DEPENDABLE UNIVERSAL BLOCKs (DUBs)

Jaroslav Borecký
postgraduální studium 1. ročník
Školitel: doc.Ing. Hana Kubátová, CSc.

Fakulta elektrotechnická, ČVUT v Praze
Karlovo náměstí 13
121 35 Praha 2

borecj2@fel.cvut.cz

Abstrakt. Metoda jak navrhnout efektivně a škálovatelně zabezpečovací zařízení pro železniční stanici. Z pěti základních bloků lze sestavit libovolné staniční zařízení pro nádraží. Každý blok je založen na konečném stavovém automatu. Tyto automaty jsou typu "Moore". Každý automat je rozdělen do tří základních částí, kde každá část je navržena jako samo-testovatelný obvod zajišťující detekci poruch. Naše metoda je určena pro koncovou implementaci v FPGA, kde se předpokládá výskyt poruch SEU.

Klíčová slova. Fault Tolerant, FPGA, Konečné stavové automaty, SEU, Zabezpečené zařízení, Železniční stanice

1 Úvod

Systémy realizované programovatelným hardwarem, jako je programovatelné hradlové pole (FPGA), jsou stále více populární a značně používaný ve více aplikacích kvůli několika výhodám, jako je cena, výkon a možná rekonfigurace aktuálních změn implementovaného obvodu.

FPGA obvody by měly být použity v úkolech kritických aplikací jako je letectví, medicína, vesmírné mise a železniční aplikace [1, 2, 3]. Mnoho FPGA čipů je založena na SRAM pamětech citlivých na Single Even Upsets (SEUs), proto je nemožné jednoduše používat FPGA obvody v misích kritických aplikací bez použití žádných metod detekce chyb.

Změna jednoho bitu v konfigurační paměti vede ke změně funkce obvodu a to často drasticky. Concurrent Error Detection (CED) techniky umožňující detekci měkkých chyb (chyby které mohou být opraveny rekonfigurací) způsobených SEUs [4, 5, 6]. SEUs mohou také změnit obsah vestavěné paměti, Look-up Tables (LUTs) a ostatních konfiguračních bitů. Tyto změny nejsou detekovatelné pomocí metod off-line testování, proto se musí používat CED techniky. Pravděpodobnost výskytu SEU v paměti SRAM je popsán v [7, 8].

Self-checking (SC) struktury se používají k detekci výskytu poruchy v testovaném obvodu. Pouze jedna kopie SC obvodu, nedostatečné ke zvýšení parametrů spolehlivosti. Proto si osvojíme použití Modified Duplex System (MDS) architektury [9, 10].

Tato publikace se zabývá zabezpečením zařízení, jejichž struktura je složena z bloků, které lze různě pospojovat a vytvořit tak libovolné struktury. Předpokládáme, že v daném

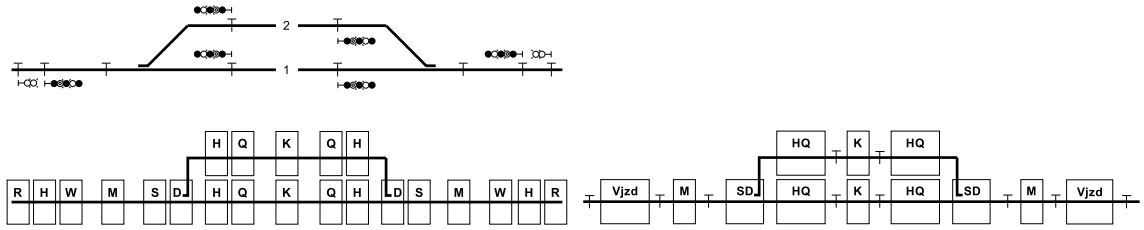
bloku se může vyskytnout pouze jedna chyba. Pro experimenty bylo použito zabezpečovací zařízení pro železniční stanice, které je v dnešní době založeno na reléových blocích. Tento systém je velmi populární kvůli vysokému bezpečnostnímu faktoru. Bezpečnostní faktor je zajištěn odpovídající strukturou s fyzickou konstrukcí železniční stanice. Tento systém je ale příliš velký. Dnešní některé reléové systémy jsou vyměněny za nové systémy založených na procesoru. Procesorově založené systémy nezachovají vysoký bezpečnostní faktor. Pravidla zabezpečovacího zařízení pro železniční stanice jsou dány programátory a ne konstrukcí, jako předchozí systém. Zabezpečovací zařízení založené na procesoru je popsáno v [15].

2 Definování řešeného problému

Většina zařízení založených na FPGA obsahují různé struktury, které jsou složeny z univerzálních bloků. Tyto bloky obstarávají různé funkce a lze je snadno propojit s jinými bloky. Aby bylo možné používat FPGA obvody v kritických aplikacích s určitou spolehlivostí, je zapotřebí tyto bloky zabezpečit. V následující podsekci je lehce popsána kritická aplikace, na jejíž blocích se prováděly experimenty se zabezpečením.

2.1 Staniční železniční systém

Na Obrázku 1 je vyobrazeno jednoduché schéma železniční stanice. Obrázek 1(a) zobrazuje původní propojení releových bloků a Obrázek 1(b) představuje propojení nových bloků realizovaných stavovými automaty. Jak je z obou obrázků patrné, některé bloky ze starého systému byly spojeny dohromady, některé odebrány a některé byly vytvořeny.



(a) Reléové bloky (b) Nové bloky pro FPGA (automaty)

Obrázek 1: Jednoduchá železniční stanice

Tento systém založený na FPGA byl řešen na naší katedře v rámci několika diplomových prací, např. v [14]. Funkce implementované uvnitř nových bloků a komunikace mezi novými bloky jsou zcela odlišné od systému založeného na relé.

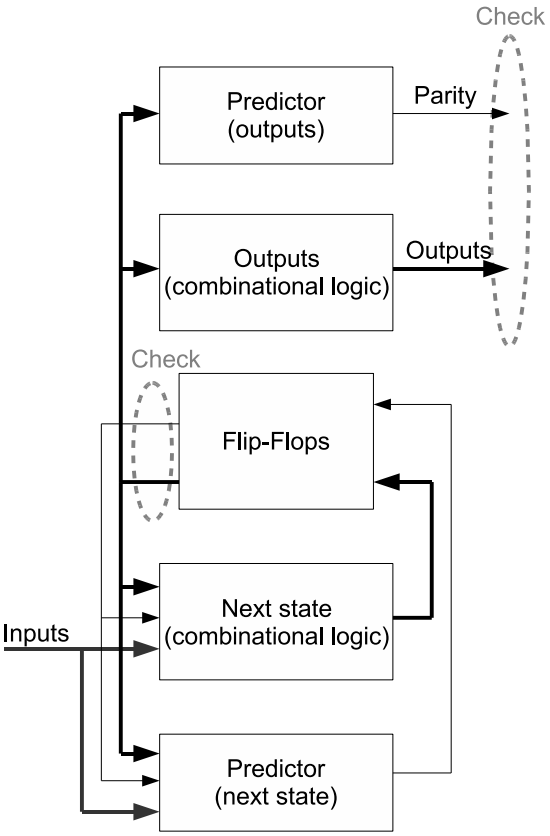
Dané bloky mají následující funkci:

- **Vjzd** blok reprezentuje vjezdové návěstidlo.
- **M** blok kontroluje přesnou pozici vlaku.
- **SD** blok reprezentuje výhybky a také řídí správnou pozici vlaku.
- **HQ** blok reprezentuje odjezdové návěstidlo.
- **K** blok reprezentuje staniční kolej, kontroluje obsazení úseku a správnost vybavování vlaku.

Z těchto základních bloků může být vygenerováno libovolné složité zabezpečovací zařízení pro železniční stanice.

3 Automat se self-checking architekturou

Náš postup vychází z návrhu totally self-checking (TSC) obvodu, s pravidlem pro spojování malých obvodů složených návrhů, který je detailně popsán v [10] a na základní architektuře automatu typu MOORE. Automat je složen ze dvou bloků kombinační logiky a řadou klopných obvodů klopných obvodů, do nichž se ukládá aktuální stav. V našem postupu si jejich reprezentaci osvojíme jako datovou cestu. Všechny stavy automatu jsou zakódovány zvoleným kódem, jenž tvoří kódová slova. Ty jsou podle kombinace vstupů a aktuálního stavu generovány jednou kombinační logikou a slouží k získání následujícího stavu. Druhá kombinační logika generuje z kódových slov výstupy. Obě kombinační logiky jsou navrženy jako self-checking a využívají kódu sudé parity k detekování poruchy. Originální obvod obsahuje prediktor k predikování paritního vodiče na výstupu ze vstupů. Navržená architektura self-checking automatu je zobrazena na Obrázku 2. V místech, která jsou zvýrazněna čárkovaně, ověřuje kontrolor správnost funkce kombinačních logik. Kontrolor následujícího stavu je umístěn za klopnými obvody, to je z důvodu zajištění self-checking vlastnosti pro celý automat.



Obrázek 2: Automat se self-checking architekturou

4 Naměřené výsledky

V následující podsekci je popsán proces syntézy použité k získání parametrů self-testing (ST), fault security (FS) a velikosti použité plochy navíc. Všechny experimenty byly provedeny s šesti kódy pro zakódování vnitřních stavů automatů: binární, Brownův, Grayův, Johnsnův, 1 z N a M z N. Všech pět základních bloků potřebných k návrhu zabezpečovacího zařízení pro železniční stanice, byly modifikovány tak aby zajistily vlastnost self-checking. Všechny tyto bloky byly v originálu v originálu napsány v jazyku VHDL.

Detailní popis těchto bloků je uveden v Tabulce 1. Kde "FSM" je název bloku, "Kolejiště I" a "Kolejiště V" jsou počty vstupních a výstupních vodičů vedoucích z a do prvků kolejiště. "Další bloky IB" a "Další bloky VB" jsou počty vstupních a výstupních vodičů, které individuálně propojují bloky dohromady. "Řídící zařízení IO" a "Řídící zařízení VO" jsou počty vstupních a výstupních vodičů připojených do obslužného zařízení. "IS" a "OS" je součet počtu vstupů a výstupů. "S" představuje počet stavů.

FSM	Kolejiště		Další bloky		Řídící zařízení		IS	OS	S
	I	V	IB	VB	IO	VO			
HQ	2	6	16	19	2	5	20	30	26
K	1	0	12	4	0	3	13	7	19
M	1	0	12	8	0	3	13	11	22
SD	3	2	44	36	0	3	47	41	37
VJZD	3	6	12	12	2	5	17	23	21

Tabulka 1: Pět základních bloků železničního zabezpečovacího zařízení

4.1 Účinnost metody

Výsledky našich experimentů byly zpracovány individuálně pro přechodovou a výstupní kombinační logiku. V Tabulce 2 se nachází výsledky již celých automatů železničních bloků pro šest různých kódů (binární, Brownův, Grayův, Johnsonův, 1 z N a M z N).

"FSM" je zde název bloku zabezpečovacího zařízení , "Kód" je název použitého kódu pro zakódování vnitřních stavů automatu, "Orig." a "Pred." udávají počet LUTů obsazených originálním obvodem a prediktorem, "Over." je overhead, neboli logika navíc vůči originálu, "Sum" je počet testovaných poruch, "ABCD" jsou třídy poruch popisujících projev poruchy (A - skryté poruchy, B - detekovatelné poruchy, C - nedetekovatelné poruchy, D - někdy detekovatelné a někdy nedetekovatelné poruchy) více v [13], "ST" indikuje jak moc obvod vyhovuje vlastnosti self-testing a "FS" indikuje jak moc obvod vyhovuje parametru fault-security.

Výsledky ukazují, že kód 1 z N je vhodný pro kódování našich bloků zabezpečovacího zařízení. Prediktor parity pro kód 1 z N je pouze konstanta, proto nám na výstupy stačí generovat logickou "1". Z čehož vyplývá, že předvídaný výstup je vždy "1". Zajímavé je, že celková plocha pro kód 1 z N vychází ze všech kódů nejlépe. Zároveň má ze všech kódů pro jednotlivé bloky téměř nejlepší pokrytí poruch. Dalším kandidátem který má nejmenší procenta plochy navíc je kód M z N, ale ten má oproti kódu 1 z N horší parametry FS. Naše výsledky dokazují, že naše metoda je vhodná pro návrh zabezpečovacího zařízení pro železniční stanice, ale kvůli skutečnosti, že FS není sto procentní, musí být použita MDS architektura k hlídání detekce SEU.

5 Cíle disertační práce

Cílem disertační práce je návrh metodiky pro realizaci a implementaci struktur s danými spolehlivostními parametry tak, aby výsledek odpovídal předem určené spolehlivosti. Tato metodika bude zaměřena na návrh pro systémy na čipu (SoC) a bude podpořena formální metodou pro modelování funkce, struktury a spolehlivosti tak, aby se spolehlivostní ukazatele daly spočítat z tohoto společného formálního modelu. Bude se využívat standardních a univerzálních bloků se známou spolehlivostí. Každý využitý blok bude zabezpečen (on-line testování). Návrh s ohledem na bezpečné chování (fail-safe), odolnost proti poruchám (fault-tolerant), popřípadně další vlastnosti z hlediska výsledného návrhu celého zařízení. V metodice bude dále zohledněna škálovatelnost, sledování změn parametrů s ohledem na změnu spolehlivostních ukazatelů. Bude se využívat standardních metod zálohování, spolu s využitím rekonfigurace programovatelných obvodů. Zároven bude také zohledněna kombinace návrhu na různých úrovních včetně zohlednění propojení a jeho zálohu.

6 Závěr

Byla představena metoda zabezpečení bloků zabezpečovacího zařízení pro železniční stanice. Z těchto pěti základních bloků může být vytvořeno zabezpečovací zařízení pro libovolnou konfiguraci železniční stanice. Každý blok je navržen jako automat typu Moore, ty jsou tvořeny dvěma kombinačními logikami a datovou cestou. Datová cesta obsahuje klopné obvody za účelem uložení aktuálního stavu. Každá datová cesta je zabezpečena kódem pro detekci chyb a všechny kombinační obvody jsou implementovány jako self-checking. Propojení mezi bloky se musí držet TSC architektury. Pokud porovnáme testované kódy podle jejich parametrů FS a režie plochy, potom kód 1 z N dosahuje vysokého skóre. Proto tento kód vyhovuje zabezpečovacímu zařízení implementovaného v FPGA pro železniční stanice. Popsaná metoda je účinná pro návrh jakékoliv struktury zabezpečovacího zařízení stanic, vytvořených ze základních bloků s možným nárůstem kontroly a predikce spolehlivostních parametrů celkového návrhu. Naše výsledky dokazují, že naše metoda je vhodná pro staniční zabezpečovací zařízení, ale kvůli skutečnosti že FS není stoprocentní, musí být použita architektura MDS k hlídání detekce SEU. Další směr výzkumu bude zjišťování zda je použitý kód pro detekci chyb dostatečný a zda by neposkytoval lepší parametry FS jiný kód např. Bergerův. Následně bude potřeba vymyslet metodu, která zajistí spolehlivost při propojení bloků, neboť všechny výstupy nevedou do dalšího bloku, ale pouze část z nich. Také je zapotřebí vybádat metody pro zabezpečení jiných bloků, nebo prvků např. automat typu Mealy, čítač, atd.

Reference

[1] *R. Dobiáš, H. Kubátová,* "FPGA Based Design of Raiway's Interlocking Equipment", In Proc. of EUROMICRO Symposium on Digital System Design, Rennes (FR), 31.8. - 3.9. 2004, pp 467-473.

[2] *D. Ratter,* "FPGAs on Mars", www.xilinx.com,Xcell Journal Online, 2004.

[3] *Actel Corporation,* "Historic Phoenix Mars Mission Flies Actel RTAX-S Devices", www.actel.com, 2007.

[4] *L. Sterpone, M. Violante,* "A design flow for protecting FPGA-based systems against single event upsets ", DFT2005, 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, pp. 436 – 444.

[5] *M. Bellato, P. Bernardi, D. Bortalato, et al.,* "Evaluating the effects of SEUs affecting the configuration memory of an SRAM-based FPGA", Design Automation Event for Electronic System in Europe 2004, pp. 584-589.

[6] *QuickLogic Corporation,* "Single Event Upsets in FPGAs", 2003, `http://www.quicklogic.com` .

[7] *E. Normand,* "Single Event Upset at Ground Level", IEEE Transactions on Nuclear Science, vol. 43, 1996, pp. 2742-2750.

[8] *Actel Corporation,* "Single-Event Effects in FPGAs",
`http://www.actel.com/documents/FirmErrorPIB.pdf`, 2007.

[9] *P. Kubalik, R. Dobias, H. Kubatova,* "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.

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

[11] *R.K. Brayton, et al.* "Logic Minimization Algorithms for VLSI Synthesis", Boston, MA, Kluwer Academic Publishers, 1984.

[12] *P. Fišer, and J. Hlavička,* "BOOM - A Heuristic Boolean Minimizer", Computers and Informatics, Vol. 22, 2003, No. 1, pp. 19-51.

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

[14] *M. Zatřepálek,* "Zabezpečovací zařízení pro železniční stanici založené na FPGA", Diploma Thesis, Czech Technical University in Prague, Faculty of Electronic Engineering, 2009. (In Czech)

[15] *V. Chandra, M.R. Verma,* "A Fail-Safe Interlocking System for Railways", IEEE Design & Test of Computers, 1991, pp. 58-66.

FSM	**Code**	**Orig.** [LUT]	**Pred.** [LUT]	**Over** [%]	**Sum**	**A**	**B**	**C**	**D**	**ST** [%]	**FS** [%]
HQ	Binary	180	43	23,89	2076	228	1516	163	169	91,18	82,03
K	Binary	125	42	33,6	1532	220	1167	47	98	96,42	88,95
M	Binary	143	54	37,76	1830	227	1439	33	131	97,94	89,77
SD	Binary	432	112	25,93	4910	802	3479	156	473	96,2	84,69
VJZD	Binary	134	47	35,07	1694	174	1327	66	127	95,66	87,3
HQ	Brown	398	49	12,31	4078	949	2323	309	497	90,12	74,24
K	Brown	193	26	13,47	2016	337	1314	130	235	92,26	78,26
M	Brown	430	42	9,77	4220	1222	2311	218	469	92,73	77,08
SD	Brown	1137	90	7,92	10666	2894	4896	1427	1449	81,64	63,0
VJZD	Brown	211	32	15,17	2228	296	1351	241	340	87,53	69,93
HQ	Gray	183	35	19,13	2020	278	1416	167	159	90,41	81,29
K	Gray	110	38	34,55	1376	220	1008	50	98	95,67	87,2
M	Gray	125	38	30,4	1516	161	1141	51	163	96,24	84,21
SD	Gray	365	93	25,48	4130	654	2815	192	469	94,48	80,98
VJZD	Gray	141	38	26,95	1650	191	1334	56	69	96,16	91,43
HQ	Johnson	185	40	21,62	2046	267	1334	230	215	87,07	74,99
K	Johnson	149	44	29,53	1746	297	1121	135	193	90,68	77,36
M	Johnson	159	55	34,59	1976	347	1231	139	259	91,47	75,57
SD	Johnson	1146	182	15,88	11662	3487	6649	653	873	92,01	81,33
VJZD	Johnson	196	47	23,98	2276	440	1447	130	259	92,92	78,81
HQ	OneHot	195	6	3,08	1896	256	1400	66	174	95,98	85,37
K	OneHot	94	5	5,32	952	151	670	65	66	91,89	83,65
M	OneHot	121	6	4,96	1198	190	854	55	99	94,54	84,72
SD	OneHot	569	2	0,35	5084	1086	3583	81	334	97,97	89,62
VJZD	OneHot	179	4	2,23	1664	220	1264	43	137	97,02	87,53
HQ	m-out-of-n	287	3	1,05	2686	450	1436	363	437	83,77	64,22
K	m-out-of-n	589	3	0,51	5190	1758	2298	566	568	83,51	66,96
M	m-out-of-n	802	4	0,5	6918	2325	3233	611	749	86,7	70,39
SD	m-out-of-n	2087	4	0,19	17852	5814	8740	974	2324	91,91	72,6
VJZD	m-out-of-n	590	4	0,68	5294	1379	2954	416	545	89,37	75,45

Tabulka 2: FS pro výstupní kombinační logiku