# Model of Modular Secured Designs for Calculations of Availability

Martin Kohlík, Hana Kubátová
*Dept. of Digital Design*
*Czech Technical University in Prague*
*Prague, Czech Republic*
*{kohlimar; hana.kubatova}@fit.cvut.cz*

A method how to calculate the steady-state availability of designs composed of two cooperating secured modules is proposed. Our main goal is to create a dependability model that is able to be used to describe designs containing cooperating secured reconfigurable modules.

An FPGA platform is considered, Single Event Upsets (SEUs) [5] are the sources of the transient faults and the reconfiguration of the FPGA is used as the recovery tool. However, the proposed model is not limited, so any source of transient faults and any recovery tool can be used.

The railway station safety devices application implemented by means of FPGAs is developed in our department [4]. Railway station safety devices are composed of cooperating FSM modules designed as a self-checking circuits based on Modified Duplex System (MDS) architecture principles [1] and [2].

The MDS architecture is similar to basic Duplex, but output code checkers are added. The probability, that these checkers detect faults in the corresponding block, mainly depends on the used detection code. Two comparators of output values form the backup fault detection mechanism. A block containing fault cannot be identified in the case of different output and the whole structure has to be reconfigured.

A basic design composed of two cooperating modules without MDS and parity checking is shown in Figure 1. Both modules and all communication channels can be affected by SEUs. The final design is obtained by adding output code checkers, adding parity checkers to both communication lines, duplicating the design, adding comparators to compare the outputs of the duplicated modules and by adding a reconfiguration unit.

The resulting design is shown in Figure 2. Blocks *a1* and *a2* are identical copies of the module *a* from the basic design and can be reconfigured independently. Blocks *A1* and *A2* contain comparators of outputs of functional blocks (*a1*/*a2*) and blocks to check the parity on received data from blocks *B1*/*B2*. Blocks *A1* and *A2* can be reconfigured independently and the reconfiguration of these blocks also causes the reconfiguration of the corresponding nested functional blocks. Blocks *b/B* have a similar function as the corresponding *a/A* blocks. The reconfiguration unit collects *Ok/Fail* signals from all checkers and comparators. These signals cause reconfiguration of the corresponding target area as shown in Table 1.

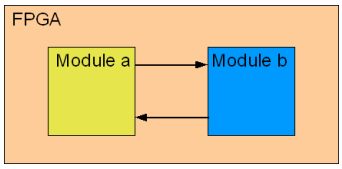


**Figure 1. The block diagram of the basic design**

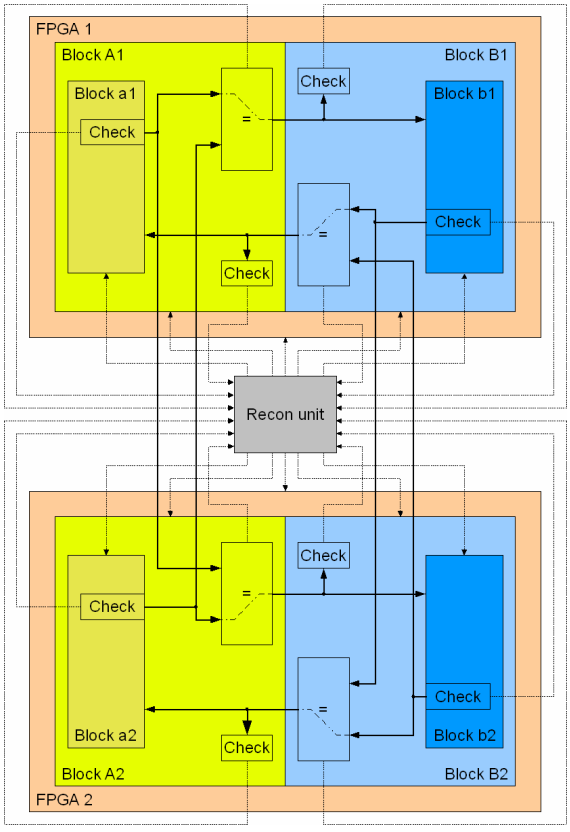


**Figure 2. The block diagram of the secured design**

**Table 1. Reconfiguration initiators and targets**

| Initiator | | Reconfigured area |
|---|---|---|
| *Name* | *Notation* | |
| Code checker in *a1* | Check | Block *a1* |
| Output comparators (*a1*-*a2*) (2x) | = | Blocks *A1* and *A2* |
| Parity check on data from *B1* | Check | Blocks *A1* and *B1* (*FPGA 1*) |
| Code checker in *b1* | Check | Block *b1* |
| Output comparators (*b1*-*b2*) (2x) | = | Blocks *B1* and *B2* |
| Parity check on data from *A1* | Check | Blocks *A1* and *B1* (*FPGA 1*) |
| Code checker in *a2* | Check | Block *a2* |
| Parity check on data from *B2* | Check | Blocks *A2* and *B2* (*FPGA 2*) |
| Code checker in *b2* | Check | Block *b2* |
| Parity check on data from *A2* | Check | Blocks *A2* and *B2* (*FPGA 2*) |

The proposed Markov chain used to calculate the steady-state availability of the described design is shown in Figure 3. The Markov chain contains a default state *Ok* representing the operational state of the design. Twelve states around the *Ok* state represent the reconfiguration of blocks as listed in Table 1 using the same colour notation. Transition rates and their description are shown in three cases only. Other rates can be calculated similarly.

Transitions leading from the *OK* state to the other states represent the detection of the fault in the corresponding block. Their rate depends on the rate of SEUs (λ) and the size of the configuration memory (s) that is used to create the function of the block. The rate of the transition to state *a1* also depends on the probability of detecting faults by the output code checker in block *a1* (the FS property of the block [3]). Faults undetected by the output code checker are detected by the comparator and the rate of transition to *"="* state depends on the (1-FS) value.

Block *A1* can be divided into two pseudo-parts. These pseudo-parts cannot be reconfigured independently. The first pseudo-part *"A1="* contains all logic and interconnection that is responsible for the comparison of the outputs. The second pseudo-part *"A1Ch"* is responsible for receiving and checking data from block *B1*. The sizes of these pseudo-parts are used in the fault rate calculations.

Transitions leading to the *Ok* state represent the reconfiguration of the damaged block. Their rate depends on the bit recovery rate (μ) and the size of the configuration memory (s) that is used in the block. The reconfiguration in FPGA 1 and FPGA 2 can be done concurrently.

If the example design is extended by an additional module *c* and new communication lines, the proposed model can be adapted easily. New states representing new output code checkers, output comparators and received data checkers are just added. Transition rates can be calculated similarly as in the case of the first module.

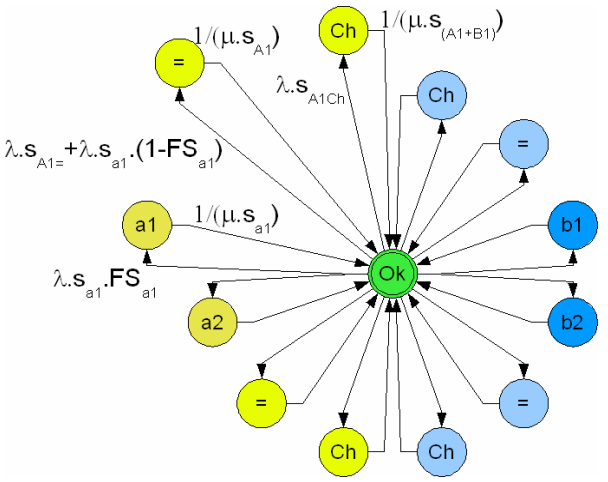


**Figure 3. Proposed Markov chain**

If the architecture of the module is changed, the corresponding fault states are replaced by the new ones matching the new architecture.

The proposed model can be adapted according to the different architectures of the modules. Moreover, more modules with communication interconnections can be added easily by adding more fault states and the corresponding transitions. The model was constructed with respect to the specific properties of FPGAs, but it can be used in other cases as well.

## Acknowledgment

This research has been partially supported by MSMT under research program MSM6840770014, GA102/09/1668 and SGS10/118/OHK3/1T/18.

## References

[1] P. Kubalík, R. Dobiáš and H. Kubátová, "Dependable Design for FPGA based on Duplex System and Reconfiguration", In Proc. of 9th Euromicro Conference on Digital System Design, Los Alamitos: IEEE Computer Society, 2006, pp. 139-145.

[2] P. Kubalík and H. Kubátová, "Dependable design technique for system-on-chip", Journal of Systems Architecture. 2008, vol. 2008, no. 54, pp. 452-464. ISSN 1383-7621.

[3] L. Kafka, P. Kubalík, H. Kubátová and O. Novák, "Fault Classification for Self-checking Circuits Implemented in FPGA", Proc. of IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop, Sopron University of Western Hungary, 2005, pp. 228-231.

[4] J. Borecký, P. Kubalík and H. Kubátová, "Reliable Railway Station System based on Regular Structure implemented in FPGA", Proc. of 12th EUROMICRO Conference on Digital System Design, Los Alamitos: IEEE Computer Society, 2009, pp. 348-354.

[5] F. L. Kastensmidt, L. Carro and R. Reis, Fault-Tolerance Techniques for SRAM-based FPGAs, chap. 2., Springer, the Netherlands, 2006.