Dependability (fidatezza)

↳ posso fidarmi del mio SW?

The extent to which a critical system is trusted by its users

depend 2013

2019.dsn.org

Più visitati · Come iniziare · Ticketlandia · Didamatica 2016 List ... · Add to Delicious · Nuova scheda · Come iniziare · Diretta news video in l...

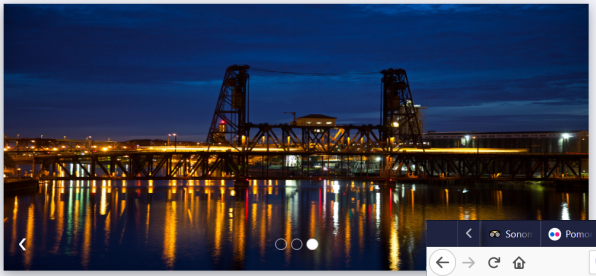
DSN 2019

The 49th IEEE/IFIP International Conference on Dependable Systems and Networks

Portland, Oregon, USA

June 24 – 27, 2019

- DSN 2019 Survey
- Student Travel Grant Survey
- Welcome
- Call for Contributions
- Committees
- Awards
- Registration
- Conference Venue
- Student Plaza
- Conference Program



Welcome

It is my pleasure to invite you to the 49th edition of the Annu

https://dsn2020.webs.upv.es

Più visitati · Come iniziare · Ticketlandia · Didamatica 2016 List ... · Add to Delicious · Nuova scheda · Come iniziare · Diretta news video in l...

Universitat Politècnica de València, València (Spain): 29th June - 2nd July, 2020.

Building 8B, Universitat Politècnica de València (UPV), Camino de Vera s/n, 46022 - València (Spain) (+34)963877007, ext:15752

DSN 2020

UPV – VALÈNCIA (SPAIN)

HOME · COMMITTEES · TRACKS · AWARDS · PROGRAM · VENUE · PREV. EDITIONS · SPONSORS

https://dsn2020.webs.upv.es/#

nternational Conference on Dependability

DEPEND 2012

ugust 19 - 24, 2012 - Rome, Italy

The Sixth I

Augu

and Logi

nal Conference on Dependability

EPEND 2016

8, 2016 - Nice, France

pporters

DEPEND 2015

ust 23 - 28, 2015 - Ve

cs Supporters

ublished by IARIA XPS

DSN 2021

The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks

Taipei, Taiwan, June 21-24, 2021

MAIN MENU
Home
Calls for Contribution ▼
Main Track
Submission
Industrial Track
Workshops
Fast Abstracts
Doctoral Forum
Final Program ▾
Keynotes
Awards ▾
Virtual Conference Platform
Video and Slides Collection
General Instructions for Zoom Sessions
Track-specific Instructions for Zoom Sessions

Welcome to the VIRTUAL 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN) - Due to the COVID-19 pandemic, the DSN-2021 will be held virtually.

It is our pleasure to invite you to the 51st edition of the Annual IEEE/IFIP

Organized by:

國立臺灣大學 National Taiwan University

Sponsored by:

IEEE COMPUTER SOCIETY

ifip

With generous support from:

MOST 科技部 Ministry of Science and Technology

中央研究院 ACADEMIA SINICA

Why dependability?

1. The enormous growth of sw applications has caused more and more a shift from technical software systems to **sociotechnical sw systems** .
2. This means that sw applications are not any more devoted only to a specific technical task in a way which is separated from a surrounding context, but, on the other hand, are part of social or organizationl processes, where the sw system plays an important role, possibly by substituting a human operator with specific **responsabilities**, or by executing a **critical** (sub)process, with critical/demanding requirements in terms of response time, precision, value of the managed data, potential negative impacts of faulty operations, and so on.
3. Moreover, more and more our society **delegates** to software systems relevant and critical task, whose correct and successful execution is absolutely necessary.

The concept of dependability

- For critical systems (safety, mission, business), it is usually the case that **the most important system property** is the dependability of the system
- The dependability of a system reflects the user's degree of trust in that system. It reflects the extent of the user's confidence that it will operate as users expect and that it will not 'fail' in normal use
- **Attenzione: Usefulness** and **trustworthiness** are not the same thing. A system does not have to be trusted to be useful.

↳ può svolgere una funzione ma magari non è sicuro.
Invece io posso svolgere (con il sw) una funzione, magari non in maniera efficiente, ma almeno sono sicuro che vada

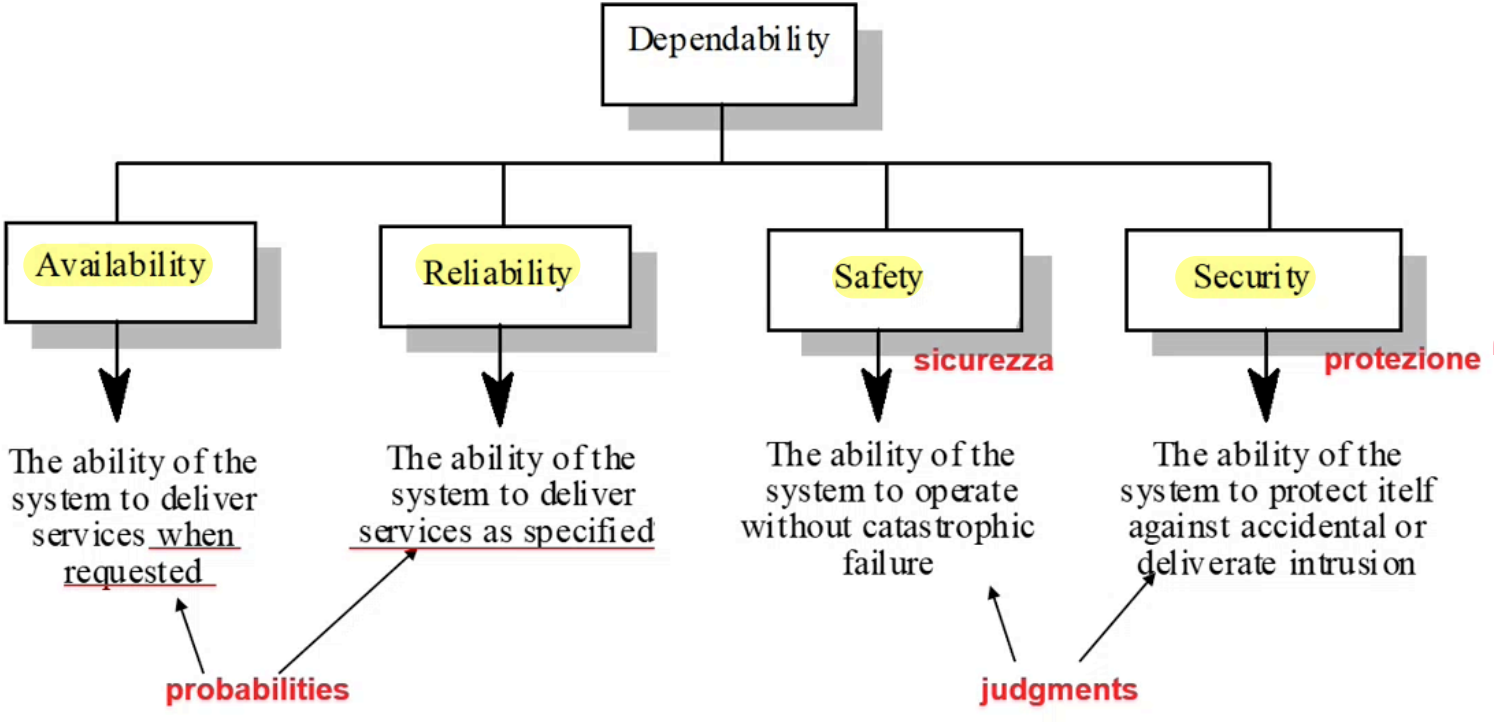
FIDATEZZA

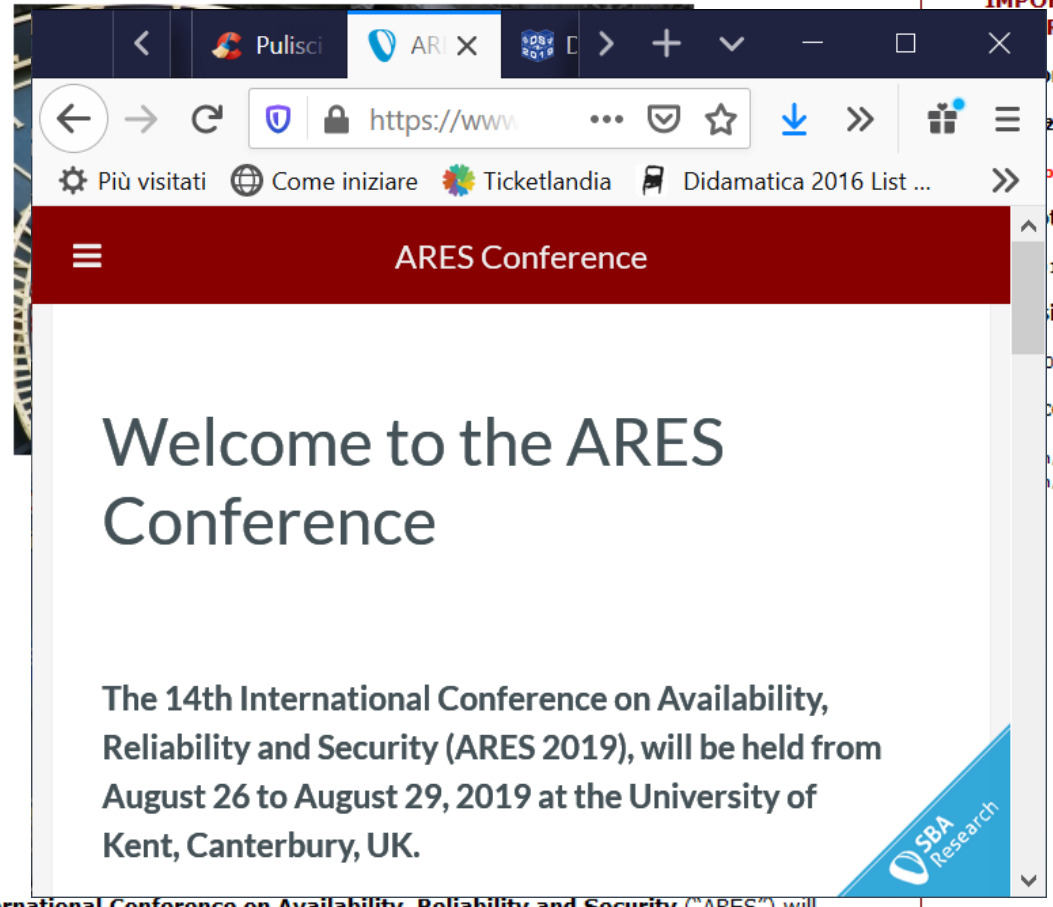
- Quanto mi posso fidare di un sistema?
- Più in dettaglio, quanto posso dipendere da un sistema, in quanto è:

1. in grado di fare ciò che mi aspetto,
2. di essere disponibile quando mi serve,
3. di svolgere il suo compito senza provocare danni e
4. proteggendo adeguatamente i suoi dati.

- Se un sistema ha queste caratteristiche, posso dipendere da esso, posso fidarmi.

4 Dimensions of dependability





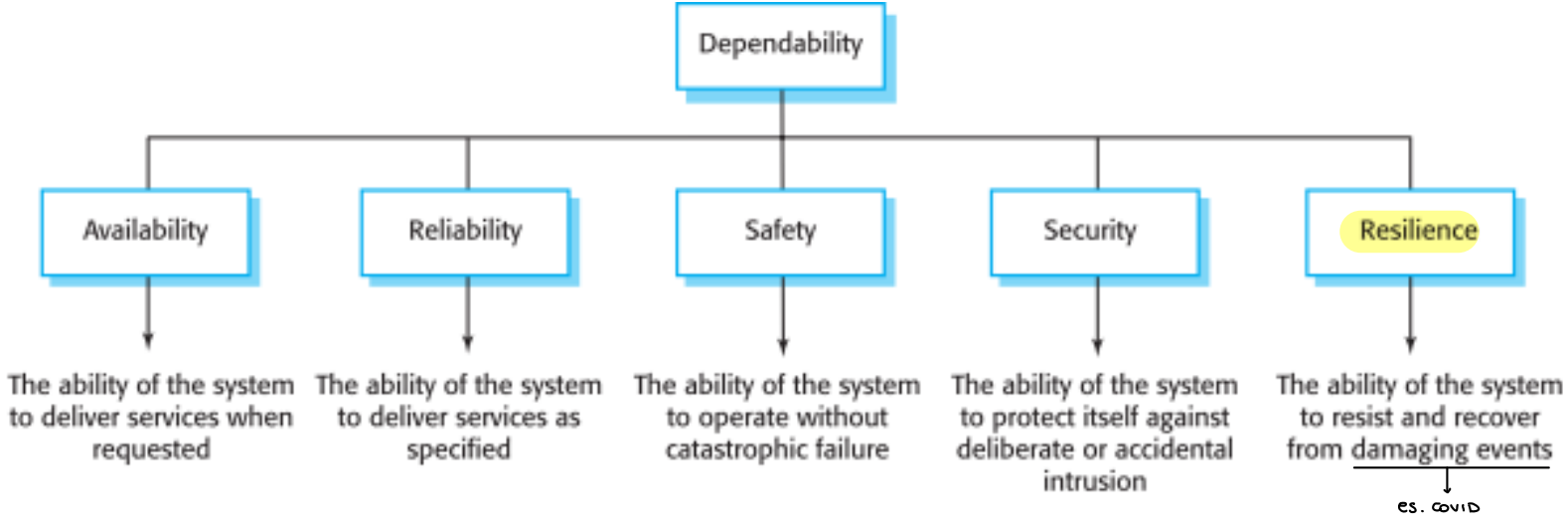
The **7th International Conference on Availability, Reliability and Security** ("ARES") will bring together researchers and practitioners in the area of dependability. ARES will

Interpretazioni intuitive per le dimensioni della 'fidatezza'

1. Affidabilità: il sw funziona bene o male, fa o non fa quello che dovrebbe fare
2. Disponibilità: il sw funziona o non funziona quando serve
3. Sicurezza (safety): il sw funziona senza causare danni a cose o persone
4. Protezione (security): il sw funziona protetto, evitando danni a sè stesso (dati)

Other possible dimensions

The principal dependability properties



Maintainability: facilità della riparazine/modifica

- A system attribute which is concerned with the **ease of repairing** the system after a failure has been discovered or changing the system to include new features
- Very important for critical systems as faults are often introduced into a system because of maintenance problems
- Maintainability is distinct from other dimensions of dependability because it is a **static** and not a dynamic system attribute. Not covered in this chapter.

Potremmo dire

- Includendo anche la maintainability, ciò che desideriamo è quindi un **sistema che funzioni nel modo che ci attendiamo (correttamente e consistentemente), senza creare danni all'esterno o a se stesso , per lunghi periodi tra una manutenzione e l'altra. In più è importante che sia operativo e funzionante nel momento in cui ci serve e che sia riparabile velocemente e facilmente quando evidenzia dei malfunzionamenti.**

[**reliability**, **availability**, **security**, **safety**, **maintainability**]

facilità di riparazione e modifica

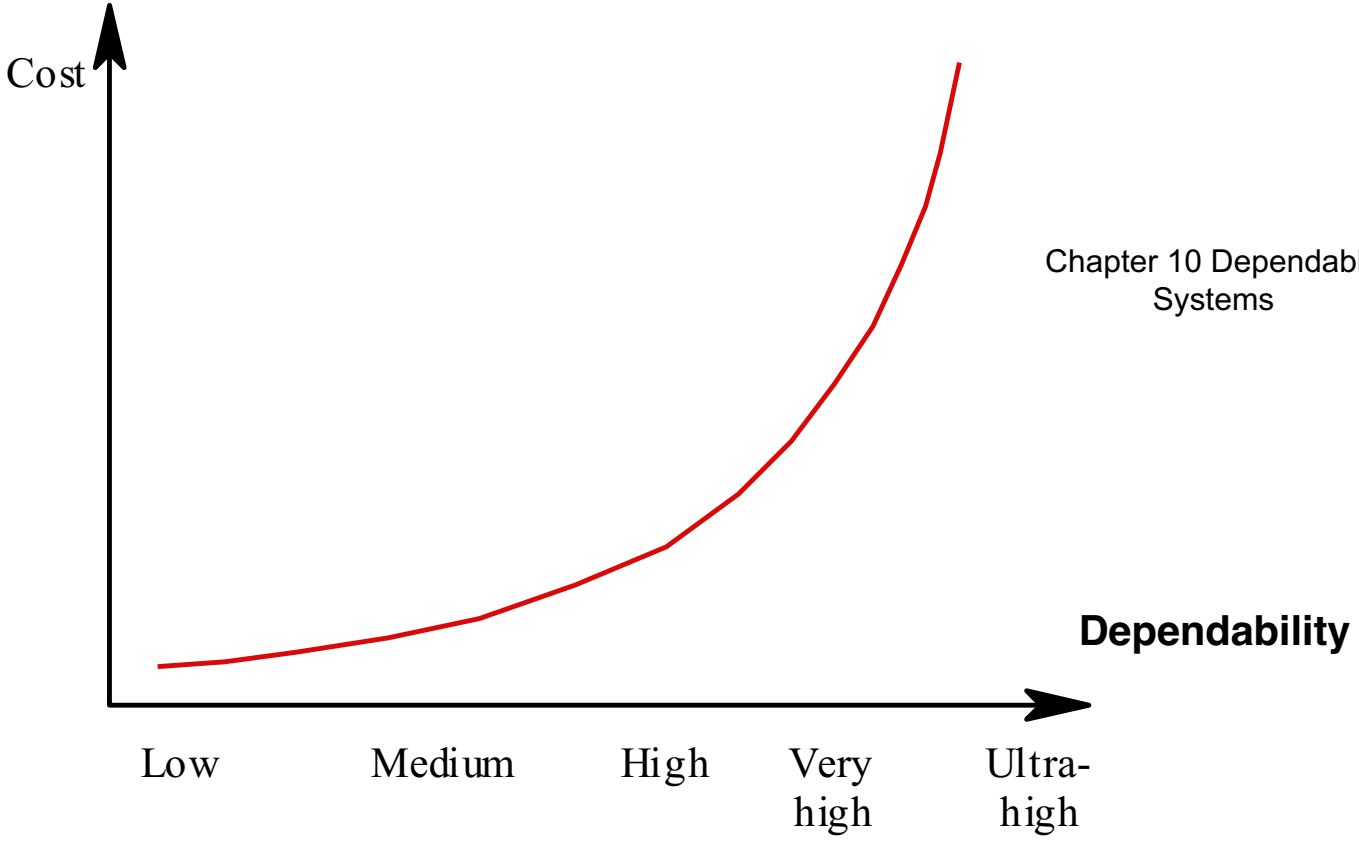
Survivability

- The ability of a system to continue to deliver its services to users in the face of deliberate or accidental attack
- This is an increasingly important attribute for distributed systems (Web) whose security can be compromised

… and others…

- More general than survivability, **Resilience**,
  - the **ability of a system to maintain the continuity of its critical services** in the presence of disruptive events such as equipment failure and cyberattacks.
- **Repairability**
  - Reflects the extent to which the system can be repaired in the event of a failure
- **Error tolerance**
  - Reflects the extent to which user input errors can be avoided and tolerated.

Costs of increasing dependability



Chapter 10 Dependable Systems

Dependability costs

- Dependability costs tend to increase exponentially as increasing levels of dependability are required
- There are two reasons for this
  1. The use of more expensive development techniques and hardware that are required to achieve the higher levels of dependability
  2. The increased testing and system validation that is required to convince the system client that the required levels of dependability have been achieved (V&V > 50%)

Dependability(↑) vs performance(↓)

Dependability is often more important than performance :

- Untrustworthy systems may be rejected by their users
- System failure costs may be very high
- Untrustworthy systems may cause loss of valuable information

- On the other hand, it may be possible to compensate for poor performance

Dependability economics & trade off

- In certe circostanze si può accettare un livello inferiore di Fidatezza! **Dipende da ciò che fa il sistema** : se va male ma si riesce ad ottenere ciò che serve, ci si accontenta….
- Because of very high costs of dependability achievement, it may be more cost effective to accept untrustworthy systems and pay for failure costs
- However, this depends on social and political factors. A reputation for products that can't be trusted may lose future business
- Depends on system type: for ex., for business systems in particular, modest levels of dependability may be adequate

Definizioni : Availability and reliability

Si misurano con delle PROBABILITÀ, fanno entrambe parte della DEPENDABILITY

- Reliability → AFFIDABILITÀ
  - The **probability** of **failure-free** system operation **1. over a specified interval of time** **2. in a given environment** **3. for a given purpose**

esente da malfunzionamenti

- Availability → DISPONIBILITÀ
  - The **probability** that a system, **1. at a point in time**, will be operational and able to **2. deliver the requested services**

in un certo momento

- Both of these attributes can be expressed quantitatively e.g. availability of 0.999 means that the system is up and running for 99.9% of the time.

Anche la maintainability ha una def. basata sulla probabilità

- Maintainability: → MANUTENIBILITÀ
  - **The probability that, for a given condition of use, a maintenance activity can be carried out within stated time interval and using stated procedures and resources**
- La manutenzione può anche essere svolta mentre il sistema è attivo.

Reliability terminology

↓ tradotti alla slide successiva

Term	Description
System failure	An event that occurs at some point in time when the system does not deliver a service as expected by its users
System error	Erroneous system behaviour where the behaviour of the system does not conform to its specification.
System fault	An incorrect system state i.e. a system state that is unexpected by the designers of the system.
Human error or mistake	Human behaviour that results in the introduction of faults into a system.

1

2

3

DIFETTO - GUASTO

4

Malfunzionamenti, difetti, errori

1

- **Malfunzionamento** del sistema (**system failure**) - visione esterna
  - Evento inatteso, servizio non conforme a ciò che l'utente si aspetta (cioè diverso dalle specifiche funzionali, prestazioni, ...)
  - il **testing** serve ad identificare i malfunzionamenti

2

- **Errore del sistema** (**system error**) - visione interna
  - Comportamento/stato interno del sistema non previsto, ossia diverso dall'atteso
  - **errore di sistema ?→(provoca) malfunzionamento**

dinamico

3

- **Difetto - guasto** (**system fault - bug**)
  - Anomalia del codice (bug), difetto (codice anomalo)

    bug ? → errore sistema ?→malfunzionamento
  - Il **debugging** serve ad identificare le anomalie del codice

4

- **Errore umano**
  - causa dell'anomalia: **errore umano ? → bug**
  - (banale distrazione, ..., errore concettuale, di progetto)

..... statico

Components/causes of Failure

- Hardware
- Software
- Operators

Relazioni tra Faults e failures

- Failures are a **usually** a result of system errors that are derived from faults in the system:
  - **Human error → Fault → System error → Failure**
- **However**, faults do not necessarily result in system errors
  - The faulty system state may be transient and 'corrected' before an fault arises
  - Effects of multiple faults may in some cases 'compensate each other'
- System errors do not necessarily lead to system failures
  - The error can be corrected by built-in error detection and recovery
  - The failure can be protected against by built-in protection facilities. These may, for example, protect system resources from system errors

Un piccolo esempio

```
1  program raddoppia (I,O);
2  var x,y: integer;
3  begin
4        read(x);
5        y:=x*x;
6        write(y)
7  end.
```

- *esecuzione con input=2, 3 ==> ….*

Oppure:

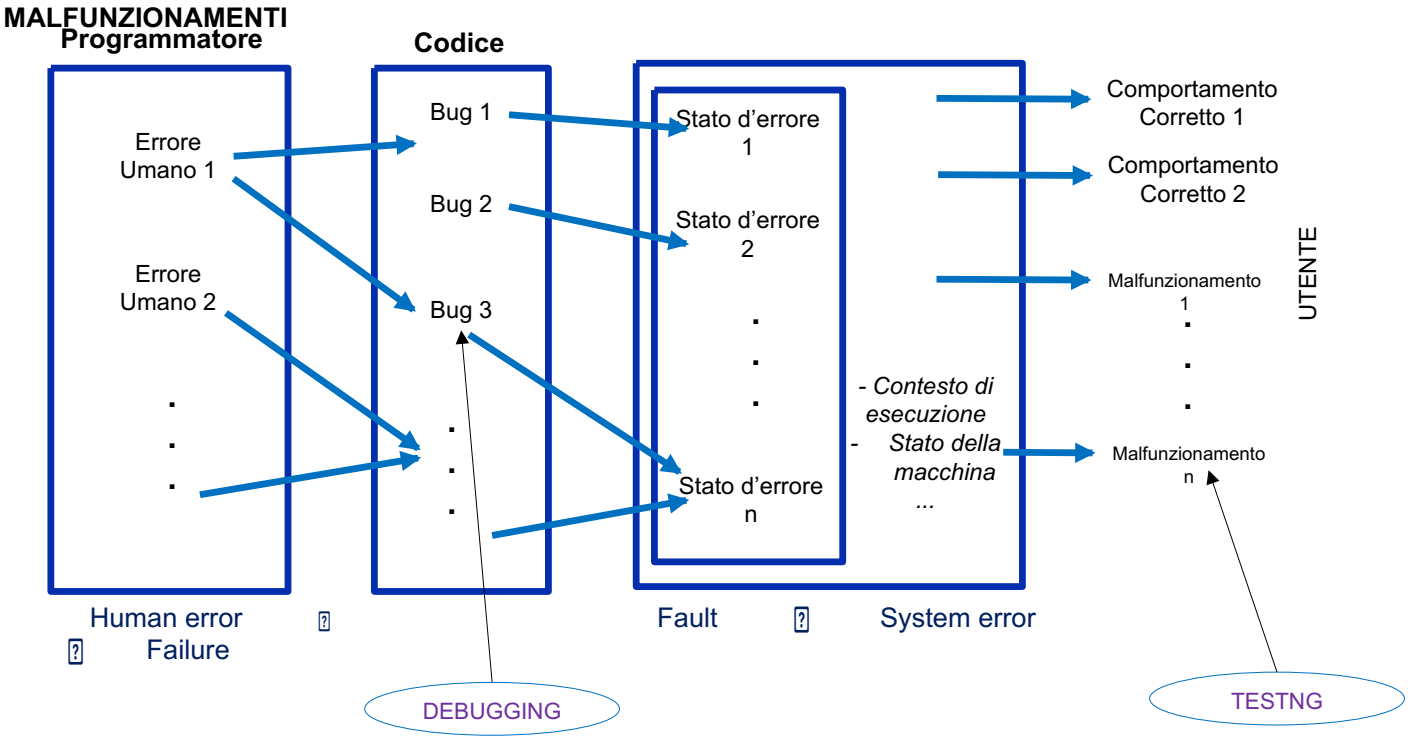
- *..cammino non percorso ==> non è rilevato alcun malf.to*
- ***DISEGNO - relazioni complesse tra errori umani, anomalie (fault) nel codice, errori del sistema e malfunzionamenti***

Le complesse relazioni fra

ERRORI UMANI

BUG nel codice

STATI d'ERRORE
del sistema in esecuzione



Testing, V&V e individuazione dei malfunzioamenti

- Il comportamento dei malf.ti (MALFUNZIONAMENTI) **dipende da** bug presenti nel codice, dall'ambiente esecutivo e dal profilo operativo dell'esecuzione (quali sono i diversi processi in esecuzione)
- L'eliminazione dei malf.ti non può avvenire se non si riesce ad evidenziarli, sollecitando il programma con opportuni input ? criticità del processo di V&V
- La completa o incompleta eliminazione dipende dall'efficienza con cui gli errori vengono trovati e rimossi (? testing e processo di V&V): se è inefficiente, comunque ad un certo momento mi fermerò, se non altro per motivi 'pratici'/'commerciali' / 'organizzativi' / 'economici' /'scadenze' / 'impegni contrattuali'

Reliability and specifications

- Reliability can only be defined formally with respect to a system specification i.e. a failure is a deviation from a specification.
- However, the specifications derived from requirements CAN BE incomplete or incorrect – hence, a sw system that conforms to its specification may work fine but the system 'fails'
- Furthermore, users don't read/know specifications so don't know how the system is supposed to behave.
- Therefore in practice what is important is the **perceived** reliability.

Perceptions of reliability

- The formal definition of reliability does not always reflect the user's perception of a system's reliability
  - The assumptions that are made about the environment where a system will be used may be incorrect (…context/goal)
    - Usage of a system in an office environment is likely to be quite different from usage of the same system in a university environment
    - Oppure stiamo usando il sistema in un 'modo sbagliato'
  - The **consequences** of system failures affects the perception of reliability
    - Unreliable windscreen wipers in a car may be irrelevant in a dry climate
    - Failures that have serious consequences (such as an engine breakdown in a car) are given greater weight by users than failures that are inconvenient

Reliability achievement

- Fault **avoidance:** **si cerca di evitare con accorgimenti durante il processo di sviluppo (più metodo, più formale, più controlli, ecc.)**
  - **Development** techniques are used that either minimise the possibility of mistakes or trap mistakes before they result in the introduction of system faults
- Fault **detection and removal:** **si cerca e si rimuove prima di mettere in produzione**
  - **Verification and validation** techniques that increase the probability of detecting and correcting errors before the system goes into service are used
- Fault **tolerance:** **si cerca di evitare con codice ad hoc nel sistema sviluppato**
  - **Run-time** techniques are used to ensure that system faults do not result in system errors and/or that system errors do not lead to system failures

Sviluppo codice

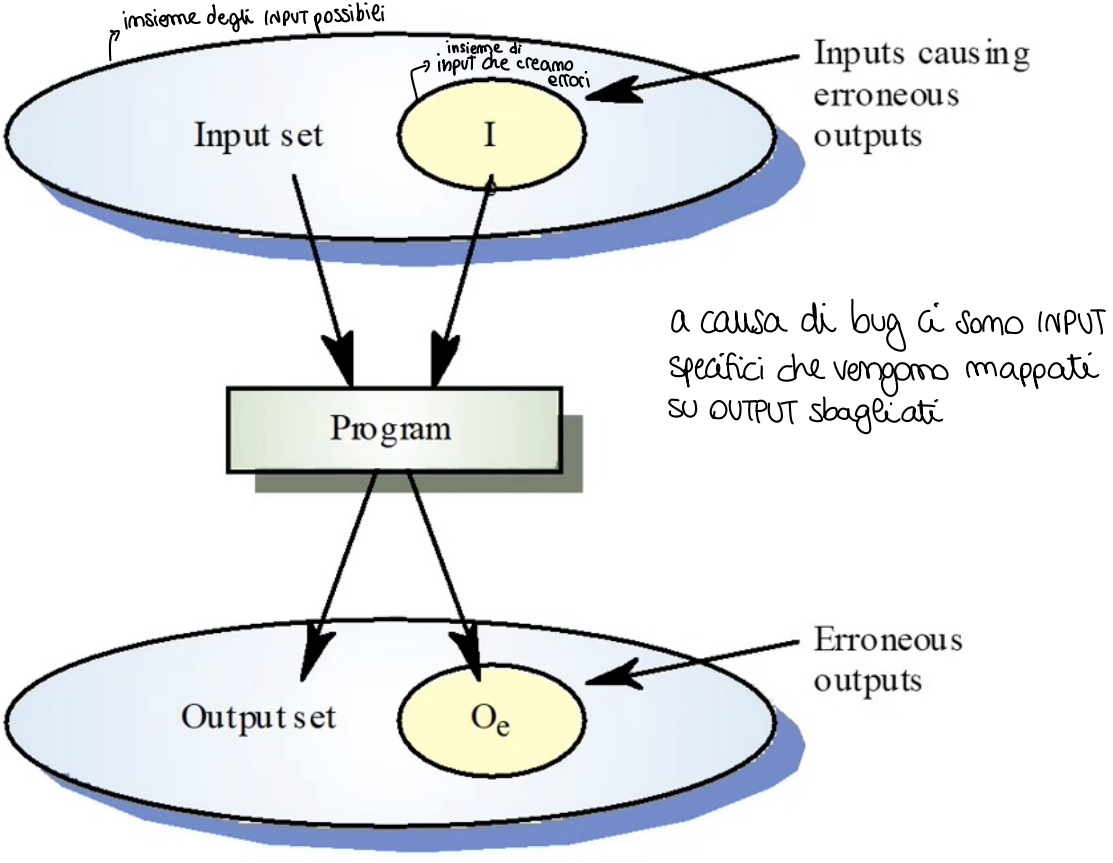
V & V

Run Time

Reliability modelling

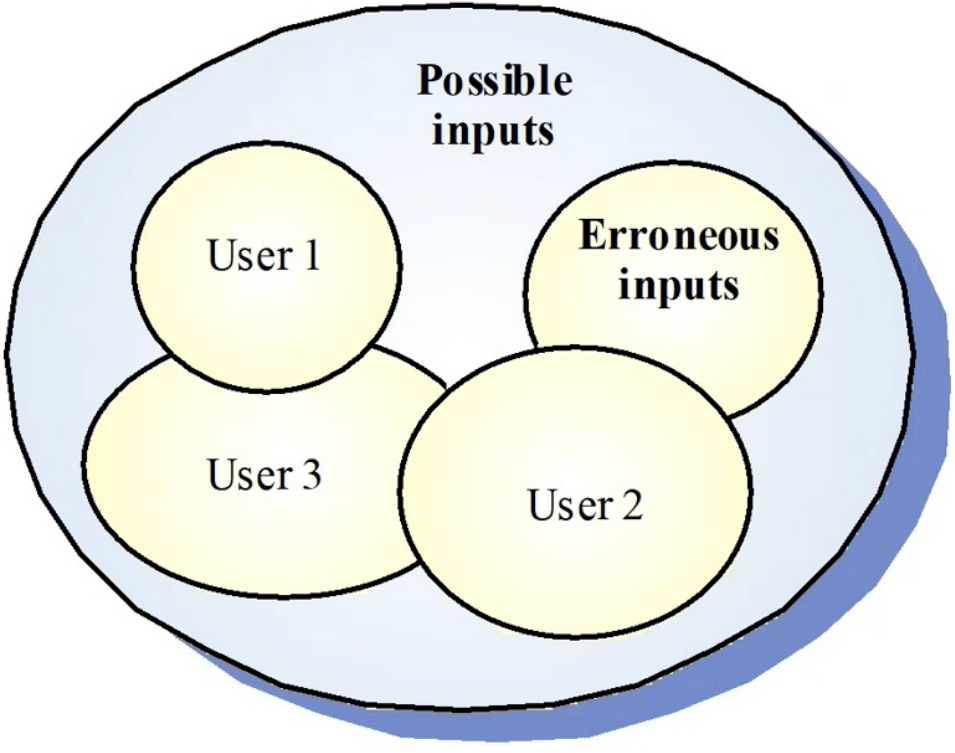
- You can model a system as an **input-output mapping** where some inputs will result in failures (i.e not-expectd outputs)
- The reliability of the system is the probability that a particular input will lie in the set of inputs that cause not -expected outputs
- HOWEVER, different people will use the system in different ways so this probability is not a static system attribute but depends on the system's environment

Input/output mapping



AFFIDABILITA`

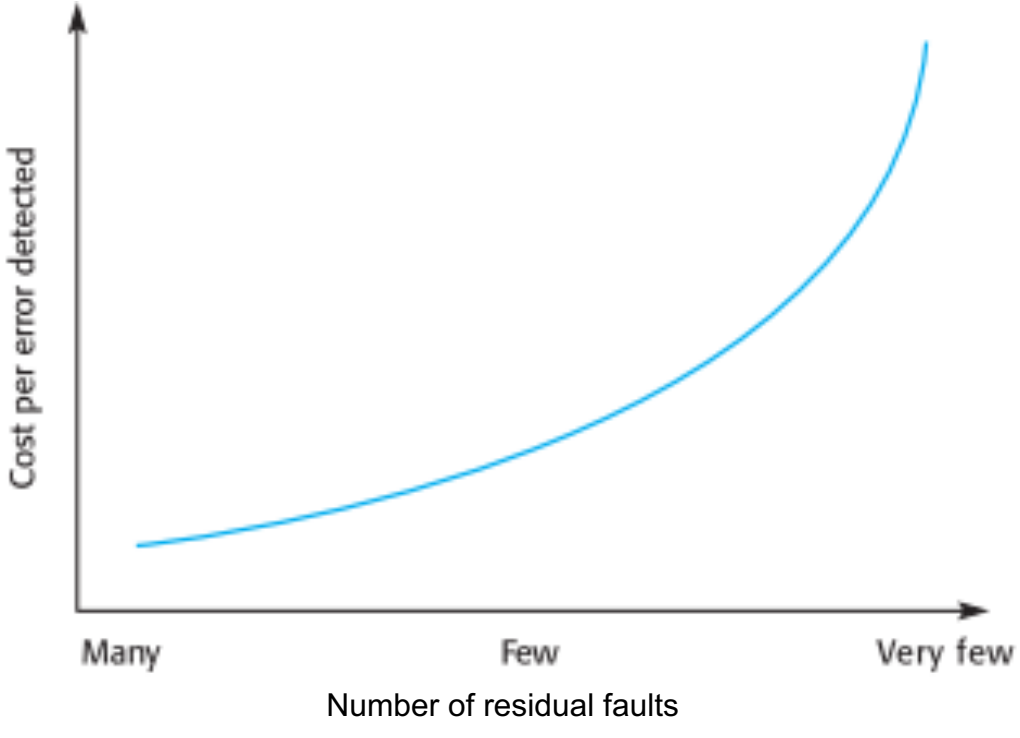
Reliability perception



Reliability improvement

- Removing X% of the faults in a system will not necessarily improve the reliability by X%. A study at IBM showed that removing 60% of product defects resulted in a 3% improvement in reliability
- Program defects may be in rarely executed sections of the code so may never be encountered by users. Removing these does not affect the perceived reliability
- A program with known faults may therefore still be seen as reliable by its users
- Users adapt their behaviour to avoid system features that may fail for them ? A program with known faults may therefore still be perceived as reliable by its users.

The increasing costs of residual fault (bug) removal



Problematiche relative alle Safety e alla Security sono trattate in altri corsi.

Set 13 - Cosa ricordare: concetti, motivazioni, conseguenze, relazioni fra concetti, ecc.

- Concetto di dependability (Fidatezza, F.) e sua motivazione, anche in prospettiva storica; fiducia nel sistema sw, sfacettature del concetto. Le 4 dimensioni della F.: 2 probabilità: affidabilità e disponibilità, e 2 giudizi: sicurezza e protezione; altre possibili dimensioni: manutenibilità, una visione d'insieme delle 5 dimensioni; survivaility e resilienza. Aspetto economico: relazioni costi di sviluppo e livello di F., possibili situazioni di compromesso. Relazioni tra nonF. (untrustworthiness) e performance.
- Definizione precisa di Affidabilità (Aff.), Disponibilità (Disp.) e Manutenibilità; relazioni tra Aff. e Disp.; Terminologia (italiano e inglese): malfunzionamento (MF) del sistema/system failure, system error/errore del sistema, system fault-bug/guasto del sistema, human error-mistake/errore umano- sbaglio. Relazione errore umano -fault- system error - failure; influenza del testing sulla scoperta dei MF, percezione dei MF anche in dipendenza delle conseguenze del MF.
- Approcci per aumentare la affidabilità (durante lo sviluppo o al run time): fault avoidance, fault detection e removal, fault tolerance. Affidabilità e mapping degli input negli output, diverse percezioni di utenti diversi, relazione tra difetti rimossi ed aumento della affidabilità e percezione dell'affidabilità

Set 13bis - Cosa ricordare: concetti, motivazioni, conseguenze, relazioni fra concetti, ecc.

- Sicurezza (Safety): definizione, tipologie di sistemi, tipologie ‘shall-not’ dei requisiti di sicurezza. Relazioni con affidabilità: sistemi affidabili ma poco sicuri.
- Protezione (Secutiy): definizione, impatto, prerequisito delle altre tre dimensioni.