Challenges and Directions for Dependable Computing: some reflections on a few open research problems

Luca Simoncini – CNUCE, Italy

- Dependable computing is still active in providing problems and opportunities to computer scientists and industry

- Significant advances have been achieved in the last decades

- The evolution of needs of our information society, the technological advances and the increasing complexity of modern applications pose new problems when applying “traditional” dependability concepts

- A broad approach is required, encompassing theoretical studies, careful consideration of possible alternatives and their likely consequences, and design and implementation activities
A few open research problems

• *usability* and *man-machine interface* are among the pressing issues we are facing today in dependable systems

• Accounting for them implies acting on
  the production process of dependable systems,
  with adequate consideration of the human factors,
  and keeping into account dependability requirements of emerging applications
Production process of dependable systems

The production process, from requirements specification to implementation, requires **continuous interactions** between the **activities at the different stages with the validation and verification of each step**.

Challenging issues in **validation** of complex systems are:

- design integration
- composition
- re-use
- usability

exacerbated by the trend of **building systems out of existing components** (legacy systems, COTS, ..)

*Environments* enabling system development through the composition of software components, offering *methods* and *tools* supporting the *design, analysis, construction and deployment* of such systems are of primary importance.
Production process of dependable system (2)

- **design integration** of a set of components - some sort of verifiable compositionality property of component parts is required

- **composition**, both at **design level** (choice of the components to integrate) and at **verification level**, where a validation framework is required including different validation techniques - criteria have to be defined on how to select the appropriate verification technique for each part of the system

- **re-use** of available components, also re-using as much as possible the verification activities already performed on them

- **usability**, both at the level of **user interface** and at the level of facilities offered by the developing environment to the designer in order to perform validation activities without requiring specific skills
Human factors

- The dependability of a system is heavily influenced by the dependability of the man-machine interaction.
- It is necessary to introduce “human in the loop” as a design pre-requisite.
- Continuous interaction between user and system, as a consequence of two aspects of a new generation of interacting systems: **ubiquity** and **invisibility**.
- Human behavior is more unpredictable than any conventional fault model → question:
  - Is it better to adopt a defensive strategy that constrains what the user can do to perturb the operations or should one design around all foreseeable situations?
Human factors (2)

• It is difficult to constrain users to adopt a simplified behavior that characterizes a state of technological awareness
  – There is a need for the systems to adapt to users, to be aware of their operating context, and to be able to take autonomous decisions to some extent
  – Human dependency on the correct behavior of systems in many (if not all) aspects of everyday life has a growing impact

• In safety critical systems, it is important to extend formal techniques to explicitly consider human factors within the design and assessment processes
Emerging applications

- Increase of new emerging application with great demand for **working and affordable dependability** (e.g., financial/banking systems, telecommunication, embedded systems, e-commerce, ..)

- The emphasis is not on pursuing top-level dependability requirements but solutions have to be defined which accommodate a **number of desired requirements**

- **Scalability, heterogeneity, flexibility, distribution, timeliness** are among the most challenging issues of dependability connected with new business and everyday life application scenarios

- **Assurance of a guaranteed level of QoS** is the research objective in such contexts, where QoS encompasses many aspects such as traditionally-related dependability attributes, performance related indicators, measures expressing user-perceived service quality
Emerging applications (2)

• The term safety critical system extends its meaning to denote a larger class of systems that are becoming critical for their impact on individual’s every-day life.

• The new form of catastrophic failure is induced by a large number of individually non-catastrophic failures (think to the very large number of the same type of embedded systems which are operated by a very large number of non-trained users).

• Again, the concepts of usability and man-machine interface are central in this area and will be a leading research problem.
Usability

• The property of an artifact of conveying the perception that it effectively performs the task for which it is being used.

• Ease of use can be measured by how quickly a task is performed, how many mistakes are made, how quickly the system is learned and how satisfied people are who perform the task.

• Usability may also include factors such as safety, usefulness, and cost-effectiveness.
# Usability

<table>
<thead>
<tr>
<th>Traditional techniques</th>
<th>Needs for basic research</th>
</tr>
</thead>
<tbody>
<tr>
<td>• prototyping</td>
<td>• cognitive modeling</td>
</tr>
<tr>
<td>• user testing</td>
<td>• syndetic modeling</td>
</tr>
<tr>
<td>• usability testing</td>
<td>• syndetic modelling with explicit variability, using native performance data of user</td>
</tr>
<tr>
<td>• usability inspection</td>
<td>behaviour expressed through time stochastic variables.</td>
</tr>
</tbody>
</table>