Reconfiguration Strategy for FPGA Dependability Characteristics Improvement based on Stochastic Petri Net

Martin Kohlík, Hana Kubátová

Department of Computer Science and Engineering,
Faculty of Electrical Engineering
Czech Technical University in Prague
(e-mail: kohlim1@fel.cvut.cz; kubatova@fel.cvut.cz)

Abstract: This paper shows the impact of the trade-off between reconfigurable and non-reconfigurable parts of the FPGA to the dependability characteristics of the whole design. Stochastic Petri nets have been used to compute reliability and dependability characteristics in a simple FPGA design with dynamically reconfigurable modules. Some parts of the design are not possible or proper to reconfigure dynamically (e.g. module interconnections, module-pin connections …). A non-reconfigurable overhead may have a significant effect to the availability of the design. The granularity of reconfigurable parts and their number can also affect dependability parameters. The method how to enumerate these effects via a formal dependability model is shown in this paper.

Keywords: FPGA, dynamic reconfiguration, Stochastic Petri net, formal availability model

1. INTRODUCTION

FPGA-based designs are sensitive to many effects that can change their programmed function. (Kastensmidt, 2006) These changes are most unwelcome when the designs are used in safety-critical applications, where the material loss or mortality can be caused because of their failure. The improvement of the reliability of the design is required to minimize the impact of such effects.

FPGA-based designs can be adapted to use the reconfiguration ability of the FPGA to recover the original bitstream. The recovering of the original bitstream removes effects of transient faults. The partial reconfiguration is able to recover the original bitstream in part of the FPGA. The dynamic partial reconfiguration is able to do the partial reconfiguration while the rest of the FPGA is operational. The time required for dynamic reconfiguration depends on the size of the reconfigured part. Reconfiguration of the small part of the FPGA can decrease the reconfiguration time significantly.

Some parts of the design are not possible or proper to reconfigure dynamically. These parts – a nonreconfigurable overhead – must be reconfigured along with the whole FPGA. Reconfiguration of the whole FPGA is much slower and decreases the availability parameter of the design.

The definition of the availability (Hlavička, 1989):

$$A_{ss} = \frac{t_{uptime}}{t_{uptime} + t_{downtime}}$$

Time t_{uptime} corresponds to the expected value of the uptime of the system and $t_{downtime}$ corresponds to the expected value of the downtime of the system.

Markov models are the common way to calculate availability parameters. Markov models are simple to create and they allow calculations of the availability of the design by solving a system of linear equations.

Stochastic Petri nets (SPNs) can be created as easy as Markov models and allow the same calculations. Moreover, SPNs are not only a dependability model, they are able to represent the structure of the design. Mathematical properties, that are available for Petri Nets, can be used to analyze SPNs.

The paper is structured as follows: A short introduction to Stochastic Petri Nets and basic types of FPGA faults and errors are in Section 2. Section 3 contains a proposed model and conditions that are necessary to its creation. Calculations, parameter settings and results are in section 4. Section 5 concludes the paper.

2. BACKGROUND

2.1 Stochastic Petri nets and their extensions

Stochastic Petri net (Bause, 2002) is formed from Place-Transition net by adding the transition rate of the transition t_i. It means that the firing time is exponentially distributed and the distribution of the random variable i of the firing time of transition t_i is given by

$$F(x) = 1 - e^{-\lambda_i x}$$

The average time for t_i to fire is $\frac{1}{\lambda_i}$.

A simple example of SPN is illustrated in Fig. 1. This SPN contains two places (*P0* and *P1*) and two transitions with an exponentially distributed firing time (*T0* and *T1*). When transition *T0* is fired, using the firing rule of Place-Transition nets, the token is moved from place *P0* to *P1*.

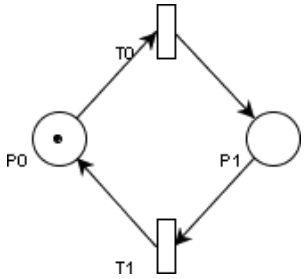

Fig. 1: A simple SPN example

Generalized Stochastic Petri nets (GSPNs) (Bause, 2002) have two different classes of transitions: immediate transitions and timed transitions. Once enabled, immediate transitions fire in zero time. Timed transitions fire after a random, exponentially distributed enabling time as in the case of SPNs.

Fig. 2 shows an example of GSPN. Transition *T4* is an immediate transition. The other transitions are exponentially distributed. The arc heading from transition *T5* to place *P0* has weight set to 2 to ensure liveness of GSPN.

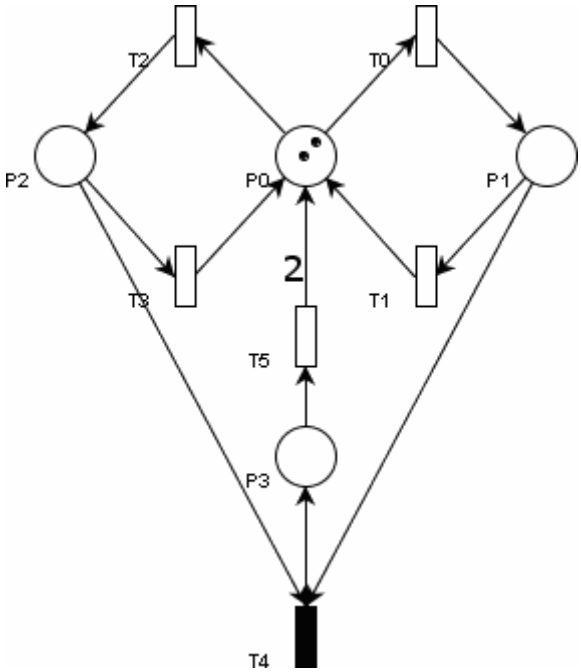

Fig. 2: A GSPN example with one immediate transition

Mathematical properties, that are available for Petri Net, can be used to analyze both SPN and GSPN as well. All proposed models are live, bounded and reversible. (Murata, 1989)

- Boundeness: If the model is not bounded, then the set of reachable markings is infinite. The probability of any marking from this reachability set will approach 0.
- Reversibility: All proposed models suppose non-destructive actions that can be undone. Undoing the actions will lead the model to its original state.
- Liveness: Every transition in proposed models represents a certain action. The transaction, that cannot be fired, represents an impossible action. An impossible action does not need to be modeled. This fact along with the reversibility property implies the liveness property.

2.2 FPGA in-operation faults and errors

The function of the FPGA may be changed during the operation due to many reasons (Novák, 1998; Kastensmidt, 2006). Some of them are listed below:

- Aging
- Stress (voltage, heat …)
- High-energy particle impact

The effect of the impact of high-energy particle can be divided into the following groups:

- Destructive (Single Event Burnout …)
- Non-destructive (Single Event Upset …)

In this paper will be only non-destructive Single Event Upsets (SEUs) taken into account. The SEU can change the configuration information – FPGA bitstream. This negative effect of the SEU can be removed by the reconfiguration of the FPGA. During the process of reconfiguration, the original bitstream is restored. Some types of FPGA are able to reconfigure its content dynamically. This feature allows the partial reconfiguration of the FPGA while the rest of the FPGA is operational. The reconfiguration of the whole FPGA is required when the dynamic reconfiguration cannot be used.

3. DEPENDABILITY ANALYSIS

3.1 Conditions for model computations

Conditions for all formal models mentioned in this paper will be defined as follows (Kubalík, 2008):

- Only a “single fault” may appear:
  - It will occur at a single time instant that is arbitrarily located at the time axis
  - The fault can destroy a data item located within the configuration memory of the FPGA. The assumed “width” of the fault is one bit in a configuration

memory. Every bit of the bitstream memory of the FPGA can be attacked with the same probability.

- The time distance between any two successive faults is large enough to recover the system from the first one (otherwise it is a multiple fault).

- The design is defined as follows:
  - The design contents a dynamically reconfigurable module and an overhead part that cannot be reconfigured dynamically.
  - The size of the configuration data of a dynamically reconfigurable module is set to 20% of the size of the configuration data of the FPGA AT94K40 ATMEL FPSLIC.
  - The size of the configuration data of an overhead part is relative to the size of a dynamically reconfigurable module S_r. This relative size $p_{non\_rec/rec}$ varies from 0% to 100% of the size S_r.
  - The module can be divided into n (e.g. 2 or 3) fractions with identical configuration data size or can be left undivided ($n = 1$).
  - Each fraction is able to detect the SEU that impacted it on. An overhead part has the same ability.
  - The reconfiguration unit loads a correct configuration data after the fault is detected. The time needed to reconfigure a faulty part depends on the configuration data size of the part. The reconfiguration unit is able to reconfigure each fraction of the module independently.
  - SEUs impacting an unused logic do not change the function of the used part. This type of impact is not considered in calculations.

Fig. 3 shows the schematic model of the design. The design with the relative size $p_{non\_rec/rec}$ set to 0.1% is located in the left part of the figure. The design with the relative size $p_{non\_rec/rec}$ set to 100% is located in the right part of the figure. Possible fractions of the reconfigurable module are represented by green lines.

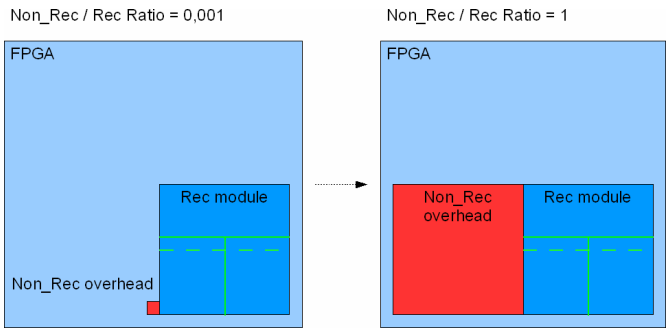

Fig. 3: The schematic model of the design with two possibilities of the relative size $p_{non\_rec/rec}$

3.2 GSPN model

A proposed GSPN model with a dynamically reconfigurable module undivided is illustrated in Fig. 4.

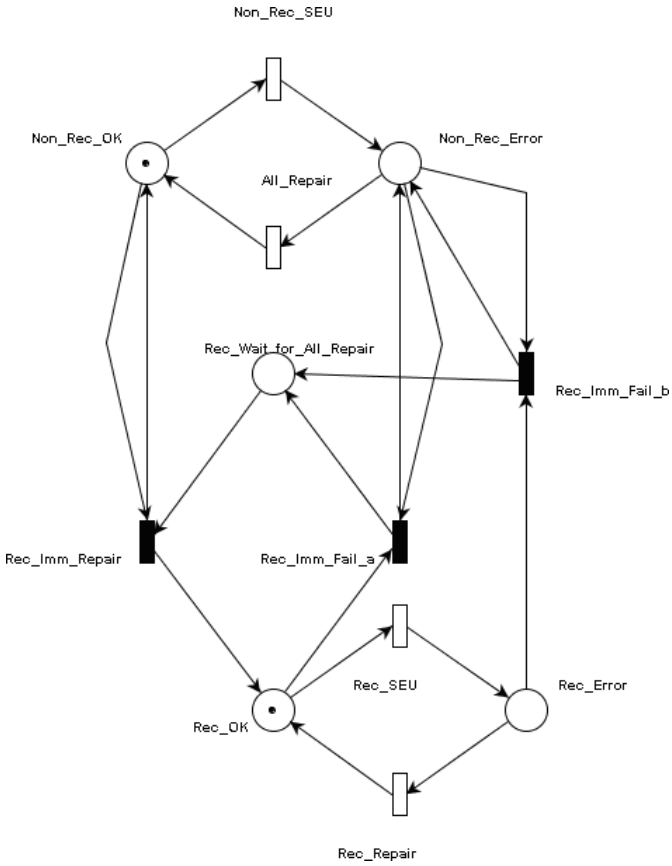

Fig. 4: A proposed GSPN model with a dynamically reconfigurable module undivided

The model for an overhead part, that cannot be reconfigured dynamically, is located in the upper part of the figure. SEU impact into the overhead part of the design is represented by *Non_Rec_SEU* transition. Firing this transition moves the token from *Non_Rec_OK* place to *Non_Rec_Error* place. *All_Repair* transition is enabled in a new marking. Firing this transition matches the end of reconfiguration of the FPGA and moves the token from *Non_Rec_Error* place back to *Non_Rec_OK* place.

The model of a dynamically reconfigurable module is located in the lower part of the figure. The meaning of places and transitions is very similar to the model for an overhead part. *Rec_Repair* transition corresponds to the dynamic reconfiguration of the module in this case.

Two immediate transitions *(Rec_Imm_Fail_a* and *_b)* located in the middle of the figure are purposed for removing the token from the lower part when the reconfiguration of the whole FPGA is running (the token is located in *Non_Rec_Error* place). There is no need to calculate a SEU probability or the reconfiguration of a dynamically reconfigurable module during the reconfiguration of the whole FPGA. A third immediate *Rec_Imm_Repair* transition

is purposed to return the token to the lower part after the reconfiguration of the whole FPGA has been finished (the token has been returned to *Non_Rec_OK* place).

Fig. 5 shows a proposed GSPN model with a dynamically reconfigurable module divided into 2 fractions.

This model is similar to that one shown in Fig. 4. The model of the second fraction of a dynamically reconfigurable module is located in the right part of the figure. It contents same places and transitions with same functions. The arc leading from *Rec_Wait_for_All_Repair* place to *Rec_Imm_Repair* transition has increased weight to ensure boundeness of the model.

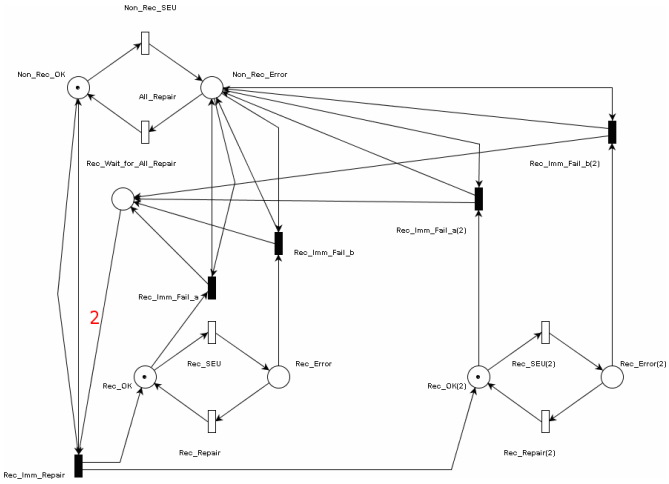

Fig. 5: A proposed GSPN model with a dynamically reconfigurable module divided into 2 fractions

A similar method is used to extend the GSPN to create the model for 3 and more fractions.

Fig. 6 contains the GSPN for the system with the same module without any dynamic reconfiguration. The whole FPGA must be reconfigured after any SEU impact in this case. The availability of the system with this configuration is required for comparison.

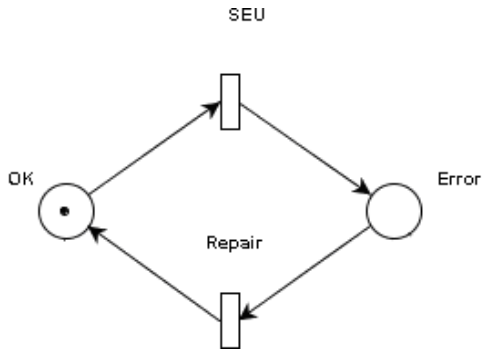

Fig. 6: A proposed GSPN model for the system without any dynamic reconfiguration

4. CALCULATIONS

4.1 Parameter settings

There are two major classes of transition rates in proposed models:

- SEU: This rate is directly proportional to the size of configuration data and the rate of a particle impact.
- Repair: This rate is inversely proportional to the size of configuration data and the period of the configuration unit's clock signal.

The rate of a particle impact is set to value:

$$\lambda = 2 \times 10^{-5} \left[hour^{-1} \right]$$

This value is taken from (Normand, 1996; Kubalík, 2008).

The size of the configuration data of the FPGA is set to the size of the configuration data of AT94K40 ATMEL FPSLIC (Atmel, 2008):

$$s = 233\ 194 \left[byte \right]$$

The size of the configuration data of a dynamically reconfigurable module is set to 20% of the size of the FPGA:

$$S_r = 93\ 277 \left[byte \right]$$

The period of the clock signal of the configuration unit:

$$t = 40 \left[ns \right]$$

4.2 Results

Availability A_{ss} results calculated from proposed models are listed in Table 1.

Table 1. Availability results

	A_{ss}		
$p_{non\ rec/rec}$	n = 1	n = 2	n = 3
0	0.999999130	0.999999565	0.999999710
0.001	0.999999126	0.999999561	0.999999706
0.002	0.999999121	0.999999556	0.999999701
0.005	0.999999108	0.999999543	0.999999688
0.01	0.999999087	0.999999522	0.999999667
0.02	0.999999043	0.999999478	0.999999623
0.05	0.999998913	0.999999348	0.999999493
0.1	0.999998695	0.999999130	0.999999275
0.2	0.999998260	0.999998695	0.999998840
0.5	0.999996955	0.999997390	0.999997535
1	0.999994780	0.999995215	0.999995360

The availability of the system with the same module without any dynamic reconfiguration:

$$A_{ss\_Static} = 0.999995650$$

The plot of availability results is shown in Fig. 7.

The red line "Static" represents the system without any dynamic reconfiguration. It is used to compare this system with the system with a dynamically reconfigurable module. The availability of the system with a dynamically reconfigurable module is increased significantly in comparison to the "Static" system until the relative size of an overhead part does not get over 80% of the size of a dynamically reconfigurable module. The design representing a real problem is required to narrow the area of interest. It is possible, that some design will have small overhead and will derive advantage from dynamic reconfiguration. The other design will have a big overhead part and its advantage from dynamic reconfiguration will be small or none.

It is obvious that dividing a dynamically reconfigurable module into fractions increases the availability of the system. This increase is not as high as the one that has been mentioned in the previous paragraph. The increment of the availability is lost when division of a reconfigurable module into two fractions costs more then 10% additional overhead. The difference between dividing into 2 and 3 fractions is even smaller (ca. 3.5%). It is supposed that dividing a reconfigurable module into more parts will increase availability even less.

5. CONCLUSIONS

The reconfiguration strategy for the FPGA has been studied. The trade-off between reconfigurable and non-reconfigurable parts was modeled by stochastic Petri net with respect to dependability parameters.

Two major facts are observable from results:

- The dynamic reconfiguration can increase the availability of the system significantly. The relative size of an overhead part is limited to ca. 80 – 95 % of the size of a reconfigurable module to preserve the advantage of a dynamic reconfiguration.
- The division of a reconfigurable module has little effect to the availability of the system in comparison with the first conclusion. The increment of the availability is lost when division of a reconfigurable module into two fractions costs more then 10% additional overhead. The difference between dividing into 2 and 3 fractions is even smaller (ca. 3.5%).

ACKOWLEDGEMENT

This research has been supported by MSMT under research program MSM6840770014.

REFERENCES

Atmel Corporation (2008). *ATMEL FPSLIC Datasheet.*

Bause, F., Kritzinger, P. (2002). *Stochastic Petri Nets -- An Introduction to the Theory (2nd edition).* Vieweg Verlag, Germany.

Hlavička, J. (1989). *Spolehlivost a diagnostika (Dependability and diagnostics)*, chap. 12.3. Ediční středisko ČVUT (CTU in Prague), Czech Republic (in Czech).

Kastensmidt, F. L., Carro, L., Reis, R. (2006). *Fault-Tolerance Techniques for SRAM-based FPGAs,* chap. 2. Springer, the Netherlands.

Kubalík, P., Kubátová, H. (2008). Dependable Design Technique for System-on-Chip. *Journal of Systems Architecture*, vol. 54, pp 452-464.

Murata, T. (1989). Petri Nets: Properties, Analysis and Applications. *Proceedings of the IEEE,* vol. 77 (No 4), pp. 541-580.

Normand, E. (1996). Single Event Upset at Ground Level. *IEEE Transactions on Nuclear Science*, vol. 43, pp. 2742-2750.

Novák, O. (2008). *Úvod do diagnostiky, základní pojmy (An Introduction to diagnostics, basic concepts).* (the lecture of 36DSP course – CTU in Prague – in Czech).

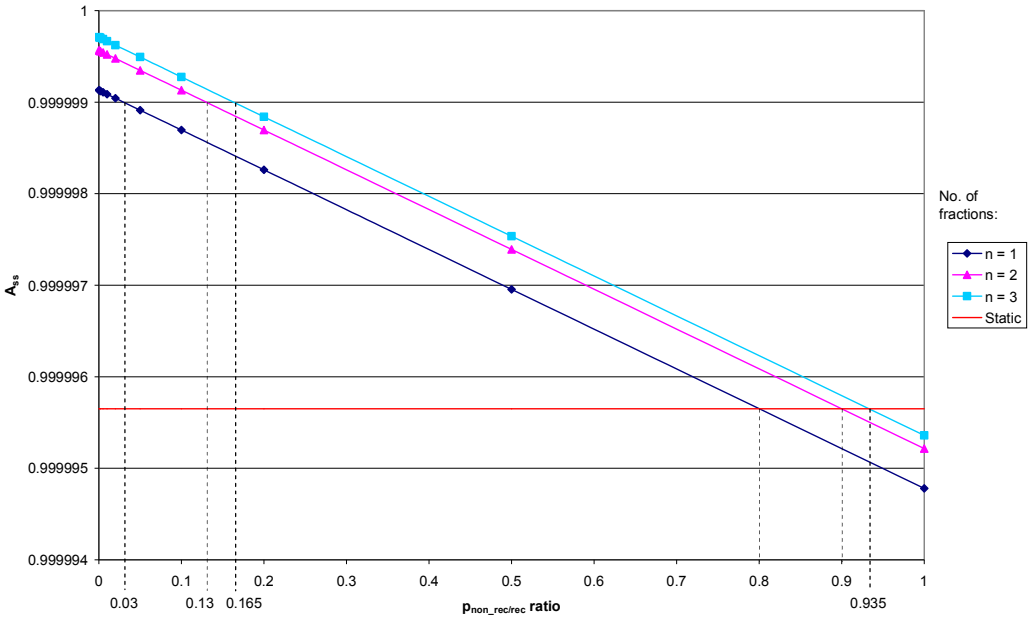

Fig. 7: Availability results for three possibilities of fractioning of a dynamically reconfigurable module and for the system without any dynamic reconfiguration