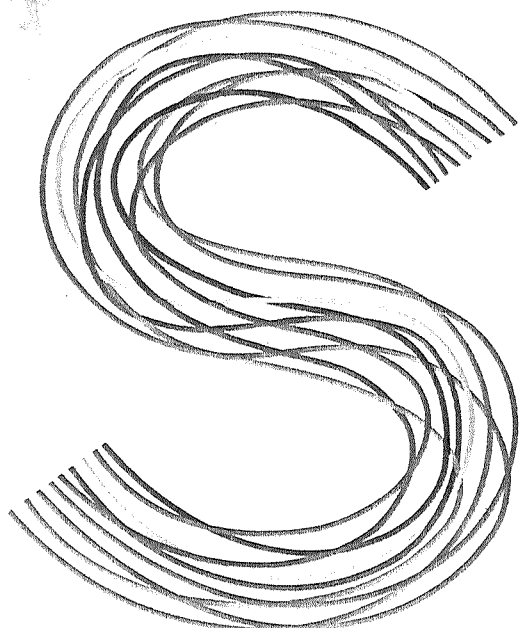


BO-08
(1990)

EDIZIONI
RITMAN



sistemi
SOFTWARE

IST. EL
BIBLIOT. A
Posiz. ARCHIVIO BO-08

MENSILE DI INFORMATICA ■ TELEMATICA ■ APPLICAZIONI

LE RETI NEURONICHE

**LA CERTIFICAZIONE
DEL SOFTWARE**

**DISCORRENDO
DI SOFTWARE ITALIANO**

**LA MANUTENZIONE
DEL SOFTWARE**

**LA SICUREZZA
DEI SISTEMI INFORMATIVI**

N° 11 - NOVEMBRE 1990

La certificazione nella tecnologia software

Un problema di crescente interesse nei suoi vari aspetti,
scientifici, tecnologici, industriali

A. Bertolino, C. Carlesi, M. Fusani, V. Lami

I prodotti della tecnologia dell'informazione hanno oggi raggiunto una notevole diffusione di carattere capillare, e che, per altro, continua a crescere. Per citare soltanto alcune delle applicazioni più comuni, il software viene adoperato per la gestione dei servizi e degli sportelli pubblici, per l'organizzazione del lavoro all'interno dell'ufficio e dell'azienda, per il controllo dei processi di produzione, e, in misura sempre maggiore, il software diviene un elemento essenziale degli altri prodotti industriali. In aggiunta, in ogni campo, le prestazioni che vengono richieste al componente software sono sempre più spinte e più complesse.

Innegabilmente, questo processo di informatizzazione ha comportato apprezzabili miglioramenti nella vita di tutti i giorni e importanti progressi nella tecnologia. Il rovescio della medaglia, tuttavia, è che parallelamente diveniamo sempre più dipendenti dal "buon funzionamento" del componente software: il software è l'elemento "critico" di tutte le applicazioni ricordate e di molte altre ancora.

Purtroppo, va detto a questo proposito che al crescere delle aspettative riposte sul software non ha

corrisposto una parallela evoluzione delle tecnologie di produzione. Certamente abbiamo ormai lasciato indietro lo stadio dell'artigianato, tuttavia ancora oggi rimangono da fare molti progressi. Ciò vale in maggior misura per quanto riguarda la qualità del prodotto software, che rimane indubbiamente l'aspetto più trascurato dalle aziende, spesse volte perché ritenuto, a torto, un costo aggiuntivo e non necessario. Al contrario, occorre abbracciare una "cultura della qualità": la qualità è, oggi più che mai, un elemento essenziale da perseguire ed un investimento che rende, poichè dà ritorni in termini di affidabilità, manutenibilità e riusabilità del prodotto software.

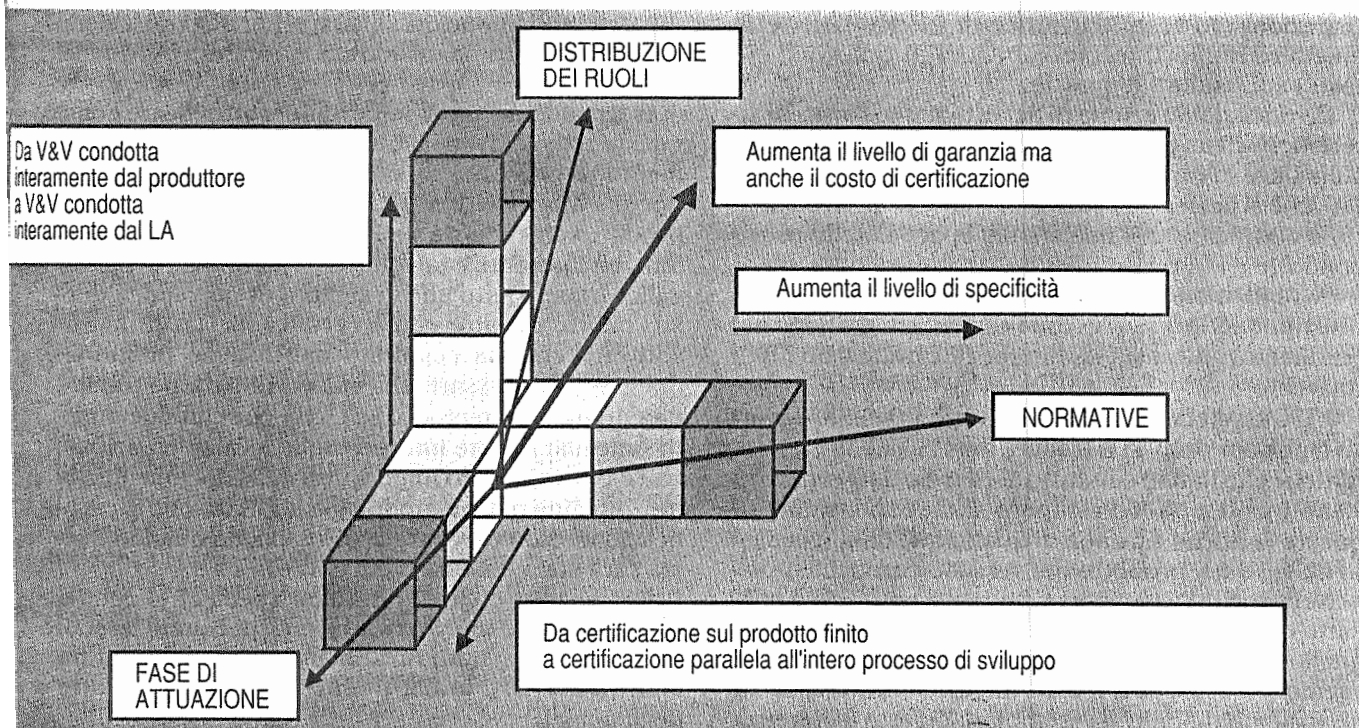
Un elemento fondamentale della qualità in tutti i settori della tecnologia, e del quale vogliamo occuparci nel seguito di questo lavoro in relazione al prodotto software, è quello della certificazione.

Recentemente, si comincia a sviluppare un certo interesse verso la certificazione dei prodotti software nei diversi ambienti scientifico, industriale ed istituzionale. I motivi di questo interesse sono economici, politici e tecnologici. In primo luogo c'è l'esigenza di consentire la circolazione di prodotti in ambito internazionale, garantendo la loro interusabilità senza doverla verificare ogni volta. Non meno importante è poi il vantaggio di disporre di dichiarazioni ufficiali e autorevoli circa certe caratteristiche funzionali, di

A. Bertolino, C. Carlesi, M. Fusani, V. Lami

Istituto di Elaborazione delle Informazioni, CNR, Pisa. Questo lavoro deriva dalla rielaborazione di una relazione (Bertolino 89) presentata al Congresso Annuale A.I.C.A., Trieste, 1989.

Qualità



sicurezza e di qualità dei prodotti. La Comunità Europea, per esempio, poichè possiede già strutture organizzative internazionali, sta affrontando il problema dell'istituzione di una disciplina globale che dovrebbe regolare l'attività di certificazione negli Stati membri.

Tuttavia, questa disciplina non è ancora matura; sono state definite alcune proposte per quanto riguarda gli aspetti gestionali e organizzativi, sulla traccia degli altri sistemi di certificazione già assestati in altre tecnologie.

Invece, gli aspetti tecnici e procedurali sono ancora oggetto di studio e di ricerca; perfino lo stesso termine di "certificazione di un prodotto software" dà ancora adito a diverse interpretazioni.

Ciò che è certo è che di certificazione del software c'è bisogno sia nel settore privato che in quello pubblico e la domanda è in continua crescita.

In questo lavoro cercheremo di chiarire anzitutto l'obiettivo ed l'importanza della disciplina della certificazione del software. Forniremo anche alcune definizioni ed alcuni criteri, ma soprattutto esporremo le nostre opinioni e le nostre interpretazioni per questo settore in cui, come accennato, quasi tutto è ancora in via di definizione, frutto di esperienza diretta e di studio, che abbiamo adottato nell'obiettivo di istituire un servizio qualificato di certificazione presso l'IEI del CNR di Pisa.

Definizioni

Allo scopo di mantenere un riferimento uniforme nel corso del lavoro, dato che nella letteratura coesistono attualmente terminologie discordanti, riportiamo in questo paragrafo alcune definizioni. In esse, e nel seguito, si farà genericamente riferimento ad un "ciclo di sviluppo" del software suddiviso in fasi sequenziali, senza, per questo, voler restringere la generalità delle considerazioni esposte ad un modello di sviluppo particolare.

Verifica: il processo rivolto a determinare se il prodotto di una data fase del ciclo di sviluppo del software soddisfi i requisiti durante la fase precedente.

Validazione: il processo rivolto a determinare se il prodotto di una data fase del ciclo di sviluppo del software soddisfi i requisiti stabiliti nella fase iniziale.

Ente Accreditato (EA): un'istituzione indipendente sia dal produttore che dall'utente del software, qualificata (accreditata) da una autorità riconosciuta (governo o organizzazione internazionale o comunità) per effettuare un processo di certificazione di software.

Laboratorio Accreditato (LA)¹ (o Laboratorio di Prova): un laboratorio, accreditato da un'autorità riconosciuta, che ha il compito di effettuare prove

Questo comporta che un sistema di certificazione di software non dovrà controllare la qualità della produzione in serie con tecniche di campionatura sui "lotti" prodotti; quello che va controllato è, invece, la progettazione del primo pezzo.

Inoltre, un grosso sforzo nel campo dell'ingegneria del software è oggi rivolto a rendere possibile la riutilizzo di moduli software [Jones84, SEJ88]. In questa prospettiva, ci chiediamo se sia attuabile una certificazione "modulare", cioè se sia pensabile la certificazione dei singoli "pezzi" di un prodotto software, oppure, se la "peculiarità" del software non si rifletta anche qui, richiedendo ogni volta la certificazione dell'intero prodotto.

Un'ulteriore osservazione può essere fatta a proposito dei test che possono essere effettuati su un prodotto software. L'efficacia del processo di test dipende pesantemente dalla professionalità dell'operatore che lo conduce e dalla conoscenza che egli ha del programma esaminato. Infatti, come noto [Adrion82], per decidere sull'esito di una prova, il comportamento del programma in seguito alle sollecitazioni applicate deve essere confrontato con il comportamento "atteso", che, generalmente, non può essere stabilito a priori basandosi su una legge fisica o matematica immutabile, come nel caso di prove condotte su prodotti meccanici o elettrici.

Per quanto riguarda problemi di carattere burocratico, basterà semplicemente accennare all'annosa mancanza di adeguate normative. Gli standard esistenti per la certificazione della tecnologia dell'informazione descrivono soltanto le procedure di validazione di alcuni campi di applicazione, come, ad esempio [M-IT-03/87], software per la comunicazione, per la grafica, CAD o, infine, alcuni linguaggi di programmazione.

Analisi della domanda di certificazione

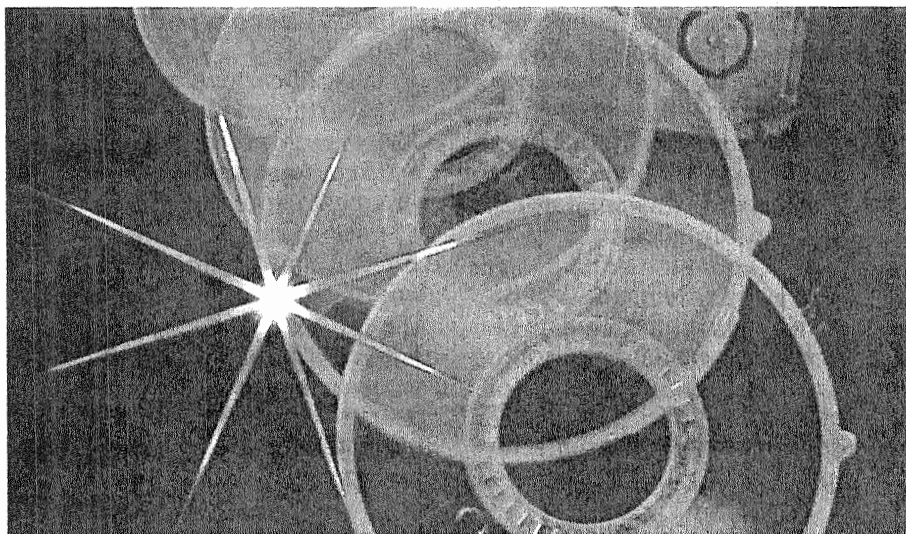
Abbiamo fin qui analizzato alcune delle problematiche insite nell'istituzione di un sistema di certificazione per il software. Cerchiamo ora di analizzare la situazione attuale della domanda per tale certificazione, individuandone i motivi.

A causa dei problemi sopra citati (peculiarità della produzione, manualità dei test, mancanza di standard generali), oggi come oggi non si è raggiunta una maturità nella scienza informatica tale da consentire una diffusa pratica di certificazione di prodotti software. Nonostante ciò, esiste una forte domanda, che, nella nostra esperienza, si è già concretizzata con alcune richieste ufficiali [Bertolino87], da parte di enti sia pubblici che privati, per un servizio di certificazione nei confronti del nostro Istituto, in qualità di ente pubblico, con competenze nel settore dell'ingegneria del software.

La domanda di certificazione è soprattutto dovuta a tre motivi:

1) *Richiesta di qualità* - Viene da parte del produttore di software, che vede la certificazione come un attestato che la sua produzione possiede effettivamente caratteristiche di qualità, cioè che egli ha preso tutte le precauzioni necessarie per ottenere un prodotto confacente alla "regola d'arte". Questa attitudine, peraltro, risulta vantaggiosa anche per il certificatore, in quanto il software "ben fatto" è più facile da certificare.

Tale richiesta di qualità proviene anche da parte di alcune categorie dell'utenza (ci riferiamo qui a grossi committenti o a produttori che acquistano all'esterno moduli software da inserire in sistemi più ampi),





che vogliono avere dei criteri per giudicare se il fornitore/processo e anche il prodotto siano adeguati alle proprie esigenze. Per fare questo, l'utente che, in generale, non si riconosca competente in materia, può operare in due modi: formare un gruppo interno di tecnici per fissare dei criteri di accettazione, oppure rivolgersi ad un ente esterno qualificato allo scopo. In pratica, questo tipo di utente è disposto ad accollarsi l'eventuale investimento iniziale necessario alla certificazione, consapevole che la qualità che ne deriva, più o meno direttamente, sul software, a lungo andare gli permetterà di recuperare i costi aggiuntivi.

C'è da sottolineare, comunque, che non tutti gli utenti pensano in questo modo; sfortunatamente, ci sono anche utenti che, credendo di risparmiare nel ridurre l'investimento iniziale, richiedono software senza espliciti attributi di qualità e al più basso prezzo possibile; di conseguenza, i produttori, dovendo sottostare alle leggi di mercato, sono costretti a produrre anche questo tipo di software, generalmente commissionandolo a produttori sempre meno qualificati, ma più a buon mercato (fino ai cosiddetti "cantinari").

2) *Rispetto di requisiti di legge* - In Italia, così come nelle altre parti del mondo, molti prodotti per essere commercializzati devono rispettare alcuni requisiti di legge, rivolti a salvaguardare il consumatore attraverso la prescrizione, per ogni prodotto, di adeguate caratteristiche di sicurezza, compatibilità, qualità, ecc... La conformità a tali requisiti è garantita attraverso un appropriato processo di certificazione.

Poichè, al giorno d'oggi, la componente è presente in molti prodotti, anzi è spesso diventata preponderante, ne consegue che il rispetto di requisiti di legge dipenderà anche da tale componente. Da qui la richiesta, ad esempio, della certificazione del software per i misuratori fiscali (già prescritta da una legge) o del software medico (che si spera sia al più presto regolata attraverso apposite leggi anche in Italia).

3) *Necessità di armonizzazione* - C'è una domanda di certificazione rispetto alle normative di standardizzazione europea che stanno per essere messe a punto dal CEN (Comité Européen de Normalisation) [M-IT-03/87] e che anche i prodotti software dovranno soddisfare per poter circolare liberamente in Europa dopo il 1992.

Riassumendo, dall'analisi sulla domanda risulta che le principali parti interessate, da punti di vista diversi, ad un eventuale servizio di certificazione sono:

- I produttori di software, che vogliono, ed in alcuni casi devono, certificare i loro prodotti.
- Gli utenti, che vedono nella certificazione un mezzo per stabilire se i prodotti che essi acquistano

possiedono il grado desiderato di qualità.

- Le istituzioni, che attraverso leggi dello stato devono garantire adeguati requisiti di affidabilità e sicurezza.

- Gli organismi europei, che tendono all'armonizzazione internazionale.

- Infine, gli EA ed i LA, che dovranno fornire il servizio in esame;

Di fronte ad una domanda così alta, ci troviamo paradossalmente di fronte ad un'offerta di metodi e strumenti per la certificazione che è del tutto inadeguata.

Per rendere effettivo un servizio di certificazione occorre però superare non solo problemi tecnici, ma anche di natura politica o commerciale (ad esempio i produttori meno qualificati vedrebbero, nell'introduzione di un certificato obbligatorio, una notevole riduzione del proprio mercato). tali problemi possono essere superati attraverso la promozione di centri o consorzi per la certificazione attraverso una forte azione di sensibilizzazione che denunci lo squilibrio fra l'attuale certificazione dei prodotti software (quasi nulla), rispetto a quella degli altri prodotti, e, infine, rendendo operative anche per il software normative in campo europeo.

Ed è appunto in questo contesto che si inserisce la nostra iniziativa di istituire un servizio qualificato per la certificazione del software.

Possibili scenari e criteri

Illustriamo di seguito alcuni possibili scenari per un sistema di certificazione, che ci serviranno di riferimento per un inquadramento della metodologia che delineeremo nel prossimo paragrafo.

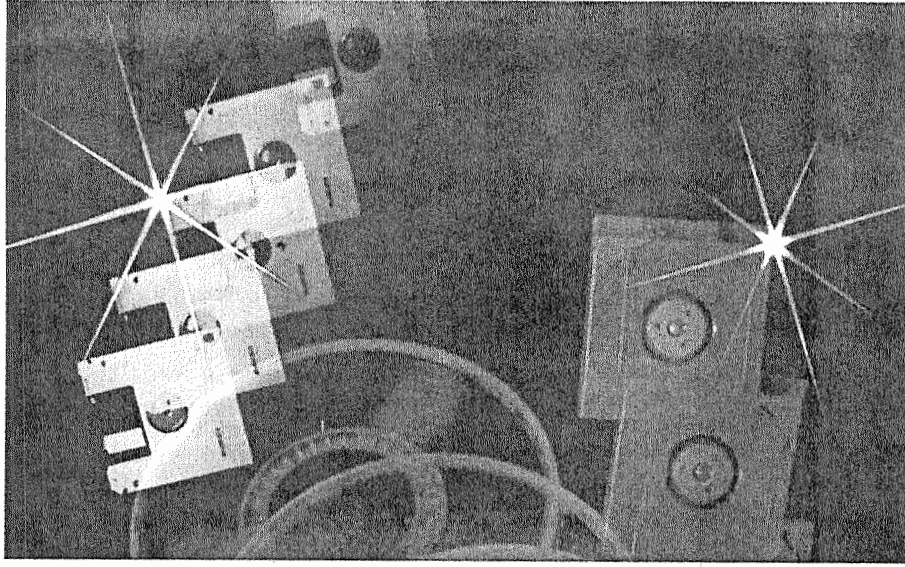
Come noto, un servizio di certificazione può essere realizzato secondo due approcci base [Copigneaux88]:

-) la certificazione del prodotto;
-) la certificazione del processo.

Certificazione del prodotto

In questo approccio il produttore sviluppa il software, seguendo una metodologia più o meno indipendente, e quindi lo sottopone all'EA per la sua certificazione.

La certificazione del prodotto può avvenire secondo diverse linee di intervento; abbiamo individuato tre parametri, al variare dei quali, parallelamente alla crescita del livello di confidenza offerto dal processo di certificazione, aumentano anche i costi del servizio. Le considerazioni seguenti sono state schematizzate



zate in Fig. 1. La prima alternativa riguarda l'identità del soggetto preposto a svolgere le attività di Verifica e Validazione (V&V). Ad un estremo, si può prevedere che tale attività sia svolta interamente dal LA e dall'EA in accordo ad una normativa (operativa e di documentazione) definita. All'altro estremo, invece, la V&V sul prodotto è svolta interamente dal produttore e l'EA interverrà soltanto successivamente per certificare che tale V&V sia stata condotta in accordo alle normative definite (certificazione dell'autovalidazione). L'EA si riserverà, ovviamente, la facoltà di ripetere alcuni test o ispezioni campione.

Un'altra coordinata del processo di certificazione è il livello di specificità delle normative che lo regolano. Tali normative riguardano sia la documentazione che deve accompagnare il prodotto, sia la procedura di V&V. Ad esempio l'EA può imporre una procedura di V&V dettagliata in ogni suo passo, oppure stabilire solo alcuni criteri di testing funzionale del codice. Infine, il terzo parametro riguarda la fase in cui ha inizio il processo di certificazione. In contrapposizione ad un intervento di V&V sul prodotto finito, si può pensare che il LA attivi una procedura di V&V parallela al processo di sviluppo, ovvero, instauri una stretta linea di collaborazione con il produttore. Quest'ultima soluzione presenta difficoltà realizzative, in quanto il LA dovrebbe entrare a far parte integrante dell'attività aziendale, e in alcuni casi addirittura sovrapporsi ai gruppi interni di V&V; non ultimo, il problema della reticenza delle aziende a divulgare verso l'esterno le proprie modalità di lavoro.

Certificazione del processo

Anziché validare il singolo prodotto software, l'EA potrebbe certificare il processo di sviluppo. Anche questo approccio può essere effettuato con diverse modalità di intervento, di livello gradatamente meno stringente nei confronti del costruttore.

Ad un estremo, l'EA prende come riferimento un processo di sviluppo standard e, in fase di certificazione, verificherà la conformità a tale modello del processo effettivamente seguito. Questa verifica potrà essere condotta mediante ispezioni in fabbrica, oppure tramite analisi della documentazione.

Ad un livello meno vincolante, l'EA segue una nor-

mativa soltanto per alcune sottofasi del ciclo di sviluppo. Ad esempio, si potrebbe richiedere una fase formale di revisione delle specifiche, oppure un adeguato livello di copertura nel testing dei moduli software.

Infine, l'approccio meno restrittivo è quello in cui l'EA non fornisce indicazioni sul procedimento da seguire, ma effettua la validazione del processo interno del costruttore tramite ispezioni. Queste ispezioni possono essere schedate in maniera periodica e concordata, oppure essere effettuate senza preavviso (spot-check).

Criteri per la definizione di una metodologia di certificazione

Abbiamo analizzato fin qui le diverse possibilità di scelta che si offrono nella definizione di un sistema di certificazione. Vediamo ora alcuni criteri che debbono essere seguiti in tale scelta.

Un criterio fondamentale è l'orientamento verso il massimo grado possibile di standardizzazione della documentazione di accompagnamento: il vantaggio di tale requisito è, ovviamente, quello di richiedere il minimo impegno di tempo e risorse per l'analisi dei documenti presentati. Si dovrà cercare, allo stesso tempo, il giusto compromesso per influenzare il meno possibile il processo di sviluppo del singolo produttore, in modo da non incidere pesantemente sui costi e le tecniche di produzione.

Un secondo criterio è quello di perseguire nella maggior misura possibile la corrispondenza fra la documentazione presentata ed il prodotto e/o il processo da certificare. In altri termini, la metodologia di certificazione dovrà essere concepita in modo da coprire l'intero processo di sviluppo, con campionamenti più o meno vicini, e da richiedere elevate caratteristiche di tracciabilità da un campione all'altro. In questo modo, eventuali tentativi di documentazione artefatta, pur sempre inevitabili, diverranno costosi e complessi quanto o in misura maggiore di una documentazione che effettivamente rispecchi il prodotto e/o il processo.

Un ulteriore criterio è quello di prevedere interventi diversificati, sia sul prodotto che sul processo, cercando di fondere in un'unica metodologia i vantaggi offerti da ciascun tipo di certificazione.



Proposta di una metodologia di certificazione

Dopo aver introdotto le problematiche connesse con la definizione di un sistema di certificazione del software, in questo paragrafo proponiamo una metodologia di certificazione, concepita a partire dal presupposto di poter essere applicata nella più ampia possibile delle generalità dei casi, o, al contrario, di essere dipendente nel minor grado possibile dalla tecnologia di sviluppo del singolo produttore.

Questa metodologia deriva in parte da un'esperienza di certificazione, svolta da parte dell'IEI del CNR di Pisa su alcuni prodotti software particolari. Il software in questione è quello dei misuratori fiscali (registratori di cassa e punti di vendita); le caratteristiche da certificare in base a prescrizioni tecniche del Ministero delle Finanze [Legge18/83] sono la garanzia del rispetto dei requisiti fiscali dei programmi, cioè solo di una parte delle specifiche funzionali del software.

Pur nelle modeste dimensioni dei prodotti in questione, si sono presentati subito grossi problemi, che erano quelli di documentazione frammentaria e linguaggio prevalentemente assembler, il che rendeva impossibile un lavoro completo a costi accettabili (Bertolino87). Eppure la cosa si doveva fare in qualche modo. Si è fatto così ricorso ad un estenuante lavoro di interazione con i costruttori (talvolta con "intermediari" nazionali che conoscevano poco il prodotto) e a ispezioni di campioni per avere informazioni su alcune parti del software fiscale. I certificati, poi, non potevano ragionevolmente garantire nulla, solo che le parti più "sensitive" erano state ispezionate con certi risultati. Sarebbe stato assurdo, date le condizioni, certificare che "il prodotto software è conforme alle prescrizioni ministeriali".

La metodologia che proponiamo di seguito è nata in seguito ad una riflessione su questi problemi e su altri che scaturiscono dall'opportunità di spostare il terreno applicativo della certificazione verso casi più generali, per i quali abbiamo potuto rilevare che esiste una discreta, crescente domanda (paragrafo 2).

La metodologia prevede, per ciascun prodotto per il quale si voglia istituire un servizio di certificazione, di due fasi distinte:

-) fase preliminare,
-) fase a regime.

Nella fase preliminare, l'EA conduce un'analisi ed una selezione dei requisiti e/o delle normative rispettate a cui debba essere condotta la certificazione e,

eventualmente, anche della classe di criticità dell'applicazione in esame.

In seguito a questa analisi l'EA (eventualmente avvalendosi della consulenza del LA) produce:

- i) un elenco dei documenti che dovranno essere presentati dal produttore;
- ii) un insieme di formulari, di seguito chiamati anche "form", che dovranno essere compilati dal produttore, uno per ciascun documento di cui sopra;
- iii) un piano di validazione del codice, ovvero un piano di testing funzionale generato a partire dai requisiti e/o dalle normative, ad un elevato livello di astrazione.

Vediamo brevemente, nell'ordine, i criteri che ci hanno condotto alla scelta dei 3 prodotti sopra elencati.

L'imposizione di un elenco minimo standard di documenti (come in i)), ovvero di prodotti intermedi del ciclo di sviluppo, corrisponde a delineare alcuni passi obbligati di tale processo e perciò, dall'analisi di tali documenti, pensiamo di poter attuare, in una certa misura, una certificazione del processo di sviluppo.

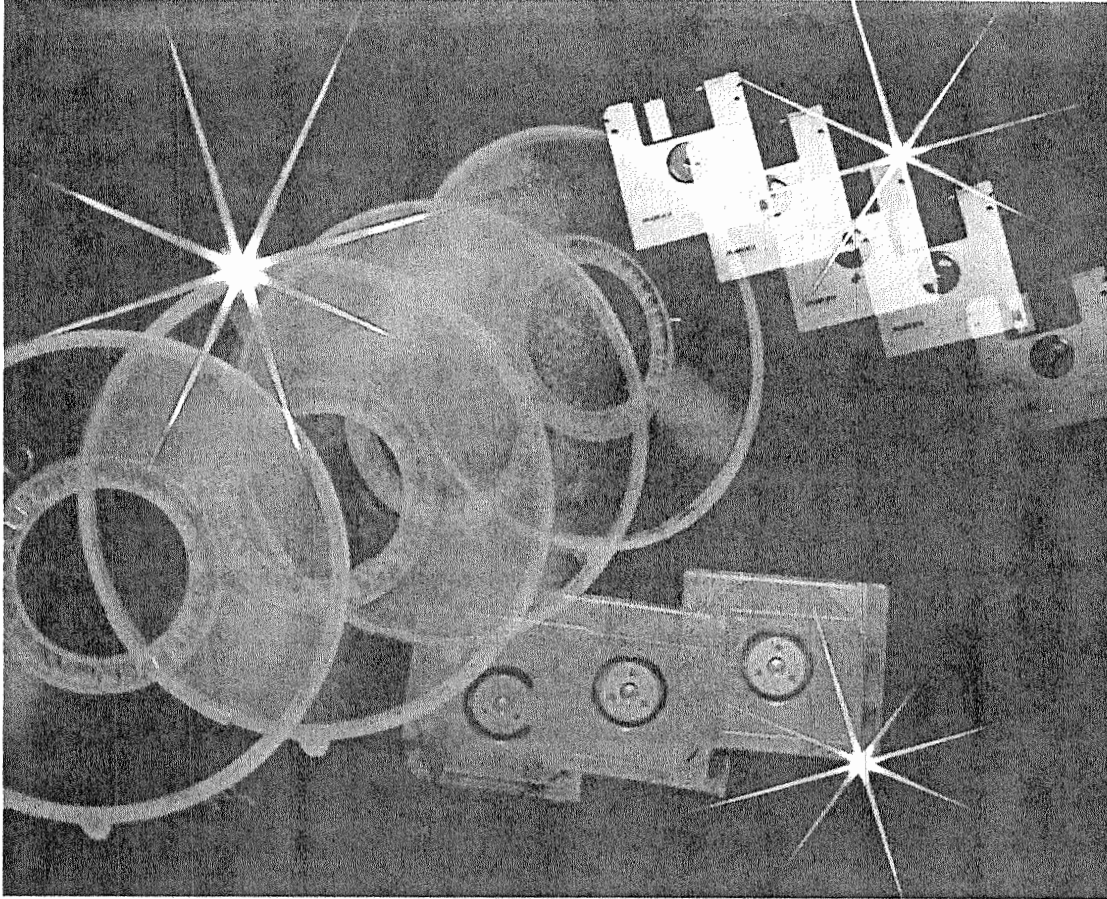
L'idea di introdurre dei formulari (come in ii)) è derivata, come sarà approfondito nel seguito, da esigenze di standardizzazione (il primo dei criteri forniti nel paragrafo precedente), da una parte, e di tracciabilità fra i singoli documenti (nell'ordine, il secondo criterio fornito), dall'altra.

Infine, richiedendo una fase di testing funzionale basato sui requisiti per soddisfare il piano imposto dall'EA (come in iii)), abbiamo voluto attuare (in accordo all'ultimo dei 3 criteri forniti) anche la certificazione del prodotto;

L'attività di analisi e di acculturamento sul prodotto, che questa fase preliminare richiede, avrà ovviamente un suo costo, e perciò la più immediata considerazione che può farsi sull'applicabilità della metodologia è se il prodotto giustifichi o meno tale sforzo, o per la sua diffusione, o, laddove si tratti di un "esemplare unico", per la sua criticità.

Questa fase corrisponde alla definizione dei criteri che rendono certificabili il prodotto in esame, come anticipato al paragrafo 2. Per "tutti i documenti necessari" sono qui intesi quelli risultanti dall'elenco i) redatto dall'EA nella fase preliminare; "adeguatamente interpretabili" significa che tali documenti debbono essere accompagnati dai relativi form compilati.

Si passa quindi alla fase di regime: il produttore che intenda sottoporre un prodotto software a certificazione presenterà al servizio i documenti richiesti in i), i form compilati e, inoltre, un rapporto sull'attività di validazione del codice. Quest'ultima sarà stata con-



dotta basandosi su un proprio piano dettagliato di test, ricavato a partire dal piano di validazione (ad alto livello) fornito dall'EA.

Più in pratica, con riferimento ad una classe di applicazione senza elevate caratteristiche di criticità, l'insieme dei documenti richiesti potrebbe essere costituito da:

- specifiche funzionali;
- specifiche di dettaglio (diagrammi del flusso di controllo e del flusso dei dati);
- codice sorgente, "adeguatamente" commentato;
- rapporto dei test;

a ciascuno dei quali è associato un set di form compilati.

Ribadiamo che il rapporto dei test contiene i risultati ottenuto dall'attività di test, condotta in base al piano di validazione fornito dall'EA; i singoli casi di test (cioè i singoli dati di input), che ovviamente sono particolari di ogni progetto, sono ricavati dallo stesso produttore.

Per ciascun prodotto sottoposto a certificazione, il LA conduce le attività di analisi della documentazione e, eventualmente, la ripetizione di un sottoinsieme campione dei test.

L'analisi della documentazione viene guidata dai form, che hanno appunto lo scopo di fornire una chiave di lettura.

L'idea dei form nasce, infatti, come compromesso tra due esigenze contrastanti: da una parte, razionalizzare la mole di documentazione proveniente da aziende diverse, e perciò redatta con metodi i più svariati possibili, che il LA deve analizzare. Dall'altra, incidere nella minor misura possibile sulla metodologia di documentazione del processo di sviluppo, e, di riflesso, sui costi del singolo produttore.

Se per soddisfare compiutamente la prima esigenza sarebbe bastato, ad esempio, imporre un formato standard per i documenti richiesti, ciò non si è ritenuto opportuno, proprio per venire incontro alla seconda esigenza.

Il vantaggio più evidente della metodologia proposta è quello della sua semplicità di applicazione: non sono richieste conoscenze di particolari tecnologie, né la disponibilità di strumenti specializzati. Per questi stessi motivi, il metodo proposto risulta particolarmente economico.

D'altra parte, le caratteristiche di semplicità prospettate non debbono essere viste come limitative all'affidabilità della metodologia, poiché rimane aperta la possibilità di integrare il metodo manuale fin qui prospettato con tecnologie avanzate, laddove ciò sia fattibile e necessario. Ad esempio, si può imporre in aggiunta che il piano di validazione sia soddisfatto con un livello minimo di copertura del codice analizzato.

Nel caso di applicazioni critiche, soprattutto, questa procedura richiede di essere affiancata da ulteriori garanzie. Infatti, l'approccio basato sui form è orientato verso la certificazione di alcuni requisiti funzionali più significativi. Questo è concettualmente diverso dall'esigenza di garantire l'affidabilità di un prodotto software critico, che richiede una procedura ben più costosa per la sua V&V globale.

Da un altro punto di vista, possiamo dire che il procedimento proposto è rivolto principalmente a verificare requisiti funzionali, e non criteri globali di qualità.

E' però anche vero che, poiché si richiede una adeguata documentazione ed un'adeguata compilazione dei form, il produttore è condotto verso un

processo di sviluppo più razionale e documentato. Perciò un effetto secondario e positivo provocato dall'asservimento a questo procedimento di certificazione è quello di iniettare un livello di qualità nel processo di sviluppo.

Per quanto riguarda gli aspetti organizzativi, l'attività si sta perfezionando nel progetto di istituzione di un servizio qualificato di certificazione del software presso l'IEI, includente il coordinamento di un Laboratorio di test esterno al CNR, ma vincolato da una convenzione.

Caratteristiche dell'attività, al momento attuale, sono:

- Avere a disposizione un ambiente (presso l'IEI stesso) dove si svolge attività di ricerca nel campo dell'Ingegneria del Software. Ciò è importante per fornire al servizio una base tecnico-scientifica in continua evoluzione.

- Mantenere un contatto di consulenza con grossi utenti nazionali di software per impieghi generali. Ad essi è rivolto il servizio, ma il servizio stesso trae, dai

problemi reali incontrati nel campo dell'accettazione dei prodotti, spunti per definirne i criteri.

- Possedere un "parco tools" per il testing statico e dinamico operante su workstations (nel caso particolare, una rete di Istituti composta da SUN 3/50). I test, come si è detto, forniscono informazioni sulla qualità del prodotto, utili nel processo di certificazione.

- Svolgere corsi sulla qualità del Software presso aziende di produzione e di utilizzazione. I corsi tendono a diffondere una "cultura della qualità", specialmente negli utilizzatori, che è il presupposto, e nello stesso tempo il risultato, di maggior domanda di certificazione.

- Mantenere relazioni con Istituzioni di ricerca applicata (come il Software Engineering Institute della CMU) e di gestione delle attività nazionali di certificazione (come il Centro Italiano Metodologie di Controllo, CIMECO, organo di coordinamento delle attività nazionali di test e certificazione nel campo della tecnica dell'Informazione secondo lo schema della Comunità Europea). ■

Riferimenti

[Adrion82] Adrion, W.R., Branstand M.A., and Cherniavsky, J.C., "Validation, Verification and Testing of Computer Software", ACM Computing Surveys, Vol. 14, No. 2, June 1982.

[Bertolino87] Bertolino, A., Fusani, M., "Software Validation: A Government-imposed Challenge to the State-of-the-Art in Certification", Computers & Standards, Vol. 6, 1987, pp. 433-436.

[Bertolino89] Bertolino, A., Carleri, C., Fusani, M., Lami, V., Leggio, F., "Una Iniziativa per un Servizio di Certificazione del Software: Considerazioni e Proposte", Atti del Congresso Annuale A.I.C.A., Trieste, 4-6 Ottobre 1989, pp. 723-734.

[CENCER86] CENCER, Specific Rules for the CENCER Certification Scheme for Information Technology, CCC1 N. 71, Rev. 2, 1986.

[Copigneaux88] Copigneaux, F., "Software Process and Product Certification", CSR Software Certification Workshop, Gatwick, September 1988.

[Deutsch88] Deutsch, M.S., Willis, R.R., Software Quality Engineering: A Total Technical and Management Approach, Prentice Hall, 1988.

[Diikstra7"] Dijkstra, E.W., "Notes on Structured Programming", in Dahl, Dijkstra and Hoare, Structured Programming, Academic Press, 1972.

[Fagan76] Fagan, M.E., "Design Code Inspections to Reduce Errors in Program Development", IBM Systems Journal, Vol. 15, No. 3, 1976.

[IEEE/729] ANSI/IEEE Std 729-1983, IEEE Standard Glossary of Software Engineering Terminology.

[Jones84] Jones, T.C., "Reusability in Programming: a survey of the state of the art", IEEE Tr. on Software Engineering, Vol. SE10, No. 5, 1984, pp. 488-493.

[Kruckeberg85] Kruckeberg, F., "Conformity Testing and Certification for Information Processing Systems", Computers & Standards, Vol. 4, 1985, pp. 21-32.

[Legge18/83] Legge N. 18/83 della Repubblica Italiana, 26 gennaio 1983.

[M-IT-03/87] CEN, CENELEC, CEPT, Memorandum M-IT-03 on Certification of Information Technology Products, 1987.

[Parnas85] Parnas, D.L., "Software Aspects of Strategic Defense Systems", Communications of ACM, Vol. 28, No. 12, 1985, pp. 26-35.

[SEJ88] IEE Software Engineering Journal, Special Section on Software Components and Reuse, Vol. 3, No. 5, September 1988.