中国航天

中国航天科技集团公司软件评测中心

嵌入式软件测试及案例

张刚

主要内容

- 嵌入式软件的特点
- 嵌入式软件测试的难点及策略
- 嵌入式软件测试案例
- 结束语

嵌入式软件的特点

- 嵌入式系统
  - 以应用为中心，以计算机技术为基础，软件硬件可剪裁，功能、可靠性、成本、体积、功耗严格要求的专用计算机系统。
  - 由硬件层、中间层、软件层、功能层组成。
- 嵌入式软件
  - 实现嵌入式系统功能的软件
- 嵌入式软件的基本分类
  - 按照软件结构分类：单线程和事件驱动

嵌入式软件的特点

-单线程： 无主控程序,循环轮询系统和状态转移图（安全性问题）

-事件驱动：

- 中断驱动系统（循环主控、优先级、错误处理）；
- 多任务（存储、I/O、调度、通信、同步、互斥、中断管理、时钟管理）

嵌入式软件的特点

嵌入式系统的特点

- 高度分散，结构和处理器种类多
- 操作系统内核小、资源少
- 实时性
- 可靠性和安全性
- 软硬件结合紧密
- 专门的环境和开发工具
- 体积小、重量轻

嵌入式软件的特点

- 嵌入式软件的特点与嵌入式系统的特点相适应

  实时性

  可靠性

  专用性

  软硬件联系紧密

主要内容

- 嵌入式软件的特点
- 嵌入式软件测试的难点及策略
- 嵌入式软件测试案例
- 结束语

嵌入式软件测试的难点及策略

- 测试难点
  - 接口
    - 有外设，数据的采集和控制输出
  - 测试结果的获得
    - 运行的数据不易观察或获得（输入是硬件的输出、没有显示），求高效，用汇编语言
  - 测试环境
    - 无真实运行环境，模拟或半仿真（仿真的正确性，代价），未完成不能运行，例如：专门建立地测环境
  - 资源有限
    - 测试时可用资源少

嵌入式软件测试的难点及策略

– 中断

周期性、非周期、影响实时性

– 可靠性

自身的正确性、对硬件的容错

– 专用性

不同的处理器，需要不同测试环境

缺乏一般测试技术和测试工具的实施的基本条件

嵌入式软件应该是最难测的一类软件

嵌入式软件测试的难点及策略

嵌入式软件测试策略

– 白盒与黑盒测试结合

对于嵌入式软件，白盒测试一般不必在目标硬件上进行，更为实际的方式是在开发环境中通过硬件仿真进行，所以选取的测试工具应该支持在宿主环境中的测试。

– 目标环境和宿主环境测试

在嵌入式软件测试中，要在基于目标的测试和基于宿主的测试之间作出折衷。基于目标的测试消耗较多的经费和时间，而基于宿主的测试代价较小，但毕竟是在模拟环境中进行的。

嵌入式软件测试的难点及策略

- 重点关注以下事宜
  - 上电或重启自检、在线自检
    - 回避系统“带病”投入运行
  - 初始化
    - 使系统SW处于完备、正确的初始状态
  - 中断分析
    - 必要时才使用中断
    - 中断嵌套、中断保护和恢复、堆栈使用、优先级和约束、资源竞争、异常处理
  - 实时性
    - 提取模型最好，最坏情况
    - 超时保护
  - 可靠性
    - 关键软件进行SFMEA（单点）、SFTA（组合）
    - 可靠性增长、可靠性验证
    - 软件正确时，对硬件的容错，例如：冗余、看门狗、内存填充

嵌入式软件测试的难点及策略

- 变量（数据）与算法处理
  - 规定的安全性子集、经过静态分析，源、宿、类型、量纲、格式、值域、分辨率
  - 递推与迭代有溢出保护
  - 对不正确反馈有保护机制
  - 算法失败均做处理
  - 无不正确的循环操作和逻辑判断
  - 数据有效位满足要求
- 接口处理
  - 接口相关文件最新，软件需求、设计、软件使用规范一致
  - 应用软件的硬件接口需求、设计和器件使用手册一致
  - 接口交换数据：源、宿、类型、格式、传输速率、分辨率、吞吐量，在传输前检查信道

嵌入式软件测试的难点及策略

– 状态转移的处理

- 转移至需求规定的不允许状态的保护机制
- 事件和操作顺序正确
- 工作模式与环境条件应片配
- 处理和决策逻辑要完备

主要内容

- 嵌入式软件的特点
- 嵌入式软件测试的难点及策略
- 嵌入式软件测试案例
- 结束语

嵌入式软件测试案例

写入地址错误引起启动失败

- 概述：实现任务管理和调度,信号量和消息队列管理
- 问题:动态覆盖测试过程中,插桩烧写到目标机运行,出现异常,启动失败
- 分析：BSP启动程序插入插桩函数,桩函数中加了任务抢占锁,正常启动前任务TCB首地址为0，任务抢占函数对地址0X50地址进行了写操作,写入地址错误,引起异常
- 处理结果:修改BSP启动过程的桩函数,取消任务保护锁
- 经验教训:加强数据流分析和代码走查

嵌入式软件测试案例

初始化不正确造成时钟错误

- 概述：主要完成接收机的数据采集和处理，运行在80C31上
- 问题:接收机上电运行时，时间系统初始化出现错误，经过多次时钟修正才恢复正常
- 分析：软件在进行时钟初始化前未对星历的有效性和正确性进行判断，造成当接收机接收到错误星历时仍然进行时钟初始化，从而影响系统时钟
- 处理结果:加入星历健康判断
- 经验教训:在设计时加强异常分析，保证设计的可靠性

嵌入式软件测试案例

任务抢占导致打印数据的破坏

- 概述：实现任务管理和调度,信号量和消息队列管理
- 问题:动态覆盖测试过程中,打印任务输出的覆盖率信息不完整
- 分析：打印任务在读覆盖数据的过程被其他任务抢占,该任务修改了覆盖率数据,导致打印任务输出的覆盖率信息不完整
- 处理结果:打印任务加上任务抢占锁
- 经验教训:加强对多任务资源竞争分析

嵌入式软件测试案例

多任务嵌套时间冲突导致串行通信失败

- 概述：大规模实时控制软件。本机为控制器，下位机为执行机构处理器,二者均为反馈控制回路的组成部件.本机与下位机通过半双工异步串行通信口交换控制信息.通讯协议规定:如果本机未能按规定的数据格式和在规定的通信时间内完成数据的发送,则下位机不执行本次指令.
- 问题:在运行过程中,当分析其他分系统设备的工程数据时,发现在某个时间段内,本应连续的控制过程有间歇停控.回放故障时间段的工程数据,显示本机与下位机硬件工作正常;控制效果与目标值一致,但控制过程的进行时间大于预期值.

嵌入式软件测试案例

- 分析：分析下位机工作参数,排除下位机异常;以本机工作参数为依据,通过故障树分析,排除通信接口硬件故障;考虑到下位机是按每个控制周期中收到的指令执行输出,控制指令由本机软件按字节发送到串行通信接口缓冲器,如果在某个控制周期中指令字节未能按程序及时送达接口缓冲器,则字节间间隔可能超过协议规定值,该控制周期的控制指令被下位机绝执行.故障定位在本机向下位机发送数据时被中断干扰. 通过人工走查程序,有A中断周期为0.5秒,服务执行时间为5ms;B中断周期为1s,中断服务超时执行时间为2ms.这两个中断都有可能造成下位机接收字节间隔大于预期的230μs.
- 处理结果:与下位机通讯时关中断
- 经验教训:任务划分是实时系统软件概要设计的一项重要工作.任务划分优先于模块划分.任务分解应考虑任务间接口,时间特征和优先级;用人工走查辅助分析任务时间资源冲突

嵌入式软件测试案例

关中断指令使用不当导致复位措施失效

- 概述：实现实时采集和自主控制，软件包括2个定时器中断，1个外部中断，另外有1个看门狗；运行在DSP上；需求规格说明可靠性需求为：
  - 当软件跑飞时，看门狗触发硬件复位
  - 使用定时器监视主循环的执行时间，当其严重超时时，强行关闭硬件的总中断，迫使硬件复位，以让软件重启
- 问题:复位措施失效
- 分析：代码审查时发现，定时器中断0程序设计错误失效，该中断在退出时使用DISABLE-GIE语句，来实现关闭所有中断，迫使硬件复位，实际上DISABLE-GIE是关闭了全局中断使用标志，中断是否被禁止是在状态寄存器ST的实现；在C语言程序被中断时，中断程序将自动保护所有用到的寄存器，该寄存器用到了ST，退出中断时恢复了ST的内容

嵌入式软件测试案例

- 处理结果: 在DISABLE-GIE后加一条无限循环语句，不能退出中断，不能恢复ST的内容，超时后，看门狗触发硬件复位，完成软件重启的要求
- 经验教训:研制人员要深入细致地理解需求，这个案例中研制人员也受到需求的误导；要深入理解中断的编写方法和计算机的中断处理过程

中国航天

主要内容

- 嵌入式软件的特点
- 嵌入式软件测试的难点及策略
- 嵌入式软件测试案例
- 结束语

结束语

- 黑盒测试结合白盒测试
- 对于关键性软件要采取白盒测试
- 测试的环境
- 关注自检、初始化、接口、实时性、中断分析、可靠性等

中国航天

欢迎批评指正！

谢谢大家！