

# 中央处理器安全测试与自修复技术研究\*

周永忠<sup>1</sup>, 洪 晟<sup>2</sup>, 姜义初<sup>1</sup>, 顾 爽<sup>3</sup>, 李 雷<sup>1</sup>, 刘 亮<sup>1</sup>, 高欣妍<sup>3</sup>, 阴宏伟<sup>2</sup>, 岳天羽<sup>2</sup>

(1.北京智芯微电子科技有限公司 数字芯片设计中心, 北京 100192;

2.北京航空航天大学 网络空间安全学院, 北京 100191;

3.北京航空航天大学 未来空天技术学院/高等理工学院, 北京 100191)

**摘 要:** 中央处理器在工业控制领域起到重要作用, 其正常工作是工业控制中的重要稳定运行保障。主要研究中央处理器的安全测试与自修复相关技术。从故障注入到故障测试再到自修复, 对相关安全技术作了比较介绍与分类总结, 包括硬软件的故障注入技术、扫描链、内建自测试、TSV 等故障测试方法, 以及以替代修复和容错自修复技术。最后提出中央处理器安全协同模型, 对各个技术的基本原理和创新点做出归纳总结, 为未来中央处理器的故障处理技术发展提供安全设计全参考, 在保证安全和性能的同时降低成本和能耗, 助力工控设备安全稳定运行。

**关键词:** 中央处理器; 故障注入; 安全测试; 自修复; 安全协同模型

中图分类号: TN409

文献标识码: A

DOI: 10.16157/j.issn.0258-7998.222712

中文引用格式: 周永忠, 洪晟, 姜义初, 等. 中央处理器安全测试与自修复技术研究[J]. 电子技术应用, 2022, 48(9): 39-43, 49.

英文引用格式: Zhou Yongzhong, Hong Sheng, Jiang Yichu, et al. Research on integrated circuit safety test and repair technology[J]. Application of Electronic Technique, 2022, 48(9): 39-43, 49.

## Research on integrated circuit safety test and repair technology

Zhou Yongzhong<sup>1</sup>, Hong Sheng<sup>2</sup>, Jiang Yichu<sup>1</sup>, Gu Shuang<sup>3</sup>, Li Lei<sup>1</sup>, Liu Liang<sup>1</sup>,

Gao Xinyan<sup>3</sup>, Yin Hongwei<sup>2</sup>, Yue Tianyu<sup>2</sup>

(1.Beijing SmartChip Microelectronics Technology Co., Ltd., Digital Chip Design Center, Beijing 100192, China;

2.School of Cyber Science and Technology, Beihang University, Beijing 100191, China;

3.School of Future Space Technology/Higher Institute of Technology, Beihang University, Beijing 100191, China)

**Abstract:** Central processing unit(CPU) plays an important role in industrial control field. Its normal operation is an important security guarantee for industrial. This paper mainly studies the security test and self-repair technology of CPU. From fault injection, fault testing to self-healing, this paper compares and summarizes the related safety technologies, including hardware and software fault injection technology, scan chain, built-in self-testing, TSV and other fault testing methods, as well as alternative repair and fault-tolerant self-healing technologies. Finally, the CPU security cooperation model is proposed, and the basic principles and innovation points of each technology are summarized so as to provide safety reference for the development of CPU fault handling technology in the future, reduce cost and energy consumption while ensuring safety and performance, and help industrial control equipment operate reliably and stably.

**Key words:** CPU; integrated circuit; fault injection; safety test; self-repair; safety-cooperation model

## 0 引言

CPU(中央处理器)系统通常由板载集成电路驱动, 具有微型化、标准化、通用化等一系列特点。随着工业控制对设备精密度、复杂度、安全度以及功能密度要求的日益提高, 中央处理器安全技术成为工业控制芯片可靠的重要保障, 因此研究其安全测试和自修复技术具有重要意义。

当前中央处理器安全测试以及测试前的故障注入成为国内外研究的重点, 研究系统面对突发情况时的自修复技术有利于更好提高工控芯片的安全性。当前技术主要是致力于学科融合, 应用生物等领域的知识硬软件结合进行, 但各方法都有所偏重, 单独的故障处理技术无法很好地满足工业控制的安全需求。因此, 有必要建立协同各方面故障处理技术的模型来指导中央处理器的安全发展方向。

本文研究中央处理器安全测试与自修复技术的整

\* 基金项目: 国家重点研发计划(2019YFB1706001)

个流程,对不同技术进行优劣对比,最终提出了一种融合各个技术的安全协同模型,对中央处理器发展的趋势作出了总结与展望,得到有意义的结论。

## 1 中央处理器安全测试与自修复进展

### 1.1 基本概念及相互关系

对中央处理器系统进行安全测试,首先需要故障注入。故障注入从本质上来说属于一种模拟,是将错误或者错误效果注入目标系统,对系统进行模拟干预来造成故障,从而为后续的测试操作作为条件和准备;安全测试是监测系统,在故障到来时采取的应对措施,用于得到系统对于故障的内部处理机制来评估系统的容错能力;自修复技术是指中央处理器在面对某些故障时所采取的调度替代、容错、重构、冗余等一系列自我保护机制,目的是排除故障对系统运行带来的不良影响。

### 1.2 实现方式及分类

#### 1.2.1 故障注入

故障注入<sup>[1]</sup>技术是判断系统可靠性和识别敏感区域的必要条件<sup>[2]</sup>,实际应用中,可以通过硬软件配合同时实现两者的优点<sup>[3]</sup>。优缺点对比如表1所示。故障注入尚存在功能引脚限制导致的指示器激活缺陷,还需要在管脚上作进一步的技术突破<sup>[4]</sup>。

表1 传统硬软件注入技术优缺点对比

技术	优点	缺点
硬件	时间精度高,速度快,不干扰已知系统	外部插入方式破坏器件结构,数据细化度不够
软件	数据细化度高,成本低,便于灵活控制	适用时机范围窄,计算开销大,软件级操作干扰目标系统

#### 1.2.2 安全测试

传统安全测试采用增加测试点的方法,效率低、成本高、可实现性低<sup>[5]</sup>。目前主要有基于扫描链的测试、TSV非接触测试和内建自测试,超大规模的集成电路多实施内建自测试电路<sup>[6]</sup>。

Stratigopoulos<sup>[7]</sup>、Roy S<sup>[8]</sup>等提到利用ML(机器学习)故障测试,通过输入原始数据来训练机器处理和测量大量数据。电路时序复杂度、模拟电路的非离散性和参数缺失性带来的计算复杂性问题可以交给ML解决;S Jayanthi<sup>[10]</sup>、Di Natale G<sup>[11]</sup>、Dalpasso<sup>[12]</sup>等提出延迟测试技术,隐藏延迟故障传感器在上升和下降的时钟边缘采集数据,还可利用纳米技术设计开关双极器件的布尔模型,可捕捉复杂器件中逻辑的瞬时切换。

#### 1.2.3 自修复技术

传统修复技术采用可替代CLB块(可配置逻辑模块),空间开销较大。现有方法包括替代修复技术、实时容错自修复技术、AES、ASIC、BISR、基于细胞阵列的自修复技术、电压对比成像技术、贝叶斯技术、NOC容错机制和基于Mesh的路由器级容错体系等。

## 2 安全测试体系

### 2.1 故障注入技术

#### 2.1.1 硬件故障注入技术

传统的硬件注入需要附加硬件设备的帮助,安全性低,不方便试验<sup>[13]</sup>。

插入法截取输入输出信号,对高速系统时序影响大,准确度较低;探针法将探针和芯片管脚捆绑改变管脚的电流,但对BGA封装芯片无效;JTAG调试技术中,BSC(边界扫描寄存器单元)正常不参与运行,但调试模式下其各单元相接,分离内部芯片和外部管脚,在三种方法中占优<sup>[13]</sup>。

#### 2.1.2 软件故障注入技术

传统软件测试需要目标系统对于实验者处于开放状态,与某些保密领域的工作要求是矛盾的<sup>[14]</sup>。Doctor集成软件开发环境<sup>[15]</sup>使主机和目标系统依托于不同结构,用定时器随机规定时间后注入错误效应;Pin法随机插入可执行程序,随机选取内存区域或通过超时、软件陷阱、硬件异常等方法,注入错误源代码;SFIS<sup>[16]</sup>基于单粒子事件,改变原有程序,但之后代码可恢复原状。对中央处理器系统进行安全测试,首先需要故障注入。故障注入从本质上来说属于一种模拟,是将错误或者错误效果注入目标系统,对系统进行模拟干预来造成故障,从而为后续的测试操作作为条件和准备;安全测试是监测系统,在故障到来时采取的应对措施,用于得到系统对于故障的内部处理机制来评估系统的容错能力;自修复技术是指中央处理器在面对某些故障时所采取的调度替代、容错、重构、冗余等一系列自我保护机制,目的是排除故障对系统运行带来的不良影响。

### 2.2 测试技术

#### 2.2.1 基于扫描链的测试方法

陆云云<sup>[17]</sup>等提到扫描链大体可以分为两种,一种存在于芯片内部独立化元件,另一种存在于芯片的I/O端口显示板级制造缺陷,原理如图1所示。Bhavani G<sup>[18]</sup>等提到,有自修复能力的扫描结构可提高故障测试的定位范围,采用延迟测试电路等技术可减小故障测试所需的功耗。

#### 2.2.2 内建自测试电路

BIST(内建自测试方法)的核心是构建最小功能单元链以及迭代的方法,结构内部由开关、CLB以及局部连线部分组成<sup>[19]</sup>。石超<sup>[20]</sup>等提到BIST可以直接得到测试结果,核心部件由ORA(输出响应分析)、BUT(被测单元)以及TPG(测试激励生成器)三部分构成,结构流程如图2所示。成本茂<sup>[21]</sup>等还提到了CUT(Circuit Under Test),若将TPG对应的电路更换成适配于CUT的电路,会使结果输出更加便捷。

#### 2.2.3 基于群时延的TSV(透硅通道)故障非接触测试方法

TSV属于密度高,间距小的复杂高速互连结构。无

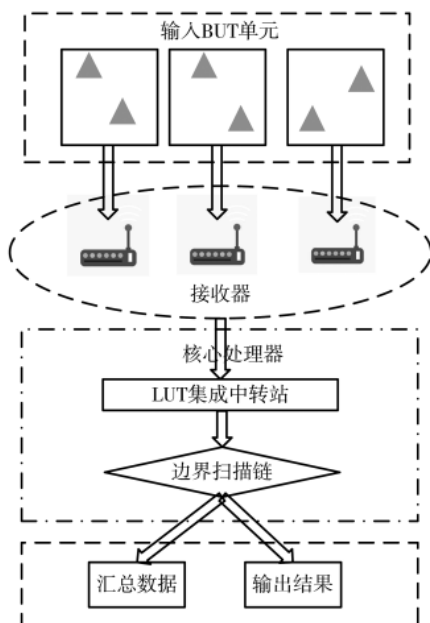


图1 边界扫描链测试方法原理

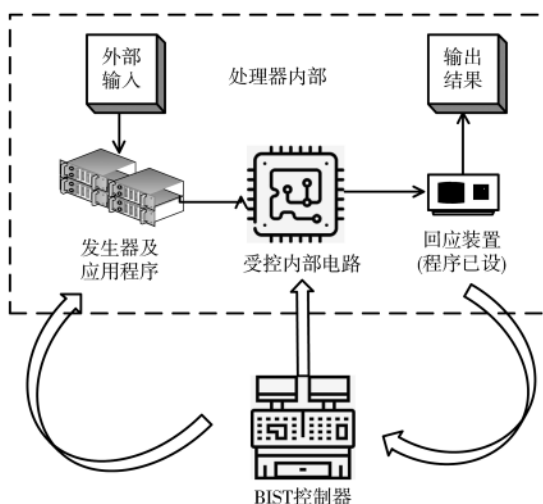


图2 内建自测试流程

探针信号可进行多音混合测试设计,通过检测器得到输入输出信号的CF值,分辨率较高<sup>[22]</sup>。Shang Yuling<sup>[23]</sup>等提出基于电特性的TSV多音混合信号模型,所用金属线功耗小,覆盖范围包括欧姆级至百万欧姆级。测试时提取并合并子测试向量,利用单卡故障模型有助于减少测试向量,从而降低VLSI测试成本<sup>[24]</sup>。不同测试技术优缺点比较如表2所示。

### 3 中央处理器自修复技术体系

#### 3.1 基于实时调度的替代修复技术

替代修复技术的起源于生物系统自修复<sup>[25]</sup>,原理如图3所示,通过划分小单元来减少故障出现时所隔离的正常单元的范围来重定位,实现了低成本,高效率<sup>[25]</sup>,但硬件资源消耗大。

基于FPGA的重构修复技术将粗粒度与细粒度划分

表2 测试技术优缺点比较

技术名称	优点	缺点
基于扫描链的测试方法	(1)可操作性强; (2)便于观察; (3)精准对点控制,避免系统因大规模错误而崩溃; (4)简化系统时序逻辑	(1)前期工作较多; (2)需要在芯片的寄存器结构之间添加接口
内建自测试电路	(1)降低测试成本; (2)提高测试效率和错误覆盖率; (3)增强服务便捷性及系统独立性	(1)附加电路结构浪费有效面积; (2)盲点存在率高
基于群时延的TSV非接触测试	(1)测试对象结构不受限制; (2)测试过程中无损伤; (4)测试电路框架灵活,测试成本低; (4)对TSV故障测试分辨率高	(1)敏感度高; (2)检测器的创建与搭建所需工作较多

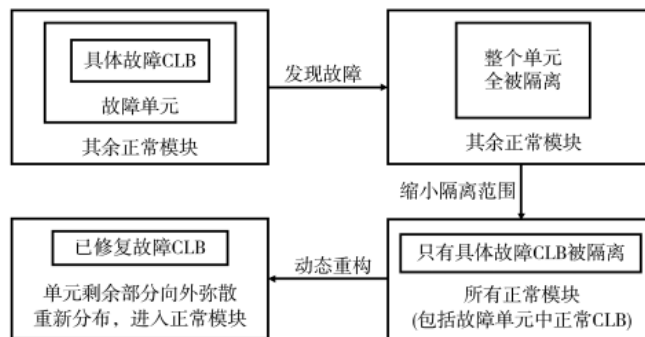


图3 实时调度自修复技术原理

相结合:只有低优先级故障时,尽可能减小隔离范围;只有高优先级故障时,使用备用模块解决;当高低优先级同时出现时,先删除部分低优先级腾出空间,再解决高优先级。

#### 3.2 实时容错自修复技术

徐伟杰<sup>[26]</sup>等提到基于SRAM型的FPGA技术,采用表决器三选二技术,只要有二个正常便不会报错,但错误逐步积累并爆发会使系统崩溃。Peña-Fernández M<sup>[27]</sup>等提到DCLS(双核锁步)进行冗余多线程支持和控制流错误检测,将两个处理器分别执行的操作步骤逐一对比,一旦出现不同步的情况便会触发报警机制。优缺点对比如表3所示。

#### 3.3 基于其他技术的自修复技术

Sheikhpour S等<sup>[28]</sup>提到AES(高级加密标准)法,包括循环码、时间、奇偶校验冗余等。Zandevakili H等<sup>[29]</sup>提到ASIC(专用集成电路结构)和BISR(内置自修复技术)。ASIC在最小延迟下,可重构基本单元自我修复后将新的路由网络替换故障部位;BISR处理永久故障,分为故障检测、故障诊断、故障隔离和冗余分配。

袁霄亮<sup>[30]</sup>等提到基于细胞阵列的自修复技术(见图4)。一个小分子工作时,其他分子处于休眠状态,总体呈动态重构,自由度、自主性提高<sup>[27]</sup>。Rahiminejad E<sup>[31]</sup>等

表 3 替代修复与容错自修复优缺点比较

技术名称	优点	缺点
基于 FPGA 的重构修复技术	(1)降低成本; (2)提高资源利用率和自修复能力; (3)增强性能	(1)消耗硬件资源量比较大; (2)实用性也相对较低
基于 SRAM 的实时容错自修复技术	(1)功耗低; (2)灵活度高,可以反复编辑; (3)容错能力强,可及时识别故障	(1)出现大规模故障时无法及时处理,导致系统崩溃; (2)单粒子效应; (3)集中式控制方式使可靠性,可控性降低
双核锁步检测技术	(1)降低成本; (2)错误检测率高; (3)方式较为宽松; (4)软件栈可实现性强	(1)(改进前)DCLS 只能检查出数据本身错误; (2)控制流错误不易检测且会产生潜在影响; (3)错误检测可能延迟

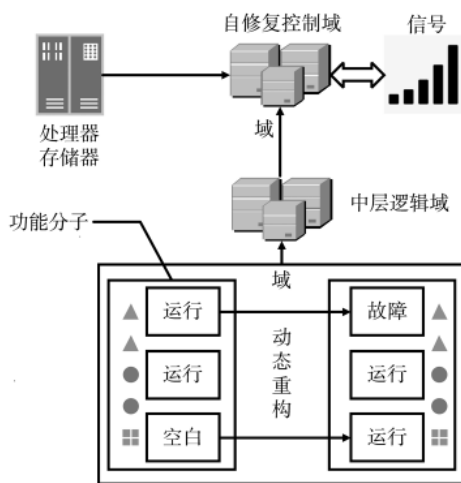


图 4 基于细胞阵列的自修复技术

提到基于神经形态的模拟集成电路,在宽频率内补偿受损突触。

Carroll R<sup>[32]</sup>等提到 IC 修复,细化识别节点后同电压对比成像结合贴合各个面;Fu W<sup>[33]</sup>等提到贝叶斯技术,以集成数据为驱动探测探针卡故障,文本转换为数字后以网络图的形式可视化;Fan W<sup>[34]</sup>等提到 NOC 内部容错机制,环面布局利用循环嵌入不完整节点;Khera V K<sup>[35]</sup>等提到基于 Mesh 的具有路由器级冗余的容错 NOC,结合重构算法和备用路由器法,每个路由器集合中可容忍一个故障路由器。

#### 4 中央处理器协同安全架构模型

综合上文对安全测试和自修复技术的研究分析,将故障注入与测试在自修复前进行来提高中央处理器安全性能,总结出如图 5 所示的安全协同结构模型。将故障注入结合 JATG 调试技术、Doctor、Pin、SFIS 可更好地提升中央处理器的安全性能。可测试设计以 TAP 为核心,根据具体情况选择芯片内部或端口的方法。对于特殊结构的封装集成电路,基本采用内建自测试电路,单粒子翻转则可用 TSV 法解决。故障修复以实时调度和实时容错自修复技术为主,结合其他领域技术进行修复也是提高性能的关键一步。

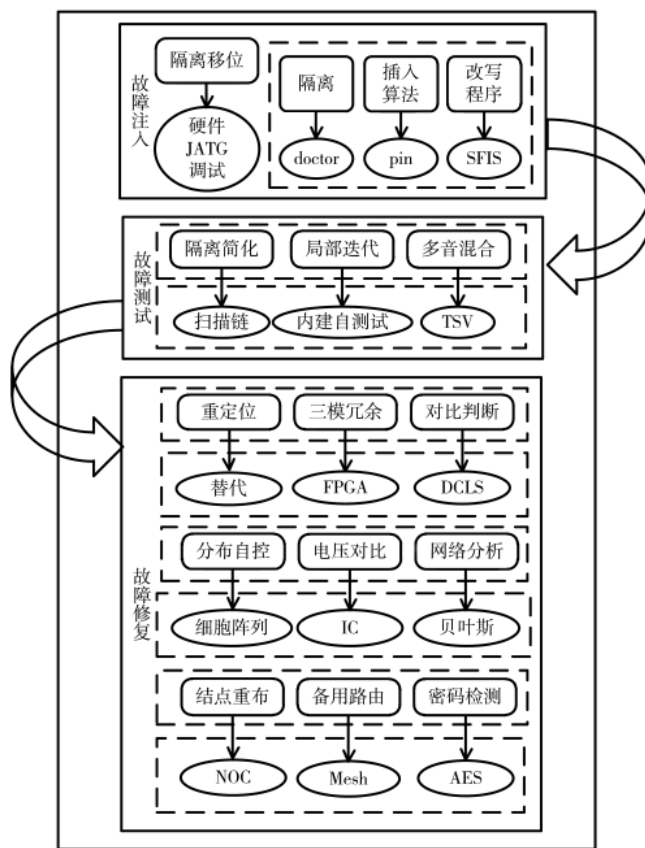


图 5 中央处理器安全协同模型

#### 5 结论

随着工业控制领域竞争日益激烈,工业控制芯片中央处理器的安全性得到广泛关注。科研工作者们发掘各种可靠测试与自修复技术模型,旨在最终提高中央处理器的安全性。现做三个方面总结:

- (1)软件和硬件结合、物理建设与模拟实验结合、设计与评价阶段结合是未来技术发展趋势。
- (2)由于硬件的物理性接触与处理器结构中微小部件的高灵敏度产生矛盾,新技术开发应以算法设计为主体。
- (3)系统容错机制的整体控制模糊性带来错误崩溃等安全隐患,采用分布式自控、精准对点、分块隔离可有效解决。



## 参考文献

- [1] 尚政国, 刘春光. 电子集成微系统技术在航空航天领域的应用[J]. 计算机科学与应用, 2017(7): 638.
- [2] ESLAMI M, GHAVAMI B, RAJI M, et al. A survey on fault injection methods of digital integrated circuits[J]. Integration, 2020, 71: 154–163.
- [3] 孙峻朝, 王建莹, 杨孝宗. 故障注入方法与工具的研究现状[J]. 宇航学报, 2001, 22(1): 99–104.
- [4] ARLAT J, CROUZET Y, LAPRIE J C. Fault injection for dependability validation of fault-tolerant computing systems[C]//The Nineteenth International Symposium on Fault-Tolerant Computing. Digest of Papers. IEEE Computer Society, 1989.
- [5] 项傅佳. 集成电路多故障测试生成算法及可测性设计的研究[D]. 哈尔滨: 哈尔滨理工大学, 2007.
- [6] HAN S, SHIN K G. Experimental evaluation of behavior-based failure-detection schemes in real-time communication networks[J]. IEEE Transactions on Parallel and Distributed Systems, 1999, 10(6): 613–626.
- [7] STRATIGOPOULOS H G. Machine learning applications in IC testing[C]//2018 IEEE 23rd European Test Symposium(ETS). IEEE, 2018: 1–10.
- [8] ROY S, MILLICAN S K, AGRAWAL V D. Special session-machine learning in test: a survey of analog, digital, memory, and RF integrated circuits[C]//2021 IEEE 39th VLSI Test Symposium(VTS). IEEE, 2021: 1–14.
- [9] WU L, RAO S, MEDEIROS G C, et al. Pinhole defect characterization and fault modeling for STT-MRAM testing[C]//2019 IEEE European Test Symposium(ETS). IEEE, 2019: 1–6.
- [10] JAYANTHY S, BHUVANESWARI M C. Delay fault testing of VLSI circuits[M]//Test Generation of Crosstalk Delay Faults in VLSI Circuits. Springer, Singapore, 2019: 15–35.
- [11] DI NATALE G, VATAJELU E I, KANNAN K S, et al. Hiddendelay-fault sensor for test, reliability and security[C]//2019 Design, Automation & Test in Europe Conference & Exhibition(DATE). IEEE, 2019: 316–319.
- [12] DALPASSO M, BERTOZZI D, FAVALLI M A. A boolean model for delay fault testing of emerging digital technologies based on ambipolar devices[C]//2018 Design, Automation & Test in Europe Conference & Exhibition(DATE). IEEE, 2018: 297–300.
- [13] 罗宗扬, 薛利兴, 左德承, 等. 基于 JTAG 的 CPU 故障注入工具的设计与实现[C]//第十四届全国容错计算学术会议(CFTC'2011)论文集, 2011.
- [14] 陆瑶. 软件注入故障的跟踪及其响应分析研究[J]. 信息与电脑(理论版), 2011(1): 36–37.
- [15] HAN S, SHIN K G. Experimental evaluation of behavior-based failure-detection schemes in real-time communication networks[J]. IEEE Transactions on Parallel and Distributed Systems, 1999, 10(6): 613–626.
- [16] 仇俊峰, 洪炳镨, 乔永强. 基于软件方法故障注入系统[J]. 哈尔滨工业大学学报, 2006, 38(6): 873–876.
- [17] 陆云云. 基于边界扫描技术实现电路板全面测试[J]. 国外电子测量技术, 2016, 35(9): 1–5.
- [18] BHAVANI G, JAMAL K, REDDY B V. Weighted pseudo-random based deterministic bist for fault testing and self-healing[C]//2019 International Conference on Communication and Electronics Systems(ICCES). IEEE, 2019: 192–197.
- [19] 吴蓬勃. FPGA 内部逻辑单元的内建自测试方法研究[J]. 信息技术与信息化, 2021(2): 143–144.
- [20] 石超, 王健, 来金梅. 基于 BIST 方法的新型 FPGA 芯片 CLB 功能测试方法[J]. 复旦学报(自然科学版), 2017(4): 488–494.
- [21] 成本茂, 黄葵, 张铜. FPGA 可编程逻辑模块的 BIST 测试方法[J]. 电子设计工程, 2016, 24(5): 152–154.
- [22] SHANG Y, ZHAO Y, LI C, et al. TSV fault contactless testing method based on group delay[J]. International Journal of Electronics, 2021, 108(9): 1570–1589.
- [23] SHANG Y, TAN M, LI C, et al. TSV manufacturing fault modeling and diagnosis based on multi-tone dither[J]. Journal of Advanced Computational Intelligence and Intelligent Informatics, 2019, 23(1): 42–51.
- [24] KHERA V K, SHARMA R K, GUPTA A K. A heuristic fault based optimization approach to reduce test vectors count in VLSI testing[J]. Journal of King Saud University-Computer and Information Sciences, 2019, 31(2): 229–234.
- [25] PRADEEP C, MADHURI E E, JOBY P P, et al. Online placement and scheduling algorithm for reconfigurable cells in self-repairable field-programmable gate array systems[J]. Computers and Electrical Engineering, 2018, 67: 836–850.
- [26] 徐伟杰, 谢永乐, 彭礼彪, 等. 基于 SRAM 型 FPGA 的实时容错自修复系统设计方法[J]. 电子技术应用, 2019, 45(7): 50–55.
- [27] PEÑA-FERNÁNDEZ M, SERRANO-CASES A, LINDOSO A, et al. Dual-core lockstep enhanced with redundant multithread support and control-flow error detection[J]. Microelectronics Reliability, 2019, 100–101: 113447.
- [28] SHEIKHPOUR S, MAHANI A, BAGHERI N. Practical fault resilient hardware implementations of AES[J]. IET Circuits, Devices & Systems, 2019, 13(5): 596–606.
- [29] ZANDEVAKILI H, MAHANI A. Built-in self-repair structure for real-time fault recovery applications[J]. Microelectronics Reliability, 2020, 111: 113726.
- [30] 袁霄亮. 基于细胞阵列结构的 FPGA 系统自修复设计研究[D]. 南京: 南京航空航天大学, 2020.
- [31] RAHIMINEJAD E, AZAD F, PARVIZI-FARD A, et al. A neuromorphic CMOS circuit with self-repairing capability[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(5): 2246–2258.

(下转第 49 页)

- [8] AL-MUSAWI L, TRAN R. The impact of EV/PHEV chargers on residential loads—A case study[C]//Transportation Electrification Conference and Expo. Detroit, 2013: 1–4.
- [9] 王增平, 赵兵, 贾欣, 等. 基于差分分解和误差补偿的短期电力负荷预测方法[J]. 电网技术, 2021, 45(7): 2560–2568.
- [10] 朱慧婷, 杨雪, 陈友媛. 电动汽车充电负荷预测方法综述[J]. 电力信息与通信技术, 2016, 14(5): 44–47.
- [11] 陈静鹏, 朴龙健, 艾芊. 基于改进贪心算法的大规模电动汽车充电行为优化[J]. 电力自动化设备, 2016, 36(10): 38–44.
- [12] 胡宇航, 皮一晨, 崔静安, 等. 电动汽车充电站负荷建模研究[J]. 电力系统保护与控制, 2017, 45(8): 107–112.
- [13] 陈静鹏, 艾芊, 肖斐. 基于用户出行需求的电动汽车充电站规划[J]. 电力自动化设备, 2016, 36(6): 34–39.
- [14] GHASNEZHAD N, FILIZADEH S. Location-based forecasting of vehicular charging load on the distribution system[C]//2014 IEEE PES General Meeting/Conference & Exposition. National Harbor, MD, USA: IEEE, 2014: 1.
- [15] 王睿, 高欢, 李军良, 等. 基于聚类分析的电动汽车充电负荷预测方法[J]. 电力系统保护与控制, 2020, 48(16): 37–44.
- [16] AZHAR U H, CARLO C, SAADANYE. Probabilistic modeling of electric vehicle charging pattern in a residential distribution network[J]. Electric Power Systems Research, 2018, 10: 126–133.
- [17] ARIAS M B, BAE S. Electric vehicle charging demand forecasting model based on big data technologies[J]. Applied Energy, 2016, 183: 327–339.
- [18] 陈丽丹, 聂涌泉, 钟庆. 基于出行链的电动汽车充电负荷预测模型[J]. 电工技术学报, 2015, 30(4): 216–225.
- [19] 张维戈, 颜飞翔, 黄梅, 等. 快换式公交充电站短期负荷预测方法的研究[J]. 电力系统保护与控制, 2013(4): 61–66.
- [20] 常德政, 任杰, 赵建伟, 等. 基于 RBF-NN 的电动汽车充电站短期负荷预测研究[J]. 青岛大学学报(工程技术版), 2014, 29(4): 44–48.
- [21] FRIEDMAN J H. Greedy function approximation: a gradient boosting Machine[J]. Annals of Statistics, 2001, 29(5): 1189–1232.
- [22] CHEN T, GUESTRIN C. XGBoost: a scalable tree boosting system[C]//The 22nd ACM SIGKDD International Conference, 2016.
- [23] 颜诗旋, 朱平, 刘钊. 基于改进 LightGBM 模型的汽车故障预测方法研究[J]. 汽车工程, 2020, 42(6): 815–819, 825.
- [24] 魏书荣, 张鑫, 符杨, 等. 基于 GRA-LSTM-Stacking 模型的海上双馈风力发电机早期故障预警与诊断[J]. 中国电机工程学报, 2021, 41(7): 2373–2383.
- [25] 刘波, 秦川, 鞠平, 等. 基于 XGBoost 与 Stacking 模型融合的短期母线负荷预测[J]. 电力自动化设备, 2020, 40(3): 147–153.

(收稿日期: 2021-11-10)

## 作者简介:

吴丹(1981-), 男, 硕士, 主要研究方向: 电力系统自动化、电力营销。

雷珽(1986-), 男, 硕士, 主要研究方向: 电力系统自动化。

李芝娟(1991-), 女, 硕士研究生, 主要研究方向: 电力系统自动化。



扫码下载电子文档

(上接第 43 页)

- [32] CARROLL R, GEER R. Fault localization in a 3D test assembly using voltage contrast imaging[J]. Microelectronics Journal, 2019, 87: 73–80.
- [33] FU W, CHIEN C F, TANG L. Bayesian network for integrated circuit testing probe card fault diagnosis and troubleshooting to empower Industry 3.5 smart production and an empirical study[J]. Journal of Intelligent Manufacturing, 2022, 33: 785–798.
- [34] FAN W, HE J, HAN Z, et al. Reconfigurable fault-tolerance mapping of ternary N-cubes onto chips[J]. Concurrency and Computation: Practice and Experience, 2020, 32(11): e5659.
- [35] CHANG Y C, GONG C S A, CHIU C T. Fault-tolerant mesh-based NOC with router-level redundancy[J]. Journal

of Signal Processing Systems, 2020, 92(4): 345–355.

(收稿日期: 2022-03-07)

## 作者简介:

周永忠(1981-), 男, 硕士, 工程师, 主要研究方向: 处理器功能安全系统方案设计与验证、处理器芯片的故障注入、故障测试技术以及自我修复方法等。

洪晟(1981-), 通信作者, 男, 副教授, 主要研究方向: 信息网络安全、集成电路安全性、复杂系统安全性, 软件安全, E-mail: shenghong@buaa.edu.cn。

姜义初(1979-), 男, 硕士, 验证工程师, 主要研究方向: CPU 核的功能安全验证, 主要是 CPU 安全验证方案的制订、验证环境的搭建以及测试点的分解等。



扫码下载电子文档

## 版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所