

ISCA - 1

Introduzione

Leonardo Daga
(leonardodaga@libero.it)
Lezioni del corso di
Ingegneria dei Sistemi di Controllo Aeronautici
Università di Bologna

Introduzione

Argomenti Trattati nel corso

- I Requisiti nei sistemi avionici
- I Bus Aeronautici
- Ingegneria dei Sistemi di Controllo
- Le Architetture Hardware
- Le Architetture Software
- I metodi di progetto del Software

Argomenti Opzionali

- La progettazione di Software Fault Tolerant
- I Sistemi Operativi Real Time

Figure Professionali interessate

- Ingegneri del software per l'avionica
- Ingegneri dei sistemi per l'avionica
- Specialisti nella progettazione di sistemi di controllo Real-Time ad alta affidabilità
- Ingegneri dei Sistemi per la realizzazione di equipaggiamenti di test

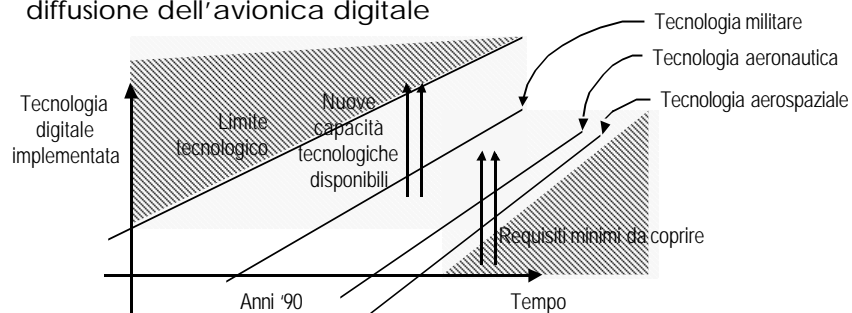
Contesti

- Avionica di bordo per l'aeronautica civile
- Avionica di bordo per l'aeronautica militare
- Avionica di bordo per la progettazione di sistemi aeronautici di terra (Sistemi di controllo del volo)
- Sistemi Navali
- Sistemi di bordo per mezzi terrestri
- Sistemi di bordo per Satelliti
- Equipaggiamento di test per sistemi aerospaziali

Storia

- Solo dagli anni 90 in poi l'avionica digitale si è affermata come disciplina fondamentale nell'aeronautica

- Le nuove capacità tecnologiche disponibili hanno fatto da traino alla diffusione dell'avionica digitale
- I requisiti da coprire hanno spinto sempre di più alla diffusione dell'avionica digitale



Storia

- Essendo una nuova disciplina, l'avionica digitale si è diffusa insieme a:
 - Metodi di progetto
 - Requisiti
 - Specifiche di progetto
 - Metodi di Test
- Molte difficoltà sono dovute ad una non perfetta standardizzazione della terminologia e degli approcci
- Molti enti differenti hanno generato diversi standard, più o meno seguiti:
 - ARINC, NASA, FAA, USAF
 - Enti nazionali europei militari e civili

Fasi di un progetto

- Il progetto di un sistema avionico si compone delle seguenti fasi:
 - Definizione dei requisiti
 - Cosa deve fare l'avionica da progettare
 - Definizione delle specifiche di progetto SW e HW
 - Come verranno soddisfatti i requisiti
 - Stesura del progetto
 - Architettura SW e HW
 - Costruzione dell'HW e stesura del SW
 - Test
 - Definizione di un documento che dettaglia tutti i test da effettuare per verificare il corretto funzionamento di SW e HW

Qualità in un progetto

- La produzione di documenti relativi ad ogni fase del progetto è la conseguenza di requisiti di qualità ai quali nessuna società di progettazione può evitare di rispondere
- I documenti di maggiore livello consentono al settore di management di prendere decisioni sull'andamento del progetto
 - Servono anche per avere maggiore visibilità
- Si ottengono maggiori benefici in termini di costi
 - Il management è costretto a formulare delle scelte chiare dalle quali non può tornare indietro
 - Il progettista ha chiaramente definite le caratteristiche del progetto da realizzare
 - Diminuiscono le contese sulla effettiva realizzazione del progetto

Qualità in un progetto

- La produzione di documenti consente al cliente di avere sul progetto:
 - Manutenibilità (documento di dettaglio)
 - Facilità di uso (manuale d'uso, architettura)
 - Portabilità (documento di architettura, dettaglio)
 - Efficienza (documenti di specifica, architettura)
 - Affidabilità (documenti di specifica, test)
 - Sicurezza (documenti di specifica, test)
 - Compatibilità (Documenti di specifica, architettura)

Qualità di un progetto

- Il raggiungimento della qualità viene ipotizzato in fase di avvio del progetto
 - La qualità in un progetto non può essere realizzata cercando di realizzare un sistema a bassa qualità e poi cercando di migliorarlo
 - Gli sviluppatori del sistema devono avere esperienza, capacità di lavorare in gruppo, conoscenti di ogni metodo, tecnica o tool software che verrà utilizzato nel progetto
 - Il metodo di sviluppo scelto deve essere ben documentato e comprensibile a tutti i membri del team di sviluppo

Qualità di un progetto

– Durante un progetto:

- I capi progetto devono assicurarsi che il progetto sia nei binari definiti dai documenti e che non stia divergendo
- Gli obiettivi e le funzionalità di un singolo task di lavoro devono essere ben compresi da chi lo deve realizzare
- La tecnica scelta per la sua realizzazione deve essere appropriata (scelta, spesso, dal capo progetto)
 - Nel caso ci siano più modi di fare una stessa cosa, deve essere preventivamente scelto quale modo deve essere utilizzato
- Il prodotto finale di un task deve essere verificato e marcato
 - Marcare un task significa attestarne il suo completamento

Definizione dei requisiti

- Ogni sistema avionico funzionante ha come premessa una chiara definizione dei requisiti sulle prestazioni del sistema
 - I requisiti vengono definiti dal cliente
 - Spesso si fa riferimento a sistemi già esistenti
- Non devono essere lasciati troppi margini all'interpretazione da parte del progettista
 - La legge di Murphy è sempre valida
 - I requisiti sono parte integrante dei contratti stipulati tra cliente e progettista

Definizione dei requisiti (aeronautica militare)

- Il cliente definisce una lista dei possibili requisiti
 - La lista viene composta definendo requisiti ad un livello molto alto
 - Tipo: Cosa dovrebbe fare l'aereo (non come dovrebbe essere fatto)
 - Le missioni che l'aereo deve compiere
 - Tipi di aerei con caratteristiche simili
 - Il progettista sceglie la migliore architettura in grado di soddisfare i requisiti

Esempio dei requisiti (aeronautica militare)

- Emessi dall'US Air Force per la definizione di un'architettura avionica per un ipotetico aereo ad alte prestazioni
 - Architettura nota con il nome di "Pave Pillar"
 - Mean time between critical failures (MTBF): 70 h
 - Una failure critica è una fallure che può impedire il completamento di una missione
 - Mean time to repair (critical functions): 1.25 h
 - include troubleshooting: 10 min
 - Fault detection: 99 percent of all possible faults
 - Fault isolation: 98 percent of all possible faults
 - Two-level maintenance
 - Ovvero: la manutenzione è possibile sia direttamente sull'aereo che nel deposito
 - Sortie rate: ≥ 4.5 per day
 - Abort rate: ≤ 1 percent
 - Combat turnaround time: ≤ 15 min

Definizione dei requisiti (aeronautica civile)

- E' normalmente il progettista che definisce le caratteristiche finali del progetto
 - Le caratteristiche vengono definite in base a:
 - richieste del mercato
 - tipo di rotte da coprire
 - numero di passeggeri o di carico utile da trasportare
 - ambiente nel quale deve operare
 - La sicurezza è SEMPRE il requisito a maggiore priorità di ogni progetto aeronautico civile
 - L'economia del progetto è il secondo requisito in termini di importanza

Definizione dei requisiti (settore aerospaziale)

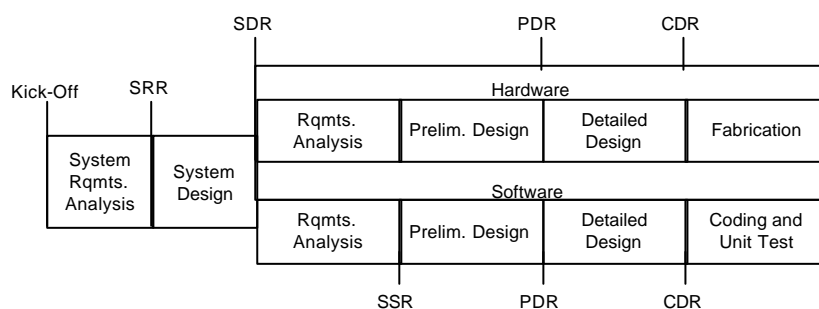
- Il cliente definisce principalmente il carico utile e l'orbita finale
 - Il tipo di carico utile condiziona:
 - tipo di assetto (spinning o controllato su tre assi)
 - precisione dell'assetto
 - L'orbita finale condiziona:
 - La quantità di carburante da caricare a bordo
 - Fattori non secondari sono:
 - l'ingombro totale (per l'allocatione in un dato vettore di lancio)
 - il peso totale (kg = spesa necessaria per mandarlo in orbita)
 - la vita del satellite
 - capacità di recupero o di mantenimento dell'orbita in caso di lancio non perfetto
 - semplicità di recupero del satellite in caso di avaria
 - Il recupero avviene tramite collegamento Terra -bordo

Definizione dei requisiti

- Come è fatto il sistema aeronautico che deve ospitare il l'avionica da progettare
- Quali sono le caratteristiche dei sistemi avionici già presenti
- Missioni che il sistema aeronautico deve compiere
- Requisiti di sicurezza da soddisfare
- Mean Time Between Failure (MTBF) e Maintenance Hours per Flight
 - Se l'apparato da realizzare è composto di molte parti, viene calcolato in funzione delle possibilità di failure di ogni componente

Ciclo di sviluppo di un progetto

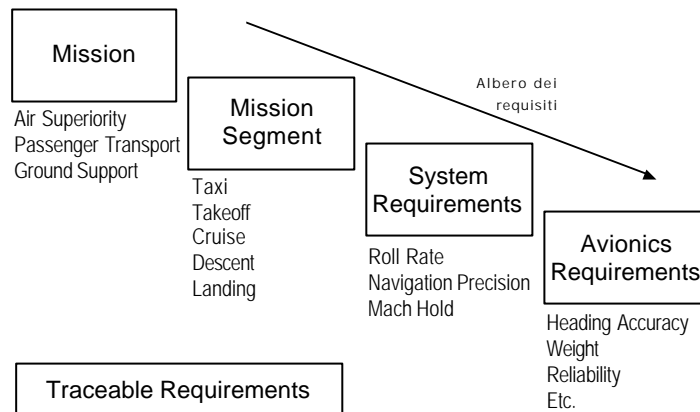
- Ogni fase del progetto è accompagnata dalla verifica della effettiva esecuzione della fase



Key: Rqmts. = Requirements
 SRR = System Requirements Review
 SDR = System Design Review
 SSR = System Specification Review
 PDR = Preliminary Design Review
 CDR = Critical Design Review

Generazione dei requisiti

- Per la definizione dei requisiti spesso viene condotta un'analisi di tipo TOP-DOWN
 - Ogni requisito deve essere affermato in maniera quantitativa e non ambigua



Documento dei requisiti di progetto (Descrizione)

- Documento emesso dal cliente
- Contiene le indicazioni sui requisiti vincolanti del sistema;
- Ogni requisito deve essere numerato e individuato separatamente;
 - La tracciabilità di ogni requisito nel corso dei documenti è mandatoria
 - Ad un requisito corrisponde una o più specifiche
 - Ad una specifica corrisponde uno o più elementi di architettura
 - Ad un elemento di architettura corrispondono uno o più componenti (SW o HW)
 - Ad un componente corrisponde un test che ne verifica le funzionalità.
 - Deve essere possibile rintracciare tutti i test che consentono di verificare la soddisfazione di dato requisito

Documento dei requisiti di progetto (Struttura)

- Introduzione
 - Descrizione del sistema aeronautico che ospita l'apparato avionico
- Requisiti Funzionali
 - Cosa deve fare l'apparato avionico
 - Come lo deve fare
- Requisiti operativi
 - In quale ambiente viene ospitato l'apparato da progettare
- Requisiti di Interfaccia
 - Come il processo si interfaccia con l'utente
 - Come il controllo si interfaccia al resto dell'avionica

Documento di specifiche di progetto (Descrizione)

- Documento realizzato dagli analisti e sottoposto all'accettazione da parte del cliente;
 - Fondamentale per ogni contesa sulla effettiva esecuzione del progetto
- Ogni requisito deve essere numerato e individuato separatamente;
 - Ogni specifica deve essere riconducibile ad almeno un requisito
- Si definisce specifica una caratteristica del sistema avionico che soddisfa ad un requisito del cliente
 - Operazioni che il sistema avionico è in grado di effettuare

Documento di specifiche di progetto (Struttura)

- Introduzione
 - Descrizione del sistema aeronautico (stessa del documento di requisiti)
 - Descrizione degli scopi dell'apparato avionico
- Specifiche Funzionali
 - Cosa farà il processo automatizzato
 - Come lo farà
- Specifiche di Interfaccia
 - Come il processo si interfaccia con l'utente
 - Come il controllo si interfaccia al processo

Documento di architettura (descr.)

- Contiene il metodo secondo il quale il componente (SW o HW) viene realizzato
- Ogni metodo deve essere numerato e individuato separatamente;
 - Ogni metodo deve corrispondere ad una specifica
- Il documento viene compilato dai progettisti dei componenti
 - Viene sottoposto al cliente come verifica di avanzamento del progetto
 - Non è di grande interesse per il cliente
 - L'architettura, tranne alcuni vincoli elencati nel documento dei requisiti, deve essere pensata dai progettisti

Documento di architettura (descr.)

- Vengono forniti i dettagli costruttivi secondo i quali il componente viene realizzato
 - I metodi implementati
 - Le funzionalità previste
 - L'interfaccia richiesta dagli altri componenti
 - L'interfaccia esportata agli altri componenti
 - Le parti condivise con altri componenti
 - Il dettaglio non include i particolari realizzativi, che vengono discussi in un altro documento

Documento di Dettaglio

- Sono contenuti i dettagli realizzativi di ogni componente
 - Per il SW questo documento potrebbe essere costituito dai listati del SW
 - Per l'HW si riportano gli schemi elettronici di ogni componente e dei collegamenti
- I componenti sono gli stessi elencati nel documento di architettura
- Sono di scarso interesse per il cliente (almeno nell'immediato)
- Vengono utilizzati per verificare eventuali malfunzionamenti o per permettere la manutenzione anche a chi non ha realizzato il sistema
- Vengono compilati dai realizzatori del SW e HW

Manuale d'uso

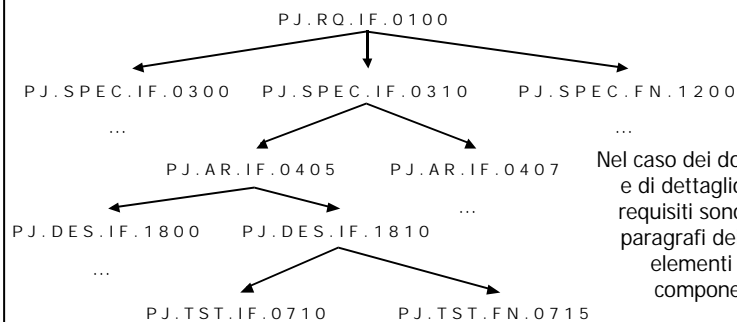
- Il manuale d'uso del SW e dell'HW devono essere disponibile prima del completamento del progetto, in modo da consentire all'utente di verificare la facilità d'uso del componente
- Molti passi compiuti in fase di test fanno riferimento al manuale d'uso per verificare determinate funzionalità

Documenti di Test

- Contengono i metodi di test con i quali la funzionalità di ciascun componente viene verificata
- Il documento viene compilato da
 - Chi realizza il documento di specifiche
 - Chi realizza il documento di architettura
- Chi realizza il SW e l'HW non deve vedere il documento di test per questioni di affidabilità della verifica
 - Il realizzatore potrebbe essere deviato a concentrarsi sul successo nei test piuttosto che sulla reale affidabilità del sistema
- Il documento viene solitamente preventivamente accettato dal cliente
 - Se i test hanno successo, dopo essere stati accettati dal cliente, il cliente è solitamente vincolato ad onorare gli impegni economici relativi al progetto

Documenti di Test

- Ogni test deve essere numerato e individuato separatamente;
 - Ogni test deve corrispondere ad un componente
 - Ogni specifica elencata nel documento di specifiche deve corrispondere ad almeno un test (matrice di tracciabilità)



Nel caso dei documenti di architettura e di dettaglio, gli identificativi dei requisiti sono spesso sostituiti dai paragrafi dei documenti in cui gli elementi di architettura e i componenti sono descritti

Notazioni

- I requisiti, le specifiche, gli elementi dell'architettura, i componenti e infine i test vengono numerati e nominati in modo significativo
 - Esempio: Progetto SCS
 - Requisito (RQ) di interfaccia (IF)
→ SCS.RQ.IF.0100
 - Esistono delle sigle standard:
 - RQ: Requisito
 - SPEC: Specifica
 - AR: Architettura
 - DES: Design (progetto, componente)
 - TST: Test
 - IF: Interfaccia
 - FN: Funzionalità
 - OP: Relativo all'operatività del componente
 - QR: Relativo alla qualità

Matrice di Tracciabilità

- La matrice di tracciabilità riporta la tracciabilità di ogni requisito rispetto ai test che verranno eseguiti

RQ.IF.3325	TST.IF.0100 TST.IF.0102 TST.IF.0105 TST.IF.0110
RQ.IF.3400	TST.IF.2100 TST.IF.2110 TST.IF.2120
RQ.FN.1200	TST.IF.0800 TST.FN.0100 TST.FN.0200 TST.OP.0505

Temporizzazione di un progetto

– Diagramma di Gantt

- diagramma temporale in cui sono definite le scadenze e allocate le risorse di lavoro

