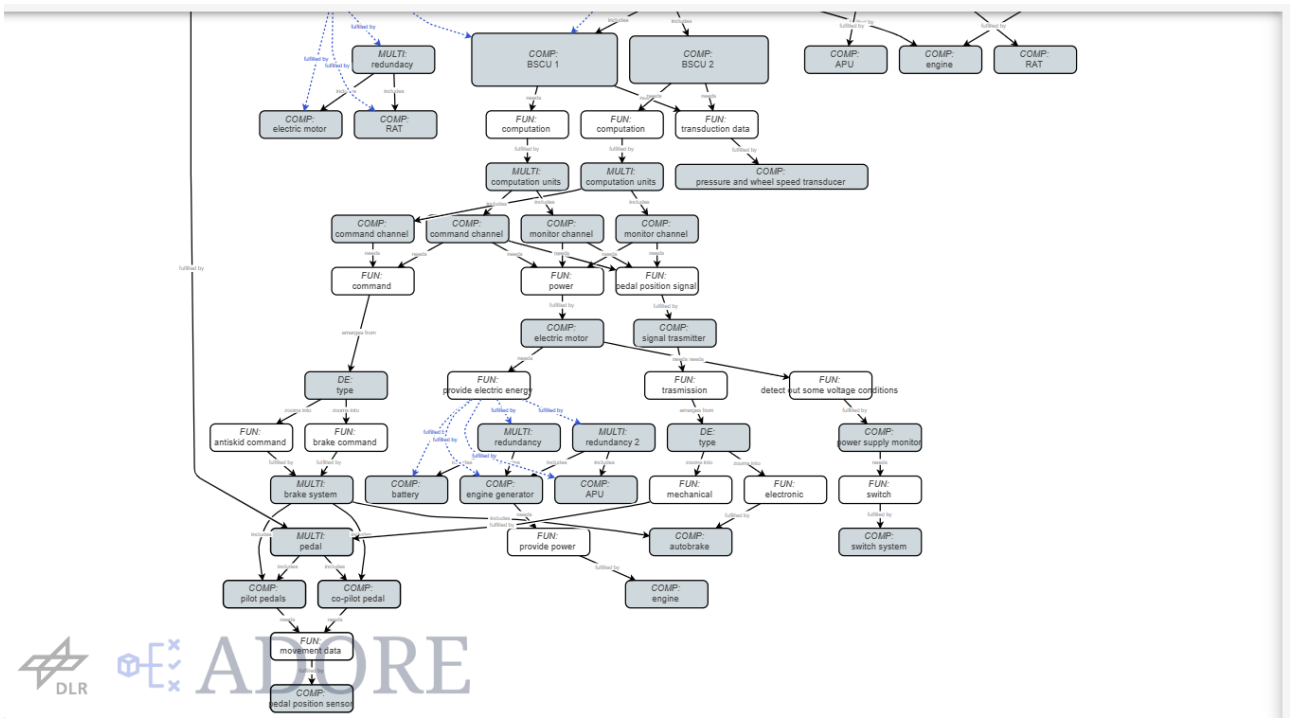


FIGURA 50

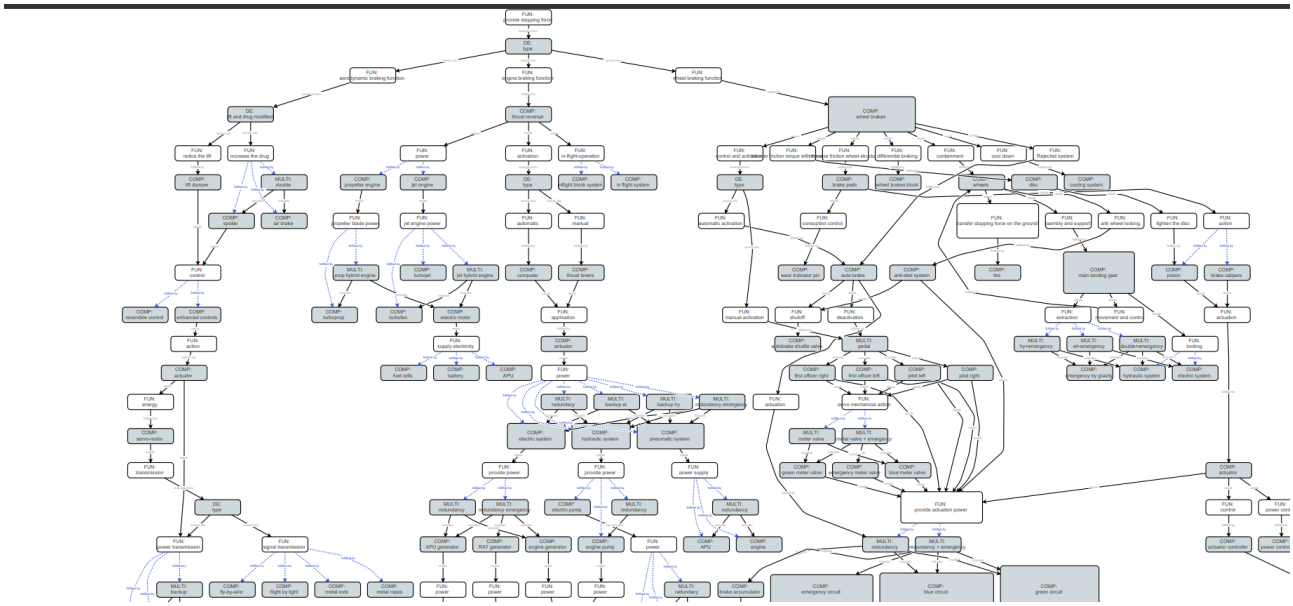


FIGURA 51

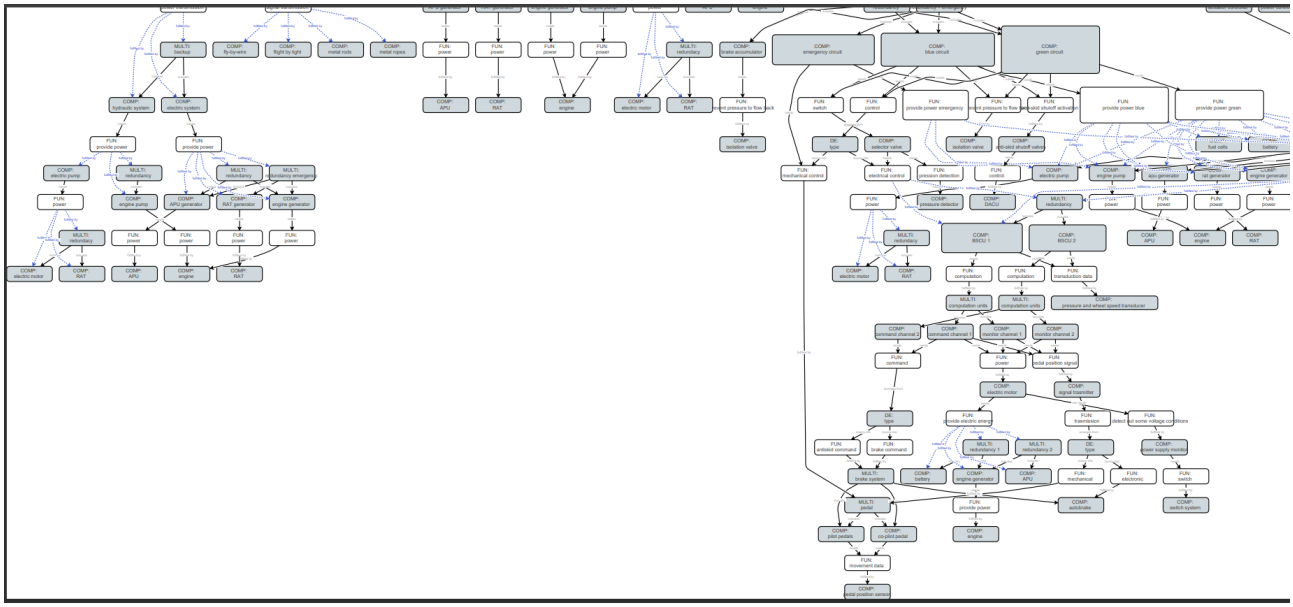


FIGURA 52

6. Il Check Certificativo

Completato il sistema si è arrivati alla fase finale del lavoro di Tesi, certificare il sistema progettato con i vincoli trovati nelle normative. Con il software ADORE si è andati a costruire diverse centinaia di migliaia di possibili architetture di un sistema di bordo. Questo aumenta il livello di scelta di progetto per arrivare a trovare la migliore soluzione possibile per ogni tipo di aereo. La grande quantità di combinazioni possibili crea un enorme spazio di progettazione di architetture che richiede altri software automatici che permettano l'esplorazione adeguata di tutte le possibili scelte. Includere aspetti certificativi nelle prime fasi di progettazione dei sistemi di bordo, e non solo nella parte di verifica (il lato destro del diagramma a V), potrebbe avere due vantaggi. Il primo è che la certificazione può essere utilizzata come filtro, ciò consente di scartare alcune architetture subito dopo che sono state generate se non sono conformi alle specifiche di certificazione. Magari quelle architetture sembrano coerenti e corrette, perché hanno abbastanza tutti gli elementi, ma invece si scopre che hanno carenza di ridondanze o di back-up energetici o altro. Le architetture scartate non necessitano di essere dimensionate e calcolate, risparmiando tempo di calcolo e costi di progettazione e lavoro. Il secondo scopo è che la certificazione incide sulla progettazione e ciò può potenzialmente portare a nuove soluzioni ottimali. Magari mostra che aggiungendo un elemento ne migliora le performance o altro. Questo lavoro di Tesi mostra come creare un collegamento tra la generazione delle architetture dei sistemi di bordo e le regole di certificazione. Ad esempio, alcuni vincoli sono legati alla sicurezza di un sistema e alla sua affidabilità minima richiesta, altri vincoli sono quelli che impongono l'esistenza di sistemi di backup per la generazione di energia, oppure che impongono l'indipendenza delle sorgenti di energia o quelli che limitano il guasto di un singolo componente che porta al guasto dell'intero sistema. I sistemi di bordo sono una parte essenziale di un aeromobile. Rappresentano una parte notevole della massa totale e incidono in maniera notevole sul consumo di carburante. La nuova generazione di aeromobili potrebbe sfruttare i vantaggi di nuovi sistemi innovativi, come migliori prestazioni, minor peso, maggiore affidabilità. Le architetture dei sistemi di bordo degli aeromobili sono definite dai diversi sottosistemi, componenti e connessioni tra loro. Le differenze prestazionali tra le architetture vengono generalmente valutate durante la progettazione preliminare dei sistemi di bordo. Ciò consente di avere una prima intuizione nel decidere se le nuove architetture sono promettenti o meno. Tuttavia, non dovrebbero essere presi in considerazione solo questi aspetti, ma dovrebbero essere presi in considerazione anche altri ambiti, come la certificazione e l'analisi della sicurezza, per verificare se le architetture sono effettivamente realizzabili o meno. La certificazione è obbligatoria per poter permettere di far produrre un sistema e un aereo; quindi, invece di consegnare il sistema e certificarlo, con il rischio di andare incontro a modifiche e ritardi dovuti a elementi non certificabili, la cosa migliore da fare è sviluppare il sistema con già in mente gli elementi certificabili e no. L'enorme quantità di architetture possibili, che possono essere milioni e decine di milioni crea un vasto numero di variabili di progettazione. Ciò crea un enorme spazio di progettazione architettonica che richiede sistemi e software di automazione per essere adeguatamente esplorato, come già detto. L'automazione si applica a tutti gli strumenti e alle connessioni tra loro. Nella maggior parte dei casi la definizione dell'architettura di un sistema viene effettuata sulla base dell'esperienza o dell'analisi dei compromessi. Esiste un paradosso nella progettazione delle architetture dei sistemi di bordo: il paradosso della conoscenza. Nella fase iniziale della progettazione è disponibile molta libertà per modificare la progettazione esistente, ma non è disponibile molta conoscenza del sistema. Non si conoscono ancora le varie sfaccettature e le esigenze vere che il sistema dovrà compiere. Esplorare meglio lo spazio di progettazione durante le fasi preliminari aiuta a mitigare questo paradosso e ad avere risultati più dettagliati durante la progettazione concettuale, supportando il processo decisionale. La scelta dell'architettura corretta è una delle decisioni che ha un impatto maggiore sulle prestazioni del sistema. Oggigiorno si parla tanto anche di '*open architecture*', un 'architettura che permetta di andare a modificarla più facilmente rispetto a quelle chiuse, in modo da aggiornarla e modificarla in base alle nuove esigenze. Ma questo non è argomento di tesi. Un concetto importante che si sta sviluppando in questi anni è l'ingegneria simultanea. È una metodologia riguardante la progettazione e lo sviluppo dei prodotti. L'obiettivo principale, e cuore del concetto, è che le diverse fasi del ciclo di vita di un prodotto siano considerate ed eseguite simultaneamente anziché consecutivamente. Ciò migliora i tempi di sviluppo del prodotto, che per gli aeromobili rappresentano una priorità. L'ingegneria simultanea mira a creare un quadro multidisciplinare con tutti i domini coinvolti nel processo di progettazione. Tutte le discipline sono esplorate in parallelo. Alcuni aspetti chiave includono la gestione della complessità suddividendo lo sviluppo in domini (*certificazione, produzione, manutenzione...).*

Questa Tesi si basa sulla certificazione e il lavoro parallelo tra certificatore e progettista. Questo argomento è stato ampiamente descritto e sviluppato nel capitolo iniziale. Alcune linee guida per la certificazione dei sistemi aeronautici sono contenute negli standard tecnici e sono relative a tecniche in uso da un po'. Il problema principale è che la maggior parte di queste tecniche e standard essi necessita di un livello di dettaglio troppo elevato per essere eseguito durante le fasi iniziali della progettazione (FMECA, FTA). Inoltre, non possono essere facilmente automatizzati a causa dell'enorme quantità di informazioni che richiedono, e bisogna sempre costruirli da zero. Bisogna quindi utilizzare un metodo per cercare di automatizzare il più possibile questo aspetto di certificazione e di controllo. Questa Tesi mostra un aspetto di questo collegamento tra la progettazione e la certificazione. Questo lavoro vuole inserirsi nel lato sinistro del diagramma a V. poi altri lavori utilizzeranno i vincoli trovati e alcune procedure per migliorare l'automazione e i software che permettono di creare al meglio il collegamento tra sistema e certificazione. La CS25, e la SAE ARP 4754 verranno utilizzate per il caso di applicazione ma per altre normative, come descritto per la CS-23, la procedura è identica, magari si semplificano molti elementi visto che si parla di piccoli aerei. Alcune regole sono qualitative, altre quantitative. Una regola quantitativa stabilisce che la sicurezza di un sistema deve essere valutata e fornisce un valore minimo di affidabilità che deve essere garantito. Per stimare ciò, viene utilizzata la tecnica del diagramma a blocchi di affidabilità (RBD, reliability block diagram) e automatizzata, che verrà svolto in futuro con i vincoli trovati in questo lavoro. Le regole qualitative sono quelle che impongono l'esistenza di sistemi di backup per la produzione di energia, la loro indipendenza, la loro ridondanza o quelle che limitano il guasto di un singolo componente che porta al guasto dell'intero sistema. Una volta fatto il sistema con ADORE si andranno a valutare alcuni requisiti. Dopo che le architetture sono state generate queste vengono filtrate seguendo specifiche normative. I vincoli e le normative per i sistemi di bordo, come detto, abbondantemente nei primi capitoli, non prevedono regole dirette o specifiche per le architetture dei sistemi di bordo di un aeromobile. Ciò significa che non esistono regole dirette riguardo, ad esempio, sul numero di attuatori o ridondanze che dovrebbe avere un componente specifico. Forniscono requisiti più generali e generici sulla sicurezza e l'affidabilità dei sistemi. [22] [23] Questi requisiti generici possono quindi essere utilizzati e applicati alle architetture dei sistemi di bordo. I primi lavori hanno identificato tre requisiti, i primi due di tipo qualitativo, mentre il terzo di tipo quantitativo.
-Requisito 1: fonte di alimentazione di riserva in caso di perdita dei motori.
-Requisito 2: condizione di guasto singolo.
-Requisito 3: Affidabilità minima.
Il primo requisito qualitativo deriva dal vincolo CS 25.671. Specifica che deve essere presente almeno un sistema di back-up di energia per garantire il corretto funzionamento del sistema di controllo di volo e del carrello di atterraggio in caso di perdita di tutti i motori. Per gli aeromobili esistenti ciò viene solitamente garantito aggiungendo un APU o una RAT. Ma sono possibili anche altre soluzioni con altre fonti di energia ridondanti non dipendenti dal motore, come le fuel cells o le batterie di nuova generazione. Il secondo requisito qualitativo deriva da CS 25.1309(b)(1)(ii) ed indica che il singolo guasto di un componente non deve mai portare al guasto dell'intero sottosistema. Ciò richiede la presenza di ridondanze, sia a livello di componenti che di linee elettriche. Questo requisito è sottolineato in ulteriori capitoli durante tutta la CS-25. Il terzo requisito è quello quantitativo e deriva sia dalla CS 25.1309(b)(1)(i) che dalla AMC 25.1309(7.c)(1)(iv)). Stabilisce che condizioni di guasto catastrofico devono verificarsi con una probabilità media inferiore a 1×10-9 per ora di volo. Per valutare i primi due requisiti bisogna osservare le architetture e vedere se sono presenti ridondanze e back-up energetici. Per valutare il terzo requisito si utilizza la tecnica del diagramma a blocchi di affidabilità (RBD). Ma qui sorge un problema non da poco. Il RBD di un sistema non è lo stesso della sua architettura fisica. Inoltre, un'architettura fisica può rappresentare diverse modalità di funzionamento che si traducono in diversi RBD. [22] L'implementazione di questo filtro viene eseguita utilizzando un software progettato dal Politecnico di Torino, in collaborazione con il DLR in Germania, ACOBS (Automated Preliminary Certification of Aircraft On-Board Systems), uno strumento con linee di codice Python. Questo software legge come input le architetture generate da ADORE e fornisce come risultato il risultato per ciascuno dei tre requisiti precedentemente spiegati. All'interno del software l'architettura viene automaticamente trasformata in un RBD e verifica ciascuno dei tre requisiti. Per il primo lo strumento cancella automaticamente tutte le linee collegate ai motori e controlla se c'è ancora almeno un sistema di back-up che fornisce energia. Per il secondo, esegue l'iterazione più volte facendo fallire ciascuno dei componenti e controllando se la funzione principale può ancora essere soddisfatta. Per il terzo requisito, il quantitativo, legge un diagramma a blocchi di affidabilità come input e fornisce la probabilità di guasto

dello stesso. Però non è automatico, perché i tassi di guasto di ciascuno dei componenti devono essere forniti come input. Se la probabilità di fallimento è superiore a quella prevista dalla normativa, il codice restituisce un warning. Ed è questo il problema principale, perché tutti i calcoli dipendono direttamente dalla stima dei tassi di guasto e queste informazioni solitamente non sono pubbliche, sono secretate, o sono obsolete e non aggiornate dalle aziende produttrici. Il confronto dei risultati con un valore fisso rende il filtro non affidabile al 100%. Il filtro di certificazione deve essere chiuso e collegato all'ottimizzatore per essere efficace. Questo lavoro di tesi si ferma subito dopo il filtro certificativo ma il vantaggio è che dopo è possibile aggiungere ulteriori analisi e vincoli di altro genere (*prestazioni, manutenzione, produzione o altre analisi del ciclo di vita*). Poiché lo scopo di questa tesi sono i vincoli di certificazione, tutto sarà basato sul modello di certificazione e vincoli normativi. Come variabili di progettazione è dato lo spazio di progettazione, le variabili di progettazione rappresentano ciascuna delle diverse architetture possibili. Come vincoli vengono utilizzati i tre requisiti inclusi nel filtro di certificazione, ovvero la condizione di backup, il caso di guasto singolo e l'affidabilità minima. Se solo una delle tre condizioni non viene soddisfatta, il filtro risulta in una condizione di non superato e l'architettura viene scartata in quanto non realizzabile o, meglio, non certificabile. Per quanto riguarda l'implementazione, ADORE è in grado di valutare l'intero processo di ottimizzazione. Ad esso si collega il filtro di certificazione ACOBS (figure 53-54) e si selezionano le quantità di ottimizzazione. L'intero processo di ottimizzazione funziona in questo modo:

• il design space è modellato in ADORE. Il software avvia il processo di ottimizzazione e genera una possibile architettura per iterazione.

• L'architettura viene inviata al software di certificazione ACOBS, dove viene tradotta in affidabilità diagramma a blocchi.

• I tre requisiti di certificazione vengono valutati automaticamente. Ognuno di essi è collegato a un vincolo. La probabilità di fallimento è data come obiettivo di ottimizzazione.

• ADORE raccoglie i risultati e analizza se i vincoli sono stati soddisfatti o meno e utilizza algoritmi di ottimizzazione per generare una nuova architettura basata sui risultati dell'obiettivo di ottimizzazione.

Questo è in sintesi il lavoro ottimizzato ADORE e ACOBS, ma questo lavoro di Tesi verrà svolto in maniera leggermente diversa, con lo stesso obiettivo. I tre requisiti si basano su tre vincoli normativi, ma i vincoli non sono solo tre, ce ne sono altri, non sono un'enormità, ma ce ne sono. I vincoli sono stati individuati e spiegati nei capitoli precedenti. Alcuni di essi non sono propriamente vincoli architettonici, ma aiutano a comprendere al meglio i vincoli, altri sono vincoli che ripetono in maniera differente lo stesso concetto, con qualche aggiunta. I vincoli non sono mai separati l'uno dall'altro, ma uno dice una cosa che è complementare ad una altro e così via. Questi vincoli verranno implementati nel software ACOBS per migliorarlo e aiutare a certificare più sistemi possibili e in maniera migliore possibile. Verranno implementati vincoli trovati anche nella CS-23, per i piccoli aerei ma utili per ogni evenienza, in modo da certificare sia sistemi di grandi aerei sia sistemi di piccoli aerei. Verranno implementati vincoli trovati anche nella SAE ARP 4754. In questo lavoro verranno valutati i vincoli qualitativi, cioè questi vincoli che non esprimono pienamente un numero di probabilità e affidabilità, ma espongono problemi architettonici su ridondanze e componenti e sorgenti. Tramite il software ADORE verranno costruiti delle architetture manualmente, tramite la scelta dei componenti in maniera manuale, non automatica. Verranno valutati e creati 5-6 architetture per ciascun dei tre impianti in cui è suddiviso l'intero impianto frenante. Si potrebbe creare una sola architettura per l'intero sistema frenante, ma il risultato sarebbe troppo confusionario e difficile da valutare in maniera manuale. Con un software si può fare, ma con la mente umana è più semplice e di migliore comprensione suddividere il sistema in tre impianti. Verrà fatto un check certificativo manuale tramite l'osservazione delle architetture costruite. Questo approccio non modificherà il risultato perché i tre impianti non hanno niente in comune, svolgono tutti e tre la stessa funzione primaria, ma i componenti non sono collegati, come si può vedere dal design space, solo la funzione primaria, cioè '*provide stopping force'*. La suddivisione dei tre impianti è già stata ampiamente spiegata nel capitolo precedente. Insieme ai tre vincoli precedenti, verranno utilizzati i vincoli proveniente dai seguenti capitoli della *CS-25: AMC 25.1309 (6)(b); 25.671 (c); AMC 25.671 (7), (8), (12)(a); 25.729 (c)(2); 25.735 (b)(1); AMC 25.735 (4)(b),(e); 25.933 (a)(2); 25.953 (a); 25.1011 (a); 25.1307 (b); 25.1351 (b),(d); AMC 25.1351; 25.1355 (c); SAE ARP 4754 capitolo 5 'REQUIREMENTS DETERMINATION AND ASSIGNMENT OF DEVELOPMENT ASSURANCE LEVEL'; SAE ARP 4761 'APPENDIX L CONTIGUOUS SAFETY ASSESSMENT PROCESS EXAMPLE'*. Per ogni sistema di impianto verranno mostrate due esempi di architettura, una qualitativamente certificabile e una non certificabile. Verrà

spiegato per ognuno perché sono o no certificabili e inoltre verranno aggiunti altri elementi che possono rendere le architetture non certificabili, ma che non sono state inserite nell'architettura d'esempio.

FIGURA 53

```
Carlos Cabaleiro
def rbd_main(in_file, max_iter, rule_1, rule_2, rule_3):
    """
    Reads the input file and a maximum number of allowed iterations for the RBD solving.
    Also reads which rules should be assessed: 0 to not evaluate, 1 to evaluate.
    Returns the results in terms of:
        - Number of components and nodes, used for testing. Integers.
        - Iteration: number of iterations needed to reduce the reliability block diagram. Integer.
        - Rule_1: results of the reliability of the system. Float.
        - Rule_2: results of the single failure requirement. 0 not-passed, 1 passed.
        - Rule_3: results of the back-up requirement. 0 not-passed, 1 passed.
    """

    if rule_1 == 1:
        num_comps, num_nodes, reliability, iteration = reliability_result(in_file, max_iter)
    else:
        num_comps, num_nodes, reliability, iteration = [0, 0, 1, 0]

    if rule_2 == 1:
        safety = single_component_failure(in_file, max_iter)
    else:
        safety = 1

    if rule_3 == 1:
        back_up = back_up_system(in_file)
    else:
        back_up = 1

    return num_comps, num_nodes, reliability, iteration, safety, back_up
```

FIGURA 54

- ARCHITETTURE DEGLI INVERSORI DI SPINTA

Il primo impianto in cui verrà fatto il check certificativo manuale è l'impianto degli inversori di spinta. Verrà analizzato la prima architettura e poi la seconda. Nelle segenti architetture si andranno ad anlizzare i due requisiti di ACOBS, insieme aivicnoli citati pocanzi.

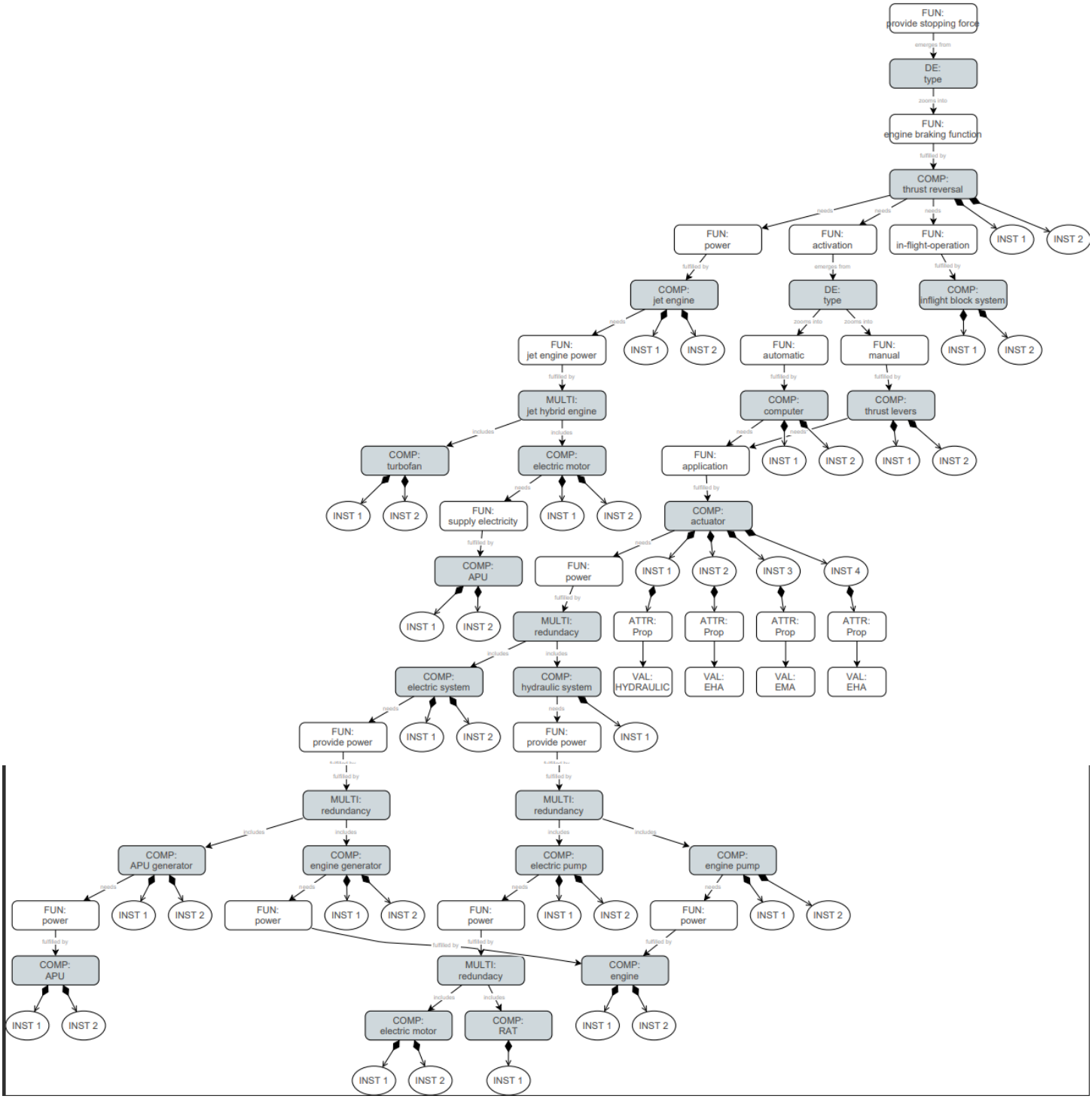


FIGURA 55

I punti principali di questa architettura di sistema sono i seguenti. Per iniziare è un bimotore. (figura 55)

- Questa architettura possiede abbastanza ridondanze dei suoi componenti per impedire una single failure. Non si vedono componenti di cui il guasto possa comportare un evento catastrofico. Anche con il guasto di un componente l'impianto e l'architettura continuerebbero a svolgere le sue funzioni, quindi il vincolo 25.1309 è rispettato.
- Per quanto riguarda le sorgenti di potenza e il loro back-up energetico, si può vedere come ogni sistema di distribuzione di energia possieda un back-up, oltre alla sorgente principale del motore. Il sistema elettrico possiede due APU generator e due APU. Mentre il sistema idraulico possiede un back-up energetico di tre componenti, due electric motor e una RAT, oltre al motore, e quindi sicurezza garantita.
- Gli attuatori sono 4, due per motore, di cui uno idraulico e tre EHA. Essendoci un sistema idraulico è corretto inserire un attuatore idraulico. Gli attuatori sono collegati a tre sistemi indipendenti, due elettrici e uno idraulico.
- Questa architettura e le prossime saranno focalizzate nell'impronta di una filosofia 'more electric', quindi il sistema elettrico sarà utilizzato maggiormente del sistema idraulico che è stato inserito come ridondanza e back.up del sistema elettrico, visto che un sistema elettrico totale non è ancora al 100% sicuro, ma deve avere almeno un sistema di backup idraulico nel caso di malfunzionamenti. I motori sono ibridi che oltre al kerosene utilizzano l'energia elettrica.
- Il sistema del blocco in volo è ridondato.
- Il sistema elettrico, secondo il vincolo 25.1307, è ridondato con due linee indipendenti.

Tutti i vincoli riguardanti gli aspetti qualitativi e i vincoli trovati sull'indipendenza dei sistemi di distribuzione di potenza sono rispettati. Questa architettura è certificabile. Adesso andremo ad analizzare la seconda architettura prodotta per questo impianto.

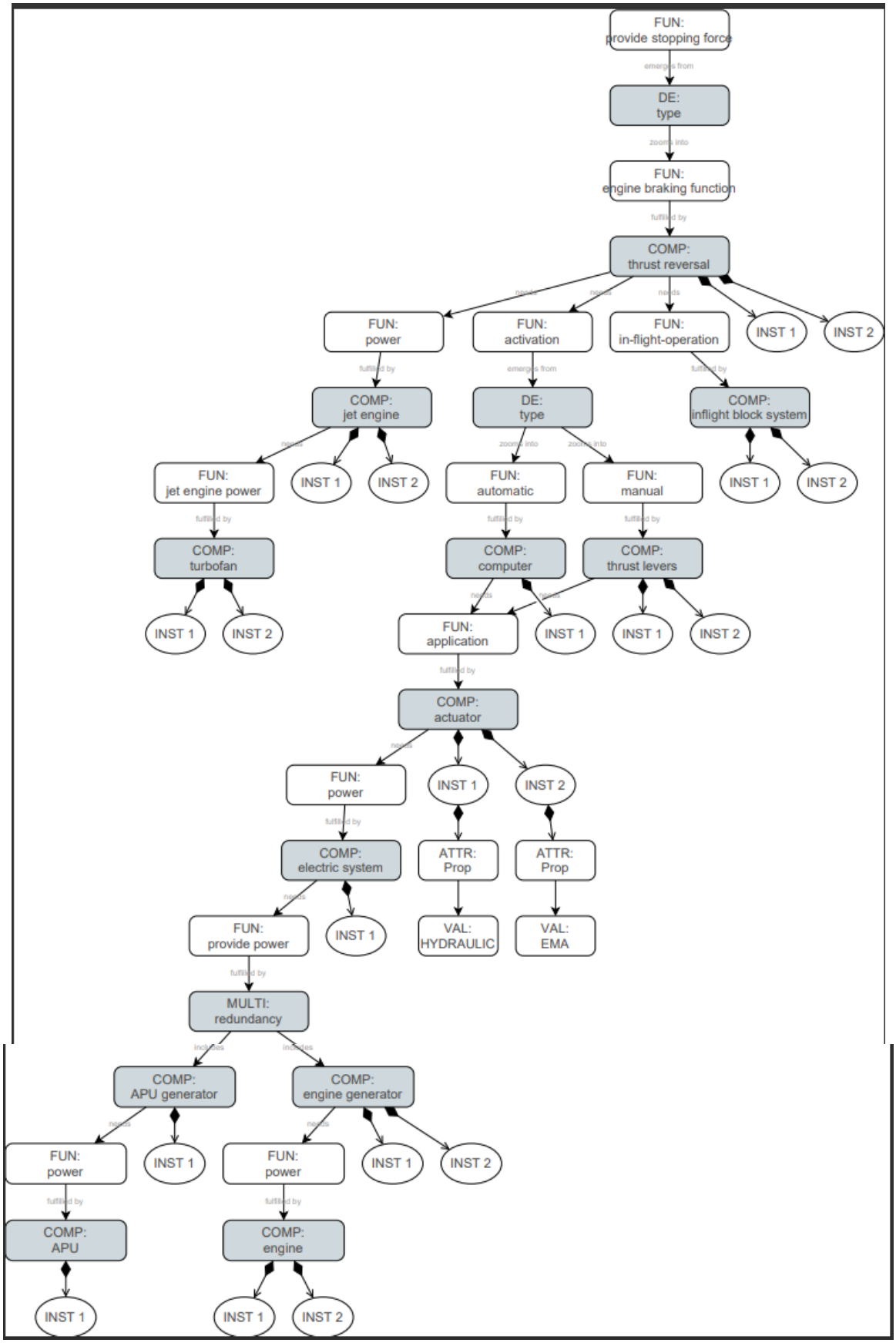

FUN:
provide stopping force
emerges from
DE:
type
zooms into
FUN:
engine braking function
fulfilled by
COMP:
thrust reversal
needs
needs
needs
FUN:
power
FUN:
activation
FUN:
in-flight-operation
INST 1
INST 2
fulfilled by
emerges from
fulfilled by
COMP:
jet engine
DE:
type
COMP:
inflight block system
needs
zooms into
zooms into
FUN:
jet engine power
INST 1
INST 2
FUN:
automatic
FUN:
manual
INST 1
INST 2
fulfilled by
fulfilled by
fulfilled by
COMP:
turbofan
COMP:
computer
COMP:
thrust levers
INST 1
INST 2
needs
needs
FUN:
application
INST 1
INST 1
INST 2
fulfilled by
COMP:
actuator
needs
FUN:
power
INST 1
INST 2
fulfilled by
COMP:
electric system
ATTR:
Prop
ATTR:
Prop
needs
FUN:
provide power
INST 1
VAL:
HYDRAULIC
VAL:
EMA
fulfilled by
MULTI:
redundancy
includes
includes
COMP:
APU generator
COMP:
engine generator
needs
needs
FUN:
power
INST 1
FUN:
power
INST 1
INST 2
fulfilled by
fulfilled by
COMP:
APU
COMP:
engine
INST 1
INST 1
INST 2

FIGURA 56

La seconda architettura che viene proposta relativa all'impianto degli inversori di spinta è visivamente meno complessa della precedente, infatti mancano delle cose fondamentali. È un bimotore turbofan non ibrido. I punti principali di questa architettura di sistema sono i seguenti. (figura 56)

- Fino agli attuatori la situazione è corretta, perché ci sono le ridondanze. Il problema viene dopo. Gli attuatori sono pochi, uno per motore, ma non è questo il problema, perché comunque potrebbero andare bene, se progettati correttamente.
- Il problema che gli attuatori sono collegati ad un solo sistema di distribuzione di potenza, quello elettrico. Non c'è un sistema di ridondanza, come l'idraulico. Inoltre, il sistema elettrico è uno soltanto, mentre il vincolo 25.1307 dice che devono essere 2 o più ed indipendenti.
- Per quanto riguarda il sistema elettrico è comunque corretto perché possiede una ridondanza delle sorgenti di potenza, come l'APU. Mancando comunque un secondo sistema di potenza e una ridondanza dei sistemi di potenza con un altro la seguente architettura non è certificabile, perché essendoci un solo sistema elettrico non si rispetta il vincolo 25.1309 della single failure, che potrebbe portare ad evento catastrofico.
- C'è anche un altro problema, non direttamente legato ai vincoli normativi ma al design. Infatti, è presente un attuatore idraulico, ma non c'è nessun sistema idraulico ad alimentarlo. Questo non è un vincolo di sicurezza, ma un vincolo di design che non è stato rispettato. Mettere un attuatore senza inserire un sistema di potenza porta a d avere un attuatore inutile e che non verrà usato. Quando si inseriscono gli attuatori e le loro possibili configurazioni bisogna fare attenzione che vengano inseriti i sistemi di potenza giusti per alimentarli.

Questi elementi, soprattutto gli ultimi tre punti, pertanto a vedere che l'architettura di questo sistema non ha rispettato i vincoli qualitativi imposti dalle normative e di conseguenza non è certificabile. Il secondo impianto cui si andrà a fare il check è il sistema degli spoiler.

- ARCHITETTURE DEGLI SPOILER

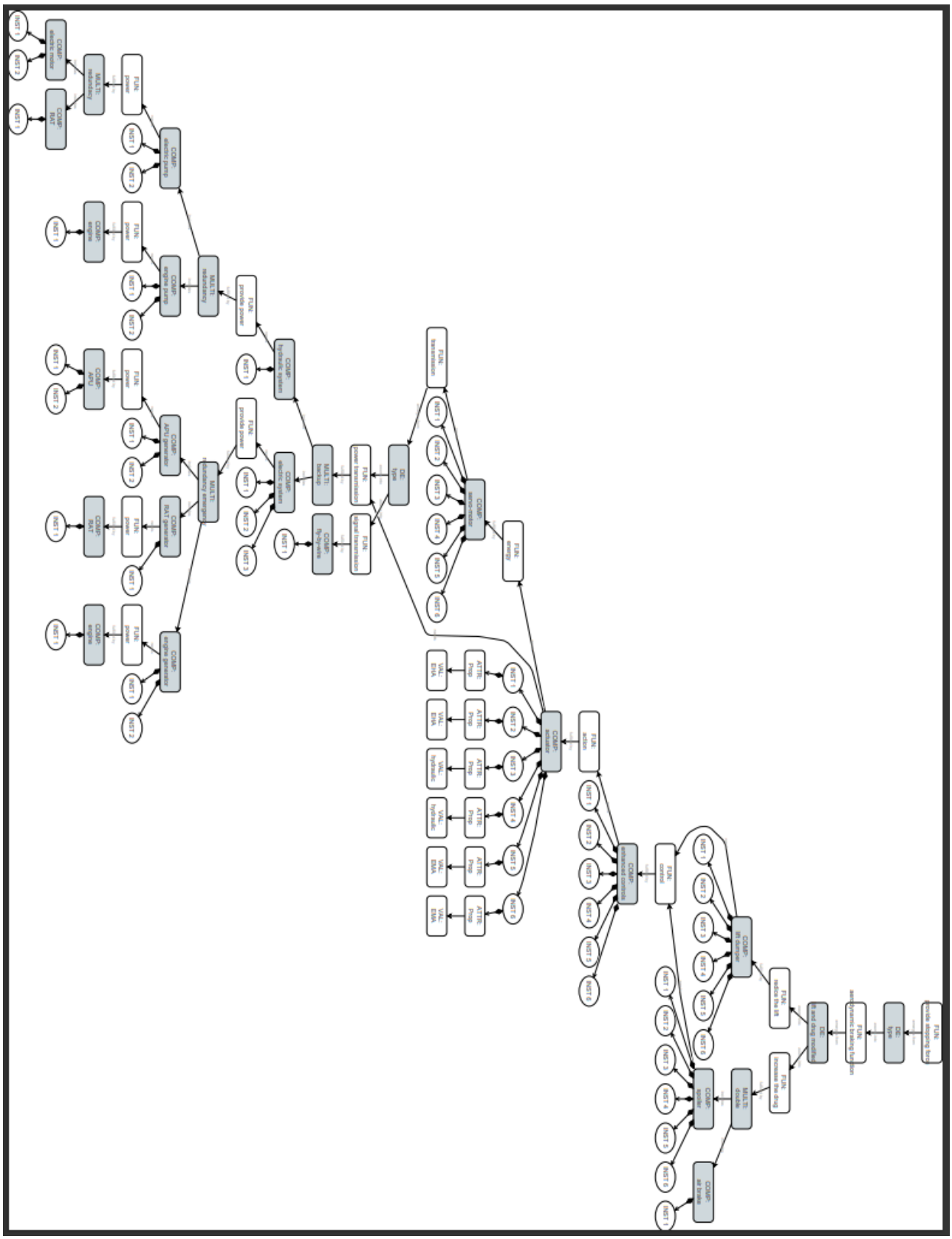


FIGURA 57

I punti importanti di questa architettura di sistema sono i seguenti. Il sistema rappresenta un bimotore. (figura 57)

- L'architettura mostra ridondanza con gli spoiler, 6 in totale. I componenti sono ridondati e non è presente un componente che possa causare da single failure un evento catastrofico. Quindi il vincolo 25.1309 è soddisfatto.
- Per quanto riguarda i sistemi di distribuzione di potenza, sono presenti 4 sistemi, 3 elettrici e uno idraulico, sempre per il discorso della filosofia more electric. Il sistema elettrico è ridondato e quindi il vincolo 25.1307 è rispettato.
- Questi sistemi sono alimentati da una ridondanza di sorgenti di potenza. Infatti, sono presenti, oltre al generatore del motore, anche dei generatori ausiliari, APU ed electric motor (*si poteva mettere anche una RAT o delle batterie, il risultato non cambia, cambiano le performance, ma l'obiettivo di questo lavoro è vedere se le architetture sono certificabili, poi una volta certificata l'impostazione si possono sostituire componenti per varie esigenze e richieste del cliente e della missione*). Anche questi generatori sono ridondati.
- A differenza dell'architettura dei sistemi di inversione di spinta, in questa architettura non si è approfondito il tipo di motore, ma si è inserito solo un generico motore a getto.
- Gli attuatori sono 6, uno per spoiler e anche i vincoli di design sono stati rispettati. Infatti, anche gli attuatori idraulici hanno il loro sistema di alimentazione, il sistema idraulico. Naturalmente gli attuatori idraulici sono in minoranza rispetto agli attuatori di nuova generazione, i tipi EHA.

Questa architettura è quindi certificabile perché ha rispettato i vincoli normativi individuati.

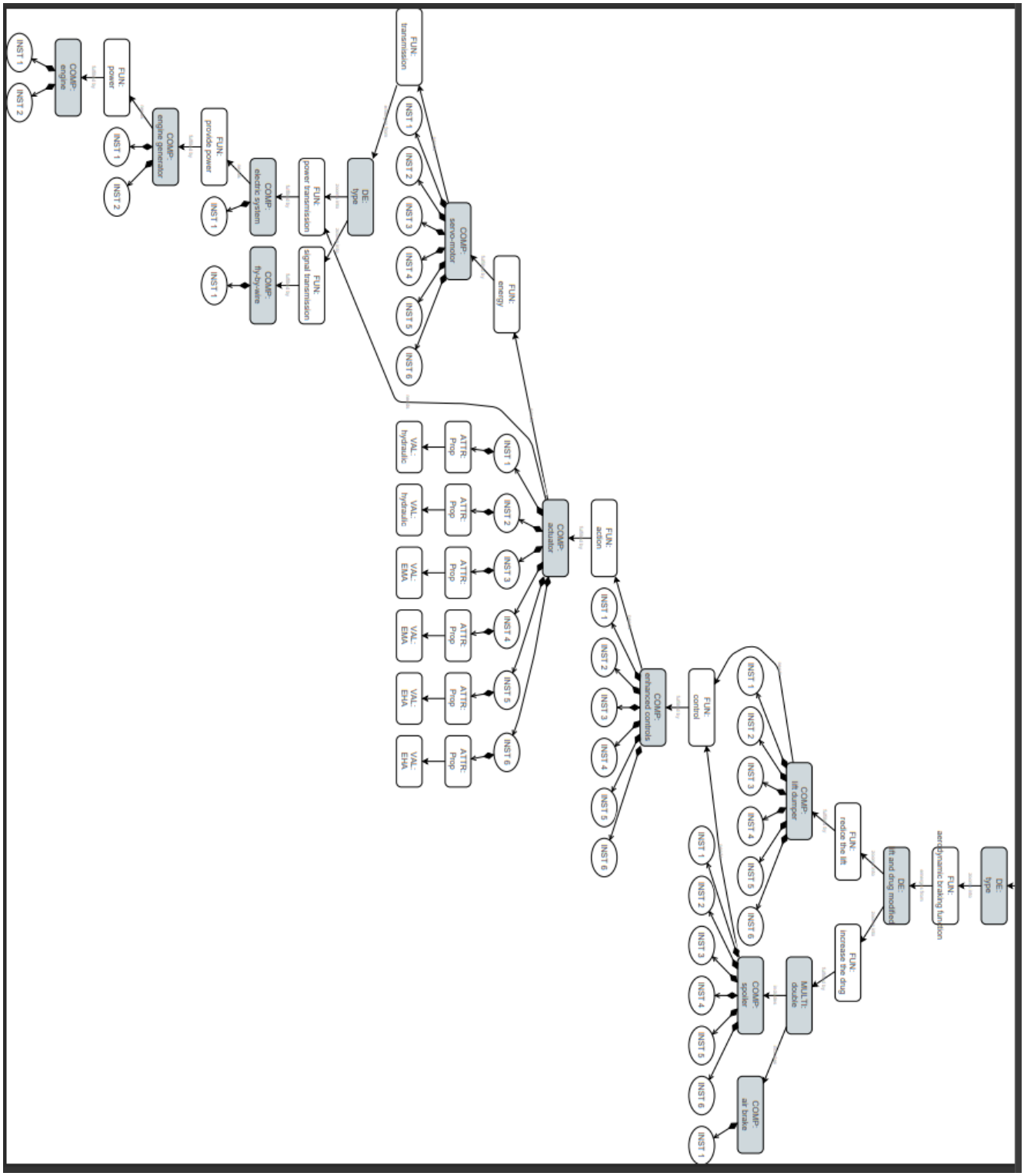

DE: type
FUN: aerodynamic braking function
DE: lift and drag modified
FUN: reduce the lift
FUN: increase the drag
COMP: lift damper
COMP: spoiler
MULTI: double
COMP: air brake
INST 1
INST 2
INST 3
INST 4
INST 5
INST 6
FUN: control
COMP: enhanced controls
FUN: action
COMP: actuator
ATTR: Prop
VAL: hydraulic
VAL: EMA
VAL: EHA
DE: type
FUN: energy
COMP: servo-motor
FUN: transmission
DE: type
FUN: power transmission
FUN: signal transmission
COMP: electric system
COMP: fly-by-wire
FUN: provide power
COMP: engine generator
FUN: power
COMP: engine

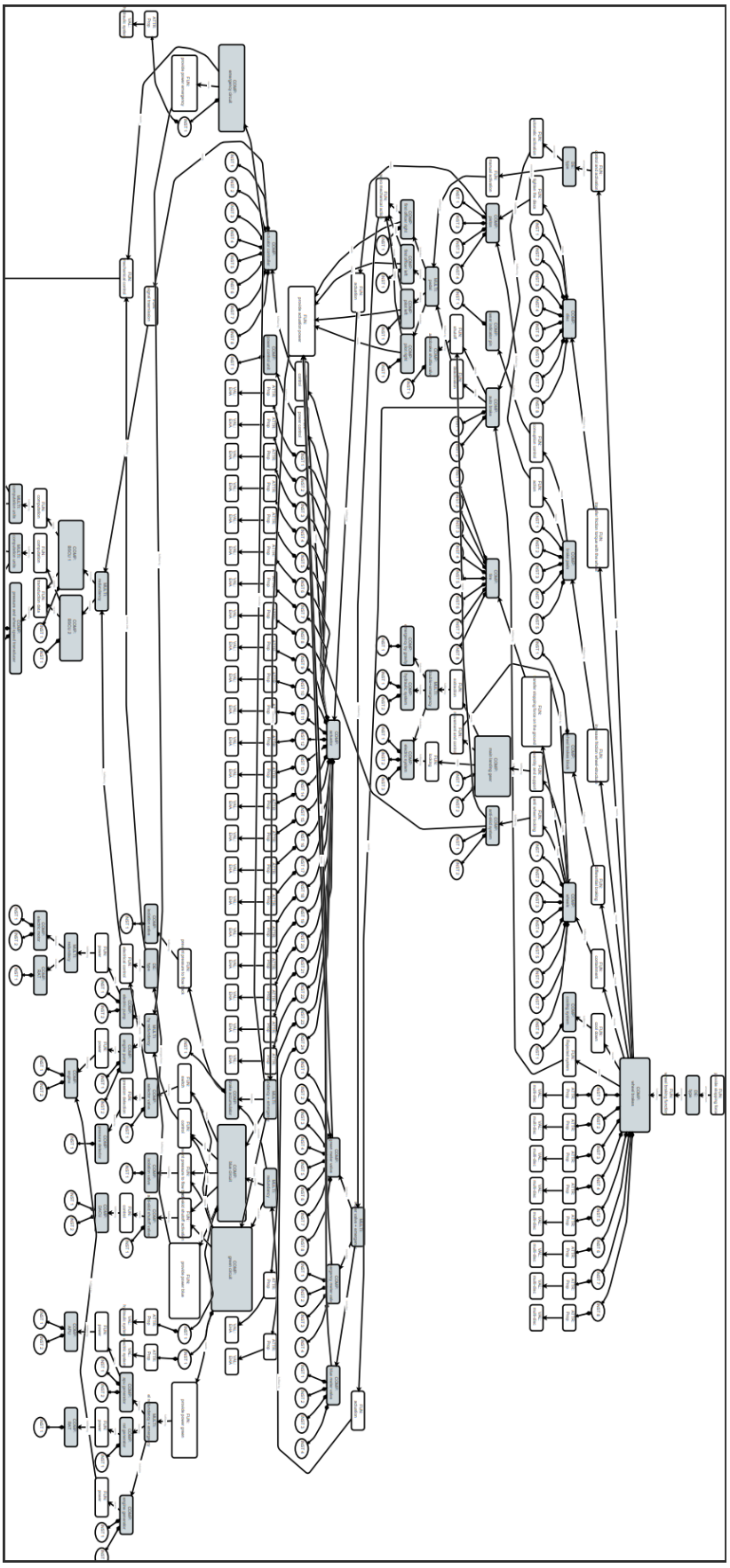
FIGURA 58

I punti importanti di questa architettura di sistema sono i seguenti. (figura 58)

- Questa seconda architettura dei comandi di volo spoiler è più scarna della precedente per un motivo molto semplice, mancano dei componenti che possano permettere la certificabilità dell'architettura.
- Fino agli attuatori, l'architettura è corretta e certificabile, ma è il dopo che è un problema. I sistemi di distribuzione dell'energia non sono ridondati, e nemmeno ce ne sono 2 o più indipendenti. Infatti, è presente un solo sistema elettrico, la cui rottura può portare ad un evento catastrofico. Quindi i vincoli dei capitoli 25.1307, 25.1309 non sono rispettati.
- A sua volta il sistema elettrico non possiede un backup energetico; infatti, l'unica fonte di energia sono i motori, non possiede niente che possa aiutare nel caso di malfunzionamenti dei motori. Quindi anche i vincoli di backup, tra cui il 25.671 e 25.1353 non sono rispettati.
- Ci sono alcuni attuatori di tipo idraulico, ma non è presente nessun tipo di sistema idraulico e quindi i vincoli di design non sono rispettati.

In conclusione, questa architettura non è certificabile perché non rispetta i vincoli qualitativi individuati nelle normative vigenti.

- ARCHITETTURA DEGLI INVERSORI DI SPINTA



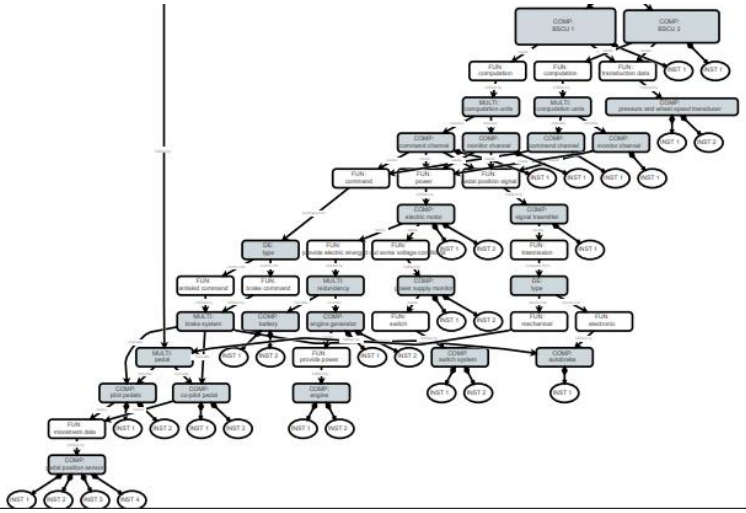
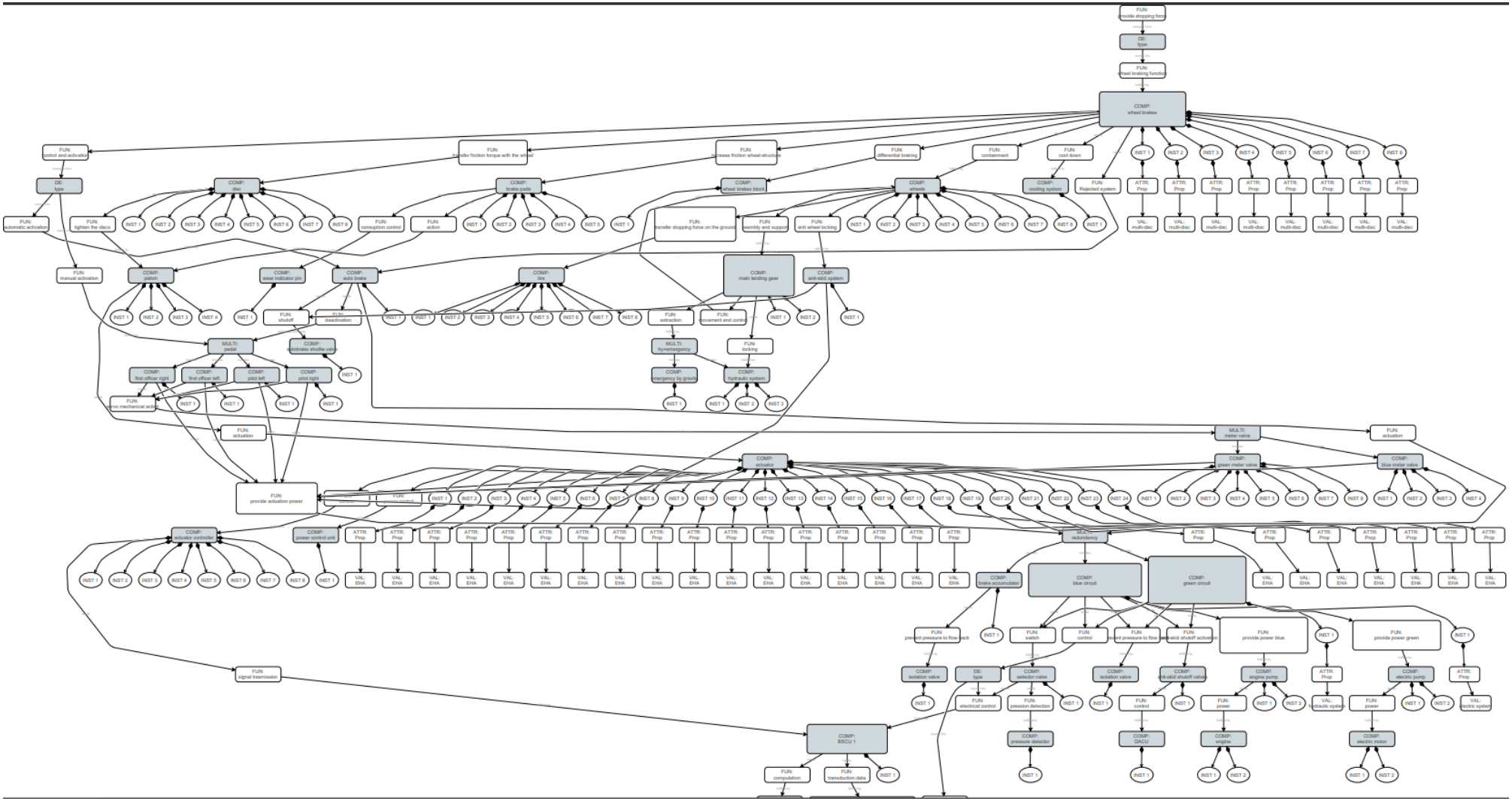


FIGURA 59-60

I punti importanti di questa architettura di sistema sono i seguenti. Questa architettura rappresenta l'impianto dei freni del carrello principale. L'architettura è abbastanza complessa per via del grande numero di componenti sia per il funzionamento dei freni sia per quanto riguarda il controllo. Il check certificativo mostra i seguenti punti. (figure 59-60)

- L'architettura creata non mostra nessun tipo di componente che possa causare, con una single failure, un evento catastrofico. Ogni componente principale, ogni sistema ha una ridondanza, mentre i componenti che sono singoli non sono fondamentali e il sistema funzionerebbe lo stesso se si guastassero. Quindi il vincolo 25.1309 sulla single failure è rispettato.
- Per quanto riguarda i sistemi di distribuzione di potenza si vede come i sistemi sono ridondati, è presente un sistema principale e un sistema secondario, ognuno con un diverso sistema. Il vincolo 25.735 è rispettato.
- Poi è presente anche un sistema di emergenza, visto che l'architettura presente rappresenta un quadrimotore. Quindi il vincolo 25.1307 è rispettato.
- Per quanto riguarda i backup energetici, si vede come ogni sistema di distribuzione, oppure i sistemi del carrello principale, possiede delle sorgenti di potenza alternativi rispetto ai motori, tra cui APU, e RAT e batterie. Il vincolo 25.671 è rispettato.
- Poi, per quanto riguarda il sistema dell'estrazione del carrello principale, è presente un sistema di emergenza per gravità.
- Il sistema dell'anti-skid è presente ridondato e quindi una sua rottura non implica un malfunzionamento del sistema principale dei freni.
- Per quanto riguarda il sistema elettrico e automatico di controllo dei freni è ben ridondato. Il sistema BSCU è presente in doppio elemento, ognuno dei quali indipendente e anche i suoi componenti, i channel e monitor, sono in doppio e diversi per ogni BSCU. Questo particolare vincolo è stato trovato nello standard SAE ARP 4761 e SAE AIR 6110. Per arrivare ad un livello di sicurezza del sistema in modo sufficiente devono essere presente due BSCU indipendenti, e forse anche di più per sistemi più complessi, ma già due sono sufficienti.

Visti tutti questi vincoli rispettati allora è possibile dire che questa architettura è certificabile perché ha rispettato tutti i vincoli qualitativi individuati.


FUN: provide stopping force
DE: type
FUN: wheel braking function
COMP: wheel brakes
FUN: control and activation
FUN: transfer friction torque with the wheel
FUN: increase friction wheel-structure
FUN: differential braking
FUN: containment
FUN: cool down
FUN: Rejected system
DE: type
COMP: disc
COMP: brake pads
COMP: wheel brakes block
COMP: actuator
COMP: cooling system
FUN: automatic activation
FUN: tighten the discs
FUN: corruption control
FUN: action
FUN: transfer stopping force on the ground
FUN: assembly and support
FUN: anti wheel locking
FUN: manual activation
COMP: piston
COMP: wear indicator pin
COMP: auto brake
COMP: tire
COMP: main landing gear
COMP: anti-skid system
FUN: shutoff
FUN: auto deactivation
FUN: extraction
FUN: movement and control
MULTI: pedal
COMP: hydrobrake shuttle valve
MULTI: hyr+emergency
FUN: locking
COMP: first officer right
COMP: first officer left
COMP: pilot left
COMP: pilot right
COMP: emergency by gravity
COMP: hydraulic system
FUN: electro mechanical actuation
FUN: actuation
MULTI: meter valve
COMP: green meter valve
COMP: blue meter valve
FUN: provide actuation power
COMP: actuator
COMP: hydraulic control
COMP: power control unit
MULTI: redundancy
COMP: brake accumulator
COMP: blue circuit
COMP: green circuit
FUN: prevent pressure to flow back
FUN: switch
FUN: control
FUN: prevent pressure to flow back
FUN: anti-skid shutoff activation
FUN: provide power blue
FUN: provide power green
FUN: signal transmission
COMP: isolation valve
DE: type
COMP: selector valve
COMP: isolation valve
COMP: anti-skid shutoff valve
COMP: engine pump
COMP: electric pump
FUN: electrical control
FUN: pression detection
FUN: control
FUN: power
FUN: power
COMP: BSCU 1
COMP: pressure detector
COMP: DACU
COMP: engine
COMP: electric motor
FUN: computation
FUN: transduction data

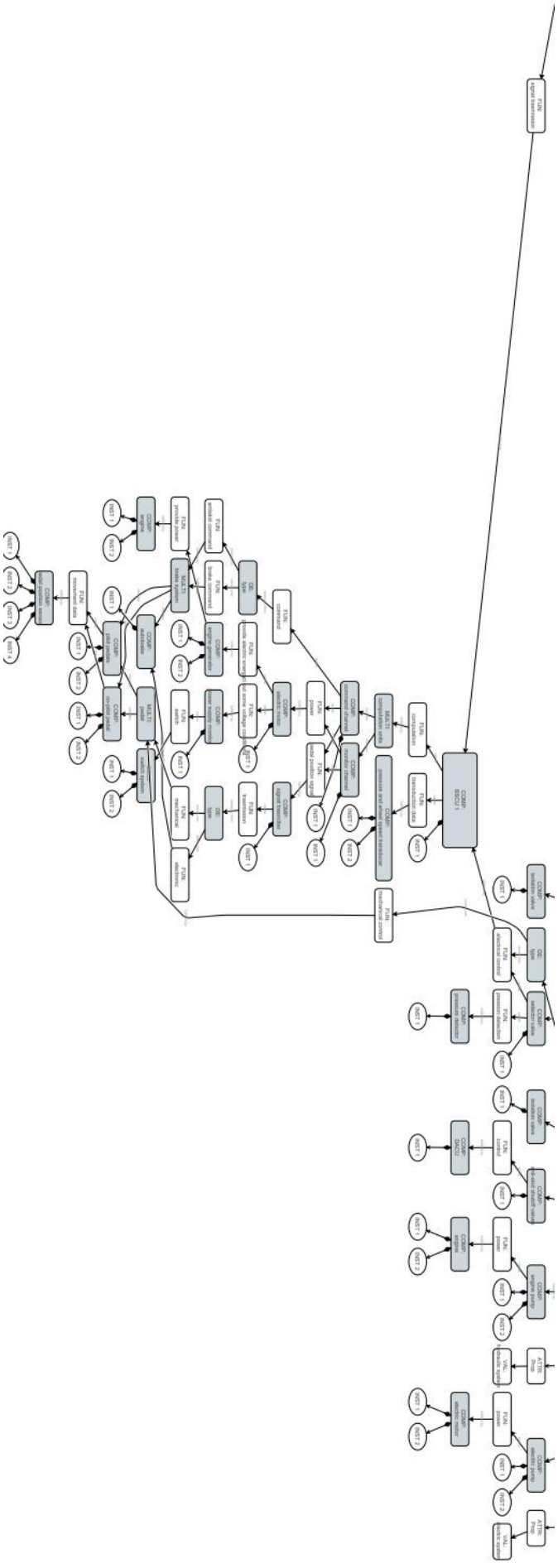


FIGURA 61-62

Questa seconda architettura dell'impianto dei freni presenta alcune criticità dei vincoli qualitativi. (figure 61-62)

- Questa architettura rappresenta un quadrimotore con due sistemi di distribuzione di potenza, uno principale e uno alternativo. Non presenta, come il precedente, un sistema di emergenza. Questo non è essenziale, quindi questa caratteristica non preclude la correttezza dell'architettura e la sua certificabilità. Quindi il vincolo 25.735 è rispettato.
- Ci sono alcuni componenti che non possiedono ridondanza, ma nel complesso non ci sono problemi per quanto riguarda single failure di eventi catastrofici. Quindi il vincolo 25.1309 è rispettato.
- I problemi di non certificabilità riguardano due aspetti fondamentali, due vincoli importantissimi. Il vincolo del backup energetico 25.671 e amc 25.671. I sistemi green e blue non possiedono nessun tipo di backup di sorgente di potenza. In questa architettura la sorgente di potenza è solamente quello del motore, che potrebbe andrebbe bene per aerei di piccole dimensioni, ma assolutamente non per aerei di grandi dimensioni. Il vincolo 26.671 non è rispettato.
- La seconda criticità riguarda il sistema di controllo elettronico, il BSCU. Secondo il vincolo SAE ARP 4761, per raggiungere i requisiti di sicurezza del sistema di controllo frenante, bisogna avere almeno due unità BSCU indipendenti, in cui ognuno due canali separati per la trasmissione e il monitoraggio. In questa architettura è stato inserito un solo BSCU e quindi il requisito SAE 4761 non è rispettato. (figura 63) [6] [19]

Nonostante alcuni vincoli rispettati, il fatto di non avere rispettato questi due vincoli qualitativi e quantitativi, porta a ritenere questa architettura non certificabile. Queste architetture hanno mostrato come sia possibile osservare e legare i vincoli normativi alla creazione delle architetture dei sistemi di bordo. Forse alcune delle architetture non certificabili scartate possono essere anche performanti, ma si vede che non rispettano i vincoli minimi di legge vigenti.

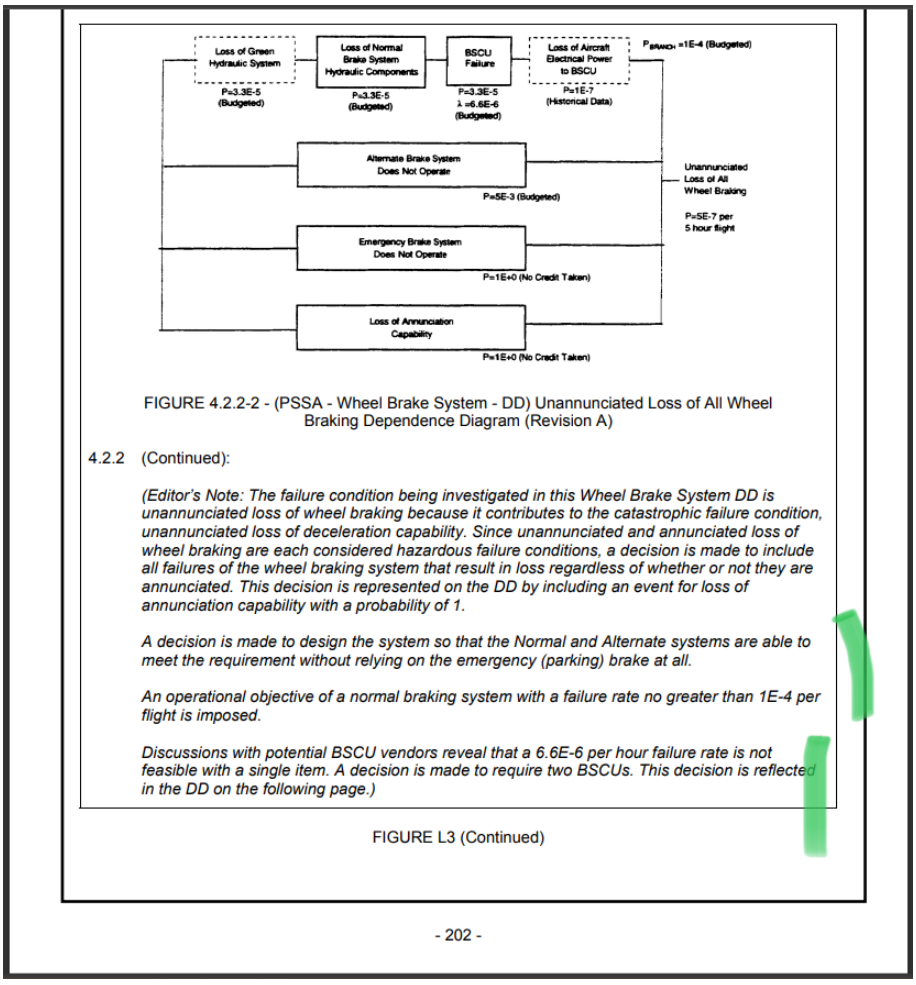


FIGURE 4.2.2-2 - (PSSA - Wheel Brake System - DD) Unannunciated Loss of All Wheel Braking Dependence Diagram (Revision A)

4.2.2 (Continued):

(Editor's Note: The failure condition being investigated in this Wheel Brake System DD is unannunciated loss of wheel braking because it contributes to the catastrophic failure condition, unannunciated loss of deceleration capability. Since unannunciated and annunciated loss of wheel braking are each considered hazardous failure conditions, a decision is made to include all failures of the wheel braking system that result in loss regardless of whether or not they are annunciated. This decision is represented on the DD by including an event for loss of annunciation capability with a probability of 1.

A decision is made to design the system so that the Normal and Alternate systems are able to meet the requirement without relying on the emergency (parking) brake at all.

An operational objective of a normal braking system with a failure rate no greater than 1E-4 per flight is imposed.

Discussions with potential BSCU vendors reveal that a 6.6E-6 per hour failure rate is not feasible with a single item. A decision is made to require two BSCUs. This decision is reflected in the DD on the following page.)

FIGURE L3 (Continued)

- 202 -

FIGURA 63

7. Conclusioni e Lavori futuri

Con questo si è alle conclusioni di questo lavoro di Tesi. Si è visto e dimostrato che è possibile unire la fase di progettazione delle architetture dei sistemi di bordo con la certificazione e i vincoli, in modo da ottimizzare e semplificare il processo di progettazione e risparmiare anche alcune centinaia di migliaia di euro o dollari. Per concludere vanno dette ancora alcune cose. L'enorme quantità di soluzioni possibili durante la progettazione delle architetture dei sistemi di bordo comporta la necessità di automazione e ottimizzazione per esplorare in maniera adeguata l'intero design space, bisogna avere strumenti in modo da visionare tutte le possibili soluzioni. Bisogna avere dei modelli e sistemi automatizzati per la progettazione delle architetture dei sistemi di bordo, anche e soprattutto servendosi dell'intelligenza artificiale, perché non è possibile valutare l'enorme numero di possibili connessioni tra i sistemi senza l'automazione. Come si è visto, includere gli aspetti di certificazione nelle prime fasi di progettazione consente di scartare alcune architetture se non sono conformi alle specifiche di certificazione. Gli aspetti di certificazione sono fondamentali per garantire che le architetture generate automaticamente siano fattibili e non fattibili, nel loro aspetto minimo. Possono magari essere performanti o avere caratteristiche particolari, ma se non rispettano le normative allora non possono essere certificate. Però bisogna anche che le normative corrano al passo con i tempi e con le nuove tecnologie. È importante quando si valutano tecnologie innovative che potrebbero richiedere un'enorme esplorazione delle architetture al fine di trovare nuove soluzioni più ottimali, cercare di vedere, insieme alle performance anche la sicurezza. Forse in futuro alcuni tipi di ridondanze non saranno più necessarie, e allora la normativa dovrà alleggerire alcuni elementi, oppure appesantire se dovessero esserci problemi. Questo vale per i sistemi di qualunque aspetto industriale, che siano aerei, navi di nuova tecnologia, macchinari industriali, auto e droni, soprattutto il mondo nuovo e sterminato dei droni. Pertanto, la certificazione guida il processo di progettazione e può essere utile e utilizzata come filtro. Per la certificazione si sono usati tre normative o, meglio, una normativa e due standard, cioè la CS-25 e le SAE ARP 4754 e 4761. Con la CS-25 si è visto anche alcuni vincoli della FAR 25 e della AC, le quali sono americane e sono uguali a quelle europee, anzi va detto che è il contrario, le CS sono uguali a quelle americane. L'Europa è da sempre, dalla Seconda Guerra Mondiale parte dell'impero americano. questi vincoli e normative spiegano quali condizioni minime devono essere applicate alle architetture dei sistemi di bordo degli aeromobili. È importante dire 'minime' perché ogni sistema può avere elementi diversi per vari tipi di missione, ma deve avere degli elementi minimi di sicurezza, e i minimi requisiti, poi si sceglieranno i requisiti di missione e del cliente, ma prima bisogna soddisfare i requisiti di safety e i derivati. Nei capitoli precedenti si è mostrato questa cosa. Questa tesi ha mostrato che non importa che tipo di architettura ci sia e si usi, deve avere degli elementi minimi voluti dalla normativa. Tutto questo serve come certificazione preliminare delle diverse architetture realizzabili per il sistema di interesse. La metodologia è completamente automatizzata. Varie architetture vengono generate automaticamente dal design space e filtrate automaticamente dalle regole delle specifiche di certificazione, quelle con vincoli non riusciti vengono scartate, anche se possono essere performanti, devono avere i minimi requisiti di normativa. I requisiti invidiati sono i seguenti. L'affidabilità minima di un sistema stabilita dalla normativa. L'esistenza di sistemi di riserva in caso di perdita di tutti i motori. Un numero minimo di ridondanze affinché il singolo guasto di un componente non comprometta il funzionamento sicuro di un intero sistema. Due o più sistemi di distribuzione di potenza. E ce ne sono altri più specifici, ad esempio sul sistema frenante o di altro tipo come le comunicazioni o l'avionica. Per il requisito dell'affidabilità di utilizza la tecnica del diagramma a blocchi dell'affidabilità che viene utilizzata e automatizzata per stimare l'affidabilità. Diverse architetture (vale a dire migliaia) vengono generate automaticamente dal design space costruito e filtrate automaticamente dalle regole delle specifiche di certificazione. Le restanti architetture sono preliminarmente certificate. Questo può essere fatto dall'intelligenza artificiale, come è stato descritto nei capitoli precedenti. Poi è l'uomo che sceglie quali architetture preferisce per le varie missioni. Quindi questo lavoro vuole mostrare come l'intelligenza artificiale e l'uomo lavorano insieme. L'AI si occupa di ottimizzare velocizzare la scelta delle architetture certificabili, e non farle a mano, mentre è l'uomo che sceglie, con la sua esperienza e fantasia, quali delle architetture certificabili siano meglio per quella determinata missione. Un altro aspetto molto importante e utilissimo sviluppato da questo processo è la creazione di un'architettura da cui sia possibile tracciare gli eventi causa-effetto dei componenti e delle loro funzioni. Infatti, con questi schemi di architettura EASA e le aziende produttrici potranno individuare meglio l'elemento guasto ed andare a operare in maniera mirata e chirurgica per sistema il problema, questo perché con questa grafica di

architettura è facile visionare l'insieme del sistema, partendo dall'azione fino al funzionamento passando per tutti gli aspetti di distribuzione. Queste sono le conclusioni di questo lavoro di Tesi, ma, come ogni lavoro che si rispetti, tutto è in evoluzione e ci sono le basi per dire alcune cose su dei possibili lavori futuri. Tutto questo ha dimostrato solo l'inizio, cioè la possibilità di unire i due lati della V-model, cioè, permettere una verifica di requisiti minimi di legge e di normativa durante la fase della progettazione e permettere un miglioramento e un'ottimizzazione delle fasi di progetto aiutando anche le aziende a risparmiare qualche migliaio di dollari e destinare i soldi risparmiati in progetti nuovi e migliorie. Tutto questo lavoro non serve puramente alla ricerca, ma serve assolutamente alla pratica e alle aziende, alle industrie che producono gli aerei o, meglio, i velivoli, o ancora meglio oggetti industriali. Questa parola è specifica sulla portata di questa ricerca. Infatti, questo metodo di ottimizzazione potrebbe e potrà essere usato anche in ambiti al di fuori di quello strettamente aeronautico, abbracciano le branche delle automotive, dello spazio, delle industrie in generale. Infatti, come è stato già detto nei primi capitoli, ogni azienda industriale che voglia fare in modo che il suo prototipo possa entrare in catena di produzione e quindi generare profitto deve farlo prima certificare. Lo si vede in ogni prodotto con le scritte CE, comunità europea, o di altro tipo, cioè che quel prodotto è stato certificato ed è sicuro. Detto questo quindi si vede benissimo come un'ottimizzazione del processo di certificazione farebbe gola, gioverebbe ad ogni azienda del pianeta. Inoltre, una piccola curiosità, gli aspetti della sicurezza e della certificazione in ambito industriale sono tanti e sviluppati proprio a partire dal campo aeronautico. È stata proprio la capacità di portare l'uomo nel cielo, più vicino a Dio, che ha portato a migliore e ad avere attenzione negli aspetti di sicurezza e di certificazione. Prima, con la rivoluzione industriale non si era valutato molto l'aspetto di sicurezza e regolamentazione, c'era solo la voglia di produrre, anche in condizioni davvero precarie e fare prodotti non sempre sicuri. Quindi capire, ottimizzare, e studiare la certificazione e la regolamentazione aeronautica è fondamentale per capire anche tutti gli aspetti dell'industria in generale. La certificazione, ricordiamolo sempre, è un aspetto di vitale importanza, che mescola sicurezza, tecnica e politica e geopolitica. Tornando ai lavori futuri su questo aspetti di ottimizzazione del processo di certificazione, in futuro, il metodo dovrebbe essere applicato a una più ampia varietà di problemi di architettura di sistema, per convalidare il suo potenziale come metodo di architettura di sistema generalmente applicabile. Quindi non solo negli aspetti prettamente dei sistemi di bordo, ma ampliarlo ad una platea di sistema più in generale. Gli esempi includono la progettazione del sistema di propulsione ibrido-elettrico, la catena di approvvigionamento di produzione e gli scenari di sistemi di sistemi dovrebbe essere sostenuto. Quindi aspetti di logistica, fondamentale nella produzione e nei prodotti industriali, civili e soprattutto militari, e anche negli aspetti di manutenzione. Un'area di interesse è la codifica delle decisioni di permutazione in variabili di progetto. La sfida sta nel mantenere piccolo il design space apparente utilizzando solo semplici variabili di progettazione intere per consentire l'uso di tecniche di modellazione che acceleri l'ottimizzazione. Inoltre, dovrebbe essere fondamentale collegare il metodo di architettura di sistema presentato al processo di ingegneria dei sistemi. È fondamentale capire quale sarebbe il miglior linguaggio di modellizzazione, dato che l'ADSG non è direttamente compatibile con nessun linguaggio esistente, come SysML. Bisogna crearne uno nuovo, ad hoc, oppure collegare a linguaggi esistenti. Un'integrazione pratica con il processo di ingegneria dei sistemi richiede anche la disponibilità di un'interfaccia utente grafica intuitiva per la creazione, l'ispezione e la modifica dell'ADSG, nonché la generazione e l'esecuzione di esplorazioni dello spazio di progettazione. Ulteriore lavoro potrebbe includere altri ambiti dopo la certificazione, come le prestazioni o la manutenzione. Ciò creerebbe anche nuovi obiettivi di ottimizzazione trasformando il quadro in un'ottimizzazione multi-obiettivo. Tutto questo, con l'aggiunta dell'intelligenza artificiale e l'esperienza dell'uomo, potrà portare alla semplificazione, senza togliere gli aspetti fondamentali e critici della safety, dei velivoli in ambito aeronautico, delle navi in ambito navale e sistemistico, delle auto in ambito automotive e degli impianti in ambito industriale in generale. Perché l'aspetto della certificazione e della safety sono critici in tutti gli aspetti industriali e dopo la prima e la seconda e terza rivoluzione industriale tutto il mondo è industriale. Tutti i paesi sviluppati e in via di sviluppo sono industriali e producono, chi più chi meno, oggetti industriali, la cosiddetta manifattura. E i prodotti industriali devono sempre essere certificati per permetterne la produzione in serie e il successivo guadagno dell'azienda suo vero obiettivo. La prima rivoluzione industriale iniziò con la creazione della macchina a vapore. La seconda rivoluzione iniziò l'introduzione dell'elettricità, dei prodotti chimici e del petrolio. La terza rivoluzione inizia con lo sviluppo massiccio dell'elettronica, delle telecomunicazioni e dell'informatica nell'industria. Il mondo aeronautico, industriale, navale, automotive, tutti industriali, saranno sempre connessi attraverso tanti elementi, uno di questo e più importante, è la certificazione.

RIFERIMENTI

[1] Certification Specifications (CSs) | EASA (europa.eu)
[2] Acceptable Means of Compliance (AMC) and Guidance Material (GM) | EASA (europa.eu)
[3] CS-27 Amdt. 1.pdf
[4] Aeroelastic 2020-12-03 - 2.pdf
[5] ARP4754A: Guidelines for Development of Civil Aircraft and Systems - SAE International
[6] ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment - SAE International
[7] B: The V-Model - Model-Based System Architecture - Wiley Online Library
[8] IEEE (June 2011). IEEE Guide--Adoption of the Project Management Institute (PMI) Standard A Guide to the Project Management Body of Knowledge (PMBOK Guide) --Fourth Edition. IEEE P1490/D1, May 2011. p. 452. doi:10.1109/IEEESTD.2011.6086685. ISBN 978-0-7381-6817-3. Retrieved May 25, 2021.
[9] Acceptable Means of Compliance (AMC) and Alternative Means of Compliance (AltMoC) | EASA (europa.eu)
[10] COMMENT RESPONSE DOCUMENT, Proposed equivalent safety finding to CS-25.671 c(2): Control System
[11] *"System Architecture Design Space Exploration: An Approach to Modeling and Optimization",* J.H. Bussemaker, P.D. Ciampa, B. Nagel, DLR (German Aerospace Center), Institute of System Architectures in Aeronautics, Hamburg, Germany.
[12] "*Tutorial: Architecture Design Space Modeling using ADORE*", MBSE Development System, ADORE, AGILE 4.0
[13] "*ADORE Quick Reference Manual*", Boggero Luca, Bussemaker Jasper, DLR – German Aerospace Center Institute of System Architectures in Aeronautics, Hamburg, Germany
[14] "*Strategy and Product Development for Complex Systems, System Architecture*", Crawley Edward, Cameron Bruce, Selva Daniel, Foreword by Norman R. Augustine, Global edition, Pearson Education Limited 2016, Edinburgh Gate, Harlow, Essex CM20 2JE, England
[15] Certification Specifications and Acceptable Means of Compliance for Engines (CS-E), Annex VII to ED Decision 2020/006/R, Amendment 6, 24 June 2020
[16] Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25), Amendment 27, 24 November 2021
[17] Certification Specifications for Normal Category Aeroplanes (CS-23) and Acceptable Means of Compliance and Guidance Material to the Certification Specifications for Normal-Category Aeroplanes (AMC & GM to CS-23), CS-23 Amendment 6 / AMC & GM to CS-23 Issue 4, 27 February 2023
[18] Easy Access Rules for Normal, Utility, Aerobatic and Commuter Category Aeroplanes (CS-23) (Amendment 4), Published June 2018
[19] "*Formal Design and Safety Analysis of AIR6110 Wheel Brake System*", M. Bozzano, A. Cimatti, A. Fernandes, Pires, D. Jones, G. Kimberly, T. Petri, R. Robinson, S. Tonetta; 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015
[20] *"Design for System Safety Analysis of the Aircraft Braking System Having Normal and Emergency Wheel Braking*", Rolwyn Marian Cardoza, Dr. M. Krishna; International Journal of Engineering Research & Technology (IJERT), Published by: www.ijert.org; Vol. 9 Issue 06, June-2020
[21] "ACTIVE AND LATENT FAILURES IN AIRCRAFT GROUND DAMAGE INCIDENTS", C. Wenner, C. G. Drury, State University of New York at Buffalo, Department of Industrial Engineering, Buffalo, NY 14260
[22] "Automated generation of aircraft on-board system architectures and filtering through certification specification requirements", Cabaleiro Carlos, Fioriti Marco, Boggero Luca
[23] "Methodology for the automated preliminary certification of on-board systems architectures through requirements analysis", Cabaleiro Carlos, Fioriti Marco, Boggero Luca, 33rd congress of the internationsl council of the aeronautical sciences, ICAS 2022 Sweden

APPENDICE A

Viene mostrata la lista completa delle diverse tipologie di normative introdotte da EASA. Questa suddivisione è presa direttamente dal sito ufficiale di EASA, aggiornato al 2023:

- Certification Specifications (CSs)
- "Additional Airworthiness Specifications

CS-26 Additional airworthiness specifications for operations
ADR - Aerodromes
CS-ADR-DSN Aerodromes Design
CS-HPT-DSN Heliports Design

- Air Operations

CS-FSTD(A) Aeroplane Flight Simulation Training Devices
CS-FSTD(H) Helicopter Flight Simulation Training Devices
CS-FTL.1 Commercial Air Transport by Aeroplane - Scheduled and Charter Operations

- Aircrew

CS-FSTD(A) Aeroplane Flight Simulation Training Devices
CS-FSTD(H) Helicopter Flight Simulation Training Devices

- ATM/ANS interoperability - Air Traffic Management/Air Navigation Services

CS-ACNS Airborne Communications, Navigation and Surveillance

- Initial Airworthiness

AMC-20 General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances
CS-22 Sailplanes and Powered Sailplanes
CS-23 Normal, Utility, Aerobatic and Commuter Aeroplanes
CS-25 Large Aeroplanes
CS-26 Additional airworthiness specifications for operations
CS-27 Small Rotorcraft
CS-29 Large Rotorcraft
CS-31GB Gas Balloons
CS-31HB Hot Air Balloons
CS-31TGB Tethered Gas Balloons
CS-34 Aircraft Engine Emissions and Fuel Venting
CS-36 Aircraft Noise
CS-APU Auxiliary Power Units
CS-AWO All Weather Operations
CS-CCD Cabin Crew Data
CS-CO2 Certification Specifications, Acceptable Means of Compliance and Guidance Material for Aeroplane CO2 Emissions (CS-CO2)
CS-Definitions on Definitions and Abbreviations
CS-E Engines
CS-ETSO European Technical Standard Orders
CS-FCD Flight Crew Data
CS-GEN-MMEL Generic Master Minimum Equipment List
CS-LSA Light Sport Aeroplanes
CS-MCSD Certification Specifications for Maintenance Certifying Staff Data
CS-MMEL Master Minimum Equipment List
CS-P Propellers
CS-SIMD Simulator Data
CS-STAN Standard Changes and Standard Repairs
CS-VLA Very Light Aeroplanes
CS-VLR Very Light Rotorcraft"

È riportato integralmente l'elenco della suddivisione delle varie AMC e GM, preso dal sito ufficiale di EASA, aggiornato al 2023:

- "Acceptable Means of Compliance (AMC) and Guidance Material (GM)

- ADR - Aerodromes

ADR - Aerodromes
Remote tower operations

- Air Operations

DEF - Definitions
GM to the Cover Regulation
Part-ARO - Authority Requirements for Air Operations
Part-CAT - Commercial Air Transport Operations
Part-NCC - Non-commercial operations with complex-motor-powered aircraft
Part-NCO - Non-commercial operations with other than complex-motor-powered aircraft
Part-ORO - Organisation Requirements for Air Operations
Part-SPA - Operations requiring Specific Approvals
Part-SPO - Specialised Operations

- Aircrew

AMC & GM to Regulation (EU) No 1178/2011
Part-ARA - Authority Requirements for Aircrew
Part-CC - Cabin Crew
Part-DTO - Declared Training Organisation
Part-FCL - Flight Crew Licensing
Part-MED - Medical Requirements for Aircrew
Part-ORA - Organisation Requirements for Aircrew

- ATCO - Air Traffic Controllers

AMC/GM to the Cover Regulation (EU) 2015/340
Part ATCO - Air Traffic Controllers
Part ATCO.AR
Part ATCO.OR
Part-ATCO.MED

- ATM/ANS interoperability - Air Traffic Management/Air Navigation Services

AMC & GM to Commission Implementing Regulation (EU) No 1207/2011

- ATM/ANS provision of services - Air Traffic Management/Air Navigation Services

AMC/GM to Regulation (EU) 2017/373
Definitions of terms used in Annexes II to XIII to Commission Implementing Regulation (EU) 2017/373
Part-AIS
Part-ASM
Part-ATFM
Part-ATM/ANS.AR
Part-ATM/ANS.OR
Part-ATS
Part-CNS
Part-DAT
Part-FPD
Part-MET
Part-NM
Part-PERS
Remote tower operations

- AUR - Airspace Usage Requirements (ACAS II)

AMC & GM to AUR

- AUR - Airspace Usage Requirements (PBN)

AMC & GM to AUR

- Balloons

AMC and GM to Articles of Commission Regulation (EU) 2018/395
Part-BFCL
Part-BOP

- Continuing Airworthiness

AMC & GM to Regulation (EU) No 1321/2014
Part-145 - Maintenance organisation approvals
Part-147 - Organisations training Part 66 license applicants
Part-66 - Maintenance certifying staff
Part-CAMO
Part-CAO
Part-M - Continuing airworthiness requirements
Part-ML
Part-T - Aircraft registered in a third country

- Initial Airworthiness

Part 21 - Airworthiness and Environmental Certification

- Sailplanes

GM to Article 3 of Commission Implementing Regulation (EU) 2018/1976
Part-SAO
Part-SFCL

- SERA - Standardised European Rules of the Air

Remote tower operations
Rules of the air

- SKPI - Safety Key Performance Indicators

SKPI-Safety Key Performance Indicators

- TCO - Third Country Operators

Part-TCO - Third Country Operators

- UAS - Unmanned Aircraft Systems

AMC & GM to Commission Implementing Regulation (EU) 2019/947
AMC & GM to Part-UAS”

RINGRAZIAMENTI

Il lavoro di Tesi magistrale finisce qui, come sono finiti anche questi 5 anni di università al Politecnico di Torino. È stata un'avventura straordinaria fatta di alti meravigliosi e un po' di scivoloni. In alcune materie so di non aver dato il massimo che potevo dare e aspettarmi, ma sono contento che in questi 5 anni sono riuscito a trovare l'ambiente tecnico che mi piace e mi appassiona. In questi 5 anni ci sono stati anche i 2 anni e mezzo di COVID-19, un qualcosa di assolutamente imprevedibile e che ha causato veramente tanti danni. Nel mio canto devo dire fortunatamente non ho subito quei danni, ma mi è dispiaciuto molto non poter essere fisicamente al Politecnico e incontrare gli amici in quel periodo. In questi anni ho conosciuto professori e persone di ogni tipo e provenienti da molte parti del globo. Queste conoscenze mi hanno mostrato una cultura e un modo di pensare che io avevo visto solo tramite uno schermo e delle serie tv, drama e film, e adesso li ho potuti vedere dal vivo e per questo li ringrazio. Che anni incredibili. Il mondo che mi aspetta al di fuori di quella porta sarà veramente incredibile e devo dive anche terribile per via di tutto quello che sta succedendo dal punto di vista umano e polito e militare. Ma questo comunque non deve spaventarmi, ma spronarmi ad essere forte e coraggioso. Ce la farò!

Questo lavoro di Tesi è iniziato un po' di mesi fa ed è stato un bellissimo lavoro che ho svolto con la massima passione. So di aver commesso alcuni errori, anche nella scrittura della Tesi, ma questi errori spero mi facciano capire e migliorare. Spero comunque che i risultati siano abbastanza corretti e soprattutto utili per il futuro. Per tutto questo lavoro devo ringraziare i miei due professori che mi hanno seguito e hanno avuto una pazienza non da poco a sopportarmi.
Ringrazio enormemente il Professor Marco Fioriti per avermi accettato come suo tesista e di avermi seguito e consigliato e corretto durante il lavoro della Tesi, e aver auto tanta pazienza con me. Grazie mille!
Ringrazio enormemente il Professor Paolo Maggiore per avermi seguito, avermi dato tanti consigli e avermi corretto quando serviva, e aver avuto tanta pazienza con me. Grazie mille!
Ringrazio il professor Carlos Cabaleiro de la Hoz, che dal DLR in Germania, mi ha aiutato nell'uso dei software e mi ha dato tanti consigli per fare un bel lavoro. Grazie mille!
Ringrazio Jasper Bussemaker del DLR in Germania, per avermi aiutato a risolvere alcuni problemi con il software che mi avevano bloccato. Grazie mille!
Ringrazio tutto il Politecnico di Torino e il DLR in Germania. Grazie mille!

Ringrazio tutti i miei amici che mi sono stati vicini in questi anni, e ci siamo divertii molto a fare tante cose, a parlare e tanto altro, ed è meglio che non dica tutto. Queste cose rimarranno nel mio cuore.

I Più grandi Ringraziamenti vanno a quattro persone.

I miei genitori, Edmond e Marjeta, che mi hanno cresciuto, amato e educato nel migliore dei modi. Mi hanno dato molto cibo squisito. Li ringrazio di tutto quello che mi hanno dato e li ringrazio di aver sopportato tutti i miei capricci, sono stati tanti. Ma li ringrazio di tutte le risate e dei momenti bellissimi che abbiamo vissuto, dei viaggi in giro per l'Europa e in nord africa. Belli belli belli! Grazie di tutte le avventure che abbiamo fatto con la mamma e le avventure fatte con il babbo. Molte andate bene, altre un po' meno. Grazie veramente di Tutto! Mi assicurerò di diventare un adulto responsabile e maturo per ripagarvi di tutto quello che mi avete dato. Grazie infinte!

Ringrazio i miei zii adottivi, Graziella e Renzo. Mi hanno cresciuto fin da infante, mi hanno amato e mi hanno dato da mangiare delle cose meravigliose, divine. Con Loro abbiamo vissuto momenti magnifici ed indimenticabili. Grazie di tutte le risate, i racconti e di tanto altro e tutto. Grazie di tutto le avventure fatte insieme. Grazie infinte dell'amore che mi avete dato.
Purtroppo, Graziella non c'è più ed è un dolore enorme non vederla e che non sia presente in questi momenti così incredibile della mia vita. spero che da lassù, dal Paradiso, dove merita di stare insieme a tutti gli angeli per tutto il bene che ha fatto, mi stia guardando e sia tanto orgogliosa di me. Ti voglio un mondo di bene.
Grazie veramente di tutto!

FIXHERALD SHAHINI