

论非功能性需求对企业应用架构设计的影响

【摘要】

2017年5月,我参加了某省质量技术监督局“生产制造一体化监管平台”项目(以下简称一体化平台),担任系统架构师职务,负责整体架构设计与中间件选型。该系统以监管企业生产制造为主线,旨在帮助各级监督部门解决监管企业生产、报审、送检、勘验、巡检和执法等问题。本文以一体化平台为例,论述了非功能需求对系统架构设计的影响。并详细说明在项目实施过程中如何通过架构设计来满足非功能需求。实践证明在架构设计中通过对非功能性需求的满足,保证了系统在质量属性和约束条件上与客户要求保持一致,使开发工作取得了成功。一体化平台于2018年10月验收上线,目前已稳定运行1年时间,得到了各级监管部门和企业一致认可和好评。

【背景】

质量技术监督在生产领域、市场流通领域等方面都起到至关重要的作用,关乎到企业生产和人民生活。某省质量技术监督局在信息化方面起步较早,先后建设了数套专项系统,但缺乏对业务的统一监管,为贯彻落实国家市场监督管理总局《关于加快推进质量体系监管信息化建设要求》,一体化平台的建设工作受到各级领导的关注。项目建设目标覆盖省、市、县区三级质量监管部门及全省三十多万家企业,为工业生产、报审、送检、勘验、巡检和执法工作提供支持。我所在公司长期从事相关行业的软件开发,对质量监督领域有着丰富经验,因此顺利中标承建了该项目,初期投入15名技术人员由我担任架构师职务,负责软件架构设计和中间件选型。

项目启动后通过对业务的梳理,初步将一体化平台划分为四大模块,其中政务服务模块针对的是通过互联网访问系统的企业用户,在功能上主要包括报审、送检、公示和政策法规宣传等功能;而其它三个模块针对的是通过电子政务外网访问系统的监管部门和事业单位用户,其中运行管理模块主要功能包括审批、勘验、颁证、建档;企业监管模块主要功能包括巡检、执法;电子监察模块主要功能包括实时监控、预警纠错和效能评估。

【回应论点二】

在架构设计开始阶段我意识到非功能性需求对架构设计的重要性。虽然在需求分析时功能性需求是客户普遍关注焦点,但作为架构师绝不能忽视对非功能性需求的分析,它与系统的总体特性相关,从质量属性和条件约束两个方面同时对架构设计产生影响。在架构设计中普遍关注的质量属性包含性能、可用性、安全性、可修改性、可靠性、易用性、可测试性等,其中前4项是质量属性效应树的重要组成部分,通过质量属性效应树又可进一步分析出架构设计中的敏感点、权衡点和问题决策带来的风险隐患。而条件约束主要来源于用户的限制包括了预算、机构政策和其它软硬件交互的外部因素,例如遵守什么样的行业标准、使用哪个厂商的产品、采用哪种开发技术等。下面从实施性能、可用性、安全性、可修改性四个质量属性和过程中受到的条件约束两方面,详细说明如何通过架构设计来满足非功能需求。

【回应论点三】

一、性能设计，性能是指系统响应能力，包括速度、吞吐量和持续高速性三方面的要求。针对性能方客户提出第一，系统应具有快速的响应能力，在网络负载正常情况下打开界面的平均响应时间小于 1.5 秒，在线查询和提交操作的处理时间小于 2 秒；第二，系统应能承受每年 11 月底全省企业集中年审带来的负载压力。对于性能需求在架构设计中可选的方案有优先级队列、增加计算资源、减少计算开销、引入并发机制、采用资源调度等。本次架构设计上我采用了优先级队列和增加计算资源两个方案，首先采用 RabbitMQ 消息组件使系统以消息为中心进行交互，可保证请求的处理顺序，特别是在高并发情况下可解决流量削峰问题。然后在数据层使用了读写分离技术，采用 Memcache 作为查询数据库，分担主库负载提高查询速度。但在接下来的主库设计上受到了用户方来自政策的约束，由于近年来政府部门推行国产化，新建系统必须使用国产数据库，经过对比分析最后选择了在政府部门应用较广的达梦数据库作为主库使用。

二、可用性设计，可用性是指系统能正常运行的时间比。针对这个方面客户提出第一，必须保证系统 7*24 小时持续提高服务的能力；第二，在网络失效或主机断电的情况下，系统必须保证在 3 分钟内启用备用设备恢复正常服务。对可用性需求在架构设计中可选的方案有心跳、Ping/Echo、冗余、进程监视器。本次架构设计上我采用了心跳技术和冗余技术，使用 keepalived 组件构件双机热备环境，用户通过虚拟 IP 访问，当 Master 宕机自动切换到 Backup 继续运行，防止因为单点故障导致系统瘫痪。但接下来在与信息中心沟通时受到了硬件资源上的约束，因服务器资源紧张部署策略不得不由双机热备后改为双机互备，在性能和可用性上求得了平衡。

三、安全性设计，安全性是指软件系统可向合法用户提供服务，以及阻止非授权使用服务的能力。针对这个方面用户提出必须保证企业用户通过互联网访问系统的安全防止欺诈和篡改。对安全性需求在架构设计中可选的方案有用户认证，用户授权，追踪审计，限制访问。本次架构设计上我采用了用户认证技术，使用 SSL 证书+Ukey 双向认证方式，只须插入 Ukey 即可登录系统，每个 Ukey 在服务端均与用户身份进行了绑定。但在方案评审时受到了用户方预算上的约束，由于因 CA 每年会向单个 Ukey 设备收取 200 元左右的年费，全省企业将是一笔巨款，因此经过折中确定为仅向大型国有企业发放 Ukey，并且费用自理，以节省资金预算。对于普通中小型企业采用了服务端 SSL 证书+客户端动态验证方式。

四、可修改性设计，可修改性是指能快速并以较高性价比对系统进行变更的能力。针对这个方面用户提出近年来国家在不断推进政府改革工作，系统应该能够适应不断变化的业务环境，可快速的实现业务的新增、修改。对可修改性需求在架构设计中可选的方案有抽象、信息隐藏、限制通信路径、运行时注册。本次架构设计上我采用 Java 语言作为主开发语言，保证程序的抽象和信息隐藏，同时使用 Spring 框架管理 JavaBean 运行时注册，最后在架构上采用了服务化设计，将系统拆分成若干独立服务相互间通过消息进行通信，降低系统耦合度。但在设计与异构系统通信时，受到了来自用户现行技术标准上的约束，由于已投入使用的部分旧系统仅支持 webservice 技术，因此一体化平台在只能采用相同的方式与这些系统进行交互。

【结尾】

实践证明在架构设计中通过对非功能性需求的满足，保证了系统在质量属性

和约束条件上与客户要求保持一致，使开发工作取得了成功。但项目过程中也遇到过问题，因客户单位部分用户派驻到办事大厅工作，窗口办公需要配合高拍仪、读卡器等硬件设备，而浏览器出于安全考虑隔离了 web 程序调取本地资源仅提供有限支持，给系统推广带来了困难。对此我采用了富客户端技术，使用 Electron 框架封装了一个客户端程序，专门负责调取硬件资源及时解决了该问题，没有对项目造成实质影响。

通过项目组全体成员的共同努力，一体化平台于 2018 年 10 月完成验收工作正式上线，截至目前系统运行稳定运维工作量可控，得到了监管部门和企业用户的一致认可和好评。通过这个项目本人更进一步了解到系统架构设计的重要性，同时积累了很多宝贵的经验。在今后的工作中我将不断总结和提升专业技术能力，争取为我国信息化事业贡献一份力量。

版权声明：本文为 CSDN 博主「飘狐」的原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接及本声明。

原文链接：<https://blog.csdn.net/hamster204/article/details/103596456>

樊樊的资料库，仅供个人学习

樊樊的资料库，仅供个人学习