内 容 提 要

嵌入式实时操作系统在通信、医疗、核电站控制等领域的广泛应用，使人们越来越关注嵌入式实时操作系统的安全性。目前，系统介绍高安全嵌入式实时操作系统测试理论和方法的文献还比较少，本书介绍了关于高安全嵌入式实时操作系统的测试理论和方法。

本书以理论为指导，提出了操作系统测试需要解决的问题，证明了基于有限状态机测试策略的正确性，使用动态代码走查方法提高代码走查的效率和效果，使用地址监控方法解决临界保护正确性测试问题。每种测试方法都以理论为指导，测试充分性得到有效保证。

本书适合于从事嵌入式操作系统设计和测试的科研人员参考和使用。

图书在版编目（CIP）数据

嵌入式实时操作系统测试理论和方法 / 张明杰等著
. --北京：航空工业出版社，2014.7
ISBN 978-7-5165-0499-4

Ⅰ. ①嵌… Ⅱ. ①张… Ⅲ. ①实时操作系统—系统测试—研究 Ⅳ. ①TP316.2

中国版本图书馆 CIP 数据核字（2014）第 143378 号

嵌入式实时操作系统测试理论和方法
Qianrushi Shishi Caozuo Xitong Ceshi Lilun he Fangfa

航空工业出版社出版发行
（北京市朝阳区北苑 2 号院 100012）
发行部电话：010-84934379 010-84936343

北京地质印刷厂印刷		全国各地新华书店经售
2014 年 7 月第 1 版		2014 年 7 月第 1 次印刷
开本：787×1092 1/16	印张：15.5	字数：410 千字
印数：1—2000		定价：48.00 元

ηqdqγeγ bƐ dəqƐbγ3ə d ɛɔɑbɔγ Jqddγqγè

前　言

嵌入式操作系统应用越来越广泛，在国民经济、国防军事、医疗设备等各方面发挥着重要作用，是信息化社会的支撑。在某些特定领域，对嵌入式操作系统的可靠性要求很高。在医疗设备中（如 CT 扫描），如果出现问题可能会对患者造成严重的伤害；核电站控制系统出现问题带来更严重的后果；手机中的嵌入式操作系统越来越复杂，虽然系统崩溃不会造成严重后果，重启往往可以解决问题，但是必须承认，可靠性不高也会影响手机的市场地位。也就是说，在很多领域对嵌入式实时操作系统的可靠性要求越来越高，在很多情况下可靠性要求甚于性能要求。

操作系统的可靠性由许多方面构成，但最重要的是其内核的可靠性，内核主要包括进程管理和存储管理等。有的嵌入式实时操作系统也包括简单的文件系统，但不是标准配置，属于可配置组件，因此本书主要关注内核的可靠性。

测试是提高嵌入式实时操作系统内核可靠性的重要技术手段，但是无论是学术界还是工程界都鲜有关于嵌入式实时操作系统测试理论方面的资料。笔者曾在一些知名的计算机学术期刊上检索以期得到一些启发，结果没有检索到相关学术研究文献。虽然 LTP（Linux Test Project）是对 Linux 操作系统进行测试的国际化项目，但是对高可靠嵌入式实时操作系统测试而言帮助甚微。笔者认为高可靠性嵌入式实时操作系统测试必须在理论指导下进行，以保证测试的充分性和可信性。

有关测试资料的缺乏在笔者看来可能是属于商业机密，或者是更多的学者更倾向于构建新的操作系统，而没有太多兴趣测试操作系统的可靠性。毕竟构建操作系统是更具创造性的活动。于是我们决定坐下来静静地思考一下嵌入式实时操作系统的测试方法，经过几年的努力有了这本书中描述的测试方法。必须说明其中的测试方法，如有限状态机方法不是笔者创造而是拿来用于指导操作系统测试。本书旨在构建高可靠嵌入式实时操作系统内核测试的框架，以供感兴趣的读者进一步探讨。

测试理论告诉我们，基于需求的测试是最有效的软件测试方法。然而基于需求的测试方法往往在现有国内软件工程情况下效果不佳。操作系统的需求往往以系统提供的系统调用为纲目进行描述，单独对系统调用进行测试，没有考虑系统调用之间相互影响可能导致的系统缺陷，往往不能发现系统深层次问题。操作系统提供大量系统调用，而应用程序使用系统调用的方式千变万化，所以必须采用

分而治之的策略才能实现对操作系统的高效测试。

本书提出了操作系统测试问题；动态的代码走查方法，提高代码走查效率；基于地址监控的临界资源保护正确性测试方法；基于有限状态机的操作系统应用编程接口测试方法。这些方面基本涵盖了嵌入式实时操作系统内核的关键机制。虽然这些方法不一定是最有效的方法，但是从一定意义上讲，测试的充分性得到了保证。

限于笔者能力水平和经验有限，同时由于成书时间仓促，书中难免存在不足之处，希望读者提出中肯的批评和建议。如果能够吸引更多读者开展嵌入式实时操作系统的测试研究将是最令人欣慰的事。

目　录

第 1 部分　嵌入式实时操作系统的基本原理

第 2 部分　嵌入式实时操作系统测试的理论和方法