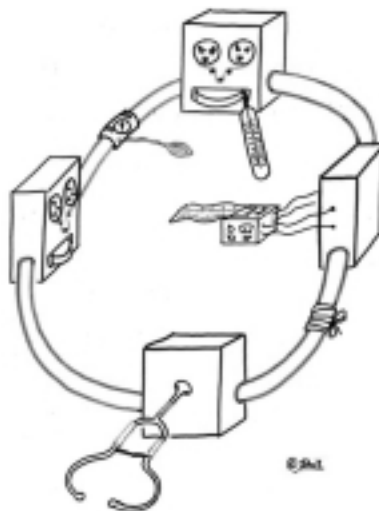


# LA “PATOLOGIA” DEI SISTEMI INFORMATIVI

PROF. FABIO A. SCHREIBER

DIPARTIMENTO DI ELETTRONICA E INFORMAZIONE  
POLITECNICO DI MILANO

## LA PATOLOGIA DEI SISTEMI INFORMATIVI



## AFFIDABILITA' DEI SISTEMI INFORMATICI

### IMPORTANZA APPLICATIVA

- TECNOLOGIE AVANZATE
- IMPATTO SOCIALE DEI SISTEMI INFORMATIVI
- SICUREZZA IN APPLICAZIONI BIOMEDICHE, AVIONICHE, ...

### QUESTIONI TECNOLOGICHE

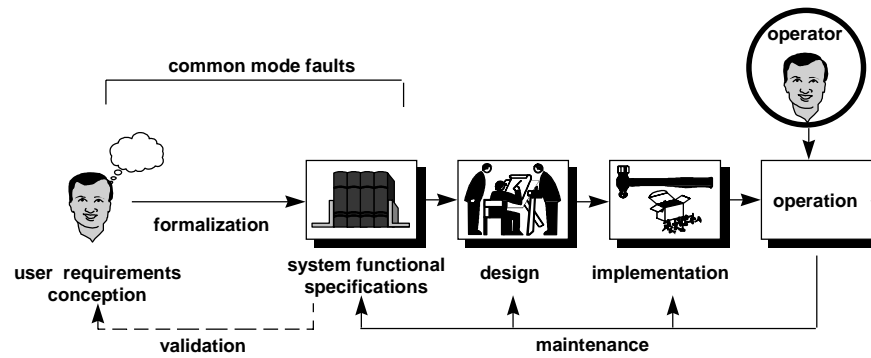
- IMPORTANZA DELLA MICROELETTRONICA
- RUOLO DELLE ARCHITETTURE DISTRIBUITE
- IL PUNTO DEBOLE: IL SOFTWARE
- L'INCOGNITA: GLI ALGORITMI

IL SISTEMA AFFIDABILE DEVE ESSERE ROBUSTO ANCHE NEI CONFRONTI DELL'OPERATORE UMANO (CAUSA DI >70% DEGLI INCIDENTI)

## LA DEPENDABILITY NEI SAFETY- CRITICAL CBS

- SPECIFICHE NEGLI STANDARD (e.g. EN 50126 Guided Transport Systems)
  - 10<sup>-9</sup> GUASTI PERICOLOSI/ORA NEL SISTEMA DI CONTROLLO →
  - 8.7x10<sup>-6</sup> GUASTI PERICOLOSI/ANNO NEL SISTEMA DI CONTROLLO AL MASSIMO LIVELLO DI INTEGRITA'
- VALORI IPOTIZZATI PER IL SOFTWARE
  - 10<sup>-2</sup> -- 10<sup>-3</sup> GUASTI/ANNO
- DEFINIRE PROCEDURE DI CERTIFICAZIONE CHIARE ED EFFICACI CHE PORTINO A VALORI QUANTITATIVAMENTE SIGNIFICATIVI
- CHI E' INTERESSATO?
  - ENTI DI CERTIFICAZIONE
  - COMPAGNIE DI ASSICURAZIONE
  - PERITI LEGALI
  - I CITTADINI UTENTI !!

## IL PROCESSO DI PROGETTAZIONE



© Fabio. A. Schreiber

Safety Critical Systems 4

## TIPI DI GUASTI E DI ERRORI

### • LOGICI

- SCELTE ARCHITETTONICHE E DI PROGETTO
- ALGORITMI

# GLI ERRORI SONO INDIPENDENTI DALLA NATURA (HW O SW) DEI COMPONENTI DEL SISTEMA

# SI POSSONO TRATTARE CON METODI FORMALI

### • FISICI

- DIFETTI DI FABBRICAZIONE
- STRESS
- ATTIVITA' OPERATIVA (USURA)

# I GUASTI SONO DOVUTI AI COMPONENTI HW

# POSSONO ESSERE TRATTATI CON METODI PROBABILISTICI

© Fabio. A. Schreiber

Safety Critical Systems 5

## ERRORI UMANI

- **CONTRIBUISCONO PER IL 60%--80% DEL RISCHIO TOTALE**
- **SOGGETTIVI (PSICOLOGICI)**  
PERCEZIONE ED ABILITA' DELL'OPERATORE
  - APPRENDIMENTO E ADDESTRAMENTO
  - DISTRAZIONE (DISATTENZIONE)
- **OGGETTIVI (INGEGNERIA)**  
ASPETTI INGEGNERISTICI DEL PROGETTO
  - USABILITA'
  - DISTRAZIONE (AMBIGUITA' DI PRESENTAZIONE)

## ARCHITETTURE PER ELEVATE DISPONIBILITA' E PRESTAZIONI

### SPECIALIZZATE

- COSTI ELEVATI
- ADATTE PER APPLICAZIONI MEDICHE, AEROSPAZIALI, CENTRALI TELEFONICHE, ECC.

### TRADIZIONALI

- UTILIZZANO SISTEMI DISTRIBUITI
- UTILIZZANO COMPONENTI COTS
- COSTI "TRADIZIONALI"
- ADATTE A CLASSI PIU' AMPIE DI APPLICAZIONI, TRA LE QUALI I SISTEMI INFORMATIVI

## PROBLEMI DI PROGETTO DI SISTEMI INFORMATIVI AFFIDABILI

### ARCHITETTONICI

- COME DISPORRE COMPONENTI RIDONDANTI IN MODO DA AUMENTARE LA DISPONIBILITA'

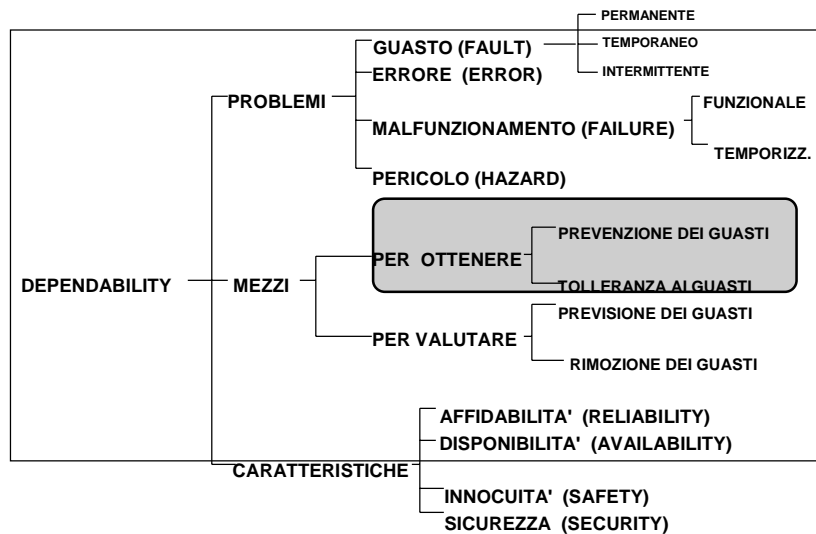
### PROCEDURE DI RIPRISTINO

- COME PROGETTARE PROCEDURE PER LA SCOPERTA ED IL RECUPERO DAI GUASTI CHE SIANO:
  - RAPIDE
  - COMPLETE
  - CHE COMPORTINO UN OVERHEAD BASSO IN CONDIZIONI NORMALI

### VALUTAZIONE QUANTITATIVA

- QUANTO BISOGNA SPENDERE PER OTTENERE UNA DATA QUALITA' DI SERVIZIO

## ALCUNI CONCETTI



## TIPI DI SISTEMI

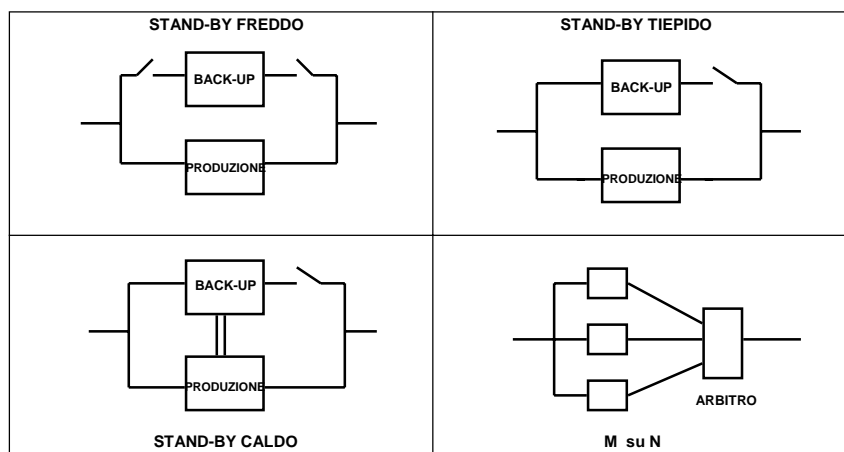
### TOLLERANTI AI GUASTI (FAULT TOLERANT)

- RIPRISTINO DI UNO STATO CORRETTO (ERROR RECOVERY)
- COMPENSAZIONE DELL'ERRORE (ERROR COMPENSATION)
- OVERHEAD TEMPORALE vs. RIDONDANZA STRUTTURALE
- IMPOSSIBILITA' DEL RIPRISTINO

### A DEGRADAZIONE GRADUALE (SOFT DEGRADATION)

- LE FUNZIONI VENGONO SVOLTE CON MINORI PRESTAZIONI
- VENGONO FORNITE SOLO ALCUNE FUNZIONALITA'

## ARCHITETTURE TOLLERANTI I GUASTI

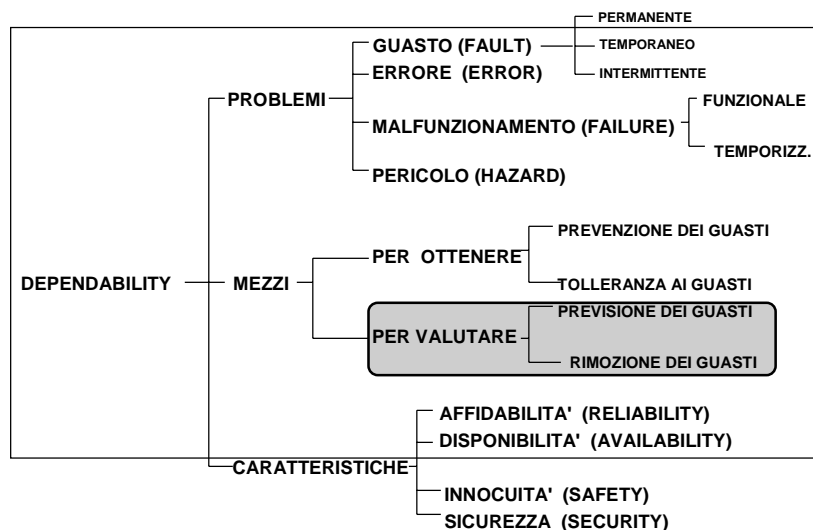


## GUASTI DI MODO COMUNE

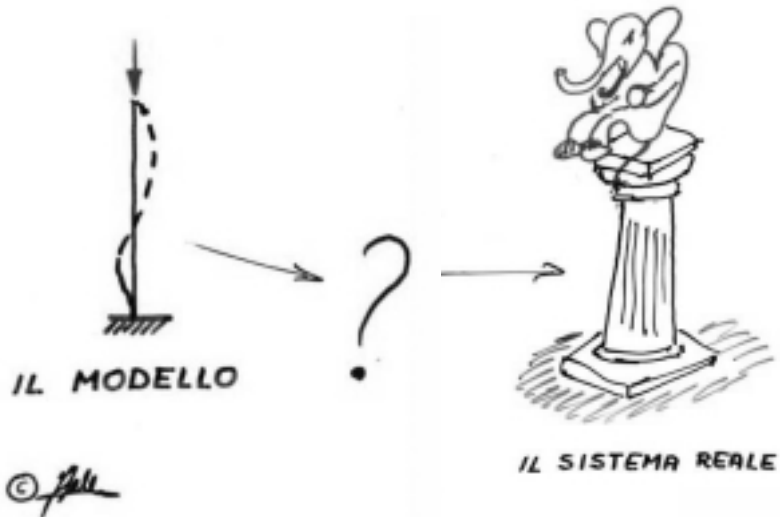
SONO I GUASTI CHE COLPISCONO CONTEMPORANEAMENTE TUTTE LE RISORSE DI UN CERTO TIPO

- ERRORI DI SPECIFICA
- CANALI TRASMISSIVI RIDONDATI CHE UTILIZZANO LO STESSO CAVO FISICO

## ALCUNI CONCETTI



## MODELLI E REALTA'



© Fabio. A. Schreiber

Safety Critical Systems 14

## DECOMPOSIZIONE DI SISTEMI COMPLESSI

### DECOMPOSIZIONE STRUTTURALE

- DIVISIONE DEL SISTEMA GLOBALE IN SOTTOINSIEMI FISICI DISTINTI
- SOLUZIONE SEPARATA DEI DIVERSI SOTTOSISTEMI
- COMBINAZIONE DELLE SOLUZIONI PARZIALI

### DECOMPOSIZIONE COMPORTAMENTALE

- SEPARAZIONE TRA COMPORTAMENTO DI GUASTO E DI RIPARAZIONE
- SOLUZIONE DEL SOTTOMODELLO CON LA TECNICA PIU' APPROPRIATA (ANALITICA, SIMULAZIONE, ECC.)
- INCORPORAZIONE DEI RISULTATI DI UN MODELLO NELL'ALTRO

### SOLUZIONI APPROSSIMATE

- DECOMPOSIZIONE ITERATIVA IN SOTTOINSIEMI PIU' PICCOLI

© Fabio. A. Schreiber

Safety Critical Systems 15

## COMPONENTI DI UN SISTEMA INFORMATIVO CARATTERISTICHE DI AFFIDABILITA'

### HARDWARE

- BEN CONOSCIUTE. METODI SOFISTICATI OTTENGONO OTTIMI RISULTATI NEL CAMPO DEI CIRCUITI ELETTRONICI

### SOFTWARE

- DISCRETAMENTE CONOSCIUTE. SONO IN CORSO RICERCHE, MA OCCORRONO PIU' ESPERIENZE E DATI PER OTTENERE DEI BUONI MODELLI PREVISIONALI

### ALGORITMI

- POCO CONOSCIUTE. DEVONO ESSERE ATTENTAMENTE VALUTATE LE PROPRIETA' DI DIPENDENZA DAL CARICO E DALLO STATO

### OPERATORI UMANI

- ????

## COMPONENTI DI UN SISTEMA INFORMATIVO CARATTERISTICHE DI AFFIDABILITA'

### HARDWARE

- BEN CONOSCIUTE. METODI SOFISTICATI OTTENGONO OTTIMI RISULTATI NEL CAMPO DEI CIRCUITI ELETTRONICI

### SOFTWARE

- DISCRETAMENTE CONOSCIUTE. SONO IN CORSO RICERCHE, MA OCCORRONO PIU' ESPERIENZE E DATI PER OTTENERE DEI BUONI MODELLI PREVISIONALI

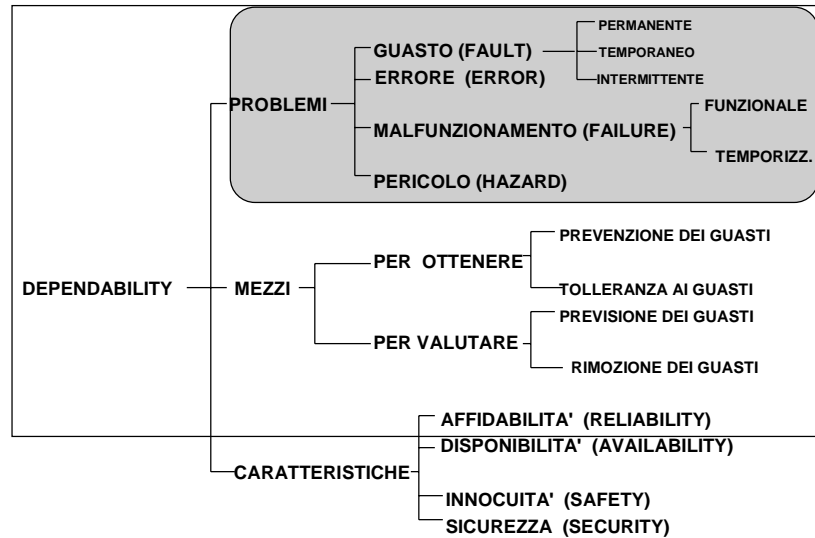
### ALGORITMI

- POCO CONOSCIUTE. DEVONO ESSERE ATTENTAMENTE VALUTATE LE PROPRIETA' DI DIPENDENZA DAL CARICO E DALLO STATO

### OPERATORI UMANI

- ????

## ALCUNI CONCETTI



© Fabio. A. Schreiber

Safety Critical Systems 18

## GUASTO

- **E' LA CAUSA PRIMA DELLA PATOLOGIA DEL SISTEMA**
- **PUO' ESSERE CLASSIFICATO IN BASE ALLA NATURA, ALL'ORIGINE, ALLA PERSISTENZA ...**
- **E' DI PERTINENZA DEL DOMINIO FISICO DEL SISTEMA**

© Fabio. A. Schreiber

Safety Critical Systems 19

## **GUASTO**

- **PERMANENTE**
  - **UNA VOLTA AVVENUTO SI STABILIZZA E PERMANE NEL TEMPO**
- **TEMPORANEO**
  - **SI VERIFICA IN UN INTERVALLO DI TEMPO FINITO E IN GENERE NON SI RIPETE**
- **INTERMITTENTE**
  - **SI VERIFICA IN MODO RIPETITIVO E IMPREDICIBILE**

## **ERRORE**

- **E' QUELLA PARTE DELLO STATO DI UN SISTEMA IN GRADO DI CAUSARE, MA NON NECESSARIAMENTE, UN Malfunzionamento**
- **E' PROVOCATO DA UN GUASTO**
- **E' DI PERTINENZA DEL DOMINIO INFORMATIVO DEL SISTEMA**

## MALFUNZIONAMENTO

- E' LA CONDIZIONE NELLA QUALE IL SISTEMA NON SI COMPORTA SECONDO LE SPECIFICHE
- PUO' ESSERE CLASSIFICATO IN BASE AL DOMINIO, AL TIPO DI CONSISTENZA, ALLA GRAVITA', ...
- E' DI PERTINENZA DEL DOMINIO APPLICATIVO DEL SISTEMA

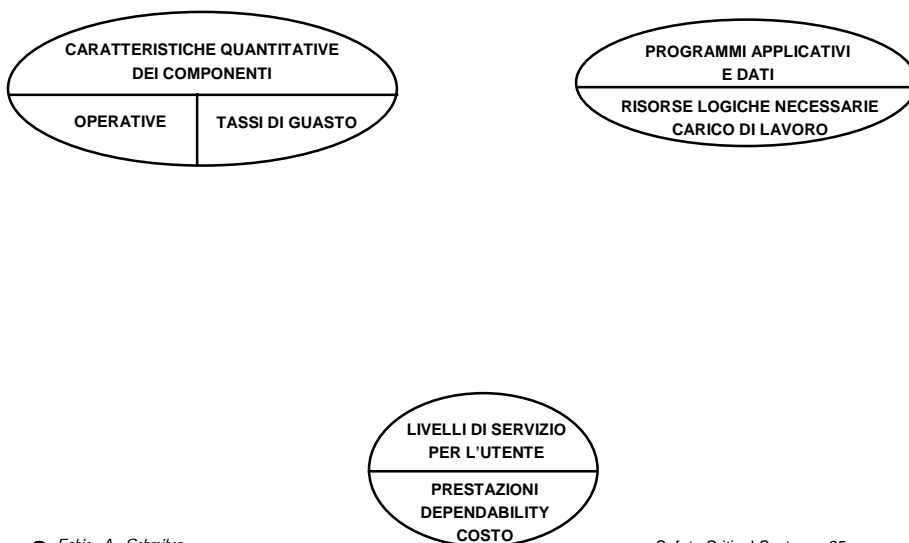
## LA CATENA FONDAMENTALE



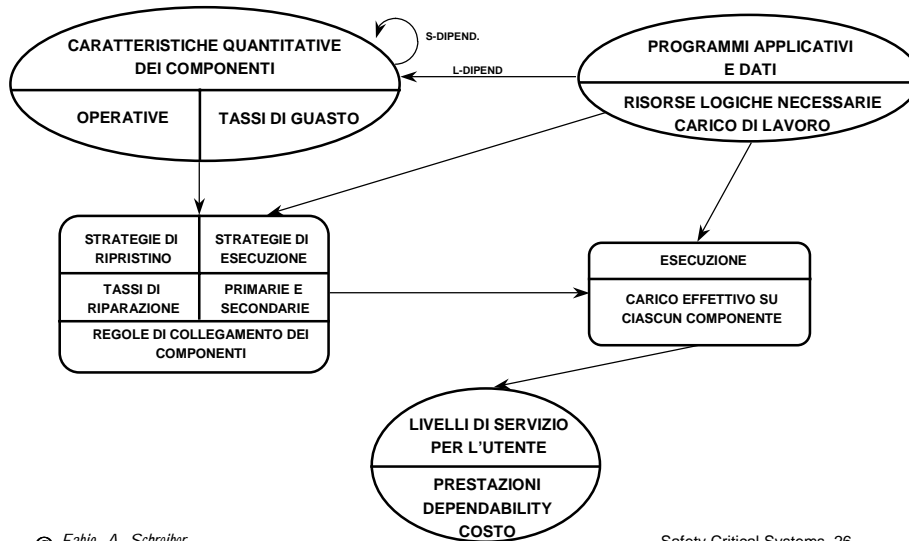
## PERICOLO

- **E' UN INSIEME DI CONDIZIONI (STATO DEL SISTEMA) CHE, IN DETERMINATE CIRCOSTANZE AMBIENTALI, POSSONO PORTARE AD UN INCIDENTE**
- **IL RISCHIO E' FUNZIONE :**
  - DELLA PROBABILITA' CHE ESISTANO UNO O PIU' PERICOLI
  - DELLA PROBABILITA' CHE SI ATTUINO LE CONDIZIONI PER UN INCIDENTE
  - DELLA MASSIMA PERDITA POTENZIALE DOVUTA AL VERIFICARSI DELL'INCIDENTE

## L'AMBIENTE DI RICERCA



## L'AMBIENTE DI RICERCA



© Fabio. A. Schreiber

Safety Critical Systems 26

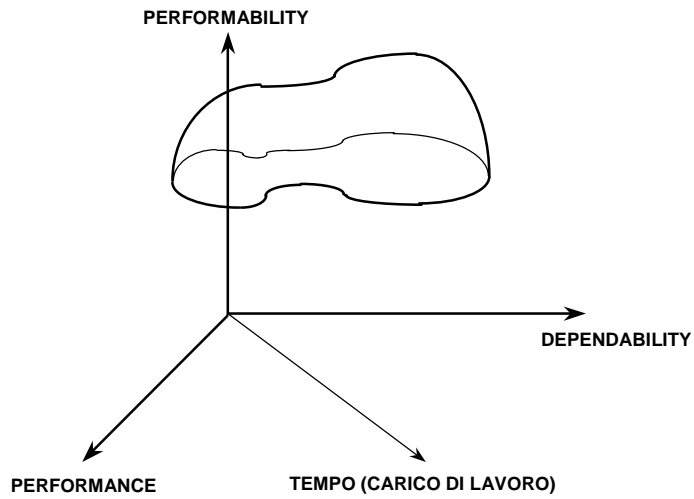
## UN MODELLO A STRATI

LIVELLO 5	IL SISTEMA INFORMATIVO	
LIVELLO 4	CONTROLLO DEL SISTEMA	CONTROLLO DELLA CONCORRENZA, ROUTING, COMMITMENT, ECC.
LIVELLO 3	UNITA' FUNZIONALI	CPU, SOTTOSISTEMA DI I/O, PACCHETTI DI SW
LIVELLO 2	SOTTOASSEMBLAGGI	SCHEDE ELETTRONICHE, SEMPLICI PROGRAMMI
LIVELLO 1	COMPONENTI SEMPLICI	CHIP, LINEE TRASMISSIVE, SOTTOPROGRAMMI, ECC.

© Fabio. A. Schreiber

Safety Critical Systems 27

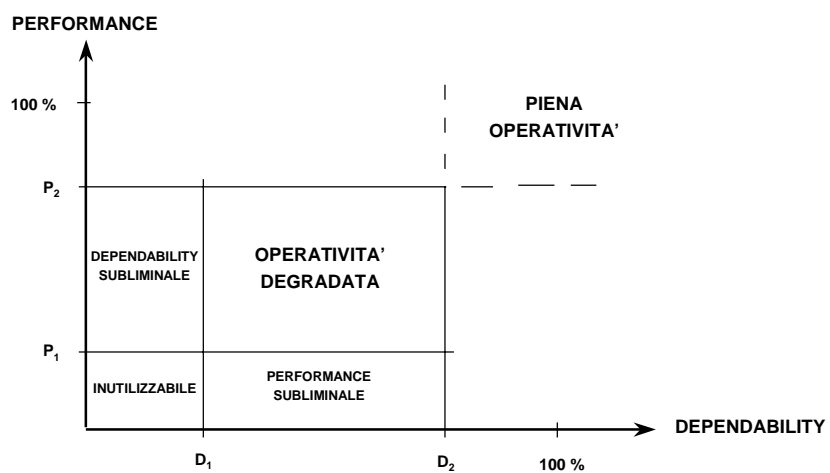
## LO SPAZIO PER LA VALUTAZIONE DEI SISTEMI



© Fabio. A. Schreiber

Safety Critical Systems 28

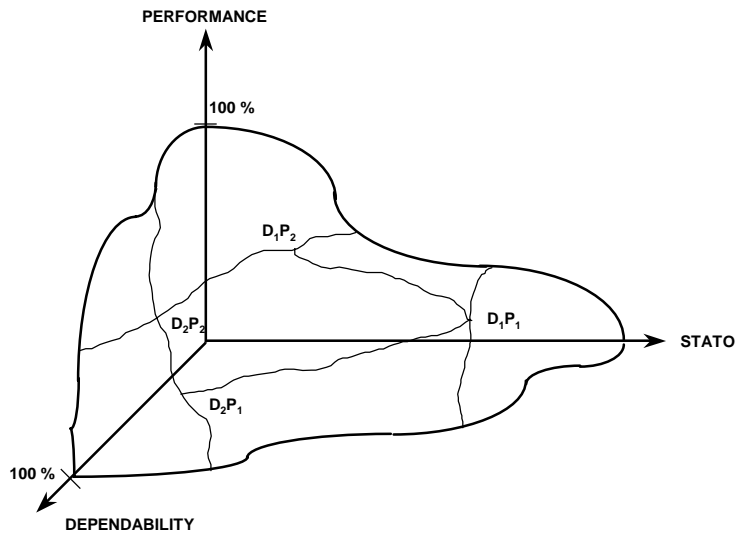
## LO SPAZIO DEI LIVELLI DI SERVIZIO



© Fabio. A. Schreiber

Safety Critical Systems 29

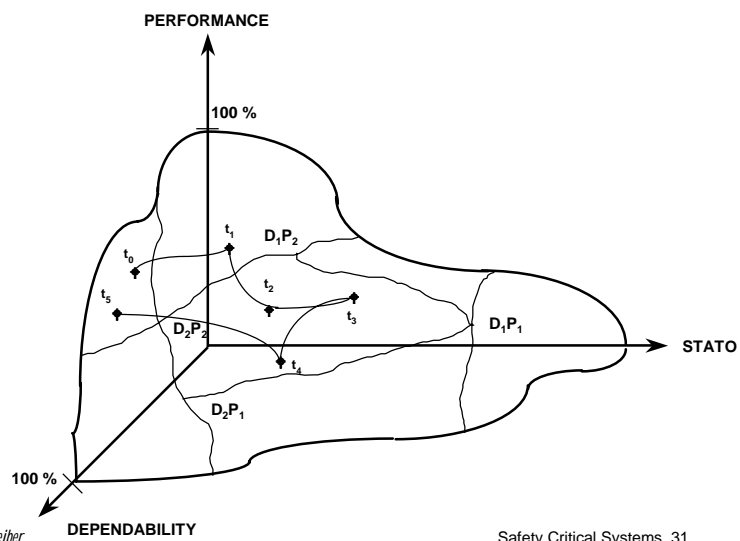
## LO SPAZIO DEI LIVELLI DI SERVIZIO



© Fabio. A. Schreiber

Safety Critical Systems 30

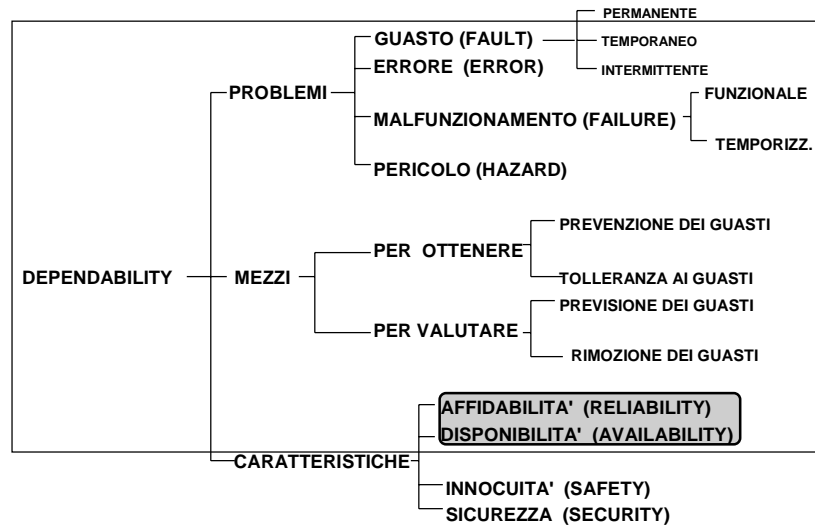
## LO SPAZIO DEI LIVELLI DI SERVIZIO



© Fabio. A. Schreiber

Safety Critical Systems 31

## ALCUNI CONCETTI



© Fabio. A. Schreiber

Safety Critical Systems 32

## TEORIA MATEMATICA DELL'AFFIDABILITA'

### E' UN INSIEME DI:

- MODELLI MATEMATICI
- METODI
- IDEE

### DIRETTI ALLA SOLUZIONE DI PROBLEMI QUALI LA PREVISIONE E/O L'OTTIMIZZAZIONE DI:

- PROBABILITA' DI SOPRAVVIVENZA
- VITA MEDIA E SUA DISTRIBUZIONE

### DI

- COMPONENTI
- SISTEMI

© Fabio. A. Schreiber

Safety Critical Systems 33

## TEORIA MATEMATICA DELL'AFFIDABILITA'

MOLTEPLICITA' DI ENTITA' E DI CONCETTI



•AMBIGUITA'  
•INCONSISTENZA



OCCORRE DEFINIRE UN'UNICA ENTITA'  
GENERALE DALLA QUALE DERIVARE LE  
QUANTITA' DI INTERESSE PRATICO

## DEFINIZIONI GENERALI

SIA  $\mathbf{X}(t) = (X_1(t), \dots, X_n(t))$  UN VETTORE DI VARIABILI CASUALI  
CON FUNZIONE DI DISTRIBUZIONE

$$F(x_1, \dots, x_n; t) \Leftrightarrow \text{Prob} [X_1(t) \leq x_1, \dots, X_n(t) \leq x_n]$$

CHE DEFINISCE LO STATO DEL SISTEMA

AD OGNI STATO  $\mathbf{x} = (x_1, \dots, x_n)$  ASSOCIAMO UN GUADAGNO  $g(\mathbf{x})$

IL CUI VALOR MEDIO ALL'ISTANTE  $t$  E'

$$G(t) = E g(\mathbf{X}(t)) = \int \dots \int g(x_1, \dots, x_n) dF(x_1, \dots, x_n; t)$$

## DEFINIZIONI GENERALI

LE QUANTITA' GENERALI PER DEFINIRE TUTTE LE ALTRE GRANDEZZE SONO:

- $G(t)$

$$\bullet H(a, b) = \int_a^b G(t) dW(t) \quad a \leq t \leq b$$

OSSIA LA MEDIA TEMPORALE DEL GUADAGNO PESATA CON UNA FUNZIONE  $W(t)$

## DEFINIZIONI PARTICOLARI

### AFFIDABILITA' (RELIABILITY)

E' LA PROBABILITA' CHE UN DISPOSITIVO COMPIA ADEGUATAMENTE LA PROPRIA FUNZIONE PER IL PERIODO DI TEMPO E NELLE CONDIZIONI PREVISTE

intervallo di tempo  $[0, t]$

$$\text{per } t=u \quad X(u) = \begin{cases} 1 & \text{se funziona} \quad \rightarrow g(1) = 1 \\ 0 & \text{se non funziona} \quad \rightarrow g(0) = 0 \end{cases}$$

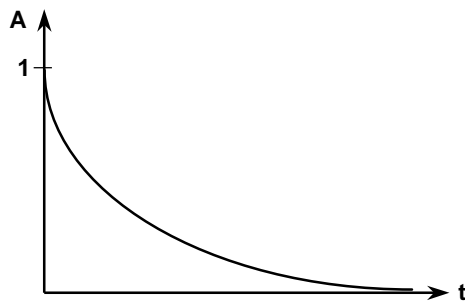
$$\text{Reliability} = G(t) = Eg(X(t)) = \text{Prob}[X(t) = 1]$$

FUNZIONAMENTO ALL'ISTANTE  $t$  IMPLICA FUNZIONAMENTO IN TUTTO L'INTERVALLO  $[0, t]$  (SENZA RIPARAZIONE O SOSTITUZIONE DI COMPONENTI)

## AFFIDABILITA'

RAPPRESENTA L'ATTITUDINE DEL COMPONENTE  
O DEL SISTEMA A NON GUASTARSI

- TENDE A ZERO AL PASSARE DEL TEMPO



© Fabio. A. Schreiber

Safety Critical Systems 38

## DEFINIZIONI PARTICOLARI

### DISPONIBILITA' ISTANTANEA (POINTWISE AVAIL.)

E' LA PROBABILITA' CHE UN SISTEMA FUNZIONI NEI LIMITI DI  
TOLLERANZA AD UN DATO ISTANTE  $t$

il guadagno sia  $\begin{cases} g(1) = 1 \\ g(0) = 0 \end{cases}$

$$\text{Ptw.}_\text{Availability} = G(t) = E g(X(t)) = \text{Prob} [X(t) = 1]$$

E' POSSIBILE RIPARARE E/O SOSTITUIRE COMPONENTI CHE SI  
GUASTINO PRIMA DELL'ISTANTE  $t$

VIENE ANCHE CHIAMATA DISPONIBILITA' SU RICHIESTA

© Fabio. A. Schreiber

Safety Critical Systems 39

## DEFINIZIONI PARTICOLARI

### DISPONIBILITA' (INTERVAL AVAILABILITY)

E' LA PERCENTUALE DI UN INTERVALLO DI TEMPO  $[a,b]$   
DURANTE LA QUALE IL SISTEMA FUNZIONA NEI LIMITI DI  
TOLLERANZA

$$W(t) = \frac{t - a}{b - a};$$

$$H(a,b) = \frac{1}{b - a} \int_a^b G(t) dt$$

Int. Availability =

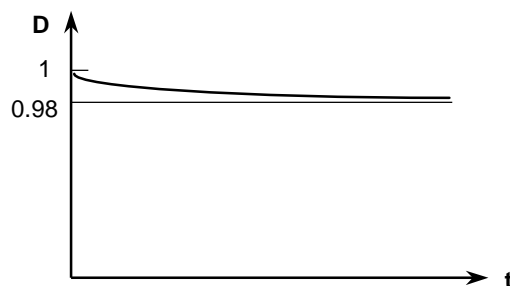
$$H(a,b) = E \frac{\int_a^b g(X(t) dt)}{b - a}$$

SONO AMMESSE RIPARAZIONI E SOSTITUZIONI DI COMPONENTI  
GUASTI

## DISPONIBILITA'

DENOTA LA PROBABILITA' DI TROVARE IL COMPONENTE O IL  
SISTEMA FUNZIONANTE IN UN CERTO ISTANTE O IN UN CERTO  
INTERVALLO DI TEMPO

- TENDE A MANTENERE UN VALORE PROSSIMO A UNO



## PROPRIETA'

- **DEI COMPONENTI**

- **DELLE STRUTTURE COMPLESSE**

## TASSO DI GUASTO

I FENOMENI CHE PORTANO UN COMPONENTE A GUASTARSI  
POSSONO ESSERE CONSIDERATI PROCESSI STOCASTICI

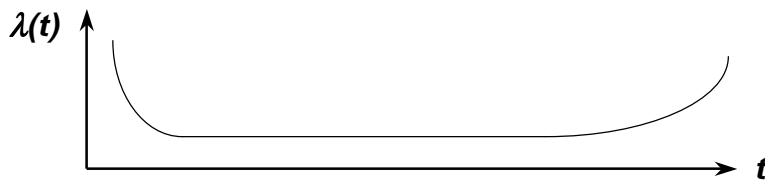
- $F(t)$  = FUNZIONE DI DISTRIBUZIONE TEMPORALE DEI GUASTI
- $f(t)$  = DENSITA' DI PROBABILITA' DI  $F(t)$
- $\lambda(t)$  = TASSO DI GUASTO

$$\lambda(t) = \frac{f(t)}{1 - F(t)}; \quad F(t) < 1$$

## TASSO DI GUASTO

$\lambda(t)d(t)$  RAPPRESENTA LA PROBABILITA' CHE UN COMPONENTE DI ETA'  $t$  SI GUASTI NELLO INTERVALLO DI TEMPO  $[t, t+dt]$

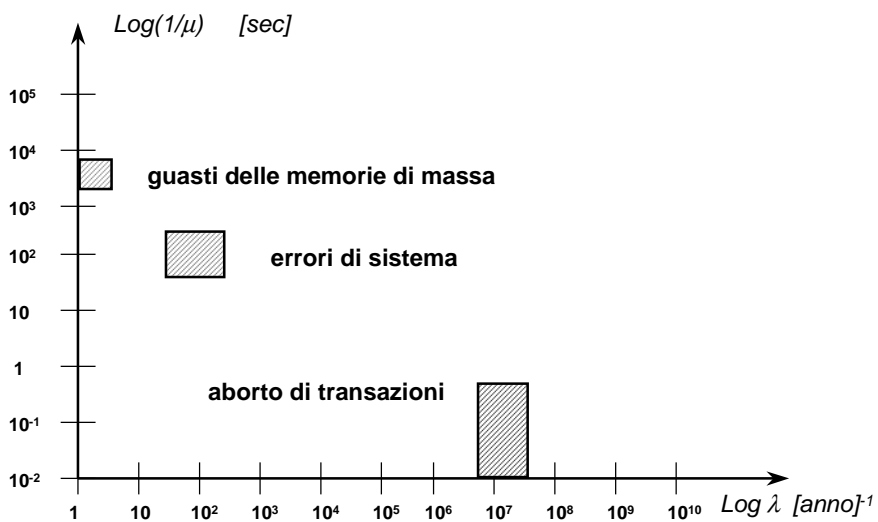
TALE PROBABILITA' VARIA NEL TEMPO CON IL TIPICO ANDAMENTO "A VASCA DA BAGNO"



© Fabio. A. Schreiber

Safety Critical Systems 44

## TASSI DI TRANSIZIONE IN SISTEMI INFORMATIVI



© Fabio. A. Schreiber

Safety Critical Systems 45

## TASSI DI TRANSIZIONE

- **INDIPENDENTI**

IL LORO VALORE NON DIPENDE DA ALCUN ALTRO PARAMETRO DEL SISTEMA

- **DIPENDENTI DAL CARICO**

IL LORO VALORE DIPENDE DAL CARICO APPLICATO AL COMPONENTE STESSO (DIRETTO) O AD ALTRE PARTI DEL SISTEMA (INDIRETTO)

- **DIPENDENTI DALLO STATO**

IL LORO VALORE DIPENDE DALLO STATO DEL COMPONENTE STESSO O DA QUELLO DI ALTRE PARTI DEL SISTEMA

## TASSI DI TRANSIZIONE

LE DISTRIBUZIONI DI PROBABILITA' USATE PER MODELLARE I TASSI DI TRANSIZIONE SONO MONOTONE, COSA CHE PERMETTE DI DIMOSTRARE MATEMATICAMENTE ALCUNE UTILI PROPRIETA'

**WEIBULL**

IFR

resistenza a fatica dei materiali

$$f(t) = \delta \alpha t^{\alpha-1} e^{-\delta t^\alpha}; \lambda(t) = \delta \alpha t^{\alpha-1}$$
$$\delta, \alpha > 0; t \geq 0$$

**ESPONENZIALE**

CFR

fusibili, apparecchiature complesse

$$f(t) = \delta e^{-\delta t}; \lambda(t) = \delta$$
$$\delta > 0; t \geq 0$$

**LOG NORMALE**

DFR

tempi di riparazione,  
software (?)

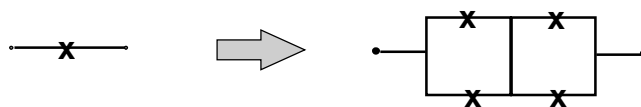
$$f(t) = \frac{1}{t\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2\sigma^2} (\log(t) - \mu)^2\right]$$
$$-\infty < \mu < +\infty; \sigma > 0; t \geq 0$$

## PROPRIETA'

- DEI COMPONENTI

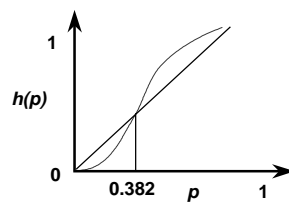
- DELLE STRUTTURE COMPLESSE

## STRUTTURE MULTICOMPONENTE



$p$  = PROBABILITA' DI CHIUSURA DI UN COMPONENTE

$h(p)$  = PROBABILITA' DI CHIUSURA DEL CIRCUITO



$$h(p) = [1 - (1 - p)^2]^2 = 4p^2 - 4p^3 + p^4$$

## STRUTTURE MULTICOMPONENTE

FORMA GENERALE DELLA FUNZIONE PER  $n$  COMPONENTI

$$h(p) = \sum_{i=0}^n A_i p^i (1-p)^{n-i} \quad ; \quad A_i = \binom{n}{i}$$

$i$  E' L'INDICE CHE INDIVIDUA I SINGOLI INSIEMI DI COMPONENTI CHE ASSICURANO LA CHIUSURA DEL CIRCUITO

LE FUNZIONI DI QUESTO TIPO, STUDIATE DA *MOORE* E *SHANNON*, SONO DENOMINATE FUNZIONI QUORUM

## FUNZIONI MONOTONE

$\varphi$  = PRESTAZIONE DELLA STRUTTURA (BINARIA)

$X_i$  = PRESTAZIONE DELL'  $i$ -esimo COMPONENTE (BINARIA)

$\varphi(x) =$  **FUNZIONE DI STRUTTURA**

SI DICONO MONOTONE LE STRUTTURE NELLE QUALI CIASCUN COMPONENTE FUNZIONANTE CONTRIBUISCE AL FUNZIONAMENTO DELLA STRUTTURA STESSA.

PER LE STRUTTURE MONOTONE VALGONO LE SEGUENTI PROPRIETA'

$$\varphi(1) = 1$$

$$\varphi(0) = 0$$

$$\varphi(x) \geq \varphi(y) \text{ quando } x_i \geq y_i ; i = 1, \dots, n$$

(cioe' i componenti funzionanti non interferiscono con il funzionamento della struttura)

## STRUTTURE MONOTONE

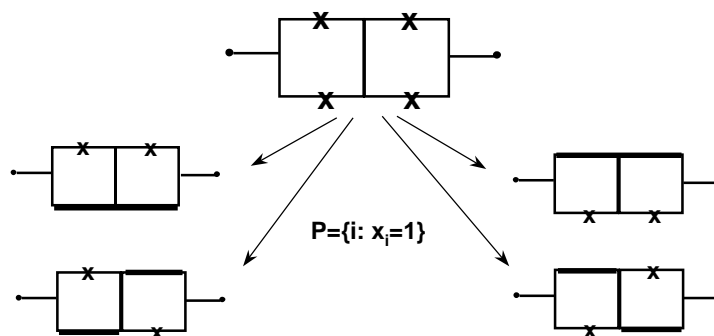
# LE RETI A DUE TERMINALI CON COMPONENTI BINARI SONO MONOTONE

© Fabio. A. Schreiber

Safety Critical Systems 52

## STRUTTURE MONOTONE

UN INSIEME MINIMO DI COMPONENTI IL CUI FUNZIONAMENTO GARANTISCE IL FUNZIONAMENTO DI UNA STRUTTURA VIENE CHIAMATO PATH (PERCORSO)

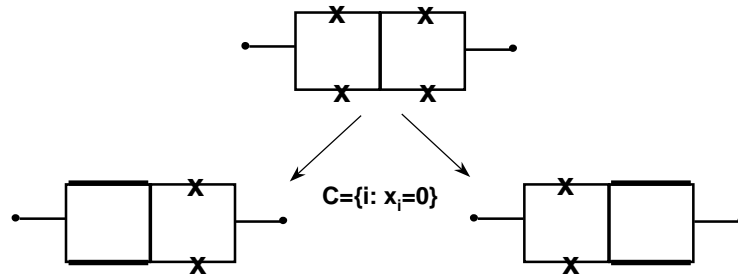


© Fabio. A. Schreiber

Safety Critical Systems 53

## STRUTTURE MONOTONE

UN INSIEME MINIMO DI COMPONENTI LA CUI ROTTURA PROVOCA IL GUASTO DELLA STRUTTURA VIENE CHIAMATO CUT (TAGLIO)



© Fabio. A. Schreiber

Safety Critical Systems 54

## STRUTTURE MONOTONE

MEDIANTE LE FUNZIONI DI PATH (PER STRUTTURE TIPO SERIE)

$$\alpha_j(x) = \prod_{i \in P_j} x_i$$

E LE FUNZIONI DI CUT (PER STRUTTURE TIPO PARALLELO)

$$\beta_k(x) = 1 - \prod_{i \in C_k} (1 - x_i)$$

E' POSSIBILE ESPRIMERE LA FUNZIONE DI STRUTTURA COMPLESSIVA

$$\varphi(x) = 1 - \prod_{j=1}^r [1 - \alpha_j(x)]$$

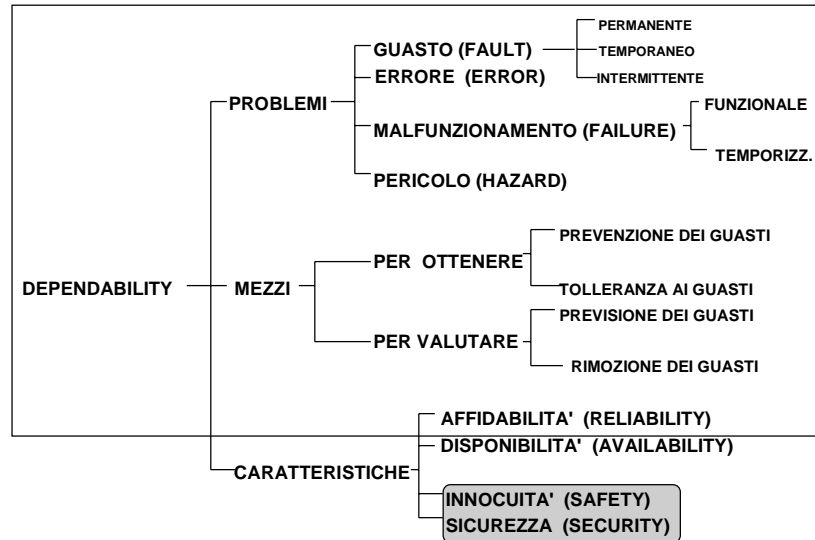
OPPURE

$$\varphi(x) = \prod_{k=1}^s \beta_k(x)$$

© Fabio. A. Schreiber

Safety Critical Systems 55

## ALCUNI CONCETTI



© Fabio. A. Schreiber

Safety Critical Systems 56

## INNOCUITA'

**E' LA PROPRIETA' DEL SISTEMA DI NON CAUSARE DANNI A PERSONE O COSE DA ESSO CONTROLLATE ANCHE IN PRESENZA DI SITUAZIONI AMBIENTALI O DI INGRESSO IMPREVISTE**

## SICUREZZA

**E' LA PROPRIETA' DEL SISTEMA DI RESISTERE AGLI ATTACCHI ALLA PROPRIA INTEGRITA' E SOPRAVVIVENZA DI NATURA PER LO PIU' DOLOSA**

© Fabio. A. Schreiber

Safety Critical Systems 57

## METODI DI ANALISI DEI PERICOLI

- HANNO LO SCOPO DI IDENTIFICARE TUTTE LE POSSIBILI CAUSE DI PERICOLO DERIVANTI DAL FUNZIONAMENTO E DALL'UTILIZZO DEL SISTEMA AL FINE DI RIMUOVERLE O PREDISPORRE OPPORTUNE CONTROMISURE
  - 35% DEI GUASTI IN VOLO NEI SISTEMI DELLA NASA E' STATO CAUSATO DA PERICOLI GIUDICATI NON CREDIBILI!
- RICHIEDONO L'INTERVENTO DI SQUADRE DI ESPERTI MULTIDISCIPLINARI
- NECESSITA' DI USARE METODI FORMALI, MA ACCESSIBILI SENZA ECCESSIVO SFORZO A TUTTI GLI ESPERTI COINVOLTI
- NECESSITA' DI USARE PIU' METODI PER GARANTIRE LA MASSIMA COPERTURA (UN SOLO METODO NON GARANTISCE UNA COPERTURA >35%)

## PRINCIPALI METODI DI ANALISI

### FMEA

FAILURE MODES AND EFFECTS ANALYSIS

### FMECA

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS

### HAZOP

HAZARD AND OPERABILITY STUDY

### FTA

FAULT TREE ANALYSIS

### ETA

EVENT TREE ANALYSIS

### MACCHINE A STATI FINITI

## **FMEA**

**METODO DI ANALISI INDUTTIVA (BOTTOM-UP) IN 4 PASSI MOLTO USATO IN CAMPO AEROSPAZIALE, NUCLEARE, CHIMICO, AUTOMOBILISTICO, APPLICABILE IN UNA FASE AVANZATA DI PROGETTAZIONE**

- **ACCERTA GLI EFFETTI DI OGNI MODALITA' DI GUASTO DI CIASCUN COMPONENTE DEL SISTEMA SULLE SUE FUNZIONALITA'**
  - **DEFINIZIONE DEL SISTEMA, SUE FUNZIONI E SUOI COMPONENTI**
  - **IDENTIFICAZIONE DELLE MODALITA' DI GUASTO DI CIASCUN COMPONENTE E DELLE LORO CAUSE**
- **IDENTIFICA LE MODALITA' DI GUASTO CHE INFLUISCONO SIGNIFICATIVAMENTE SULLA DEPENDABILITY (SAFETY)**
  - **STUDIO DEGLI EFFETTI DI CIASCUNA MODALITA' DI GUASTO**
  - **CONCLUSIONI E RACCOMANDAZIONI**

## **FMECA**

**ESTENSIONE DI FMEA NELLA QUALE SI VALUTANO**

- **LA PROBABILITA' DI OCCORRENZA DI CIASCUNA MODALITA' DI GUASTO**
  - **I LIVELLI DI CRITICITA' DEGLI EFFETTI DEL MALFUNZIONAMENTO**
    - **4 LIVELLI DI SEVERITA' DELLE CONSEGUENZE**
      - **MINIMA**
      - **SIGNIFICATIVA**
      - **CRITICA**
      - **CATASTROFICA**
- VENGONO ACCOPPIATI ALLA PROBABILITA' DELL'EVENTO**

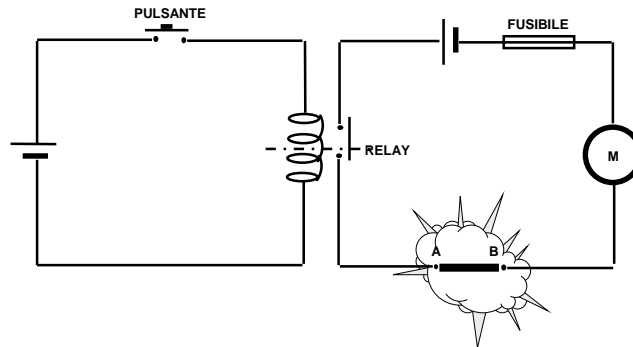
## HAZOP

- **UTILIZZATO PER IMPIANTI IDRAULICI IN INDUSTRIE CHIMICHE, CONSISTE NELLA COMPILAZIONE DI UNA TABELLA SEGUENDO UN INSIEME DI PAROLE GUIDA**
- **PER OGNI DEVIAZIONE DI FUNZIONALITA' CORRISPONDENTE AD UNA PAROLA GUIDA SI ESAMINANO LE POSSIBILI**
  - CAUSE
  - CONSEGUENZE
  - AZIONI RICHIESTE
- **PUO' ESSERE CONSIDERATO UN'ADATTAMENTO DI FMEA APPLICABILE, PER RAFFINAMENTI SUCCESSIVI, IN OGNI FASE DEL PROGETTO**

## FTA

- **METODO DI ANALISI DEDUTTIVO (TOP-DOWN) MOLTO USATO, APPLICABILE AL PROGETTO COMPLETO DOPO AVER IDENTIFICATO I PERICOLI CON FMEA**
- **IDENTIFICA LE POSSIBILI COMBINAZIONI DI EVENTI CHE PORTANO AD UN EVENTO INDESIDERABILE**
- **UTILIZZA UN FORMALISMO AD ALBERO**
  - LE FOGLIE RAPPRESENTANO EVENTI ELEMENTARI INDIPENDENTI LA CUI PROBABILITA' DI OCCORRENZA E' NOTA
  - I NODI INTERMEDI SONO REALIZZATI CON PORTE LOGICHE
  - LA RADICE E' L'EVENTO INDESIDERATO

## FTA: ESEMPIO



- PREMENDO/RILASCIANDO IL PULSANTE SI ATTIVA/FERMA IL MOTORE CHE LAVORA SOLO PER BREVI PERIODI
- IL FILO A-B PASSA IN UNA ZONA CONTENENTE GAS ESPLOSIVI. UN SURRISCALDAMENTO E' PERICOLOSO
- DOPO UNA CORRENTE DI CORTO CIRCUITO, IL RELAY RESTA CHIUSO ANCHE IN ASSENZA DI ALIMENTAZIONE

© Fabio. A. Schreiber

Safety Critical Systems 64

## FTA: ESEMPIO

### COSTRUIRE L'ALBERO DI GUASTO PER L'EVENTO SURRISCALDAMENTO DEL FILO A-B

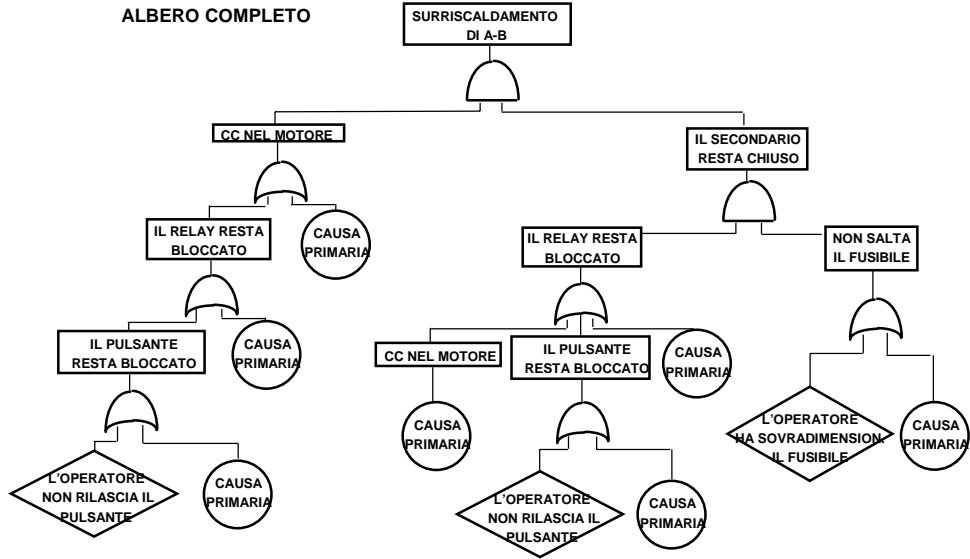
- L'EVENTO E' CAUSATO DA UNA FORTE CORRENTE NEL CIRCUITO SECONDARIO POSSIBILE PER
  - CC NEL MOTORE E ...
  - PERSISTENZA DELLA CHIUSURA DEL CIRCUITO SECONDARIO
- PER OGNUNA DELLE DUE CAUSE SI PROCEDE ITERATIVAMENTE CERCANDO
  - GUASTI PRIMARI (EVENTI DI BASE)
  - GUASTI SECONDARI (CAUSE ESTERNE)
  - GUASTI/ERRORI DI COMANDO-CONTROLLO

© Fabio. A. Schreiber

Safety Critical Systems 65

## FTA: ESEMPIO

ALBERO COMPLETO

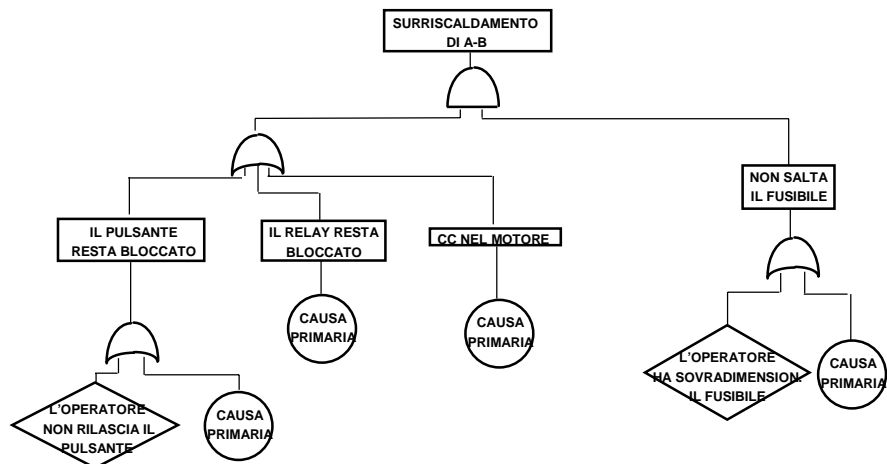


© Fabio. A. Schreiber

Safety Critical Systems 66

## FTA: ESEMPIO

ALBERO RIDOTTO



© Fabio. A. Schreiber

Safety Critical Systems 67

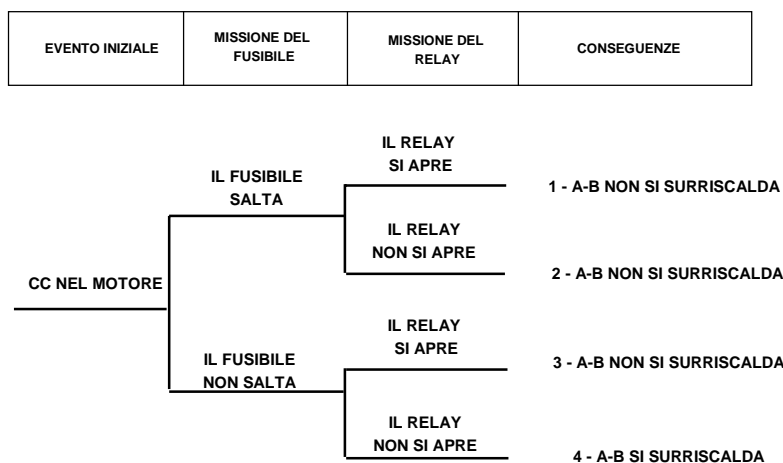
## ETA

- METODO DI ANALISI INDUTTIVA (BOTTOM-UP) APPLICABILE A PROGETTI COMPLETI O A IMPIANTI ESISTENTI
- RAPPRESENTA GRAFICAMENTE UNA STRUTTURA SEQUENZIALE DI EVENTI CON PIU' ESITI POSSIBILI
- INVESTIGA GLI ESITI DI EVENTI FORNENDO LA PROBABILITA' DI OGNI PERCORSO DELL'ALBERO
- UTILE PER EVENTI INDIPENDENTI E CRONOLOGICAMENTE STABILI CON STATI FINALI MULTIPLI (NON TUTTI PERICOLOSI)
- RICHIEDE DATI STORICI PER VALUTARE LE PROBABILITA' DEGLI EVENTI
- SI INTEGRA CON FTA FORNENDO GLI EVENTI RADICE

© Fabio. A. Schreiber

Safety Critical Systems 68

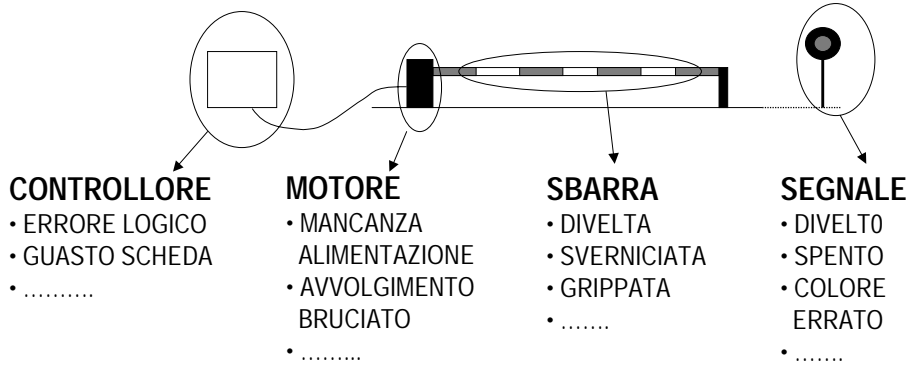
## ETA: ESEMPIO



© Fabio. A. Schreiber

Safety Critical Systems 69

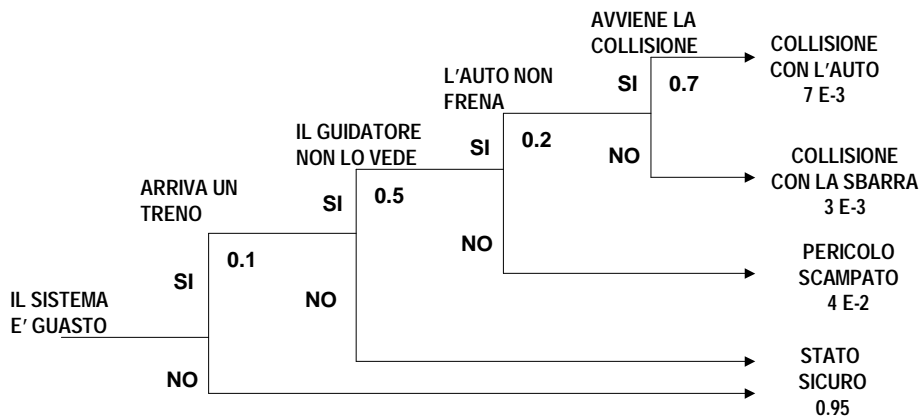
## ESEMPIO PASSAGGIO A LIVELLO: FMEA



© Fabio. A. Schreiber

Safety Critical Systems 70

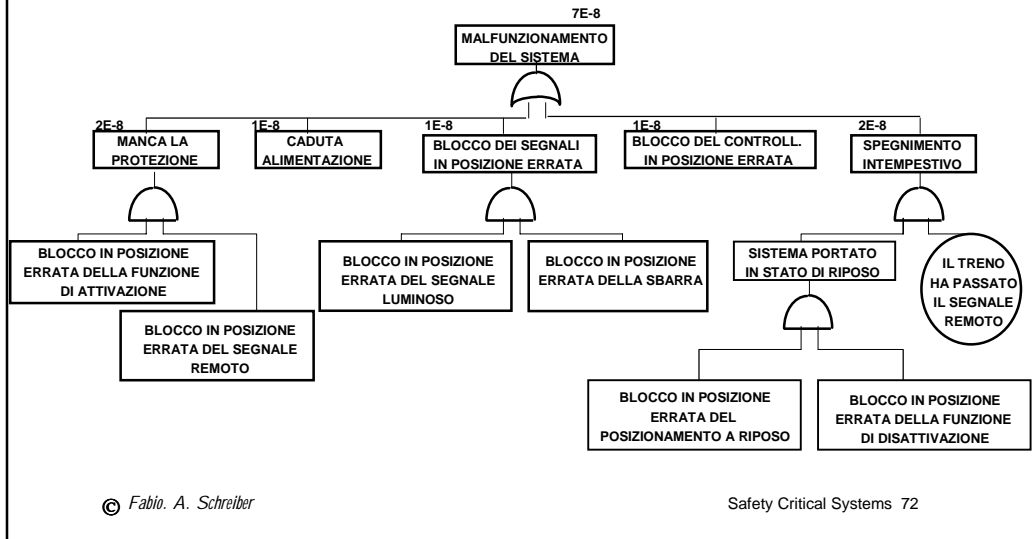
## ESEMPIO PASSAGGIO A LIVELLO: ETA



© Fabio. A. Schreiber

Safety Critical Systems 71

## ESEMPIO PASSAGGIO A LIVELLO: FTA



## BIBLIOGRAFIA

- VILLEMEUR A. - **RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY ASSESSMENT** - WILEY, 1991
  - VOL 1° **METHODS AND TECHNIQUES**
  - VOL 2° **ASSESSMENT, HARDWARE, SOFTWARE AND HUMAN FACTORS**
- BARLOW R.E., PROSCHAN F. - **MATHEMATICAL THEORY OF RELIABILITY** - WILEY, 1965