Sisteme de Încredere (*eng.* Dependable Systems) - Introducere -

Ciprian Dobre
ciprian.dobre@cs.pub.ro

Aspecte administrative

Reguli, notare, …

Notare

- Verificați regulamentul postat…
- 1 prezentare în cadrul cursului: 20% (max 2)
  - Verificați aspecte privind organizarea și desfășurarea
- Proiect: 50%
- Examen final: 40%

Informații

- Site-ul cursului: http://curs.cs. pub.ro
- Open-office (EG303):
  - Luni, 10-12am
  - Miercuri, 10-12am
- E-mail: ciprian.dobre@cs.pub.ro

Proiect

- Proiectul trebuie să se finalizeze cu un articol
  - Format indicat
  - Minim 6 pagini – Introducere, Related Work, Contribuția articolului, Rezultate
- Se alege în primele săptămâni de școală
- Se predă maxim până la data specificată pe site

Prezentări

- Se aleg în primele 4 săptămâni de școală
- Prezentările încep cu săptămâna 5
- Fiecare student are la dispoziție maxim 20 de minute

- Aspecte de evidențiat (obligatoriu):
- Este problema reală?
- Care este principala contribuție a articolului?

Prezentări

- Prin ce diferă soluția de lucrările anterioare?
- Autorii lucrării (sau voi) identifică abstractizări sau limitări fundamentale ale soluțiilor anterioare?
- Credeți că lucrarea va avea un efect în următorii 10 ani? De ce sau de ce nu.
- Încercați să formulați o perspectivă critică asupra viitorului: probleme, soluții…
  - Verificați lucrările din trecut pentru exemple de pornire

Cuprins

- Introducere în problematica cursului
- Trecere în revistă a principalelor atribute ale Sistemelor de Încredere
- Cerințe pentru creșterea proprietății de Încredere

Definiție

- Definiția cu care lucrăm în cadrul cursului:

  "Dependability is the property of a system such that we can justifiably place our reliance on the service it delivers"

  J.C. Laprie (IFIP Working Group 10.4)

  IEEE Transactions on Dependable and Secure Computing, Vol. 1, No.1, pp. 11-32, 2004

Definiție

"Dependability is the property of a system such that we can justifiably place our reliance on the service it delivers"

J.C. Laprie (IFIP Working Gro

IEEE Transactions on Depen

Computing, Vol. 1, No.1, pp.

Totalitatea organizațiilor, oamenilor, hardware, software, etc. care compun un sistem

Definiție

"Dependability is the property of a system such that we can justifiably place our reliance on the service it delivers"

J.C. Laprie (IFIP Working Group 1

IEEE Transaction e
Computing, Vol.

Necesită o demonstrație, dovadă sau argument justificabil

Definiție

"Dependability is the property of a system such that we can justifiably place our reliance on the service it delivers"

Ne "bazăm" pe sistem pentru un anumit scop particular

oup 10.4)

ndable and Secure

11-32, 2004

Definiție

"Dependability is the property of a system such that we can justifiably place our reliance on the service it delivers"

J.C. Laprie (IFIP Wor
IEEE Transactions o
Computing, Vol. 1, N

Elemente produse de acesta, datele generate, efectele fizice create, experiența furnizată

Definiție

- Proprietatea de “încredere” poate fi văzută ca:
  - Funcționarea corectă a sistemului
  - Încrederea în sistem
- Atribute ale încrederii?
- Metode de asigurare a încrederii?

Din ce perspectivă? Cum se demonstrează?

Justificarea încrederii

- Se poate evalua încrederea unui sistem prin compararea funcționării cu specificația acestuia?
  - Ușor
  - Dar specificațiile pot fi incorecte/ incomplete
- Sau vs. așteptările utilizatorilor?
  - Managerii pot avea așteptări nerealiste
  - Încrederea depinde în final de perspectiva prin care o definim

Principalele atribute ale încrederii

- Fiabilitate (*eng.* Reliability)
  - Continuitate în livrarea unui serviciu corect
- Disponibilitate (Availability)
  - Disponibilitate în livrarea unui serviciu corect
- Siguranță (Safety)
  - Absența consecințelor catastrofice pentru utilizator/mediu
- Securitate (Security)
  - Rezistența la atacuri împotriva sistemului

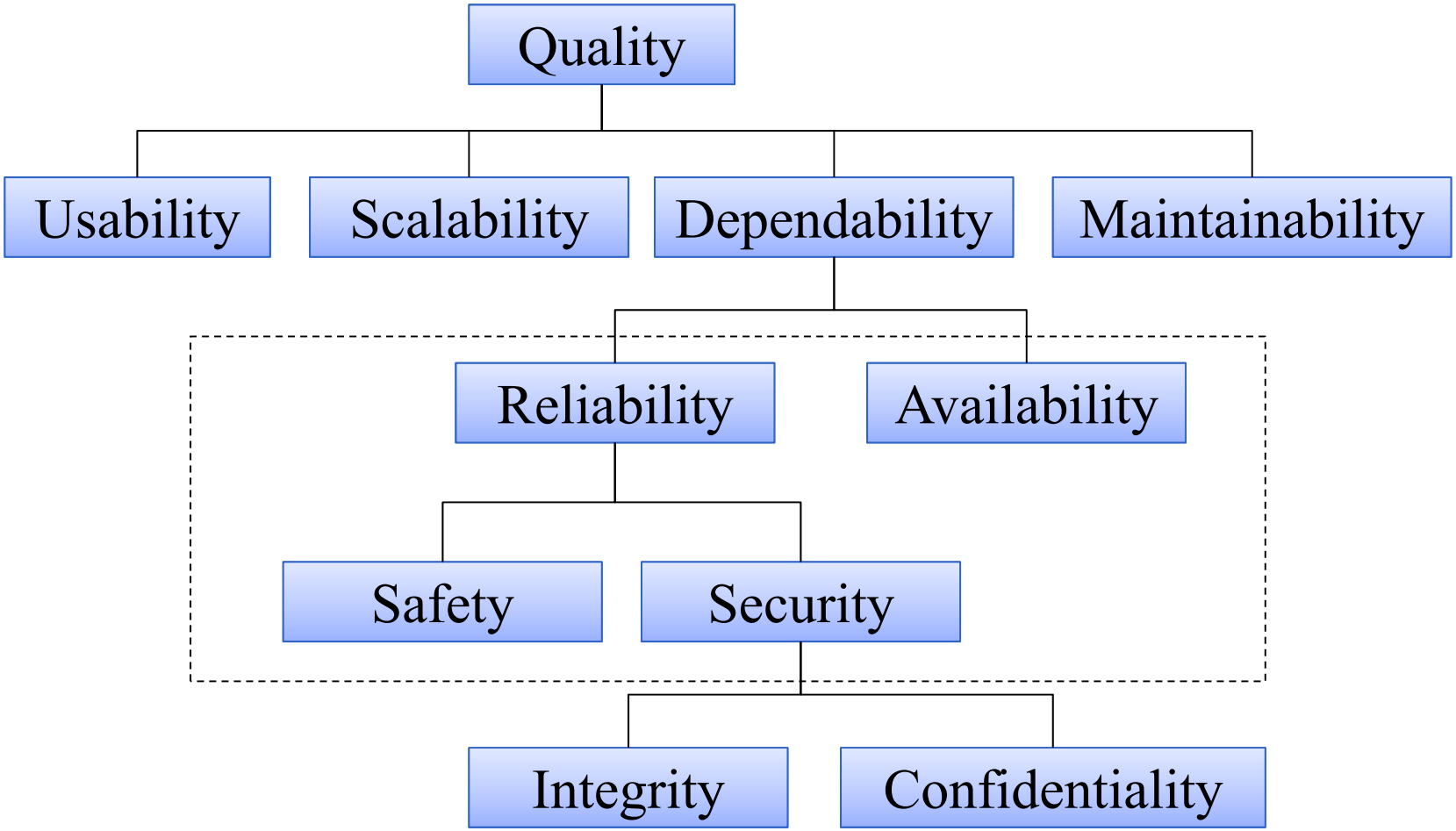
Fiabilitate

Disponibilitate

Siguranță

Securitate

O ierarhie a proprietăților



Ierarhia proprietăților

- Ce alte atribute pot fi adăugate?
- Exemple:
  - Performanță
  - Accesibilitate
  - Supraviețuire
  - Adaptabilitate
  - Portabilitate
  - Robustețe
  - Corectitudine

Fiabilitatea

- Corectitudinea funcționării unui serviciu:
  - Abilitatea unui sistem sau a unei componente de a efectua funcțiile cerute, în condiții date și pentru o perioadă de timp specificată.

Exemplu

- Presupunem un sistem având un MTBF (Mean Time Between Failure) de 3 ani, sau 26.280 de ore (calculați).
- Ne interesează probabilitatea ca acest sistem să nu sufere întreruperi pentru o perioadă de observație de 1 an.
- Pentru aceasta putem folosi formula:

$$R = e^{-\frac{t}{MTBF}}$$

unde

R = Reliability (Fiabilitatea)
e = 2.71828182845904, baza logaritmului natural
t = perioada de observație
MTBF = Mean Time Between Failure pentru sistemul specificat

Folosind această formulă probabilitea obținută este de 0,7165.

Aceasta corespunde unei probabilități de apariție a unei întreruperi în timpul de 1 an de 1-0.7165=0.2835 (~28%).

Disponibilitatea

- Disponibilitatea unui serviciu atunci când este cerut
  - Procentul de timp în care sistemul funcționează conform așteptărilor.

- Măsurătorile care stau la baza calculării acestui procentaj pot fi discrete (de câte ori un motor a pornit cu succes dintr-o serie de 1000 de încercări) sau continue (numărul de ore dintr-un an în care un sistem este operațional pe parcursul unui an).

Disponibilitatea

- Pentru calculul disponibilității se folosește formula:

$$A = \frac{MTBF}{MBTF + MTTR}$$

unde

A = Availability (Disponibilitatea)

MTBF = Mean Time Between Failure în cazul sistemului aflat sub observație

MTTR = Mean Time To Repair

Maintainability = ușurința în restaurarea funcționării

Mentenabilitatea unui sistem

- Usurinta functiei de restaurare
  - Masura ca timpul necesar functiei de restaurare a serviciului sistemului

Timp de Restaurare = Pregatirea reparatiei + Reparatia + Timpul de Startup

MTTR = Mean Time to ~~Repair~~ Restore

Siguranta

- Minimizarea riscului de distrugere in cazul oamenilor sau mediului
  - In timpul operațiilor normale sau anormale efectuate asupra sistemului
- Este f. important pentru sisteme critice!
- Adesea indicata prin “nivelul de integritate”
  - Masuri cantitative sunt mai greu de determinat
- Sistemele sunt clasificate ca Primare/Secundare
  - Potentialul de a cauza distrugeri direct/indirect

Securitate

- Rezistența la defecte accidentale/intenționate
- Rezistența la folosire/acces neautorizat
- Protecția împotriva factorilor externi
- Importantă pentru toate sistemele critice
- Încorporeaza integritate + confidențialitate
- Esențială pentru protejarea altor atribute
- Adesea indicată prin “nivelul de integritate”

Siguranță și securitate

- Siguranță:
  - Protecția împotriva defectelor accidentale
- Securitate:
  - Protecția împotriva defectelor intenționate

Studiu de caz: Proprietatea de încredere și iPod

- Fiabilitatea
  - Decodare corectă MP3
  - Ordine corectă de redare
  - Nu necesită resetare !!!
- Disponibilitatea
  - Pornește atunci când doriți redarea unei melodii
  - Nu face pauze lungi între melodii
  - Durată lungă a bateriei
- Siguranța
  - Nu se sparge în buzunarul utilizatorului sau nu provoacă tăieturi acestuia
  - Nu electrocutează la utilizare
  - Bateria nu se scurge în buzunar
- Securitatea
  - Nu corupe fișierele MP3
  - Are funcție de protecție prin parolă
  - Suportă conector pentru lacăt

Cerințe ale Încrederii

- Fiecare aspect al încrederii...
  - Siguranță
  - Securitate
  - Fiabilitate
  - Disponibilitate

…poate implica alte cerințe noi ale sistemului

Implicări ale cerințelor

- Cerințe funcționale:
  - Verificarea la erori
  - Redundanță
  - Protejarea componentelor
- Cerințe non-funcționale:
  - Constrângeri asupra fiabilității și disponibilității
  - Adesea se bazează pe alte cerințe funcționale
- Cerințe dis-funcționale:
  - Considerații asupra siguranței și securității de tipul “Shall Not”

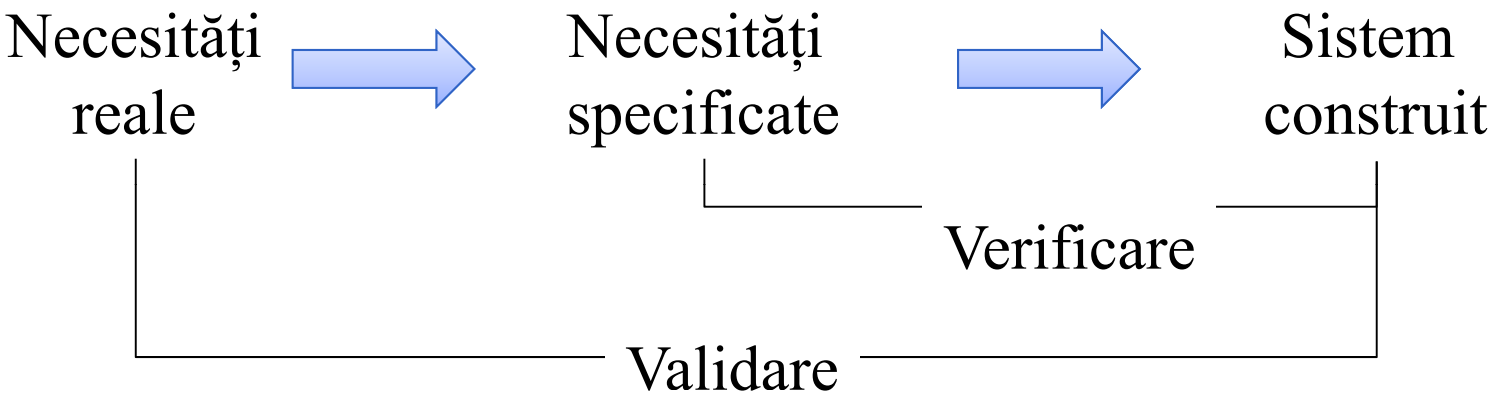
Exemple de cerințe

- Cerințe funcționale:
  - Sistemul va trebui să cripteze detaliile cărții de credit ale utilizatorului
- Cerințe non-funcționale:
  - Sistemul va trebui să furnizeze un răspuns în maxim 10 secunde
- Cerințe dis-funcționale:
  - Sistemul nu va trebui să permită accesul neautorizat

Exemple de Criterii Măsurabile

- Timpul necesar efectuării unor task-uri
- Fog index (lizibilitatea limbajului natural)
- Numărul de defecțiuni găsite
- Numărul de defecte (pe unitatea de timp)
- Numărul de erori (pe unitatea de timp)
- Complexitatea ciclomatică
- Lungimea manualului utilizatorului
- Timpul de start-up sau restart
- Timpul (mediu) de execuție
- Timpul (mediu) de reparare
- Numărul de persoane accidentate / ucise

Validare și verificare



- "Sistemul întrunește specificațiile" sau "Sistemul întrunește necesitățile clientului"
- Care este măsura corectă a calității?