# Position Paper

# Production Process of Dependable Systems / Human Factors / Emerging Applications

*A. Bondavalli*, F. Di Giandomenico**, L. Simoncini****

*University of Florence, Italy
**IEI-CNR, Pisa, Italy
***CNUCE-CNR and University of Pisa, Italy

**41st Meeting of IFIP WG 10.4**

**Saint John, US Virgin Islands — January 4-8, 2002**

# Introduction

- **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,**
- **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, ..)

**NEED of *Environments* for developing systems out of components offering *methods* and *tools* supporting the *design*, *analysis*, *construction and deployment* of such systems**

# Production process of dependable system (2)

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

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

# Production process of dependable system (3)

- **re-use** of available components, also re-using as much as possible the **verification** activities already performed on them - stress on the following problems
  - –*how to ensure that only "**proper services**" will be requested to the re-used component*
  - –*how to verify that **dependability properties already verified** on the re-used component as stand-alone **will be preserved after integration***
  - –*well proven components may be **source of system failure** when re-used in a new system because of **misuse***
- **usability**, both at the level of **user interface** and at the level of **facilities offered by the developing environment** to the designer 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 widespread embedding of computation, operated by non-trained users, exacerbates the problem of the **large-scale impact on the criticality** of specific products
- The widespread embedding of computation within everyday objects and appliances exacerbates the problem of **catastrophic failure induced by a large number of individually non-catastrophic failures**
- Again, the concepts of **usability** and **man-machine** interface are central in this area and will be a leading research problem