



**Impatti operativi del 40°
aggiornamento della circolare
285/2013 della Banca d'Italia e
regolamento DORA. Le regole per
la resilienza operativa digitale nel
settore finanziario**

Continuità operativa in DORA

Ing. Massimo Marrocco
Vice Presidente Commissione Informatica
Ordine degli Ingegneri della Provincia di Roma

Roma, 20 marzo 2024



Il trattamento del rischio come base delle scelte progettuali: Continuity by Design an by Default”



Assieme agli aspetti di cyber security la resilienza operativa del settore finanziario dipende anche dalla capacità dell'infrastruttura logistica ed impiantistica di garantire il funzionamento senza interruzioni dell'hardware in produzione



RISCHIO: *fattore di incertezza nel raggiungimento degli obiettivi (di Continuity)*

ISO 31000 2.1

Risk: effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)



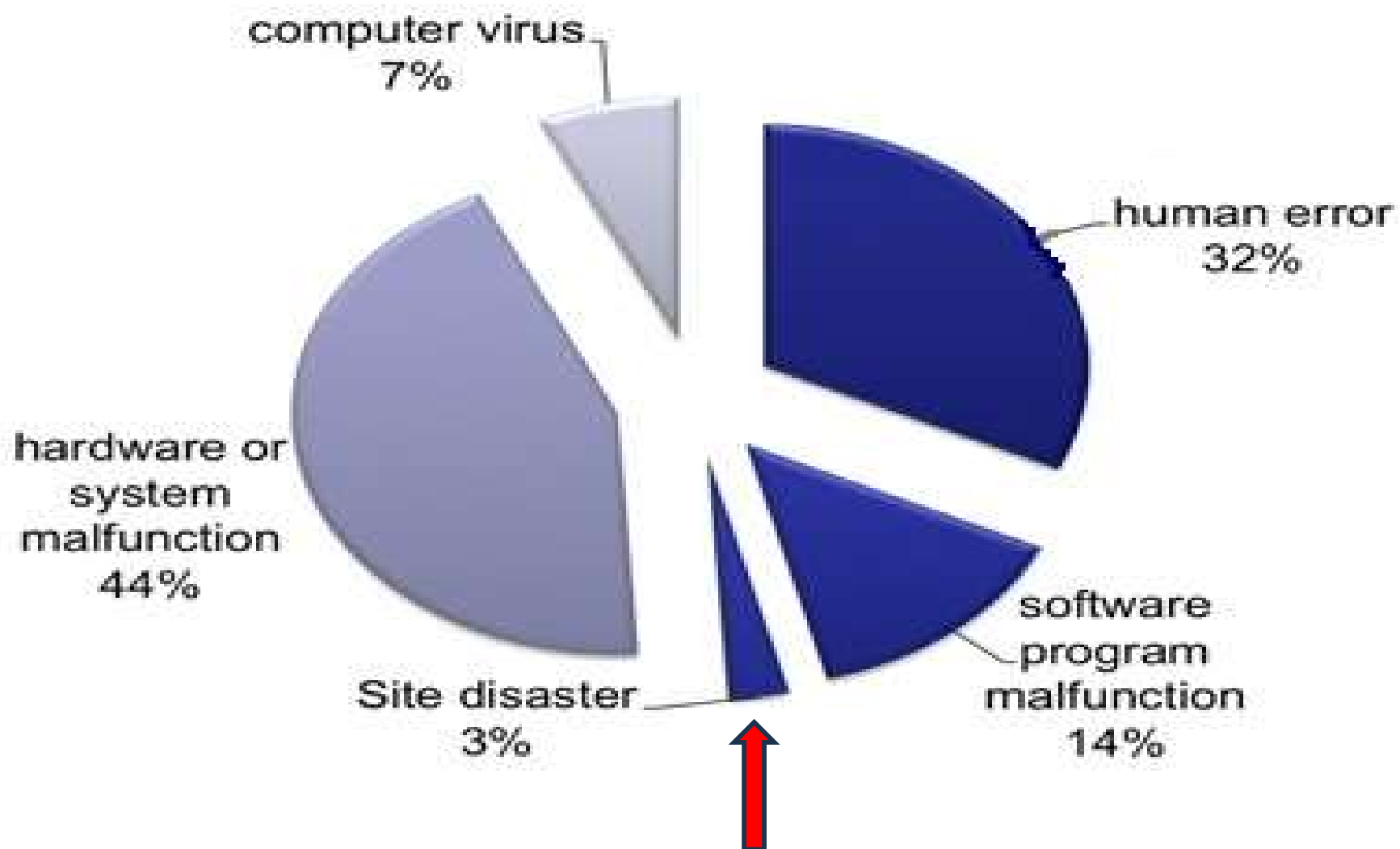
In questo intervento parleremo di obiettivo Continuità Operativa che nella norma ISO 22301 è definita:

Capacità dell'Organizzazione a continuare il rilascio di prodotti o servizi ad un predefinito livello in seguito ad incidenti distruttivi



Esempi di Rischi

Tipologia rischio	Descrizione di riferimento
Legati alla produzione	Rischi di security insiti nella attività dell'Organizzazione intesa come processo di produzione di servizio/prodotto, rischi da obblighi normativi
Contesto locativo	Rischi insiti nella collocazione geografica e tipologia edilizia degli immobili utilizzati dall'Organizzazione: terremoti, allagamenti, fulmini, inondazioni, crolli, smottamenti
Danni al patrimonio	Furti, incendi, sabotaggi, attentati, frodi finanziarie, furto proprietà intellettuali.
Danni di compliance ambientale	Emissioni nocive gas , liquidi e solidi , rifiuti, emissione elevate di: rumori, vibrazioni, onde magnetiche,
Danni con azione di malintenzionati	Attacchi informatici, infedeltà dei dipendenti, furto dati riservati, rapimenti di dipendenti, attacchi all'immagine aziendale, attacchi NBC,
Altri danni derivati da	Fermo della produzione, pandemie, modifiche equilibri politici del paese, richieste malavita organizzata, fermo dei vettori di trasporto, blocco della circolazione viaria, scioperi,





Rapporto incidente-rischio in CO

Abbiamo detto che il Rischio è l'effetto dell'incertezza nel raggiungimento degli obiettivi che nel caso della Continuità Operativa sono la prosecuzione costante del rilascio di prodotti o servizi che può, tale attività di rilascio, essere oggetto di rischio di interruzione a seguito di incidenti distruttivi (per esempio terremoti, sospensione erogazione energia elettrica, incendi, attacchi informatici, alluvioni, frane, crolli, pandemie, attacchi terroristici, ecc), quindi l'incidente è un rischio che deve essere ridotto con l'implementazione di un progetto in grado di porre rimedio alla perdita di produzione/servizio di ogni asset costituente la catena di produzione, comprese le risorse umane.



Approccio al rischio

- ✓ **evitare il rischio:** non eseguire le attività che comportano i rischi individuati (es rinunciare ad un settore di attività o alla produzione di qualcosa i cui rischi associati non sono trattabili, per esempio perché il trattamento risulta troppo oneroso);
- ✓ **spostare il rischio o parte di esso su un altro soggetto:** es. assicurazione, outsourcing. In questo caso però è bene ricordare che alcuni rischi non possono essere spostati (es responsabilità penali) oppure, non tutto il rischio può essere spostato (es il danno di immagine collegato al fermo di un servizio determinato da un outsourcer rimane su chi eroga il servizio);
- ✓ **accettare il rischio:** in questo caso, ove consentito (non è possibile accettare il rischio della mancata applicazione della legge) devono essere cambiati i livelli di propensione al rischio dell'Organizzazione ed eventualmente le azioni di protezione (esempio riserve in bilancio);
- ✓ **trattare il rischio:** individuare contromisure (misure di riduzione Attive, Passive e Organizzative di Opposizione) atte a ridurre (controllare) i rischi per riportarli nelle soglie di accettabilità definite



Misure Passive Attive Organizzative di Opp.

Per semplificare l'indicazione di tutte le misure di riduzione del rischio le suddivideremo in tre tipologie di base:

- Misure passive
- Misure attive
- Misure organizzative

In seguito vedremo come l'implementazione di una o più di tali misure, anche di tipo diverso e contemporaneamente, rappresenta un utile modello di riferimento per la gestione del rischio

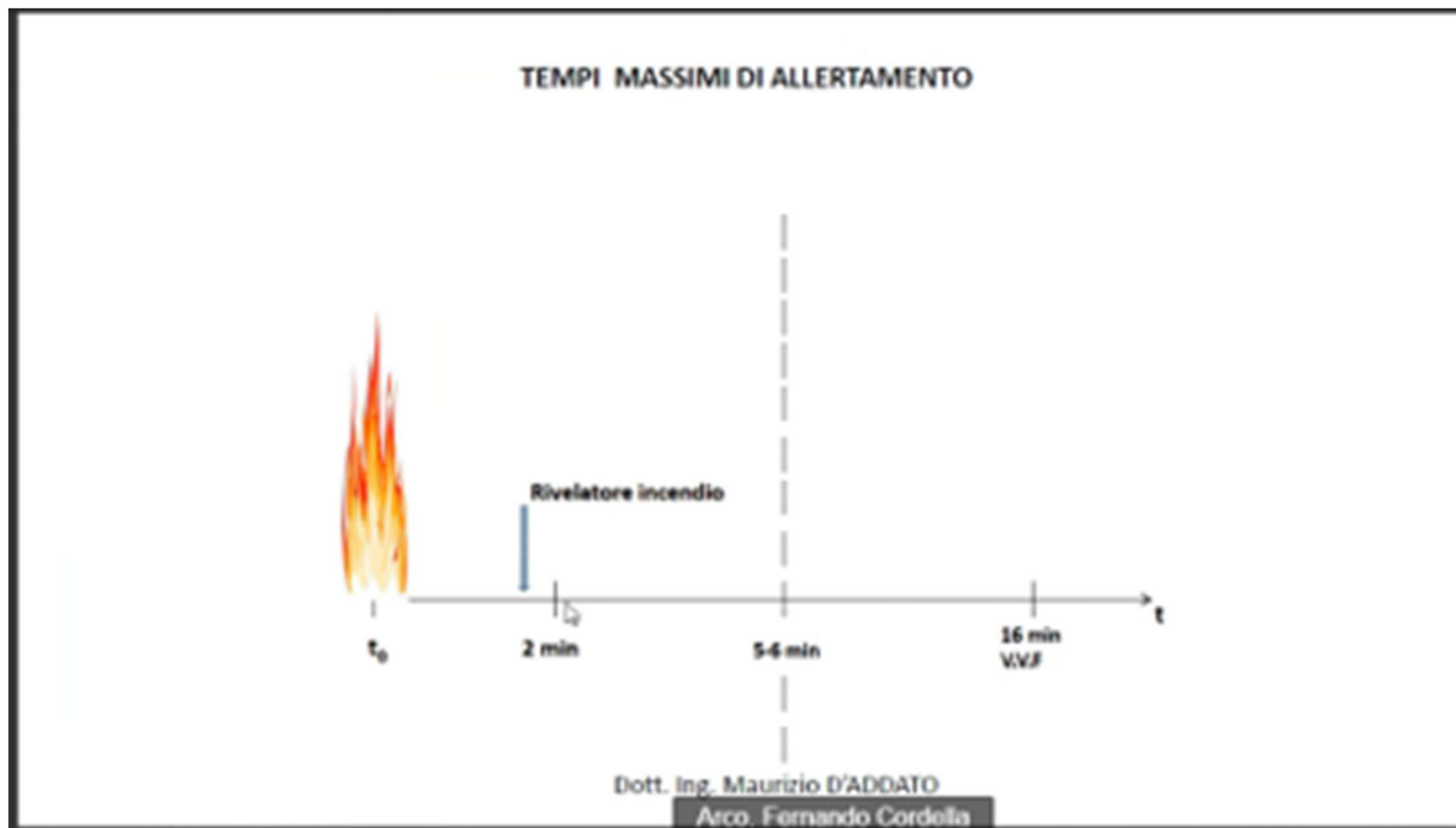


Equazione del Tempo di Opposizione

Funzione che lega gli effetti delle Misure Passive, Attive e Organizzative di Opposizione al fine di ridurre o azzerare il concretizzarsi del DANNO, secondo la seguente equazione:

- a) **Tempo di ritardo** (misura passiva)
- b) **Tempo di evidenziazione** (misura attiva)
- c) **Tempo di attuazione contromisura** (Organizzativa di Opposizione)

$$T_r > T_e + T_o$$





MTPD

Maximum Tolerable Period of Disruption

Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

Maximum acceptable outage

tempo massimo di guasto a seguito di impatti negativi, che potrebbero verificarsi e causare il fermo della produzione/ servizio o l'esecuzione di un'attività, fino a diventare con livello inaccettabile (della produzione/servizio)



TIA-ANSI 492-A

Classificazione dell'affidabilità dei CED
TIER (da I a IV)



Da quanto abbiamo finora detto , in particolare relativamente alle criticità legate al mantenimento in funzione delle strutture ICT, si comprende come sia vitale ed indissolubile il legame tra la continuità operativa dei processi critici (mission critical) ed il livello di disponibilità dei sistemi impiantistici che li sostengono, primo fra tutti quello Power (alimentazione elettrica) seguito dal Cooling (condizionamento) e dai presidi di monitoraggio e controllo



Per spiegarci meglio facciamo degli esempi di specie:
UPS Off line o On line?
Gas estinguente a nebulizzazione o Novec 1301?
Interruttori standard o di alta qualità prestazionale?
Distribuzione a barre o a cavi?
Monitoraggio tecnologico con interruttori motorizzati?
Gruppi elettrogeni di produzione nazionale o meno?



Teniamo sempre in massima considerazione le quattro macro aree che costituiscono le componenti di supporto logistico alle applicazioni ICT:

1. Sistema elettrico (dal punto di consegna gestore alla singola PDU)

2. Sistema CDZ (dal sistema di alimentazione elettrica servizi alla singola bocchetta di distribuzione)

3. Sistemi di sicurezza (controllo accessi, monitoraggio tecnologico, antincendio, allagamento..)

4. Gestione e manutenzione (h24, formazione, tracing, continuo miglioramento)



Ora che abbiamo identificato gli asset chiave ritorniamo al concetto di «Fidatezza» nel significato di:

l'insieme delle proprietà che descrivono la disponibilità e i fattori che la condizionano:

- ✓ *Affidabilità*
- ✓ *Manutenibilità*
- ✓ *Logistica della manutenzione*



La fidatezza, nel nostro caso, implica verificare a priori l'esistenza della ragionevole certezza che ogni singolo componente della «catena» della continuità sia in grado di dare il suo specifico contributo al prodotto in maniera sempre ed ininterrottamente soddisfacente in qualsiasi situazione ci si venga a trovare, nel caso di guasto sia facilmente sostituibile senza necessità, ove possibile, di tecnici altamente specializzati.



In termini generici si tratta di mantenere sempre prioritaria la fidatezza come obiettivo di progetto che si sostanzia in una organizzazione di componenti tecnologiche e fattori umani finalizzati a progettare, realizzare e mantenere la struttura di « Continuità operativa» in modo da rendere minimi e comunque accettabili i danni correlabili alle vulnerabilità del sistema nell'impossibilità di azzeramento dei rischi del contesto.



In concreto, per esempio, il sistema di alimentazione di un DC in continuità operativa non può essere la semplice somma di apparecchiature elettriche e cavi di collegamento progettati come se si trattasse di edifici di civile abitazione o uffici generici: nello scopo di fornire energia deve essere tenuto conto della differenza qualitativa della dimensione temporale di interruzione accettabile pari a max 0,002 sec. nel caso in esame.



Quindi il concetto base è che il livello atteso della prestazione elaborativa non è garantito senza adeguata efficienza dell'infrastruttura logistica

Livello affidabilità ICT $\leq$ Livello affidabilità site



Attualmente esistono varie tipologie di architetture ICT destinate alla continuità operativa le cui caratteristiche variano a seconda del tempo massimo di ripristino accettato ed ai limiti della tecnologia disponibile



RTO = 0

sito primario e sito secondario in «Mirroring Sincrono»

RTO > 24h<48h

sito primario e sito secondario in «Mirroring»

RTO > 48 h

sito primario elabora e sito secondario si attiva su dati salvati su supporti informatici

Dove è ammesso il DR può anche essere in cloud



RTO > 24h<48h

sito primario e sito secondario in «Mirroring»

Questa tipologia realizzativa è quella a medio grado di affidabilità perché i dati di input e di output raggiungono i due siti ma con una differenza temporale di elaborazione. Le strutture ICT sono interamente ridondate in ambienti di livello almeno TIER III:

PRO :

- ✓ RTO diverso da 0 ma comunque limitato = mantenimento livello elaborativo con accettazione rischio di danni per perdita elaborativa;
- ✓ Possibilità di collocare i due siti a maggiore distanza e quindi ridotto rischio in caso di calamità metropolitane;

CONTRO:

- ✓ costi di realizzazione e di gestione comunque alti per la necessità di presidio di tecnici specializzati h24/365;



RTO > 48 h

sito primario elabora e sito secondario si attiva su dati salvati su supporti informatici

Questa tipologia realizzativa è quella a grado di affidabilità minore perché l'elaborazione è attiva solo sul sito primario, mentre il sito secondario – spesso in locazione presso strutture terze – viene attivato solamente dopo la caduta del primario utilizzando copie degli ultimi dati disponibili su supporti digitali :

PRO :

- ✓ Costi di realizzazione e gestione più contenuti;
- ✓ Possibilità di distanziare il sito primario dal sito di recovery anche a livello continentale;

CONTRO:

- ✓ RTO molto elevato con assunzione del rischio perdite economiche per fermi elaborativi e perdite dati molto alte



Principi progettuali di infrastrutture destinate alla continuità operativa





Glossario base

- ✓ Disaster Recovery : piano di ripresa della produzione/servizio in caso di fermo del sito primario costituito da Hw, SW duplicati e risorse umane vitali che possano operare;
- ✓ Sovradimensionamento : modalità realizzativa che privilegia l'installazione di infrastrutture impiantistiche di livello di prestazioni superiore a quello necessario da progetto;
- ✓ Ridondanza : modalità realizzativa che impone la predisposizione delle infrastrutture impiantistiche necessarie in maniera duplicata , separate , protette ed equi fungibili (cioè una è in grado di sopperire completamente al fermo dell'altra) :
 - **N+1** accanto alla componente di servizio ne viene predisposta un'altra di pari prestazioni disponibile sul posto
 - **S** la seconda componente disponibile è accesa, funzionante ed in grado di subentrare alla principale in tempo reale



Glossario base

- ✓ Disaster Recovery : piano di ripresa della produzione/servizio in caso di fermo del sito primario costituito da Hw, SW duplicati e risorse umane vitali che possano operare;
- ✓ Sovradimensionamento : modalità realizzativa che privilegia l'installazione di infrastrutture impiantistiche di livello di prestazioni superiore a quello necessario da progetto;
- ✓ Ridondanza : modalità realizzativa che impone la predisposizione delle infrastrutture impiantistiche necessarie in maniera duplicata , separate , protette ed equi fungibili (cioè una è in grado di sopperire completamente al fermo dell'altra) :
 - **N+1** accanto alla componente di servizio ne viene predisposta un'altra di pari prestazioni disponibile sul posto
 - **S** la seconda componente disponibile è accesa, funzionante ed in grado di subentrare alla principale in tempo reale



All'origine delle best practices occorre sempre considerare la gestione del rischio secondo la ISO 31000:

Rischio uguale effetto di incertezza rispetto agli obiettivi

nel caso di Data Center (o attività produttive) in continuità operativa possiamo dire che tali obiettivi siano il mantenimento in produzione anche in caso di disastro e comunque in un ***predefinito livello minimo***.



Per il concetto di Continuità operativa è bene considerare che la capacità di mantenere la produzione è costituita da tre diversi fattori ugualmente critici:

- 1) Architettura Hardware e Software
- 2) Resilienza del sito (primario e secondario)
- 3) Disponibilità di risorse umane critiche



Da queste premesse consegue che la comune prassi progettuale deve essere ripensata nel caso in esame e ciò non solo nell'individuazione del corredo tecnologico da utilizzare ma soprattutto nella visione globale del progetto che deve prevedere scelte tecnologiche delle componenti selezionate non solo per la loro efficacia ma soprattutto per il loro contributo atteso nell'integrazione di sistema. Nell'ottica del mantenimento della continuità operativa la «catena tecnologica», intesa come insieme di asset di produzione, deve essere il ***più possibile omogenea nel livello di «fidatezza»*** che si vuole raggiungere.



MACRO AREE

- Analisi dei rischi da fattori esterni
- Caratteristiche costruttive dell'edificio con particolare attenzione alla superficie dove ubicare il CED all'interno dello stesso
- Indicazione delle caratteristiche prestazionali di progetto



- Sismicità e prossimità zone instabili;
- Allagamenti, straripamenti, dighe, invasi;
- Vulcani attivi ed emissioni polveri;
- Vicinanza a siti sensibili quali fabbriche chimiche , biologiche, depositi rifiuti pericolosi;
- Vicinanza a siti sensibili per attentati o sabotaggi;
- Pandemie;
- Vicinanza aeroporti ;
- Vicinanza siti militari;



- Sismicità e prossimità zone instabili;
- Allagamenti, straripamenti, dighe, invasi;
- Vulcani attivi ed emissioni polveri;
- Vicinanza a siti sensibili quali fabbriche chimiche , biologiche, depositi rifiuti pericolosi;
- Vicinanza a siti sensibili per attentati o sabotaggi;
- Pandemie;
- Vicinanza aeroporti ;
- Vicinanza siti militari;



In linea generale:

- Attrezzabilità del sito ed eventuali vincoli;
- Tipo della struttura portante e caratteristiche antisismiche;
- Tipo e portata dei solai, compatibilità con la posa di pavimenti sopraelevati;
- Tipo e caratteristiche di isolamento termico delle pareti;
- Resistenza passiva dei solai e delle pareti alla penetrazione;
- Quantità e caratteristiche dei vani porta e/o finestre;
- Grado di idoneità alla installazione di condutture e/o apparecchiature sia in orizzontale che in verticale;
- Idoneità al collegamento con l'esterno per il passaggio di macchinari.



Più in particolare:

Collocazione dell'area scelta all'interno del sito:

(si tratta di ottimizzare la posizione della superficie da allestire all'interno del volume coperto dell'immobile secondo i seguenti criteri generali)

- È preferibile una collocazione in un piano basso ma non il più basso perché quest'ultimo è generalmente interessato dai collettori di raccolta e distribuzione acque e quindi soggetto a rischio di perdite o reflussi;
- è preferibile una collocazione in una zona con pareti opache sia per garantire una migliore protezione contro le intrusioni che un maggior isolamento termico;
- I solai dei piani bassi hanno una portata compatibile con le esigenze dei CED, diversamente occorreranno interventi di rinforzo;



- È bene prendere in considerazione un'area facilmente sezionabile rispetto ai percorsi interni per garantire un miglior controllo degli accessi;
- Detta area deve essere facilmente raggiungibile da cavi e tubazioni sia in senso orizzontale che verticale;



Caratteristiche strutturali dell'immobile:

- La portata dei solai dei centri elaborazione dati deve essere compresa tra i 1000 ed i 2500 Kg/mq., a seconda del livello Tier, in seguito descritto, a cui ci si riferisce ;
- le pareti divisorie devono essere possibilmente di buon livello di resistenza passiva e di isolamento termico, in considerazione che il funzionamento h24 impone una particolare attenzione sui consumi energetici;
- l'altezza utile del sito deve essere idonea all'installazione di pavimento sopraelevato di almeno 50 cm. e di tubazioni a soffitto, quindi è da considerare idonea un'altezza utile del locale pari almeno a 3.50/4.00 mt.;
- il sito dovrà essere sufficientemente separato da aree destinate a garage per evitare il rischio di coinvolgimento in caso di incendio, come anche da centrali termiche, archivi cartacei, ecc.



Impianto di alimentazione elettrica:

- Energia elettrica erogata da due linee distinte e separate che si estendano in maniera parallela dalla fonte di erogazione ad ogni singolo apparato utente ;
- Il sito dovrà essere dotato di tecnologie in grado di assicurare la continuità di erogazione anche in caso di black out ;
- La rete di distribuzione interna dovrà essere realizzata con una tipologia che preveda minor numero possibile di componenti preferendo quelle a maggior affidabilità e facilmente manutenzionabili (il livello di affidabilità totale è pari alla affidabilità della componente più debole) ;
- Dovrà essere previsto il monitoraggio da control room di tutte le componenti attive;
- I gruppi elettrogeni dovranno essere in grado di garantire una continuità di funzionamento a tempo illimitato (min 48 ore) con idonei serbatoi di scorta carburante;
- Nella scelta delle componenti privilegiare la qualità ma anche la facilità di manutenzione/reperimento ricambi



Impianto di climatizzazione:

dovrà essere costituito da apparati attivi dimensionati in modo di poter sopperire al guasto di uno o più elementi del sistema stesso, in particolare occorrerà conciliare:

- ✓ le esigenze di rispetto dei parametri di esercizio degli apparati Hardware;
- ✓ le buone prassi di risparmio energetico;
- ✓ il rispetto dei parametri climatici secondo le normative per la salute dei lavoratori;

Prevedere continuità di erogazione elettrica anche per la climatizzazione;

Anche in questo caso privilegiare componenti di qualità ma facilmente manutenzionabili/sostituibili.



Impianti rilevazione e spegnimento incendi:

- Dovranno essere costituiti da un adeguato numero di rilevatori di fumo e da impianti automatici di estinzione compatibili con il funzionamento degli apparati hardware;
- Occorrerà conciliare l'eventuale scarica delle sostanze estinguenti con i tempi di ripristino della vivibilità ambientale per garantire la continuità operativa del sito.



impianti rilevazione allagamenti:

- dovranno essere costituiti da un adeguato numero di rilevatori di allagamento e prevedere eventuali vasche di raccolta con pompe di esaurimento a funzionamento automatico



impianti per il controllo accessi ed antintrusione:

- il controllo accessi dovrà permettere l'ingresso solamente al personale autorizzato e registrarne i tempi di permanenza all'interno del sito;
- il sistema antintrusione dovrà garantire la rilevazione immediata di ogni intrusione con forzature delle difese attive e passive;
- ambedue i sistemi dovranno conciliare le esigenze di registrazione degli eventi con il rispetto della privacy;



L'attuale riferimento più accreditato per la definizione di standard di valutazione dell'affidabilità di infrastrutture IT è l'Uptime Institute di Santa Fe che ha definito uno standard dei livelli prestazionali dei siti che gode del riconoscimento normativo nell'ambito della best practice ANSI/TIA-942/2005-2008-2010-2012 (American National Standard Institute , Telecommunication Industry Association). Quest'ultima **ANSI-TIA 942 – A** descrive e codifica quattro livelli di performance identificati da TIER I a TIER IV in ordine crescente.



Ridondanza secondo la TIA/ANSI 942

Providing secondary components that either become instantly operational or are continuously operational, so that the failure of a primary component will not result in mission failure. There are three level of redundancy:

- **N** where the number of component provided is only the number of component required;
- **N+1** where the number of component provided is one more than the number (N) of component required:
- **2(N+1)** consist of two N+1 systems in parallel. One side can be taken down for maintenance and the other side will be protected from exposure to the risk of downtime by its own redundant module.
- **S** where the systems are two, (N+N) or 2(N+1) and both are at the same time active



N componente attiva

N+1 componente attiva più altra in stand by

S componente attiva in sincrono con altra

Table 1

	Tier I	Tier II	Tier III	Tier IV
Number of delivery paths	1	1	1 Active 1 Passive	2 Active
Redundancy	N	N+1	N+1	S+S or 2(N+1)
Compartmentalization?	No	No	No	Yes
Concurrently maintainable?	No	No	Yes	Yes
Fault tolerant to worst event	No	No	No	Yes

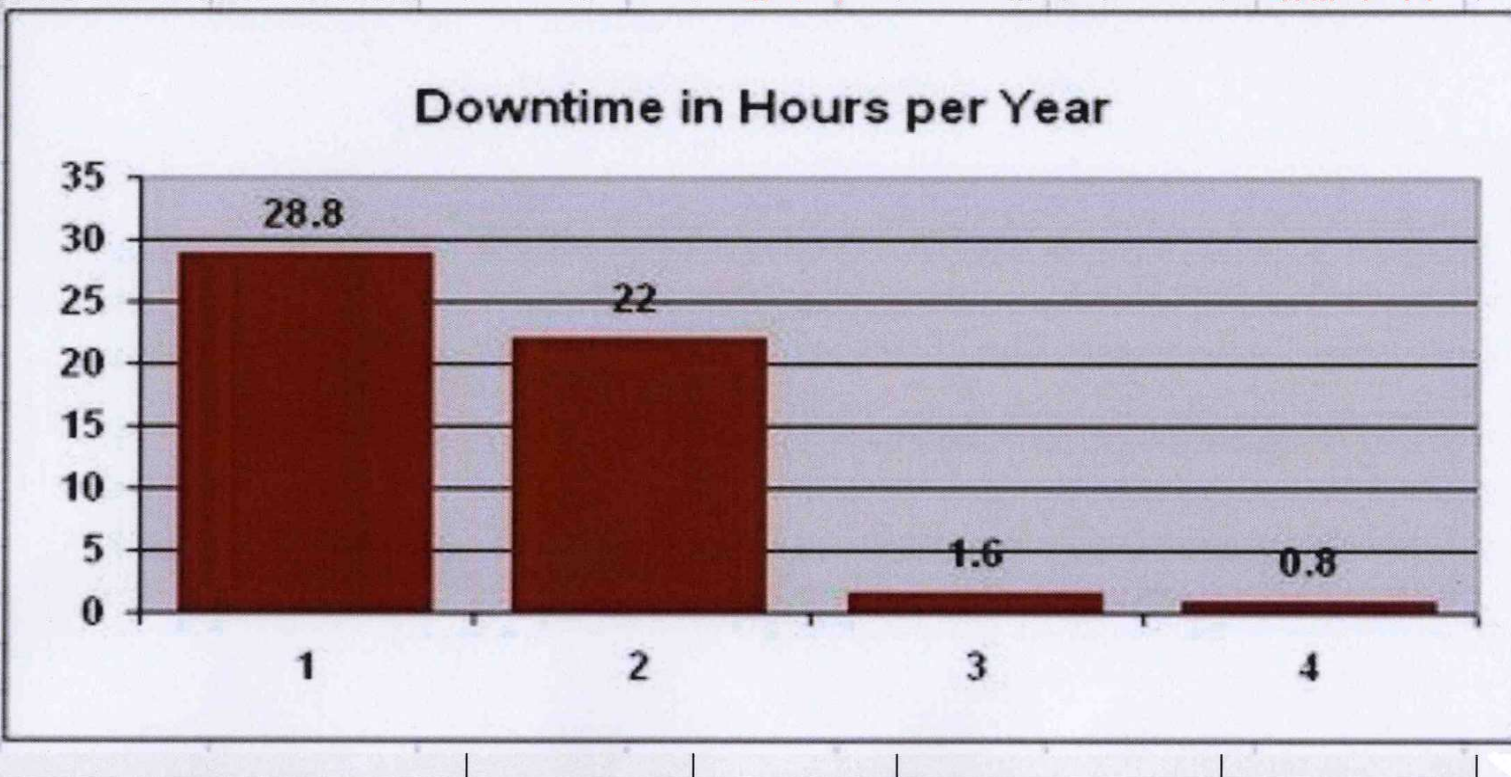


C	Business characteristics	Effect on system design
1	• Typically small businesses • Limited online presence • Low dependence on IT • Perceive downtime as a tolerable Inconvenience	• Numerous single points of failure in all aspects of design • No generator if UPS has 8 minutes of backup time • Generally unable to sustain more than a 10 minute power outage
2	• Some online revenue generation • Multiple servers • Phone system vital to business • Dependent on email • Some tolerance to scheduled downtime	• Some redundancy in power and cooling systems • Generator backup • Able to sustain 24 hour power outage • Minimal thought to site selection • Vapor barrier • Formal data room separate from other areas
3	• World-wide presence • Majority of revenue from online business • VoIP phone system • High dependence on IT • High cost of downtime • Highly recognized brand	• Two utility paths (active and passive) • Redundant power and cooling systems • Redundant service providers • Able to sustain 72-hour power outage • Careful site selection planning • One-hour fire rating • Allows for concurrent maintenance
4	• Multi-million dollar business • Maj. of rev from electronic transactions • Business model entirely dependent on IT	• Two independent utility paths • 2N power and cooling systems • Able to sustain 96 hour power outage



Attribute / Statistic	Tier I	Tier II	Tier III	Tier IV
Power and Cooling Delivery Paths	1 Active	1 Active	1 Active 1 Passive	2 Active
Redundant Components	N	N + 1	N + 1	2N/N + 1

Sup
Floc
Init
Ulti
Rais
Floc
sqft
Utili
Mor
Yea
Con
Ann
to S
Site



Source: The Uptime Institute



Il tempo di vita di un DC è spesso breve rispetto ad altri manufatti quali edifici di civile abitazione, ospedali, opifici, ecc. sia per naturale invecchiamento di apparati in funzione h24/365 sia per mutate esigenze connesse al rinnovo dell'HW che modifica le caratteristiche dei servizi di supporto.

E' bene quindi in fase di analisi preventiva di progetto cercare di definire un margine di crescita compatibile con la realizzazione ma non eccessivo perchè il costo di mantenimento in servizio di un mq. di area Ced è molto elevato.



E' opportuno quindi orientare la progettazione verso una tipologia che privilegi la «Modularità» in un'ottica di «Scalabilità» sia di incremento che in decremento al fine di mantenere - nel limite del possibile - i maggiori livelli di affidabilità e ottimizzazione dei costi/rendimenti .

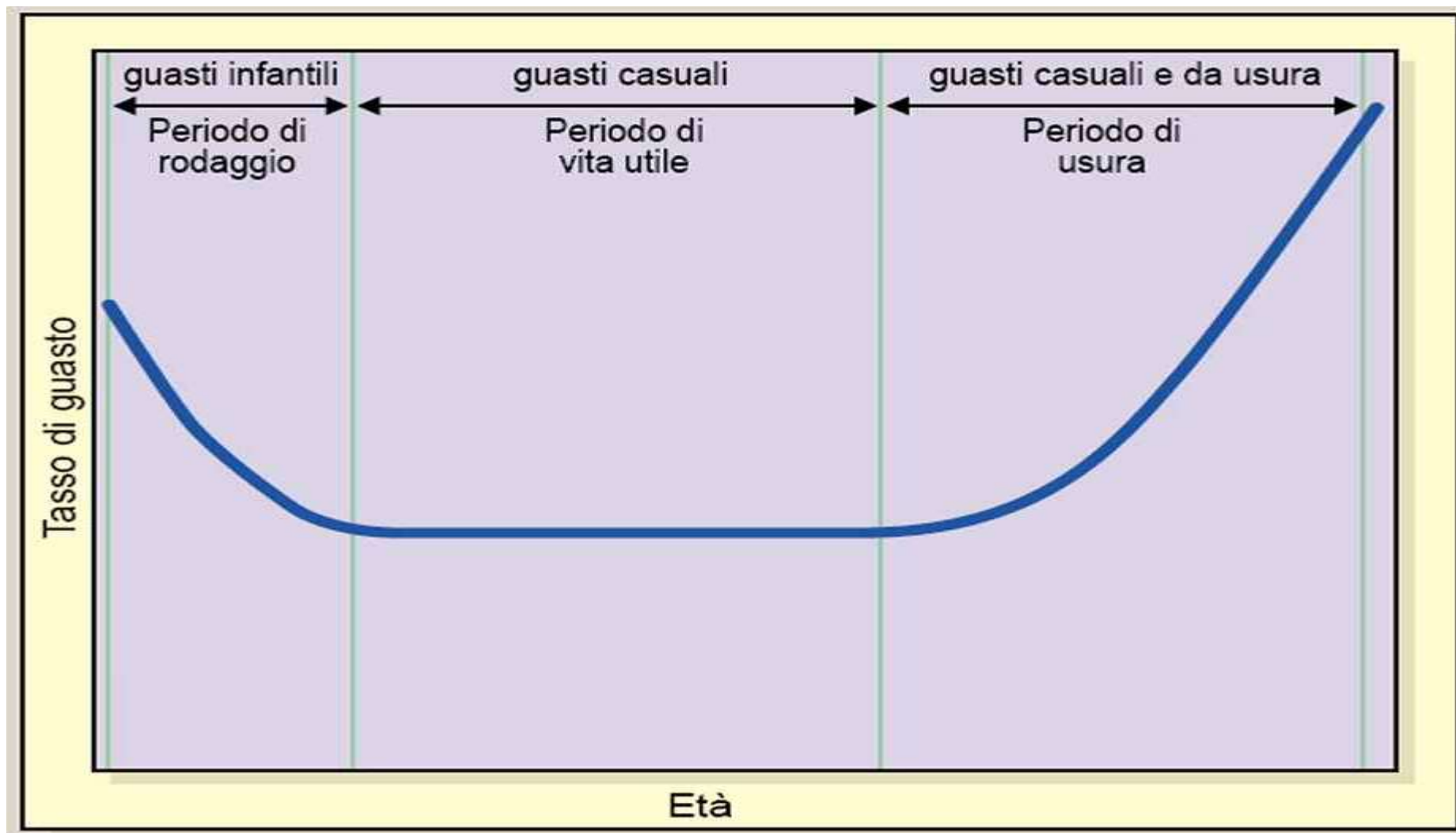


L'infrastruttura di un Data Center è da un lato molto complessa e sofisticata e dall'altro soggetta ad un forte tasso di usura in quanto funzionante h24/365.

Inoltre il necessario livello di sofisticazione richiesto dall'aggiornamento sia del Sw che dell'Hw impone continue valutazioni su interventi di sostituzione componenti attive ed in produzione, non ultimi i cablaggi in relazione alla qualità trasmissiva.

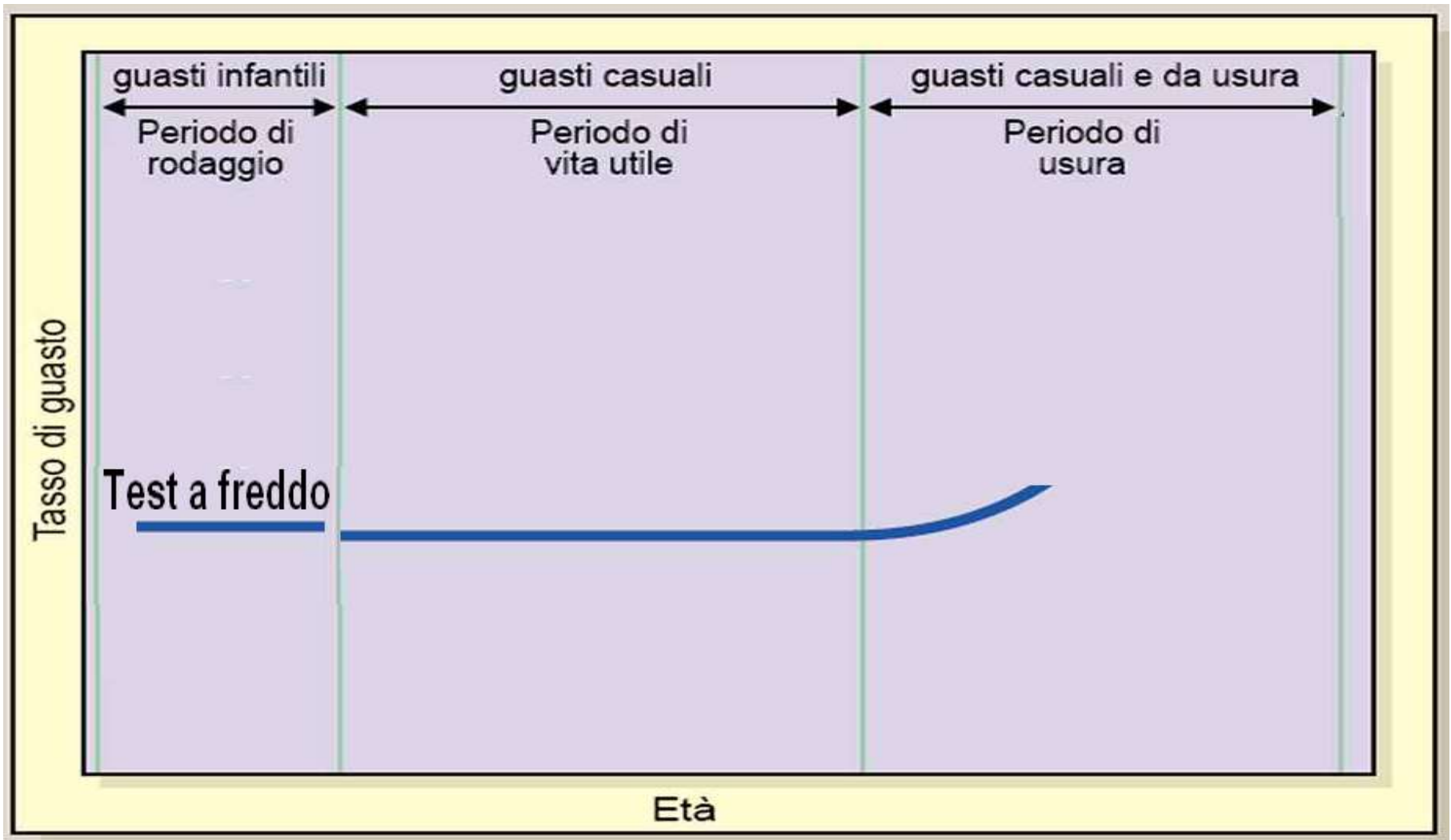


Curva tasso di guasto /tempo di esercizio



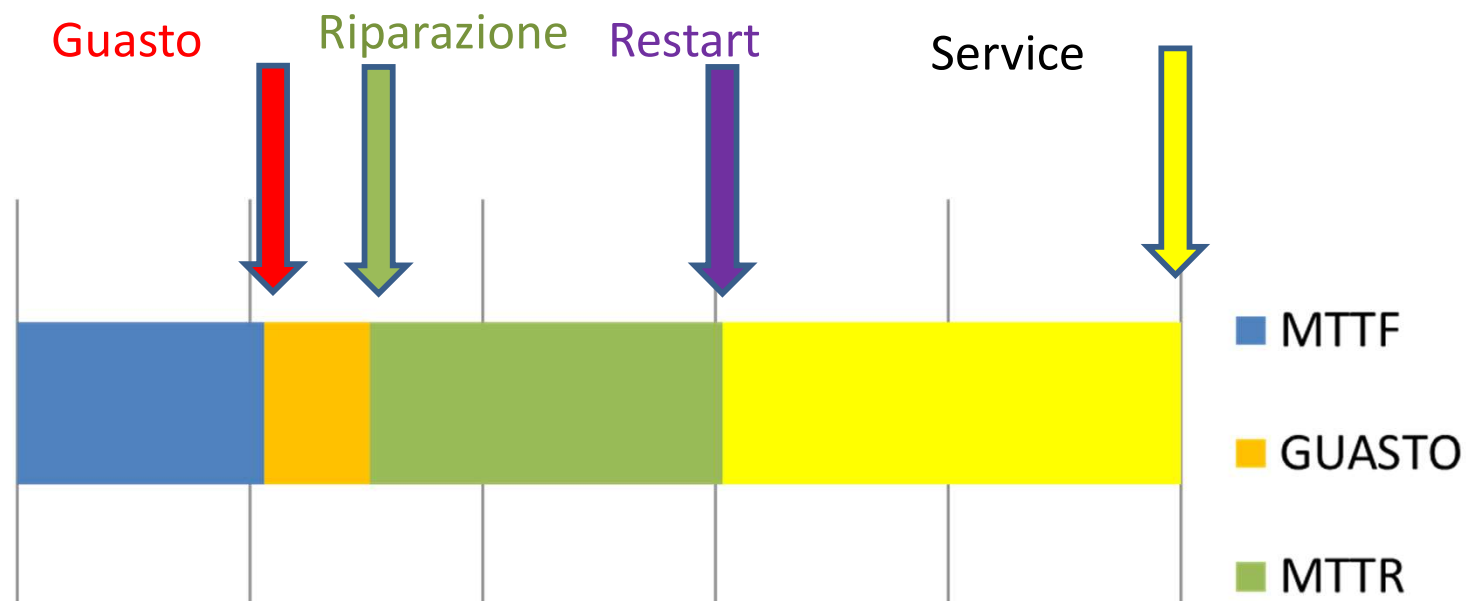


Curva tasso di guasto /tempo di esercizio





Fidatezza CEI CT56



MTTF Mean Time To Failure
MTTR Mean Time To Restore



GRAZIE PER L'ATTENZIONE

Ing. Massimo Marrocco
ingmarroccomassimo@tiscali.it



Relatore

Titolo intervento

Data

pag. 56