Il software nel settore aerospaziale: indicazioni per la certificazione

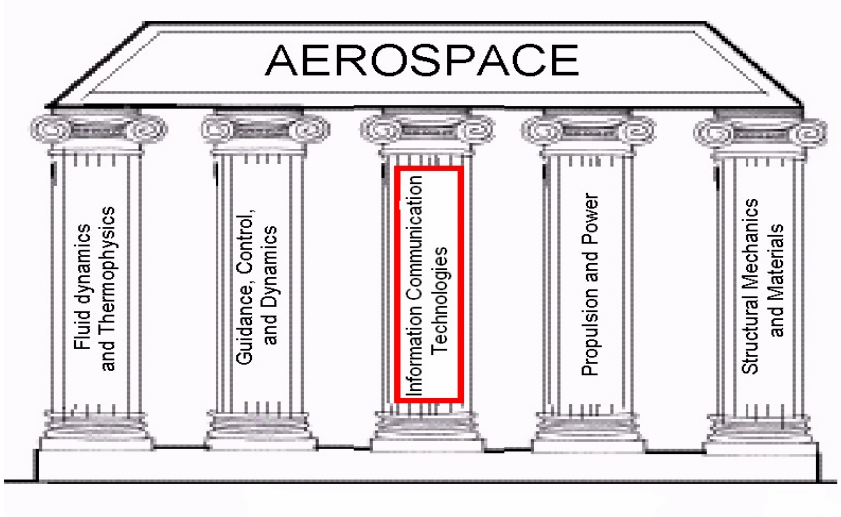
AGENDA

- Criticità del software nel settore aerospaziale
- Standard di riferimento esistenti e loro similitudini/differenze (panoramica e confronti)
- Consigli per la certificazione (approccio e problemi).

Diffusione del Software nei sistemi aerospaziali

- Il Boeing 777 ha 4 milioni di linee di codice ed utilizza 1280 processori embedded
- The F/A-22 Raptor ha 2 milioni di linee di codice
- I sistemi autonomi richiedono software complesso non deterministico per gestire correttamente situazioni non previste

Questo implica che ai 4 pilastri classici nell'ingegneria aerospaziale ne va aggiunto un altro: Tecnologie dell'informazione e della comunicazione (ICT).



... un programma che non funziona è sicuramente errato; ma un programma che funziona non è necessariamente corretto ...

Due termini con significato distinto:

- Safety i requisiti di safety tendono a rendere il sistema incapace di produrre danni catastrofici
- Affidabilità (reliability): riguarda la prevenzione di ogni tipo di errore che possa condurre ad un guasto di sistema

Ai fini della safety non è importante prevenire ogni guasto, ma assicurare che quelli che avvengano abbiano conseguenze tollerabili

CERTIFICAZIONE DEL SOFTWARE SAFETY CRITICAL

La certificazione del software è semplicemente il processo di generare un certificato che può contenere le seguenti informazioni:

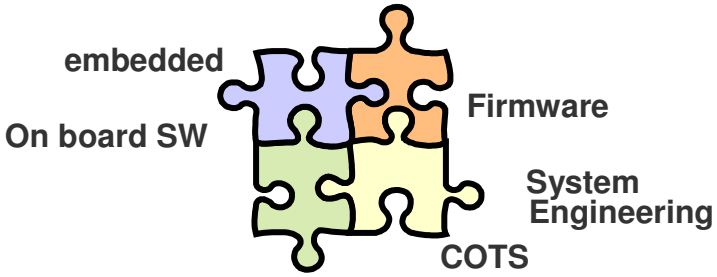
1. conformità allo standard (certificazione di processo)
2. conformità al suo scopo (certificazione di prodotto)
3. conformità ai requisiti (certificazione di prodotto)

CERTIFICAZIONE DEL SOFTWARE SAFETY CRITICAL

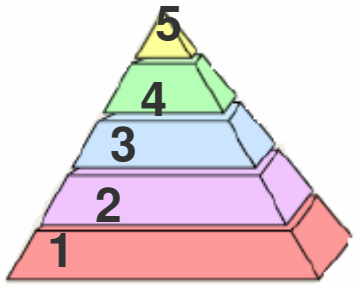
Si definisce *safety critical software* o *safety related software* se un suo malfunzionamento può provocare o contribuire ad un incidente fatale.

Certificazione prodotto + **Certificazione processo** = Independent Software Verification and Validation

Nasce la necessità di un approccio integrato al sistema software con tutte le sue componenti e verso i processi che lo caratterizzano.



In particolare serve valutare la maturità del prodotto e del processo ed intraprendere un miglioramento continuo.



STANDARDS E NORMATIVE

ISO - International Organization for Standardization

ISO/IEC 12207 definisce i processi del Ciclo di Vita del Software, dalla formulazione dei requisiti, allo sviluppo, all'esercizio ed alla manutenzione.

ISO 9126 definisce il modello dei requisiti qualitativi del Prodotto Software.

ISO 15504 – S.P.I.C.E.: Software Process Improvement and Capability Evaluation

MIL - STD: Military Standards

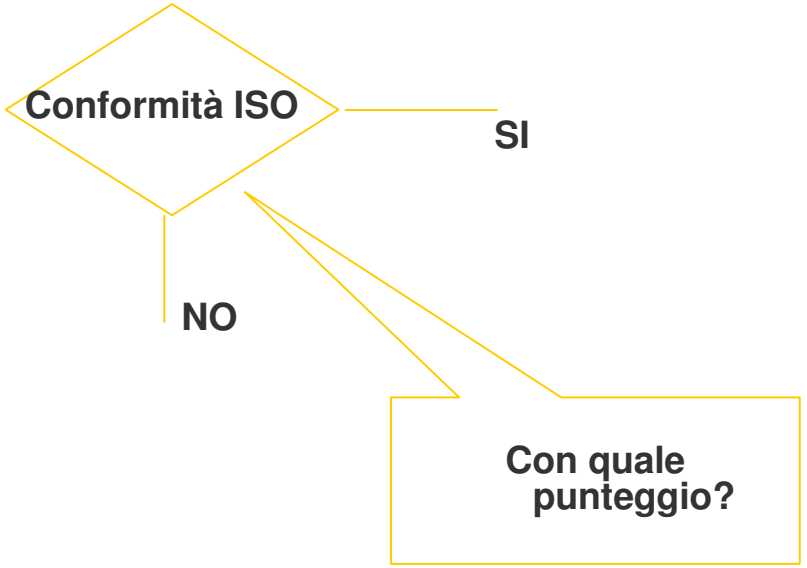
MIL 498(derivato da ISO 12207,ISO 9001 e ISO 9126) valutazione del prodotto software

ESA ECSS: Space Standards (derivati da tailoring di ISO /IEC 12207 per lo spazio)

ECSS-E-40 software engineering

ECSS-Q-80 software product assurance

Alcuni limiti delle norme ISO



Soluzione

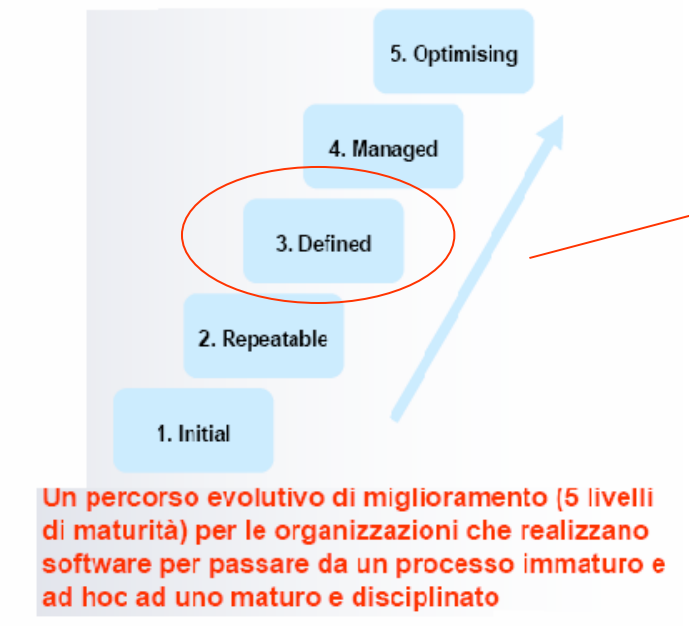
Misurare per Migliorare

CERTIFICAZIONE

Scade il 31/12/2009

CMM la risposta per misurare e migliorare continuamente

Un modello molto conosciuto nel settore dell'Ingegneria del Software è il CMM-Capability Maturity Model del Software Engineering Institute (basato su Mil-Std-498)



Un percorso evolutivo di miglioramento (5 livelli di maturità) per le organizzazioni che realizzano software per passare da un processo immaturo e ad hoc ad uno maturo e disciplinato

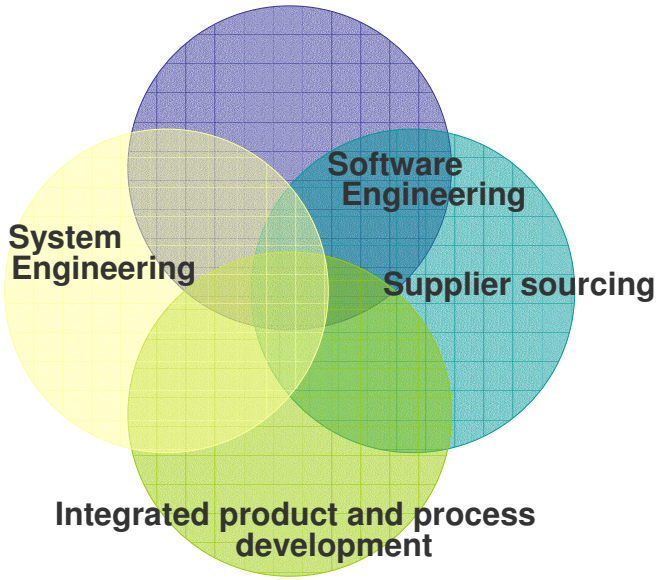
Il CMM si pone come un modello di valutazione e miglioramento dei processi aziendali che supera i limiti citati del sistema ISO 9000 in quanto ha come obiettivo il miglioramento delle prestazioni aziendali in senso lato, partendo dall'analisi dello stato dei processi, passando alla pianificazione del miglioramento per poi monitorare i risultati raggiunti e valutarli in una scala.

Evoluzione verso CMMI

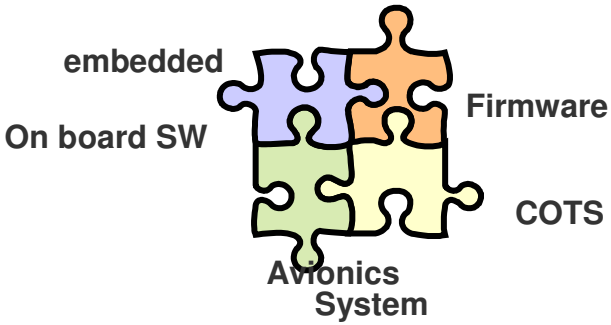
C.M.M. è divenuto la base da cui si sono evolute altre metodologie di valutazione, arricchitesi poi di tecniche di indagine più sofisticate, di metriche più complete e di estensioni alle attività di supporto.

Ragioni commerciali e di contenuto hanno spinto ad una radicale revisione e alla nascita di un modello il **CMMI** per:

- Costruire un insieme di modelli integrati;
- Migliorare le best practices a partire da un modello di partenza basato sull'esperienza;
- Stabilire un'infrastruttura che favorisca l'integrazione di futuri modelli;



Discipline Integrate nel Modello



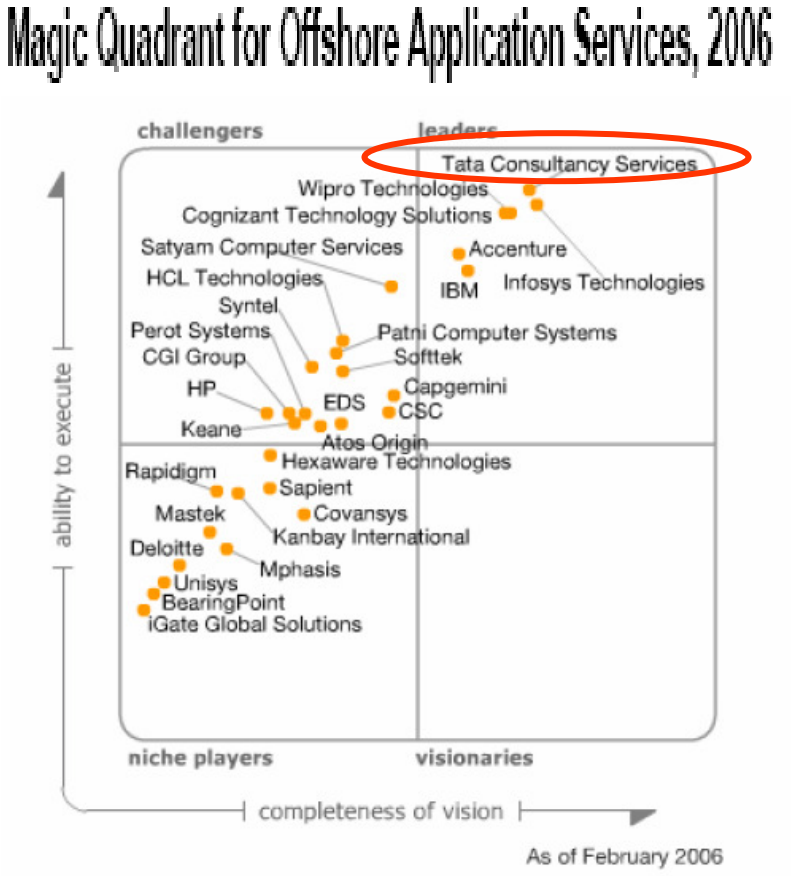
Software integrato in un sistema complesso con vincoli di safety e reliability

Situazione mondiale

- There are 80 software centers on the planet that are assessed at CMM Level 5.
- Of all those centers, 60 are in India”
- L’ente che ha « lanciato il CMMI è il SEI (Software Engineering Institute) della Carnegie Mellon
- The SEI is a federally funded research and development center conducting software engineering research in acquisition, architecture and product lines, process improvement and performance measurement, security, and system interoperability and dependability

TCS – Jewel in the Crown

- Started Indian IT Industry in 1968
- Largest IT company in Asia in terms of
  - revenue of $3.5 bn for rolling 12 months
  - Only organization with Enterprise-wide Integrated CMMi, PCMM, ISO 9001:2000, BS 7799 -2:2002 and BS 15000-1:2002
  - Over 80,000 employees with 65 nationalities
  - Market Capitalization (over $28 bn)
- Highest Quality Standards
  - First Indian company to receive AS9100, Rev B certification for design of airframe structure
- Operations in 47 countries, 160 Offices in 34 countries
- 748 Active Customers
  - 7 out of Top 10 Fortune 500 US Companies
  - 37 of the Top 100 Fortune 500 US Companies
- Customer Loyalty – 95.2% revenue from repeat business



CONCLUSIONI

Questa veloce panoramica dei modelli di maturità e dei metodi di miglioramento suggerisce *specifiche raccomandazioni per applicazioni safety critical*

- usare un approccio **basato su obiettivi** per la certificazione dei sistemi che integri aspetti relativi al prodotto ed ai processi
- dimensionare l'impegno e la profondità di SV&V&C con la **criticità** del sistema.
- ricorrere ad un **ente indipendente ISV&V&C** nell'eseguire la verifica, la validazione e la certificazione di componenti critiche (sia rispetto alla safety che alla security)
- scegliere con **massima libertà metodi e strumenti** nella definizione del framework di ISV&V&C ma definire rigorosamente i passi da seguire.
- utilizzare tecniche avanzate di analisi statistica