论软件的可靠性设计与应用

摘要

当今各软件运行大环境日趋复杂化和多元化，高可靠性这一质量特征在软件的生命周期具有举足轻重的作用。全文以笔者所在公司为某省安全科学研究院开发的智慧管网系统为实例展开，浅谈了软件的可靠性设计与应用的必要性和重要性认知；由于此管网系统的核心功能是对客户端请求消息的分阶段解析与处理，并要求在 HTTP 报头分离、SOAP 报文解析等过程中具有高可靠性。项目组结合软件可靠性设计与应用的原则，结合此前类似系统的设计实现经验，决定应用管道－过滤器架构风格和责任链设计模式，并使用 RocketMQ 作为消息中间件对高并发消息进行处理，对交互的数据进行强数据验证机制，软件系统中采用软件容错的 N 版本程序设计技术，对消息通讯、封层架构模块进行负载均衡设计。最终项目于 6 个月后成功交付验收，在项目系统投运后一直非常稳定，得到该研究院的一致好评。

正文

2017 年 3 月，我作为项目负责人参与了为某省安全科学研究院开发的智慧管网平台系统的设计实现工作。该系统面向于三类方向：与异构云平台数据集成、与企业信息系统数据集成、面向企业终端的业务控制。具有数据获取、数据清洗、消息通讯、业务处理、分层架构的功能。其核心流程为：实现通过无线传输 SINK 节点，以服务器联网通过 TCP/IP 按照既定传输数据解析协议将数据上传到服务器，并以控制协议，接收/解析控制指令。系统为 Java Web 项目，采用技术包括 Springboot、数据持久层 Mybatis、权限 Shiro 实现。

一、影响产品可靠性的原因

要提高产品的可靠性指标，首先要分析影响产品可靠性的原因。一般来说影响产品可靠性的原因有如下一些：

1、运行环境，软件可靠性定义是相对于运行环境而言的，一样的软件在不同的运行环境下其可靠性是不一样的。不同的用户操作习惯不同，会影响软件的可靠性。软件的可靠性是软件缺陷和用户的可预测性的一个复杂函数。

2、软件规模，也就是软件的大小。一个只有几百行代码的软件和一个几千万行代码的软件是不能相提并论的。

3、软件内部结构，结构对软件可靠性的影响主要是软件的复杂程度，一般来说，结构越复杂的软件，所包含的软件缺陷数就可能越多。在进行软件设计时就要有意识地采用各种降低复杂度的架构策略，如模块化设计，分层设计等等。分而治之的方法是最好的降低复杂度的方法。

4、软件的开发环境和开发方法，软件工程表明，软件的开发方法对软件的可靠性有显著地影响。例如，与非结构化开发方法相对，结构化方法可以明显减少软件的缺陷数。

5、软件的可靠性投入，软件在生命周期中的可靠性投入包括可靠性设计、可靠性测试、可靠性管理和可靠性评价等方面投入的人力、资源、资金和时间等。

二、主要的软件可靠性设计技术

1、容错设计技术。对于软件失效后果特别严重的场合，例如宇航器控制系统、空中交通控制和核反应堆控制系统等，可采用容错设计方法。常用的软件容错技术主要有恢复块设

计、N 版本程序设计和冗余设计。恢复块设计就是选择一组操作作为容错设计单元，从而把普通的程序块变为恢复块。一个恢复块中包含有若干功能相同、设计差异的程序块，每一时刻有一个程序块处于运行状态，一旦某程序块出现故障，则用备份程序块予以替换。N 版本程序设计的核心是通过设计出多个模块或不同版本，对于相同初始条件和相同输入的操作结果进行多数表决（防止因其中某一软件模块 / 版本的故障而提供了错误的服务，以实现软件容错）。冗余设计的思路来源于硬件系统，但有所不同。软件冗余设计技术是采用多种不同路径、不同算法或不同实现方法的模块或系统作为备份，在出现故障时进行替换，维持系统的正常运行。

2、检测技术。在无须在线容错或不能采用冗余设计技术的部分，但又有较高的可靠性要求时，一般采用检测性设计，在软件出现故障后能及时发现并报警。但其明显的缺点是不能自动解决故障，如果没有人工干预，最终将导致系统不能正常运行。

3、降低复杂度设计。软件的复杂性与软件可靠性有密切关系。软件复杂性是产生软件缺陷的重要根源。降低复杂度设计的思想就是在保证实现软件功能基础上，简化软件结构。

结束语

经过项目组近 6 个月的努力，该智慧管网平台项目自成功交付验收后，运行一直非常稳定，得到该研究院的一致好评。通过本次开发实践我明白了软件的可靠性在实际应用中的重要地位。要提高软件的可靠性就要在先期开发时就重视软件的可靠性设计，实施可靠性管理，并将软件的可靠性原则和思想贯穿于在项目的各阶段和各生命周期。