NÁVRH OBVODŮ S VOLITELNOU ÚROVNÍ SPOLEHLIVOSTI NA BÁZI FPGA

Pavel Vít
Prezenční studium, 1. ročník
Školitel: doc. Ing. Hana Kubátová, CSc.

Fakulta informačních technologií, ČVUT v Praze
Kolejní 550/2
160 00 Praha 6
vitpave1@fit.cvut.cz

Abstrakt. Příspěvek popisuje motivaci, cíle a postupy studenta při zadávání a řešení disertační práce. Cílem by měla být metodologie návrhu číslicových systémů s předem danými a volitelnými spolehlivostními parametry. Tento princip bude využit a testován při tvorbě zabezpečovacího zařízení pro železniční stanici. Tato aplikace vyžaduje vysokou spolehlivost funkčních bloků. V úvodu práce je popsáno, proč se autor bude zabývat tímto tématem a jaký je jeho smysl. Dále je uvedeno, jakým směrem bude práce postupovat a jaký je očekáván výsledek. V závěru je shrnut přínos této činnosti pro obecné i praktické využití.

Klíčová slova. Zabezpečené zařízení, železniční stanice, FPGA, SEU.

1 Úvod

V dnešní době velkého rozvoje vestavných systémů, programovatelných a rekonfigurovatelných obvodů lze velmi těžko verifikovat a testovat vše, co průmysl dokáže navrhnout a vyrobit. Programovatelná hradlová pole (FPGA) se čím dál tím častěji využívají v kritických aplikacích jako je železnice, letectví, medicína atd. V těchto prostředích je kladen veliký důraz na spolehlivost. Motivace k tomuto tématu vycházela z diplomové práce. Ta se zabývala zabezpečovacím zařízením železniční stanice založené na FPGA. Při práci a zkoumání funkce FPGA byla zjištěna potřeba zabezpečení funkčních bloků proti poruchám. Tím se již delší dobu zabývá početná skupina lidí na Katedře číslicového návrhu Fakulty informačních technologií, ČVUT.

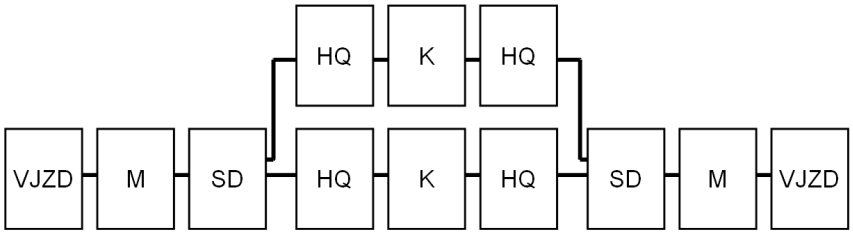
1.1 Generátor zabezpečovacího zařízení

Diplomová práce se zabývá tvorbou nástroje pro generování libovolného staničního zabezpečovacího zařízení pro železnici. Tento software vytváří VHDL modul, který využívá již připravených pěti stavebních bloků. Tyto bloky byly vytvořeny jako diplomová práce[2], která se inspirovala původním reléovým zabezpečovacím zařízením. Výsledkem diplomové práce je aplikace naprogramovaná v jazyce Java, která podle vstupního XML souboru propojí bloky zabezpečovacího zařízení.

Bloky a jejich funkce:

- **VJZD** – blok ovládající vjezdové návěstidlo

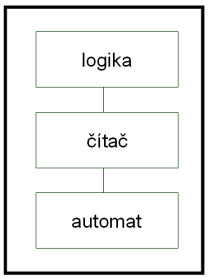
- **M** – blok kontrolující obsazenost bezvýhybkového úseku
- **SD** – blok kontrolující nastavení výhybky a polohu vlaku
- **HQ** – blok ovládající odjezdové návěstidlo
- **K** – blok kontrolující úsek staniční koleje



Obrázek 1: Sestavení bloků pro jednoduché zabezpečovací zařízení

1.2 Bloky zabezpečovacího zařízení

Hlavní bloky se skládaly ze tří částí, které byly společně vloženy jako procesy do jednoho souboru VHDL. Hlavní funkci bloku vykonává stavový automat. Další částí je čítač sloužící k měření času a třetí částí jsou logické funkce, které ovládají funkci návěstidel. Pro jednodušší a efektivnější způsob zabezpečení jednotlivých částí jsem rozdělil jeden původní soubor do tří. Každý proces je přepsán na entitu a uložen v samostatném souboru. Jednotlivé entity lze samostatně zabezpečit proti poruchám jiným způsobem. Tím můžeme docílit vyššího stupně zabezpečení při nižším overheadu (tj. logika, která je nutná k zabezpečení a je v obvodu navíc oproti originálu).



Obrázek 2: Rozdělení procesů do tří souborů

2 Definice problému

Spolehlivost je vlastnost obvodu, kdy je schopen plnit požadovanou funkci při zachování provozních podmínek. Na spolehlivost mají vliv chyby a poruchy obvodu. Poruchou se rozumí stav, kdy obvod přestane plnit požadovanou funkci. Chyba je pak rozdíl mezi očekávaným výstupem z obvodu a skutečným. Chyba je obvykle důsledkem nějaké poruchy, zatímco porucha nemusí nutně projevit jako chyba.

Systémy bezpečné při poruše (fail-safe) lze dosáhnout pomocí průběžného testování obvodu. Toho se dosahuje použitím různých bezpečnostních kódů a samočinným testováním. V případě detekce poruchy se musí obvod sám vrátit z poruchového stavu do bezporuchového. Většina FPGA je založena na pamětech typu SRAM, které jsou náchylné na Single Event Upsets (SEUs). Změna libovolného bitu v konfigurační paměti SRAM může změnit funkci celého obvodu. Proto nelze zaručit bezproblémový chod ve všech kritických prostředích a situacích a je tedy nutná detekce chyb. Tyto poruchy se řadí do kategorie měkkých chyb, to znamená, že poruchy mohou být odstraněny rekonfigurací. Tyto změny v pamětech nejsou detekovatelné pomocí off-line testování, protože poruchy se mohou vyskytnout kdykoliv během funkce FPGA a nikoliv pouze během testu. Je tedy

potřeba testovat obvod on-line a využít self-checking (SC) obvodů, které budou kontrolovat svoji funkci za běhu a budou tedy spadat do kategorie obvodů bezpečných při poruše.

2.1 Spolehlivost složitých obvodů

Mnoho obvodů je v dnešní době na vysoké úrovni a skládá se z velkého množství jednodušších částí, jako jsou stavové automaty, čítače a logické výrazy. Tyto části jsou mezi sebou propojeny a ve výsledku vytváří velice složitou funkci. Určování spolehlivosti celého takto složitého obvodu vůči SEU je těžké. Spočítat spolehlivost jednoduchých částí lze snadněji. Poté je nutné pomocí různých modelů přesně spočítat výslednou spolehlivost složitějšího obvodu.

2.2 Stupeň spolehlivosti

Docílení vysokého stupně spolehlivosti lze za cenu velkého množství okolní logiky oproti původnímu obvodu. To se projevuje na složitosti obvodu a zabraných prostředcích na FPGA. Tím hlavně pro průmyslovou výrobu roste cena návrhu a výsledné realizace. Naopak nízký stupeň zabezpečení může mít za následek v některých případech i ztráty na lidských životech. Honba za nejnižší cenou výrobku, a tím pádem za jednodušším a menším obvodem, není vždy správná.

3 Postup řešení

Řešení problémů by se mělo zaujímat směrem k vytváření jednoduchých částí obvodů s jednoduše spočetnými spolehlivostními parametry. Tyto zabezpečené části se budou propojovat do větších celků, kde bude následovat výpočet spolehlivosti podle příslušného modelu a tím i jednodušší postup pro určení spolehlivosti celého složitého obvodu. Během práce bude nutné nastudovat a případně vhodně upravit spolehlivostní modely, podle kterých budou probíhat všechny výpočty.

Počáteční představou autora je shromáždění postupů a metod pro vytváření základních obvodů s libovolným parametrem spolehlivosti. Základními obvody se rozumí čítače, stavové automaty, kombinační logika a podobné běžně používané části obvodů. Následně by ke zjednodušení mohla být vytvořena aplikace, která bude generovat tyto základní obvody s libovolným stupněm spolehlivosti. Aplikace by tedy měla vytvářet jak zabezpečovaný obvod, tak i logiku potřebnou pro docílení zvoleného stupně spolehlivosti.

Bloky zabezpečovacího zařízení pro železnici jsou vhodné pro testování zabezpečení obvodu proti SEU a určování jejich spolehlivosti. Tyto bloky je potřeba zabezpečit na takovou úroveň, aby vyhovovaly normám pro provoz na železnici. Během zabezpečování bloků bude možno určovat velikost logiky overheadu vzhledem k úrovni zabezpečení. Tím bude možno pro různé aplikace zvolit poměr mezi úrovní zabezpečením a cenou produktu.

4 Závěr

Cílem práce je se zaměřit na poruchy typu SEU v FPGA. Dále zjednodušit určování spolehlivosti pro složité obvody postupem od nejjednodušších obvodů ke složitějším. Sepsat postupy, jak vytvářet obvody s libovolným stupněm zabezpečení a zmapovat množství použité logiky overheadu. Vytvořit aplikaci, která bude generovat základní obvody s libovolným stupněm spolehlivosti.

Přínosem této práce by měl být jasný přehled o tom, kolik logiky stojí jaká úroveň zabezpečení a jestli se tedy ještě vyplatí jak po stránce bezpečnostní, tak i finanční. Naopak by tyto postupy měly upozornit na nedostatečnou úroveň zabezpečení některých obvodů ve snaze docílení nejnižší ceny.

Poděkování

Tato práce je částečně podporována z MSMT pod výzkumným programem MSM6840770014, GA102/09/1668 a SGS10/118/OHK3/1T/18.

Reference

[1] *J. Borecký*: Dependable universal blocks, PAD 2009, ISBN 978-80-7318-847-4

[2] *M. Zatřepálek*: Zabezpečovací zařízení pro železniční stanici založené na FPGA, 2008

[3] *R. Dobiáš*: Stanovení spolehlivosti a bezpečnosti pro systémy odolné a bezpečné proti poruše, PAD 2004

[4] *Actel Corporation*, „Singel-Events Effects in FPGAs“, http://www.actel.com/documents/FirmErrorPIB.pdf, 2007

[5] *J. Hlavička* (1989): Spolehlivost a diagnostika, kapitola 12., Editační středisko ČVUT v Praze

[6] *O. Novák* (2009): Úvod do diagnostiky, základní pojmy (cvičení z předmětu X36DSP, ČVUT v Praze)

[7] *P. Kubalík, H. Kubátová*: Postgraduate study report 2004, ČVUT v Praze