Risk Management and Dependability – What Are the Key Factors?

Chair: Fevzi Belli
University of Paderborn, Germany
(belli@upb.de; http://adt.upb.de)

Prologue

On June 4th, 1996, the maiden flight of the Ariane 5 launcher exploded about 37 second after lift-off. Scientist with experiments on board that had taken years to prepare were devastated. For many software engineering researchers, however, the disaster is a case study rich in lessons [1].

The very first questions were: *How come? Who dunnit?*

And the next one: *How to avoid this in future?*

A. Sketching the Topic

1. Dependability is defined as
   - *The ability to deliver service that can justifiably be trusted.* J.-C. Laprie

or

   - *Ability to perform as and when required.* IEC, TC 56/ISO TC 176; adopting in ISO 9000 pending.
2. Characteristics of dependability as *risk factors* are (not complete)
   - *Attributes*
   - ▪ Safety
   - ▪ Security
   - ▪ Reliability
   - ▪ Availability
   - ▪ Maintainability
   - ▪ Confidence
   - ▪ Integration
   - ▪ …
   - *Means*
   - ▪ Fault prevention
   - ▪ Fault tolerance
3. These characteristics of dependability are disciplines of their own. We have even renowned conferences, journals named after those factors.
4. Development and deployment of large, complex computer systems are risky.
5. Risk Management: tentatively defined via (subject to be changed/to be discussed, [2])

   Risk Exposure (Impacts/Costs) ≅
   Probability (Loss) * *Size (Loss)*

B. Some of the Questions to be Discussed

1. Are these characteristics to be handled equally when managing risks?
2. Or, should we decide for one key factor and forget the others?
3. Or, should we decide for a selection of (privileged) key factors?
4. Or, is there a standard/canonical ranking of them, e.g., safety before reliability before confidence, etc.?
5. If ranking, do they cause pair wise conflict(s) when assigning priorities, e.g., security vs. fault tolerance?
6. After the next disaster: We do not want to ask "Who Dunnit"? Better, we should ask to avoid any disaster: **Whose job is it?**
   - Project manager's?
   - Test & Quality engineer's?,
   - Designer's?
   - Programmer's?
   - Or, whoever else?

C. Documentation

The documentation of the discussion can be visited under http://adt.upb.de/aktuelles/veranstaltungen/comp-sac2004/

Arguments and positions can be sent to belli@upb.de (also after the conference).

D. Participants

Dr. HUI Chi Kwong, Lucas

(hui@cs.hku.hk, http://www.csis.hku.hk/~hui)

is the founder and Honorary Director of the Center for Information Security & Cryptography, and concurrently an associate professor in the Department of Computer Science, The University of Hong Kong.

Dr. KOCHS, Hans-Dieter

(kochs@uni-duisburg.de,
www.mti.uni-duisburg.de/~kochs)

is a professor and the chair of the Institut für Informationstechnik/Informationslogistik (Institute for Information Technology and Information Logistics) of the Univ. Duisburg/Essen, Germany. He was one of the analysts of mechatronic dependability among this topic including analysis of the Concorde disaster.

Dr. LAPRIE Jean-Claude

(laprie@laas.fr, http://www.laas.fr/laasve/index.htm)

is the research director with the Dept. Dependable Computing and Fault Tolerance of the LAAS (Laboratoire d'Analyse et d'Architecture des Systèmes, Analysis and Architecture of Systems), Toulouse, France, which is a particular research unit of the CNRS (National Center for Scientific Research).

Literature

[1] B. Nuseibeh, "Ariane 5: Who Dunnit?", IEEE Software, pp. 15-16, 1997

[2] R. Fairley, "Risk Management for Software Projects", IEEE Software, pp. 57-67, 1994