Chapter 8

Technological and Educational Challenges of Resilient Computing

Luca Simoncini
University of Pisa, Italy

ABSTRACT

The adjective resilient has been used in dependable computing essentially as a synonym of fault-tolerant, thus ignoring the unexpected aspect of the phenomena the systems may have to face. These phenomena are very relevant when moving to systems like the future large, networked, evolving systems constituting complex information infrastructures that are the emergence of the ubiquitous systems that will support Ambient Intelligence. From an educational point of view, very few Universities offer a comprehensive track that is able to prepare students able to cope with the challenges posed by the design of ubiquitous systems. To fill both gaps, a European Network of Excellence, ReSIST – Resilience for Survivability in IST, was run from January 2006 to March 2009 (see http://www.resist-noe.org/). In this article the technological challenges, the related educational issues and a proposed MSc curriculum in Resilient Computing that arise from the results of ReSIST are presented and discussed.

INTRODUCTION

The current state-of-knowledge and state-of-the-art reasonably enable the construction and operation of critical systems, both safety-critical (e.g., avionics, railway signaling, nuclear control) or availability-critical (e.g., back-end servers for transaction processing).

The situation drastically worsens when considering large, networked and evolving systems either fixed or mobile, with demanding requirements driven by their application domain, i.e. ubiquitous systems. There is statistical evidence that these emerging systems suffer from a significant drop in dependability and security in comparison with the former systems. There is thus a dependability and security gap opening in front of us that, if not filled, will endanger the very basis and advent of Ambient Intelligence (AmI).
Filling the gap clearly needs dependability and security technologies to scale up, in order to counteract the two main drivers of the creation and widening of the gap: complexity and cost pressure. Coping with complexity and cost certainly demands significant progress in the rigorous design of the functionalities provided by the information infrastructures. However, the interplay between: a) rigorous design on one hand, and b) complexity and cost on the other, will inevitably lead to residual development defects, vulnerabilities, and room for interaction mistakes.

It is therefore mandatory to provide pervasive information infrastructures with scalable resilience for survivability in direct support of the emerging pervasiveness of computing systems.

To succeed in this goal it is important to reach a common, agreed definition and understanding of the term resilience that has already been used, sometimes with different meaning, for some specific domains, strongly influenced by scalability, interdependency and evolutionary complexity.

This article first introduces a presentation and discussion on the term resilience to identify the meaning that such term may have when dealing with complex, ever changing, ubiquitous and pervasive systems. Then, a discussion is done on challenges that are posed by scalable resilience for such systems. We then introduce educational issues in Computer Science and Engineering and how present higher education institutions deal with the challenge of preparing persons able to cope with the problem of designing, evaluating and operating ubiquitous systems. Finally, the proposed MSc Curriculum in Resilient Computing is presented. The conclusions of the article, more than providing solutions, try to open a discussion on all these issues.

On the Term Resilience (Laprie, 2008)

The term resilience has been used in many fields and, as a property, two threads can be identified: a) in social psychology (Claudel, 1965), where it is about elasticity, spirit, resource and good mood, and b) and in material science, where it is about robustness and elasticity.

The notion of resilience has then been elaborated:

- In child psychology and psychiatry (Engle, 1996), referring to living and developing successfully when facing adversity;
- In ecology (Holling, 1973), referring to moving from a stability domain to another one under the influence of disturbances;
- In business (Hamel, 2003), referring to the capacity to reinvent a business model before circumstances force to;
- In industrial safety (Hollnagel, 2006), referring to anticipating risk changes before damage occurrence.

A common point to the above senses of the notion of resilience is the ability to successfully accommodate unforeseen environmental perturbations or disturbances.

The adjective resilient has been in use for decades in the field of dependable computing systems, e.g. (Laprie, 2008), and is more and more in use, however essentially as a synonym of fault-tolerant, thus generally ignoring the unexpected aspect of the phenomena the systems may have to face. A noteworthy exception is the preface of (Anderson, 1985), which says: