

可编程器件的选择性双模冗余加固方法

郑美松^{1,2)}, 王子龙²⁾, 涂吉^{1,2)}, 王骏也^{1,2)}, 李立健^{1)*}

¹⁾(中国科学院自动化研究所空天信息中心 北京 100190)

²⁾(中国科学院研究生院 北京 100049)

(lijian.li@ia.ac.cn)

摘要: 针对现有 FPGA 加固方法开销过大的问题, 提出一种利用逻辑门对故障的屏蔽效应进行选择性加固的双模冗余方法. 首先建立待加固电路的查找表结构模型, 根据故障的传播概率按电路结构依次计算每个查找表的故障敏感度; 然后将故障敏感度高的查找表进行双模冗余, 并根据要屏蔽的故障类型在冗余后的查找表输出端添加“与”, “或”逻辑进行表决; 最后对加固后的电路进行故障注入, 验证加固效果. 对 MCNC 测试集电路的实验结果表明, 与现有方法相比, 在同等开销下, 文中方法对故障的屏蔽效果更显著; 全冗余时, 该方法可将故障平均减少 84.3%, 对于 apex2, spla 等大电路则能减少超过 97%.

关键词: FPGA; 容错; 双模冗余; 故障敏感度

中图法分类号: TP302.8

A Selective Dual Modular Redundancy Approach for FPGA Hardening Technique

Zheng Meisong^{1,2)}, Wang Zilong^{1,2)}, Tu Ji^{1,2)}, Wang Junye^{1,2)}, and Li Lijian^{1)*}

¹⁾(Aerospace Information System Research Center, Institute of Automation, Chinese Academy of Sciences, Beijing 100190)

²⁾(Graduate University of Chinese Academy of Science, Beijing 100049)

Abstract: Aiming at the excessive hardware overhead of existing FPGA hardening techniques, this paper proposes a selective dual modular redundancy scheme by utilizing the fault masking properties of logic gates to tolerate faults in FPGAs. Firstly, look up table (LUT) structure circuit model is established for each circuit, and fault sensitivity of each LUT in given circuit is calculated level by level according to fault propagation probability. Secondly, LUTs with higher fault sensitivity are duplicated, and an AND or OR logic is added to the duplicated LUT output as a voter so that certain faults are masked. Finally, fault injection experiments are carried on the hardened circuits to verify the proposed hardening technique. The experimental results on MCNC test set circuits show that, under the condition of the same overhead, the proposed approach can reduce more faults compared with existing methods. At the full redundant mode, the proposed approach can reduce faults by 84.3% on average, and for large circuits like apex2 and spla can reduce more than 97%.

Key words: FPGA; fault tolerance; dual modular redundancy; fault sensitivity

近年来, 基于 SRAM(static random access memory)的 FPGA(field programmable gate array)在电子

收稿日期: 2015-02-12; 修回日期: 2015-05-13. 基金项目: 国家自然科学基金(61073035). 郑美松(1989—), 女, 博士研究生, 主要研究方向为集成电路测试、FPGA 容错设计; 王子龙(1988—), 男, 博士研究生, 主要研究方向为集成电路可测性设计、片上系统体系结构设计; 涂吉(1986—), 男, 博士研究生, 主要研究方向为超大规模集成电路测试、数据压缩; 王骏也(1990—), 男, 硕士研究生, 主要研究方向为 GPU 设计、片上系统体系结构设计; 李立健(1960—), 男, 博士, 研究员, 博士生导师, 论文通讯作者, 主要研究方向为集成电路可测性设计、集成电路微体系结构设计.

系统中的应用越来越广泛. 但由于 FPGA 的可编程功能的实现全部依赖于其内部的 SRAM 配置单元, 而六晶体管结构的 SRAM 配置单元在空间辐射环境中极易发生单粒子翻转, 从而导致 FPGA 逻辑功能的改变, 极大地降低了电子系统的可靠性^[1-2].

结合配置刷新的三模冗余(triple module redundancy, TMR)技术是目前比较成熟有效的 FPGA 电路加固方法^[3], 但该方法给电路带来了超过 200% 的硬件开销和时延、功耗负担. 利用新结构 FPGA 中 6-输入查找表可拆分性和进位链逻辑提出的原地缓解方法^[4-7]能在基本不带来额外开销的基础上一定程度地缓解单粒子效应, 但对系统可靠性的提升较小, 用原地缓解方法加固的 FPGA 电路的平均无故障时间一般还难以胜任实际应用.

为了适当减少 TMR 的硬件开销, Samudrala 等^[8]提出了选择性 TMR, 并被应用到 FPGA 的查找表结构电路中^[9], 但实验结果表明, 该方法在查找表结构电路中表现并不好, 最后还需要通过仿真对查找表进行筛选和冗余. Pratt 等^[10]提出了只对电路中带反馈回路的部分进行 TMR 的细粒度部分冗余方法, 并设计了选择性 TMR 工具 BLTmr, 该工具可以根据用户预设的电路开销自动对电路进行选择性冗余加固.

双模冗余(dual module redundancy, DMR)的额外开销能比 TMR 减少一半, 也是对 FPGA 电路进行加固的选择之一^[11], 但 DMR 电路无法用“少数服从多数”特性的表决器表决出正确结果, 只能通过比较得出电路有错误的结论, 此时就需要停止电路并刷新才能解决问题. de Lima 等^[12]提出了结合比较和并发错误检测的 DMR 方法, 当检测到错误时只需等待 1 拍便可判断哪部分电路出错, 并在下一拍选择正确电路作为输出; 但该方法的编解码电路较难设计, 几乎无法用于复杂电路.

本文利用与(或)门电路能屏蔽固定 1(0)故障的特点, 设计了一种不需要判断哪部分电路出错便能输出正确结果的 DMR 方法, 并借助 Xilinx 公司的 Virtex 系列 FPGA 内部丰富的三态门资源设计 DMR 输出表决器, 充分实现了电路可靠性和硬件开销之间的平衡. 该方法比 TMR 开销小, 且无需像现有 DMR 方法那样, 在发生故障时停机修复或等待额外的判断电路定位错误模块. 但由于在错误发生时, 本文方法并不能指定是何种特定故障, 因此该方法适用于不需要检测错误而只对错误进行屏蔽的应用.

1 问题的提出

稳定运行中的数字电路只有 2 种逻辑状态: 逻辑“1”和逻辑“0”. 由于数字电路自身结构特点及其应用环境不同, 电路运行过程中其内部各节点将呈现出不同的逻辑“1”和逻辑“0”偏好, 即某些节点以较大的概率呈现逻辑“1”电平, 某些节点以较大的概率呈现逻辑“0”电平. 逻辑“1”呈现概率较高的节点, 若发生固定 1 故障是较难表现出来的, 若发生固定 0 故障则表现出故障的可能性较高; 同理, 逻辑“0”呈现概率较高的节点, 若发生固定 1 故障则表现出故障的可能性也较高. 本文主要针对逻辑“1”呈现概率较高节点的固定 0 故障和逻辑“0”呈现概率较高节点的固定 1 故障进行屏蔽, 从而达到器件加固的效果.

如图 1 所示的 3-输入、1-输出组合逻辑电路由与门 AND 和或门 OR1 构成, 假设电路有如图所示的输入序列, 3 根输入线 A , B , C 呈现逻辑“1”和逻辑“0”的概率均为 1/2; 对应地, 中间线 D 和输出线 E 上将输出图示的序列, 由于电路的结构特点, 线 D 呈现出逻辑“0”的概率较高, 输出线 E 呈现出逻辑“1”的概率较高, 均为 3/4. 对于输出线 E 来说, 若发生固定 1 故障, 只有线 E 被敏化逻辑“0”时电路才表现为故障电路, 那么在图示的输入下电路能表现出错误的概率仅有 1/4; 反之, 若 E 发生了固定 0 故障则电路表现出错误的概率有 3/4. 因此, 按本文的设计思想, 针对此电路的加固技术应考虑如何屏蔽线 E 上的固定 0 故障.

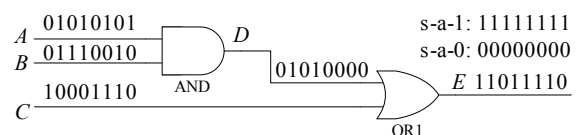


图 1 组合逻辑电路的故障

2 查找表电路的故障模型及故障传播概率

本文主要对组合电路进行加固, 将 FPGA 内部电路结构简化为由查找表和查找表之间连线构成的组合逻辑电路, 通过对查找表内部的配置单元进行编程可实现不同的逻辑功能. 图 2 所示为 MCNC 测试集中的 cm152a 电路 4-输入查找表结构.

2.1 查找表电路的故障模型

图 2 所示的 FPGA 模型存在 2 种故障: 查找表

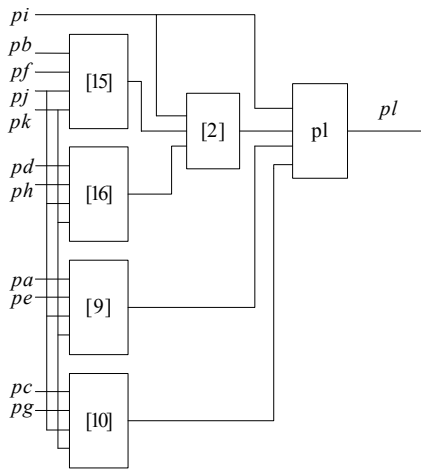


图 2 cm152a 的 4-输入查找表结构

配置位的翻转故障和连线故障。尽管对于 FPGA 的测试来说, 用查找表输出线上的固定故障表征查找表配置位翻转故障不具有完备性^[13-14], 但文献[15]证明, 查找表之间连线的固定故障可以覆盖所有位翻转故障, 本文加固方法只是对 FPGA 电路故障进行屏蔽, 并不需要像 FPGA 的测试一样判断出错误的具体发生位置, 因此可以用查找表输出线上的固定 1(0)故障代表其配置位的 0 1(1 0)翻转故障。

根据前述查找表结构模型, 将图 1 中描述的 3-输入、1-输出组合逻辑电路映射为一个 3-输入查找表如图 3 所示。该查找表有 $2^3=8$ 个配置位: $C_0\sim C_7$, 电路运行过程中根据输入线 A, B, C 上施加的不同的逻辑值, 输出线 E 上输出对应地址的配置位的值, 从而实现相应的逻辑功能。

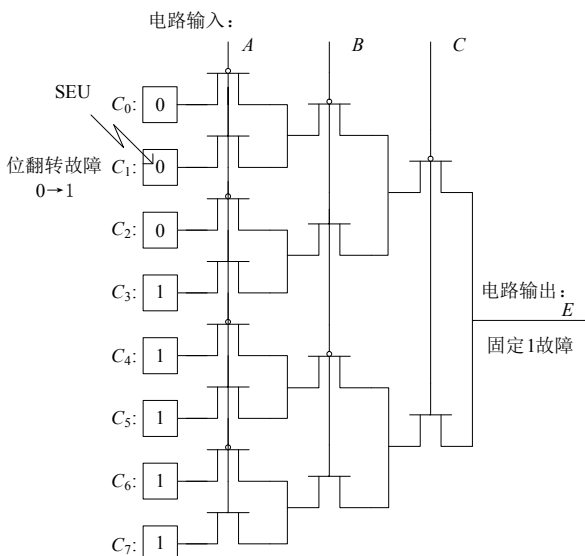


图 3 查找表电路故障模型

假配置位 C_1 被单粒子打翻, 由原来的逻辑“0”状态翻转为逻辑“1”状态, 那么在查找表的 3 根输入线 C, B, A 的逻辑电平不选通配置位 C_1 时查找表 LUT_E 表现无故障; 当输入线 $CBA=\{001\}$ 时配置单元 C_1 的状态被选通到查找表的输出线 E 上, 此时配置位 C_1 的位翻转故障可以看作是输出线 E 上的固定 1 故障。不考虑连线故障, 输出线 E 上的固定 1 故障由配置位 C_0, C_1, C_2 的 0 1 翻转故障组成, 固定 0 故障由配置位 C_3, C_4, C_5, C_6, C_7 的 1 0 翻转故障组成, 根据每个配置位被选通的概率可计算线 E 上固定故障的发生概率。

2.2 查找表电路单固定故障的敏化

假设查找表电路各配置位被打翻的概率相同, 查找表电路的单固定故障发生概率可定义如下:

定义 1. 对于一个查找表结构的组合逻辑电路, 当其配置位被打翻的概率均等, 为一固定常数时, 查找表之间连线上发生固定 1(0)故障的概率与其表现为逻辑“0”(逻辑“1”)的概率呈线性关系, 而某一查找表的输出线表现为逻辑“0”(逻辑“1”)的概率是其所有配置位为 0(1)的概率之和。

例如, 图 3 中的查找表 LUT_E 的输出线 E 上发生固定 1 故障的概率

$$P_{sa1}(E)=P_{c0}(E)\times\delta.$$

其中, δ 是由 FPGA 芯片特性和单粒子事件发生概率联合确定的常数; $P_{c0}(E)$ 是输出线 E 能被控制为 0 的概率,

$$P_{c0}(E)=P_{c0}(C)P_{c0}(B)P_{c0}(A)+P_{c0}(C)P_{c0}(B)P_{c1}(A)+P_{c0}(C)P_{c1}(B)P_{c0}(A).$$

假设查找表的 3 个输入端 A, B, C 被控制为 0 和 1 的概率相同, 即 $P_{c1}(A)=P_{c1}(B)=P_{c1}(C)=0.5$, 则有 $P_{c0}(E)=0.375$, 对应地, $P_{c1}(E)=1-P_{c0}(E)=0.625$. 那么连线 E 上发生固定 1 故障的概率为 $P_{sa1}(E)=0.375\times\delta$; 发生固定 0 故障的概率为 $P_{sa0}(E)=0.625\times\delta$.

对于一个输入概率已知的查找表结构电路, 可根据定义 1 从前向后逐级计算每个查找表输出线的概率。不同电路的输入概率会有所不同, 本文假设电路所有输入为逻辑“1”状态和逻辑“0”状态的概率相同, 均为 0.5。

2.3 查找表电路单固定故障的传播

第 2.2 节讨论的是电路连线上单固定故障被敏化的概率, 由于只有能传播到电路输出线上的故障才被表现出来, 而不能传播至输出的故障并不需要进行屏蔽, 因此还要考虑被敏化到的故障的

传播概率。文献[16]表明,查找表中的大部分故障在传播过程中都会被后级逻辑湮没,传播级数不超过 10 个节点的故障约占到所有故障的 82%。本文采用电路测试中的可观测性来表征查找表故障的传播概率,仍用概率的方法计算^[17-18],定义如下:

定义 2. 当某一查找表输出线 O 的故障传播概率已知的情况下,该查找表的某根输入线 I 的故障传播概率

$$P_o(I) = P_o(O) \times P\{O \leftrightarrow |_{I \leftrightarrow}\};$$

其中, $P\{O \leftrightarrow |_{I \leftrightarrow}\}$ 表示输出线 O 的逻辑变化只受输入线 I 的逻辑变化控制的概率。

以图 3 中的输入线 C 的故障传播概率 $P_o(C)$ 的计算为例:根据查找表 LUT_E 的配置位情况,当输入线 $BA = \{00\}, \{01\}, \{10\}$ 时输入线 C 的逻辑电平变化均能引起输出线 E 的逻辑电平变化,即 E 的逻辑电平只受 C 控制,此时可以通过输出线 E 观测到输入线 C 的逻辑状态变化。假设输出线 E 上的故障传播概率已知为 $P_o(E) = 1$, 那么有

$$P_o(C) = P_o(E) \times (P_{c0}(B)P_{c0}(A) + P_{c0}(B)P_{c1}(A) + P_{c1}(B)P_{c0}(A)) = 0.75.$$

类似地,可以计算输入线 B, A 上的故障传播概率分别为

$$P_o(B) = P_o(E) \times P_{c0}(C) \times P_{c1}(A) = 0.25,$$

$$P_o(A) = P_o(E) \times P_{c0}(C) \times P_{c1}(B) = 0.25.$$

由于多扇出节点的故障可通过任意一条扇出茎传播,本文定义多扇出节点的故障传播概率

定义 3. 对于有 n 个扇出分别为 t_1, t_2, \dots, t_n 的连线 v , 其固定故障传播概率

$$P_o(v) = 1 - \prod_{i=1}^n \{1 - P_o(t_i)\}.$$

在电路测试领域,关于有扇出连线的可观测性的计算有最大值法、求和法^[18]等。最大值法忽略了扇出源通过其他扇出茎被观测到的概率,明显低估了扇出源的可观测性;而求和法没有考虑扇出线在电路后级有可能重汇聚的问题,又对扇出源的可观测性估计过高,往往甚至大于 1。考虑到若某多扇出连线的所有扇出茎上的故障都无法传播则该连线的故障无法传播,本文采用定义 3 计算多扇出节点的故障传播概率。

对于整个电路来说,由于电路的输出端上的故障将直接表现为电路错误,因此首先设定电路输出端上的故障传播概率为 1,其他电路连线的故障传播概率可根据电路拓扑结构,按定义 2, 3 经由

输出从后向前逐级计算。

2.4 故障敏感度的定义

定义 4. 对于一个查找表电路,将其内部连线的故障敏感度分为固定 0 故障敏感度 S_{sa0} 和固定 1 故障敏感度 S_{sa1} 2 种,电路中连线的故障敏感度根据连线上固定故障发生概率和故障传播概率综合计算。对于电路中某根连线 L 有

$$S_{sa0}(L) = P_{sa0}(L) \times P_o(L),$$

$$S_{sa1}(L) = P_{sa1}(L) \times P_o(L).$$

其中, $S_{sa0}(L)$ 和 $S_{sa1}(L)$ 分别表示连线 L 的固定 0 故障敏感度和固定 1 故障敏感度, $P_{sa0}(L)$ 和 $P_{sa1}(L)$ 分别表示用定义 1 算得的连线 L 的固定 0 和固定 1 故障发生概率, $P_o(L)$ 表示用定义 2, 3 计算得到的连线 L 的固定故障传播概率。

根据定义 4 可以算得查找表结构电路中所有连线的故障敏感度,查找表输出线上的故障敏感度代表了该查找表的故障敏感度,当查找表结构电路中所有连线的故障敏感度计算完毕就获得了电路中的查找表敏感度信息,从而可以根据开销约束对查找表进行冗余加固处理。

3 选择性双模冗余加固方法

本文利用逻辑门对固定故障的屏蔽效应和 FPGA 电路中各节点的故障表现来对 FPGA 电路进行选择性 DMR, 首先根据定义 1~4 计算电路中所有连线的固定 0, 1 故障敏感度,再根据查找表输出线上的故障敏感度大小判断是否需要对其进行冗余加固,最后根据要屏蔽的故障类型选择加固后的表决方式。

3.1 逻辑门对固定故障的屏蔽效应

对于与门电路来说,逻辑“0”是其控制值,即当与门的一个输入为 0 时,无论其他输入的逻辑电平是什么值,其输出恒为 0。与门的这一性质配合 DMR 可用来屏蔽电路中的固定 1 故障;同理,或门配合 DMR 可以屏蔽电路中的固定 0 故障。

如图 4 所示,将图 1 中描述的和或门组合逻辑电路进行 DMR,按照前述分析,由于输出线 E 上的固定 0 故障对电路的影响较大,在 DMR 电路的输出端添加或门 OR2 以屏蔽输出线 E 的固定 0 故障。

由于电路中同时有多个配置位被打翻的发生概率极低,可假设电路运行中一次只会出现一个错误,即输出线 E 及其备份输出 E' 不会同时出现故障。那么该电路可能有如下 2 种故障: 1) E 或 E'

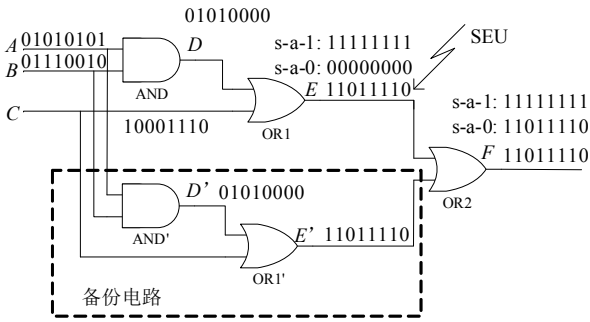


图 4 或门对固定 0 故障的屏蔽

的单固定 0 故障; 2) E 或 E' 的单固定 1 故障。

没有故障发生时, E 和 E' 输出同为逻辑“1”或逻辑“0”, 经或门 OR2 后 F 输出与 E, E' 相同的逻辑值, 电路输出正确结果; 假设输出线 E 上发生 1) 固定 0 故障, 当电路运行结果为逻辑“0”时, 连线 E, E' 和 F 的逻辑电平同为“0”, 电路结果正确, 当电路运行结果为逻辑“1”时, E 虽因固定 0 故障保持逻辑电平“0”不变, 由于 E' 的逻辑电平“1”是或门 OR2 的控制值, 最终线 F 仍能输出逻辑“1”, 电路结果仍正确; 假设输出线 E 上发生 2) 固定 1 故障, 那么由于 E 保持或门 OR2 的控制值, 线 F 将始终输出逻辑“1”, 则在图 4 所示的输入序列下电路将以 1/4 的概率表现出错误。

根据上述分析, 逻辑门只能屏蔽某一种单固定故障, 因此本文将筛选电路中固定故障敏感度高的节点进行 DMR, 并根据故障类型选择“与”逻辑或“或”逻辑对输出进行表决。

3.2 加固查找表的选择

根据定义 1~4 计算得到 cm152a 电路各查找表输出线故障敏感度如表 1 所示, 其中, 第 2, 3 列 $P(0)$ 和 $P(1)$ 分别表示查找表输出线表现为逻辑“0”和逻辑“1”的概率; 第 4 列 P_o 表示查找表输出线的故障传播概率; 第 5, 6 列 S_{sa1} 和 S_{sa0} 分别表示查找表输出线的固定 1 故障敏感度和固定 0 故障敏感度。

从表 1 可以看出, 查找表 p1 和查找表[2]输出线的固定 1 故障敏感度均为 0.61δ , 明显高于电路

表 1 cm152a 电路查找表输出线故障敏感度

查找表	$P(0)$	$P(1)$	P_o	S_{sa1}	S_{sa0}
p1	0.61	0.39	1	0.61δ	0.39δ
[2]	0.781	0.219	0.781	0.61δ	0.17δ
[9]	0.75	0.25	0.293	0.22δ	0.07δ
[10]	0.75	0.25	0.293	0.22δ	0.07δ
[15]	0.75	0.25	0.293	0.22δ	0.07δ
[16]	0.75	0.25	0.293	0.22δ	0.07δ

中其他节点, 因此这 2 根连线上若发生固定 1 故障则电路表现出故障的可能性较高, 应考虑将这 2 个查找表进行 DMR 加固并添加“与”逻辑表决器以屏蔽固定 1 故障。

3.3 加固方法与流程

Xilinx 公司的 Virtex 系列 FPGA 每个可配置逻辑模块上都有 2 个三态门资源, 可用来构成具有“少数服从多数”功能的 TMR 电路表决器^[3]。本文也利用该三态门结构设计“与”, “或”逻辑表决器, 如图 5 所示, 因此表决器的插入不会引起额外的查找表开销。

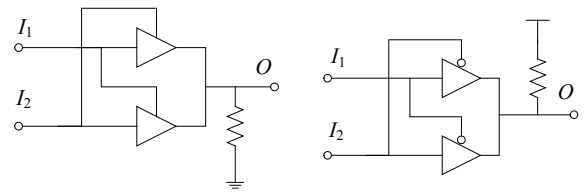


图 5 用三态门结构实现与、或逻辑

将 cm152a 电路按本文方法加固后如图 6 所示, 加固后的电路只比原来多了 2 个冗余查找表, 表决器的插入并未引入额外的查找表开销。

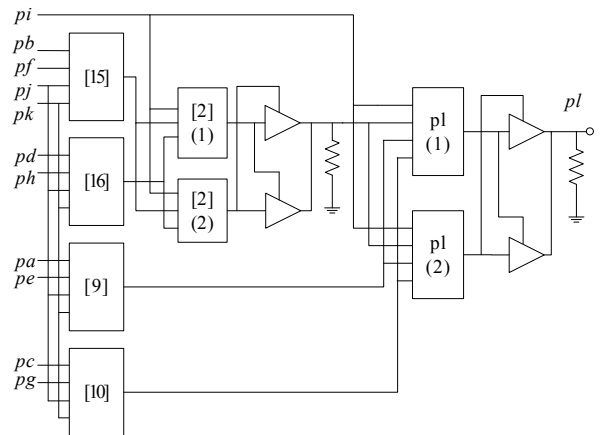


图 6 cm152a 电路的选择性加固

由于 FPGA 电路逻辑资源有限, 应用中过多的资源使用率往往带来布线困难、时延约束不满足等问题, 在本文方法的具体实施中将以面积约束为导向, 根据系统硬件开销要求计算可冗余的查找表个数, 并根据前述步骤计算出的查找表敏感度对需要冗余的查找表进行筛选以最大地提高系统可靠性。

为了对本文方法进行验证, 设计故障仿真实验, 每次对测试电路随机注入一个故障, 利用线性

反馈移位寄存器产生随机测试向量加载到电路输入端, 观察电路输出端的输出向量是否与未注入故障时相同, 若 2 次输出不相同表示注入的故障导致电路输出错误, 记录该故障. 步骤如下:

建立简化的基于 4-输入查找表的 FPGA 电路模型

测试电路映射为 4-输入查找表结构的 FPGA 电路

```
for (电路中每个查找表节点){
    计算电路每个节点的固定 0, 1 故障敏感度;
    按敏感度对查找表节点排序
    while (未达到预设的冗余度){
        对故障敏感度大的查找表进行 DMR
        if (要屏蔽的是固定 0 故障) {
            查找表输出端添加或门}
        else {
            查找表输出端添加与门}}
    故障仿真, 验证加固效果
```

4 实验结果与分析

选取 MCNC 基准测试电路集中的部分电路对方法进行验证, 用 RASP 工具将电路映射成 4-输入查找表结构的 FPGA 模型, 并编写选择性 DMR 加固方法的 C++ 程序对该模型进行加固.

为了比较加固效果, 将本文方法(DMR)筛选出来的需要冗余的查找表同时做了 TMR 进行对比. 考虑到冗余度相同时 TMR 对电路造成的额外开销

刚好是 DMR 方法的 2 倍, 表 2 列出了 2 种方法按冗余度分别为原始电路的 25%、50%和 100%加固后的结果, 这样, 冗余度为 25%和 50%时 TMR 方法加固后的电路硬件开销刚好与冗余度为 50%和 100%时的 DMR 相同.

对原始电路(ORI), DMR 和 TMR 加固电路分别进行故障仿真. 实验中对每个测试电路注入 1 000 个随机故障并记录这 1 000 个故障最终表现到输出端的个数, 其中, ORI, DMR 和 TMR 加固电路的故障点保持一致, 结果如表 2 所示. 表 2 中, 第 2 列给出了各测试电路经 RASP 映射后使用的查找表数, 各测试电路按规模从小到大的顺序从上向下排列; 第 3~11 列为不同冗余度下各测试电路在故障仿真过程中最终表现出来的故障数, 其中第 3~5 列冗余度为 25%表示测试电路可冗余的查找表个数为 ORI 查找表个数的 25%, 例如, 4 575 个查找表的 pdc 电路可冗余的查找表个数为 $4575 \times 25\% = 1144$ 个, 那么 DMR 加固后的电路将占用 $4575 + 1144 = 5719$ 个查找表, 而 TMR 加固后的电路将占用 $4575 + 1144 \times 2 = 6863$ 个查找表. 第 3 列中, ORI 表示对原始电路注入 1 000 个随机故障最终表现到输出端的故障个数, pdc 测试电路在未加固的情况下表现出了 217 个故障; 第 4 列中, DMR 表示同样的故障点下对测试电路用本文方法加固后的电路最终表现到输出端的故障个数, pdc 测试电路在用本文方法加固后表现出了 124 个故障, 比原始电路减少了 42.9%; 第 5 列中, TMR 表示同样的故障点下对测试电路用 TMR 方法加固后的电路最终表现到输出

表 2 对 MCNC 测试集中部分电路的加固效果

电路名称	查找表数	故障数								
		冗余度 25%			冗余度 50%			冗余度 100%		
		ORI	DMR(减少%)	TMR(减少%)	ORI	DMR(减少%)	TMR(减少%)	ORI	DMR(减少%)	TMR(减少%)
cm152a	6	564	474(16.0)	379(32.8)	544	344(36.8)	197(63.8)	549	201(63.4)	0(100)
term1	88	204	40(80.4)	14(93.1)	171	30(82.5)	0(100.0)	187	33(82.4)	0(100)
c432	124	250	145(42.0)	124(50.4)	302	127(57.9)	68(77.5)	263	81(26.3)	0(100)
c880	174	452	291(35.6)	239(47.1)	414	190(54.1)	108(74.0)	456	89(80.5)	0(100)
ex5p	1 064	422	234(44.5)	233(44.8)	407	128(68.6)	122(70.0)	414	52(87.4)	0(100)
misex3	1 397	490	255(48.0)	253(48.4)	492	83(83.1)	80(83.7)	497	6(98.8)	0(100)
alu4	1 522	289	130(55.0)	123(57.4)	260	24(90.8)	20(92.3)	264	4(98.5)	0(100)
des	1 591	676	492(27.2)	487(28.0)	695	299(57.0)	247(64.5)	673	134(80.1)	0(100)
seq	1 750	410	163(60.2)	163(60.2)	423	24(94.3)	19(95.5)	450	6(98.7)	0(100)
apex2	1 878	352	122(65.3)	121(65.6)	337	3(99.1)	1(99.7)	357	1(99.7)	0(100)
spla	3 690	464	292(37.0)	286(38.4)	485	125(74.2)	118(75.7)	462	9(98.1)	0(100)
pdc	4 575	217	124(42.9)	120(44.7)	230	64(72.2)	56(75.7)	223	6(97.3)	0(100)
平均	1 488	399	230(46.2)	212(50.9)	397	120(72.6)	86(72.8)	400	52(84.3)	0(100)

端的故障个数, pdc 测试电路在用本方法加固后表现出了 120 个故障, 比原始电路减少了 44.7%; 第 6~8 列和第 9~11 列分别为冗余查找表个数为原始电路的 50%和 100%时电路输出的故障情况。

由表 2 可以看出, 相同冗余度的情况下, 对本文方法选出的查找表来说, 进行 TMR 并未比 DMR 减少太多故障, 却比 DMR 对电路造成的额外开销大 1 倍, 说明根据固定故障类型选择待冗余查找表并借助“与”, “或”逻辑对固定故障的屏蔽作用容错的方法十分有效。而比较第 5 列与第 7 列、第 8 列与第 10 列可以看出, 当电路面积相同时部分 TMR 方法可靠性明显不如本文方法, 这是由于 TMR 需要将电路复制成 3 倍, 同等开销的情况下其查找表冗余度只能达到本文方法冗余度的一半。

在冗余度为原始电路的 100%, 即全冗余时, 本文方法将故障数平均减少了 84.3%, 对 apex2,

spla 等大电路均接近 TMR 方法的 100%, 若配合 FPGA 的定时刷新技术即可保证系统长时间稳定工作, 而此时的电路面积只是 TMR 方式的 2/3。

向各测试电路随机注入 1 000 个故障, 将本文方法与文献[9]提出的部分 TMR 方法进行对比, 结果如表 3 所示。

表 3 中, 第 2, 3 列为文献[9]选用的原始测试电路所用查找表数和表现出的故障数; 第 6, 7 列分别为用文献[9]方法加固后的电路查找表数和故障数。为了方便对比, 本文采用和文献[9]相同的查找表开销对测试电路进行加固, 但由于文献[9]中 des 和 ex5p 的开销超过了原始电路的 100%, 而本文所用 DMR 方法的最大开销就是 100%, 因此对这 2 个测试电路采用最大开销。第 5 列所示为本方法加固后的故障数, 可以看出, 同等开销的情况下本文方法故障数均低于文献[9]方法。

表 3 本文方法与文献[9]的比较

电路名称	原始电路查找表数	原始电路故障数	本方法查找表数 (额外开销%)	本方法故障数	RTMR 查找表数 (额外开销%)	RTMR 故障数
alu4	1 522	275	2 959(94.42)	3	2 959(94.42)	7
apex2	1 878	350	2 974(58.36)	2	2 974(58.36)	0
des	1 591	699	3 182(100.00)	151	3 850(141.99)	68
misex3	1 397	512	2 723(94.92)	5	2 723(94.92)	17
pdc	4 575	248	8 661(89.31)	5	8 661(89.31)	13
seq	1 750	413	3 371(92.63)	6	3 371(92.63)	7
spla	3 690	460	7 222(95.72)	12	7 222(95.72)	13
ex5p	1 064	394	2 128(100.00)	39	2 442(129.51)	21

5 结 语

本文提出一种对 FPGA 进行选择性的双模冗余的加固方法, 利用“与”, “或”逻辑对固定故障的屏蔽效应最大化地减少查找表故障对电路最终输出的影响, 并从理论上分析了该方法的可行性。实验结果表明, 在开销相同的情况下本文提出的方法对电路故障数的减少均优于现有的冗余加固方法。本文的优点在于取得了硬件开销和可靠性之间的平衡, 是一种有效且较易实现的 FPGA 加固方法。

参考文献(References):

- [1] Normand E. Single event upset at ground level[J]. IEEE Transactions on Nuclear Science Part 1, 1996, 43(6): 2742-2750
- [2] Baumann R C. Radiation-induced soft errors in advanced semiconductor technologies[J]. IEEE Transactions on Device

and Materials Reliability, 2005, 5(3): 305-316

- [3] Carmichael C. Triple modular redundancy design techniques for Virtex FPGA's [M]. San Jose: Xilinx, 2006
- [4] Huang K H, Hu Y, Li X W. Reliability-oriented placement and routing algorithm for SRAM-based FPGAs[J]. IEEE Transactions on Very Large Scale Integration Systems, 2014, 22(2): 256-269
- [5] Lee J Y, Feng Z, He L. In-place decomposition for robustness in FPGA[C] //Proceedings of IEEE/ACM International Conference on Computer-Aided Design. Los Alamitos: IEEE Computer Society Press, 2010: 143-148
- [6] Hu Y, Feng Z, He L, *et al.* Robust FPGA resynthesis based on fault-tolerant Boolean matching[C] //Proceedings of IEEE/ACM International Conference on Computer-Aided Design. Los Alamitos: IEEE Computer Society Press, 2008: 706-713
- [7] Huang K H, Hu Y, Li X W, *et al.* Exploiting free LUT entries to mitigate soft errors in SRAM-based FPGAs[C] //Proceedings of the 20th Asian Test Symposium. Los Alamitos: IEEE Computer Society Press, 2011: 438-443
- [8] Samudrala P K, Ramos J, Katkooori S. Selective triple modular redundancy (STMR) based single-event upset SEU tolerant

- synthesis for FPGAs[J]. IEEE Transactions on Nuclear Science Part 4, 2004, 51(5): 2957-2969
- [9] Chandrasekhar V, Mahammad S N, Muralidaran V, *et al.* Reduced triple modular redundancy for tolerating SEUs in SRAM-based FPGAs[OL]. [2015-02-12]. http://klabs.org/mapld05/papers/204_kama_paper.pdf
- [10] Pratt B, Caffrey M, Carroll J F, *et al.* Fine-grain SEU mitigation for FPGAs using partial TMR[J]. IEEE Transactions on Nuclear Science Part 1, 2008, 55(4): 2274-2280
- [11] Reorda M S, Sterpone L, Ullah A. An error-detection and self-repairing method for dynamically and partially reconfigurable systems[C] //Proceedings of the 18th IEEE European Test Symposium. Los Alamitos: IEEE Computer Society Press, 2013:1-7
- [12] de Lima Kastensmidt F G, Neuberger G, Hentschke R F, *et al.* Designing fault-tolerant techniques for SRAM-based FPGAs[J]. IEEE Design & Test of Computers, 2004, 21(6): 552-562
- [13] Rebaudengo M, Reorda M S, Violante M. A new functional fault model for FPGA application-oriented testing[C] //Proceedings of the 17th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Los Alamitos: IEEE Computer Society Press, 2002: 372-380
- [14] Zhou Fabiao, Yang Haigang, Qiu Xiaoqiang, *et al.* A technique for FPGA test configuration analysis and evaluation[J]. Journal of Computer-Aided Design & Computer Graphics, 2011, 23(10): 1672-1679(in Chinese)
(周发标, 杨海刚, 秋小强, 等. FPGA 测试配置完备性的分析评价方法[J]. 计算机辅助设计与图形学学报, 2011, 23(10): 1672-1679)
- [15] Borecky J, Kohlik M, Kubalik P, *et al.* Fault models usability study for on-line tested FPGA[C] //Proceedings of the 14th Euromicro Conference on Digital System Design, Los Alamitos: IEEE Computer Society Press, 2011: 287-290
- [16] Cong J, Minkovich K. LUT-based FPGA technology mapping for reliability[C] //Proceedings of the 47th ACE/IEEE Design Automation Conference, Los Alamitos: IEEE Computer Society Press, 2010: 517-522
- [17] Wang L T, Wu C W, Wen X Q. VLSI test principles and architectures: design for testability (Systems on Silicon)[M]. San Francisco: Morgan Kaufmann Publishers, 2006 : 45-47
- [18] Jain S K, Agrawal V D. Statistical fault analysis [J]. IEEE Design & Test of Computers, 1985, 2(1): 38-44