University of Twente
The Netherlands

==== NIRICT // CeDAS ====

3TU Centre of Excellence for Design, Analysis and Synthesis of Dependable Systems

Boudewijn Haverkort

CTIT Annual Symposium, May 2006

what is dependability?

definition provided by IFIP WG 10.4 & IEEE TC on Fault-tolerant computing (cf. http://www.dependability.org/):

“trustworthiness of a (computing) system which allows reliance to be justifiably placed on the services it delivers”

key dependability attributes

1) availability
2) reliability
3) safety
4) integrity
5) maintainability
6) confidentiality

but we also require:

- usability
- performance
- power awareness
- security (“1+4+6”)
- …

attributes should always be quantifiable!

limited dependability budget

- achieving dependability, with limited budget, asks for design choices across the system hierarchy
- simple hardware requires costly mechanisms in software to “repair hardware failures”
- special hardware allows for “leaner software”
- design cost *vs.* operational cost
- dependability solution impacts performance
- cross-layer design and optimization needed

example: dependable networking (1)

- cross-layer approach needed to get the best out of the dependability budget
- dependability of TCP/IP achieved through software (slow) is only feasible for reliable (“cabled”) underlying links
- extra link-layer capabilities would be benificial when using wireless links, to avoid performance problems

example: dependable networking (2)

- scale determines provable dependability
- owning party has overall (local) control
- world-wide scale: end-to-end control does not exist, which hampers provable dependability
- deal with “holes” in dependability specs
- on-line (re)configurations required, on a very large scale; must be self-configurations
- control theory for dynamic-redundant systems

CeDAS will…

focus on design of high-quality dependable systems, using sound integrated system modeling, analysis & synthesis techniques:

- improve on methods for model/system construction, analysis and synthesis
- real-life (industrial) application of these
- hence, substantially improve thrustworthiness of computer & communication systems

CeDAS *vs*. grand challenges of the BCS

- science for global ubiquitous computing
  systems, models, design, software construction, verification
- scalable ubiquitous computing systems
  selfstar systems, correctness, performance, quantitative properties, verification
- dependable systems evolution
  theory—tools—real systems
- NSF program “science of design”

current CeDAS activities

- 12 chairs labelled “CeDAS chair”
- 6 new CeDAS chairs being hired
- work on CeDAS research profile by three coordinators:
  - Van Gemund, TUD
  - Van der Aalst, TU/e
  - Haverkort, UT
- SmartMix proposal, with ESI (Brinksma)

CeDAS research profile

- initial group of 12+6 chairs
- mostly interaction among coordinators
- activities grouped along two axes:
  - systems axis:

    application, communication, transmission, embedded
  - methodology axis:

    design, modeling, analysis, synthesis
- plenary CeDAS meeting being planned

SmartMix proposal

- mix of exploratory (“academic”), application-oriented (“industry as laboratory”), and application (“industry”) projects
- firm basis in (general) dependable system design methods and techniques
- tailored to important application areas, such as healthcare and logistics
- strong industrial involvement
- volume about 7.5 MEuro/year, for 5 years

12 initial CeDAS chairs

- always 2 EE and 2 CS
- TUD:
  Vassiliadis, Lagendijk, Van der Veen, Van Deursen
- TU/e:
  Van der Aalst, Groote, Corporaal, Koonen
- UT:
  Brinksma, Nauta, Hartel, Haverkort