华东师范大学软件学院课程作业

课程名称：软件质量分析	年级：2023 级本科	姓名：张梓卫
作业主题：总结软件可靠性定义	学号：10235101526	作业日期：2024/10/16
指导老师：陈仪香	组号：	

目录

一 C919 的可信属性模型

1 可靠性

1.1 结构完整性

- 机身结构设计
- 高强度材料应用
- 抗疲劳性能

1.2 飞行控制可靠性

- 冗余飞行控制系统
- 自动驾驶仪可靠性
- 软件验证与验证（V&V）

1.3 发动机可靠性

- 发动机性能稳定性
- 故障保护机制
- 实时监控与诊断
- 自动化应急处理
- 乘客和机组安全措施

1.4 系统可靠性

- 各系统稳定运行
- 故障率低
- 关键组件高可靠性
- 供应链质量管理

2 可维护性

2.1 维护便捷性

- 模块化设计
- 易于更换的部件
- 全球备件网络
- 快速供应链响应

2.2 诊断与技术支持

- 内置健康监测
- 预防性维护
- 详细维护手册
- 培训与支持服务

3 安全保障

3.1 网络安全

- 防范网络攻击
- 通信加密
- 数据加密存储
- 访问权限控制

3.2 物理安全

- 未授权进入防护
- 安全的舱门设计

4 性能

4.1 燃油效率

- 空气动力学优化
- 高效发动机技术
- 低排放技术
- 降噪设计

4.2 航程和载荷

- 满足设计航程
- 优化载客量

4.3 环境性能

5 人机工程

5.1 驾驶舱设计

- 人体工程学布局
- 直观的界面
- 自动化辅助
- 降低飞行员疲劳

5.2 乘客舒适性

- 优化客舱环境
- 座椅和空间配置

6 可支持性

6.1 培训计划

- 飞行员培训
- 维护人员培训
- 24/7 支持服务
- 全球服务网络

6.2 客户服务

- 售后支持
- 客户反馈机制

7 运营效率

7.1 成本效益

- 降低运营成本
- 燃油经济性
- 快速登机卸货
- 地面服务优化

7.2 基础设施兼容

- 适应现有机场设施
- 兼容地面设备

8 创新性

8.1 先进技术

- 新材料应用
- 先进制造工艺
- 产品升级计划
- 技术研发投入

8.2 数字化

- 数字孪生技术
- 智能数据分析

二 安全属性的定义

软件产品质量属性中的安全性是指在软件生命周期内 [1]，应用安全性工程技术，防范和应对各种恶意攻击、非法使用以及内部泄漏，从而确保软件在系统上下文中执行不会导致系统发生不可接受的风险 [2]，防止对程序及数据的非授权的故意或意外访问，确保降低错误已控制在可接受风险水平内的与软件能力有关的软件属性。其包含三个子属性：信息保护性、数据完整性、可恢复性。[3, 4, 5]

三 安全属性的三个子属性及涵义

1 数据保密性 [6]

涵义：通过加密、访问控制等技术手段，确保只有被授权的用户才能访问或修改特定数据。

2 代码安全性

涵义：以代码审查、签名验证和防篡改等技术，确保代码的完整性和可靠性，防止恶意代码注入。

3 控制保密性

涵义：从控制命令加密、身份验证等手段中，防止系统控制权限被未授权用户获取或篡改，确保操作安全。

四 基于全生命周期的度量元设计

1 数据保密性

- **需求分析阶段**：定义需要保护的敏感数据类型和访问策略的完善程度。
- **设计阶段**：加密算法的强度及数据加密传输的覆盖率。
- **实现阶段**：数据加密机制的实现情况及身份验证机制的实施效果。
- **测试阶段**：通过渗透测试和漏洞扫描验证数据保密性的有效性。

2 代码安全性

- **需求分析阶段**：代码安全需求的识别和完整性。[6]
- **设计阶段**：防篡改设计方案的健全性，代码签名和验证机制的设计。
- **实现阶段**：代码静态分析工具的应用及漏洞修复率。
- **测试阶段**：动态分析及模糊测试的通过率，是否存在潜在的代码漏洞。

3 控制保密性

- **需求分析阶段**：控制命令安全需求的定义及控制访问策略的制定。
- **设计阶段**：控制命令加密机制的强度及访问控制机制的设计。
- **实现阶段**：控制命令加密及访问控制机制的实施情况。
- **测试阶段**：通过安全审计和模拟攻击验证控制保密性。

五 基于出厂报告的度量元设计

1 数据保密性

- **A 级**：敏感数据的加密和访问控制机制非常完善，所有数据均通过高级加密标准加密，且通过了严格的安全测试。
- **B 级**：大部分敏感数据均已加密，只有少数非关键数据未完全加密，安全测试基本通过。
- **C 级**：只有部分敏感数据进行了加密处理，存在部分漏洞，安全测试结果显示数据有泄露风险。
- **D 级**：数据加密及访问控制机制不完善，敏感数据容易被未授权访问，安全风险较高。

2 代码安全性

- **A 级**：代码经过全面的静态分析、动态分析及安全审计，所有已知漏洞均已修复，代码签名验证机制完整。
- **B 级**：代码经过部分静态分析和审计，主要漏洞已修复，但存在少量未修复的低风险漏洞。
- **C 级**：代码只经过简单的安全审计，未能修复所有发现的安全漏洞，存在中等安全风险。
- **D 级**：代码未经过系统性的安全审计，存在大量已知和潜在的安全漏洞，安全风险极高。

3 控制保密性

- **A 级**：控制命令经过严格的加密和访问控制，具备全面的审计和恢复机制，且通过了高强度的安全测试。
- **B 级**：控制命令大部分经过加密处理，访问控制机制较为完善，但未覆盖所有控制指令。
- **C 级**：控制命令只有少部分进行了加密，访问控制机制存在漏洞，未能防止未授权访问。
- **D 级**：控制命令未经过加密处理，访问控制机制薄弱，系统面临较高的被篡改或攻击风险。

六 参考资料

- 软件产品质量模型 8 个属性：https://www.jianshu.com/p/89cff6038bea
- 11 种方法判断软件的安全可靠性 ：https://blog.csdn.net/qq_44005305/article/details/139471105
- 提升数据保密性的策略：https://wenku.baidu.com/view/29dd73485322aaea998fcc22bcd126fff6055d50.html

参考文献

References

[1] NA Space. “National Aeronautics and Space Administration”. In: *Retrieved from National Aeronautics and Space Administration: www. nasa. gov* (1977).

[2] Nancy G Leveson. “Software safety: Why, what, and how”. In: *ACM Computing Surveys (CSUR)* 18.2 (1986), pp. 125–163.

[3] 沈国华 et al. “软件可信评估研究综述: 标准, 模型与工具”. In: *软件学报* 27.4 (2016), pp. 955–968.

[4] 王怀民 et al. “基于网络的可信软件大规模协同开发与演化”. In: *中国科学: 信息科学* 44.1 (2014), p. 1.

[5] 刘彦钊 et al. “一种基于属性划分的软件可信性度量模型研究”. In: *Computer Science and Application* 2 (2012), p. 121.

[6] Istehad Chowdhury, Brian Chan, and Mohammad Zulkernine. “Security metrics for source code structures”. In: *Proceedings of the fourth international workshop on Software engineering for secure systems*. 2008, pp. 57–64.