DOI:10.7544/issn1000-1239.20210181
59(7):1428-1438,2022

基于动态自适应冗余的现场可编程门阵列容错方法

李泽宇[1] 王 泉[1] 杨鹏飞[1] 许志伟[2] 梁金鹏[1] 高 歌[1]
[1](西安电子科技大学计算机科学与技术学院 西安 710071)
[2](中国科学院计算技术研究所 北京 100190)
(634787770@qq.com)

FPGA Fault Tolerance Based on Dynamic Self-Adaptive Redundancy

Li Zeyu[1], Wang Quan[1], Yang Pengfei[1], Xu Zhiwei[2], Liang Jinpeng[1], and Gao Ge[1]
[1](*School of Computer Science and Technology, Xidian University, Xi'an* 710071)
[2](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)

Abstract Field programmable gate array (FPGA) is extremely susceptible to failures caused by high-energy particle radiation in space, thereby affecting the normal execution of on-chip tasks. At present, the triple modular redundance (TMR) method is usually used for fault-tolerant design. Although well fault-tolerant effect can be achieved, a large amount of resource expenditure is required. Especially when the radiation level is low, the implementation of TMR method for all tasks can aggravate the above problem of high resource overhead. In view of this, a method of FPGA fault tolerance based on dynamic self-adaptive redundancy is proposed. First of all, using the high sensitivity of on-chip block RAM (BRAM) to space particle radiation, the BRAM-based radiation level monitor is designed and improved to periodically monitor the radiation level of the space environment. Secondly, slack time of execution cycle and current radiation level are standard for evaluating the reliability levels of tasks, and then a task is used as a granular for dynamic self-adaptive matching redundancy strategy under different radiation levels to ensure the successful execution of on-chip tasks while avoiding high resource overhead. Simulation results show that the FPGA with this method has high reliability under different radiation levels. Compared with the popular FPGA fault tolerance method based on redundancy, the on-chip task completion is increased by 57.2% on average under the same radiation level.

Key words field programmable gate array (FPGA); self-adaptive redundancy; fault tolerance (FT) mechanism; radiation monitoring; mission reliability

摘 要 现场可编程门阵列(field programmable gate array, FPGA)极易遭受由空间高能粒子辐射引发的故障,进而影响片上任务的正常执行.目前常采用三模冗余(triple modular redundance, TMR)进行容错设计,尽管可以取得较好的容错效果但存在资源开销大的问题.尤其当辐射水平较低时,对全部任务采用三模冗余方式执行能使上述资源开销大的问题更加严重.针对此,提出了一种基于动态自适应冗余的容错方法(fault tolerance based on dynamic self-adaptive redundancy, FTDSR).首先,利用片上块存储(block RAM, BRAM)对空间粒子辐射的高敏感性,设计改进了基于 BRAM 的辐射水平监测器,

收稿日期:2021-03-04;**修回日期**:2021-09-24
基金项目:国家自然科学基金项目(61972302);陕西省重点研发计划项目(2021ZDLGY07-01)
This work was supported by the National Natural Science Foundation of China (61972302) and the Key Research and Development Program of Shaanxi Province (2021ZDLGY07-01).
通信作者:杨鹏飞(pfyang@xidian.edu.cn)

周期性监测空间环境的辐射水平;其次,以每个任务执行周期的松弛度时间和当前辐射水平为标准评估任务的可靠性等级,进而在不同辐射水平下以单个任务为粒度动态自适应地匹配冗余策略,保证片上任务成功执行,同时避免高资源开销.仿真实验表明,采用 FTDSR 的 FPGA 在不同辐射水平下具备高可靠性,与目前主流的 FPGA 冗余容错方法相比,在同一辐射水平条件下,片上任务完成量平均提高了 57.2%.

关键词 现场可编程门阵列;自适应冗余;容错机制;辐射监测;任务可靠性

中图法分类号 TP302.8

FPGA 具有低功耗、高并行、深度灵活可定制的特性,非常适合执行空间应用中的计算任务.但是,由于其配置位易翻转的特性,容易受到来自太空环境中高能粒子的冲击而产生单粒子翻转(single event upset, SEU)故障[1],从而影响片上任务的成功执行.近年来,随着 FPGA 制程工艺尺寸的缩小,器件面临加速老化问题的同时也增加了这种故障发生的概率[2],必须减轻或修复这些故障以获得可靠的操作.

目前,针对 SEU 容错的方法大致分为 2 类:基于制造工艺的容错技术和基于设计的容错技术.制造工艺容错主要是从工艺设计方面来提高器件的容错性能,一般多为对产品的封装材料或单元结构进行抗辐射设计,增强器件对辐射的屏蔽功能.目前常用的方法是利用硅技术(silicon on insulator, SOI)工艺加固 FPGA[3],或在部分工程实践中直接采用抗辐射器件进行太空应用,例如使用 XILINX 公司针对航天应用特别研制的 Virtex-4QV FPGA 或反熔丝 FPGA[4-5].尽管这种方法可以从工艺层面上提高器件抗辐射性能,但其工艺制造技术要求高、代价高昂,随着集成电路尺寸越来越小,工艺加固一旦失效就会导致整个电路的逻辑功能失效,且无法自动修复,严重时导致整个 FPGA 失效,造成巨大损失.

基于设计的容错技术主要是纠错码(error correcting code, ECC)和三模冗余.ECC 算法大多采用奇偶校验码或汉明码,可以检错并修正单个配置位翻转,但无法屏蔽故障和修复其他软故障[6].而三模冗余(triple modular redundance, TMR)针对故障具有广泛的容错能力,降低了单个功能模块对 SEU 的敏感性,但代价是使资源用量增加了 200%[7].同时,太空环境中 SEU 的异常率很少达到需要 TMR 的水平,从 2010—2019 年,要求进行 TMR 的粒子通量水平(例如太阳粒子事件)的出现时间仅为 6.9%[8],这使得单一利用 TMR 进行容错造成的资源开销问题更加严重.有研究提出可以根据辐射水平的变化动态改变片上所有任务的冗余方式[9],尽管这在一定程度上缓解了高可靠性依赖资源开销过度的问题,但却没有考虑到任务可靠性要求的差异.如果可以以单个任务为粒度进行动态自适应容错,那么将进一步缓解为保障可靠性而带来的高资源开销问题.

为了解决高可靠性依赖资源开销过度的问题,本文提出了一种基于动态自适应冗余的容错方法(fault tolerance based on dynamic self-adaptive redundancy, FTDSR).基于动态可重构特性,FPGA 片上可编程区域被设计为自适应资源,使其能够实现 N 个动态调整可重构模块,以构造单模、双冗余,三模冗余等容错执行方式.同时,利用片上块存储(block RAM, BRAM)对单粒子效应的高度敏感性,将片内 BRAM 内嵌块作为辐射水平监测器,用于感知单粒子翻转.设计的基于 BRAM 的辐射水平评估模块,包括多个基于 BRAM 的辐射监测器(BRAM 监测器)、故障统计单元和故障计算单元.BRAM 监测器实时监测所有发生的 SEU,利用计数器统计数值并写入故障统计单元,同时采用自带的 ECC 刷新器修正翻转位,缓解 BRAM 中的 SEU.故障计算单元周期性地读取故障统计单元的内容,计算当前故障翻转率并传输给控制单元.控制单元评估当前的辐射水平,并结合每个任务执行周期的松弛度时间来判断各个任务需要采取的冗余方式.控制单元控制自适应系统的动态可重构控制器,通过可编程资源的内部配置访问端口 PCAP,将部分比特流文件配置到对应的可重构区域中,实施高可靠的执行方式,总体方案架构如图 1 所示.

本文主要贡献包括 3 个方面:

1) 改进了一种基于片上 BRAM 的外部辐射水平监测器,使得片上 BRAM 资源在满足用户逻辑功能的同时具备辐射监测功能,从而可以最大化地构造辐射监测器,增加辐射监测密度进而提高辐射水平评估的准确性.

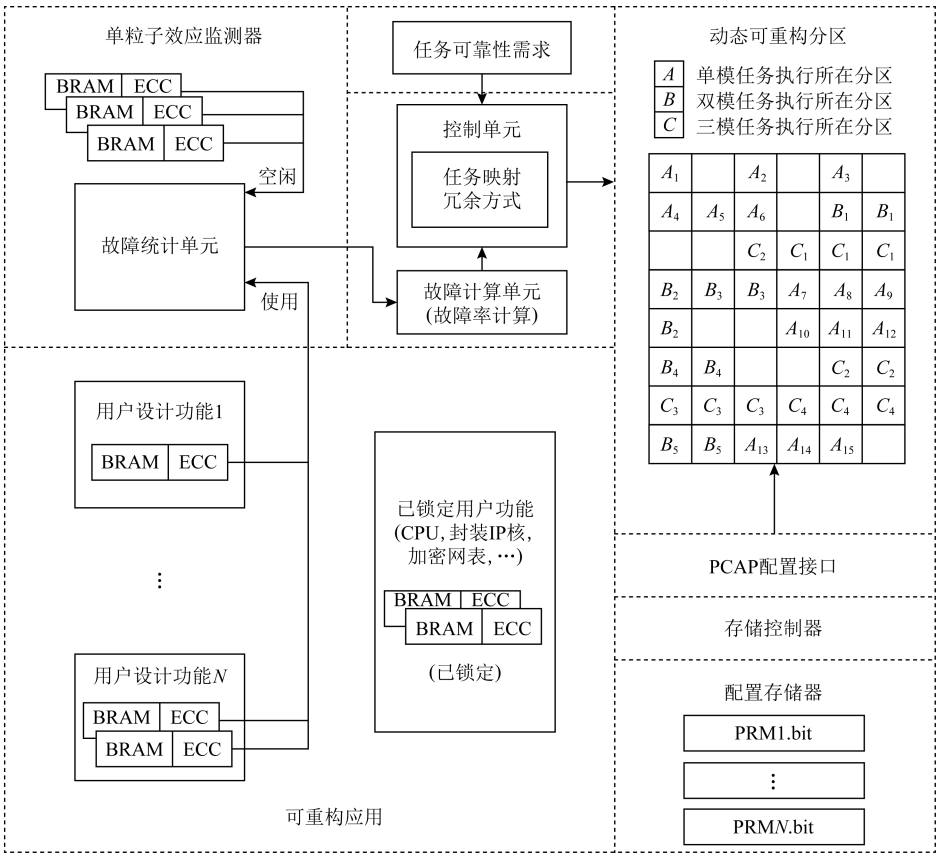


Fig. 1 Dynamic self-adaptive fault tolerance architecture diagram of the tasks on FPGA chip

图 1 FPGA 片上任务动态自适应容错架构图

2) 提出了一种以单个任务为粒度的可靠性评估策略,以任务执行周期的松弛度时间进行可靠性等级判定,并进一步在满足任务可靠性要求的前提下对资源用量进行优化,实现了针对单个任务在当前辐射水平下的可靠性评级,同时提高了片上资源利用率.

3) 基于自适应容错思路,动态评估辐射水平变化时任务的可靠性等级,在满足资源和可靠性条件下实现每个任务冗余架构的动态调整,以适应不同辐射水平下各个任务的容错要求.

1 相关工作

FPGA 片上容错相关技术主要基于冗余、配置刷新和动态可重构等.冗余包括三模冗余、双机冷/热备份、时间冗余等,其中最有代表性的就是三模冗余及其改进技术,该架构具备故障检测和故障屏蔽的功能,在故障发生后可以确保任务的不间断执行,满足任务的实时性要求,但代价是资源的严重浪费[8].配置刷新技术是可编程器件广泛应用的容错手段,因其具备可重新配置的特性,可以在软故障发生后重写比特流,从而恢复任务的正常功能[10].近年来,伴随着 FPGA 部分动态可重构功能(dynamic partial reconfiguration, DPR)的发展和逐步实现,可以实现片上资源的动态复用,为 FPGA 片上容错技术的发展提供了更为先进的方法.将 DPR 与冗余、配置刷新等传统的容错技术相结合,可以克服原有技术的不足,更好地实现细粒度的冗余和部分动态的配置刷新,在满足容错的同时节约资源并满足任务实时性要求[11].

值得关注的是,FPGA 基于部分动态可重构功能,可以根据运行环境的变化加载具有不同冗余结构的执行方式,这种方法称为自适应故障缓解(adaptive error mitigation, AEM)[12].文献[13-14]介绍了 FPGA 自适应故障缓解方法,但它们没有分析系统在辐射环境中的可靠性,也没有考虑评估辐射水平.文献[15-16]提出利用片外监测器对辐射进行监测,代价是增加了体积和功耗,并且没有提出对任务进行自适应容错设计.文献[9]提出根据外部环境变化自适应地调整可编程器件的冗余方式,但该

方法采用了粗粒度的容错方式,仅考虑将片上任务全部部署为一种冗余方式,如双模备份和三模冗余.文献[9,12-16]的研究没有考虑任务对可靠性要求的差异,简单采用统一的冗余方式会造成严重的资源浪费,甚至由于资源限制造成计算性能低下并降低系统可用性.针对该问题,从每个任务的可靠性要求出发,结合外部辐射水平进行容错冗余设计,兼顾实现了任务的高可靠性、高时效性和片上资源的高利用率.

2 SEU 辐射水平评估

2.1 基于 BRAM 的辐射水平监测器

辐射水平采用 BRAM 监测器进行监测评估.基于 BRAM 对 SEU 高度敏感的特性,将片内 BRAM 内嵌块作为 SEU 监测器的核心部分,用于感知单粒子翻转.同时,XILINX 公司的 BRAM 可以开启自带的 ECC 校验功能,纠正任意单位翻转故障或监测任意双位翻转故障[17],这样可以将所发生的翻转故障进行记录.

片上 BRAM 主要分为 3 种:锁定 BRAM、未使用 BRAM 和已使用 BRAM.其中,锁定 BRAM 一般存在于锁定的 IP 核和嵌入式微处理器中,无法访问修改不能作为辐射监测器使用.已有的方法仅采用未使用 BRAM 作为辐射监测器[18],这样整个片上的辐射监测器数量就会受到极大的限制,而辐射监测器的密度直接影响对外部辐射水平评估的准确性.当选取少量 BRAM 配置为监测器时,无法保证辐射水平评估的准确性;而选取大量 BRAM 配置为监测器又会影响用户逻辑功能的实现.

为了既保证辐射水平评估的准确性,又使得更多的 BRAM 资源用于配置用户逻辑功能,本文改进了现有的 BRAM 监测器.配置开启 BRAM 真双端口结构,一个端口用于配置用户逻辑功能,它与不带 ECC 的非擦除 BRAM 资源有相同的功能,可在 1 个周期内执行读取和写入操作;另一个端口用于连接故障统计单元,这样可以并行执行故障统计和常规 BRAM 访问.同时,在 BRAM 内部配置了清理、纠错和计数器单元,用于辐射监测并校正翻转故障.其中的 ECC 是实时执行的,可以将所有翻转次数累加到计数器,并将统计的数值单独输出到故障统计单元.通过这种设计,一个完整的 BRAM 监测器可以在实现用户逻辑功能的同时对翻转故障进行监测和计数,这样可以最大化地生成整个 FPGA 片上的辐射监测器数量,保证辐射水平评估的准确性.

2.2 辐射水平评估方案

BRAM 监测器是辐射水平评估中的核心器件,同时还包括故障统计单元和故障计算单元,整体 SEU 辐射评估功能模块如图 2 所示:

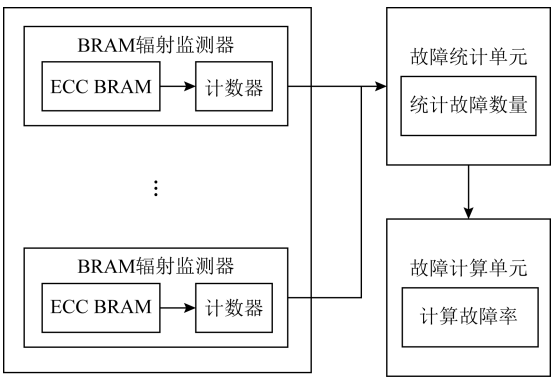
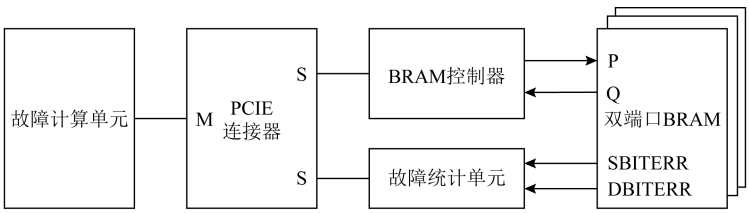


Fig. 2 Radiation evaluation function module diagram

图 2 辐射评估功能模块图

BRAM 监测器分布在片上动态可重构区域,故障统计单元位于静态区域,故障计算单元部署在上位机,BRAM 监测器需要被 BRAM 控制器进行管理调用,故障统计单元和故障计算单元通过 PCIE 总线进行通信,整体连接示例如图 3 所示.

监测周期为 1 次单事件效应(single event effect, SEE)周期,BRAM 监测器在设定周期内实时监测 SEU 并在计数器中累计发生的粒子翻转次数(1 次



注:① P为读取端口,Q为写入端口;② SBITERR为单位故障统计端口,DBITERR为双位故障统计端口.

Fig. 3 Example wiring diagram of radiation evaluation of dual-port BRAM module

图 3 双端口 BRAM 模块的辐射评估示例连线图

单位或双位翻转只计数 1 次,1 个周期内如发生多次翻转进行累加),完成 1 个统计周期后,BRAM 监测器将这些计数器的值写入故障统计单元.每个辐射监测器带有 ECC BRAM 刷新器,如果是单位 SEU,在向计数器累加计数的同时会自动校正翻转,缓解 BRAM 中的故障.故障统计单元在 1 个统计周期完成后将所有 BRAM 监测器中监测的故障数量传输到故障计算单元.故障计算单元放置在上位机端进行故障翻转率计算并以最坏情况评估片上可重构分区可能发生故障的数量,并将结果输送到总控制单元,为自适应调整任务的冗余方式提供依据.

辐射水平强度用位翻转数 P_{bu} 表征,其指一次 SEE 周期内发生单/多位翻转的总数 B_{SEE} 与所有 BRAM 监测构成总的位数 B_{all} 的比值,再乘以 10^6 量化为每 Mb 下发生翻转的数量,单位是 FIT/Mb,表示可编程器件工作 1 个 SEE 事件周期中每 Mb 存储位发生位翻转的数量[19],具体公式为:

$$P_{\mathrm{bu}}=B_{\mathrm{SEE}}/B_{\mathrm{all}}\times 10^6. \tag{1}$$

3 任务可靠性等级评估策略

3.1 预评估策略

任务的可靠性评估策略是对每个片上任务的可靠性等级进行分级,这是实现以单个任务为粒度自适应匹配冗余方式的前提.假设一次 SEE 中,各个任务对应的执行区块内发生故障的次数不大于一次,假定所有任务实现一次故障后容错,满足可靠性要求体现为任务在截止时间前成功执行,因此可以以任务执行周期的松弛度时间作为可靠性等级的判别条件.据此将任务的可靠性级别设定为 3 个等级,分别是实时可靠性级别(A 类,松弛度时间为 0)、低延时可靠性级别(B 类,松弛度时间小)和高延时可靠性级别(C 类,松弛度时间大).实时容错级别的任务满足故障屏蔽、一次故障后任务不间断的要求;低延时容错级别的任务不具备故障屏蔽的能力,在故障后的较短时间内恢复并继续执行任务;高延时容错级别的任务则是在故障后允许一定时间间隔再继续执行任务.为满足设定的可靠性要求,它们对应的冗余方式分别是三模冗余、双模冗余和单模执行.

此外,任务类型明确规定是实时容错级别的任务,其必须满足故障屏蔽和一次故障后任务不间断的要求,对应的冗余方式直接采用三模冗余.没有明确给定任务类型,就需要采用可靠性评估策略对任务进行分级.为了进一步推导可靠性评估策略,引入任务失效时间和松弛度时间的概念,如图 4 所示:

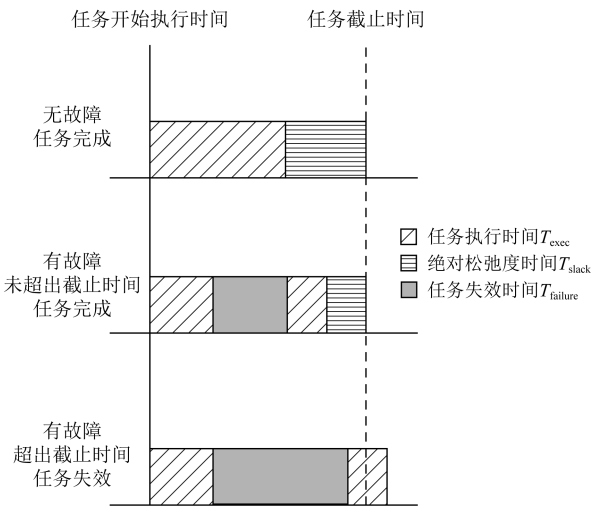


Fig. 4 The execution schedule of a task under the three different conditions

图 4 任务在 3 种不同情况下的执行时间表

正常情况下,任务的最长可执行周期时间等于任务执行时间加松弛度时间,即

$$T_{\mathrm{exec\_cycle}}=T_{\mathrm{exec}}+T_{\mathrm{slack}}, \tag{2}$$

其中,$T_{\mathrm{exec\_cycle}}$ 为任务的最长可执行周期,T_{exec} 为任务的正常执行时间,T_{slack} 为松弛度时间.当有故障出现时,松弛度时间可用于处理故障,但是当松弛度时间小于故障处理时间就会使得任务的实际完成时间超过任务的截止时间,会破坏用户体验甚至造成严重的事故风险.此处任务故障后的处理时间定义为任务失效时间:

$$T_{\mathrm{failure}}=T_{\mathrm{F}}+T_{\mathrm{wait}}, \tag{3}$$

其中,T_{F} 表示故障后必要的容错时间,T_{wait} 表示监测到故障后可重构管理模块对其进行处理前的等待时间.判断 T_{slack} 与 T_{failure} 的大小关系是对任务进行可靠性分级的关键,目的是使得任务失效时间小于任务松弛度时间,旨在保障任务的成功执行.其中 T_{slack} 对于每个任务来说是个定量,而 T_{failure} 则与该任务采取的冗余方式和系统整体运行情况相关.冗余方式直接关系到容错时间开销,系统运行所处的辐射环境及处理器执行时间都会影响到故障处理所需的等待时间,本文不考虑可重构模块本身的通信延时和开销,则 T_{wait} 由当前故障模块的数量和全体任务的冗余执行方式决定.任务未分级时对应的匹配方式无法确定,此时 T_{wait} 只与故障模块的数量有关,其中故障模块的数量直接受到外部辐射强度的影响.

对于三模冗余方式来说,一次故障后任务不间断,即 $T_F=0$,可以不立即对故障进行修复,此处 $T_{wait}=0$;对于双模热备份,考虑故障模块定位的时间,T_F 等于故障定位时间 T_L,需要通过可重构管理模块进行比特流回读故障定位,此处 T_{wait} 为等待可重构管理模块处理的时间;当采用单模执行时,T_F 包括任务恢复时间 T_{rec} 和执行状态复位时间 T_{rs},由于需要通过可重构管理模块对功能进行重配置,此处 T_{wait} 为等待可重构管理模块处理的时间.

T_{wait} 与当前的故障模块数量相关,按最坏情况考虑,如果有大量的故障模块需要处理,则假设某个故障模块会等待之前故障模块全部处理完成后才得到处理,故障模块的数量与所处工作环境辐射强度直接相关.工作环境中影响任务执行可靠性的因素主要是辐射,不同辐射强度基于片上 BRAM 块单粒子翻转率进行统计,由于 BRAM 对单粒子效应的高敏感性,将 BRAM 内嵌块作为监测器,用于感知单粒子翻转.

若采用的 FPGA 配置存储位容量为 a(单位为 Mb),位翻转数 P_{bu} 为 λ(单位为 FIT/Mb),可编程器件的敏感单元所占比例为 μ,那么该配置区块内出现软故障(soft error rate, SER)的数量为

$$C_{SER}=a\lambda\mu. \tag{4}$$

在得到 C_{SER} 后,按照最坏情况估计一次 SEE 造成的故障分散发生在不同分区,则 T_{wait} 进一步量化为

$$T_{wait}=(\lceil C_{SER}\rceil-1)\times T_{conf}, \tag{5}$$

其中,C_{SER} 向上取整表示最大可能发生的故障数量,T_{conf} 为模块平均重配置时间.如果任务执行周期内的时间满足关系:

$$T_{wait}+T_{rec}+T_{ls}\leqslant T_{slack}, \tag{6}$$

那么该任务可靠性级别为高延时可靠性级别.如果不满足式(6),检查其截止时间是否满足:

$$T_L+T_{wait}\leqslant T_{slack}. \tag{7}$$

如果该任务满足式(7)时序,那么该任务属于低延时可靠性级别;如果该任务时序要求不满足式(7)或任务类型设定为实时可靠性级别,那么该任务分类为实时可靠性级别.

3.2 评估策略优化

3.1 节中所述的方法策略初步实现了任务的可靠性分级,但当前任务分级后对应匹配的冗余方式可能会影响实际的等待时间,T_{wait} 可能会随着匹配三模冗余方式执行任务的数量增加而降低,部分任务的可靠性等级也可能发生改变.基于此,本文提出优化匹配算法(optimize matching strategy, OMS)对预评估策略进行优化,在满足任务可靠性的前提下进一步优化任务的可靠性等级,从而改变部分任务匹配的冗余执行方式以降低总体资源开销,优化匹配算法的伪代码如算法 1 所示:

算法 1. 优化匹配算法 OMS.

输入:初始任务集 Φ($\Phi=\Phi_A\cup\Phi_B\cup\Phi_C$,其中 Φ_A,Φ_B,Φ_C 分别表示 A 类、B 类、C 类任务集合,$\Phi_A=\{task_A(i)\}$,$\Phi_B=\{task_B(j)\}$,$\Phi_C=\{task_C(k)\}$,i,j,$k=1,2,\cdots$)、初始资源量 R($R=3\times\Phi_A.size()+2\times\Phi_B.size()+\Phi_C.size()$)、位翻转数 λ;

输出:优化后的任务集 Φ'、优化后的资源量 R'.

① $max=a\lambda\mu$; /* 计算当前辐射条件下可能发生的最大故障数量 */

② $N=\Phi_B.size()+\Phi_C.size()$; /* 计算当前执行双模和单模冗余的任务数 */

③ if $N<max$ do /* 判断需要容错等待的任务数和最大故障数量的关系 */

④ $T_{wait}=T_{conf}\times(max-N-1)$; /* 重新计算等待时间 */

⑤ $List_B[]=Sort(\Phi_B.T_{slack})$; /* B 类任务按照松弛度时间大小降序排列 */

⑥ $List_C[]=Sort(\Phi_C.T_{slack})$; /* C 类任务按照松弛度时间大小降序排列 */

⑦ loop do /* 遍历 B 类任务中是否存在可以降级的任务 */

⑧ if ($List_B[i].T_{slack}>T_{wait}+T_{rec}+T_{rs}$) do

⑨ $task_B(i)\rightarrow task_C$;

⑩ if $i==last-1$ do /* 判断是否 B 类任务的最后一个 */

⑪ loop do /* 遍历 A 类任务中是否存在可以降级的任务 */

⑫ if ($List_C[j].T_{slack}>T_{wait}+T_L$) do

⑬ $T_{wait}=T_{conf}\times((max-N-1)++)$;

⑭ if $re\text{-}calculation()=1$ do /* 判断所有任务的可靠性是否满足要求 */

⑮ $task_A(j)\rightarrow task_B$;

⑯ if $j==max-N$ do /* 判断是否达到辐射造成故障的初始块数 */

⑰ return $\Phi_A\rightarrow\Phi_{A'}$,$\Phi_B\rightarrow\Phi_{B'}$,$\Phi_C\rightarrow\Phi_{C'}$; /* 更新 A 类、B 类、C 类任务集合并输出 */

```
⑱          return R′=3×Φ_A′.size()+
              2×Φ_B′.size()+Φ_C′.size();
              /* 更新总的资源量并输出 */
⑲         else do
⑳          j++;
㉑         end if
㉒        else do
㉓         break;
㉔        end if
㉕       else do
㉖        break;
㉗       end if
㉘      end loop
㉙     else do
㉚      i++;
㉛     end if
㉜    else do
㉝     break;
㉞    end if
㉟  end loop
㊱  return Φ_B→Φ_B′, Φ_C→Φ_C′; /* 更新 B 类、
      C 类任务集合并输出 */
㊲  return R′=3×Φ_A.size()+2×
      Φ_B′.size()+Φ_C′.size();
      /* 更新总的资源量并输出 */
㊳ else do
㊴  break;
㊵ end if
```

预设定任务的可靠性级别后，将重新计算目前分级匹配策略下的故障处理等待时间 T_{wait}，该时间不只与辐射水平相关，也与采用三模冗余的任务数量相关，因为以三模冗余执行的任务不需要故障后立即处理，间接影响了 T_{wait}.当 T_{wait} 减小后，其中某些任务的可靠性等级可以考虑降级，从而减少总体资源，达到优化资源的目的.算法 1 的行①计算当前辐射水平下可能发生的最大故障数 max；行②将预评估策略的双模和单模执行任务数相加得到 N，N 和 max 共同决定了 T_{wait} 是否发生变化；行③～㊲是 T_{wait} 发生变化后的优化过程，其中行④重新计算了 T_{wait}，行⑤⑥分别对 B 类、A 类任务按照各任务的 slack 进行排序，保证拥有较大 slack 的任务先考虑降级；从行⑦开始，对所有 B 类任务重新进行级别判断，由于先执行 A 类任务降级会再次改变 T_{wait} 值，因此从 B 类任务优先开始.如果 B 类任务满足式(6)的时序关系，则将 B 类任务降级为 C 类任务，然后依次对 B 类任务判别，其中只要有一个 B 类任务不满足式(6)的时序，则跳出循环，同时将 B 类、C 类任务集更新并输出更新后的资源总量，算法结束.如果全部 B 类任务满足式(6)的时序，则从行⑪开始对 A 类任务进行判别，依次看 A 类任务是否满足式(7)的时序关系，注意每当一个 A 类任务满足式(7)的时序时，并不先将其转换成 B 类任务，因为每一个 A 类任务的减少也可能会影响到 T_{wait} 值，此时需要重新计算 T_{wait} 值.观察当前 T_{wait} 值是否满足其他任务的可靠性要求，如果满足则对当前 A 类任务降级，如果不满足则跳出循环，同时更新 A 类、B 类、C 类任务集并输出更新后的资源总量，算法结束.如果 A 类任务依次满足式(7)的时序关系并顺利降级，则当 A 类任务遍历到第 j 个时(j 值等于辐射造成故障的初始块数)，跳出循环，更新 A 类、B 类、C 类任务集并输出更新后的资源总量，算法结束；行㊳㊴是 T_{wait} 未发生变化的情况，当前不需要对预分级结果进行优化.

3.3 示例分析

设定 FPGA 片上动态可重构分区数量为 25 个，$T_{conf}=5$ s，$T_{rec}=T_{rs}=T_L=3$ s.共有 10 个任务，其中任务类型属于实时容错级别的任务有 2 个，直接选择三模冗余的方式执行，其余任务的松弛度时间分别是 10 s，15 s，15 s，20 s，20 s，30 s，30 s，30 s.设定当前辐射强度最大可影响分区数量是 3 个，根据本文的式(5)可以计算出 $T_{wait}=10$ s.将 T_{rec}，T_{ls}，T_L，T_{wait} 分别代入式(6)(7)，经过计算和汇总得到 A 类任务数为 3，B 类任务数为 2，C 类任务数为 5.将 A 类、B 类、C 类输入算法 1，当前资源需求是 18 个动态可重构分区，判断得到当前任务执行方式不影响实际等待时间，A 类、B 类、C 类任务的数量不变.当辐射强度增强，设定当前辐射强度最大可影响分区数量是 5 个，根据本文的式(5)，可以计算出 $T_{wait}=20$ s.将 T_{rec}，T_{ls}，T_L，T_{wait} 分别代入式(6)(7)，经过计算和汇总得到 A 类任务数为 7，B 类任务数为 0，C 类任务数为 3.将 A 类、B 类、C 类输入算法 1，当前资源需求是 24 个动态可重构分区，判断得到当前任务执行方式会影响实际等待时间，此时最多影响 3 个任务的等待时间，经过算法优化得到 A 类任务数为 6，B 类任务数为 1，C 类任务数为 3，此时资源需求是 23 个动态可重构分区，在保证相同可靠性的前提下节约了资源.

4 实验验证与分析

4.1 实验方案设计

实验首先验证了 BRAM 监测器数量与辐射水平评估准确性的关系,旨在证明利用改进 BRAM 监测器的方式可以在片上最大化地构造监测器,以提高对外部辐射水平评估的准确性;其次验证了所提出的 FTDSR 针对 FPGA 在辐射水平变化条件下的可靠性,可保证任务完成的情况,并与目前常用的 4 种片上容错方法[14,16,20]进行对比:

1) 全任务的自适应方法(F-Strategy).片上所有任务随辐射条件的变化而改变运行方式,在辐射水平正常情况下采用单模方式运行,在辐射水平较坏情况下采用双模方式运行,在辐射水平最坏情况下采用三模方式运行.

2) 全三模冗余方法(S-TMR).无论何种辐射水平,片上任务均采用三模冗余方式运行.

3) 全双模热备份方法(S-DWC).无论何种辐射水平,片上任务均采用双模热备份方式运行.

4) 全无冗余方法(S-NOR).无论何种辐射水平,片上任务均采用单模方式运行.

为了确保实验的可重复性,使用仿真实验来评估上述 4 种片上容错方法.仿真实验代码采用 Python 语言编写,运行环境采用 x86-64 位 Windows 10 操作系统,硬件配置为 i7-9750H CPU @2.6 GHz,16 GB 内存容量.值得注意的是,本文改进的 BRAM 辐射监测器和任务冗余结构的动态变换均已经在 Z-7010-XC7Z010 片上实现.为了进一步量化实验结果,选取 2 个指标进行对比:

1) 可靠性.辐射水平动态变化情况下,容错方法保证片上任务成功完成的概率.

$$Reliability = 1 - \gamma\mu, \tag{8}$$

其中,γ 是辐射故障率,μ 是容错冗余策略不满足任务可靠性级别的任务数量与全部任务数量的比值.

2) 任务完成量(amount of tasks completion, ATC).片上资源量给定时,容错方法在理论条件下确保最多可以完成的任务数量.

为了证明实验的有效性并符合现实情况,选取 Benchmark 常用基准中的任务 B_1 到 B_{20} 作为基准任务[21],并在此基础上对任务的类型、执行时间和截止时间等参数进行不同的设置,共生成 100 个实验任务,将其分为 10 个集合(组),每个集合有 10 个任务.实验设计了 3 个不同等级的辐射强度,分别是正常辐射强度、较坏辐射强度和最坏辐射强度.每个集合的实验仅更改一个变量,同时保持其他参数不变,采用不同的任务集运行 10 次取平均结果.

4.2 实验结果与分析

基于未使用 BRAM 和已使用(未锁定)BRAM 构造片上监测器,一个 BRAM 监测器可以覆盖 36 Kb 的块,Z-7010-XC7Z010 器件 PL 端共包含 2.1 Mb(60 个 BRAM)容量的 BRAM 资源,最多可以配置 60 个 BRAM 监测器.表 1 表明了 SEU 检测率与片上监测器的数量呈正相关关系,监测器数量越多,检测率就越高.基于改进方法,PL 端配置位在未大量使用锁定 IP 核的情况下可以最大化实现片上监测器,意味着可以通过评估监测器信息较为准确地评估当前辐射水平,从而为自适应容错提供必要的参考.同时,由于监测器工作基本不影响用户功能的实现,因此几乎不会额外造成片上资源的浪费.

Table 1 SEU Detection Rate of BRAM-Based Radiation Monitors in Different Radiation Modes

表 1 不同辐射强度下基于 BRAM 辐射监测器的 SEU 检测率

辐射强度	监测器个数	监测位/Mb	注入 SEU 个数	检出 SEU 个数	检测率/%
正常辐射强度	20	0.72	150	47	31.3
正常辐射强度	40	1.44	150	98	65.3
正常辐射强度	60	2.10	150	150	100.0
较坏辐射强度	20	0.72	600	205	34.2
较坏辐射强度	40	1.44	600	401	66.8
较坏辐射强度	60	2.10	600	600	100.0
最坏辐射强度	20	0.72	1 200	397	33.1
最坏辐射强度	40	1.44	1 200	812	67.7
最坏辐射强度	60	2.10	1 200	1 200	100.0

表 2 反映了不同容错方法具备的功能,分别从容错能力(fault tolerance capability, FTC)、辐射

Table 2 Functional Characteristics of Different Fault Tolerance Methods

表 2 不同容错方法的功能特性

方法	FTC	REF	DAF
FTDSR	√	√	√
F-Strategy	√	√	√
S-NOR			
S-DWC	√		
S-TMR	√		

注:"√"表示方法具备该功能.

水平评估功能(radiation level evaluation function, REF)和动态自适应容错功能(dynamic adaptive fault tolerance function, DAF)等方面进行比较.可以看出 FTDSR 方法相比 S-NOR,S-DWC,S-TMR 具备更多容错相关功能.尽管 F-Strategy 也具备相同的功能,但其无法满足单个任务对可靠性的要求并通常造成额外的资源浪费.

不考虑片上资源限制,不同容错方法可提供的可靠性随着辐射水平加剧的变化情况,如图 5 所示.其中,FTDSR 和 S-TMR 在所有辐射条件下均可以 100%地保证任务成功执行,但其根本原因不同,图 5 中 2 个线条重叠且位于纵轴最大值.S-TMR 对所有任务采用三模冗余执行,可以保证在不同辐射水平下所有任务的可靠性要求;FTDSR 则是根据每个任务对可靠性的要求在不同辐射水平下动态调整冗余方法,从而保证所有任务的成功执行.F-Strategy 由于在正常辐射水平和较坏辐射水平下分别采用单模和双模冗余执行任务,有一定的概率会导致任务的失败;而在最坏辐射水平下,对全部任务均采用了三模冗余执行,所以可靠性达到了 100%.S-DWC 和 S-NOR 的可靠性会随着辐射水平的加剧而进一步下降,尤其是 S-NOR 在最坏辐射水平时只能保证不高于 80%的任务成功执行,这是由于随着辐射水平的加剧会引发更多的故障并在短期内无法对所有故障任务进行容错,进而导致任务执行失败.

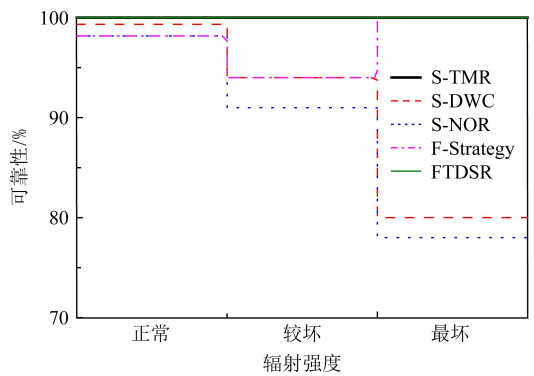


Fig. 5 Reliability provided by various strategies under different radiation levels

图 5 不同辐射水平下不同策略的可靠性

不同容错方法在不同辐射水平条件下执行任务需要的资源开销,如图 6 所示.可以明显看出 S-TMR 方法所需的资源量是最大的,这是为保证任务的高可靠性付出的资源代价,相比较来看,FTDSR 在提供相同可靠性的前提下只需要 S-TMR 策略平均 60%的资源开销,足以证明自适应冗余方式的优势.辐射强度在正常和较坏水平时,FTDSR 的平均资源开销略高于 S-NOR 和 F-Strategy,但可以提供更高的可靠性;相对于 S-DWC,FTDSR 则拥有更低的资源开销和更高的可靠性.尤其是在辐射强度达到最坏情况下,FTDSR 与 S-DWC 和 S-NOR 相比更具优势,在资源开销增加 10%的情况下,提高了 20%以上的可靠性.

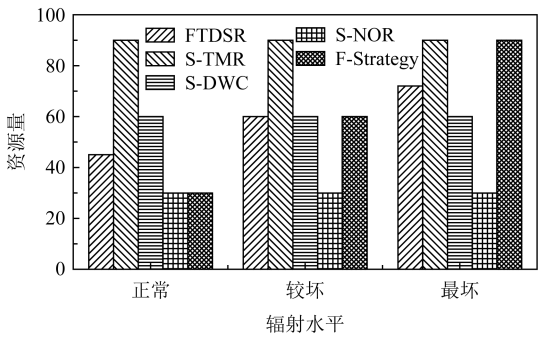


Fig. 6 Resources required by various strategies under different radiation levels

图 6 不同辐射水平下不同策略所需的资源量

资源受限条件下,图 7 反映了 5 种容错方法在不同辐射水平下可以完成的最大任务数量.由于 S-TMR 可以在任何辐射水平下满足任务对可靠性的要求,因此其可完成任务的数量只与片上资源呈正相关,所以在资源一定时其完成任务的数量保持不变,但是在辐射水平较低条件下,该方法的短板非常明显.相对而言,S-DWC 和 S-NOR 在辐射水平较低时还具备一定优势,一旦随着辐射水平的加剧,它们可以完成的任务数量会明显下降.F-Strategy 在一定程度上弥补了 S-DWC 和 S-NOR 方法的不足,但全体任务随着辐射水平的变化而同时改变冗余方式,也会造成不必要的资源开销,从而限制可以完成的任务数量.FTDSR 方法不同于 F-Strategy 方法对

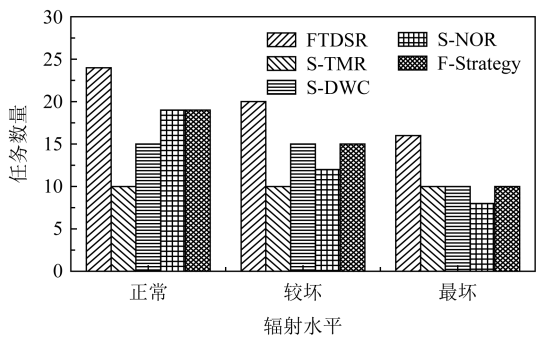


Fig. 7 ATC under different radiation levels

图 7 不同辐射水平下的任务完成量

全体任务冗余方式的改变,而是针对单个任务在不同辐射水平下的可靠性要求进行细粒度的冗余匹配,兼顾了可靠性和资源效率,从图 7 中可以看出 FTDSR 在任务完成量方面占有绝对优势,平均比其他 4 种方法高出 57.2%.

以上实验结果可以看出,FTDSR 与目前常用的 4 种 FPGA 容错方法相比具有非常明显的优势,可以随着辐射水平的变化动态自适应地为单个任务匹配相应的冗余策略,兼顾了系统高资源利用率和高可靠性等方面的要求.

5 结束语

目前常用的 FPGA 容错方法很少考虑辐射水平变化对任务可靠性的影响,直接为片上任务加载三模冗余方式执行,尽管满足较高的可靠性要求,但往往造成极大的资源开销.本文提出的 FTDSR 方法随着辐射水平的变化评估每个任务的可靠性等级,以单个任务为粒度动态自适应地匹配相应的冗余方式,兼顾了系统资源利用率和高可靠性要求,同时改进了基于 BRAM 的辐射监测器,最大化地构造片上 BRAM 监测器来提高辐射水平评估的准确性.

未来的工作可以分析辐射对片上故障分布的影响,从而更加准确地评估该环境下任务所在执行模块发生故障的概率,或者在给定资源条件下对任务匹配策略进一步优化,实现更有针对性的容错设计.

作者贡献声明:李泽宇负责提出研究方案和论文撰写;王泉负责方案设计和论文修订;杨鹏飞负责实验设计和论文撰写;许志伟负责论文修订;梁金鹏和高歌负责实验执行和论文修订.

参 考 文 献

[1] Gao Zhen, Zhu Jinhua, Han Ruishi, et al. Design and implementation of configuration memory SEU-tolerant viterbi decoders in SRAM-based FPGAs [J]. IEEE Transactions on Nanotechnology, 2019, 18(99): 691-699

[2] Wang Zhen, Jiang Jianhui, Chen Naijin, et al. Effects of three factors under BTI on the soft error rate of integrated circuits [J]. Journal of Computer Research and Development, 2018, 55(5): 1108-1116 (in Chinese)
(王真, 江建慧, 陈乃金, 等. BTI 作用下三因素对集成电路软差错率的影响[J]. 计算机研究与发展, 2018, 55(5): 1108-1116)

[3] Wu Lihua, Han Xiaowei, Zhao Yan, et al. Design and verification of radiation-hardened by SOI-based FPGA [J]. Information and Electronic Engineering, 2012, 10(5): 627-632

[4] Rezgui S, Louris P, Sharmin R. SEE characterization of the new RTAX-DSP(RTAX-D) antifuse-based FPGA [J]. IEEE Transactions on Nuclear Science, 2010, 57(6): 3537-3546

[5] Qi Liuyu, Liu Guodong, Zhao Zhengyang. Design of a SRAM FPGA single event effect reinforcement platform [J]. Electronic Technology Applications, 2019, 45(5): 84-86, 94 (in Chinese)
(齐刘宇, 刘国栋, 赵正阳. 一种 SRAM 型 FPGA 单粒子效应加固平台设计[J]. 电子技术应用, 2019, 45(5): 84-86, 94)

[6] Harb S, Jarrah M. FPGA implementation of the ECC over GF (2m) for small embedded applications [J]. ACM Transactions on Embedded Computing Systems, 2019, 18(2): 1-19

[7] Yao Erlin, Zhang Jiutian, Chen Mingyu, et al. Detection of soft errors in LU decomposition with partial pivoting using algorithm-based fault tolerance [J]. International Journal of High Performance Computing Applications, 2015, 29(4): 422-436

[8] Glein R, Rittner F, Heuberger A. Detection of solar particle events inside FPGAs [C/OL] //Proc of the 16th European Conf on Radiation and Its Effects on Components and Systems(RADECS). Piscataway, NJ: IEEE, 2016 [2020-03-20]. https://ieeexplore.ieee.org/document/8093159

[9] Yang Mengfe, Liu Bo, Gong Jian, et al. Architecture design for reliable and reconfigurable FPGA-based GNC computer for deep space exploration [J]. Science China Technological Sciences, 2016, 59(2): 289-300

[10] Santos R, Venkataraman S, Kumar A. Scrubbing mechanism for heterogeneous applications in reconfigurable devices [J]. ACM Transactions on Design Automation of Electronic Systems, 2017, 22(2): 1-26

[11] Zhang Chengcheng, Ban Tian. Research on reconfigurable fault tolerant structure of SRAM FPGA [J]. Electronic Measurement Technology, 2016, 39(11): 41-45 (in Chinese)
(张程程, 班恬. SRAM 型 FPGA 的可重构容错结构研究[J]. 电子测量技术, 2016, 39(11): 41-45)

[12] Glein R, Mengs P, Rittner F, et al. BRAM implementation of a single-event upset sensor for adaptive single-event effect mitigation in reconfigurable FPGAs [C/OL] //Proc of the 11th NASA/ESA Conf on Adaptive Hardware and Systems (AHS). Piscataway, NJ: IEEE, 2017 [2020-03-21]. https://ieeexplore.ieee.org/document/8046352

[13] Jacobs A, Cieslewski G, George A D, et al. Reconfigurable fault tolerance: A comprehensive framework for reliable and adaptive FPGA-based space computing [J]. ACM Transactions on Reconfigurable Technology and Systems, 2012, 5(4): 1-30

[14] Bolchini C, Miele A, Sandionigi C. A novel design methodology for implementing reliability-aware systems on SRAM-based FPGAs [J]. IEEE Transactions on Computers, 2010, 60(12): 1744-1758

[15] Darvishi M, Audet Y, Blaquiere Y. Delay monitor circuit and delay change measurement due to SEU in SRAM-based FPGA [J]. IEEE Transactions on Nuclear Science, 2018, 65(5): 1153-1160

[16] Savani V, Gajjar N. Development of SEU monitor system for SEU detection and correction in virtex-5 FPGA [C/OL] //Proc of the Nirma University Int Conf on Engineering. Piscataway, NJ: IEEE, 2020 [2020-09-21]. https://ieeexplore.ieee.org/document/6153268

[17] XILINX. AXI block RAM(BRAM) controller product guide [R/OL]. 2019 [2020-10-30]. https://china.xilinx.com/content/dam/xilinx/support/documentation/ip_documentation/axi_bram_ctrl/v4_1/pg078-axi-bram-ctrl.pdf

[18] Wang Xiangfen, Wu Jianxin, Gao Cheng. A dynamic adaptive SRAM FPGA system fault tolerance method based on BRAM monitoring: China, CN111338833[P]. 2020-06-26 (in Chinese)
(王香芬, 吴建新, 高成. 一种基于 BRAM 监测的动态自适应 SRAM 型 FPGA 系统容错方法:中国, CN111338833[P]. 2020-06-26)

[19] XILINX. Devicereliability report [R/OL]. 2020 [2020-11-05]. https://china.xilinx.com/content/dam/xilinx/support/documentation/user_guides/ug116.pdf

[20] Afzaal U, Lee J A. A self-checking TMR voter for increased reliability consensus voting in FPGAs [J]. IEEE Transactions on Nuclear Science, 2018, 65(5): 1133-1139

[21] EPFL. Combinational benchmark suite [EB/OL]. 2015 [2020-11-10]. https://lsi.epfl.ch/benchmarks

Li Zeyu, born in 1991. PhD candidate. Student member of CCF. His main research interests include FPGA fault tolerance, FPGA aging resilience and heterogeneous computing system fault tolerance.
李泽宇,1991 年生.博士研究生,CCF 学生会员.主要研究方向为 FPGA 容错、FPGA 老化缓解和异构计算系统容错.

Wang Quan, born in 1970. PhD, professor, PhD supervisor. Member of CCF and ACM. His main research interests include hardware security, embedded systems, wireless networks and 3-D printing.
王 泉,1970 年生.博士,教授,博士生导师,CCF 和 ACM 会员.主要研究方向为硬件安全、嵌入式系统、无线网络和 3D 打印.

Yang Pengfei, born in 1985. PhD, associate professor, master supervisor. Member of CCF. His main research interests include embedded system architecture, memory security, heterogeneous parallel computing.
杨鹏飞,1985 年生.博士,副教授,硕士生导师,CCF 会员.主要研究方向为嵌入式系统架构、内存安全、异构并行计算.

Xu Zhiwei, born in 1978. PhD, associate professor, master supervisor, Member of CCF. His main research interests include network performance analysis and the related mathematics problems.
许志伟,1978 年生.博士,副教授,硕士生导师,CCF 会员.主要研究方向为网络性能分析和相关的数学问题.

Liang Jinpeng, born in 1995. Master. Student member of CCF. His main research interests include SOPC fault tolerance and network model compression.
梁金鹏,1995 年生.硕士,CCF 学生会员.主要研究方向为 SOPC 容错和网络模型压缩.

Gao Ge, born in 1996. Master. His main research interests include FPGA dynamic reconfiguration technology, FPGA resource scheduling and on-chip fault tolerance.
高 歌,1996 年生.硕士.主要研究方向为 FPGA 动态重配置技术、FPGA 资源调度和片上容错.