

航空电子设备单粒子效应风险防护措施

任晓琨 王山虎

中航民机机载系统工程中心有限公司, 上海, 200241;

摘要: 随着高能宇宙射线向地球辐射的活动变得活跃以及先进工艺制程的集成芯片在航空电子设备中的应用, 单粒子效应对航空电子设备的影响已变得越来越不可忽视, 对军用航空和民用航空的航空安全构成了巨大威胁。本文从航空电子设备所处环境、主流元器件选用等开展分析, 从缓解防护、设计加固、检测、告警处置等多个维度提出相应的防护措施, 提出了部分设计解决思路并给出应用建议。

关键词: 单粒子效应; 单粒子翻转; 单粒子缓解防护

Risk protection measures for single-particle effects of avionics equipment

Ren Xiaokun, Wang Shanhu

Civil Aircraft Airborne System Engineering Center Co.Ltd of AVIC, Shanghai, 200241;

Abstract: With the activity of high-energy cosmic rays radiating to the Earth and the application of integrated chips with advanced processes, the impact of Single Event Effects(SEE) on avionics has become more and more non-negligible, posing a huge threat to the aviation safety of military aviation and civil aviation. In this paper, the environment of avionics equipment and the selection of main electronic components are analyzed, and the corresponding protective measures are proposed from multiple dimensions such as mitigation protection, design reinforcement, detection, alarm disposal. Some design solutions and application suggestions are presented.

Keywords: Single Event Effects; Single Event Upset; Single Event Mitigation Protection.

DOI:10. 69979/3041-0673. 24. 4. 048

引言

单粒子效应 (Single Event Effects, SEE) 是指由单个粒子 (如太阳能粒子、高能中子和质子、宇宙射线等) 的冲击引起的半导体器件的响应。宇宙射线穿过大气层时, 会与大气层的原子相互作用产生带电粒子和不带电中性粒子构成的混合复杂大气电离辐射环境。会对飞经此环境的航空电子设备的电子元器件产生三种辐射效应, 包括单粒子效应 (SEE)、电离辐射总剂量效应 (TID) 和位移损伤效应 (DD)^[1]。经过研究表明, 在民航万米高空, 航空电子设备主要是受 SEE 影响, 在大气层 10 km 高度附近 SRAM 型存储芯片的单粒子翻转率大概在 10~8 SEUs/bit/day 量级, 其余两项的影响可以忽略不计^[2]。其中, SEE 对电子设备的影响主要是以 (Single Event Upset, SEU)、(Multi-Bit Upset, MBU) 和 (Single Event Transient, SET) 造成的数字逻辑电路“0”、“1”翻转为主, 极少发生永久性损伤。因此, 航空电子设备的单粒子效应防护主要是以防护、检测、纠正此类软错误为主^[3]。

当前, 随着航空电子设备向综合化、集成化不断发展, 具备先进算力的电子元器件在新型的航空电子设备上得到了越来越广泛的应用。更低的工艺制程、最高的集成密度、更低的内核电压意味着其对大气辐射环境的敏感度更高^[4]。另一方面, 航空产业仍在磅礴发展, 飞

机升限更高, 数量更多, 航线越来越密集, 临近空间的航空器也层出不穷, 这也导致航空电子设备经受单粒子效应影响的风险越来越大, 必须从设计层面进行特定风险分析及设计防护, 防止因单粒子效应影响造成影响飞机安全的灾难性事件。

针对单粒子效应的防护, 主要是防护思路包括: (1) 尽可能提高设备自身特别是敏感元器件的抗扰度; (2) 采用设计容错技术, 针对关键重要的功能进行多余度容错设计; (3) 采用多重数据完整性检测技术, 在经受单粒子翻转后及时检测锁定安全输出避免产生灾难性后果; (4) 在及时检测发生单粒子翻转后, 及时进行告警和系统重构处理, 尽快让系统恢复正常工作状态。

1 航空电子设备单粒子效应设计防护

根据实验研究, 航空电子设备中随机静态存储器 RAM 特别是大容量工艺制程低的 RAM 相关工艺器件最易经受单粒子效应影响。包括所有的 RAM 芯片、基于 SRAM 工艺的 FPGA 芯片、包含 RAM 的集成芯片、处理器、通信协议芯片、包含大量寄存器的 FPAG、处理器、通信协议芯片等^[5]。

针对以上薄弱点, 通常采用以下几种形式进行设计加固:

- 1) 选择宇航级抗辐射芯片;
- 2) 器件选型进行功能替代;

- 3) 器件筛选;
- 4) 防护材料应用及防护结构设计;
- 5) 容错设计。

选择宇航级抗辐射芯片可以解决普通航空电子设备的单粒子效应防护问题,因为航空电子在大气层中经受的单粒子效应相对于宇宙空间的辐射来说微不足道,类似于“大马拉小车”。但采用宇航级芯片来做单粒子效应防护并不现实,因为民用航空电子设备的经济性要求无法支撑选用宇航级芯片。一颗宇航级芯片价格可能是同指标工业扩展级芯片的上千倍,因此,选用宇航级芯片进行防护设计原理上可行,现实却不可行。

更为现实的防护设计方法是尽可能规避敏感器件,选用同功能的其它器件进行功能替代。例如,选用内部含有软错误修复(SEM)的FPGA芯片,选用对单粒子效应相对较不敏感的基于Flash工艺的FPGA芯片。选用自带ECC控制器(Error Checking and Correcting, 错误检查和纠正)的处理器芯片和支持ECC功能的外部存储芯片。选用基于SOI(绝缘体上硅基)新工艺的RAM芯片(采用SOI技术,能够将SRAM产品的抗单粒子翻转性能提高 $2\sim 5$ 倍)。以及选用其它支持内纠错技术的集成电路芯片^[6]。

第三种方法为借鉴航天工程,针对敏感器件进行抗单粒子效应能力评估及筛选,但此种方法会带来研制周期和研制成本的显著上升,仅推荐对安全关键等级较高的航空电子设备所选用的敏感元器件采用此种方法。

此外,还可以采用相应的防护材料对敏感器件进行加固设计。根据NASA研究,部分聚乙烯和环氧复合物对于辐射屏蔽具有一定效果,且新型材料正层出不穷,利用新型材料进行器件加固防护也逐渐成为有效的防护手段。

容错技术也是进行单粒子防护的重要手段,其中三模冗余TMR(Triple Modular Redundancy)是最常见的缓解措施。三模冗余是指采用三个相同的模块同时执行相同的操作,3路信号通过多数表决器进行3取2表决,确保一路信号发生翻转后不会影响该路信号的输出^[7]。

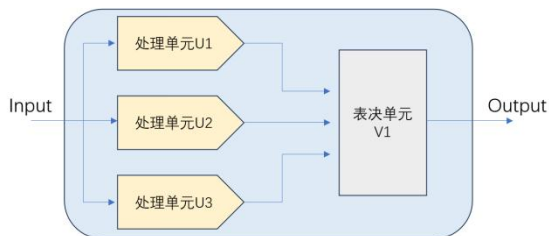


图1 FPGA内部三模冗余基本架构

FPGA内部可以采用上述三模冗余架构进行多余度表决设计,可以依据信号重要程度和FPGA资源量进行局部或者全局三模冗余设计。局部三模冗余是将设计中

的触发器冗余为3份,并在其输出端添加表决器进行表决,输入数据、控制信号和时钟均由冗余触发器共享,因此并不能为复位信号、控制信号等共享信号提供保护。全局三模冗余是将所有组合逻辑单元、触发器、信号、表决器均冗余三份,通过3个时钟域来保证全部信号不收SEE影响,但此种方式对FPGA逻辑资源消耗较大,在高速信号处理中,需要注意对信号时序的影响。

除FPGA内部的三模冗余外,针对SRAM的三模冗余,可以通过复制三个SRAM芯片电路,通过读写请求对三个SRAM进行相同操作,对SRAM读取数据进行多余度表决,针对发现的错误数据进行修正操作。但本方法需要处理器前端架构的支持,且硬件电路开销较大。3单粒子效应故障检测方法

单粒子效应等软错误对航空电子设备的主要影响是破坏数据传输、处理的完整性,进而导致逻辑运算出现错误,进而影响飞机的功能安全。因此,完善数据完整性检测方法,及时发现数据传输、运算处理过程中的数据翻转错误,及时进行故障处置对于防范发生安全事故至关重要。检测单粒子效应故障的主要方法包括:数据传输校验技术、恒定数据周期读取检测技术、输出数据回采检测。

数据传输校验技术包括ECC校验(Error Checking and Correcting, 错误检测及纠正),奇偶校验、CRC校验、自订的校验算法等。

其中,ECC校验提供了较为完整的数据完整性检验,ECC校验是基于汉明码,在正常的数据位之外添加了N位的校验位,可以纠正数据中1位错误,检测2位错误。ECC校验需要处理器内部的ECC控制器、外部RAM芯片和Flash芯片支持ECC校验。在每个处理器的读写周期内,处理器内部的ECC控制器均可以对读写的数据进行校验,以保证数据存储的完整性。目前ST、NXP等最新工艺制程(低于55nm)的面向工业控制、车载等高可靠性应用场景的单片机均自带ECC控制器。未来,面向安全关键领域的先进制程处理器芯片内部自带ECC校验已是必然。

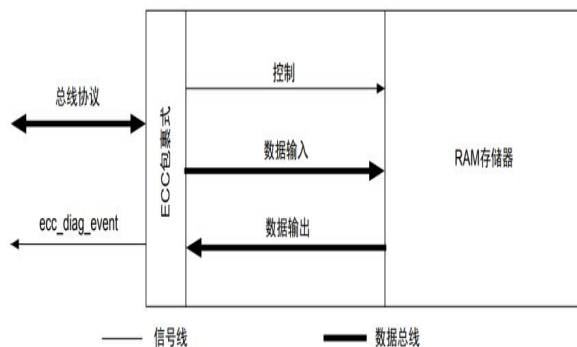


图2 某型处理器RAM ECC控制器与内存单元接口

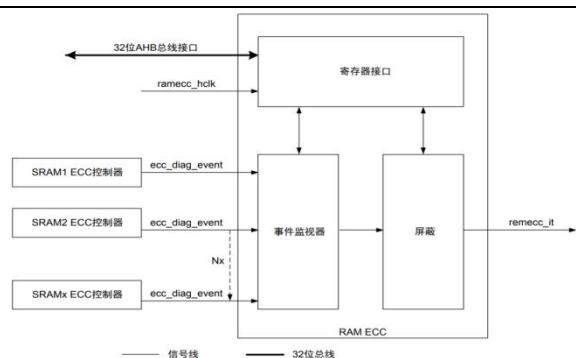


图 3 ECC RAM 简化框图

部分项目基于继承性,选用的处理器较为老旧,处理器内部不支持 ECC 校验,此时,应考虑其它方式缓解单粒子效应的影响。例如,可以将某些固定数据(本次上电的上电 BIT 结果、产品型号、软件版本等)存入内存固定地址,以上数据通常在上电时进行上电 BIT 检测,在本次上电过程中不会发生变化,可以在软件周期任务中周期读取以上数据,若检测到数据发生了跳变,则认为可能发生了单粒子翻转或者最小系统数据读写异常,此时,切断对外的输出,上报自身故障,将自身设备置于安全态,保证系统安全。此种方法的故障检测覆盖率较为有限,仅可作为一种辅助检测手段。

针对数据传输过程的完整性,需要在设备设计时进行辅助加强,针对 SPI 无底层数据校验,RS-422、ARINC 429 底层仅有奇偶校验的缺陷,在数据层面增加相应的 CRC 数据校验,传输路径上两端接收到完整数据包后,通过 CRC 数据校验算法进行比较,若数据一致,则可判定为数据在传输过程中保证了数据完整性。此种方法的缺陷在于增加了处理负担,影响了处理效率,因此,需根据实际情况确定采用 CRC8、CRC16 或更高等级的校验算法。

针对单个逻辑位发生跳转导致误输出的情况,在关键输出信号可以增加多拍指令连续确认,输出状态与当前指令状态回读比较的形式,防止单个逻辑位错误造成误输出,造成故障蔓延。

3 告警及处理策略

对于航空电子设备来说,自身并无法准确分辨是否是经受了单粒子效应导致了数据发生了翻转,因此电子设备只能存储发生了数据错乱故障。对于单次单粒子翻转的故障,若软错误得以恢复,通常此类故障记录在电子设备内部的 NVRAM 中。若发生硬错误,此时故障应一直持续,若此时电子设备的处理器仍在运行,则应上报自身故障,及时切换备份控制器,进行自身重启复位操作。多次重启复位故障仍未恢复,设备应维持进行故障安全态直至本次飞行结束。若此时电子设备的处理器经受了单粒子效应的硬错误造成无法正常运行,可以通过预先设置的心跳信号向外表征自身的运行状态,心跳持续长时间无法翻转,证明此时电子设备运转不正常。

及时切换备份控制器,进行故障设备重启复位操作。

总结

在综合考虑安全性、成本、经济性、技术实现难度的基础上,对于航空电子设备,应考虑多种方式结合的形式进行单粒子防护设计,较为现实的设计方法为:

器件选型设计是基础,应尽可能选择敏感度加强的元器件,如采用 SOI 新型工艺技术的 RAM 芯片,Flash 工艺型 FPGA 芯片,选用自带 ECC 控制器的处理器芯片和支持 ECC 校验的外围 RAM 和 Flash 芯片。

在器件选型的基础上,对端到端的数据传输、存储、处理的各环节进行数据校验,在发生单粒子翻转时能够及时检测进行及时处理确保不引起灾难性安全事件。

对安全关键的输出功能应进行全方面故障检测,检测是否存在与预期指令不符的输出动作,在发生非预期指令输出时切断对外输出或切断对外输出的电源,确保对外输出安全状态。

通过以上设计方法的结合,可以确保将单粒子效应造成的安全影响限制到可接受的安全水平。

参考文献

- [1]刘必臻,杨平会,蒋孟虎,王雯雯,张磊.航天器单粒子效应的防护研究[J].航天器环境工程,2010,27(6):693-697.
- [2]Reza OmidGosheblagh, Karim Mohammadi. Dynamic Partial based Single Event Upset (SEU) Injection Platform on FPGA[J]. International Journal of Computer Applications,2013,76(3):19-24.
- [3]Lorenzo Ciani,Marcantonio Catelani.A fault tolerant architecture to avoid the effects of Single Event Upset (SEU) in avionics applications[J]. Measurement,2014,54(8):256-263.
- [4]Hongwei Zhang,Yang Guo,Shida Wang,Yi Sun.Simulation Study on the Charge Collection Mechanism of FinFET Devices in Single-Event Upset[J]. Micromachines,2024,15(2):201-213.
- [5]W.-T. Yang,Chaohui He,X.-C. Du,S.-S. Shen. Single Event Upset Diagnosis and Recovery in On-Chip-Memory[J]. Nuclear Electronics & Detection Technology,2017,37(2):138-141.
- [6]Tianwen Li,Hongjin Liu,Haigang Yang. Design and Characterization of SEU Hardened Circuits for SRAM-Based FPGA[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems,2019,99(2):1-8.
- [7]S. Wu,X.-G. Zhou,L.-L. Wang. RAM-Based FPGA SEU Fault Propagation Model[J],2017,45(8):1976-1984.