A systematic approach to the description of fault-tolerant systems

Jakub Lojda, xlojda00@stud.fit.vutbr.cz
Zdeněk Kotásek, kotasek@fit.vutbr.cz

October 10, 2015

Raising the level of integration on chip significantly increases the risk of failure. Moreover, the pressure on reliability is also increasing. This leads to implementing digital circuits with the requirement to be fault-tolerant. *FPGA* (Field Programmable Gate Array) integrated circuits are often used for this purpose.

Fault-tolerant system is a system, that has the capability to perform its function even in the presence of faults or errors. Fault is a phenomenon of losing the capability to perform its function. Generally, we distinguish three types of faults: permanent, transient and intermittent faults. Permanent faults usually can not be fixed. In such case, the affected unit is moved into the dedicated backup section of the FPGA. Transient faults are appearing and disappearing unexpectedly during the use of the circuit. These faults are mainly caused by external influences, for example cosmic radiation. This type of fault may also result in permanent fault. The solution is to reconfigure the affected area of FPGA. Intermittent faults are caused by aging of the circuit and degradation of properties. The concept of error is used in the sense of dissimilarity of measured value and proper value. A particular error is a result of failure, but there are failures, that do not cause an error. The fundamental specific principles of fault-tolerant systems are for example *NMR* (N-modular Redundancy), *DwC* (Duplication with Comparison) etc. Each of these principles consists in the transformation of a part of the circuit. For different parts of the circuit, different principles of fault-tolerance may be suitable.

This complexity of digital systems design is further enhanced by increasing the level of integration. From this point of view, it would be interesting to have a tool, that would somehow automate the process of fault-tolerant systems design, based on the digital system description, e.g. in VHDL, that is not fault-tolerant. The tool would automatically, possibly with the assistance of a circuit designer, put proper kind of fault-tolerance in the right place in the circuit. The output of such tool would be the description of digital circuit also in VHDL, however fault-tolerant. For development of such tool, there is need to have some formal base. The intention of this work is to formalize the description of a fault-tolerant digital circuit and its internal representation. Then each fault-tolerant digital system design phase, especially algorithms used for transformation of internal representation of digital circuit into its fault-tolerant version.

Based on

[1] Martin Straka: *Methodology of highly reliable systems design*, PhD thesis, Brno, FIT BUT, 2013