【博客藏经阁丛书】

嵌入式系统可靠性设计技术及案例解析

武晔卿 编著

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

【博客藏经阁丛书】

嵌入式系统可靠性设计技术及案例解析

武畔卿 编著

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

内 容 简 介

本书介绍了嵌入式系统设计中，哪些地方最可能带来可靠性隐患，以及从设计上如何进行预防。内容包括：启动过程和稳态工作中的应力状态差别等可靠性基础知识及方法；降额参数和降额因子的选择方法；风扇和散热片的定量化计算选型和测试方法、结构和电路的热设计规范；PCB板布线布局、系统结构的电磁兼容措施；电子产品制造过程中的失效因素（包括EOS、ESD、MSD等）及预防、检验方法；可维修性设计规范、可用性设计规范、安全性设计规范、接口软件可靠性设计规范等方面的技术内容。同时，针对相关内容进行实际的案例分析，以使读者更好地掌握这些知识。

本书适用于交通控制、电力电子、消费电子、医疗电子、控制电子、军工产品等以电子、机电一体化为主体内容的相关技术领域，既可作为工程技术人员的技术参考书，也可作为相关专业的高年级本科生、研究生、教师的设计参考书。

图书在版编目(CIP)数据

嵌入式系统可靠性设计技术及案例解析 / 武晔卿编著. — 北京 : 北京航空航天大学出版社，2012.7

ISBN 978-7-5124-0822-7

Ⅰ. ①嵌… Ⅱ. ①武… Ⅲ. ①微型计算机—系统设计—案例—分析 Ⅳ. ①TP360.21

中国版本图书馆CIP数据核字(2012)第099046号

嵌入式系统可靠性设计技术及案例解析

武晔卿 编著

责任编辑 刘 星

*

北京航空航天大学出版社出版发行

北京市海淀区学院路37号(邮编100191) http://www.buaapress.com.cn

发行部电话：(010)82317024 传真：(010)82328026

读者信箱：emsbook@gmail.com 邮购电话：(010)82316936

涿州市新华印刷有限公司印装 各地书店经销

*

开本：710×1 000 1/16 印张：16.5 字数：371千字

2012年7月第1版 2012年7月第1次印刷 印数：4 000册

ISBN 978-7-5124-0822-7 定价：36.00元

前　言

评选一个可靠的设计，不是比拼谁的设计方案更高明，而是比拼谁更少犯错误。因为其优点而选择，却因为其缺点而发生故障。因此，可靠性设计的工作就是研究哪些地方容易发生问题，以及如何预防和解决这些问题的方法。

比如二极管 1N4148，正向导通压降是多少？在一些技术培训课上，我曾经就此发问，0.7 V 的答案占了主导，也有 0.3 V、0.4 V、0.6 V 等说法。但实际上二极管的 $V-I$ 特性是一条曲线（横轴是电压，纵轴是电流），其压降并非一个定值，正向导通压降的数值与其导通电流大小相关，随着电流的变化，压降也在变化。

比如某器件指标 $T_{max}=80$ ℃，$P_R=1$ W，现在 $T=60$ ℃，$P=0.75$ W，请问器件能否长期可靠的工作？虽然单个指标都在正常范围内，并且有一定程度的降额，但答案仍然是“No”。任何器件都会有一条负荷特性曲线，形状为直角梯形，在一定温度后，随着温度的增加，P_R 的值是线性下降的，60 ℃时，P_R 都可能下降到了 0.75 W 以下了。

再比如，大气压这个指标，系统中有水、气，大气压自然会产生影响，但即使没有这些，大气压对电解电容、爬电距离和电气间隙等也会有直接的影响，而这在我参与过的部分企业的技术审核中也屡屡发生，甚至不乏很大规模的企业。

由此可见，司空见惯的经验性的东西，很多理解都未必是对的，或者被忽视，而这正是可靠性问题的根源。本书阐述的恰恰就是这些内容。

一、可靠性观点

读完此书，除了几个具体的知识点，还希望读者能形成以下几个基本观点：

1. 产品故障 ≠ 产品不可靠；
2. 系统启停和波动的过渡过程 ≠ 稳态过程；
3. 降额并不简单；
4. 电子可靠性问题的解决有时需要从机械、软件方面着手；
5. 器件再简单，datasheet 的完整版本都必须拿到并通读；
6. 可维修性和可使用性与电子工程师关系很大，因为研究可靠性的核心追求是利润；
7. 制程控制不好未必是工艺人员的问题；

8. 有些设计隐患是根本测试不出来的，即使我们明明知道它有隐患，但它确实又会在用户现场发生。

二、可靠性设计工作方法

16 年前，刚刚研究生毕业的我，一样也都经历过以上类似的问题，但就是在这段并不算很长的工作经历中，曾经有两位、也许他们自己并不觉得对我有很大影响的老师：一位戚老师（美国留学归来的老研究员），使我领会了可靠性设计应该从哪里去钻研；一位张老师（项目总师，自学成才的老研究员），教会了我如何用工程数学计算的方式分析电子技术问题。本书的诸多思想起源就是这里。

由此有三点总结：

一是作为电子技术工程师，要学会感恩，没有人有义务必须对你好，但也有很多人在无意之中帮到了你；

二是要善于思考钻研；

三是要学会用数学来指导工程实践。

我先在航天做技术开发，后在民营企业做研发管理，再又独立创业，经历了一个完整的从“工程师—技术经理—综合管理—创业者”的全过程。一路走来，深切理解做好可靠性工作，需要技术和管理的综合作用。因此，给公司起名字的时候，选择了瑞迪航科（北京）技术有限公司，其英文 RDCOO SpaceTech(Beijing)Co.，Ltd. 中的 RDCOO，就是 Research & Design Chief Operation Official 的简写。研发的运营，包含了技术和管理，构成了保证产品可靠性的基础。

三、致 谢

书稿完成后，掩卷回首，有些许的遗憾。核心遗憾就是字字啼血，但趣味性不足，一个快餐文化的社会环境，让读者去细细咀嚼每一句话、每一个段落，从每个细节中去发现对自己有用的知识点、思想点和方法论，确实略显枯燥。但念及《道德经》、《孙子兵法》，又心下释然，《道德经》5 000 多字，《孙子兵法》7 300 多字，与之相比，本书几十万字，已经算是很通俗了。

在这里，要感谢许许多多我可能都不知道名字的读者，是你们的每一次博客留言，让我有了写下去的动力，让我知道，自己的点滴知识、经验、思想，正在某个未知的角落发挥着作用。“兴趣和需要”是最大的动力，这两者中，“兴趣”来自于我自己的内心，而“需要”恰恰就来自于你们。

感谢 eet-china（电子工程专辑）的网站编辑 MIKE，是您的支持才使更多读者能读到我的文章，使我有了在深夜中、瞪着充满血丝的小眼，用文思泉涌的写作激情享受着自己的快乐；也是因为博客这个平台，使我的文章被发现，才有了此书的出版。

感谢北京航空航天大学出版社的工作人员，你们专业的眼光让我有了千里马对

伯乐的感恩，你们的帮助，使我从一个野路子的写手，转变成为一个思路严谨，符合出版业专业要求的作者。

感谢我的同事兼合伙人王洪东先生，是他替我分担了很多具体的技术工作，使我有时间润色修改书稿，也是他给我提供了很多技术细节上的帮助。

感谢我的同学石小兵先生，作为资深的军工可靠性技术专家，在可靠性的概念、系统性的技术方法等方面，以严谨的学术态度帮助核实并修订了诸多的细节内容。

感谢吴浩先生、王敬军先生、胡作清老师、韩树东先生、于金标先生、彭伟先生、彭宝兴先生、尹辉先生、王云格女士、于娜女士，在本书成书的过程中，提出中肯的修改意见，是你们见证并帮助了本书的成长。

感谢此书写作过程中时刻关注其进展的朋友们，你们的关注，是对我懈怠的鞭策。

如果您是科研开发一线的工程师，本书的内容可以直接参考用于日常设计；

如果您是技术管理者，您将明了技术团队可能会犯错的地方，并提前加以检查预防；

如果您是工艺和制造工程师，您将预知设计的隐患，并在生产环节加以弥补；

如果您是老师，将使您的技术思维不再停留在象牙塔里，而是深刻认识到影响产品可靠性的自然界的各种复杂要素，并将此传授给自己的学生；

如果您是在校生，本书将让您了解在工程现场的现实应力，研究除功能参数设计之外，系统设计和容差设计两大部分的内容；

如果您不是电子技术领域的从业人员，但您的朋友、家人、同学有人在做这方面的工作，作为礼物，您送去的将不仅是一本普通的书，而是一个美好的职业未来。

武晔卿
2012 年 3 月于北京

作者简介：

武晔卿，工学硕士，瑞迪航科(北京)技术有限公司技术总监，专注于电子系统可靠性设计和测试技术。

联系方式：18601144058　13601139543
400-6800-965
010-88754188　88754189　88754190

电子邮件：wuyeqing@rdcoo.com

公司网址：www.rdcoo.com

博　　客：http://forum.eet-cn.com/BLOG_wuyeqing_51.HTM

目 录

第0章

可靠性设计方法论

作为嵌入式电子工程师，在设计产品时，会遇到一种现象，实验室中的开发样机工作正常，进入批产、现场运行时，就容易出现一点或多点的规律性问题或随机偶发性问题。问题一般包括了花屏、测量误差大、生产批次一致性不能保证、器件烧毁或失效、接触不良、发热、维修拆装麻烦、界面操作不习惯等。要解决这些问题，需了解起因，了解起因则必须先了解器件的工作原理、失效机理和制造及运行过程可能引入的隐患。了解了病症发生的机理和诱发的因素，在设计阶段就能找到基于失效机理的预防性设计方法，这将是本书所关注的内容。

0.1 可靠性设计的目的

在开始技术内容之前，先提出一个问题，统一一下我们的思想。

“在企业中，研究嵌入式可靠性技术的终极目的是什么？”

曾经这个问题激发了不下十种答案，“让产品更可靠”、“增强客户满意度”、“降低维修成本”都被罗列其中。但这些都不能算是正确答案，它们只是可靠性设计的中间产物，真正的终极目的是“利润”。听到这个答案的工程师，很少有人会诧异和惊喜，因为钱虽然不是万能，但没有钱却是万万不能。没有合理的利润，就不能招聘到高水平的资深工程师，不能给工程师更好的培训机会和交流学习机会，不能投资购买更先进的测试设备，不能试验更好的技术创新，公司自然也不能得到更好的发展。

而追求“利润”的可靠性设计技术与追求“客户满意度”的可靠性设计技术之间有着不小的差别。这个提法并不是鼓励工程师设计粗制滥造不可靠的产品，因为粗制滥造会引起用户的反感，没有人买，企业会死得更快；而是鼓励工程师遵循可靠性的定义“在规定的时间里、规定的条件下，完成规定功能的能力”，更理性地分析实际需求和条件，做出成本合理的可靠产品来。所以在组织内部，作为组织，而非个体，开展嵌入式可靠性技术工作的时候，需要时刻警醒，用利润的目标来检视可靠性技术点的选择。

0.2 可靠性设计的内容

嵌入式系统可靠性设计是一门并不简单的工程学科，它包括了系统设计、功能参

数设计、容差设计三部分的内容。功能参数设计部分是较常规的技术，并且此部分与具体的行业需求紧密相连，不是本书讨论的重点；系统设计和容差设计较容易被缺乏实际工程经验的年轻工程师所忽视，而恰恰又是最容易引起设计问题的地方。

0.2.1 系统设计

系统设计可以简化理解为接口设计。作为一个技术机构，作为一个完整的项目，必须有这样一个岗位或部门承担起系统设计的工作。这份工作的内容在前苏联时期的军工系统做得比较完善，作为曾经的两个军备技术超级大国，前苏联和美国有着不同的特点和技术路线：美国在专项技术的突破方面有着得天独厚的优势，其开放的科研环境和精英辈出的社会科研体制，吸引着全球的天才们在那里贡献着自己的创新思维和实践，专题技术的进展明显优于前苏联；但前苏联也并不乏可圈可点之处，即便在半导体、新材料等方面不占优势的情况下，依然第一个将人送上了太空，并建立了可以长期居留的空间站，第一个设计出了速度超3马赫的战斗机米格-25，这一切的成就都不得不归功于其系统设计的突出成就，将不先进的技术用先进、有机、合理的方式组织协调起来，也能发挥出综合效益。就像管理，同样一批人，用不同的管理方式，可以做出不同的成就。典型的一点，前苏联以系统设计师个人的名字来命名的科研机构非常多，如米里设计局（直升机）、努德尔曼-卡拉什尼科夫设计局（机枪）。这是从管理机制上对系统设计的一个肯定。

那么系统设计的内涵都是什么？就是系统组成各部分之间的接口关系，这个接口不要狭隘地理解为只有接插件的才叫接口。广义的接口包括了四个方面的内容：电气接口、信息接口、机械接口、环境接口。比如电路板的安装柱，是电路板和安装机构之间的机械接口，从表面来看，似乎没有太大用处，但当我们做设计更改的时候，为了可维修性中的备品备件库存考虑，很重要的一点就是必须实现板卡升级时的“接口向前兼容”，其意为改动后的设计板卡，其机械接口的安装方式必须能将老版本的板卡兼容进去。除了机械接口，电气接口、信息接口、环境接口亦同理处理，如此在老板子发生维修需要更换时，在安装方式上可以直接拿新板子顶上，这就是机械接口向前兼容的作用；原PCBA（PCB Assemble，指已将元器件焊接好的电路板）升级后，原机器的电源或信号插头仍然能直接与新PCBA的接插件直接相连，这是电气接口向前兼容的结果；而软件协议上可以直接读取和控制相关的端口，就是信息接口的作用。

从系统设计时的接口设计考虑，在可靠性方面，需要关注四个方面，分别是防错措施、判错措施、纠错措施、容错措施。在出现接口的干扰问题时，这四类措施中只要有其中一种发挥了作用，就能确保系统是安全的。防住了错误的输入自然容易理解；如果能把错误判断出来，纠错自然也就好处理了，最坏的结局不过是把该控制信号或采集数据丢弃掉；容错措施虽然不能确保系统仍然正确工作，但能保证一点，无论如何错误，系统依然能是最安全的。

0.2.2 容差设计

另一部分内容是容差设计，在电路可靠性的分析里面，有一种分析方法为 WCCA(Worst Circuit Condition Analysis，最坏电路情况分析)。容差设计的本质就是把电路系统中，各器件或分模块部分的参数漂移正负的最大值都列出来，找出系统中各器件偏差漂移后的最坏组合，然后通过工程计算的方式，确认在最坏情况下，电路是否仍能工作在有效的范围内，具体详述见 1.6 节。

0.2.3 可靠性目标

在以上几个问题之外，再补充一个关于产品可靠性的说明。“产品的可靠性是产品在规定的时间里、规定的条件下，完成规定功能的能力”，仅从定义上分析，假设有一台汽车，有一项规定的环境条件是“在－20～＋40 ℃、相对湿度≤93%的情况下，汽车仍然具备正常开动、受控停车、报警的功能”。那在＋40 ℃、相对湿度 20%时，汽车仪表盘在静电的作用下，屏幕有闪动现象，但汽车工作仍然正常，这个产品算不算是可靠的？答案是“YES”。但客户会不会满意？答案不言自明。总结起来，可靠性定义中的规定时间、规定条件、规定功能的定义要基于客户的满意度和主观感受来确定，而不仅是从技术性能来入手。

0.2.4 实现手段

在 0.1 节已经阐明，嵌入式系统可靠性设计的核心目的是利润，为了利润，有两个途径，一是开源，二是节流。虽然 0.2.3 小节的汽车案例中，屏幕闪动不会产生功能失效的致命危害，但它会严重打击用户的信心，失去了信心的潜在购买者，没有足够的决心来购买，靠开源多卖几辆车获取利润的途径就被堵塞。再假设，把汽车的外观做得很时尚，操作起来手感非常好，也会吸引一部分偏感性的购买者，尤其是女性客户。这时，屏闪的问题会被忽略掉，在具体应用中，非专业用户会将这类问题也归入产品可靠与否的范畴，但其实它不属于可靠性，而是可使用性的问题。现在在东南亚地区，尤其以韩国、日本为代表，产品造型越来越被重视，并在产品质量无差异化竞争的时候，靠着美观时尚的感官刺激和操作便捷的手感，也能大大提升销售。

操作方法、界面、外观结构的设计，不仅是美学的考虑，也可以避免人的疲劳和错误。

- 背景和字体及波形的对比色反差大而清晰，读数就不易出错；
- 界面设计上的参数设置，如果在设置后，有个“设置成功”的提示或“设置生效”的结果显示，那设置值出错的可能性会大大降低。

这些都是可使用性问题。可使用性不仅是美学的概念，也是技术和艺术的结合。单纯讲究艺术，是花拳绣腿；单讲技术，又让用户在使用中枯燥乏味。

利润的另一来源是节流。节流中，维修费用部分占了很大一块，若换个风扇都要厂家派工程师去现场，差旅费的花费自然不会少；拆装检查判断故障和维修的过程需