Chapter 35
Fault-Tolerant and Fail-Safe Design based on Reconfiguration

Hana Kubatova
Czech Technical University in Prague, Czech Republic

Pavel Kubalik
Czech Technical University in Prague, Czech Republic

ABSTRACT

The main aim of this chapter is to present the way, how to design fault-tolerant or fail-safe systems in programmable hardware (FPGAs) and therefore to use FPGAs in mission-critical applications, too. RAM based FPGAs are usually taken for unreliable due to high probability of transient faults (SEU) and therefore inapplicable in this area. But FPGAs can be easily reconfigured. The authors' aim is to utilize appropriate type of FPGA reconfiguration and to combine it with well-known methods for fail-safe and fault-tolerant design (duplex, TMR) including on-line testing methods for fault detection and then startup of the reconfiguration process. Dependability parameters' calculations based on reliability models is integral part of proposed methodology. The trade-off between the requested level of dependability characteristics of a designed system and area overhead with respect to FPGA possible faults the main property and advantage of proposed methodology.

INTRODUCTION

Field-programmable gate arrays (FPGAs) are configurable VLSI devices which can implement various logic functions. Classical SRAM-based FPGA chips introduced in 1984 were designed to be configured only once at the beginning of their operation (at power-up) and to enable a designer to improve the functionality (or correct bugs) after a device had been shipped to the end user. This factor together with the possibility to personalize an FPGA in the field has resulted in their increasing popularity. Now, almost two decades later, the current FPGA technology has introduced the concept

DOI: 10.4018/978-1-4666-3886-0.ch035

of dynamic reconfigurability (also called runtime reconfigurability). At present devices that support limited or full dynamic reconfigurability are available, e.g Xilinx or Atmel. The term reconfiguration can be qualified using several different aspects. Reconfiguration can be either static or dynamic. The system with static reconfiguration remains the same throughout the application lifetime. On the contrary, the configuration of a dynamically reconfigured system changes during the application lifetime. There exist two basic approaches that can be used to implement dynamically reconfigurable applications: full reconfiguration and partial reconfiguration. Fully reconfigurable systems allocate all FPGA resources in each configuration step. Partial reconfiguration may change any portion of the reconfigurable resources at any time. Partially reconfigurable FPGAs offer a faster way to change an active FPGA circuit since only those parts that need to be reconfigured are stopped. The FPGA devices with the partial reconfiguration can be further qualified according to the size of its basic reconfiguration element as fine-grain or coarse-grain reconfiguration architectures. The first architecture can reconfigure the smallest available elements without affecting other resources. The latter architecture allows only the reconfiguration of the bigger and more complex elements. Both types have their strengths and drawbacks. For our aim it is necessary to choose appropriate type of reconfiguration and moreover with respect to desired dependability parameters, including the time of reconfiguration process and its synchronization.

The determination and definitions of dependability terms (based on Pradhan, 1996)) and used abbreviations will be presented in the following text:

- Reliability is the probability of a component or a system functioning correctly over a given period of time under given set of operating conditions. This is a standard definition of the reliability. The set of operating conditions is usually defined in the technical specification of the system or the component.
- Availability of a system is the probability that the system will be functioning correctly at given time.
- Maintainability is the ability of a system to be maintained.
- Maintenance is the action taken to retain a system in, or return a system to its designed operating condition.
- Safety is a property of system that will not endanger human life or the environment. This definition of the safety is true, but it says nothing about measurable level of the safety. For this reason it is also used following definition:
- Safety is the probability that a system will have no non-detected errors on its outputs. The second one is a case where the safety is described as a dependability parameter; the first one is a case where the safety is described as a property of a system.
- This term dependability covers considerations of reliability, availability, safety, maintainability and others issues of importance in critical systems. Dependability is a property of a system that justifies placing one's reliance on it.
- A fault is a defect within the system.
- An error is a deviation from the correct value detected in the system or subsystem.
- A system failure occurs when the system fails to perform its required function. The required function of the system is specified in its technical specification.
- A hazard is a situation which is actual or potential danger to people or to the environment.
- A fault-tolerant system is able to perform the required function with the defined number of faults occurred within the system.
- A safety-critical system is one for which the safety of equipment or of a plant is assured.