Dependable Systems Specification

Processes and techniques for developing a specification for system availability and reliability

Come si misura la reliability

A reliability/availability specification…

affidabilità

disponibilità

- Such as "….should have at least 95% of …"

- **IS IT A FUNCTIONAL OR A NON FUNCTIONAL specificatoin?**

Both Functional and non-functional requirements **are concerned**

- **Non-functional** requirements may be generated to specify the required reliability and availability levels of the system.
- System **functional** requirements may be generated to define error checking and recovery facilities and features that provide protection against system failures.

System reliability specification: three components to consider

- *Hardware reliability*

  cause di malfunzionamento

  - What is the probability of a hardware component failing and how long does it take to repair that component?

- *Software reliability*

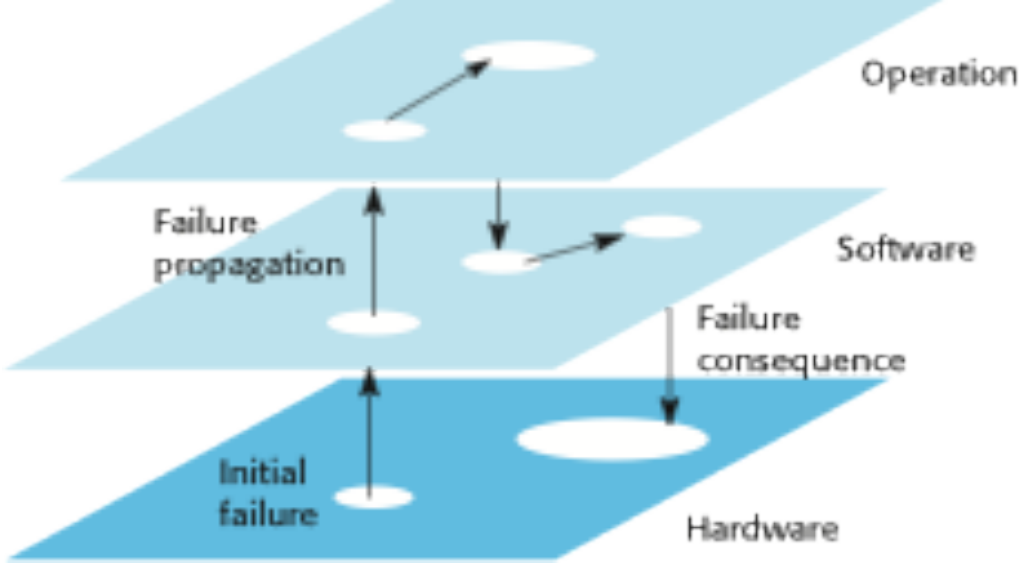
  - How likely is it that a software component will produce an incorrect output. Software failures are different from hardware failures in that software does not wear out. It can continue in operation even after an incorrect result has been produced.

- *Operator reliability*

  - How likely is it that the operator of a system will make an error?

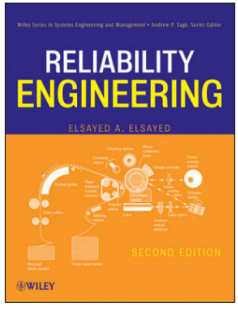
- Failures are not independent and they propagate from one level to another.

Failure propagation



Affidabilità: Hardware vs. Software

- Causa del malfunzionamento
  - Hw: è l'usura, si rompe qc., , la scarsa manutenzione, raramente il progetto
  - Sw: non l'usura, non la manutenzione, ma il progetto (cioè bug nel codice)
- Quando varia l'affidabilità
  - Hw: durante l'uso, a quel punto si ripara/rimpiazza il componente e ritorna a funzionare
  - Sw: durante lo sviluppo, o (meno frequentemente) durante l'uso, quando un fault causa una failure
- Come varia l'affidabilità
  - Hw: in modo più definito e controllabile. La riparazione ripristina la R.
  - Sw: in modo più casuale. La riparazione può migliorare o peggiorare la R.
- La produzione di copie del prodotto
  - Hw: è critica
  - Sw: non è critica
- Guasti nel tempo
  - Hw: permanenti
  - Sw: spesso transitori, variazioni nel tempo (ad es. per interventi di correzione sul codice)
- Obiettivo della 'reliability engineering'
  - Hw: stabilizzare il livello.
  - Sw: far crescere il livello



Non-functional reliability specification

- The required level of system reliability should be expressed **quantitatively**
- Reliability is a dynamic (legata all'esecuzione, il sistema deve esistere ed essere funzionante) system attribute, since reliability specifications related to the source code are meaningless.
  - No more than N faults/1000 lines.
  - This is only useful for a post-delivery process analysis where you are trying to assess how good your development techniques are.
- An appropriate reliability **metric** should be chosen to specify the overall system reliability

Reliability metrics*

metodo di misura su conteggi e tempi

- Reliability metrics are units of measurement of system reliability
- System reliability is measured by counting the number of operational failures and, where appropriate, relating these to the demands made on the system OR the time that the system has been operational
- **Statistical** measurements → A **long-term** measurement programme is required to assess the reliability of critical systems

(*) Metrica = (metodo di) misura quantitativa di una proprietà

Possibili unità di misura di tempo e richieste

- Tempo di calendario
- Tempo cronometrico
- Tempo di esecuzione (CPU)

- Numero di: transazioni, richieste di servizio, failure.

Tipiche misure per valutare l'affidabilità

- Tempo di rilevamento del malfunzionamento (quando s'è verificato)
- Intervallo di tempo fra malfunzionamenti successivi
- No. totale di malfunzionamenti rilevati
- No. di malfunzionamenti rilevati in un intervallo di tempo predefinito
- Tempo di riparazione e di riavvio

Sono tutte variabili **casuali**(*), perchè:

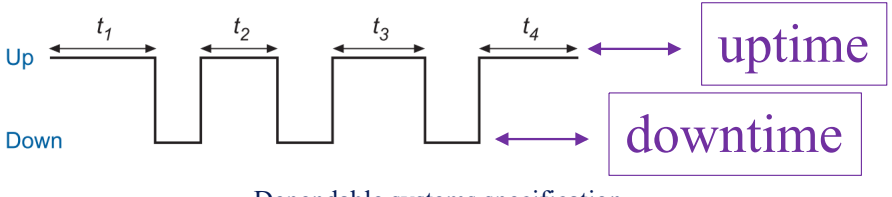
- è impredicibile la **localizzazione** degli errori
- le **condizioni** di esecuzione sono impredicibili/difficilmente controllabili
- è molto complessa la **relazione** tra posizione degli errori nel codice e gli stati nell'esecuzione (cfr slide set n. 10).

(*) Una variabile è casuale (o aleatoria o stocastica) se il suo valore non è predicibile con certezza (in modo deterministico), quali ad es., il lancio di un dado, ma solo attraverso una distribuzione di probabilità. ? approcci statistico/probabilistici

Una variabile casuale può dipendere da altri fattori (o variabili a loro volta casuali)

Reliability and availability **metrics**

Metric	Explanation
POFOD Probability of failure on demand	The likelihood that the system will fail when a service request is made. For example, a POFOD of 0.001 means that 1 out of a thousand service requests may result in failure.
ROCOF Rate of failure occurrence	The frequency of occurrence with which unexpected behaviour is likely to occur. For example, a ROCOF of 2/100 means that 2 failures are likely to occur in each 100 operational time units. This metric is sometimes called the failure intensity.
MTTF Mean time to failure	The average time between observed system failures. For example, an MTTF of 500 means that 1 failure can be expected every 500 time units.
MTTR Mean time to repair	The average time between a system failure and the return of that system to service.
AVAIL Availability	The probability that the system is available for use at a given time. For example, an availability of 0.998 means that in every 1000 time units, the system is likely to be available for 998 of these.



Availability

AVAIL - Availability

- Measure of the **fraction of the time** that the system is available for use
- Takes repair and restart time into account
- Availability of 0.998 means software is available (up) for 998 out of 1000 time units
- Relevant for non-stop, **continuously** running systems
  - telephone switching systems, railway signalling systems, continuous services such as e-mail, …

Availability specification

Availability	Explanation
0.9	The system is available for 90% of the time. This means that, in a 24-hour period (1,440 minutes), the system will be unavailable for 144 minutes.
0.99	In a 24-hour period, the system is unavailable for 14.4 minutes.
0.999	The system is unavailable for 84 seconds in a 24-hour period.
0.9999	The system is unavailable for 8.4 seconds in a 24-hour period. Roughly, one minute per week.

Probability of failure on demand (POFOD)

- This is the probability that the system will fail when a **service request is made**.
- POFOD 0.001 means that 1 out of 1000 service requests may result in failure
- Useful when demands for service are **intermittent** and relatively infrequent
- Appropriate for safety/protection systems where services are demanded occasionally and where there are serious consequence if the service is not delivered: systems designed to be working in background, monitoring a process, but not doing anything until a safety limit is exceeded when they must take some action to keep the process safe. Example
  - Emergency shutdown system in a chemical plant

Reliability

Rate of fault occurrence (ROCOF) (failure intensity – failure rates - cfr slide 15) intensità di fallimento

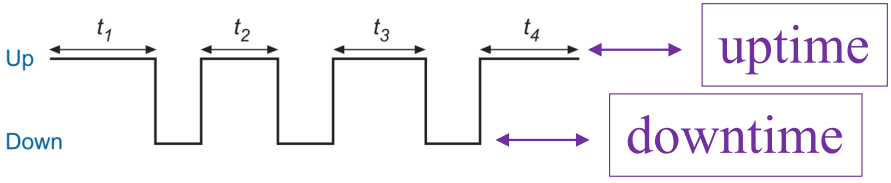
- Reflects the **rate of occurrence of failure over time** in the system
- ROCOF of 0.002 means 2 failures are likely in each 1000 operational **time units** e.g. 2 failures per 1000 hours of operation
- Relevant for operating systems, data processing systems, transaction processing systems where the system has to process a **large** number of similar requests that are **relatively frequent, such as** credit card processing system, airline booking system
- Reciprocal of MTTF

Failure rate, λ

$$= \frac{\text{Number of failures}}{\text{Total operating time}}$$

$$= \frac{k}{T}$$

Mean time to failure (MTTF o MTBF)



- Measure of the mean operating time, i.e.**time between observed failures** of the system. Is the reciprocal of ROCOF for stable systems
- MTTF of 500 means that the mean time between failures is 500 time units
- Relevant for systems with **long transactions** i.e. where system processing takes a long time. MTTF should be longer than transaction length
  - Computer-aided design systems where a designer will work on a design for several hours, word processor systems

$$\text{MTBF} = \frac{1}{\lambda}$$

Failure consequences effetto della failure

- Reliability measurements do NOT take the consequences of failure into account, BUT it is not just the number of system failures that matter but the consequences of these failures
- Transient faults may have no real consequences but other faults may cause data loss or corruption and loss of system service
- Failures that have serious consequences are clearly more damaging than those where repair and recovery is straightforward
- May be necessary to identify **different** **failure classes** and use different specifications and different metrics for each of these. The reliability specification must be structured.

Failure classification

Classificazione in base a:

- come si presenta temporalmente la failure
- come si può ripristinare
- ee sonopresenti danni o meno

Failure class	Description
Transient	Occurs only with certain inputs
Permanent	Occurs with all inputs
Recoverable	System can recover without operator intervention
Unrecoverable	Operator intervention needed to recover from failure
Non-corrupting	Failure does not corrupt system state or data
Corrupting	Failure corrupts system state or data

Failure severity (U.S: Military Standard MIL-STD-1629A)

Anche l'entità del danno (severity) può essere classificata in diverse livelli:

- **Catastrophic** – morte o perdita sistema
- **Critical** – gravi danni a cose e persone, non si raggiunge l'obiettivo
- **Marginal** – danni minori, che causano ritardi, minor disponibilità, raggiungimento parziale degli obiettivi
- **Minor** – conseguenze non gravi e non tali da causare danni, ma che richiedono interventi di manutenzione o riparazioni non previsti

Procedura di Misura

- Si tratta di un procedimento **statistico**, perciò si **ripetono le misure più volte**, nelle condizioni e con lo scopo definito. (vedi concetto di profilo operativo nelle slide successive).
- Durante il procedimento si effetuano le misure di tempo e di eventi (failure) previsti dalla METRICA individuata.
- Si mediano i risultati
- Ed eventualmente vi si applicano vari test statistici

Statistical testing (o Reliability testing)

- Testing software for reliability rather than fault detection
- An acceptable level of reliability should be specified and the software tested and amended until that level of reliability is reached
- **NB.** Il **defect testing** (trattato nella parte di corso su V&V) ha l'obiettivo di indivuduare failure per poi, mediante debugging, rimuovere difetti/bug, mentre **lo statistical testing** intende solo misurare l'affidabilità.

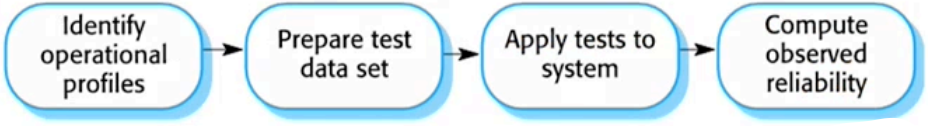
→ uso dati del passato per prevedere il futuro

- Measuring the number of errors/failures/etc. allows the reliability of the software to be predicted (attualmente anche con tecniche di Machine Learning)

↳ io misuro l'affidabilità del sw

Steps of statistical testing

1. Establish the operational profile for the system
2. Construct test data reflecting the operational profile
3. Define environment & Install the system in an environment corresponding to the final one
4. Test the system and observe the number of failures and the times of these failures
5. Compute the reliability after a statistically significant number of failures have been observed

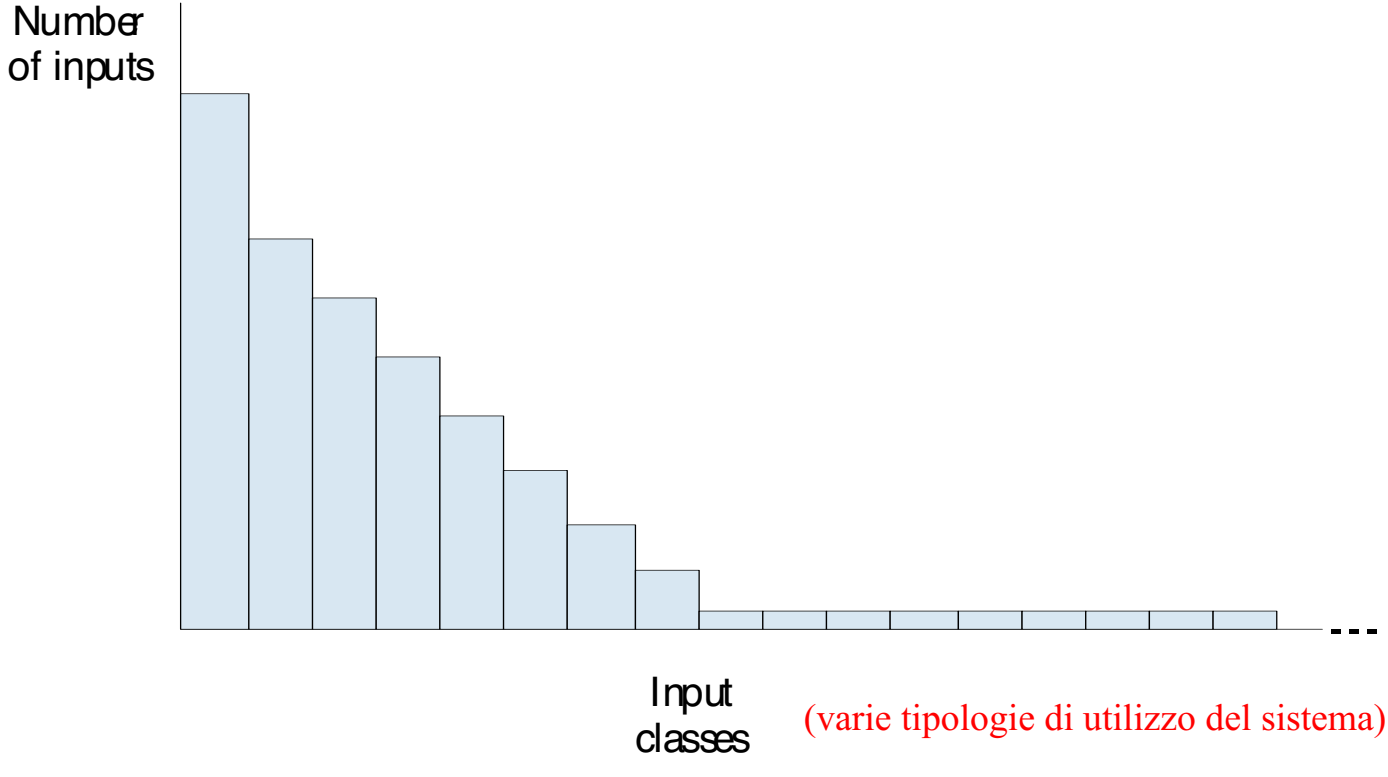


Operational profiles

PROFILO OPERATIVO

- An operational profile is a set of test data whose frequency matches the actual frequency of these inputs from 'normal' usage of the system. A close match with actual usage is necessary otherwise the measured reliability will not be reflected in the actual usage of the system
- Can be generated from real data collected from an existing system or (more often) depends on assumptions made about the pattern of usage of a system

An operational profile



(varie tipologie di utilizzo del sistema)

Operational profile generation

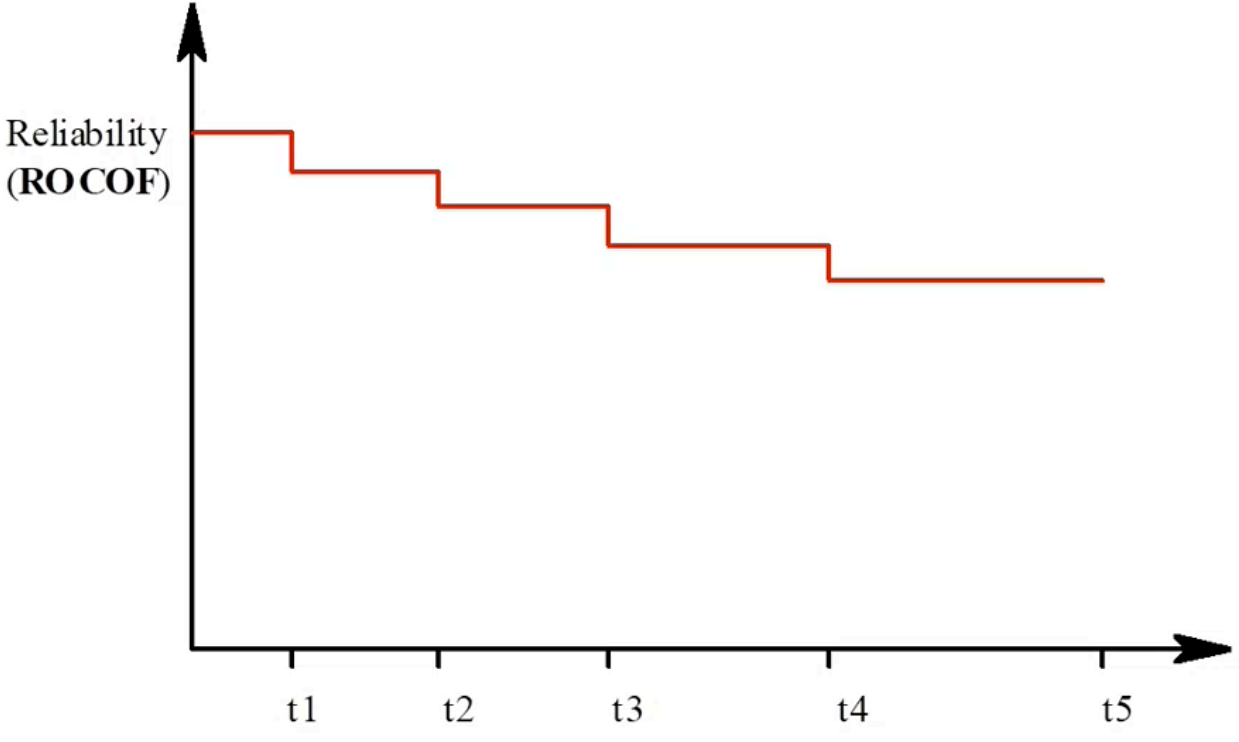
- Should be generated automatically whenever possible (osservando le modalità di utilizzo di sistemi simili)
- Automatic profile generation is difficult for interactive systems
- May be straightforward for ‘normal’ inputs but it is difficult to predict ‘unlikely’ inputs and to create test data for them

Reliability modelling

che andamento dovrebbe avere la reliability

- A **reliability growth model** is a mathematical model of the system reliability change as it is tested and faults are removed
- Used as a means of **reliability prediction** by extrapolating from current and historic data
- Simplifies test planning and customer negotiations
- Registrando durante ogni progetto come varia l'affidabilità in fase di testing, quante failure vengono rilevate e quando, quanti fault vengono rimossi e quando, si costruisce una base storica che permette di sviluppare (ad esempio con tecniche Statistiche e/o di Machine Learning) dei **modelli predittivi** che permettono di prevedere l'andamento e la durata della fase di testing, da cui possiamo stabilire quanto continuare col testing, quando fermarsi ecc.

1 .Equal-step reliability growth

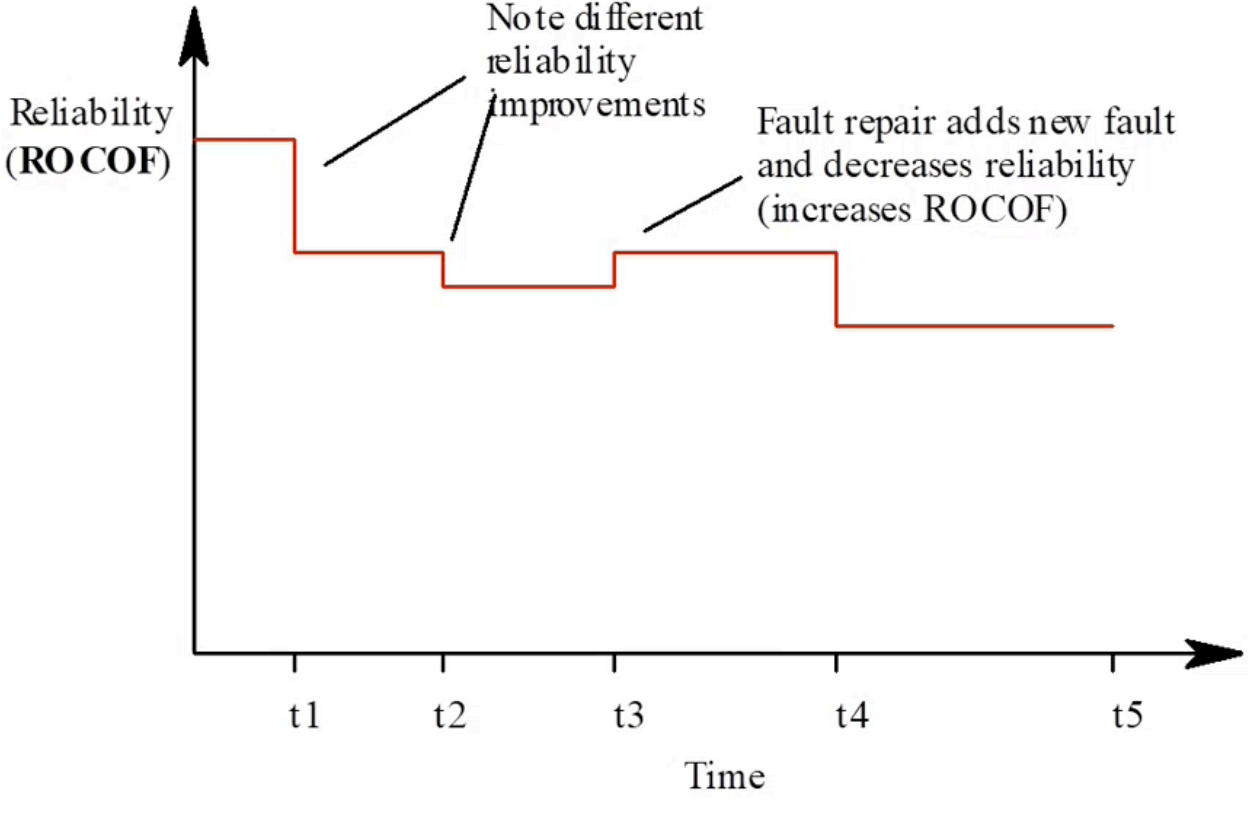


ROCOF = Failure intensity

Observed reliability growth

- Simple equal-step model but does not reflect reality
- Reliability does not necessarily increase with change as the change can introduce new faults
- The rate of reliability growth tends to slow down with time as frequently occurring faults are discovered and removed from the software
- A random-growth model may be more accurate!
- "Software Reliability is dynamic and stochastic in nature so we may say that reliability is a probabilistic measure that assumes that the occurrence of failure of software is a random phenomenon" [Quyoum et al. 2010]

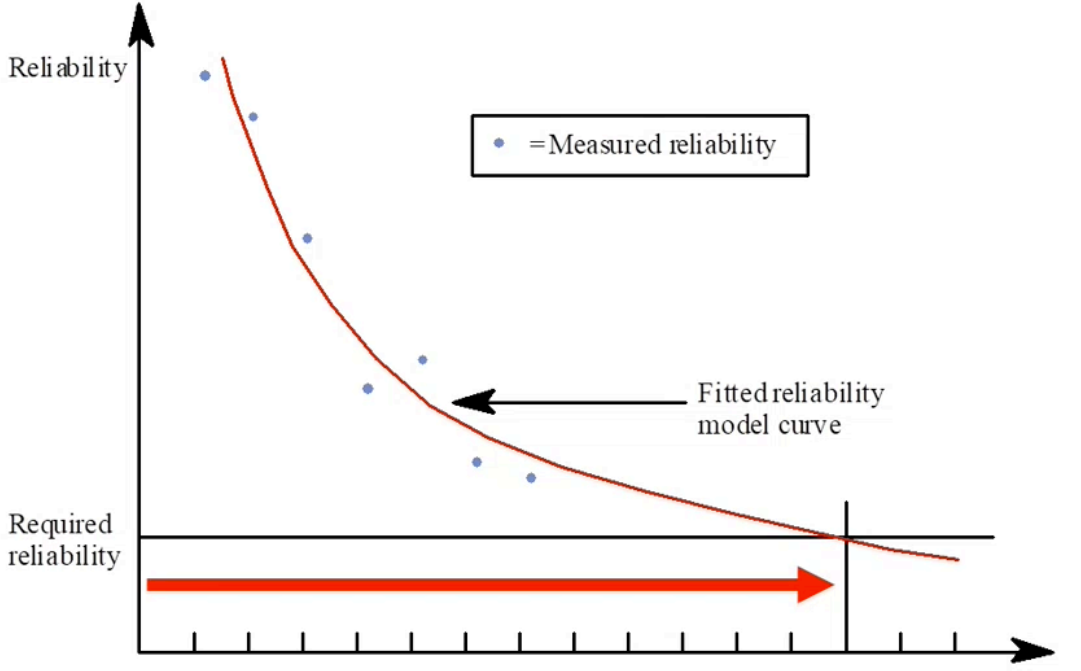
2. Random-step reliability growth



Growth model selection

- Many different reliability growth models have been proposed
- No universally applicable growth model
- **AD-HOC, specific model**: Reliability should be measured and observed data should be fitted to several models
- Best-fit model should be used for reliability prediction

Reliability prediction



How much time for testing and debugging in order to achieve the required reliability level

Reliability prediction & ML

Machine learning techniques for predicting software reliability based on past failures of software products

The primary goal of software reliability modeling is to find out the probability of a system failing in a given time interval or the expected time span between successive failures

Set 14 - Cosa ricordare: concetti, motivazioni, conseguenze, relazioni fra concetti, ecc.

- Specificazione Affidabilità (A)/Disponibilità (D): aspetti funzionali o non funzionali.
- Cause delle failure: hw, sw, operatore. Differenze failure hw e sw.
- Approccio alla specificazione di A e D: non statico, ma dinamico, metriche, loro natura, approccio statistico. Unità di misura di tempo e di richieste, varie tipologie di misura, causalità delle misure. Metriche: AVAIL, POFOD, ROCOF, MTBF.
- Conseguenze dei malfunzionamenti, tipologie di failure e tipologie di conseguenza (severità).
- Misura di A e di D. Statistical Testing: procedura, profilo operativo.
- Modellizzazione e predizione dell'andamento della reliability.