AFFIDABILITA' DEI SISTEMI COMPLESSI

a cura di Angelo Boni

Redox s.r.l. Via Manodori 7 – Reggio Emilia, Italy

REDOX
PROGETTI PER L'INDUSTRIA

- **Che cos'è l'affidabilità di un sistema complesso?**
  L'affidabilità è la capacità di un sistema di operare nel modo dovuto, senza malfunzionamenti o guasti.

- **Come definire l'affidabilità di un sistema?**
  (L'esempio è preso da un'azienda che produce sistemi di gestione merci tramite RFID)

  Definizione vaga: "Questo sistema non si deve rompere".

  Definizione corretta: "Il sistema composto da un insieme di 5 computer, 5 postazioni di lettura RFID, 2 stampanti, un ponte radio, un server ed un gruppo di continuità deve funzionare senza guasti per almeno tre anni, operando in condizioni normali".

- **La definizione stessa di guasto è ambigua**:

  il bloccaggio momentaneo di un computer sotto Windows ed il relativo riavvio è da molti ritenuto un funzionamento “quasi” normale.

  Per un utente Apple o Linux, il bloccaggio del computer è ritenuto un guasto da investigare.

Possiamo distinguere per chiarezza tre classi di guasto:

- **Tipo 1**: blocco totale del sistema

  E' necessaria l'assistenza e/o parti di ricambio per ripristinare il sistema.

- **Tipo 2**: bloccaggio temporaneo del sistema

  Ripristino da personale non qualificato.

- **Tipo 3**: difetti leggeri nelle funzionalità del sistema che si ripristinano senza l'intervento dell'operatore.

Introducendo l'MTBF (Mean Time Between Failures)

L'MTBF esprime il tempo medio di guasto del sistema. La definizione corretta di affidabilità data prima per il nostro sistema di esempio contiene tutti i dati per calcolare l'MTBF.

Vediamo in dettaglio:

Condizioni di utilizzo normali nel nostro esempio significano:

10h al giorno per 300 giorni/anno = 3000 h/anno per 3 anni = 9000 h complessive

La vita richiesta al sistema sarà perciò di 9000 h totali.

Sorgono queste considerazioni:

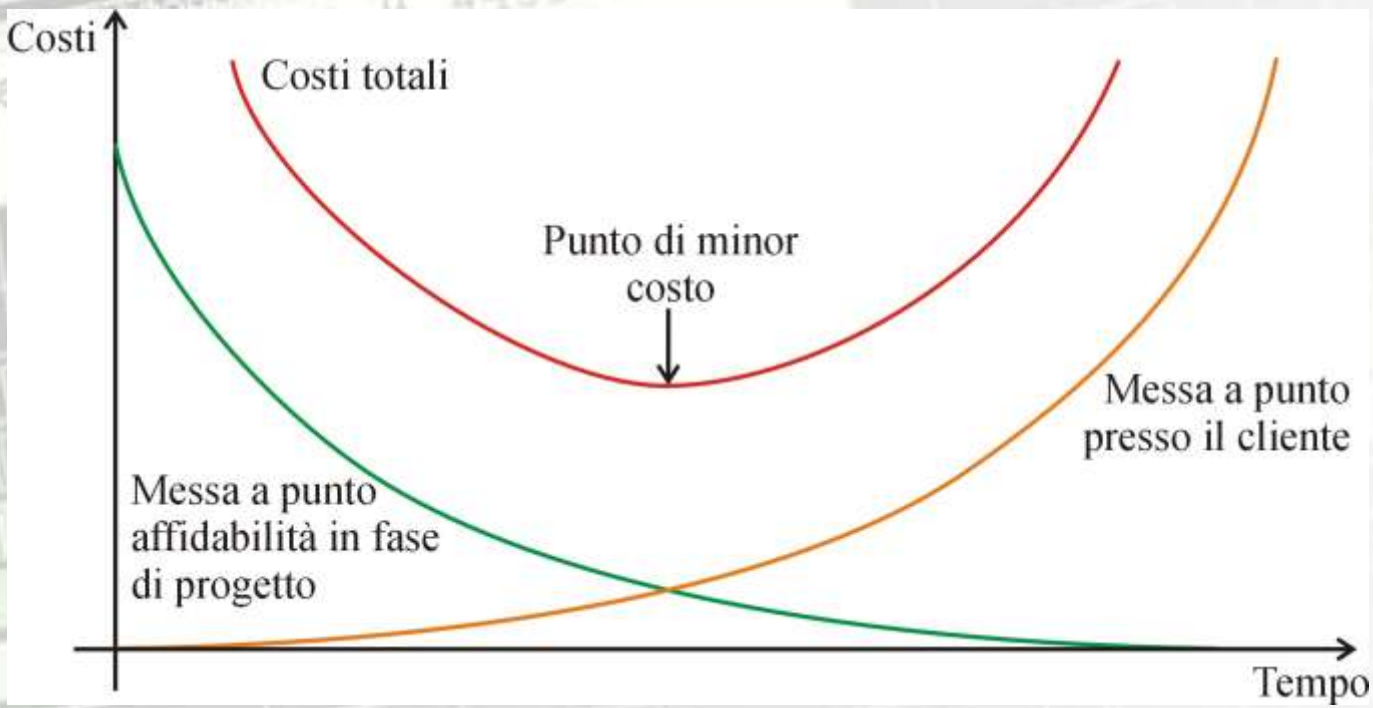
a) Il guasto di uno dei 5 computer o di un lettore RFID, oppure di una delle 2 stampanti, in generale non produce un collasso del sistema, al massimo qualche disagio.

b) Il guasto del ponte radio o del server, invece bloccano completamente il sistema.

c) IL gruppo di continuità è un elemento unico, ma non indispensabile nel sistema, in quanto la sua rottura lascia il sistema comunque funzionante. La sua MTBF in questo caso non viene conteggiata.

Le apparecchiature ridondanti, quali computer, stampanti lettori RFID possono avere una vita dalle 2 alle cinque volte la MTBF, in quanto si può accettare che qualcuno di questi si guasti entro i tre anni di vita utile. Il ponte radio ed il server invece non si devono guastare, è quindi corretto in prima approssimazione scegliere una vita utile 10 volte quella attesa, cioè 90.000 ore. La progettazione del sistema dovrà perciò tener conto di questi dati.

➢ Quanto costa instaurare un sistema di controllo dell' affidabilità nell' Azienda?



- Gestire l'affidabilità dei prodotti nell'Azienda può costare meno di quanto già non si spenda oggi globalmente per la gestione dei resi e dei guasti. Molte aziende, tenendo conto del danno di immagine per cattivi funzionamenti, spostano il punto di pareggio della curva molto più a destra (zero defect)

REDOX
PROGETTI PER L'INDUSTRIA

Introduciamo la "Failure Analysis"
(analisi dei meccanismi di guasto)

La FA si è evoluta negli anni 60, è stata usata nei programmi spaziali e militari, come tecnica di analisi e predizione dei meccanismi di guasto.

Essa si occupa di analisi dei guasti correlati a:

Progetto

Produzione

Testing

Uso

Manutenzione

REDOX
PROGETTI PER L'INDUSTRIA

➢ Guasti correlati al progetto:

- Progetto non in linea con le richieste del cliente
- Guasti inerenti alla componentistica elettronica
- Guasti inerenti alla tipologia di circuito utilizzata
- Guasti inerenti al FW ed al SW
- Guasti inerenti alla meccanica
- Guasti inerenti al test del progetto

➢ Guasti correlati alla produzione:

- Mancanza di documentazione adeguata
- Processo produttivo non adatto
- Componentistica non adeguata
- Scarsa ingegnerizzazione del progetto

➢ Guasti correlati al testing:

- Test insufficienti
- Test non parametrici
- Test con strumentazione non calibrata
- Test non correlati all'uso del prodotto

➢ Guasti correlati all'uso ed alla manutenzione:

- Imballaggio insufficiente, spedizione non controllata
- Impiego in condizioni oltre i limiti
- Istruzioni insufficienti o non chiare
- Mancanza di manutenzione programmata
- Rete di assistenza insufficiente / impreparata

➢ Come può ovviare la FA ai meccanismi di guasto elencati?

- Di seguito viene presentata un'antologia di tecniche per migliorare l'affidabilità dei sistemi complessi.

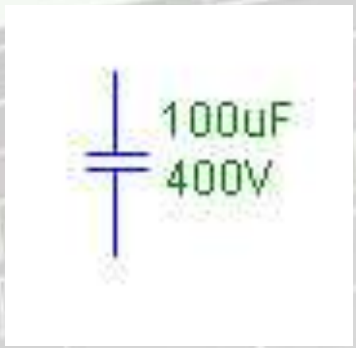
- La presentazione, per ovvi motivi di spazio, è ben lungi dall'essere completa, lo scopo principale è di promuovere la cultura dell'affidabilità.

- Questa presentazione è inoltre una buona base per stendere documenti operativi sulle procedure di affidabilità dei prodotti e/o sistemi.

Affidabilità dei componenti del sistema

- Ogni componente o parte elettronica o meccanica ha una vita propria, che è funzione della percentuale di utilizzo, della temperatura di lavoro, della criticità del valore e dello stress meccanico ed ambientale cui il componente è sottoposto.

- Ogni componente ha meccanismi di guasto diversi. Il progettista deve conoscere la tipologia di guasto dei diversi componenti per realizzare circuiti affidabili.



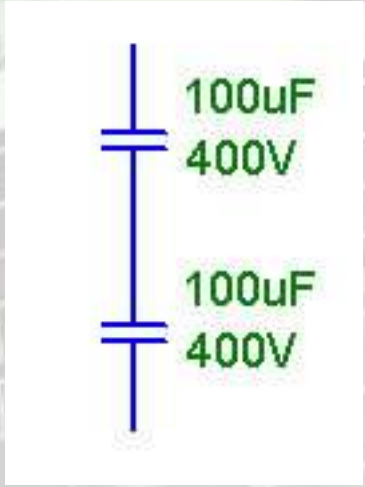
- Esempio: Condensatore elettrolitico
  Durata 1000 ore a 400V e 85C°
  Meccanismo di guasto: calo di capacità, aumento della resistenza serie, circuito aperto.

REDOX
PROGETTI PER L'INDUSTRIA

- Utilizzando lo stesso condensatore a 75C° avremo una vita utile doppia, di 2000 ore. A 65C° la vita si allungherà fino a 4000 ore.

- Se la tensione applicata al condensatore viene ridotta del 20%, di nuovo la vita utile raddoppia.

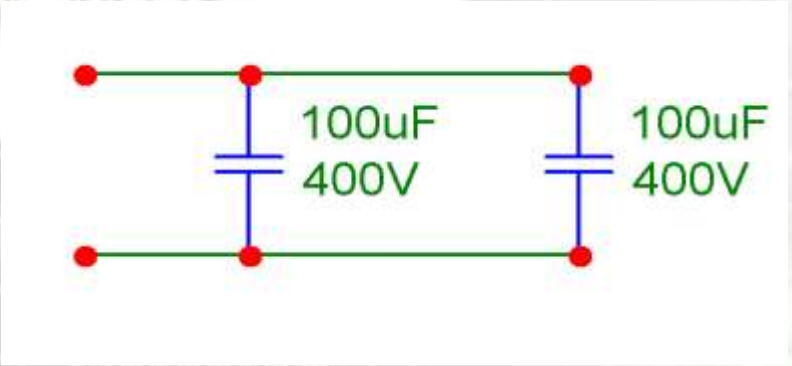
  Se uso il condensatore a 65C° e 360V la vita diventerà 8000 ore!



Se pongo in serie due condensatori ed applico 800V a 85C°, la vita sarà di 500 ore, considerato che ciascuno dei due condensatori può aprirsi, raddoppiando la probabilità di guasto.

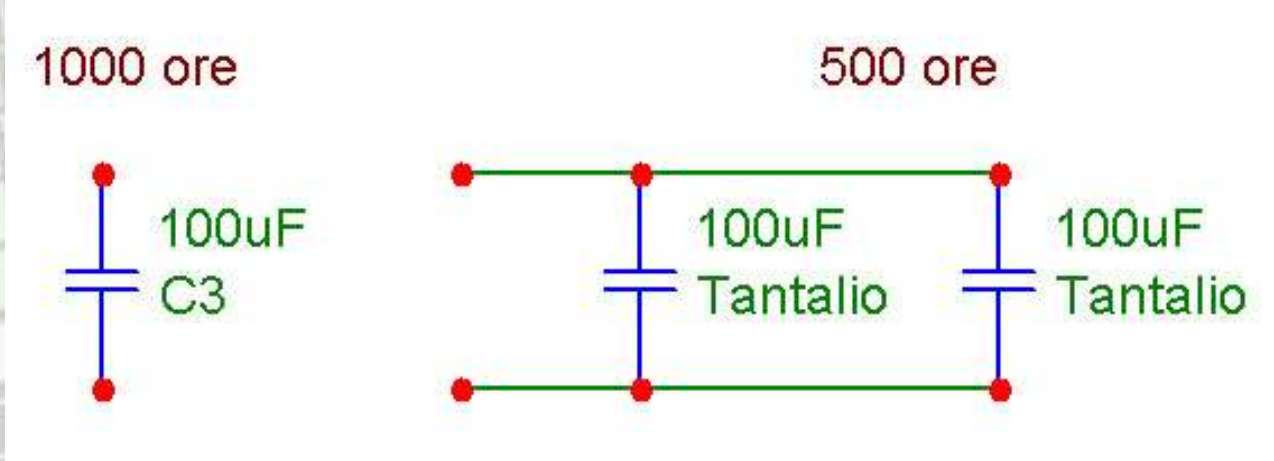
REDOX
PROGETTI PER L'INDUSTRIA

- Una soluzione interessante dal punto di vista dell'affidabilità è la connessione in parallelo di due condensatori.



- Ci si aspetterebbe, per analogia, il doppio della vita, se uno si rompe, l'altro ancora funziona. In realtà il caso è molto più favorevole e ci avviciniamo alle 10.000 ore. Il meccanismo di guasto del condensatore è la riduzione del valore di capacità e l'aumento della resistenza interna. La vita di 1000 ore è calcolata per una variazione del 20% di entrambe, mentre il circuito parallelo può sopportare una variazione del 50% ed ancora operare correttamente. In queste condizioni la vita del parallelo è circa dieci volte maggiore, ossia 10.000 ore.

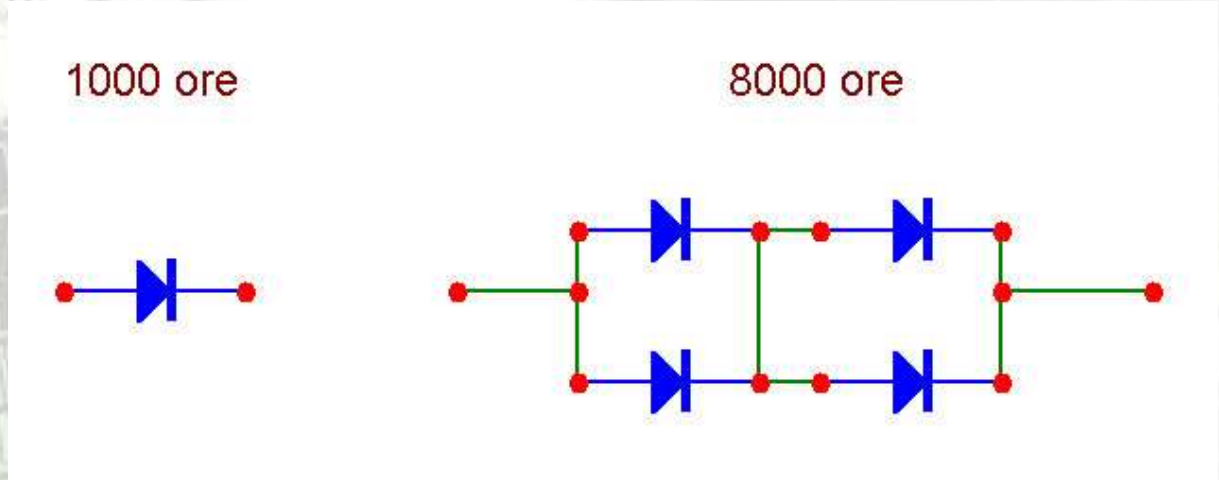
- **Non bisogna però pensare che tutti i condensatori posseggano lo stesso meccanismo di guasto.**
- I condensatori al Tantalio, per esempio, tendono a guastarsi andando in corto-circuito.



Quindi la vita totale si dimezza ponendone due in parallelo. Esiste tuttavia un rimedio, che è quello di porre in serie ad ogni condensatore una pista fusibile che si apra in caso di corto circuito.

REDOX
PROGETTI PER L'INDUSTRIA

- **Esistono inoltre componenti che hanno meccanismi di guasto sia in apertura che in corto-circuito**, ad esempio i diodi.



- La connessione serie-parallelo ne aumenta notevolmente l'affidabilità.
- Questo circuito è stato intensivamente usato nelle prime sonde spaziali.
- I semiconduttori di oggi sono in generale molto affidabili e solitamente non c'è bisogno di questi artifici circuitali.

➢ Affidabilità dei componenti meccanici

- I principali componenti meccanici sono i connettori, le scatole ed i contenitori, gli interruttori e le tastiere, i relè e le ventole, i cavi di connessione, i PCB.
- I meccanismi di guasto generati da questi componenti sono naturalmente molto diversi dai precedenti.
- La corrosione, la compatibilità elettrochimica e la compatibilità fra gomme, plastiche, solventi ed olii, decidono dell'affidabilità a lungo termine dei componenti meccanici, specie se esposti alle intemperie.

- **I connettori, gli interruttori, i relè** hanno una corrente minima di funzionamento (oltre che una massima) al di sotto della quale tendono a non chiudere il contatto o ad avere un funzionamento intermittente. Alcuni componenti di questo tipo sono realizzati con il contatto biforcato o multiplo per ridurre la possibilità di guasto. Ad alte correnti si può invece verificare l'incollaggio dei contatti. Nei relè e negli interruttori la vita è misurata più in numero di operazioni che in ore di lavoro.
- **Le ventole** hanno il problema generale dell'intasamento o del bloccaggio, specialmente in ambienti polverosi o sporchi. Esistono ventole ad alta affidabilità, ma solo la manutenzione programmata (pulizia) può dare risultati certi.

- **I cavi** se protetti adeguatamente da fusibili sono soggetti ai soli guasti meccanici (calpestio, strappo, taglio), solo eccezionalmente in ambienti molto aggressivi potranno avere problemi di compatibilità chimica e perdita di isolamento.

- **I PCB**, cuore di ogni sistema elettronico, meriterebbero da soli un trattato sull'affidabilità.

  I meccanismi di guasto possono essere: cattiva metallizzazione dei fori, delaminazione dovuta ad un processo di saldatura troppo caldo, bave e corti circuiti dovuti ad una cattiva incisione, finitura superficiale ossidata e/o non planare, solder non resistente o disallineato……. ecc. ecc.

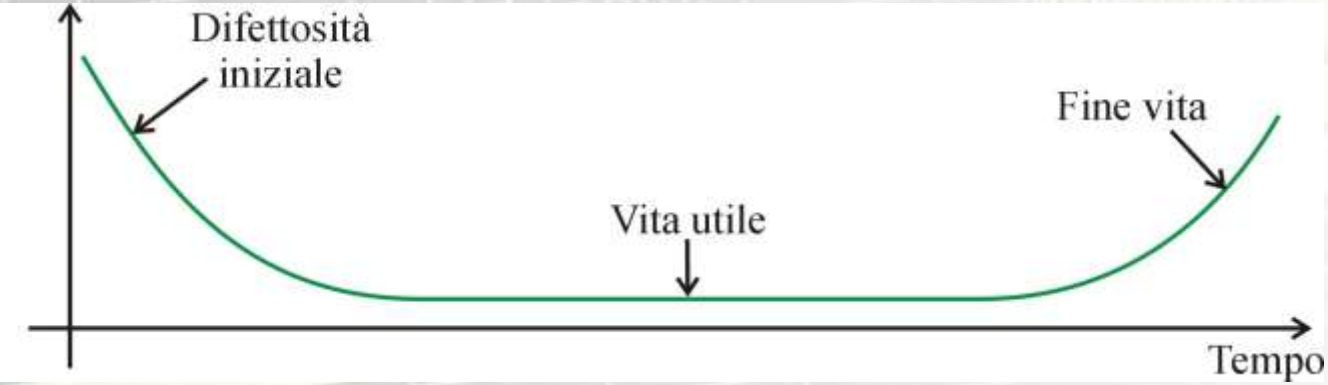
➢ Come reperire i dati di affidabilità e di MTBF dei componenti?

- Le norme MIL-STD americane sono una fonte esauriente di dati storici su ogni tipo di componente.
- I data sheet od i siti dei principali produttori contengono informazioni su MTBF o FIT (Failure in Time).
- I dati storici provenienti dai prodotti dell'azienda, dagli installatori, dall'assistenza.

➢ Quando sono validi i dati di Affidabilità?

- In generale i dati di affidabilità sono validi se i componenti non sono usati al di là dei limiti massimi. Se un qualsiasi apparato industriale viene connesso ad una rete trifase non filtrata, ove in caso di commutazione anomala di linea si raggiunge il doppio della tensione nominale, ebbene tale apparato durerà fino all'accadere di tale fenomeno.
- Un cattivo progetto, in cui alcuni componenti (od anche uno solo) lavorino a temperature eccessive, a tensioni troppo elevate, senza protezione dalle inversioni di polarità e così via….. è destinato ad avere vita breve.
- Se la valutazione del fattore di utilizzo è sbagliato, la vita del sistema sarà differente in proporzione. Ad esempio: se un sistema di amplificazione è nato per sonorizzare un ambiente e viene invece montato su un autobus potremo aspettarci, a causa delle vibrazioni e delle variazioni di temperatura una vita 10-15 volte inferiore.
- Solo nel caso il prodotto od il sistema sia progettato correttamente per l'uso richiesto, possiamo fare un analisi di affidabilità che abbia un senso compiuto.

- La produzione, il collaudo e l'imballo non devono introdurre difettosità nel prodotto.
- Il FW / SW che governa il sistema deve essere privo di errori significativi.
- La distribuzione della difettosità deve essere compatibile con la durata del sistema.



La difettosità presenta una curva a "vasca da bagno", ove la difettosità iniziale elevata può essere intercettata dal Burn-in, mentre l'aumento di difettosità a fine vita prodotto può essere evitato solo con il riprogetto ad MTBF più lunga. Un esempio per tutti, se un prodotto deve durare 5 anni ed al suo interno ha una batteria di back up che dopo 3 anni si scarica, avremo il 100% del prodotto non funzionante a 5 anni.

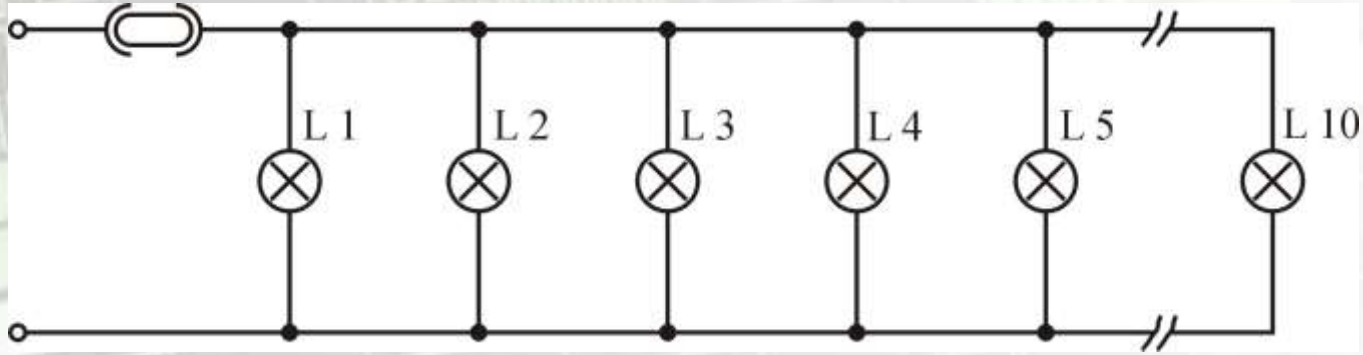
➢ La failure analysis del sistema

- Finora abbiamo analizzato i meccanismi di guasto dei singoli componenti e le loro interazioni semplici in serie-parallelo.
- Possiamo spingerci molto più in là analizzando i meccanismi di guasto nei vari blocchi del sistema.
- **Questo approccio è definito FMEA (Failure Modes and Effects Analysis).**
- Possiamo dividerlo in due sottoinsiemi:

  FMEA dell'HW

  FMEA del FW/SW

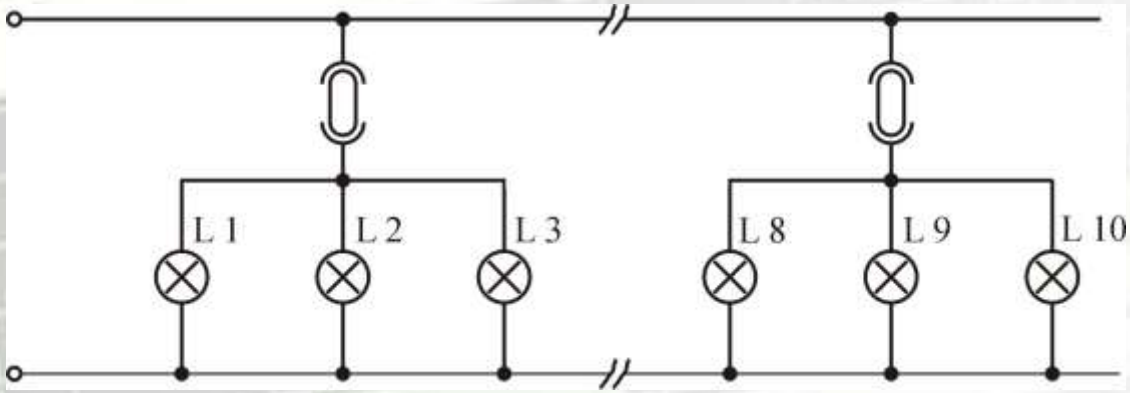
- **FMEA dell'HW**
- A titolo di esempio vediamo un gruppo di 10 lampade connesse sotto allo stesso fusibile. Ogni volta che una lampada brucia crea un momentaneo corto circuito, che fa saltare il fusibile e mette al buio l'intera area.



- Se modifichiamo il circuito, ponendo un fusibile in serie ad ogni lampada (o se troppo costoso in serie ad ogni gruppo di tre lampade), avremo che la bruciatura di una lampada porrà al buio solo una zona molto limitata dell' area, eliminando il black-out.

REDOX
PROGETTI PER L'INDUSTRIA

- In questo modo l'affidabilità è sicuramente aumentata, con un aggravio di costo contenuto.



- L'esempio scelto è volutamente molto semplice, ma si lascia alla valutazione dei presenti l'impatto che può avere sulla qualità dei prodotti che un'azienda commercializza e/o produce, l'applicazione dei criteri di analisi FMEA, specialmente in un mercato caratterizzato dalla rapida evoluzione del prodotto.

- **FMEA del FW/SW**
- L'affidabilità del FW passa per alcuni presupposti di standardizzazione:
  - E' necessario scrivere il FW in linguaggi ad alto livello. (Linux, C Ansi standard, Visual basic, ecc.). Da evitare per quanto possibile l'uso del linguaggio macchina.
  - Il FW deve essere comprensibile e manutenibile.
  - Il FW deve essere ragionevolmente robusto (non deve ignorare gli errori).
  - Il FW deve essere espandibile.
  - Il FW deve essere efficiente.
  - Il FW deve essere testabile.

Più in dettaglio:

- Le variabili, o le costanti non possono chiamarsi Pippo, Verona, Palle o 233XKMN++ a discrezione dei programmatori. Una variabile di ingresso incomincerà per In…. e poi a seguire i dati di detto ingresso. Una variabile di tempo, al pari, incomincerà per T…. e così via.
- Tutti i settaggi iniziali, le password, le calibrazioni, saranno scritte in almeno tre diverse locazioni di memoria, ed all'inizializzazione in caso di disparità verrà fatto il recovery della locazione fallata.
- I registri usati dal programma verranno artificialmente "sporcati" con dati sbagliati per vedere se il programma è in grado di recuperare da situazioni anomale.
- Il test del FW comprenderà l'analisi su carta dello stato delle variabili e dei registri, dell'azzeramento dei medesimi al cambio d'uso (evitarlo se possibile).

Ed inoltre:

- Verranno previsti WDT multipli, utilizzando i counter interni o gruppi RCD esterni per monitorare il bloccaggio del Micro e dei DSP.
- Verranno predisposti dei contatori diagnostici di errore per monitorare ad esempio il N° di byte interpolati nell' audio, il N° di recovery dei settaggi e delle password, il numero di volte che i WDT sono andati in timeout, ecc. ecc.
- **IL rilascio di una versione di FW è una cosa seria, non si può rilasciare una versione di FW alle 10, un'altra a mezzogiorno ed una terza alle 17,30!!!!**
- Tutto questo può sembrare banale, ma l'80% dei problemi di SW/FW vengono eliminati attraverso queste semplici precauzioni.

- **Cosa può fornirvi REDOX ?**

- Failure analysis, FMEA ed in generale analisi delle problematiche di qualità
- Analisi dei resi dal campo per migliorare l'affidabilità del prodotto
- Progettazione completa ad alta affidabilità, a norme MIL o a normativa del cliente
- Progettazione di banchi di collaudo automatico, funzionali e parametrici, per alta frequenza e Microonde, per applicazioni di alta potenza
- Produzione di alta qualità con macchinari di ultima generazione per Fine pitch, BGA, montaggi in doppia faccia, secondo lo standard RoHS

- Visitate il nostro sito: www.redoxprogetti.it
- Contattateci a: info@redoxprogetti.it

- Redox è certificata ISO9001:2008
- Redox è accreditata alla RETE ALTA TECNOLOGIA
- Redox è LABORATORIO MIUR
- Redox è iscritta all'ALBO DELLE RICERCHE del CNR

Ministero dell'Istruzione dell'Università e della Ricerca

Anagrafe Nazionale delle Ricerche

Roma, li 28/6/2011
Prot. n. 21

Redox S.R.L.
Via Manodori, 7
42100 REGGIO EMILIA (RE)

Oggetto: Iscrizione schedario Anagrafe Nazionale delle Ricerche, Art. 64, comma 1, DPR 11 luglio 1980 n. 382
Attribuzione Codice Definitivo

Con riferimento alla richiesta di iscrizione allo Schedario dell' Anagrafe Nazionale delle Ricerche si comunica che vi è stato attribuito il codice definitivo:

602598LD

Detto codice è obbligatorio per accedere ai finanziamenti pubblici in materia di ricerca e/o formazione e costituisce un identificativo dell'ente per la finalità previste dal D.P.R. 11/7/1980 n. 382, inoltre dovrà essere riportato in tutti gli atti previsti dalla normativa vigente in tema di finanziamenti per la ricerca scientifica e tecnologica.

Si ricorda che l'iscrizione all'Anagrafe Nazionale delle Ricerche ha validità triennale ed il soggetto è tenuto ad aggiornare costantemente la propria posizione qualora intervengano delle variazioni alle informazioni a suo tempo comunicate, e a procedere, decorso il triennio, con il rinnovo dell'iscrizione; in caso di mancato aggiornamento triennale il soggetto è cancellato dall'ANR.

Si precisa che l'inserimento nello schedario dell'Anagrafe Nazionale delle Ricerche non certifica e/o attesta alcuna competenza del soggetto iscritto nel campo della ricerca e/o della formazione.

IL DIRIGENTE
(Dott. Massimo Ghilardi)

DNV

DET NORSKE VERITAS

QUALITY MANAGEMENT SYSTEM CERTIFICATE

Certificate No. / Certificato No. CERT-14307-2004-AQ-BOL-SINCERT

Si attesta che / This certifies that

IL SISTEMA DI GESTIONE PER LA QUALITÀ DI / THE QUALITY MANAGEMENT SYSTEM OF

REDOX S.r.l.
Via Manodori, 7 - 42100 Reggio Emilia (RE) - Italy

È CONFORME AI REQUISITI DELLA NORMA PER I SISTEMI DI GESTIONE PER LA QUALITÀ
CONFORMS TO THE QUALITY MANAGEMENT SYSTEMS STANDARD

UNI EN ISO 9001:2000 (ISO 9001:2000)

Questa certificazione è valida per il seguente campo applicativo:
This certificate is valid for the following products or services:

Progettazione, prototipazione, produzione ed assistenza post vendita di apparecchiature elettroniche HW e SW su idea del cliente

...pping, manufacture and after-sales assistance of electronic HW and SW devices according to customer ideas

...ARCELLO CAPURANCO

SINCERT

per l'Organismo di Certificazione
For the Accredited Unit
Det Norske Veritas Italia S.r.l.

Leonardo Gondro Zerbi
Management Representative

Laboratorio MIUR
Ministero dell'Istruzione dell'Università e della Ricerca

RETE ALTA TECNOLOGIA
EMILIA-ROMAGNA
HIGH TECHNOLOGY NETWORK

REDOX
PROGETTI PER L'INDUSTRIA

Grazie per l'attenzione