METODOLOGIE NÁVRHU OBVODŮ SE ZVÝŠENOU SPOLEHLIVOSTÍ ZALOŽENÝCH NA FPGA

Martin Straka
Informační technologie, 3. ročník, prezenční studium
Školitel: Doc. Ing. Zdeněk Kotásek, CSc.

Fakulta informačních technologií, Vysoké učení technické v Brně
Božetěchova 2, Brno 612 66

strakam@fit.vutbr.cz

Abstrakt. Příspěvek charakterizuje motivaci, cíle a dosavadní výsledky studenta při řešení jeho disertační práce. Jako první jsou popsány mezní etapy v návrhu metodologie pro konstrukci odolných architektur s různou úrovní diagnostiky založených na obvodech FPGA. Dále je popsáno, jak lze zlepšit spolehlivostní parametry u architektur odolných proti poruchám doplněných o hlídací obvody oproti systému TMR a duplex. Pro určení spolehlivosti jsou využity Markovské spolehlivostní modely. Srovnání všech sledovaných parametrů pro odolné architektury je diskutováno. V závěru je popsán další směr výzkumu a jsou shrnuty cíle disertační práce.

Klíčová slova. systém odolný proti poruchám, spolehlivost, hlídací obvod, architektura, spolehlivostní model, TMR, duplex, FPGA, VHDL.

1 Úvod

Nové možnosti při návrhu číslicových systémů s vysokou spolehlivostí nabízí přístupy založené na obvodech FPGA [1]. Hlavní výhodou těchto přístupu je snadná implementace cílového systému v jazyce pro popis číslicových systémů (HDL), jeho simulace a následná syntéza právě do obvodu FPGA [2]. Další výhodou současných obvodů FPGA je možnost využít částečné dynamické rekonfigurace, jež vnáší do návrhu číslicových systémů nové možnosti a vylepšení v oblasti spolehlivosti a diagnostiky [3]. Často se vedle bezpečnostní kódů a zálohovacích technik uplatňují pro zvýšení spolehlivosti techniky založené na replikaci funkčních jednotek, jako jsou architektury tří-modulové redundance (TMR) nebo duplex [4]. Tyto architektury se také uplatňují při konstrukci systémů odolných proti poruchám [5]. V zhledem k velkému množství diagnostických technik lze uplatnit metodické postupy, které by ze známých odolných architektur (zejména pak TMR a duplex) vytvářely složitější a lépe diagnosticky vybavené architektury s vyšší spolehlivostí. Tyto architektury by tak našli uplatnění v systémech, kde je potřeba zaručit nejdelší možnou životnost systému a vysokou spolehlivost.

Zajímavou diagnostickou metodu popisují autoři v [6]. Metoda je založena na duplexním režimu využívající dvě hradlová pole FPGA. První část jejich přístupu srovnává primární výstupy obou FPGA, druhá detekuje a označí vadný FPGA. Oba systémy využívají technik samočinné kontroly a zabezpečení s využitím parity. Pro každý systém autoři sestrojili Markovský spolehlivostní model reflektující jednotlivé spolehlivostní parametry metody. Další články se zabývají diagnostikou propojovací sítě v FPGA a detekcí poruch funkčních částí číslicového obvodu v FPGA [7].

2 Motivace a definice problému

Cílem výzkumu je navrhnout kompletní metodologii pro tvorbu systémů se zvýšenou spolehlivostí využívající techniky odolnosti proti poruchám na bázi obvodů FPGA. Existuje několik přístupů, jak zvyšovat odolnost systému proti poruchám. Doposud se výzkum zabýval mimo jiné i konstrukcí hlídacích obvodů pro komunikační protokoly a jednoduché číslicové obvody na úrovni RT, které byly začleněny do známých architektur TMR či duplex a tím přispěly k jejich vyšší spolehlivosti [8]. Ovšem existují obvody, pro které není možné hlídací obvody vytvořit, nebo složitost a velikost hlídače značně převyšuje parametry hlídaného obvodu. Proto je třeba najít vhodné diagnostické postupy či metodiku, jak pro takové obvody provést kontrolu jejich správné funkce a tyto postupy různě kombinovat podle zadaných kritérií. Lze tedy využít třeba diagnostiku na pozadí, což může být sada testovacích vektorů nasazená na obvod v určitých okamžicích, softwarové řešení, speciální bezpečnostní architektury nebo bezpečnostní kódy. Zde se tedy otvírá prostor pro navrhnutí a implementaci metodiky, která by podle vhodných kritérií vytvářela různé typy architektur s různou úrovní diagnostiky (typem kontroly) s využitím principů odolnosti proti poruchám. Tyto architektury by pak byly zasazeny do implementace výsledného systému a realizovány na platformě FPGA.

3 Metodika pro tvorbu FT architektur s různou úrovní diagnostiky

Metodika by našla uplatnění třeba v situaci, kdy návrhář nebo uživatel přijde s požadavkem na vytvoření číslicového systému, který musí splňovat určitá kritéria, jako je celková jeho spolehlivost, odolnost proti poruchám, míra zabezpečení, kterou je nutno dodržet. Požaduje, aby systém, který bude implementován v obvodu FPGA splňoval požadovanou dostupnost, plnil svoji funkci i při výskytu poruchy a jeho spolehlivost neklesla pod stanovený práh. Výsledkem metodiky by bylo vygenerování příslušné posloupnosti architektur s různou úrovní diagnostiky respektující tyto požadavky.

3.1 Spolehlivost a dostupnost systému

Pojmem dostupnost systému rozumíme dobu, po kterou systém dokáže vykonávat svojí funkci a produkuje správné výsledky i při výskytu poruchy. Snahou je, aby tato doba byla co nejdelší i s ohledem na omezenost prostoru v FPGA. Lze toho dosáhnou vhodnou volbou konfigurací systému, při kterém z počáteční architektury postupně ubíráme diagnostické prvky a přecházíme do jiné architektury, která zajišťuje plnou funkčnost systému, disponuje jinou diagnostikou, neporušuje podmínky pro odolnost proti poruchám a nespadá svoji spolehlivostí pod stanovené minimum.

3.2 Vstupy a výstupy metodiky

Navrhovaná metodika se bude opírat o formální model testovatelného obvodu, který vznikl na FIT VUT v Brně. Tento formální model bude rozšířen o další definice a množiny reprezentující mimo jiné také diagnostické zabezpečení, míru spolehlivosti, a další mezní parametry. Hlavním vstupem metodiky bude soubor několika parametrů a zdrojových kódů:

- Strukturální popis obvodu (top_level.vhd)
- Behaviorální popis komponent (komponenta.vhd)
- Předepsaná spolehlivost (dostupnost v %)
- Typ FPGA (velikost ve slices, rychlost, počet FPGA)
- Velikost obvodu (slices)

Hlavními výstupy metodiky budou reporty typu:

- Doporučené diagnostické prostředky pro obvod
- Posloupnosti FT architektur s různou diagnostikou

a. Informace o spolehlivosti
b. Odhad velikosti jednotlivých architektur
c. Využití částečné dynamické rekonfigurace pro diagnostiku

- Spolehlivostní parametry pro FT architektury

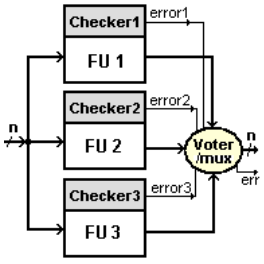
4 Vysoce odolné FT architektury s kontrolními obvody

Mezi nejpoužívanější odolné systémy patří systémy více-modulové redundance a také systémy založené na duplexním provedení. Klasický systém TMR skládající se ze 3 stejných modulů umožňuje systému jako celku podávat správné hodnoty v případě poruchy jednoho modulu a to na základě rozhodnutí hlasovacího obvodu, jež je součástí systému. Hlasovací obvod realizuje majoritní funkci a vyhodnocuje hodnoty na všech třech svých vstupech. Nevýhodou tohoto přístupu je, že při poruše jednoho modulu pravděpodobnost bezporuchového provozu R(t) TMR prudce klesá, a tedy od jistého okamžiku je R(t) TMR nižší, než R(t) samostatného modulu. Tím i střední doba bezporuchového provozu poměrně klesá, což snižuje celkovou dostupnost systému. Při poruše dalšího modulu se systém TMR stává nefunkčním. Dalším nedostatkem TMR je možný problém lokalizace poruchy, jedná-li se o systém implementovaný v obvodu FPGA.

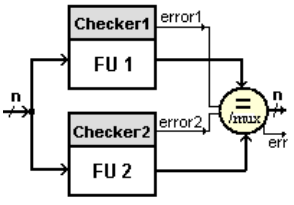
Tyto skutečnosti by se daly ovšem minimalizovat nebo odstranit doplněním klasické TMR architektury o další zabezpečující a lokalizační prvky, jako jsou kontrolní součty, bezpečnostní kódy nebo techniky využívající on-line diagnostiku. Jednou z možností, jak zlepšit vlastnosti architektur TMR, je využít kontrolních obvodů, jež kromě detekce poruchy mají schopnost lokalizovat poruchu v hlídaném modulu a vyvolat tak akce k případné rekonfiguraci poškozeného modulu.

4.1 Architektura TMR3CH a Duplex2CH

Vylepšená architektura TMR, která je doplněná o hlídací obvod každého modulu a speciální úpravou architektury rozhodovacího členu, přináší lepší diagnostiku a životnost celého systému. Doplnění o hlídače přináší nejen přesnější detekci a lokalizaci poruchy ale taky zvyšuje dostupnost a spolehlivost systémů, který propouští správné výsledky i v případě poruchy dvou modulů součastně, což u klasického propojení TMR nebylo možné. Propojení architektury TMR3CH s hlídači je vidět na obrázku 1. Funkce rozhodovacího obvodu byla doplněna o vstupy z jednotlivých hlídačů, které signalizují poruchu příslušného modulu. Pokud pracují všechny tři moduly správně nebo jeden z nich vykazuje poruchu, plní rozhodovací člen funkci majority jak u klasického TMR. Jakmile se vyskytne současně porucha na dalším modul, majoritní funkce je potlačena a na výstup se propouští správné hodnoty pouze z modulu, jehož hlídač nehlásí poruchu.



Obrázek 1: Architektura TMR3CH.



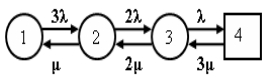
Obrázek 2: Architektura Duplex2CH.

Další architekturou je duplexní provedení funkčních modulů osazených hlídači a vylepšenou konstrukcí porovnávacího prvku. Blokové schéma systému je zobrazeno na obrázku 2. Schéma jsme označili jako duplex2CH. Tato architektura je FT architekturou protože narozdíl od klasického provedení duplexního systému, který v případě poruchy se stává nefunkčním, může naše řešení

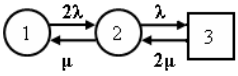
propouštět správné hodnoty na výstup v případě poruchy jednoho modulu. Vznikne-li porucha na jednom modulu, komparátor se chová jako multiplexor, který na základě informací poskytovaných hlídači propustí na výstup hodnoty funkčního modulu. V případě poruchy obou modulů se systém stává nefunkčním.

4.2 Spolehlivostní model a výsledky

Pro obě architektury byl sestaven jednoduchý Markovský model pro obnovitelný systém, který ovšem neuvažuje selhání hlídacího prvku. Model vychází z popisu vlastností architektur popsaných výše. Model pro architekturu TMR3CH je na obrázku 3, model pro Duplex2CH je na obrázku 4.



Obrázek 3: Spolehlivostní model pro TMR3CH.



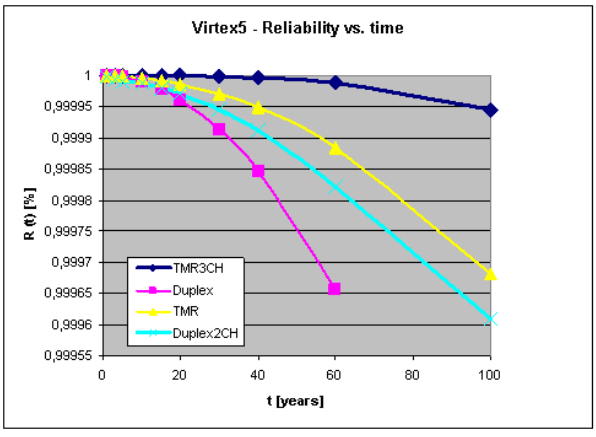
Obrázek 4: Spolehlivostní model pro Duplex2CH.

Posuzované spolehlivostní parametry byly pravděpodobnost bezporuchového stavu R(t), střední doba bezporuchového provozu (Ts) a celková dostupnost systému (Kp). Tabulka 1 ukazuje hodnoty spolehlivosti 5ti rozdílných architektur pro intenzitu poruchy (λ) stanovenou pro operační prostředí na povrchu země pro platformu SRAM FPGA Virtex5. Hodnota intenzity poruchy byla převzata z dokumentace XILINX [9] a článku [10], kde se uvádí průměrná hodnota intenzity poruchy pro tento typ FPGA $1{,}8\text{x}10^{-4}$ [h^{-1}]. Doba opravy jednoho modulu (μ) byla stanovena na 0,05 [h^{-1}]. První sloupec tabulky označuje typ architektury. Druhý sloupec definuje velikost architektury v počtu slices a procento využití z celkového počtu slices v FPGA. Třetí sloupec ukazuje hodnotu parametru dostupnosti a v posledním sloupci je příslušná střední doba bezporuchového provozu. Ze získaných hodnot je patrné, že námi navrhnuté architektury s hlídači a úpravami rozhodovacích prvků, TMR3CH a duplex2CH vylepšily spolehlivostní parametry o proti klasickému TMR a duplex. Na obrázku 5 je pak graf závislosti R(t) na čase pro jednotlivé architektury.

Tabulka 1: Spolehlivostní parametry architektur.

λ =1,8x10^{-4} [h^{-1}] μ =0,05 [h^{-1}]

FPGA Virtex5 Architecture for counter	Overhad [slices]	Kp [%]	Ts [years]
TMR3CH	**21 (2%)**	**0,9999999**	**16448**
TMR	9 (1%)	0,9999615	29
Duplex2CH	**16 (1%)**	**0,9999871**	**88,7**
Duplex	12 (1%)	0,9999123	7,1
Simple	5 (1%)	0,9964129	0,6



Obrázek 5: Graf závislosti R(t) na čase.

5 Závěr a další výzkum

V příspěvku byly prezentovány cíle a mezní výsledky práce studenta na tématu disertační práce. Byly provedeny experimenty s využitím hlídacích obvodů v architekturách FT a stanoveny příslušné

spolehlivostní parametry, které byly srovnány se systémy TMR a duplex. Dále byla nastíněna metodika, která umožní generovat posloupnosti FT architektur s různou úrovní diagnostiky. Další etapu plnění cílů disertační práce představuje navržení podrobného blokového schéma popisující kroky metodiky, rozšíření již zavedeného formálního modelu testovatelného obvodu o potřebné konstrukce a vlastní implementace jednotlivých kroků metodiky.

6 Cíle disertační práce

Cílem výzkumu je tedy navrhnout kompletní metodologii pro tvorbu systémů se zvýšenou spolehlivostí využívající techniky odolnosti proti poruchám na bázi obvodů FPGA. Práce by se měla opírat o možnosti využití různých diagnostických metod v různých architekturách odolných proti poruchám a tyto architektury vhodně modifikovat podle zadaných spolehlivostních parametrů. Dalším důležitým kritériem při tvorbě metodiky je zohlednění omezenosti zdrojů FPGA. Konkrétní výsledky by měly zahrnovat následující postupy a cíle:

1. Vytvořit formální prostředky pro popis vlastností, které musí kontrolovaný obvod splňovat a jejich transformace do obvodové realizace v jazyce VHDL.
2. Vytvořit obecný postup, který umožní reflektovat při návrhu kontrolního obvodu prioritní nebo vytipované funkce kontrolovaného obvodu a vytvářet hierarchicky funkční celky s různou (zadanou) úrovní kontroly správné funkce. Vytvořit postup, který umožní kvantifikovat objem kontrolovaných funkcí.
3. Pro účely popisu vlastností a hlídaných funkcí obvodu rozšířit již vytvořený definiční jazyk a metodiku pro generování hlídačů prezentovanou v kapitole 4. Porovnat obvody a jejich hlídače z hlediska objemů, které obvody představují v FPGA.
4. Pro účely implementace systému odolného proti poruchám do FPGA vytvářet metodiku pro generování sekvence dílčích architektur lišících se úrovní zabezpečení kontroly funkcí, zohlednit požadovanou dobu života systému. Výsledkem bude posloupnost architektur, každá z nich jinak diagnosticky vybavena tak, aby splňovala požadavky na spolehlivost. Tyto požadavky stanoví uživatel nebo návrhář. Pro každou architekturu a celý systém mít k dispozici spolehlivostní model. Celý postup a všechny kroky vhodně transformovat do ucelené metodiky.
5. Implementace a experimentální ověření navržených metodik.

Poděkování

Výzkum je podporován projekty financované Grantovou Agendou České Republiky pod číslem GD102/09/H042 – „Matematické a inženýrské metody pro vývoj spolehlivých a bezpečných paralelních a distribuovaných počítačových systémů“, dále GD102/09/1668 – „Zvyšování spolehlivost a provozuschopnosti v obvodech SoC„ a projektu č. MSM 0021630528 – „Výzkum informačních technologií z hlediska bezpečnosti“.

Literatura

[1] Bolchini, C., Miele, A., Santambrogio, M. D.: TMR and Partial Dynamic Reconfiguration to mitigate SEU faults in FPGAs. In: Proceedings of the 22nd IEEE international Symposium on Defect and Fault-Tolerance in VLSI, 2007, IEEE Computer Society, Rome, Italy, ss. 87-95

[2] Galke, C., Grabow, M., Vierhaus, H. T.: Perspectives of combining on-line and off-line test technology for dependable systems on a chip. In: Proceedings of the 9th IEEE International Symposium on On-Line Testing, 2003, Paris, France, ss. 183-188

[3] Sedcole, P., Blodget, B., Becker, T., Anderson, J., Lysaght, P.: Modular dynamic reconfiguration in Virtex FPGAs. In: IEEE Proceedings Computers and Digital Techniques, 2006, IEEE Computer Society, New York, USA, ss. 157–164

[4] D'Angelo, S., Metra, C., Pastore, S., Pogutz, A., Sechi, G. R.: Fault-Tolerant Voting Mechanism and Recovery Scheme for TMR FPGA-Based Systems. In: Proceedings of the 13th international Symposium on Defect and Fault-Tolerance in VLSI Systems, 1998, IEEE Computer Society, Cannes, France, ss. 233-240

[5] Frigerio, L., Salice, F.: RAM-based fault tolerant state machines for FPGAs. In: Proceedings of the 22nd IEEE international Symposium on Defect and Fault-Tolerance in VLSI Systems. 2007, IEEE Computer Society, Rome, Italy, ss. 312-320

[6] Kubalik, P., Dobias, R., Kubatova, H.: Dependable Design for FPGA Based on Duplex System and Reconfiguration. In: Proceedings of the 9th EUROMICRO Conference on Digital System Design, 2006, IEEE Computer Society, Dubrovnik, ss. 139-145

[7] Straka, M., Kotasek, Z. and Winter J.: Digital systems architectures based on on-line checkers. In DSD ’08: Proceedings of the 11th EUROMICRO Conference on Digital System Design. 2008, IEEE Computer Society, Parma, Italy, ss. 81–87

[8] Straka, M., Tobola, J., and Kotasek Z.: Checker design for on-line testing of XILINX FPGA communication protocols. In DFT ’07: Proceedings of the 22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems. 2007, IEEE Computer Society, Rome, Italy, ss. 152–160

[9] Xilinx Inc. Experiments of Atmospheric Neutron Effects on *SRAM-FPGA - WP286*. San Jose, September 2005 and Xilinx Inc. *Device Reliability Report - UG116*. San Jose, February 2009.

[10] O. Heron, T. Arnaout, and H.-J. Wunderlich. On the reliability evaluation of sram-based fpga designs. In *FPL ’05: International Conference on Field Programmable Logic and Applications*, Tampere, Finland, 2005, ss. 403–408