MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	101993900329783
Data Deposito	05/11/1993
Data Pubblicazione	05/05/1995

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F		

Titolo

GENERAZIONE AUTOMATICA DI UN'ANALISI AD ALBERO DEI GUASTI FUNZIONALE DI UN SISTEMA A PARTIRE DA UNA SUA DESCRIZIONE IN ANALISI STRUTTURATA.

DESCRIZIONE dell'invenzione industriale dal titolo: "Generazione automatica di un'analisi ad albero dei guasti funzionale di un sistema a partire da una sua descrizione in analisi strutturata"

Di: CENTRO RICERCHE FIAT Società Consortile per Azioni, nazionalità italiana, Strada Torino 50, 10043 Orbassano (Torino)

Inventori designati: Massimo OSELLA, Alessandra MERIGA, Alessandro MATARAZZO

Depositata il: . . 1993 TO 93A000833

* * *

DESCRIZIONE

Campo dell'invenzione

La presente invenzione fa riferimento in generale ai procedimenti, o metodologie, per l'analisi di sistemi e più specificamente fa riferimento ai procedimenti per l'analisi di sistemi elettronici complessi atti ad individuare errori di progettazione latenti, hardware e/o software, che potrebbero causare malfunzionamenti nei sistemi stessi.

L'invenzione nasce dall'esigenza di utilizzare uno strumento di analisi di sistemi dedicato all'analisi di affidabilità e sicurezza quale l'analisi ad albero dei guasti, o Fault Tree Analysis, d'ora in poi abbreviata F.T.A., in

BM/sr

connessione con le metodologie di analisi funzionale strutturata, o Structured Analysis, di Yourdon - DeMarco, d'ora in poi abbreviata S.A., durante le fasi preliminari della progettazione di sistemi elettronici, in particolare sistemi di controllo a microprocessore, per apparecchiature destinate all'impiego veicolare.

Mediante uno strumento di questo tipo è possibile individuare, durante le varie fasi della progettazione, difetti e criticità del sistema in fase di progetto e quindi modificare il sistema stesso al fine di eliminare i difetti così individuati. Lo strumento rende quindi possibile progettare, validare e realizzare sistemi complessi aventi un elevato grado di affidabilità riducendo nel contempo i costi e la durata delle fasi di progettazione e sviluppo.

Descrizione della tecnica nota

Ne consegue la necessità primaria di analizzare le due metodologie indicate, individuarne le rispettive potenzialità e quindi determinare come queste possano interagire al fine di offrire una progettazione più accurata, realizzata mediante il supporto di analisi affidabilistiche. Nel seguito verranno sinteticamente illustrate, per una migliore comprensione, tali metodologie.

Analisi strutturata (S.A.)

Tale metodologia viene attualmente utilizzata dal progettista per definire, a partire dalle specifiche, un modello funzionale del sistema da realizzare che permetta di valutare l'operabilità del sistema stesso e ne evidenzi le principali funzionalità. Il modello viene realizzato mediante una descrizione funzionale gerarchica utilizzando una sintassi grafica definita da Yourdon - DeMarco, si veda "Structured Analysis and System Specification" di Tom DeMarco, Prentice-Hall Inc., 1979, che evidenzia il flusso dei dati (Data Flow Diagram) all'interno del sistema.

Il sistema in oggetto viene decomposto funzionalmente fino ad identificare delle funzioni elementari o nuclei elementari di elaborazione che trasformano i flussi di dati in ingresso in flussi di dati in uscita. La descrizione comportamentale delle funzioni elementari avviene attraverso l'utilizzo di pseudocodice oppure attraverso linguaggi formali di programmazione.

La modellazione del comportamento dinamico del sistema, ovvero l'evoluzione del sistema attraverso degli stati definiti a fronte di eventi, si ottiene utilizzando l'estensione alla metodologia prodotta

da Ward - Mellor, si veda "Structured Development for Real-Time Systems" di Paul Ward, Stephen Mellor, Prentice-Hall Inc. 1985, che prevede l'introduzione di flussi di controllo (o eventi del sistema) e di processi di controllo che vengono descritti attraverso delle macchine a stati (State Transition Diagram).

L'analisi viene effettuata ad un livello completamente astratto, prescindendo dalla successiva partizione che definirà quali funzioni debbano essere assolte mediante procedure software e quali mediante componentistica hardware. Questa analisi preliminare consente quindi lo studio del sistema nei diversi stati di funzionamento, onde verificare la completezza del progetto, ma non dà alcuna indicazione sul comportamento del sistema in caso di deterioramento e tantomeno evidenzia la criticità delle diverse funzioni che lo costituiscono ai fini del corretto funzionamento dell'apparato.

L'Analisi Strutturata realizza quindi lo studio di un sistema nell'ipotesi che tutte le funzioni elementari descritte al suo interno vengano assolte in modo corretto e che le informazioni fornite al sistema dall'esterno siano esatte.

Il modello prevede una scomposizione del siste-

ma in funzioni (graficamente rappresentate come bolle) ciascuna ulteriormente scomponibile in funzioni più elementari fino ad un livello di discretizzazione tale da permettere una caratterizzazione comportamentale di ciascuna funzione mediante un dato linguaggio. La caratterizzazione delle funzioni prevede unicamente il loro comportamento nominale, e prescinde da possibili errori, guasti od altre anomalie di funzionamento.

A ciascun livello, le funzioni vengono collegate mediante i dati che queste si scambiano ed i rispettivi controlli, utilizzando la logica delle macchine a stati.

Analisi dell'albero dei guasti (F.T.A.)

La F.T.A. è tra le metodologie affidabilistiche più diffusamente utilizzate nell'analisi di sistemi. La sua modalità di applicazione si riferisce tipicamente ad un sistema formato da sottosistemi e componenti fisici identificati, interagenti fra loro per dare luogo al sistema complessivo.

I concetti su cui si basa questa metodologia sono però sufficientemente generali da consentirne l'applicazione anche a sistemi concepiti come "funzioni complessive" costituite da "funzioni elementari", invece che a sistemi costituiti da componenti

fisici. Quindi tale metodologia è utilizzabile anche in fase di definizione concettuale del sistema una volta che siano state identificate le funzioni elementari componenti il sistema ovvero ne sia stata compiuta l'analisi funzionale.

In tal caso però non si possono disporre dei dati numerici (tassi di guasto) relativi alle funzioni elementari, e quindi non è possibile compiere una analisi quantitativa dell'affidabilità bensí ci si limita ad una analisi qualitativa che è comunque utile per l'identificazione delle criticità nella struttura funzionale.

Verranno analizzate ora le principali caratteristiche della F.T.A. senza peraltro entrare nella descrizione dettagliata della metodologia, si veda al riguardo "System Reliability Evaluation and Predictivity Engineering" di A. Pages, M. Gondrand, North Oxford Academic.

La F.T.A. adotta un approccio di tipo sintetico e permette di tenere presente più di un guasto alla volta, ma in modo indipendentemente dalla loro sequenza. Ciò che concerne la sinteticità piuttosto che l'esaustività può essere considerato un vantaggio dal punto di vista dell'applicabilità ma uno svantaggio dal punto di vista della completezza

dei risultati: va quindi valutato a seconda delle finalità dell'applicazione.

Un'ulteriore limitazione nella modellazione con la F.T.A. è l'impossibilità di rappresentare fenomeni di sequenzialità, priorità, parallelismo tra eventi; elementi dinamici che possono avere in realtà un notevole impatto sulle possibili conseguenze. L'unico modo di analizzare tali fenomeni attraverso la F.T.A. è la generazione di un albero di guasto per ciascuno stato di evoluzione dinamica del sistema.

Ciò comporta un notevole sforzo di modellazione a meno di disporre di strumenti automatici di supporto nella costruzione degli alberi di guasto. Inoltre la F.T.A. consente di valutare il sistema in relazione ad un solo evento indesiderato alla volta, il quale deve essere precedentemente identificato e definito.

Scopi e sintesi della presente invenzione

Lo scopo della presente invenzione è quello di realizzare uno strumento integrato ossia un procedimento, o metodologia, di analisi affidabilistica e modellazione di sistemi complessi che permetta di risolvere in modo soddisfacente le limitazioni degli strumenti, descritti in precedenza, secondo la

tecnica nota.

Secondo la presente invenzione, tale scopo viene raggiunto grazie ad un procedimento avente le caratteristiche indicate nelle rivendicazioni che seguono la presente descrizione, che prevede l'integrazione, secondo modalità che verranno descritte nel seguito, delle due metodologie, S.A. ed F.T.A., secondo la tecnica nota, sopra indicate.

Obiettivi e vantaggi dell'integrazione

Dalla descrizione dei due strumenti metodologici emergono immediatamente due aspetti che giustificano pienamente una loro integrazione:

I) la S.A. non permette l'analisi affidabilistica del sistema e l'individuazione delle funzioni critiche a cui si deve dedicare particolare attenzione durante la progettazione del sistema, tale analisi può invece essere realizzata mediante la F.T.A.;

II) sia la S.A. che la F.T.A. richiedono un modello funzionale del sistema allo studio per realizzare la loro parte di analisi, pertanto l'integrazione dei due strumenti consente il riutilizzo delle informazioni necessarie ad entrambi gli ambienti evitando la realizzazione di due modelli separati che causerebbe maggiori costi

ed il rischio di lavorare su modelli privi di coerenza.

L'integrazione tra la S.A. e la F.T.A. permette invece di effettuare, durante le fasi preliminari della progettazione in cui la caratterizzazione del sistema è molto astratta, un'analisi di affidabilità del sistema, evidenziando così le funzioni più critiche e le minime combinazioni di funzioni non assolte che degradano le funzionalità del sistema complessivo (i cosiddetti "minimal cut sets", o insiemi minimi di taglio, ricavabili dall'albero di guasto funzionale).

L'individuazione delle funzioni critiche e degli insiemi minimi di taglio consente così di orientare in modo più proficuo le fasi successive della progettazione prestando particolare cura alle funzioni rilevatesi essenziali per il sistema o addirittura riorganizzandone la struttura per ottenere insiemi minimi di taglio di ordine superiore.

Il valore aggiunto principale dell'integrazione consiste però nel minimizzare notevolmente gli sforzi di modellazione del sistema mediante l'utilizzo di una sintassi unica sia per gli aspetti funzionali che per quelli affidabilistici. Tale

semplificazione facilita lo sviluppo di un progetto in quanto consente una più chiara definizione dei problemi evitando la dispersione e la ridondanza delle informazioni, e quindi permette di abbreviare notevolmente i tempi di analisi e progetto dei sistemi. Inoltre una sintassi unica favorisce lo sviluppo di strumenti automatici computerizzati per il supporto alla progettazione dei sistemi producendo un ulteriore beneficio sulla semplicità e sui tempi di applicazione della metodologia di progetto.

Questa riduzione dei tempi nelle fasi di progetto dei sistemi elettronici, pur mantenendo una completa e approfondita analisi funzionale e affidabilistica, rappresenta un notevole vantaggio industriale.

L'Analisi Strutturata, come già detto, permette una rappresentazione gerarchica del sistema in esame, tale rappresentazione permette all'analista di sviluppare per passi successivi il modello funzionale esplodendo ogni volta ciascuna funzione in un livello successivo di maggiore dettaglio. Si ritiene che sia particolarmente vantaggiosa l'applicabilità della metodologia F.T.A. a diversi livelli di astrazione del modello, permettendo di volta in

volta la scelta del livello di dettaglio (livello della rappresentazione gerarchica) a cui effettuare l'analisi.

Il procedimento integrato secondo la presente invenzione permette facilmente la scelta del livello di analisi e può inoltre far intravedere ulteriori sviluppi nell'applicazione del procedimento, non solo a livello astratto-funzionale, ma anche nelle fasi esecutive della progettazione per le quali è già stata effettuata una ripartizione hardware/ software e sono stati identificati i componenti fisici del sistema.

A questo livello l'analisi affidabilistica consente anche la determinazione quantitativa dell'affidabilità del sistema e quindi, in base ad essa, l'ottimizzazione del progetto. Anche in questo caso vi è il vantaggio di poter mantenere lo stesso tipo di sintassi di modellazione dei sistemi, semplificando il lavoro di apprendimento dei progettisti e riducendo l'impatto dell'introduzione aziendale della metodologia.

Descrizione particolareggiata dell'invenzione

Ulteriori vantaggi e caratteristiche della presente invenzione risulteranno evidenti dalla seguente dettagliata descrizione, effettuata con

l'ausilio degli annessi disegni, forniti a titolo di esempio non limitativo, in cui:

- la figura 1 è un diagramma schematico di contesto di un sistema di climatizzazione modellato mediante la metodologia secondo la presente invenzione,
- la figura 2 è una prima espansione gerarchica del sistema di climatizzazione di figura 1,
- la figura 3 è una seconda espansione sulla funzione "Gestione-miscelazione" di figura 2,
- la figura 4 è un diagramma a stati schematico per il controllo del sistema,
- le tabelle 1A, 1B e 2A, 2B rapporesentano modelli utilizzati per le funzioni del sistema di climatizzazione,
- le figure 5A, 5B e 5C sono una rappresentazione schematica di un albero dei guasti generato secondo la presente invenzione in base al modello,
- la tabella 3 rappresenta schematicamente un insieme di taglio minimo con indici di indisponibilità, e
- la tabella 4 rappresenta schematicamente alcune criticità degli eventi primari (modi di guasto delle funzioni).

Tuttavia prima di cominciare la descrizione

dettagliata della metodologia secondo la presente invenzione verranno qui di seguito approfonditi alcuni aspetti delle due metodologie secondo la tecnica nota (S.A. ed F.T.A.) per permettere una migliore comprensione dell'integrazione che conduce alla presente invenzione.

Informazione disponibile a richiesta

Prima di entrare nel merito dell'integrazione tra le due metodologie ci si sofferma ancora sulle loro caratteristiche al fine di individuare, in modo dettagliato, l'informazione che esse gestiscono e quindi risalire al contenuto informativo comune utilizzato da entrambe. Questo permetterà di evidenziare la conoscenza disponibile in ambiente S.A. che potrà essere utilizzata dalla F.T.A., onde evitare una duplice definizione, minimizzare le possibilità di errore e mantenere la coerenza tra i due modelli.

S.A.

La metodologia S.A., come già indicato, utilizza un modello funzionale gerarchico del sistema in esame. Ciascun livello della gerarchia è caratterizzato da una struttura topologica che collega tra loro le diverse funzioni descritte (tipicamente rappresentate graficamente come bolle, vedere figure

1 a 4). Ne deriva quindi che per ciascun livello l'ambiente dispone dell'informazione relativa alle bolle in esso contenute ed alle connessioni realizzate tra le diverse bolle.

Ciascuna connessione è caratterizzata da una rappresentazione grafica che agevola la leggibilità della rappresentazione e da un identificativo che permette di accedere al tipo di informazione trasferita dalla connessione stessa (segnali o controlli). I segnali possono essere di tipo continuo oppure discreto; i controlli sono discreti ed in generale non presentano un ordine (es. [aperto|chiuso]).

Alle bolle contenute ai livelli gerarchici più profondi, per ciascun ramo, viene inoltre associato il modello comportamentale scritto dall'analista in un dato linguaggio formale o attraverso pseudocodice, a partire dalle specifiche di progetto.

Alcune bolle particolari, presenti ai diversi livelli, realizzano il ruolo di controllore, trasmettono cioè alle bolle adiacenti dei segnali per il loro controllo. La descrizione della dinamica del controllo avviene attraverso una schematizzazione a parte (State Transition Diagram) in cui si riportano i possibili stati del sistema e le possibili

transizioni tra essi, a ciascuna transizione è anche associato l'evento o il comando che induce la transizione.

F.T.A.

L'analisi affidabilistica F.T.A., deve essere compiuta a partire da una descrizione fisica del sistema. Normalmente tale descrizione viene fornita su un modello piatto del sistema. Ovvero, il modello è costituito da un insieme di oggetti (i componenti) collegati da un certo numero di connessioni fisiche (linee elettriche, idrauliche, pneumatiche, ecc.).

Nell'utilizzo qui previsto la F.T.A. viene applicata a livello funzionale, ovvero i componenti fisici sono le funzioni elementari e le connessioni fisiche sono il flusso di informazioni; senza però alterare la natura dell'analisi. La sola informazione globale è rappresentata dalla struttura topologica che indica come i diversi componenti sono collegati tra di loro e con i sistemi periferici.

Ciascun componente rappresenta un "oggetto", caratterizzato da un set di attributi che ne descrivono le proprietà quali il suo comportamento, i suoi modi di guasto, i parametri affidabilistici e di progetto, e tutte le informazioni che possono rendersi necessarie per l'analisi da effettuare.

Ai fini della costruzione degli alberi di guasto e della loro analisi, le informazioni necessarie risultano essere:

- la struttura topologica del sistema;
- la lista dei componenti che lo costituiscono e per ciascuno di essi:
  - il nome;
  - la lista dei modi di guasto;
  - la lista dei parametri affidabilistici (rateo di guasto, rateo di riparabilità, intervallo di test, indisponibilità su domanda) per ciascun modo di guasto (opzionali per l'analisi qualitativa);
  - il modello logico di comportamento nominale e degradato;
  - lo stato del componente assunto per l'analisi in corso.

Gli attributi citati sono quelli che risultano indispensabili per un'analisi affidabilistica quantitativa, ciò non esclude che l'analista possa aggiungere altri attributi che permettano di arricchire la rappresentazione.

Per quanto riguarda lo stato del componente, va ricordato che la metodologia degli alberi di guasto è, come già detto in precedenza, di tipo statico

ossia permette l'analisi del sistema in un particolare stato di funzionamento (o fase operazionale) oppure durante la transizione tra due stati successivi, ma non è in grado di studiarne la dinamica di comportamento. Per tale motivo, prima di effettuare la costruzione dell'albero dei guasti, è necessario fissare lo stato di tutti i componenti al fine di determinare in modo univoco lo stato del sistema complessivo.

Dalle indicazioni riportate emergono le caratteristiche essenziali che differenziano le due metodologie:

- la S.A. utilizza un modello gerarchico mentre la F.T.A. lavora con un modello piatto;
- la S.A. effettua un'analisi anche del comportamento dinamico del sistema mentre la F.T.A. effettua l'analisi per una particolare configurazione del sistema;
- la S.A. analizza esclusivamente il comportamento nominale del sistema (in assenza di guasti o errori) mentre la F.T.A. analizza esclusivamente il comportamento degradato del sistema (in presenza di guasti o errori).

Nonostante tali differenze, esse presentano anche diverse caratteristiche comuni:

- entrambe rappresentano il modello funzionale topologico del sistema ottenuto mediante un certo numero di oggetti (bolle o componenti) interconnessi da flussi;
- entrambe le metodologie prevedono un modello di comportamento nominale del sistema. A questo proposito va notato che la S.A. descrive un modello funzionale quantitativo, espresso cioè mediante descrizione algoritmica delle funzioni elementari e definizione della tipologie dei dati, mentre nella F.T.A. è necessario un modello logico qualitativo, descritto da linguaggi logici a regole e sostenuto da tipologie di dati discretizzati;

La presenza di informazioni comuni giustifica pienamente l'integrazione in oggetto.

La soluzione integrata

Il procedimento, o metodologia, integrato secondo la presente invenzione in sostanza permette l'analisi affidabilistica del sistema modellato in S.A. mediante l'utilizzo della tecnica F.T.A.. La realizzazione di tale analisi richiede essenzialmente quattro fasi (si veda la Tabella delle Fasi, riportata qui di seguito), la prima dedicata alla analisi funzionale del sistema (attraverso la S.A.),

la seconda relativa al trasferimento del modello in ambito F.T.A., la terza per definire gli scenari dinamici per i quali l'affidabilità del sistema deve essere studiata ed infine la quarta ed ultima per effettuare l'analisi affidabilistica secondo la F.T.A. propriamente detta.

Le prime tre fasi possono essere effettuate un'unica volta per ciascun sistema da analizzare, queste realizzano un modello e più scenari che possono poi essere utilizzati ripetutamente per effettuare le diverse analisi di affidabilità richieste per lo studio del sistema al variare dell'evento principale, o evento top, dello scenario per il quale si realizza l'analisi e così via. Eventualmente si può ripetere anche la terza fase qualora si vogliano studiare scenari nuovi non previsti durante la preparazione del modello. Nel seguito si entrerà nel merito delle diverse fasi, indicando le singole attività che queste prevedono.

Tabella delle Fasi

Fase 1. - Realizzazione del modello funzionale in S.A.

Fase 2. - Realizzazione di un modello affidabilistico necessario per la F.T.A.

F2.1. - Discretizzazione delle deviazioni

dei segnali e dei controlli

F2.2. - Traduzione dei modelli di comportamento nominale delle funzioni

F2.3. - Trasferimento della rappresentazione gerarchica del sistema

F2.4. - Introduzione dei modi di guasto e relativi modelli di comportamento

Fase 3. - Definizione degli scenari di analisi

Fase 4. - Definizione dell'analisi affidabilistica

F4.1 - Scelta del livello di dettaglio (profondità nella gerarchia)

F4.2 - Definizione dell'evento top

F4.3 - Scelta dello stato del sistema

F4.4 - Costruzione dell'albero dei guasti

F4.5 - Analisi dell'albero dei guasti

Fase 1: Realizzazione del modello funzionale in S.A.

Deve essere compiuta seguendo la metodologia S.A. (si vedano i già citati testi di DeMarco e di Ward-Mellor) per la modellazione delle funzionalità, del flusso di dati e della dinamica del sistema.

Fase 2: Realizzazione del modello affidabilistico

In pratica è la fase di conversione del modello secondo la S.A. nel modello secondo la F.T.A. ed è suddivisa in quattro sottofasi.

F2.1 La fase di modellazione prevede innanzi tutto la scelta relativa alla discretizzazione delle variabili (segnali o controlli) gestite dal sistema, ed in particolare la discretizzazione delle loro deviazioni rispetto ai valori assunti nominalmente per una data configurazione (stato) del sistema. Tale discretizzazione permette lo studio del comportamento deteriorato del sistema a seguito di funzioni non assolte o deviazione nei segnali provenienti dall'ambiente esterno. Ad esempio il dato "temperatura" di tipo intero limitato nel range da [-30,+120] nella S.A., viene discretizzato su due valori di deviazione [high, low] con il seguente significato: high, identifica una deviazione, dovuta ad un guasto, del segnale "temperatura" verso valori più elevati di quello nominale (in dipendenza del particolare stato in cui si trova il sistema); viceversa low, identifica deviazioni verso valori inferiori a quello nominale.

F2.2 La discretizzazione risulta necessaria per il passo successivo che prevede la traduzione dei modelli di comportamento nominale quantitativi in modelli di comportamento nominale qualitativi, adatti per l'analisi affidabilistica. Questi modelli servono per comprendere come le funzioni elementari

corrette propagano, nella loro trasformazione di dati, una deviazione presente sui dati in ingresso. Ad esempio per una funzione con due ingressi A e B e una uscita C definita come C = A/B, una deviazione high sul segnale A, provoca una deviazione high anche sul segnale C; mentre la stessa deviazione high sul segnale B, provoca una deviazione low su C; viceversa capita con deviazioni low. Tale traduzione deve essere effettuata per ciascuna funzione presente ai livelli del modello gerarchico S.A. per i quali si intende realizzare la costruzione dell'albero di guasto.

F2.3 La modellazione prosegue con il trasferimento dell'informazione topologica contenuta nel modello S.A. in una analoga utilizzabile dalla F.T.A.. Ovvero attraverso una trasformazione della rappresentazione gerarchica strutturata del sistema in una rappresentazione piatta dove tutte le connessioni tra i componenti vengono esplicitate e propagate. Tale trasformazione non deve necessariamente produrre un modello topologico piatto rappresentabile graficamente, in quanto ciò porterebbe notevoli problemi di sbrogliatura delle connessioni. È sufficiente l'informazione, anche tabellare, delle connessioni logiche tra tutte le funzioni.

F2.4 L'ultima attività richiesta è la definizione dei modi di guasto per ciascuna funzione. La definizione dei modi di guasto può essere data attraverso regole "IF - THEN" che esprimano il valore di deviazione dei dati in uscita in relazione ai diversi modi di guasto possibili della funzione, ai valori dei dati in ingresso e allo stato del sistema. Con questa informazione si identificano le deviazioni dei segnali in uscita della funzione a fronte dei possibili modi di guasto interni alla funzione stessa, supponendo corretti i dati in ingresso. Tale operazione deve essere realizzata per tutte le funzioni che appartengono ai livelli del modello gerarchico che verranno analizzati in fase di costruzione automatica dell'albero di guasto. Inoltre possono essere introdotti gli eventuali parametri affidabilistici (ratei di guasto, indisponibilità su domanda, intervalli di test e ratei di riparazione) utili per una analisi affidabilistica quantitativa.

Fase 3: Definizione degli scenari di analisi

La terza fase richiesta per l'analisi del sistema è la definizione degli scenari di studio intesi come successioni di stati del sistema per le quali si desidera effettuare l'analisi affidabili-

stica. Va infatti ricordato che per l'analisi di affidabilità mediante alberi di guasto deve essere definito un ben preciso stato di funzionamento del sistema e che per ottenere un'analisi affidabilistica completa è necessario studiare tutti gli stati attraversati dal sistema durante il suo funzionamento. Nella F.T.A tradizionale la selezione dello stato del sistema viene compiuta implicitamente da chi realizza l'analisi, avendo esso in mente un particolare modo di funzionamento. In un'ottica di integrazione delle metodologie si può invece pensare di riutilizzare l'informazione disponibile nella S.A. che prevede la definizione di diagrammi di transizione degli stati per la modellazione dell'evoluzione dinamica del sistema. Utilizzando tali modelli è infatti possibile individuare automaticamente i diversi stati di funzionamento assunti dal sistema, e quindi individuare lo scenario comportamentale dell'evoluzione corretta del sistema riducendo notevolmente l'impegno dell'analista.

Fase 4: L'analisi affidabilistica

Quest'ultima fase realizza l'analisi affidabilistica vera e propria. Si compone di 5 sottofasi più elementari che prevedono:

F4.1 La definizione del livello di dettaglio a cui

effettuare l'analisi, tale operazione permette all'analista di scegliere per ciascun ramo della rappresentazione gerarchica il livello che si intende considerare per la costruzione dell'albero di guasto. Ciò è utile per permettere all'analista una maggiore flessibilità di analisi ed approfondire l'affidabilità la dove siano già state identificate delle funzioni critiche per la sicurezza.

F4.2 La definizione dell'evento top che si intende studiare mediante l'albero di guasto. Essa avviene tramite la specificazione della deviazione di un dato, tipicamente di un dato in uscita del sistema.

F4.3 La definizione dello stato del sistema. Ciò significa l'identificazione di tutti i valori dei segnali di controllo interni al sistema relativi allo specifico stato che si desidera analizzare. Lo stato scelto deve essere tra quelli identificati nella Fase 3.

F4.4 Costruzione dell'albero dei guasti. Dopo aver effettuato tutte le precedenti fasi, tutte le informazioni necessarie per la costruzione dell'albero risultano formalizzate e facilmente accessibili. La costruzione dell'albero risulta pertanto molto semplificata e facilmente implementabile attraverso procedure automatiche

supportate da elaboratore.

F4.5 L'ultima fase della metodologia descritta è l'analisi dell'albero costruito. Questa si svolge nel modo tradizionale secondo la metodologia F.T.A. (si veda il già citato testo di Pages e Gondrand) e consente sia l'analisi qualitativa con il calcolo dei minimal cut set e dell'indice di criticità dei componenti, che l'analisi quantitativa con il calcolo dell'indisponibilità dell'evento top e della probabilità associata a ciascun cut set. Le prime tre operazioni citate possono essere svolte nell'ordine dettato dal tipo di analisi che si intende effettuare, a seconda che si desideri analizzare lo stesso evento top per più configurazioni del sistema oppure si intenda verificare come il livello di dettaglio dell'analisi incida sul risultato o ancora che si desideri esaurire l'analisi per una stessa configurazione del sistema analizzando eventi top differenti.

La progettazione di sistemi elettronici è ormai, anche a livello industriale, assistita da alcune metodologie di progetto supportate da strumenti automatici (CAE/CASE, Computer Aided Engineering, Computer Aided Software Engineering). La tendenza evolutiva di tali strumenti e

metodologie porta verso una maggiore accuratezza dello sforzo progettativo nelle fasi alte dello sviluppo. Ovvero l'investimento in termini di mezzi e risorse nella realizzazione di sistemi elettronici si sposta dalla fase implementativa a quella del progetto funzionale.

La metodologia qui descritta si colloca in questa fase di progetto funzionale di un sistema. In tale fase progettuale è indispensabile studiare e assestare le logiche funzionali del sistema in questione ma è altresì importante definire l'architettura affidabilistica del sistema necessaria a soddisfare i requisiti di sicurezza.

Al momento attuale esistono metodologie per l'analisi degli aspetti funzionali di un sistema (quali la S.A.) e metodologie per l'analisi affidabilistica (quali la F.T.A.). La metodologia qui descritta propone di analizzare congiuntamente i due aspetti partendo da una sintassi comune. I vantaggio evidente che una tale integrazione apporta è la riduzione delle fasi di modellazione funzionale e affidabilistica del sistema in un unico modello che considera entrambi gli aspetti.

Ciò permette una riduzione complessiva dei tempi di analisi del sistema e mantiene la coerenza

tra le analisi dei diversi aspetti. Si pensi, per comprendere l'importanza di questi vantaggi, alle frequenti modifiche della struttura funzionale che avvengono durante la fase di assestamento delle specifiche dovute ad esempio alle interazioni tra cliente e fornitore del sistema.

Inoltre la modellazione di un sistema con un unica sintassi che sia in grado di soddisfare le esigenze di diversi tipi di analisi consente una più facile automatizzazione della metodologia attraverso strumenti di calcolo, e permette la crescita di tali strumenti verso un ambiente progettativo unificato in cui il progettista abbia facilmente sottomano, in forma coerente e facilmente aggiornabile, tutti gli aspetti riguardanti lo sviluppo di un nuovo sistema.

Esempio applicativo

Per una migliore comprensione di quanto descritto finora verrà ora fornito, con riferimento anche alle figure 1 a 5C ed alle tabelle 1A a 4, un esempio applicativo della metodologia secondo la presente invenzione per lo studio affidabilistico del sistema di controllo di un sistema di climatizzazione per autoveicoli.

L'esempio non intende esaurire le possibilità di impiego della metodologia secondo l'invenzione,

bensì illustrare le diverse fasi dell'analisi, i criteri di modellazione del sistema e dei componenti o funzioni che lo costituiscono e quindi indicare i risultati ottenibili. Per questa ragione non si è data particolare importanza né alla completezza del modello né tantomeno alla correttezza del modello di comportamento delle singole funzioni, si sono invece illustrate nel dettaglio tutte le potenzialità modellistiche della metodologia e gli aggiornamenti che questa richiede per l'utilizzo sopra indicato.

Modellazione del sistema

L'esempio che si vuole considerare è un sistema di controllo elettronico per un impianto di climatizzazione di autovetture. Il sistema legge in ingresso i valori di alcuni sensori (temperatura ambiente, temperatura esterna, irraggiamento solare, ecc.) e pilota, in funzione di una determinata strategia di controllo, i diversi dispositivi meccanici e/o elettrici di attuazione (movimentazione delle portelle di climatizzazione, ventilatore, compressore, ecc.).

Realizzazione del modello funzionale in S.A.

Nelle figure 1, 2, 3 e 4 viene riportata l'Analisi Strutturata del sistema Climatizzatore. Si può osservare la struttura gerarchica della descri-

zione funzionale a partire dal diagramma di contesto in fig. 1, scendendo nel dettaglio della descrizione nelle fig. 2 e 3. In fig. 4 è rappresentato il diagramma a stati che descrive il comportamento dinamico del sistema di controllo a fronte dell'evoluzione degli eventi.

Per semplicità si è riportata la descrizione riguardante la sola funzionalità di "Gestione_miscelazione" e si sono trascurate le altre funzionalità del sistema. La sintassi usata per questa modellazione è naturalmente quella descritta da Yourdon e DeMarco aumentata con le estensioni dovute a Ward e Mellor.

Realizzazione del modello affidabilistico

Oltre alla descrizione del modello topologico del sistema (avvenuta nella fase 1) l'analisi affidabilistica necessita di una descrizione dei modi di guasto di ciascun componente o funzione descritta, dei parametri affidabilistici, dei modelli di propagazione dei guasti all'interno delle singole funzionalità e della descrizione dello stato in cui si trova il sistema al momento dell'analisi. Nelle tabelle 1A, 1B e 2A, 2B vengono riportati i modelli utilizzati nell'applicazione pilota del climatizzatore. Di seguito viene descritto il

significato di ciascun campo descritto nella tabella.

Per ciascun componente o funzione nella tabella viene riportato:

- nome: il nome dell'oggetto, utilizzato per identificare la funzione od il componente nell'ambito del modello;
- descrizione: un testo di descrizione della funzione realizzata;
- ingressi: l'elenco dei segnali in ingresso al componente od alla funzione, caratterizzati ciascuno da un numero d'ordine, un tipo (segnale/controllo) e dalle possibili deviazioni che il segnale od il controllo può assumere in seguito a guasti esterni all'oggetto;
- uscite: l'elenco dei segnali in uscita dal componente o dalla funzione, caratterizzati ciascuno da un numero d'ordine, un tipo (segnale/controllo) e dalle possibili deviazioni che il segnale od il controllo può assumere in seguito a guasti interni all'oggetto;
- stati di funzionamento: l'elenco dei possibili stati di funzionamento di una funzione o di un componente, selezionabili mediante gli ingressi di controllo;

- stato nominale: uno degli stati indicati al punto precedente in cui la funzione dovrebbe trovarsi in caso di corretto funzionamento del sistema per la fase operazionale in esame (si ricordi che l'albero dei guasti è una metodologia statica che permette l'analisi di una particolare fase operazionale predefinita o della transizione tra una fase predefinita e la successiva);
- modello comportamentale: un modello rappresentabile attraverso delle regole di produzione, cioè regole del tipo "IF-THEN", che pone in relazione le deviazioni dei segnali o controlli in ingresso ai componenti con le deviazioni dei segnali o controlli in uscita, in funzione dello stato di funzionamento e del modo di guasto della funzione o del componente;
- modelli di guasto: un modello rappresentabile attraverso delle regole logiche del tipo "IF-THEN" che descriva i guasti caratteristici del componente o della funzione in oggetto.

Gli attributi citati sono essenziali per la costruzione dell'albero dei guasti e per l'analisi dello stesso. Come accennato in precedenza si ricorda che i modelli comportamentali introdotti

nell'esempio sono puramente indicativi, e quindi non rappresentano effettivamente il comportamento del sistema, ma in ogni caso illustrano il tipo di informazione che l'analista deve fornire per realizzare il modello.

Di seguito si indicano alcune osservazioni relative ai modelli riportati nelle tabelle 1A, 1B.

- Le connessioni tra le funzioni sono state suddivise in due principali categorie: i segnali ed i controlli; si è quindi supposta un'unica possibile deviazione per i controlli (controllo falso) e due deviazioni per i segnali (high e low) che stanno ad indicare lo scostamento assunto rispetto ai valori che si avrebbero qualora tutto l'apparato funzionasse correttamente.
- I possibili stati di ciascuna funzione sono stati ottenuti mediante combinazione dei valori assunti dagli ingressi di controllo di ciascuna bolla (si veda l'esempio relativo alla funzione Gest-dist).
- Nell'esempio si è assunto in generale un unico modo di guasto per motivi di semplicità, nonostante ciò non esiste un limite a tal numero; a titolo di esempio si è supposto che la fun-

zione Calc-tt ammetta due possibili modi di guasto: un errore in eccesso (/errore_+) ed un errore in difetto (/errore_-).

- I modelli comportamentali introdotti possono essere classificati in modelli di comportamento nominale e in modelli di comportamento dedicati al componente guasto. I modelli di comportamento nominale mettono in relazione le deviazioni delle variabili di ingresso con le deviazioni delle variabili di uscita come indicato nelle prime tre regole relative alla funzione Gest_dist, i modelli relativi al comportamento a seguito di guasti presentano sempre dei modi di guasto nell'antecedente della regola e ne indicano le conseguenze in termini di deviazioni delle variabili (segnali o controlli) in uscita alla funzione.
- Sempre in riferimento alla modellazione comportamentale si fa notare come sia possibile aumentare il potere descrittivo del modello mediante l'utilizzo di condizioni (c: $DefaultPos ...): tali condizioni indicano il contesto in cui può essere applicata la regola a cui tali condizioni sono associate (esempio: la prima regola relativa al comportamento

nominale della funzione Calc_tt potrà essere applicata solo qualora lo stato nominale per cui si realizza l'analisi è "vent" e non potrà essere applicata in altri contesti).

Quanto indicato illustra, anche se in modo molto sintetico, le peculiarità modellistiche dell'approccio ed indica i dati necessari per effettuare l'analisi di affidabilità a livello funzionale onde determinare le funzioni critiche per il sistema in esame.

Definizione degli scenari di analisi

Dalla figura 4 sono ricavabili gli stati in cui evolve il sistema, in caso di corretto funzionamento, a seguito di eventi esterni quali l'intervento dell'utente su alcuni tasti o il disinserimento del sistema da chiave. Nell'esempio si è considerato il funzionamento corretto del sistema unicamente nello stato denominato "acceso" e sono state considerate le deviazioni da questo stato dovute ad alterazioni erronee dei segnali di controllo.

L'analisi affidabilistica

Il livello di dettaglio scelto per l'analisi affidabilistica è stato in questo caso lo stesso livello raggiunto della descrizione in Analisi Strutturata.

L'evento top definito nell'analisi è stato lo studio dell'eccessiva apertura della portella di miscelazione. L'evento top in questione è stato espresso secondo la sintassi descritta come:
valore high sul segnale di uscita della funzione Calc_apm .

La propagazione dell'evento attraverso il sistema, seguendo il modello affidabilistico descritto, ha permesso la costruzione dell'albero di guasto che è riportato nelle figure 5A, 5B e 5C. Va osservato che l'albero è strettamente correlato ai modelli comportamentali associati alle funzioni e pertanto anch'esso è del tutto indicativo e non rispondente ai requisiti di una reale analisi del sistema climatizzatore.

Sono stati introdotti successivamente dei dati affidabilistici per gli eventi relativi al contorno del sistema e quindi si è effettuata anche l'analisi quantitativa dell'affidabilità. I risultati ottenuti sono riportati nelle tabelle 3 e 4. Nella tabella 3 sono riportati i dati relativi all'albero ed i risultati ottenuti con l'elenco degli insiemi minimi di taglio e l'indisponibilità degli eventi al tempo di missione fissato pari a 8760 h (1 anno). In totale sono stati ottenuti dieci insiemi minimi di

taglio di cui nove di ordine 1 ed uno di ordine 2.

Nella tabella 4 si riporta l'elenco degli eventi di guasto primari con l'indice di criticità calcolato.

Trattandosi di un'analisi ad un livello di rappresentazione del sistema molto astratto (modello funzionale), la determinazione della criticità degli eventi primari (modi di guasto delle funzioni) risulta essere l'informazione più interessante in quanto individua in modo inequivocabile le funzioni che presentano un ruolo determinante per il corretto funzionamento del sistema.

Da quanto precede risultano quindi evidenti i vantaggi e le potenzialità del procedimento secondo la presente invenzione per ridurre i tempi ed i costi di progettazione industriale, oggigiorno piuttosto rilevanti, dei sistemi elettronici.

Naturalmente, fermo restando il principio dell'invenzione, i particolari di realizzazione e le forme d'attuazione potranno essere ampiamente variati rispetto a quanto descritto ed illustrato, senza per questo uscire dall'ambito della presente invenzione.

RIVENDICAZIONI

1. Procedimento per effettuare un'analisi di affidabilità di un sistema elettronico, detto sistema elettronico impiegando una specifica configurazione fisica ed operando in base a specifiche procedure operative, caratterizzato dal fatto che comprende le seguenti fasi:

- rappresentare detto sistema in modo funzionale mediante una metodologia del tipo analisi strutturata,
- generare un modello di analisi affidabilistica, secondo una metodologia del tipo ad albero dei guasti, in base a detta rappresentazione funzionale,
- effettuare un'analisi affidabilistica di detto albero dei guasti in vista di rilevare condizioni di uscita critiche di detto sistema,
- modificare detta specifica configurazione fisica e/o dette specifiche procedure operative in vista di eliminare dette condizioni di uscita critiche,

dette fasi essendo automatizzate mediante l'impiego di un elaboratore elettronico.

2. Procedimento secondo la rivendicazione 1, caratterizzato dal fatto che detta fase di rappresentare detto sistema in modo funzionale, secondo detta metodologia del tipo analisi strutturata, comprende

la fase di rappresentare detta specifica configurazione fisica e dette specifiche procedure operative utilizzando una medesima sintassi.

3. Procedimento secondo la rivendicazione 2, caratterizzato dal fatto che detta metodologia del tipo analisi strutturata è una metodologia del tipo Yourdon-DeMarco e Ward-Mellor.

4. Procedimento secondo una qualsiasi delle rivendicazioni 1 a 3, caratterizzato dal fatto che detta rappresentazione funzionale di detto sistema comprende informazioni scelte nel gruppo costituito da:

- la struttura topologica di detto sistema,
- la lista di componenti costituenti detto sistema e per ciascuno di essi:
  - un nome,
  - una lista dei modi di guasto,
  - una lista di parametri affidabilistici per ciascun modo di guasto,
  - un modello logico di comportamento nominale e degradato,
  - lo stato del componente assunto per l'analisi in corso.

5. Procedimento secondo la rivendicazione 3 o la rivendicazione 4, caratterizzato dal fatto che detta

fase di generare un modello di analisi affidabilistica comprende le fasi di:

- discretizzare variabili gestite dal sistema,
- convertire modelli di comportamento nominale quantitativi di detto sistema in modelli di comportamento nominale qualitativi,
- trasformare una rappresentazione gerarchica funzionale di detta specifica configurazione fisica di detto sistema in una rappresentazione connettiva esplicita di detta specifica configurazione fisica,
- generare una pluralità di modi di guasto per almeno parte di elementi di detta rappresentazione funzionale di detto sistema.

6. Procedimento secondo la rivendicazione 5, caratterizzato dal fatto che detta fase di effettuare un'analisi affidabilistica di detto albero dei guasti comprende la fase di generare una pluralità di scenari di analisi, ognuno di detti scenari di analisi essendo corrispondente ad un differente stato di detto sistema.

7. Procedimento secondo la rivendicazione 6, caratterizzato dal fatto che detta fase di generare una pluralità di scenari di analisi viene effettuata in modo automatico in base a diagrammi di transizione di stato facenti parte di detta rappresentazione

funzionale di detto sistema.

8. Procedimento secondo la rivendicazione 6 o la rivendicazione 7, caratterizzato dal fatto che detta fase di generare una pluralità di scenari di analisi comprende la fase di generare uno scenario di analisi per ogni stato di detto sistema.

9. Procedimento secondo una qualsiasi delle rivendicazioni 6 a 8, caratterizzato dal fatto che detta fase di effettuare un'analisi affidabilistica di detto albero dei guasti comprende inoltre le fasi di:

- definire un livello di dettaglio per detta analisi affidabilistica,
- definire una pluralità di eventi principali da studiare mediante detta analisi affidabilistica,
- identificare, per ogni stato del sistema, il valore di tutti i segnali di controllo di detto sistema,
- costruire almeno un albero dei guasti,
- analizzare detto almeno un albero dei guasti mediante una metodologia del tipo ad analisi ad albero dei guasti.

10. Procedimento secondo la rivendicazione 9, caratterizzato dal fatto che detta fase di costruire almeno un albero dei guasti comprende la fase di

costruire un albero dei guasti per ogni evento principale.

11. Procedimento secondo la rivendicazione 9 o la rivendicazione 10, caratterizzato dal fatto che detta fase di costruire almeno un albero dei guasti comprende la fase di costruire un albero dei guasti per ogni scenario di analisi generato.

12. Procedimento secondo una qualsiasi delle rivendicazioni 9 a 11, caratterizzato dal fatto che detta fase di analizzare detto almeno un albero dei guasti comprende la fase di identificare almeno una funzione critica di detto sistema.

13. Procedimento secondo la rivendicazione 12, caratterizzato dal fatto che detta fase di analizzare detto almeno un albero dei guasti comprende la fase di identificare tutte le funzioni critiche di detto sistema.

14. Procedimento secondo una qualsiasi delle rivendicazioni 9 a 13, caratterizzato dal fatto che detta fase di analizzare detto almeno un albero dei guasti comprende la fase di identificare almeno un insieme minimo di taglio di detto sistema.

15. Procedimento secondo la rivendicazione 14, caratterizzato dal fatto che detta fase di analizzare detto almeno un albero dei guasti comprende la fase

di identificare tutti gli insiemi minimi di taglio di detto sistema.

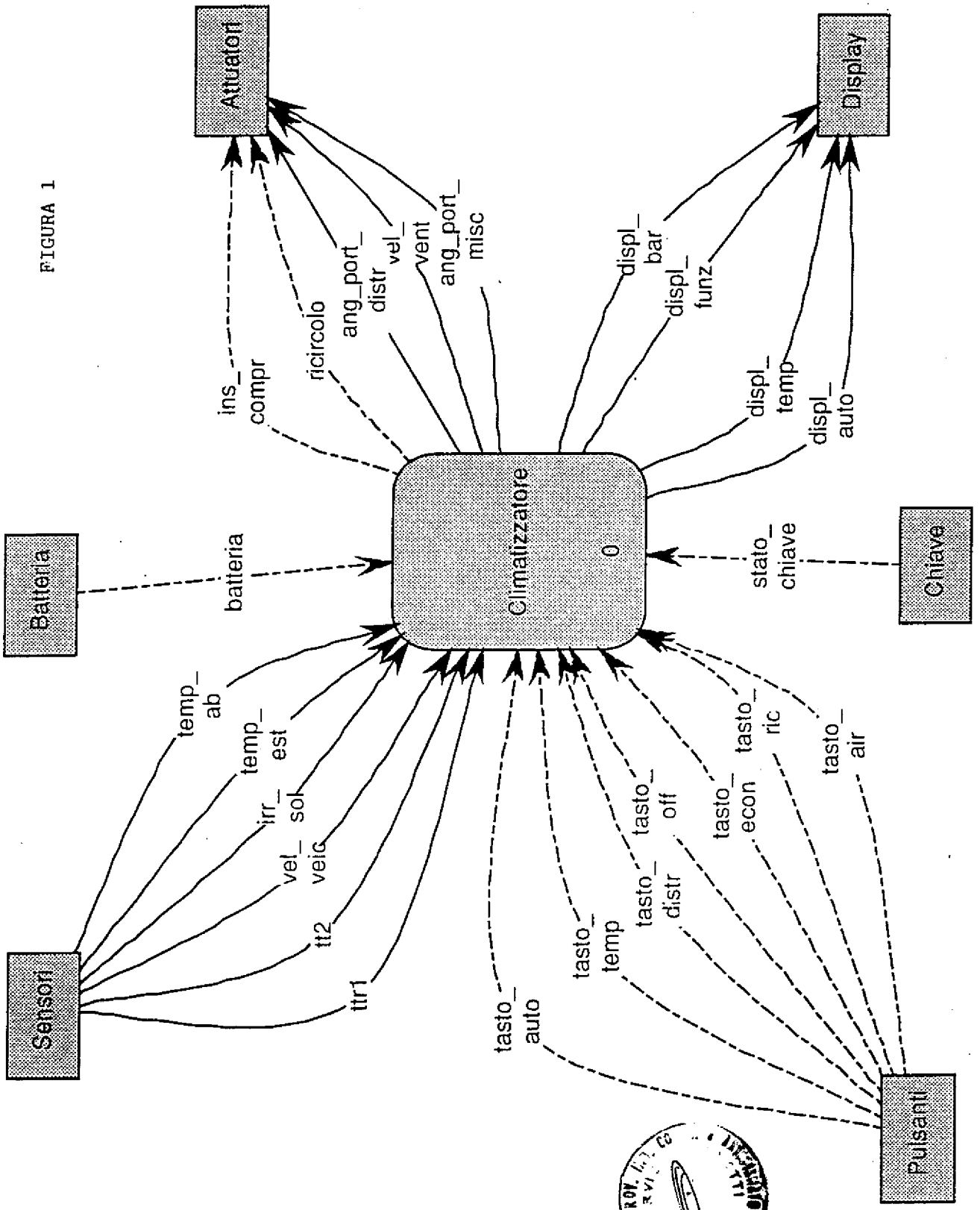
16. Procedimento secondo le rivendicazioni 13 e 15, caratterizzato dal fatto che detta fase di modificare detta specifica configurazione fisica e/o dette specifiche procedure operative comprende la fase di ridurre dette funzioni critiche ed aumentare detti insiemi minimi di taglio.

Il tutto sostanzialmente come descritto ed illustrato e per gli scopi specificati.

PER INCARICO

Dott. Francesco CERRA
N. Iscriz. 430 BM
(In proprio e per gli altri)

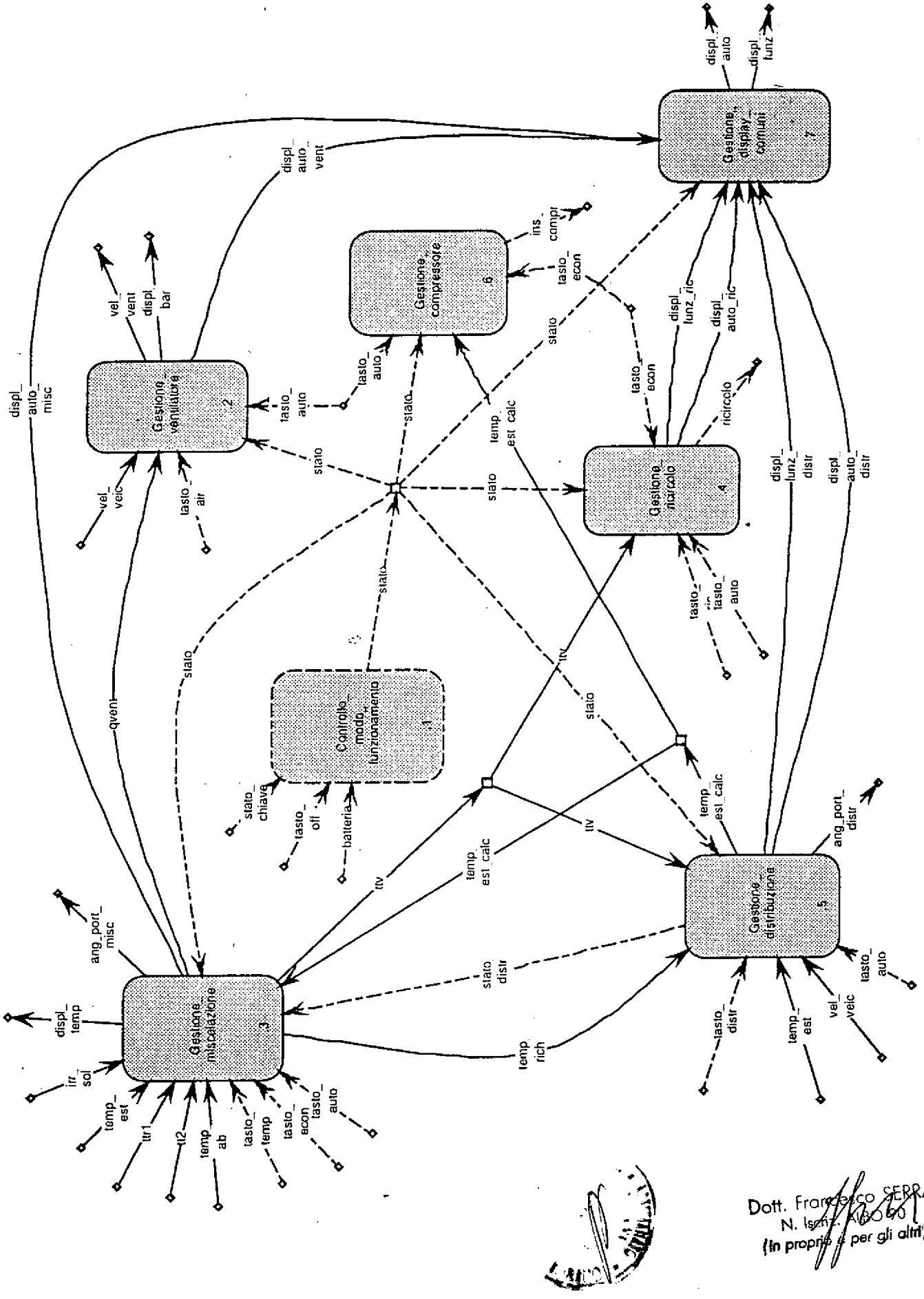
FIGURA 1



Dott. Francesco SERRA
N. Iscriz. ALBO 90
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

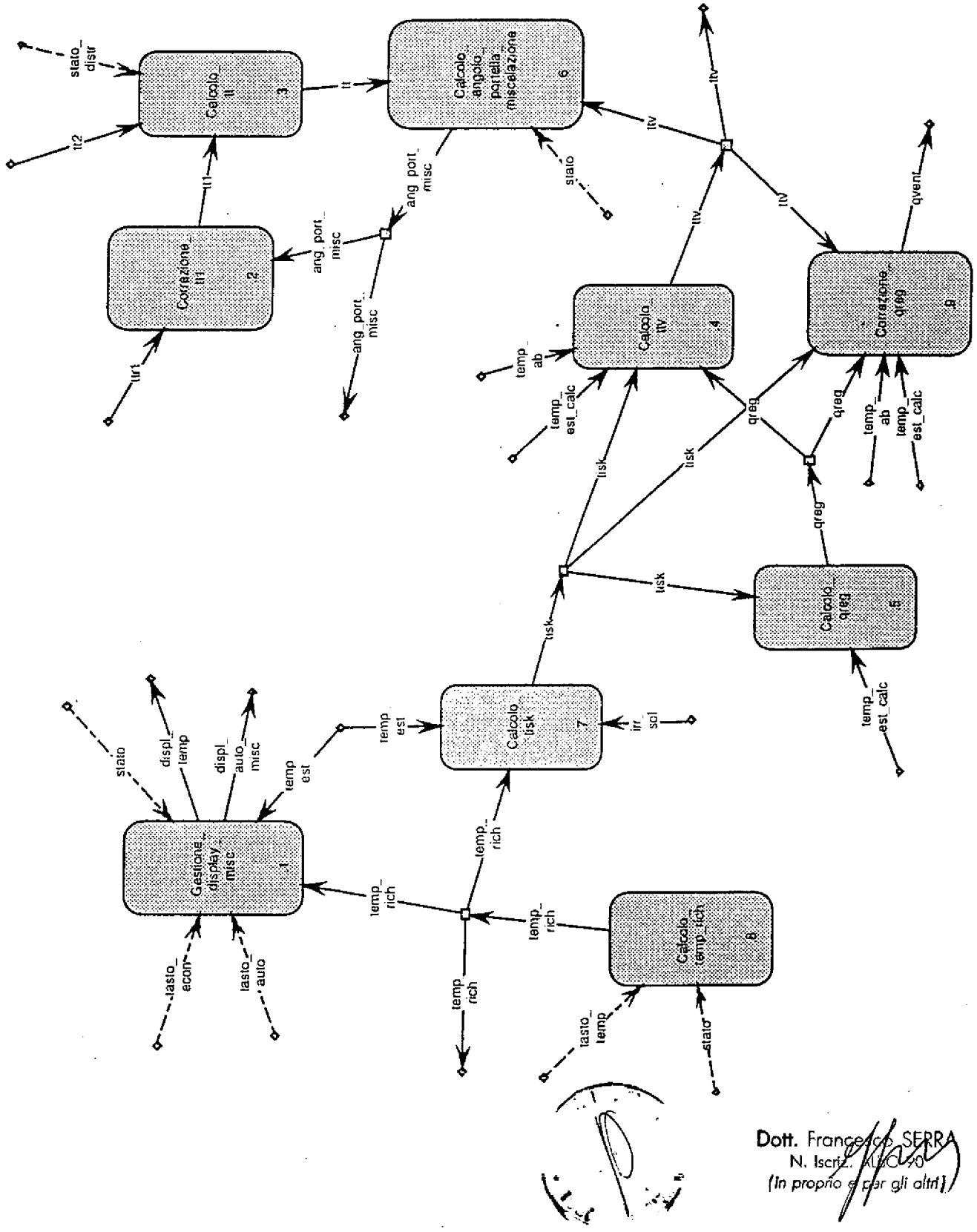
FIGURA 2



Dott. Francesco SERRA
N. Iscr. 430660
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

FIGURA 3



Dott. Francesco SERRA
N. Iscriz. [illegible]
(In proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

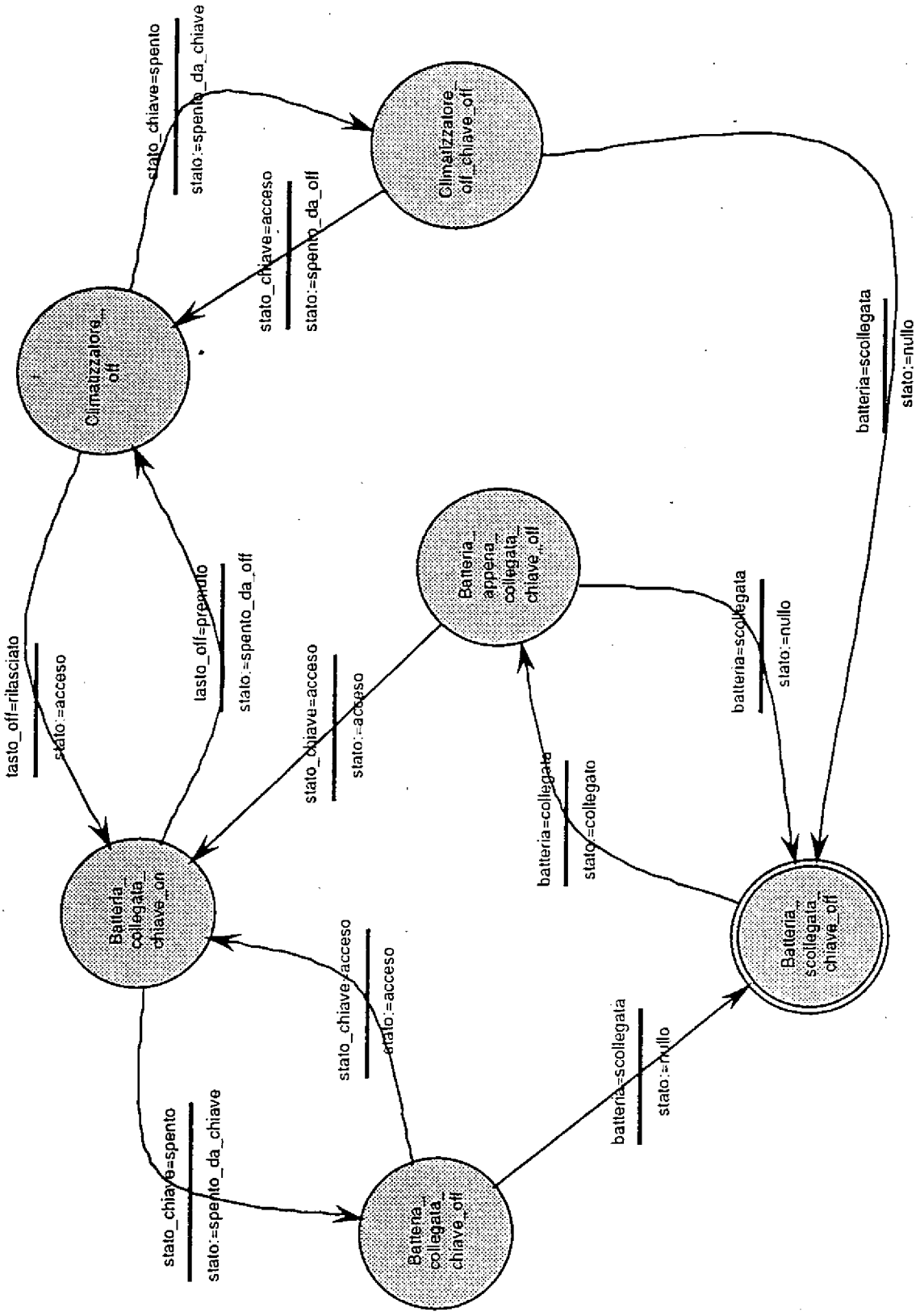


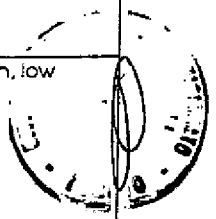
FIGURA 4

Dott. Francesco SERRA
N. Iscriz. Albo 98
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

TABELLA 1A

Funzione		Ingressi				Uscite			
Nome	Descrizione	ID	Nome	Tipo	Deviazione	ID	Nome	Tipo	Deviazione
Gest_dist	Gestione distribuzione	1	tasto_auto	ctrl	falso	9	stato_distr	ctrl	falso
		2	vel_veic	segnale	high				
		3	temp_est	segnale	high, low				
		4	tasto_distr	ctrl	falso				
		5	temp_rich	segnale	high, low				
		6	ttv	segnale	high, low				
		7	stato	ctrl	falso				
Ctrl_funz	funzionamento	1	stato_chiave	ctrl	falso	9	stato	ctrl	falso
		2	tasto_off	ctrl	falso				
		3	batteria	ctrl	falso				
Corr_tt1	Correzione tt1	1	ttr1	segnale	high, low	9	tt1	segnale	high, low
		2	ang_port_misc	segnale	high, low				
Calc_tt	Calcolo tt	1	ttr1	segnale	high, low	9	tt	segnale	high, low
		2	tt2	segnale	high, low				
		3	stato_distr	ctrl	falso				
Calc_apm	Calcolo angolo poteella misc.	1	tt	segnale	high, low	9	ang_port_misc	segnale	high, low
		2	ttv	segnale	high, low				
		3	stato	ctrl	falso				
Calc_ttv	Calcolo ttv	1	temp_ab	segnale	high, low	9	ttv	segnale	high, low
		2	temp_est_calc	segnale	high, low				
		3	tisk	segnale	high, low				
		4	qreg	segnale	high, low				
Calc_qreg	Calcolo qreg	1	tisk	segnale	high, low	9	qreg	segnale	high, low
		2	temp_est_calc	segnale	high, low				
Calc_tisk	Calcolo tisk	1	temp_est	segnale	high, low	9	tisk	segnale	high, low
		2	temp_rich	segnale	high, low				
		3	irr_sol	segnale	high, low				
Calc_t_rich	Calcolo temp rich	1	tasto_temp	ctrl	falso	9	temp_rich	segnale	high, low
		2	stato	ctrl	falso				



Dott. Fra... SCIRA
N. Iscriz. Albo 90
(In proprio e ...

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

TABELLA 1B

Batteria		1	batteria	ctrl	falso
Chiave		9	stato_chiave	ctrl	falso
Pulsante_ta		9	tasto_auto	ctrl	falso
Pulsante_tt		9	tasto_temp	ctrl	falso
Pulsante_to		9	tasto_off	ctrl	falso
Pulsante_td		9	tasto_distr	ctrl	falso
Sensor_ta		9	temp_ab	segnale	high, low
Sensor_ttr1		9	ttr1	segnale	high, low
Sensor_te		9	temp_est	segnale	high, low
Sensor_ls		9	irr_sol	segnale	high, low
Sensor_tt2		9	tt2	segnale	high, low
Sensor_w		9	vel_veic	segnale	high, low
Attuatore	1 ang_port_misc segnale high, low				

Dott. Francesco SERRA
N. Iscriz. [illegible]
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

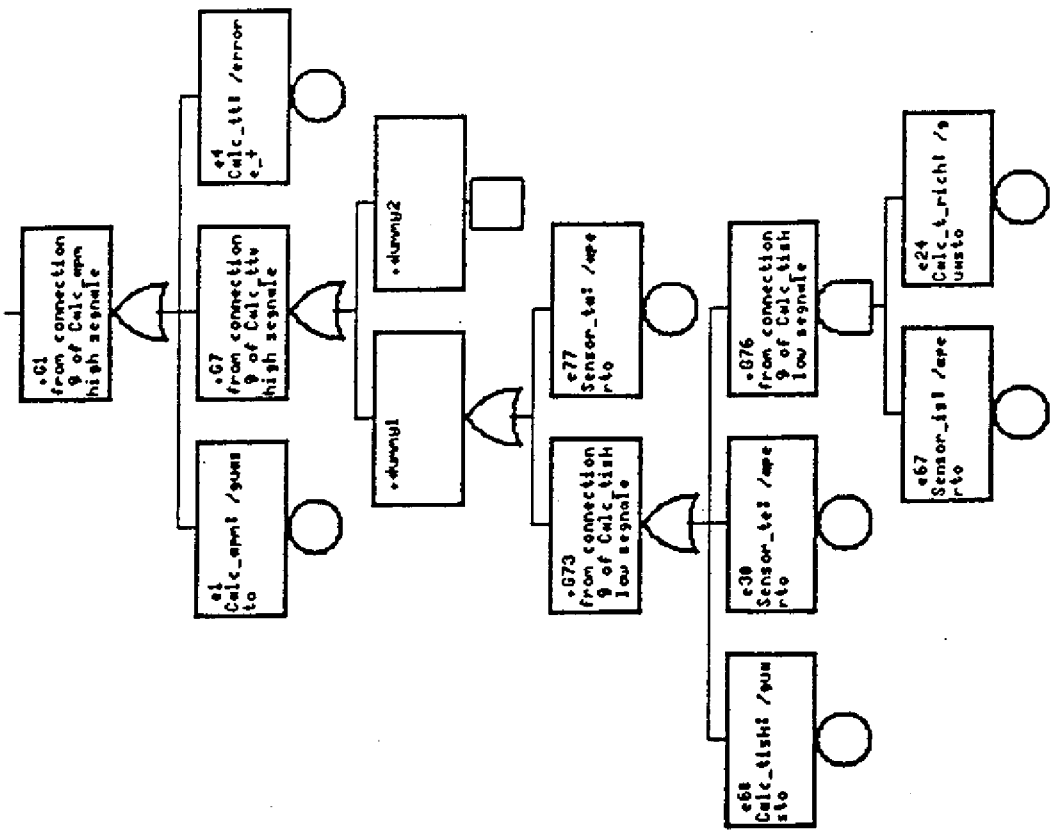
TABELLA 2A

Funzione		Modello Comportamentale			
Nome	Descrizione	Stato	Modi di Guasto	Stati	regole
Gest_dist	Gestione distribuzione	stato1 (tap,floor,colleg) stato2 (tap,vent,colleg) stato3 (tap,bllev,colleg)	nil		IF from connection 1 falso ctrl THEN from connection 9 falso ctrl IF from connection 2 low segnale THEN from connection 10 high segnale IF from connection 2 high segnale THEN from connection 10 low segnale IF from connection 3 high segnale THEN from connection 11 high segnale IF from connection 3 high segnale and from connection 4 falso ctrl THEN from connection 10 low segnale IF from connection 5 low segnale THEN from connection 10 high segnale IF from connection 3 low segnale and from connection 7 falso ctrl THEN from connection 10 high segnale
			/guasto	tutti	IF /guasto AND from connection 2 high segnale THEN from connection 10 high segnale IF /guasto THEN from connection 9 falso ctrl
Ctrl_funz	funzionamento	stato1 (bat_coll_chiave_off) stato2 (bat_coll_chiave_on) stato3 (bat_appena_coll_chiave_off) stato4 (clima_off) stato5 (clima_off_chiave_off) stato6 (batt_scoll_chiave_off)	nil		IF from connection 1 falso ctrl THEN from connection 9 falso ctrl c: $DefaultPos = stato3_to_stato2 IF from connection 1 falso ctrl THEN from connection 9 falso ctrl c: $DefaultPos = stato1_to_stato3 IF from connection 2 falso ctrl THEN from connection 9 falso ctrl c:$DefaultPos = stato4_to_stato2
			/guasto	tutti	IF /guasto THEN from connection 9 falso ctrl
Corr_ff1	Correzione ff1	stato1	nil		IF from connection 1 high segnale THEN from connection 9 high segnale IF from connection 2 high segnale THEN from connection 9 high segnale IF from connection 1 low segnale THEN from connection 9 low segnale IF from connection 2 low segnale THEN from connection 9 low segnale
			/guasto	tutti	IF /guasto THEN from connection 9 low segnale
Calc_ff	Calcolo ff	floor def vent bllev floor_man vent_man bllev_man	nil		IF floor AND from connection 1 low segnale THEN from connection 9 low segnale c: $DefaultPos = vent IF from connection 2 low segnale THEN from connection 9 low segnale c: $DefaultPos = vent IF from connection 3 falso ctrl THEN floor c: $DefaultPos = vent
			/errore_+	tutti	IF /errore_+ THEN from connection 9 high segnale
			/errore_-	tutti	IF /errore_- THEN from connection 9 low segnale
Calc_apm	Calcolo angolo poteella misc.	on	nil		IF from connection 2 high segnale THEN from connection 9 high segnale IF from connection 2 low segnale THEN from connection 9 low segnale IF from connection 1 high segnale THEN from connection 9 high segnale IF from connection 1 low segnale THEN from connection 9 low segnale
			/guasto	tutti	IF /guasto THEN from connection 9 high segnale
Calc_ttv	Calcolo ttv	stato1	nil		IF from connection 1 low segnale THEN from connection 9 low segnale IF from connection 3 low segnale THEN from connection 9 low segnale IF from connection 4 low segnale THEN from connection 9 low segnale

TABELLA 2B

					IF from connection 1 high segnale THEN from connection 9 high segnale IF from connection 3 high segnale THEN from connection 9 high segnale IF from connection 4 high segnale THEN from connection 9 high segnale
			/guasto	tutti	IF /guasto THEN from connection 9 high segnale
Calc_qreg	Calcolo qreg	stato1	nil		IF from connection 1 low segnale AND from connection 2 low segnale THEN from connection 3 low segnale IF from connection 1 high segnale AND from connection 2 high segnale THEN from connection 3 high segnale
			/guasto	tutti	IF /guasto THEN from connection 3 high segnale
Calc_tisk	Calcolo tisk	stato1	nil		IF from connection 1 low segnale THEN from connection 4 low segnale IF from connection 3 low segnale AND from connection 2 low segnale THEN from connection 4 low segnale IF from connection 1 high segnale THEN from connection 4 high segnale IF from connection 3 high segnale AND from connection 2 high segnale THEN from connection 4 high segnale
			/guasto	tutti	IF /guasto THEN from connection 4 low segnale
Calc_t_rich	Calcolo temp rich	stato1	nil		IF from connection 1 low ctrl THEN from connection 3 high segnale IF from connection 2 high ctrl THEN from connection 3 low segnale
			/guasto	tutti	IF /guasto AND from connection 2 low ctrl THEN from connection 3 low segnale
Batteria		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Chiave		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Pulsante_ta		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Pulsante_tf		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Pulsante_to		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Pulsante_td		stato1	/guasto	tutti	IF /guasto THEN from connection 1 falso ctrl
Sensor_ta		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Sensor_tfr1		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Sensor_te		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Sensor_ts		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Sensor_tf2		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Sensor_w		stato1	/aperto	tutti	IF /aperto THEN from connection 1 low segnale
			/corto_circuito	tutti	IF /corto_circuito THEN from connection 1 high segnale
Attuatore		stato1			

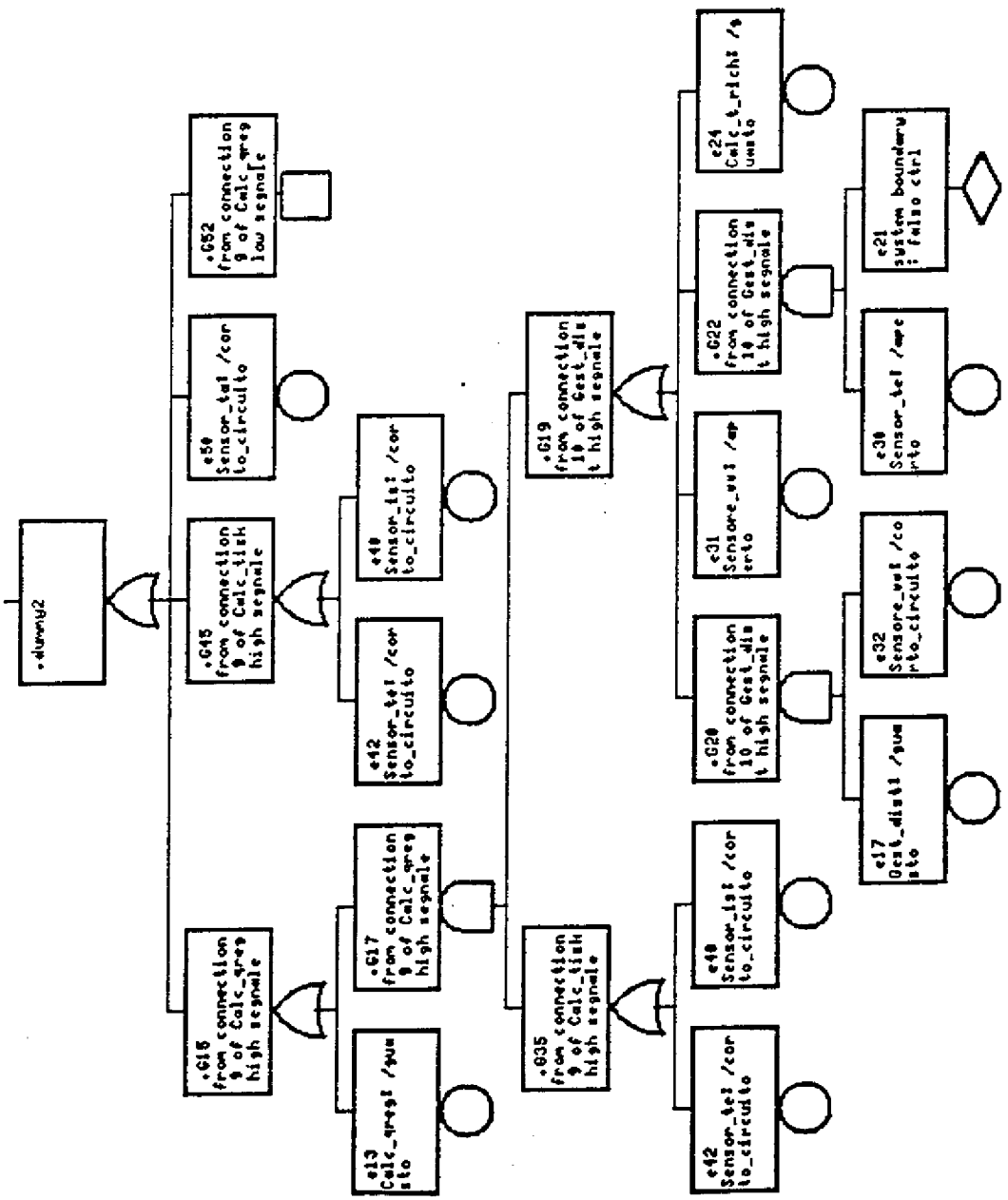
FIGURA 5A



Dott. Francesco SERRA
N. Iscriz. Albo 96
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

FIGURA 5B



Dott. Francesco SERRA
N. Iscr.
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

FIGURA 5C

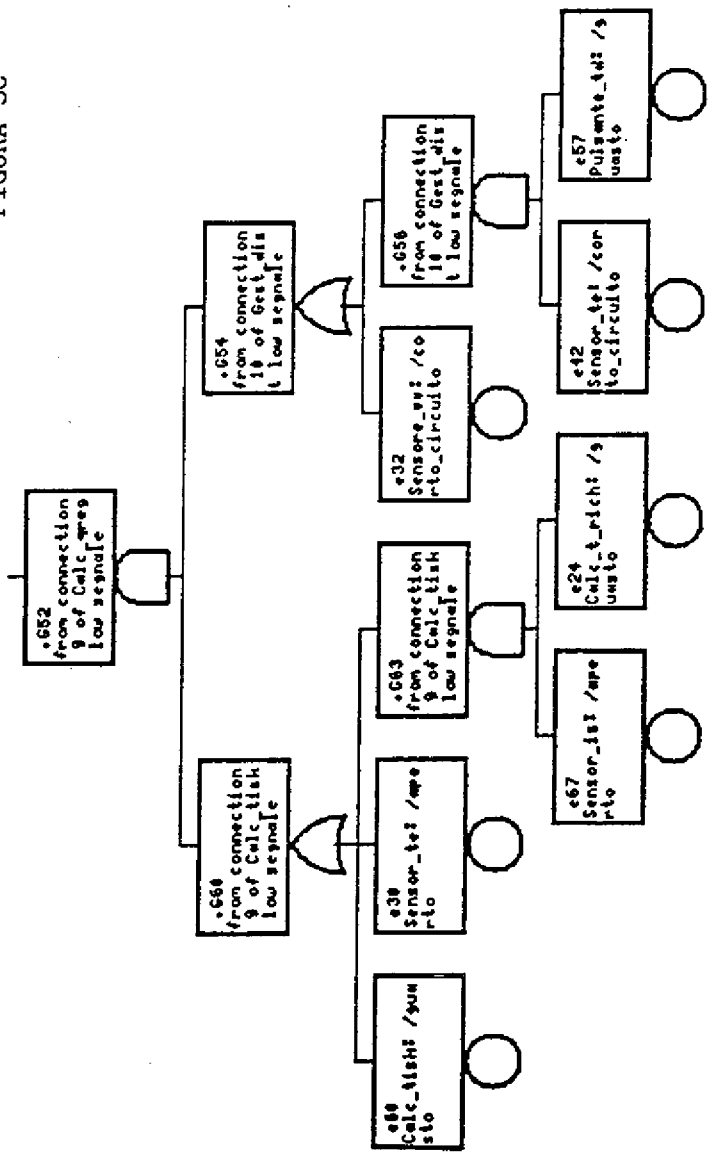


TABELLA 3

n.	indisponibilità	Minimal Cut Set	ord.
1	8.3873E-02	e4	1
2	8.3873E-02	e1	1
3	8.3873E-02	e77	1
4	8.3873E-02	e13	1
5	8.3873E-02	e50	1
6	8.3873E-02	e30	1
7	8.3873E-02	e60	1
8	8.3873E-02	e40	1
9	8.3873E-02	e42	1
10	7.0346E-03	e67 e24	2

Dott.
N. Iscriz.
(in proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni

TABELLA 4

evento primario	indice di criticità
e42	1.100E-01
e40	1.100E-01
e13	1.100E-01
e50	1.100E-01
e30	1.100E-01
e4	1.100E-01
e1	1.100E-01
e60	1.100E-01
e77	1.100E-01
e67	9.220E-03
e24	9.220E-03

Dott. Francesco [illegible]
N. Iscriz. [illegible]
(In proprio e per gli altri)

per incarico di: CENTRO RICERCHE FIAT Società Consortile per Azioni