Challenges in Nanocomputing for Dependability and Security

Takashi Nanya
University of Tokyo, Tokyo, Japan
nanya@hal.rcast.u-tokyo.ac.jp

Abstract

Physical phenomena with nanocomputing technology may cause a threat against dependability and security. Many of the existing solutions based on redundancy and diversity for traditional computing systems can also be applied to nanocomputing systems. Difficult, but important challenges are to define metrics of dependability and security from user's point of view, make them visible and map them to economic values.

1. State-of-knowledge

With the amazingly rapid pace, called the Moore's law, of improvement in its integration level as well as the decreased cost-per-function, the VLSI technology has contributed to the significant enhancement in quality of life through the continuous advances in computing and communication technologies. It must be pointed out, however, that further improvement predicted to continue for another decade or more may cause serious problems in the dependability and security of coming information society due to inexperienced physical phenomena such as current leakage, process and environment parameter variations, soft errors, cross talks, IR drops etc. that are caused by smaller feature sizes and weaker signal strength in the foreseen future-generation semiconductor technology. These emerging physical phenomena are major sources of a larger defect rate in production, a higher level of transient faults in operation, and a shorter life of workable components in systems' life cycle

In addition, ever-increasing demands for the enhancement of system functionality and performance have already resulted in a formidable level of design complexity in embedded systems. Most problems in the design and architecture of modern networked systems are caused by complexity, openness, large scale, uncertainty, heterogeneity, interdependency in nature of software and VLSI systems. These cause new types of vulnerability and threats of malicious and accidental nature, e.g. uncontrolled interactions in networked information systems with human behavior being pervasively involved.

2 Difficult, but important challenges

There have already existed many dependability methodologies, including methods for fault prevention, fault tolerance, defect tolerance and yield enhancement, so far accumulated for a variety of computing systems based on the general principle of incorporating redundancy and diversity. Many of them can also be applied validly to VLSI system design with future nanocomputing technologies. However, no solutions exist for bridging a huge gap between the dependability & security intended and implemented in VLSI components of an information system and the dependability & security perceived by customers of the service delivered from the information system. Customers don't care about how fault-tolerant and defect-tolerant VLSI components are used in a system, but want to be confident in how dependable and secure the services the system delivers are.

Consequently, difficult, but important challenges are, first, to define a set of metrics that represent the degree of dependability and security from user's point of view for services provided by the system at the end-user interface so that the value of dependability and security can be made visible and mapped to economic values, and then, to specify the design goal of each level of system hierarchy so that the dependability and security specifications at the top level are reduced consistently to the lower-level design specifications. These challenges give a strong incentive for industries to work explicitly toward dependability-oriented design and development that never happened in the past when only performance and functionality can be priced in the market of information systems. Specific challenges that make the problem difficult includes 1) human-made-fault modeling, and 2) dependency of the required level of service quality on applications, environments and conditions with which information systems provide their services. Solving the problem requires not only established research approaches to identify metrics and methods for measurement and evaluation, but also interdisciplinary approaches that may well be taken with international, both industrial and academic, collaborations toward global standards.