

嵌入式软件可靠性课程

目 录

《嵌入式软件可靠性与功能安全设计课程》大纲	- 1 -
-----------------------------	-------

《嵌入式软件可靠性与功能安全设计课程》大纲

课程介绍:

嵌入式软件的可靠性由两部分保证, 50%的工程化开发设计技术, 50%的工程化开发管理控制。开发技术的内容是嵌入式软件可靠性设计的规范, 开发控制的内容则由测试和过程管理共同完成。

嵌入式软件不同于管理系统类的上位机软件, 它与硬件的相互作用更为紧密, 与电路部分会产生更多更强的相互作用和影响。

因此, 无论是设计规范, 测试技术, 还是开发过程管理方面, 都有与硬件开发、系统软件开发不同的很多地方。重点体现在软硬接口、代码架构、变量和存储、人机接口、编译器、文档、测试方法等几个方面。

基于以上特点, 本课程从嵌入式软件的系统设计、需求分析、接口、模块、变量控制、软件测试、安全性分析、硬件匹配设计、测试方法的选择、测试用例的设计、测试内容等进行了总结讲授。

在交通设施、电梯等行业, 功能安全认证(SIL 或 ASIL)的推行, 也要求嵌入式软件部分有一些特定的设计内容, 这些内容规范的要求, 是为了保证产品运行中不至于因为产品的任何可能潜在问题而导致乘客、操作者、设备的安全隐患。作为可靠性要求的一部分内容, 本课程单独为此设计了一个章节。

本课程适于软件工程师、电子工程师、系统工程师、可靠性工程师、测试工程师、项目经理等。

讲师介绍:

武晔卿: 电子工程硕士, 专注于电子产品系统可靠性设计与测试技术, 曾任航天总体设计所主任设计师、高级项目经理, 电子产品制造企业研发总监, 北京市级优秀青年工程师, 科协委员。出版《嵌入式系统可靠性设计技术及案例解析》(北航出版社)。

曾为比亚迪、中电 30 所、29 所、中科院声学所、北京华峰测控、北京航天长峰、普析通用仪器、航天二院、航天五院、深圳蓝韵、伯特利阀门集团、松下电工、上海电气集团研究院等企业提供专业技术辅导、培训和咨询。

课程大纲:

1. 嵌入式软件可靠性基础
 - 定义软件可靠性定义
 - 软件可靠性的度量与评估
 - 软件与电子的失效率特性区别
 - 影响嵌入式软件可靠性的因素
 - 嵌入式软件归档及配置管理过程控制注意事项
 - 嵌入式软件可靠性系统分析方法与软件 DFMEA 的运用
2. 编译器问题嵌入式软件可靠性的影响

3. 代码编程规范对嵌入式软件可靠性的影响
 - 语句通用设计规范
 - 冗余设计
 - 睡眠设置抗干扰
 - 软件、结构、电路相结合的电磁兼容解决方法
 - 软件架构的设计方法
 - 安全性内核
 - 设计更改规则
 - 防跑飞的软件陷阱
 - 圈复杂度与软件测试
4. 与硬件接口问题对嵌入式软件可靠性的作用和影响
 - 时间受控
 - 空间受控
 - I/O 吞吐能力
 - 执行时间
 - 串并联接法导致的信号波动
 - 数据传输速率限制
 - 上电时序引起的硬件故障及软件初始化对策
 - 死机的机理及对策
 - 显示处理措施
 - SFC 下, 输出保证安全
5. 变量与存储问题成因与防护
 - 防止过程中存储被刷
 - 块存储特性
 - 备份技巧
 - 寄存器防刷处理
 - 强数据类型
 - 存储成功提示
6. 人机接口问题与防护
 - 对人工误操作的防护措施
 - 参数设置控制策略
 - 界面数据设置和布局方法
 - 界面设计规范
7. 报警
 - 报警分类设置
 - 报警编程处理
 - 报警频率、声音、占空比要求
8. 软件测试
 - 单元测试方法与系统测试的区别
 - 测试工具与人工测试
 - 测试职责与测试分工
 - 基于 SFC 的接口测试
 - 全覆盖测试(路径覆盖与数据覆盖)
 - 一致性测试, 通过软件测试发现硬件隐患
 - 人机接口测试
9. 嵌入式软件功能安全设计
 - 软件安全功能的要求
 - 软件结构的要求与措施
 - 详细设计和开发要求
 - 代码实现要求与措施

- 软件模块测试要求
 - 软件集成测试的要求
 - 功能安全评估方法
10. 总结: 嵌入式软件可靠性设计规范