嵌入式软硬件系统的可靠性设计

李文泉
（山西安数智能科技有限公司 山西太原 030001）

摘要：近年来，信息技术和计算机技术的发展越来越快，嵌入式系统是信息处理技术和计算机技术共同作用下的新兴技术，具有系统精炼简洁、目标性强、功能强大、程序质量高、系统可靠性强等特点。在本文中，针对 ARM 的嵌入式软硬件系统设计进行分析。

关键词：嵌入式系统；软硬件；可靠性设计

1 硬件系统可靠性设计

1.1 可靠性模型的建立

首先根据此硬件的功能特点来确定其可靠性模型，同时对硬件的功能进行分类，并以此为基础确定所有用到的元器件。此硬件系统可以分为以下几个模块。a)CPU 小系统模块 CPU 小系统模块包含了 CPU、桥片、BOOTROM、FLASH、DDRSDRAM 和实时时钟等电路，负责对信息和数据进行运算和处理，对系统进行控制。b)CPCI 模块完成从 PCI 总线到 PCI 总线的转换，提供总线的仲裁，完成作为 CPCI 主设备或从设备的功能。c)千兆以太网模块对外提供一个十兆、百兆和千兆的自适应的网络接口。d)RS422 模块提供 4 路 RS422 接口。e)PMC 模块提供外接 PMC 扩展卡的接口。f)USB 模块提供 2 路 USB 接口，支持 U 盘、移动硬盘等 USB 存储设备。g)电源模块提供板上各芯片正常工作所需要的各种电源。h)时钟模块提供板上芯片正常工作所需要的各种时钟。根据以上的功能模块，就可以确定所选用的器件类别了。

1.2 可靠性设计实现

为了保证此硬件系统的可靠性，在设计上采取了以下措施。a)电路模块化设计选用了高可靠、低失效率的元器件，并不等于组装起来的产品就是高可靠，还必须在电路设计上给予保证。在满足技术要求的前提下，系统在设计中应尽可能地选用成熟的、典型的电路，尽量采用数字电路和集成电路。同时，单板上设有故障指示灯，故障定位准确，可以大大提高系统的可维修性。b)元器件的选用与控制元器件的选用应尽量在元器件选用目录范围内选择，考虑多年设计使用中时效证明故障率低、可靠性高的产品和厂家，或选用优化了的进口产品。电阻器、电容器和电感器等均按军用产品质量等级进行选取，在同等失效率情况下，选用那些成熟系数高、质量系数好的产品。晶体二极管、三极管及集成电路等均限定选用军用产品或进口军用器件，决不允许随意使用民用产品上机。同类产品中选用成熟系数高、失效率低，对环境适应性强的产品。元器件在使用前由质量部门进行筛选或认真检查确认后方能上机使用。c)降额设计对元器件的应力分析均取较大的裕量，功率和耐压系数均取 0.3 左右。在可靠性预计方面，使用质量等级 B 作为预测参数，能充分满足对新型国产及进口元器件的筛选要求。d)热设计充分考虑发热器件的布局，采用了整板覆盖散热板的作法，有效地将热量通过空气对流，散热板散热，机箱导冷等方式散出，降低了元器件的温度。e)电磁兼容设计在设计中充分考虑电磁兼容性问题，在原理图阶段充分考虑电源的滤波，信号的滤波，信号的匹配，在布局布线阶段充分考虑信号的完整性，减少串扰，寄生耦合等。f)连接器在设计中选用高可靠的连接器，以提高互联设计的可靠性。g)试验验证主要通过环境试验包括温度冲击试验、高低温贮存试验、高低温工作试验，和连续工作试验来检验和提高产品的可靠性。

2 软件系统可靠性设计

经过几年的实践并借鉴航天系统软件管理经验，我们通常将嵌入式软件的可靠性设计分为以下几个阶段：

2.1 软件需求分析阶段

相关的可靠性设计保障有：a）进行软件可靠性预计，以及可靠性与成本、进度、功能和技术能力约束等方面的权衡分析。在此基础上，确定相关的质量保证活动，包括与可靠性相关的全部活动。b）进行接口可靠性分析。进行软硬件接口分析，考察软硬件接口容错设计的合理性，需要更改硬件设计时应与总体协商。c）进行软件失效分析。在系统任务失效分析的基础上，继续进行功能层次上的软件失效影响分析，并确定失效的严重性等级。d）进行软件确认测试计划审查和软件验收测试计划审查。e）进行软件任务书的可追踪性分析，确保任务书对软件的要求全部在软件需求规格说明中进行了描述。

2.2 软件设计

相关的可靠性设计保障有：a）进行软件可靠性指标分配。在完成软件结构设计的基础上，考虑包括物理系统特性、早期积累的经验数据、关键部件的追踪，以及数据收集的资源要求等一系列因素，确定每一个软件配置项的可靠性指标。计算各软件配置项可靠性指标对软件系统总体可靠性目标的影响，分析时间、困难与风险，必要时调整配置项的可靠性指标，直到满足系统可靠性要求为止。b）进行接口可靠性分析。对软件配置项之间、软件模块之间的接口设计合

（下转第 11 页）

（上接第 9 页）

理性进行分析，需要时进行设计调整。c）进行可靠性设计。依据软件需求、功能剖面和功能关键等级等进行软件设计，必要时应制定软件恢复策略，保证软件能够修复可能破坏的关键数据，特定失效发生时能够实现失效检测、限制破坏范围、从某一已知的参照点开始进行失效恢复。d）进行可靠性设计准则符合性分析。依据有关标准，限制模块的规模与复杂度，保证模块的可测试性。e）进行设计失效分析。应用数据库分析、规模与时序分析、数据流分析、算法分析以及软件设计 FMEA、FTA 等方法进行软件设计分析，标识高风险区域。f）进行软件需求的可追踪性分析，确保全部软件功能、性能以及相关的可靠性需求等在设计中得到了正确的体现。g）对于安全性关键软件还应进行软件设计安全性分析等。

2.3 软件实现阶段

相关的可靠性设计保障有：a）使用正式评审与文档审查验证需求、设计文档、源代码、用户手册与测试文档（包括测试用例、测试程序与测试结果）。b）审查与测试时应保证设计人员与总体人员的有效通讯、交流与沟通，并按照功能关键等级与功能使用频率，合理调整资源，保证关键模块的审查与测试。c）限制需求的改变，对需求变化的提交、追踪和实现要规定严格的管理程序。d）对于超可靠软件或安全性关键软件，需要进行软件代码的安全性分析，包括逻辑、中断、接口、资源和时序等全方位的分析。e）软件需求及设计的可追踪性分析，确保全部软件功能、设计要求等在编码与测试中得到了正确的体现。通过以上软件研制生命周期的控制，可以将软件可靠性设计的风险降到最低，但是从软件设计及编码本身来讲，还应该遵循一定的方法和规则。通常我们采用通行的结构化程序设计技术。

3.结束语

实践证明，通过此方法设计的软硬件系统在对抗震动、温度湿度以及庞大数据输入处理等工作作业中，实现 0 故障的运行效果。同时保证了软硬件的运行稳定，保证能够满足产品的需求。

参考文献：

[1]周新蕾，卿寿松.软件可靠性保证及相关技术[J].质量与可靠性，2005，（6）：25-28.

[2]徐晓春.软件测试的方法和工具[J].计算机世界，1999，（12）：17-19.