系统分析师论文（60 页）

论软件的组件式开发

摘要：

在我所担任的某移动短消息增值应用系统的规划和开发工作中，面对移动短消息广阔的应用领域，和众多不同行业的 ASP，巨大的软件开发工作量。我们选择了组件式软件开发方式，在系统的功能、性能、开发效率和投资等方面都达到了理想的效果。

正文：

2000 年 10 月我开始担任四川某网络公司移动短消息增值应用系统（简称 SMASP）开发部的负责人，主要工作是对 SMASP 进行规划并实施开发，为总经理提供 SMASP 开发的参考方案。SMASP 的通信服务提供商为中国联通公司，服务内容提供商为如：出租车调度系统的出租车管理公司；电码防伪系统的商用电码公司；水电气三表抄表系统的水电气公司；移动证券系统的证券公司等，还有许多已知的和未知的对移动短消息增值应用有潜在需求的应用领域会不断地加入到 SMASP 中来。SMASP 首期工程应用到联通四川公司，二期工程将推广到山东、河南、广东、福建、湖北等省市，并逐步推广应用到全国联通。由于项目处于起步阶段，还没有定型的系统模型及成功的应用模式，因此，选择一个好的系统体系结构和开发模式就成为当务之急。

对领域的选择。通常一个领域的专用资产要应用到不相关的领域是比较困难的，组件式开发的首要工作是领域工程，在这个领域内提取可被复用的系统对象，创建可复用资产，开发复用组件。而 SMASP 正好是这样一个面对具体应用领域的，系统需要不断升级，有着长期的持续开发需求。因此，在 SMASP 建设的初级阶段，为 SMASP 创建复用资产是可行的，有回报的。

对组件（COM）式体系结构的选择。SMASP 已经有一部分应用是建立在 Windows/NT 服务器上了，但考虑到本系统将推广到全国各地联通公司，将来的远程系统维护和远程操作控制以及系统整体性能的需要，我建议公司将系统后台应用部分移植到以 SUN 系统为主的 UNIX 系统上来，这一建议得到了公司的支持。我们的服务内容提供商是各式各样的，处在不同的行业，有不同的应用系统在运行，对 UNIX、WINDOWS、WINDOWS/NT、LINUX、NETWARE 等都有应用，是一个多平台系统。为对这样一个多平台、多应用、长期持续开发的系统选择一个良好的体系结构和开发方式，将决定在将来的开发实践中 SMASP 的质量、连续可用性、可升级维护性、可扩展性、开发工作量和投资等各项指标。经过反复考虑，我们将整个系统划分为各个独立的组成对象，各对象独立工作又相互协调来完成系统的功能，这样各个独立的对象就形成了系统的组件。在这些组件中，有些是 SMASP 内通用的，其功能定义在系统内长期稳定；也有面对不同 ASP（服务内容提供商）的各式各样的组件。这些组件的开发工作均相对独立，互不干扰，因此可以实现系统的无代演进。

创建复用资产和复用组件。通常可以被复用的资产是在领域内通用性比较好的对象。通过深入的分析，我们决定建立短消息增值应用系统平台 MISPlatform。MISPlatform 本身是由多个组件构成的多层次的、组件化的体系结构，在他上面运行的 ASP 的各种应用也可看作 MISPlatform 的各个组件。MISPlatform 的体系结构，各组件的详细定义，接口定义，专化规范，大量代码以及各部分的文档都是潜在的可复用资产。复用资产和复用组件之间有一定区别，复用资产的范围相对广泛，而复用组件则更为具体，通常指可以直接嵌入到目标系统内或独立运行以完成某一特定功能的程序模块或对象。并不是所有可复用资产都可以制作成复用组件的，在划定了复用资产后还要进一步提炼，如我们在 MISPlatform 中创建的基本表管理组件、索引管理组件、TCP/IP 通信组件、接口组件、加密组件等，都具有很好的通用性。

通用接口的定义。在组件式开发中，由于系统是依靠预制的或独立运行的组件协同工作来达到系统功能目标，各组件之间对信息的交换就成为必然，而要使各组件之间顺利交换信

息，就需要定义一个各组件都能解析的通信接口。在我们的系统中 SORBA（短消息对象请求代理结构）承担了这个角色，他的定义能为 MIS Platform 中所有组件识别和解析，成为组件协同工作的纽带。SORBA 的定义要考虑到独立于平台、独立于操作系统、独立于编译系统、独立于开发工具，因为在这个应用范围广大的多平台、长期持续开发的应用系统中，我们无法保证大家都使用相同的开发工具，即使开发工具相同，也不可能保证通信的数据结构绝对不发生改变，因此 SORBA 的定义的独立性和灵活性就相当重要。

在各种平台下实现组件。由于我们的系统是多平台的，所以复用组件也需要在多平台下实现。而目前大家讨论得多的如 COM、CORBA、ActiveX 等是以 WINDOWS 为平台的，WINDOWS 能够提供给组件的实现方式为 DLL 或 OLE 技术。而我认为，这个理解是狭隘的，组件可以以多种方式在多种平台下实现。在 WINDOWS 系统上除了 DLL 和 OLE 外，还可以使用静态连接、消息队列等方式来实现；在 UNIX 上可以采用静态连接、消息队列、共享内存等技术来实现。可以看出，在 UNIX 和 WINDOWS（2000 以上版本）上均提供了消息队列。MISPlatform 中独立运行的组件是通过消息队列联系起来的，在 UNIX 和 WINDOWS 下均采用这个机制，如加密组件和通信组件之间、短消息处理中心和通信组件之间、通信组件和 ASP 应用组件之间均通过消息队列通信。而嵌入式组件如基本表、索引、SORBA 接口协议等组件在 UNIX 下的实现采用的是静态连接技术，在 WINDOWS 下采用静态连接和 DLL 两种技术。不管是嵌入组件还是独立运行的组件，在实现的时候都应当考虑多平台的需求，组件要独立于开发工具、具有高度的可塑性、接口清晰可靠。

对第三方开发的支持。我们不能保证在整个 SMASP 的建设过程中始终都由我们一家承担所有的软件开发工作，MISPlatform 提供对第三方开发的支持是必须的。第三方开发者只要得到 SORBA 接口组件“DataPack.DLL”（在 Windows 下）或“DataPack.Lib”（在 Windows 下或 Unix 下），及相关的文档资料，他们即可访问 MISPlatform，不管 MISPlatform 如何升级换代，也不管 MISPlatform 是由什么平台来提供服务，我们的客户都不必修改他们的应用系统。

重视培训工作。我们的多层次组件式体系结构首先是由极少数的几个核心开发人员所掌握的，而在 SMASP 的建设工作中，其他软件人员的工作也是不能忽视的，还有人员的流动更新。大家在 SMASP 中的工作是协作性的，为了把大家都纳入到整个系统的应用体系结构中，必须首先让大家了解体系结构，熟练掌握可复用资产和复用构件，这样才能使大家知道自己所做的工作在整个系统中的位置，以及怎样使自己所做的软件和整个系统有机地结合起来，怎样进行组件的专化。最初，我们认为只要将构件的设计文档等资料共享给大家，我们的程序员就知道去学习和使用，而实际上，这些程序员都养成了不爱看别人软件及文档的习惯，他们喜欢无论什么都自己做，所以，尽管我们的 SORBA 接口和系统体系结构的相关文档都共享了，但大家只对 SORBA 接口看了一些，而对体系结构就不怎么关心了，更谈不上遵守系统体系结构。培训工作实际上是非常重要的，没有培训工作，大家就很难理解整个系统的体系结构，复用资产也形同虚设。在 SMASP 的开发中，组件也不是一成不变的，需要升级和增加新的内容，大家对体系结构的认识应当不断强化，因此，我们培训工作也需要不断的开展，持之以恒。

综上所述，在组件式软件系统开发工作中，我们首先要选定一个领域，然后确定软件的体系结构，挖掘潜在的可复用资产，创建复用构件，持之以恒的培训工作，让我们的软件人员都在充分理解系统体系结构以后随心所欲地使用复用构件，我们的组件式开发工作就能达到满意的效果。

远程接入中的安全访问控制

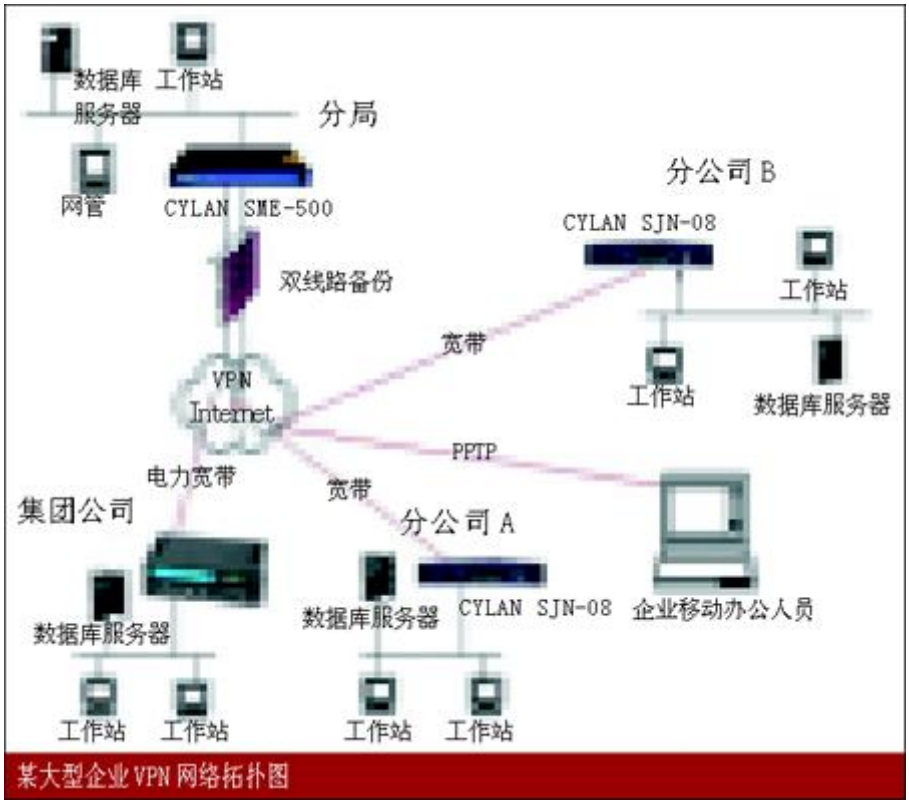
VPN 技术、防火墙的安全过滤技术、三层交换机的路由和控制技术共同实现了远程用户对企业不同应用域的安全访问控制。

大型企业通常会有若干分驻全国各地的分支机构和为数不少的出差人员，为了解决这些员工的远程办公问题，使他们能够及时了解企业运转情况和参与生产、经营、管理工作的流程运转，远程接入成为一个现实的需求。而 VPN 的出现使得安全、经济地实现远程办公成为可能。通过 VPN 接入，企业可以保证出差在外的员工访问公司里的信息，更进一步，通过笔记本电脑和一张带基于 VPN 的 CDMA1X 卡，员工可以真正实现随时随地访问企业局域网的愿望。

远程访问的主要技术手段

附图是某大型供电企业网络远程访问系统的拓扑图，主要由 VPN 客户端软件、VPN 客户端 E-Key、VPN 网关、密钥管理中心、防火墙和策略路由交换机组成。该系统解决了企业员工通过多种网络环境，利用互联网通道访问企业内部网络资源的需要。通过身份认证系统确保了远程网络用户的真实性；通过对网络传递数据的加密，确保了网络传输数据的机密性、真实性和完整性；通过对用户的分级管理和访问管理域的划分，设定了不同类别的认证用户对 OA 办公区域、输变电生产管理区域、配网生产管理区域、市场营销管理区域等不同应用区域的访问权限，有效降低了企业信息资源的潜在风险。

如附图所示，系统主要采用了 PKI 技术、IPSec 技术、防火墙技术和策略路由交换技术。其中，IPSec 技术是一个关键组成部分，而经济、灵活、安全是该企业选择 IPSec 技术的主要原因。



经济：不用承担昂贵的固定线路的租费。DDN、帧中继、SDH 的异地收费随着通信距离的增加而递增，分支越远，租费越高，而基于 Internet 则只承担本地的接入费用。此外，VPN 设备功能强劲但造价低廉。

灵活：连接 Internet 的方式可以是 10M、100M 端口，也可以是 2M 或更低速的端口，还可以是便宜的 DSL 连接，甚至可以是拨号连接。

广泛：IPSecVPN 的核心设备扩展性好，一个端口可以同时连接多个分支，包括分支部门和移动办公的用户，而不像 SDH、DDN 等一个端口对应一个远端用户。

多业务：远程的 IP 话音业务和视频也可传送到远端分支和移动用户，连通数据业务一起，为现代化办公提供便利条件，节省大量长途话费。

安全：IPSecVPN 的显著特点是它的安全性，这是它保证内部数据安全的根本。在 VPN 交换机上，通过支持所有领先的通道协议、数据加密、过滤/防火墙、通过 Radius、LDAP 和 SecurID 实现授权等多种方式保证安全。同时，VPN 设备提供内置防火墙功能，可以在 VPN 通道之外，从公网到私网接口传输流量。

系统的实现

该大型企业采用北电的 PP8606 路由交换机，以提供不同应用安全域的网段划分和策略控制。同时，部署有带 VPN 功能的 NetEye 防火墙，它集 VPN 网关、密钥管理中心、防火墙于一体，提供密钥的生成、管理与分发，完成认证区域的划分、用户的接入和用户的认证、用户 IP 地址的分配与访问控制功能。

1.通信密钥的生成与管理。VPN 网络安全的关键是保证整个系统的密钥管理安全。NetEyeVPN 采用基于 PKI 的密钥管理框架，实现安全可靠的密钥分发与管理。

密钥管理中心设立在网络中心。登录密钥管理中心后，在密钥加密卡内生成 RSA 公私钥对，通过使用专用的密钥加密卡作为密钥传递介质，并采用密钥加密密钥，保证了密钥颁发过程中的安全性。然后通过密钥管理中心，添加 VPN 网关的 IP 地址和密钥交换端口信息，生成网关密钥和全局公钥文件，全局公钥文件使用管理中心的私钥签名，可以防止在传送过程中被替换或篡改。

2.VPN 网关的密钥配置及用户 E-Key 的生成。上载合适的 License 许可后，就开启了 NetEyeVPN 防火墙的 VPN 功能，形成 VPN 网关。对 VPN 网关注入密钥管理中心生成的网关密钥对和全局公钥文件后，就可以在 VPN 网关上建立用户认证域。创建时可以选择本地认证或 Radius 认证，在认证域中创建用户，添加用户名和用户密码信息，生成用户 E-Key。用户 E-Key 主要保存用户认证证书文件和用户名信息，以增强用户认证的安全性。

3.用户的登录认证与数据传输安全性的保证。当 VPN 用户通过 VPN 客户端软件和 VPN 客户端 E-Key 对 VPN 网关发送连接请求时，VPN 网关对 VPN 用户进行鉴别与认证。其中会话密钥按照 IKE 协议，自动协商生成，并用协商好的密钥对数据进行加密。用户认证成功后，通过创建 SA 以及 SA 的组合(AH、ESP、IPIP)建立远程用户的访问隧道。NetEyeVPN 遵循 IPSec(IPSecurity)安全协议，采用隧道方式为用户数据提供加密、完整性验证，并通过集成的认证服务，为信息传输提供安全保护。NetEyeVPN 采用 IP 封装，将原来的 IP 包加密并添加认证信息后，完全封装在新的 IP 包中。新 IP 包中 IP 头的源地址和目的地址分别是用户端和 VPN 网关的外部地址，IP 包经过这样的封装后，在公网上传输时隐藏了内部网拓扑，增强了网络的安全性。另外，通过采用标准的 AH 和 ESP 协议，保证了 IP 包的机密性与完整性。

4．应用区域的划分。在 VPN 网关的认证域中创建用户时，针对不同性质的用户创建了多个角色名称，分别对应于 OA、生产、配网、营销等应用区域。设定 VPN 网关隧道虚拟设备 IP 地址池，将池中 IP 地址分别分配到角色中，对应各应用域。在用户登录并经过认证后，用户将根据自己所属的角色分配 IP 地址，并自动加入到自己的应用域中。

系统的安全访问控制

VPN 用户和 VPN 网管之间在公网上建立 VPN 网络通道之后，还需要进一步通过安全策略和安全规则的制定，把网络分成不同的安全访问区域，控制用户对不同安全区域的访问，

使网络的安全性得到进一步提升。访问控制系统一般针对网络资源进行安全控制区域划分，以实施区域防御策略。通常在区域的物理边界或逻辑边界设置许可或拒绝访问的集中控制点，结合局域网络内部利用智能化以太网络交换设备所提供的虚拟网络、ACL 访问控制列表、多层过滤等功能或广域网络的路由设备进行访问控制。但这些技术本质上都是基于 MAC 地址或 IP 地址、端口号列表的静态过滤控制，对于安全要求更高的用户则需要采用基于 IP 会话状态检测的动态防火墙技术。

防火墙一般位于企业网络的边缘控制点，如与 Internet 连接处，甚至还可以部署在企业网络内部的安全区域控制点上。安全区域防御的弱点是不能抵御来自区域内部的"合法"用户的攻击，如恶意或无意的内部用户，没有防火墙和安全保护较弱的远程移动工作者或 SOHO 被身份窃取者，以及安全区域存在的后门漏洞(无线网络、远程访问)等情况。为进一步提高网络的安全控制，分布式防火墙模式应运而生，一般在主机或工作站点安装软件防火墙，实施对资源点的保护。不过，软件分布式防火墙是基于操作系统之上的，如果操作系统本身存在安全漏洞或因为用户的使用管理问题使该防火墙被关闭，将造成严重的安全隐患。

采用防火墙技术，通过制定安全策略，可以实现对用户的访问进行控制和过滤。主要过滤内容为用户访问信息的源目的 IP 地址、目的端口号、连接协议等。经过防火墙安全控制策略过滤后的 VPN 用户将根据其所属角色及分配的 IP 地址范围访问经过授权的应用域，比如只能访问 OA、生产管理、配网管理和营销应用域的其中之一或者几个域的组合。

采用北电的 PP8606 路由交换机，对不同的被访问应用安全域进行网段划分，建立网段连接路由信息和 VPN 客户 IP 返回路由。在路由交换机与 VPN 网关的互连端口上进行访问过滤控制策略，制定只允许合法的源 IP 地址、协议访问对应的应用域。以进一步加强 VPN 用户对应用安全域的访问控制，从而在最大程度上减少了安全风险和不安全因素。

网络安全评估

网络架构分析

网络架构分析的主要内容包括根据 IATF 技术框架分析网络设计是否层次分明，是否采用了核心层、汇聚层、接入层等划分原则的网络架构（划分不规范不利于网络优化和调整）；网络边界是否清晰，是否符合 IATF 的网络基础设施、边界/外部连接、计算环境、支撑基础设施的深度防御原则（边界不清晰不便于安全控制）。应考虑的安全点主要有：

1.网络架构设计应符合层次分明、分级管理、统一规划的原则，应便于以后网络整体规划和改造。

2.根据组织实际情况进行区间划分，Internet、Intranet 和 Extranet 之间以及它们内部各区域之间结构必须使网络应有的性能得到充分发挥。

3.根据各部门的工作职能、重要性、所涉及信息等级等因素划分不同的子网或网段。

4.网络规划应考虑把核心网络设备的处理任务分散到边缘设备，使其能将主要的处理能力放在对数据的转发或处理上。

5.实体的访问权限通常与其真实身份相关，身份不同，工作的内容、性质、所在的部门就不同，因此所应关注的网络操作也不同，授予的权限也就不同。

6.网络前期建设方案、网络拓扑结构图应和实际的网络结构一致;所有网络设备（包括交换机、路由器、防火墙、IDS 以及其他网络设备）应由组织统一规划部署，并应符合实际需求。

7.应充分考虑 Internet 接入的问题，防止出现多 Internet 接入点，同时限制接入用户的访问数量。

8.备份也是需要考虑的重要因素，对广域网设备、局域网设备、广域网链路、局域网链路采用物理上的备份和采取冗余协议，防止出现单点故障。

网络边界分析

边界保护不仅存在于组织内部网络与外部网络之间，而且也存在于同一组织内部网络中，特别是不同级别的子网之间边界。有效的边界防护技术措施主要包括网络访问控制、入侵防范、网关防病毒、信息过滤、网络隔离部件、边界完整性检查，以及对于远程用户的标识与鉴别/访问控制。边界划分还应考虑关键业务系统和非关键业务系统之间是否进行了分离，分离后各业务区域之间的逻辑控制是否合理，业务系统之间的交叠不但影响网络的性能还会给网络带来安全上的隐患。应考虑的安全点主要有：

1.Internet、Intranet 和 Extranet 之间及它们内部各 VLAN 或区域之间边界划分是否合理;在网络节点（如路由器、交换机、防火墙等设备）互连互通应根据实际需求进行严格控制;验证设备当前配置的有效策略是否符合组织确定的安全策略。

2.内网中的安全区域划分和访问控制要合理，各 VLAN 之间的访问控制要严格，不严格就会越权访问。

3.可检查网络系统现有的身份鉴别、路由器的访问控制、防火墙的访问控制、NAT 等策略配置的安全性;防止非法数据的流入;对内防止敏感数据（涉密或重要网段数据）的流出。

4.防火墙是否划分 DMZ 区域;是否配置登录配置的安全参数。例如:最大鉴别失败次数、最大审计存储容量等数据。

5.网络隔离部件上的访问通道应该遵循"默认全部关闭,按需求开通的原则";拒绝访问除明确许可以外的任何一种服务，也就是拒绝一切未经特许的服务。

6.实现基于源和目的的 IP 地址、源和目的端口号、传输层协议的出入接口的访问控制。对外服务采用用户名、IP、MAC 等绑定，并限制变换的 MAC 地址数量，用以防止会话劫持、中间人攻击。

7.对于应用层过滤，应设置禁止访问 JavaApplet、ActiveX 等以降低威胁。

8.采用业界先进的安全技术对关键业务系统和非关键业务系统进行逻辑隔离，保证各个业务系统间的安全性和高效性，例如:采用 MPLS-VPN 对各业务系统间逻辑进行划分并进行互访控制。

9.必要时对涉密网络系统进行物理隔离;实现 VPN 传输系统;对重要网络和服务器实施动态口令认证;进行安全域的划分，针对不同的区域的重要程度，有重点、分期进行安全防护，逐步从核心网络向网络边缘延伸。例如，网络可以分成三个区域:信任域、非信任域和隔离区域。信任域和隔离区域进行重点保护，对于非信任域，可根据不同业务系统的重要程度进行重点保护。

10.整体网络系统统一策略、统一升级、统一控制。

网络协议分析

深入分析组织整个网络系统的协议设计是否合理，是否存在协议设计混乱、不规范的情况，是否采用安全协议，协议的区域之间是否采用安全防护措施。协议是网络系统运行的神经，协议规划不合理就会影响整个网络系统的运行效率，甚至带来高度隐患和风险。应考虑的安全点主要有：

1.路由协议、路由相关的协议及交换协议应以安全的、对网络规划和设计方便为原则，应充分考虑局域网络的规划、建设、扩充、性能、故障排除、安全隐患、被攻击可能性，并应启用加密和验证功能。

2.应合理设计网络路由协议和路由策略，保证网络的连通性、可达性，以及网络业务流向分布的均衡性。

3.启用动态路由协议的认证功能，并设置具有一定强度的密钥，相互之间交换路由信息的路由器必须具有相同的密钥。默认的认证密码是明文传输的，建议启用加密认证。

4.对使用动态路由协议的路由设备设置稳定的逻辑地址，如 Loopback 地址，以减少路由振荡的可能性。

5.应禁止路由器上 IP 直接广播、ICMP 重定向、Loopback 数据包和多目地址数据包，保证网络路径的正确性，防止 IP 源地址欺骗。如禁止非公有地址、组播地址、全网络地址和自己内部的网络地址访问内部网络，同时禁止非内部网络中的地址访问外部网络。

6.重要网段应采取 IP 地址与 MAC 地址绑定措施，防止 ARP 欺骗。

7.如果不需要 ARP 代理（ARPProxy）服务则禁止它。

8.应限制 SYN 包流量带宽，控制 ICMP、TCP、UDP 的连接数。、

9.ICMP 协议的安全配置。对于流入的 ICMP 数据包，只允许 EchoReply、DestinationUnreachable、TimeOut 及其他需要的类型。对于流出的 ICMP 数据包，只允许 Echo 及其他必需的类型。

10.SNMP 协议的 CommunityString 字串长度应大于 12 位，并由数字、大小写字母和特殊字符共同组成。

11.禁用 HTTP 服务，不允许通过 HTTP 方式访问路由器。如果不得不启用 HTTP 访问方式，则需要对其进行安全配置。

12.对于交换机，应防止 VLAN 穿越攻击。例如，所有连接用户终端的接口都应从 VLAN1 中排除，将 Trunk 接口划分到一个单独的 VLAN 中；为防止 STP 攻击，对用户侧端口，禁止发送 BPDU；为防止 VTP 攻击，应设置口令认证，口令强度应大于 12 位，并由数字、大小写字母和特殊字符共同组成；尽量将交换机 VTP 设置为透明(Transparent)模式。

13.采用安全性较高的网络管理协议，如 SNMPv3、RMONv2。

网络流量分析

流量分析系统主要从带宽的网络流量分析、网络协议流量分析、基于网段的业务流量分析、网络异常流量分析、应用服务异常流量分析等五个方面对网络系统进行综合流量分析。应考虑的安全点主要有：

1.带宽的网络流量分析。复杂的网络系统中不同的应用需占用不同的带宽，重要的应用是否得到了最佳的带宽？所占比例是多少？队列设置和网络优化是否生效？通过基于带宽的网络流量分析会使其更加明确。采用监控网络链路流量负载的工具软件，通过 SNMP 协议从设备得到设备的流量信息，并将流量负载以包含 PNG 格式的图形的 HTML 文档方式显示给用户，以非常直观的形式显示流量负载。

2.网络协议流量分析。对网络流量进行协议划分，针对不同的协议进行流量监控和分析，如果某一个协议在一个时间段内出现超常流量暴涨，就有可能是攻击流量或有蠕虫病毒出现。例如：CiscoNetFlowV5 可以根据不同的协议对网络流量进行划分，对不同协议流量进行分别汇总。

3.基于网段的业务流量分析。流量分析系统可以针对不同的 VLAN 来进行网络流量监控，大多数组织都是基于不同的业务系统通过 VLAN 来进行逻辑隔离的，所以可以通过流量分析系统针对不同的 VLAN 来对不同的业务系统的业务流量进行监控。例如：CiscoNetFlowV5 可以针对不同的 VLAN 进行流量监控。

4.网络异常流量分析。异常流量分析系统支持异常流量发现和报警，能够通过对一个时间窗内历史数据的自动学习，获取包括总体网络流量水平、流量波动、流量跳变等在内的多种网络流量测度，并自动建立当前流量的置信度区间作为流量异常监测的基础。通过积极主动鉴定和防止针对网络的安全威胁，保证了服务水平协议(SLA)并且改进顾客服务，从而为组织节约成本。

抗击异常流量系统必须完备，网络系统数据流比较大，而且复杂，如果抗异常流量系统不完备，当网络流量异常时或遭大规模 DDOS 攻击时，就很难有应对措施。

5.应用服务异常流量分析。当应用层出现异常流量时，通过 IDS&IPS 的协议分析、协议识别技术可以对应用层进行深层的流量分析，并通过 IPS 的安全防护技术进行反击。

网络 QoS

合理的 QoS 配置会增加网络的可用性，保证数据的完整性和安全性，因此应对网络系统的带宽、时延、时延抖动和分组丢失率等方面进行深入分析，进行 QoS 配置来优化网络系统。应考虑的安全点主要有：

1.采用 RSVP 协议。RSVP 使 IP 网络为应用提供所要求的端到端的 QoS 保证。

2.采用路由汇聚。路由器把 QoS 需求相近的业务流看成一个大类进行汇聚，减少流量交叠，保证 QoS。

3.采用 MPLSVPN 技术。多协议标签交换(MPLS)将灵活的 3 层 IP 选路和高速的 2 层交换技术完美地结合起来，从而弥补了传统 IP 网络的许多缺陷。

4.采用队列技术和流量工程。队列技术主要有队列管理机制、队列调度机制、CAR 和流量工程。

5.QoS 路由。QoS 路由的主要目标是为接入的业务选择满足其服务质量要求的传输路径，同时保证网络资源的有效利用路由选择。

6.应保证正常应用的连通性。保证网络和应用系统的性能不因网络设备上的策略配置而有明显下降，特别是一些重要应用系统。

7.通过对不同服务类型数据流的带宽管理，保证正常服务有充足的带宽，有效抵御各种拒绝服务类型的攻击。

网络的规范性

应考虑的安全点主要有：

1.IP 地址规划是否合理，IP 地址规划是否连续，在不同的业务系统采用不同的网段，便于以后网络 IP 调整。

2.网络设备命名是否规范，是否有统一的命名原则，并且很容易区分各个设备的。

3.应合理设计网络地址，应充分考虑地址的连续性管理以及业务流量分布的均衡性。

4.网络系统建设是否规范，包括机房、线缆、配电等物理安全方面，是否采用标准材料和进行规范设计，设备和线缆是否贴有标签。

5.网络设备名称应具有合理的命名体系和名称标识，便于网管人员迅速准确识别，所有网络端口应进行充分描述和标记。

6.应对所有网络设备进行资产登记，登记记录上应该标明硬件型号、厂家、操作系统版本、已安装的补丁程序号、安装和升级的时间等内容。

7.所有网络设备旁都必须以清晰可见的形式张贴类似声明:"严格禁止未经授权使用此网络设备。

8.应制定网络设备用户账号的管理制度，对各个网络设备上拥有用户账号的人员、权限以及账号的认证和管理方式做出明确规定。对于重要网络设备应使用 Radius 或者 TACACS+的方式实现对用户的集中管理。

网络设备安全

对设备本身安全进行配置，并建设完备的安全保障体系，包括:使用访问控制、身份验证配置;关闭不必要的端口、服务、协议;用户名口令安全、权限控制、验证;部署安全产品等。应考虑的安全点主要有：

1.安全配置是否合理，路由、交换、防火、IDS 等网络设备及网络安全产品的不必要的服务、端口、协议是否关闭，网络设备的安全漏洞及其脆弱的安全配置方面的优化，如路

由器的安全漏洞、访问控制设置不严密、数据传输未加密、网络边界未完全隔离等。

2.在网络建设完成、测试通过、投入使用前，应删除测试用户和口令，最小化合法用户的权限，最优化系统配置。

3.在接入层交换机中，对于不需要用来进行第三层连接的端口，通过设置使其属于相应的 VLAN，应将所有空闲交换机端口设置为 Disable，防止空闲的交换机端口被非法使用。

4.应尽量保持防火墙规则的清晰与简洁，并遵循"默认拒绝，特殊规则靠前，普通规则靠后，规则不重复"的原则，通过调整规则的次序进行优化。

5.应为不同的用户建立相应的账号，根据对网络设备安装、配置、升级和管理的需要为用户设置相应的级别，并对各个级别用户能够使用的命令进行限制，严格遵循"不同权限的人执行不同等级的命令集"。同时对网络设备中所有用户账号进行登记备案。

6.应制订网络设备用户账号口令的管理策略，对口令的选取、组成、长度、保存、修改周期以及存储做出规定。

7.使用强口令认证，对于不宜定期更新的口令，如 SNMP 字串、VTP 认证密码、动态路由协议认证口令等，其口令强度应大于 12 位，并由数字、大小写字母和特殊字符共同组成。

8.设置网络登录连接超时，例如，超过 60 秒无操作应自动退出。

9.采用带加密保护的远程访问方式，如用 SSH 代替 Telnet。

10.严格禁止非本系统管理人员直接进入网络设备进行操作，若在特殊情况下（如系统维修、升级等）需要外部人员（主要是指厂家技术工程师、非本系统技术工程师、安全管理员等）进入网络设备进行操作时，必须由本系统管理员登录，并对操作全过程进行记录备案。

11.对设备进行安全配置和变更管理，并且对设备配置和变更的每一步更改，都必须进行详细的记录备案。

12.安全存放路由器的配置文件，保护配置文件的备份和不被非法获取。

13.应立即更改相关网络设备默认的配置和策略。

14.应充分考虑网络建设时对原有网络的影响，并制定详细的应急计划，避免因网络建设出现意外情况造成原有网络的瘫痪。

15.关键业务数据在传输时应采用加密手段，以防止被监听或数据泄漏。

16.对网络设备本身的扩展性、性能和功能、网络负载、网络延迟、网络背板等方面应充分考虑。设备功能的有效性与部署、配置及管理密切相关，倘若功能具备却没有正确配置及管理，就不能发挥其应有的作用。

17.网络安全技术体系建设主要包括安全评估、安全防护、入侵检测、应急恢复四部分内容，要对其流程完备性进行深入分析。

18.安全防护体系是否坚固，要分析整个网络系统中是否部署了防火墙及 VPN 系统、抗拒绝服务系统、漏洞扫描系统、IDS&IPS 系统、流量负载均衡系统部署、防病毒网关、网络层验证系统、动态口令认证系统，各个安全系统之间的集成是否合理。

19.应安全存放防火墙的配置文件，专人保管，保护配置文件不被非法获取。

20.及时检查入侵检测系统厂商的规则库升级信息，离线下载或使用厂商提供的定期升级包对规则库进行升级。具体包括：

●查看硬件和软件系统的运行情况是否正常、稳定；

●查看 OS 版本和补丁是否最新；

●OS 是否存在已知的系统漏洞或者其他安全缺陷。

网络管理

网络管理和监控系统是整个网络安全防护手段中的重要部分，网络管理应该遵循

SDLC(生命周期)的原则，从网络架构前期规划、网络架构开发建设到网络架构运行维护、网络架构系统废弃都应全面考虑安全问题，这样才能够全面分析网络系统存在的风险。应考虑的安全点主要有：

1.网络设备网管软件的部署和网络安全网管软件的部署；部署监控软件对内部网络的状态、网络行为和通信内容进行实时有效的监控，既包括对网络内部的计算机违规操作、恶意攻击行为、恶意代码传播等现象进行有效地发现和阻断，又包括对网络进行的安全漏洞评估。

2.确认网络安全技术人员是否定期通过强加密通道进行远程登录监控网络状况。

3.应尽可能加强网络设备的安全管理方式，例如应使用 SSH 代替 Telnet，使用 HTTPS 代替 HTTP，并且限定远程登录的超时时间、远程管理的用户数量、远程管理的终端 IP 地址，同时进行严格的身份认证和访问权限的授予，并在配置完后，立刻关闭此类远程连接；应尽可能避免使用 SNMP 协议进行管理。如果的确需要，应使用 V3 版本替代 V1、V2 版本，并启用 MD5 等验证功能。进行远程管理时，应设置控制口和远程登录口的超时时间，让控制口和远程登录口在空闲一定时间后自动断开。

4.及时监视、收集网络以及安全设备生产厂商公布的软件以及补丁更新，要求下载补丁程序的站点必须是相应的官方站点，并对更新软件或补丁进行评测，在获得信息安全工作组的批准下，对生产环境实施软件更新或者补丁安装。

5.应立即提醒信息安全工作组任何可能影响网络正常运行的漏洞，并及时评测对漏洞采取的对策，在获得信息安全工作组的批准的情况下，对生产环境实施评测过的对策，并将整个过程记录备案。

6.应充分考虑设备认证、用户认证等认证机制，以便在网络建设时采取相应的安全措施。

7.应定期提交安全事件和相关问题的管理报告，以备管理层检查，以及方便安全策略、预警信息的顺利下发。检测和告警信息的及时上报，保证响应流程的快速、准确而有效。

8.系统开发建设人员在网络建设时应严格按照网络规划中的设计进行实施，需要变更部分，应在专业人士的配合下，经过严格的变更设计方案论证方可进行。

9.网络建设的过程中，应严格按照实施计划进行，并对每一步实施，都进行详细记录，最终形成实施报告。

10.网络建设完成投入使用前，应对所有组件包括设备、服务或应用进行连通性测试、性能测试、安全性测试，并做详细记录，最终形成测试报告。测试机构应由专业的信息安全测试机构或第三方安全咨询机构进行。

11.应对日常运维、监控、配置管理和变更管理在职责上进行分离，由不同的人员负责。

12.应制订网络设备日志的管理制定，对于日志功能的启用、日志记录的内容、日志的管理形式、日志的审查分析做明确的规定。对于重要网络设备，应建立集中的日志管理服务器，实现对重要网络设备日志的统一管理，以利于对网络设备日志的审查分析。

13.应保证各设备的系统日志处于运行状态，每两周对日志做一次全面的分析，对登录的用户、登录时间、所做的配置和操作做检查，在发现有异常的现象时应及时向信息安全工作组报告。

14.对防火墙管理必须经过安全认证，所有的认证过程都应记录。认证机制应综合使用多种认证方式，如密码认证、令牌认证、会话认证、特定 IP 地址认证等。

15.应设置可以管理防火墙的 IP 范围，对登录防火墙管理界面的权限进行严格限制。

16.在防火墙和入侵检测系统联动的情况下，最好是手工方式启用联动策略，以避免因入侵检测系统误报造成正常访问被阻断。

17.部署安全日志审计系统。安全日志审计是指对网络系统中的网络设备、网络流量、

运行状况等进行全面的监测、分析、评估，通过这些记录来检查、发现系统或用户行为中的入侵或异常。目前的审计系统可以实现安全审计数据的输入、查询、统计等功能。

18.安全审计内容包括操作系统的审计、应用系统的审计、设备审计、网络应用的审计等。操作系统的审计、应用系统的审计以及网络应用的审计等内容本文不再赘述。在此仅介绍网络设备中路由器的审计内容：操作系统软件版本、路由器负载、登录密码有无遗漏，enable 密码、telnet 地址限制、HTTP 安全限制、SNMP 有无安全隐患;是否关闭无用服务;必要的端口设置、Cisco 发现协议（CDP 协议）;是否已修改了缺省旗标（BANNER)、日志是否开启、是否符合设置 RPF 的条件、设置防 SYN 攻击、使用 CAR（ControlAccessRate）限制 ICMP 包流量;设置 SYN 数据包流量控制（非核心节点)。

19.通过检查性审计和攻击性审计两种方式分别对网络系统进行全面审计。

20.应对网络设备物理端口、CPU、内存等硬件方面的性能和功能进行监控和管理。

●系统维护中心批准后，根据实际应用情况提出接入需求和方案，向信息安全工作组提交接入申请;

●由申请人进行非上线实施测试，并配置其安全策略;

●信息安全员对安全配置进行确认，检查安全配置是否安全，若安全则进入下一步，否则重新进行配置。

21.网络设备废弃的安全考虑应有一套完整的流程，防止废弃影响到网络运行的稳定。任何网络设备的废弃都应进行记录备案，记录内容应包括废弃人、废弃时间、废弃原因等。

电子政务项目中的计划管理

成功的项目是周密计划的结果，而不单纯是良好的实施过程的结果。

信息系统工程项目具有一些鲜明的特点:技术含量高、技术更新快、交付物的性质变化快、涉及面广、人员影响特别大等，因而项目的管理非常复杂，为此，必须在信息系统工程建设中科学地运用项目管理的思想和工具，实行科学规范的管理，以保证信息系统项目保证质量，缩短开发和建设周期，达到信息系统工程预期的目的。

项目的总体规划

云南省电子政务二期工程是一项覆盖省委、省人大等 10 个重点部门,全省 16 个州(市)级横向网络、部分县级横向网的重点应用系统建设。由于本工程各项目设备供货商及软件开发商多，专业项目多，技术复杂，各种应用系统互相关联接口关系复杂，组织协调工作量大，为了科学地组织、协调、管理该项目，保证项目成功达到预期的各项目标，依靠并运用科学的项目管理的理论和工具成为必然的选择。而项目管理的核心思想就是以科学、周密、详尽的项目计划提前规划项目实施中的时间、人员、资源。

1.确定总体计划和项目管理框架

针对项目实际任务，并结合电子政务一期的经验，云南电子政务二期项目组制定了周密的工程总体计划，并颁布了《云南省电子政务二期工程项目管理规范》，通过《项目管理规范》建立了二期工程建设的总体管理框架。在《规范》中，事先对承建单位的工程实施进行了约束和规范，明确了所有分项工程建设，无论是总体工作还是各阶段工作，必须严格按照“计划→执行→控制→收尾”的过程进行。在这个总体框架下，对工程编制了计划和 WBS（WorkBreakdownStructure）结构分解，制订了项目总体 WBS 字典，并按照 PMP 项目管理体系的约定，对各过程的输入、输出做了约定。

通过项目管理规范的执行，使得众多承建单位、分项工作的实施和管理在一个共同的项目管理体系中进行。业主、监理、承建单位用同一种科学的方法去实施和工作，众多承建单位之间用统一的思路和工具去协调，在大的框架上减少了可能的分歧和偏差。

2.分项计划的制订

针对信息系统工程建设中存在的计划要素不全、计划粗略、单纯用时间计划代替整体计划的普遍现象，在该电子政务项目管理规范中，对工作计划进行了明确要求。

以实施方案为例，项目要求必须有组织形式、质量管理、进度管理、变更管理、资源管理、风险管理、沟通交流机制等要素。通过这样的方式，不但规范了工程实施的行为，而且迫使各承建单位人员特别是项目经理更多地考虑计划、组织、协调问题，从而在项目计划阶段就提前发现和解决了一批问题，提高了项目实施的起点，为项目后期的实施奠定了基础。

在工程建设中引入项目管理的思想和方法，把工程建设的重点由工程实施向工程计划倾斜，进而以计划指导实施，这正是项目管理的核心思想，也正是目前信息系统工程建设中欠缺的。在电子政务二期工程建设的实践中表明了这一思想和方法的正确，整个工程涉及单位众多，约有 26 个承建单位，涉及网络、软件、安全、办公系统、网站、视频会议等众多分项，建设范围覆盖全省，涉及 600 多个单位，时间又相当紧，工程的技术难度和组织管理难度很大。但在整个建设过程中，工程始终处于有序、可控状态，各方配合良好，有节奏、有控制地逐步按照计划推进。目前已经按期完成主要工作，顺利进入项目收尾阶段。

项目计划的优化

在对各承建单位的项目计划做出要求后，下一步就是进行项目总体计划的集成和综合。各承建单位制订了各自的分项计划，但都是单项工作计划。比如，信息发布系统根据规范要求，制订了自己的实施计划。但这只是自身工作的计划，没有考虑和电信、网络工程、主机系统、网络安全系统的协调。从信息发布系统承建单位的立场和所掌握的工程信息而言是无可厚非的，但是作为项目的指挥和控制角色，必须通盘考虑整体项目建设计划安排。网络不建成、主机不搭建，信息发布系统是无法建设的。因此，必须在不同承建单位的工作计划中，建立工作步骤、工作顺序的搭接关系。比如信息发布系统的建设遵循这样的顺序：电信线路准备完毕、网络建设完毕、主机到位、网络安全开放端口、信息发布系统建设开始。

以工期计划为例。初期制定了 3 个月的工期，各承建单位都承诺可以完成，也都提交了各自的计划。但根据总体要求，编制出“电信、网络、主机、信息发布”的工作顺序后，后面两个分项目都觉得无法在 3 个月内完成。因为项目参与者原来只是排定了自己的单项工作计划，一旦自己的工作需要等到其他分项工作完成后才能开始，就觉得无法实现和控制。

项目组整理了各项工作关系后，运用项目管理中的 PERT/CPM 技术，计算出项目关键路径，优化了工作关系，科学安排并发工作之间的关系。如网络设备到货时间长，在这期间可以安排服务器和软件的安装，这样，优化调整了分项工作的顺序和工作搭接关系，使得项目整体任务可以按期完成。各分项实施单位在听取了介绍、优化、整体安排后，也树立了信心，积极调整计划，主动协调和其他单位的工作，相互配合，在工程中起到了很好的效果。

计划与质量控制

质量是项目关注的核心要素，但大多数是事中或事后的质量控制，如果对计划进行预审比项目完成后的审查，代价会小很多。在项目管理过程中，项目组始终坚持“质量是计划和执行的结果，而不是检查的结果；纠正错误的代价远高于预防错误的代价”，并坚持采用质量控制理论中的 PDCA 循环控制方法，即 Plan、Do、Check、Action 四个环节的循环，对项目进行把关。

1.计划先行，提前发现问题

在项目计划阶段应尽可能细化工作步骤和技术参数，特别是不同系统之间的接口参数。因为在招投标阶段，通过对招投标方案的评审和对承建单位的资格审查发现，各分项工程自身的技术方案基本是完备和可行的，而信息系统工程建设最难的技术层面在不同系统、不同项目的接口和配合上。因此，项目在技术方案评审阶段更多的是组织了技术方案的交叉会审和交叉摸底，使各分系统尽早发现技术接口问题和工作衔接配合问题。

2.模拟运行，提前解决问题

在实施前，搭建测试和模拟环境，启动试点工程，将方案和计划在类似演习和预演的环境中进行系统集成和工作协调，提前发现问题，是很有必要的。在模拟测试环境中，项目组先后解决了网络和网络安全系统、全文检索和信息发布系统、主机和操作系统等分项目之间隐含的技术问题。在全省工程实施之前，启动了玉溪地区试点工程，将工程所有实施内容预演一次。结果在试点中发现了一些问题，及时总结后重新调整工作计划和实施方案，优化了工作流程，避免了技术问题的扩散。同时根据试点情况，优化了工作流程，仅此一项，就节省了将近 10 天工期。

3.在过程中检验计划的可行性

计划是否成功最终要落实到项目实际操作工程中。在项目实施过程中，一方面加强测试和监控，提前启动调试和测试流程，通过测试和联调，发现问题，及时解决，避免质量问题的"群聚效应"发生。而另一方面是及时总结，以利于未来的项目建设和管理。

总体而言，在云南省电子政务二期工程的项目实践中，由于工程实施中全力推行并运用项目管理的思想和工具，同时由于各承建单位的项目经理大都经过了信息产业部的项目经理培训，对项目管理的知识有一定了解，具有丰富的实践经验，因此整个项目的质量、进度、费用都在控制范围内，项目利益的相关方都比较满意。

链接:云南电子政务项目计划的优化过程

云南省电子政务二期工程项目实施计划实际经历了一个总、分、合、协、优的过程。

总:即事先制订总体计划，约定项目实施的总体计划和规范。

分:各承建单位在大计划和规范要求下，根据各自工程特点，制订分项工作计划。

合:在分项工作计划的基础上，建立不同子项目和工作阶段之间的工作逻辑和工作搭接关系，确定工作顺序和工作衔接，发现工作接口和技术接口，制订工作初步集成总体计划。

协:在初步集成总体计划的基础上，再次要求各分项承建单位调整、细化各自的工作计划，了解自己需要和其他分项工作如何衔接、如何配合、提前做好配合准备和事先协调，并在自己的工作计划中体现和其他单位工作的配合和衔接。

优:在各单位考虑到和其他单位配合并调整计划后，再次根据协调中出现的问题，集成所有分项目的工作计划，运用项目管理技术和方法，优化工作流程和工作结构，制订总体工作计划，并作为工程总体实施计划颁布执行。

应用 CMM 改进软件维护过程

应用 CMM 对软件维护过程进行改进，不但能帮助我们迅速解决工作中遇到的问题，同时还可以促进维护人员之间的交流。

CMM 是现在用来衡量软件公司软件开发管理水平的重要参考因素和软件过程改进的认证标准之一。软件过程成熟度的提高是一个渐进的过程，需要一个长远的、可持续发展的过程作为保证。CMM 代表着目前软件发展的一种思路，一种提高软件过程能力的途径。本文介绍我中心如何通过应用 CMM 持续不断地改进软件维护过程，如何通过建立一个软件维护项目数据库，解决一些以前难以处理的问题，不断完善软件维护的科学管理方法。

改进之前的维护状况

南平医保中心现有的医保信息管理系统由本中心信息科来进行维护。我们刚开始接管这套系统的时候，在如何对系统进行管理和维护上存在诸多的困难:

1.该软件的开发，我们科室的成员没有跟进参与;

2.该软件在移交时文档不齐全，甚至连源程序也不齐全，原软件公司的这些资料都掌握在各个开发程序员的手上，没有一个统一的管理，这对我们后期了解这套软件也加大了困

难；

3.原软件公司没有对我们进行一个规范化的规范，就连一个整体的技术介绍也没有给我们，所以我们对该软件缺乏一个系统的认识。

通常测定软件维护工作量都用下面的这个模型表示:M=P+Kc-d（其中:M是维护所需的总工作量;P是生产类活动的工作量;K是经验常数;c是软件的复杂程度;d是维护人员对软件的熟悉程度）。对于一个具体的维护来说，确认需求和设计工作量与问题的难易和大小有关，这一过程相对来说比较稳定，编码工作则与软件本身的质量有很大的关系，如果原来的编码格式混乱，注释不清，就会使生产类活动的工作量（P）增大，在软件的复杂度（c）相同的前提下，维护人员对软件的熟悉程度（d）越低，则维护工作量呈指数规律增加;同样，如果由于开发混乱，导致软件复杂度（c）增加，从而使维护人员理解软件的难度增加，对软件的熟悉程度（d）也降低，那么维护工作量就会以更快的速度上升。

这套系统已经运行了三年多，在这段时间里，我们主要的维护工作有两大类：

1.改正性维护。尽管该软件在当初开发过程中经过严格的测试，但并不能保证该软件就彻底没有错误，随着运行时间的延续，数据量的积累，各种应用环境的变化，一些潜伏的错误不断暴露出来。比如:已出院人员还能冲销费用;通过接口能随意更改已出院人员的出院日期等。

2.完善型维护。随着前台业务操作人员在使用过程中对软件的不断熟悉，会提出一些功能或者操作上的改进需求,而业务管理人员在对业务流程的完善过程中也会提出增加系统功能的需求，为了满足这些需求，就必须对软件进行不断的改进和完善，这样的维护几乎占到维护工作量的一半以上，比如滞纳金功能的启用，电子病历的传送等。

在2002年7月我们接管之初，由于经验不足，对该软件的认识了解不够，以及当初的维护工作的不规范等原因导致在最初的维护过程中忽略了很多的问题。随着时间的推移，那些遗留问题对该系统维护的影响也越来越明显，有的甚至制约了后期的可修改，这样就给后期维护造成了很大的困难。就此我们总结了以往的经验教训，找出了以前管理维护过程中存在的一些主要的问题。

1.随意性大

每次需求立项刚开始就成了"实验田"，做与不做，什么时候做等多凭个人的主观意愿，没有参考以往经验，也没有充分考虑有效的利用资源，"打补丁"现象较多，业务使用不方便，导致后期维护困难。

2.个人智慧多

以前因为时间紧，很多需求都是交给具有相当才干的骨干人员处理，但由于他们的经验没有被很好地总结、归纳，且处理过的事件没有统一形成文档，一段时间后，就忘记了曾处理的事件和如何处理的过程。当再次遇到类似问题的时候，还要凭记忆去处理，如果该人员走了，类似的问题再发生的时候，处理人员还要从头摸索，这样不但浪费了大量的人力和物力，同时由于解决问题不及时，也给我中心造成了一些不良的影响，致使整体的维护质量下降，这说明原维护工作多依赖个人智慧而不是整个团队。

3.版本不规范

在早期的软件维护过程中，由于我们对软件的版本控制不严格，完全由开发人员手工进行操作，在这种情况下，版本控制经常出现问题，有时同一模块被不同的人员同时修改，有时将本应该发给甲用户的程序发给了乙用户，又或者开发人员自以为手上的代码是最新的，而出现已改过的BUG又重复出现的现象。这样做的另一个问题是版本的历史很难追踪，由什么人在什么时候做了什么样的修改完全没法掌握。

将CMM引入维护工作

为了避免在以后的维护工作中继续出现上述问题，我们考虑引入CMM，试图把个人的脑

力劳动结果规范为有纪律有智力的产品。

首先，我们先自行培训了 CMM 的基础理论，重点围绕软件维护这部分进行深入的学习和讨论，力争把每一次的维护需求都当成一个项目来进行处理。

其次我们建立一个软件维护项目数据库，内容包括:申请人、申请时间、申请单位、申请科室、需求或问题、领导意见、分析评审结果（如是否可行，为什么，由谁负责等）、处理过程（如涉及到的模块，对哪些项目进行修改，修改的前后差异，处理结束时间，此改动是否影响业务前台操作流程，如果有都有哪些变动等）在改动中的心得，是否涉及版本控制，验收人，验收意见，是否有新的变更要求等。

在需求管理方面，我们努力地贯彻 CMM 需求管理的精神。每一次的需求提出，我们都让业务人员详细填写需求单（如表所示）。

表单编号: ----------

申请人		日期	年 月 日	单位	
科室	□主任 □信息科 □医务科 □基金科 □财务科 □综合科				
需求或问题	（对具体需求和运行问题的描述）				
领导意见					

表需求表单

需求管理一直是用户和开发人员争论的焦点，从 CMM 的角度来说，用户的需求中既有技术层面的，也有非技术层面的，即便是技术层面的需求，也并非面面俱到都要开发。例如，一些技术上不可行或资源要求不能满足的需求就必须剔除，只有适合软件开发的需求才会被最终制作成规格说明，但是这些就一定要和用户之间做好沟通，让他们理解为什么行与不行。

在通常的维护过程中，有一系列的变更请求或问题报告要求需要满足，这些变更请求和问题报告既有可能单个提出的，也有可能是为了分析实现之便综合成相互联系的一组提出的。对于各种不同情况，我们都按 CMM 的要求，把它们规范化、文档化，控制好过程中的每个环节，保证它们被所有的受影响组通过，保证软件维护计划和活动与它们一致，并且对它们来说这个过程是可追踪的。为了满足达到预期的效果，在执行中，我综合了 CMM 需求管理的要求制定了如下步骤（具体的项目操作应根据实际项目的需要进行）：

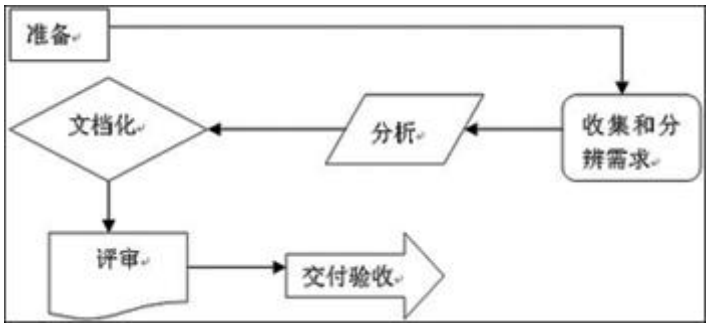
1.需求分析。首先，确认此需求适用的范围，达到的目标;其次，明确申请方参与需求调研活动的职责（如有无决策权、所需配合的活动、所需提供的资源等）;第三，分辨技术与非技术需求;第四，收集相关技术需求;第五，分析申请方业务工作流程;第六，制作需求说明文档，在每个模块分析时均注上标号，便于其后需求变更的跟踪及修改;第七，对本次需求活动拟一个时间进度表。

2.需求评审。根据需求单上所涉及的部门，确定需求评审小组成员要求，明确评审方式，确定评审内容。如对于给定的需求文档记录是否完整及有无遗漏项，文字说明是否前后一致、清晰适当，变更依据是否充分，是否有正常的记录，以及功能的可测试性等。

3.交付验收。在交付给申请人验收时，需附上:功能分析文档、需求规格说明书、需求验收文档。申请人对确定的需求无疑义，在验收文档上签字，若申请人提出相应的变更，则为变更做好记录，修改后的变更依然应通过评审才能交付，申请方所签收的需求作为系统的需求基线确立下来。

4.需求调研。严格依照拟定的需求管理计划进行项目的实际需求调研活动，在活动中记录与各部门进行交流的内容，记录各阶段产生的变更项、变更原因，按预先规定的书面策略进行双方活动的制约。

整体活动图如图所示。



图需求管理的整体过程

在需求的实施方面，我们也加强了过程的跟踪和监控。在 CMM 实行初期，由于工作流程的改变，在每次项目启动的初期，开发人员要花很大的一部分时间写文档资料，工作压力比以前大了很多，导致一段时间内效率降低，当大家逐渐习惯后，感觉文档是开发人员劳动成果最好的记录，工作比以前清晰，规范的文档减少了对个人的依赖，使软件开发过程的上下环节紧密衔接。而且我们还能根据所有文档内容对每个过程进行检查，不仅提高了工作效率，也规范了管理。

在进度控制方面，我们首先制定了全面的开发计划和进度计划，要求开发人员填写详细的工作计划和实际工作量周报，并根据此绘制项目进度图，随时了解项目进展，并根据项目的进展情况适当调配人手，整个项目比计划略早完成，具体实施的详细步骤要视实际中项目大小而定。

在质量保证方面，我们组织几个骨干人员成立了专门的 SQA 小组，根据 CMM 管理规范来检查软件开发过程标准，规程的合理性，文档的电子化，对项目的监督"对事不对人"并定期公布监督结果。

在版本控制方面，通过项目数据库，要求开发人员在每次开发所修改的最终版本上备注版本号和存放路径，以便下一个变更的时候能够拿到最新的一个版本的修改。

由于引进了 CMM，加强软件维护过程管理，直接解决了原来开发团队所遇到的一些难以处理的问题。项目数据库的建立使维护人员只需要读懂设计文档，和读懂程序比起来，既节约了大量的时间，也要容易得多。在这样的基础上做出修改后出现的问题也越来越少，使软件更加可靠，且能完全满足软件开发人员的需求。

论改进 Web 服务器性能的有关技术——论文 1：银行业的应用

【摘要】

基于 Web 技术的数据库应用是当前应用的一个热点，在用户数目与通信负荷很大的场合，提高 Web 服务器性能是一个迫切的课题。本文从笔者参与某个银行系统项目开发的经历出发，阐述了提高 Web 服务器的性能应渗入到项目论证、选型、开发、运行和管理的各个环节，只有各个环节都能充分考虑到性能与质量的需要，系统的性能才是真正可保证的和可扩充的。

文章从系统的实际运行与相应的经验出发，阐述了性能改进方面的一些具体措施。

比如：在本文中讨论了 Web 服务器平台的选型考虑；Web 服务器的配置管理；应用系统本身的优化与预先设计系统时可扩性的性能保障等具体内容。

通过技术上的分析与改进，综合性地运用多类措施与手段，在实际系统中，Web 服务器运行的性能得到了一定程度的保证。

【正文】

我所在的单位是把目标定位于金融领域开发 IT 应用的一家信息技术公司。随着金融电子化建设的发展和商业银行之间市场竞争的加剧，各主要商业银行不断通过信息技术提供新的金融产品，并且希望能整合市场渠道。比如主要的商业银行不断推出形形色色的网上银行服务。在这种背景下，本人参与了开发新一代网上银行产品，涉及到提供网上个人理财服务、网上外汇买卖服务、网上企业服务等具有市场竞争力的产品。作为项目开发的组织者之一和主要的技术骨干，在整个项目开发过程中始终要处于第一线，从而在改进 Web 服务器性能、提高整个网上平台系统性能方面收获良多，在本文中简要讨论如下，希望与读者们共享经验。在 Web 服务器配置与优化方面，我有如下几方面主要的体会：

第一方面是 Web 服务器选型考虑。

在 Web 服务器选型及网上平台搭建之初，我们就已充分考虑整个网上平台的性能及可扩展性问题。这一考虑为该系统的稳定性及扩展性能力方面打下了坚实的基础。

某银行原有的一些网上产品由于开发较早，故而采用的是老式的 HTTPServer+CGI 程序调用的方式。这时，每一客户请求需要对应于后端系统的系统进程来运行 CGI 程序来处理，系统的开销相当大，系统的扩展能力也很差，性能已不能满足业务处理的需要，故而在为此银行系统具体选型的时候，我们一开始就否决了这种方案。

通过市场上同类产品的比较选择，我们选择了国际商业机器有限公司 IBM 的 WebSphere产品系列作为该行网上银行系统的建立平台。作出这样选择是因为WebSphere 基于使 HTTPServer 和应用服务器相分离的整体架构，同时支持 JSP、Servlet 和企业组 JavaBean 等轻量级线程规范，所有的请求对应于应用服务器上的处理线程，系统的开销低、效率非常高，同时 WebSphere 整个体系结构相当的灵活，为适应扩展需要可以作不同的横向和纵向扩展，从而可以满足各银行未来的扩展需要。

正是因为在一开始选型的时候我们就已考虑到未来的扩展需要，整个系统在接下来的几次性能改进方面，我们大体上都能相对顺利地达到了预期目标。

第二方面是 Web 服务器的性能配置。

在一开始系统上线的时候，由于系统的负荷不是很大，为了节省系统总拥有成本 TCO 投资，我们在一台较低配置的 IBMRS6000 上投产了该系统。整个系统的 HTTP 服务器、应用服务器、通信服务器等均位于该台机器上，由于初始投产时用户不多，所以系统的性能基本上能令人接受。

但随着业务的发展和用户访问量的增大，我们发现该服务器的响应变慢，系统的 CPU 利用率和内外存交换显著增大。经过跟踪，我们发现关键原因之一是系统的内存不足的缘故。由于网上服务器把大量用户的会话信息保存在内存中供给应用系统使用，当内存不足时，大量 Session 信息被迫交换至硬盘，大量 CPU 时间消耗在等候内外存的交换上，系统效率迅速下降。

鉴于这种情况，我们把该服务器的内存由 2GB 扩充为 4GB，同时相应调整用户会话信息的保存时间，这样整个系统的效率又回到较为理想的状况。

由于新应用的不断投产及数据库操作的日益增加，我们后来逐渐监控到系统的数据库处于繁忙状态，系统的错误日志也记录下了供应用服务器使用的数据库连接处出现资源不足的情况。在这种背景下，我们认为整个系统由于硬件配置所限，应该进行横向扩展，因此我们把数据库服务器分离出来，配置到另一较高性能的服务器上，相应定义的数据库资源也大幅增加，这样整个系统的性能又处于较为理想的状况。

第三方面是对应用系统进行相应的优化以提高性能。

Web 服务器配置及相应的硬件扩展不失为解决系统性能问题的一条捷径，但应用系统的优化也是应该重点加以考虑的，毕竟它能够在投入较少的情况下提高系统的运用效率。

在开发的初期，我们就已经十分注意系统的利用效率，比如提醒程序员尽量不要利用用户会话信息（Session）来传递大的对象，对于内存要注意回收等。同时，通过内部的交流会推广与介绍一些小的、有用的编程技巧来提高开发人员的水平，通过代码的抽查，希望能在早期就发现问题等。

在系统运行期间，我们通过监控发现，应用服务器所基于的 Java 虚拟机，其内存堆的空闲空间有不断下降的趋势，每隔若干天导致空间消耗殆尽、无法分配新对象空间，从而导致系统重启。在排除了系统本身问题的原因外，我们确定为应用系统的开发有问题。通过从网上万载 IBM 公司检测 Java 虚拟机的相关工具对 JVM 进行监控后终于发现系统内部存在着不能回收内存的对象，再通过查找相应的程序发现在该程序中有“环状”的对象引用，从而导致对象使用后不能被垃圾收集器所回收。这个问题的解决过程虽然十分艰苦，但由于该问题不能通过升级硬件或增加资源配置而得到根本解决，会给系统带来很大的隐患。所以，整个过程的分析与解决是完全值得的，更何况通过查找故障原因的过程，给整个项目组上了生动的一堂软件质量保证课，对项目组的质量意识起了很大的促进作用。

所以说改进 Web 服务器的性能并不单纯是系统管理方面的工作，它渗透到开发以及

系统运行等一系列环节中。

第四方面预先考虑未来的扩展与性能需要。

随着系统的发展及成熟，考虑到用户访问量的不断上升，为了预留系统的发展空间，我们最近又对整个系统作了一个系统性的升级。通过引入多台 HTTP 服务器及应用服务器并行工作提高整个系统吞吐量及单点故障克服能力。由于在一开始选型的时候就已经充分考虑到动态负载均衡及横向扩展方面的需要，这一项的升级无需对整个系统的体系结构作根本的变革，对应用程序来说，更是没有造成任何影响。

整个项目历时近两年，从这两年的系统情况来看，整个系统是成功的。根据我亲身的经历，系统性能并不单纯是系统运行与管理阶段的问题，而是渗透在项目论证、开发以及运行的各个阶段。只有在各个阶段都能充分考虑性能方面的需要，在实际运行时，整个系统的性能才可能真正有保障。在技术方面来看，可以综合利用选型评估、硬件扩展、应用优化和系统配置优化等一系列的手段；比如在硬件扩展方面，又可以分为主要部件扩容，纵向升级、横向升级等方面。在我们的项目实践中，曾综合地利用了上述的各种手段。比如某银行的整个系统从日访问量不足 1 万至现在的每日超过 I0 万次以上的点击的发展情况来看，整个系统的性能保障及提高方案是比较成功的。

评注：实践过程较有说服力。条理与思路相当清晰，技术措施与管理措施的推进也很明确。所论述的技术还有一些局限，不够开阔。（本文主要参考了广州黄昌湛等人的论文）

界面设计指导原则

八条黄金规则：一是尽量保持一致性；二是为熟练用户提供快捷键；三是提供反馈信息；四是设计完整的对话过程；五是提供简单的错误处理机制；六是允许撤销动作；七是提供控制的内部轨迹；八是减轻短轻记忆负担。

论开放系统应用的互操作性

分布式系统的主要特点包括资源共享、开放性、并发性、可伸缩性、容错性以及透明性。实现分布式系统的体系结构主要包括两种，一种是客户/服务器体系结构，另一种是分布式

对象体系结构，不区分服务器和客户机，将系统当成交互的一组对象，它们的位置是无关紧要的，服务提供者和消费者之间没有界限。

基于 RUP 的软件过程及应用

1 引言

软件过程（Software Process）是人们建立、维护和进化软件产品整个过程中所有技术活动和管理活动的集合 [1]。目前，软件过程技术是一个非常活跃的研究领域，吸引了大批来自学术界和工业界的专家和学者。从 1984 年起每年有软件过程国际研讨会（ISPW），从 1991 年起开始召开软件过程国际会议（ICSP），每个国家几乎都有自己的软件过程改进网络（SPN）。软件过程技术的研究主要有三个 方向：

（1）软件过程分析和建模。软件过程建模方法是软件过程技术的起点，其中形式化半形式化建模方法有基于规则的，基于过程程序的等等。过程分析和过程建模对于保证过程定义的质量、建立全面和灵活的过程体系具有重要的作用。

（2）软件过程支持。软件过程支持主要是指研究和开发支持软件过程活动的 CASE 工具，过程支撑工具作为一种技术基础设施能够很好地支持、管理并规范化软件过程。软件过程支持工具主要包括软件过程流程工具、过程文挡工具、评审工具和人员管理工具。

（3）软件过程评估和改进。软件过程改进对生产高质量软件产品和提高软件生产率的重要性已被越来越多的软件开发组织所认同。由美国卡耐基 ·梅隆大学软 件工程研究所（CMU/SEI）提出的软件能力成熟度模型（SW-CMM）除了用于软件过程评估外，还向软件组织提供了指导其进行软件过程管理和软件过程 改进的框架。

Rational Unified Process(RUP)是 Rational 软件公司的一个软件过程产品，是由 Objectory 过程演化而来的，其初始版本为 5。0，先后经历了 5。 1、5。1。1、5。5 等版本直到最新的 Rational Unified Process 2000 版本。RUP 将项目管理、商业建模、分析与设计等统一起来，贯穿整个开发过程。RUP 采用 Internet 技术，可以增强团队的开发效率，并为所 有成员提供最佳的软件实现方案，它使团队中每个开发人员的见解和思想得到统一，使开发小组成员的沟通更为容易，而这正是任何项目要取得成功的关键因素；它 可以增强开发人员对软件的预见性，最终的好处就是提高了软件质量，并有效缩短了软件从开发到投放市场的时间。RUP 过程为软件开发提供了规范性的指南、模 板和范例，可用来开发所有类型的应用。

本文的第 2 节讨论基于 RUP 的软件过程，第 3 节给出一个应用实例，第 4 节是本文的结论。

2 基于 RUP 的软件过程

RUP 中的软件过程在时间上被分解为四个顺序的阶段，分别是初始阶段(Inception)、细化阶段(Elaboration)、构建阶段(Construction)和交付阶段(Transition) [2]。每个阶段结束时都要安排一次技术评审，以确定这个阶段的目标是否已经满足。如果评审结果令人满意，就可以允许项目进入下一个阶段。基于 RUP 的软件过程模型如图 1 所示。

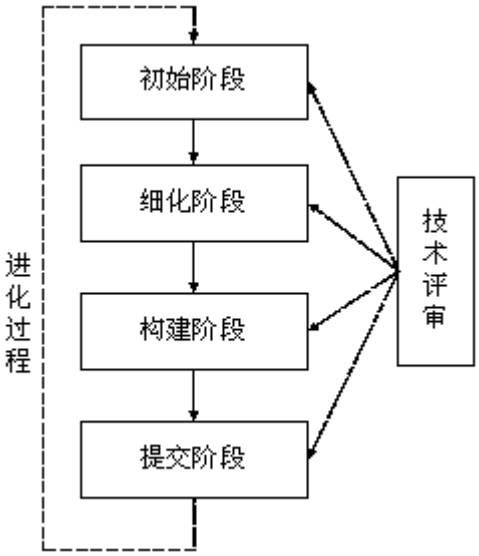


图 1 基于 RUP 的软件过程

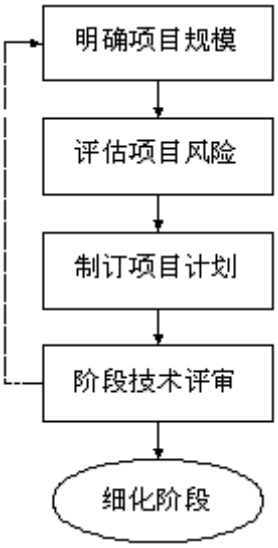


图 2 初始阶段子过程

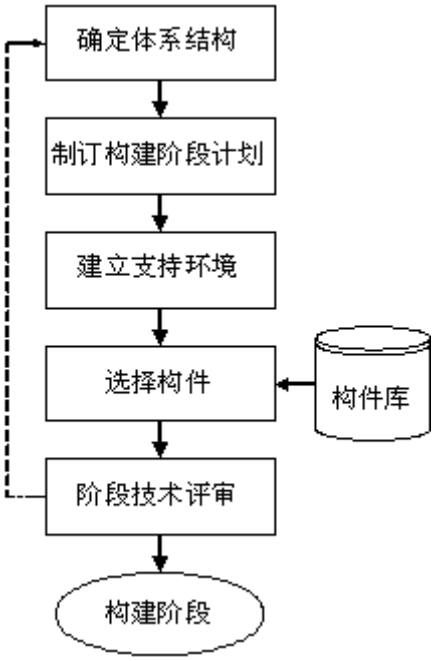


图 3 细化阶段子过程

从 图 1 中可以看出，基于 RUP 的软件过程是一个迭代过程。通过初始、细化、构建和提交四个阶段就是一个开发周期，每次经过这四个阶段就会产生一代软件。除非 产品退役，否则通过重复同样的四个阶段，产品将进化为下一代产品，但每一次的侧重点都将放在不同的阶段上。这些随后的过程称为进化过程。

用户需求的变化、运行环境的变更、基础技术方面的变更等都会引发进化过程。通常情况下，进化过程的初始阶段和细化阶段都比较简单，因为基本产品定义和体系结构在前面的开发过程就已经决定。但也有例外情况，例如对软件体系结构(Software Architecture)进行重新定义的进化过程。

2.1 初始阶段

初始阶段的任务是为系统建立业务模型并确定项目的边界。在初始阶段，必须识别所有与系统交互的外部实体，定义系统与外部实体交互的特性。在这个阶段中 所关注的是整个项目的业务和需求方面的主要风险。对于建立在原有系统基础上的开发项目来说，初始阶段可能很短。初始阶段的实现过程如图 2 所示。

（1）明确项目规模

建立项目的软件规模和边界条件，包括验收标准；了解环境及重要的需求和约束，识别系统的关键用例(Use Case)。

（2）评估项目风险

软件过程主要关心的是软件开发的已知方面，只能准确描述、计划、分配和评审那些已经知道将要完成的事情。风险管理则主要关心未知方面。在基于 RUP 的 迭代式软件过程中，很多决策要受风险决定。要达到这个目的，开发者需要详细了解项目所面临的风险，并对如何降低或处理风险有明确的策略。

（3）制订项目计划

估计整个项目的总体成本、进度和人员配备。综合考虑备选体系结构，评估设计和自制/外购/重用方面的方案，从而估算出成本、进度和资源。在这个过程 中，要通过对一些概念的证实来证明可行性，该证明可采用可模拟需求的模型形式或用于探索高风险区的初始原型。初始阶段的原型设计工作应该限制在确信解决方 案可行就可以了，具体实现留到细化阶段和构建阶段。

（4）阶段技术评审

初始阶段结束时要进行一次技术评审，检查初始阶段的目标是否完成，并决定继续进行项目还是取消项目。在评审过程中，需要考虑项目的规模定义、成本和进 度估算是否适中，估算根据是否可靠？需求是否正确，开发方和用户方对软件需求的理解是否达成一致?是否已经确定所有风险，并且有针对每个风险的规避策略等 问题。

2.2 细化阶段

细化阶段的任务是分析问题领域，建立健全的体系结构基础，淘汰项目中最高风险的元素。在细化阶段，必须在理解整个系统的基础上，对体系结构做出决策， 包括其范围、主要功能和诸如性能等非功能需求，同时为项目建立支持环境。细化阶段的实现过程如图 3 所示。

（1）确定体系结构

确保体系结构、需求和计划足够稳定，充分减少风险，从而能够有预见性地确定开发所需的成本和开发进度。通过处理体系结构方面重要的场景(Scene)，建立一个已确定基线的体系结构。证明已建立基线的体系结构将在适当时间、以合理的成本支持系统需求。

（2）制订构建阶段计划

为构建阶段制订详细的过程计划并为其建立基线。

（3）建立支持环境

建立支持环境，包括开发环境、开发流程、支持构建团队所需的工具和自动化/半自动化支持。

（4）选择构件

评估现有的(构件库)和潜在构件，充分了解自制/外购/重用决策，以便有把握地确定构建阶段的成本和进度。集成所选构件，并按主要场景进行评估。

（5）阶段技术评审

评审时，需要检验详细的系统目标和范围、体系结构的选择以及主要风险的解决方案。在技术评审中，需要考虑的问题有：

（1）产品需求是否稳定，体系结构是否是稳定的？

（2）可执行原型是否表明已经找到了主要的风险元素，并且得到妥善解决？

（3）构建阶段的迭代计划是否足够详细和真实， 是否有可靠的估算支持，可以保证工作继续进行？

（4）所有与项目有关的人员是否一致认为，如果在当前体系结构环境中执行当前计划来开发完整的系统，则当前的需求可以实现？

（5）实际的资源耗费与计划的耗费相比是否有偏差，该偏差是否可以接受？

2.3 构建阶段

在构建阶段，要开发所有剩余的构件和应用程序功能，把这些构件集成为产品，并进行详细测试。从某种意义上说，构建阶段是一个制造过程，其重点放在管理资源及控制操作，以优化成本、进度和质量。

构建阶段的主要任务是通过优化资源和避免不必要的报废和返工，使开发成本降到最低；完成所有所需功能的分析、开发和测试，快速完成可用的版本；确定软件、场地和用户是否已经为部署软件作好准备。

在构件阶段，开发团队的工作可以实现某种程度的并行。即使是较小的项目，也通常包括可以相互独立开发的构件，从而使各团队之间实现并行开发。这种并行性在较大幅度地加速开发进度的同时，也增加了资源管理和工作流程同步的复杂程度。

构建阶段结束时也要进行技术评审，评审产品是否可以在 β 测试环境中进行安装和运行。在评审中，需要考虑的问题有：

（1）该产品发布版是否足够稳定和成熟，可安装和运行在用户的实际环境中？

（2）所有与项目有关的人员是否已准备好将产品发布给用户？

（3）实际的资源耗费与计划的耗费相比是否有偏差，该偏差是否可以接受？

2.4 交付阶段

当基线已经足够完善，可以安装到最终用户实际环境中时，则进入交付阶段。交付阶段的重点是确保软件对最终用户是可用的。

交付阶段的主要任务是进行 β 测试，制作产品发布版本；对最终用户支持文档定稿；按用户的需求确认新系统；培训用户和维护人员；获得用户对当前版本的反馈，基于反馈调整产品，如进行调试、性能或可用性的增强等。

根据产品的种类，交付阶段可能非常简单，也可能非常复杂。例如，发布现有桌面产品的新发布版可能十分简单，而替换一个国家的航空交通管制系统可能就非常复杂。

交付阶段结束时也要进行技术评审，评审目标是否实现，是否应该开始进化过程，用户对交付的产品是否满意等。

2.5 技术评审

在每个阶段结束时都要进行一次技术评审，以确定在完成该阶段的最终迭代后是否应该让项目进入下一阶段。 技术评审要考虑的主要问题应该主要与项目管理有关，因为主要的技术问题应该已经在该阶段的最终迭代以及随后的活动中得到解决。技术评审的步骤如图 4 所示。

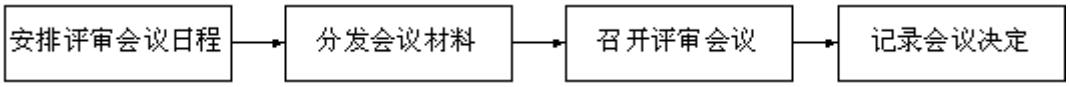


图 4 技术评审的步骤

（1）安排评审会议日程

技术评审会议的参加者必须包括外部人员（用户代表和领域专家）、项目的管理团队（项目经理以及项目团队各功能区域的团队负责人）和项目评审委员会。

与会者一旦确定，就应安排会议的召开日期和时间，以便为与会者留出充足的准备时间，让他们能够评审有关材料。

（2）分发会议材料

在会议召开之前，应当将技术评审材料分发给评审人员。要在会议召开之前及早地将这些材料分发出去，让评审人员有充足的时间对其进行审阅。

（3）召开评审会议

在会议期间， 评审人员主要关注状态评估。在会议结束时，评审人员应作出是否批准的决定。 技术评审会议可能会得到以下结果之一：

（ I）阶段被接受：评审委员会认为项目实现了该阶段的预期目标，可以进入下一阶段。

（ II）有条件接受：评审委员会同意项目可以进入下一阶段，但必须先完成指定的纠正操作。如果发现的问题很少并且不是很重要，则客户可能决定在项目团队执行某些纠正操作的同时有条件地接受该产品。在这种情况下， 项目经理需要根据问题的重要性，或选择开始新的迭代，以处理所出现的问题，或只是通过延长最终迭代来处理问题，二者的差异在于所需的计划工作量。

（III）阶段不被接受：项目没有实现该阶段的预期目标，项目经理就可能必须开始另一次迭代，甚至项目经理无法决定对问题的解决方案，而需要由有关人员根据合同重新确定项目规模或终止项目。

（4）记录会议决定

在会议结束时应完成评审记录，其中包括重要的讨论或活动以及评审的结果。如果结果是"阶段不被接受"，则应暂时安排一次后续复审。

3 应用实例

在为某水电厂开发的综合信息管理系统中，我们全面采用了基于 RUP 的软件过程。水电厂综合管理信息系统是一个大型信息管理系统，其中包含运行管理、设 备管理、安全管理、图形开票、生产技术管理、行政管理、人事管理、技术台帐管理、班组建设、学习培训、系统维护等十多个模块。不仅如此，系统还要与现有的 某些监控设备接口，从中获取数据。系统能对水电厂实行全面的运行管理，能及时对系统的信息作统计分析处理，能给管理者提供及时准确的数据，对水电厂的运行 决策提供必要的依据。

在项目的初始阶段，我们主要建立项目的软件规模和边界条件，明确用户的需求，形成规格说明书，作为验收标准。同时，估计了整个项目的总体成本和进度， 评估了潜在的风险，作出了具有 20%资源预留的项目计划。最后，根据客户要求，我们选择了 Rational Rose 2000 作为分析和建模工具、Project 2000 作为项目管理工具。系统开发工具采用 Visual Studio 6。0，后台数据库管理系统采用 MS SQL Server 7。0。

在项目的细化阶段，我们根据实际需求，选择了 B/S 和 C/S 混合的异构软件体系结构。对一些关键性的算法，制作了探索型的原型。并在此基础上，为构建 阶段制订了详细的迭代计划。在构件的选择方面，我们决定主要采用已有构件（我们曾经开发过变电站综合管理信息系统），对构件库中没有的构件，则重新开发。

在项目的构建阶段，我们的主要任务是完成新构件的开发和测试，集成所有构件，进行集成测试。在这一阶段，我们采用并行开发方式，大大地提高了开发效率。

在项目的交付阶段，我们把经过集成测试的软件制作安装盘，安装在水电厂，接受实际环境的测试。然后对有关用户和维护人员进行培训和指导。

在以上各阶段结束时，我们都进行了阶段技术评审。在评审中，我们不但按要求邀请了客户代表，还邀请了第三方专家参与评审。

由于全面采用了基于 RUP 的软件过程，规范了管理和开发流程，有效地控制了资源，该项目在没有使用预留资源的情况下顺利完成。在系统运行期间，根据水 电厂的要求和我单位的商业战略，我们又对该软件进行了三次进化过程，最终由软件项目过渡到一个产品。现在，该软件产品已经在全国的多个水电站使用，用户反 映良好。

4 结论

RUP 在迭代的开发过程、需求管理、基于构件的体系结构、可视化软件建模、验证软件质量及控制软件变更等方面，针对所有关键的开发活动为每个开发成员提供了必要的准则、模板和工具指导。它建立了简洁和清晰的过程结构，为开发过程提供较大的通用性。

本文讨论了基于 RUP 的软件过程，并把该过程应用于水电厂综合管理信息系统的开发。与传统的软件过程相比较，基于 RUP 的软件过程可以降低产品风险，规范管理和开发流程，有效地控制资源，提高开发效率。

长春经济技术开发区的网络安全建设

一、系统安全目标

保证电子政务内部网络、外部网络的信息传输、信息存储是安全的、保密的，确保电子政务网络系统安全、可靠、平稳地运行，我们要实现如下系统安全目标：

1．建成开发区完整的网络安全体系，并建立一套可行的网络安全与网络管理策略；

2．采用防火墙系统对开发区电子政务内、外网络进行安全访问控制；

3．通过网络监控系统，全面监视和跟踪进、出网络的所有访问行为，

发现不安全的操作和黑客攻击行为，及时告警和拒绝；

4．建设网络定期安全扫描系统，检测网络安全漏洞，及时了解和掌握计算机当前或近

期使用情况，减少被黑客利用的不安全因素；

5．建立病毒防范体系，防止网络系统被病毒的侵害；

6．通过 CA 认证和 PKI 数据加密技术进行用户身份识别，为电子政务系统提供安全保障；

7．对内、外网络的信息发布平台 WEB 进行保护，防止网站网页被非法人员篡改，为领导决策提供安全的文件传输服务；

8．利用安全评估系统进行系统审计、敏感信息检查，确保电子政务信息的安全；

9．进行重要数据库系统的冗余备份，以备不测或灾难时快速恢复网络系统。

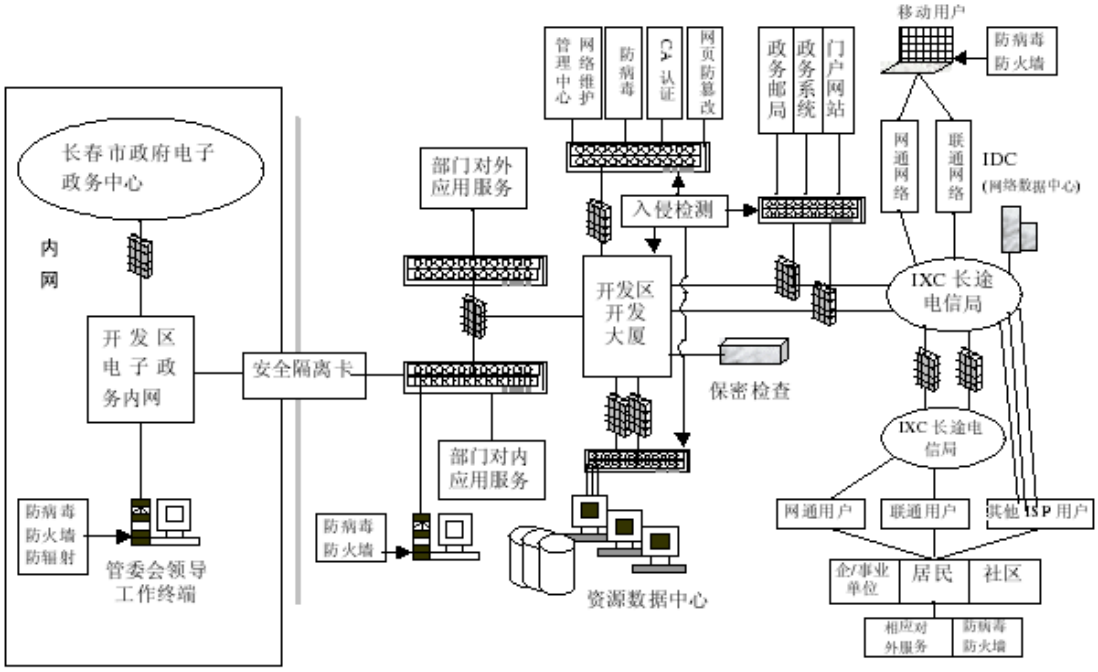


图 5.1 长春经济技术开发区电子政务网络安全结构图

二、实施方案

1、物理安全体系

物理安全是整个系统安全的前提，是保护设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故、人为操作失误或各种计算机犯罪行为导致的破坏的过程。具体实施方案包括机房、通讯线路、物理隔离卡、设备和电源的安全措施。

（1）机房环境安全

接地系统：对政务中心所在的开发大厦内所有计算机和各种地线系统采用统一的防雷处理，即建筑物内共地系统，保证设备安全，并能防止电磁信息泄漏。

防雷措施：开发区在楼顶安装了避雷设施，即在主机房外部安装了接闪器、引下线和接地装置，吸引雷电流，并为泄放提供了一条低阻值通道。机房内部采取屏蔽、合理布线、过电压保护等技术措施，以此达到防雷的目的。另外，还采取相应的防盗、防静电、防火、防水等措施。

（2）通信线路安全

主要是对电源线和信号线采取加装性能良好的滤波器功能，减小阻抗和导线间的交叉耦合，阻止传导发射。对机房水管、暖气管、金属门采用各种电磁屏蔽措施，阻止辐射发生。

3、物理隔离卡

物理隔离卡系统从安全的角度出发，提供了一种安全的用户访问机制，终端用户可以在多网物理隔离的条件下安全自由地访问其中任意一个网络。为如何解决开发区管委会领导班

子、机关处室、企事业、驻区单位等既要接入电子政务内网又要接入电子政务外网的实际需求提供了一套经济、高效、安全的解决方案。根据开发区各部门接入的政务网络类别和数量，选择双网线隔离卡来实现相关功能设计。

4．设备、电源安全

主要是加强对网络系统硬件设备的使用管理，强调坚持做好硬件设备（如交换机、路由器、主机、显示器等）的日常维护和保养工作，定期检查供电系统的各种保护装置及地线是否正常。电源系统电压的波动、浪涌电流和突然断电等意外情况的发生可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生，必须依照国家的相关标准配备。

2、防火墙

将防火墙部署在路由器与受保护的内部网络之间，作为数据包进/出的唯一通道。过滤进、出网络的数据，管理进、出网络的访问行为，封堵某些禁止的业务，记录通过防火墙的信息内容和活动，对网络攻击进行检测和告警。同时，通过设置 DMZ（Demilitarized Zone）实现政府对外网站及信箱与外部畅通的访问。它具体适用范围包括：长春经济技术开发区电子政务门户网站的出入口处；长春经济技术开发区管委会下属各部门的电子政务办公网与电子政务公共网的连接处；长春经济技术开发区电子政务系统的资源中心、数据中心、管理中心、CA 中心的边缘。

在电子政务门户网站的出、入口处，资源数据中心与电子政务连接处，各配置两台千兆防火墙，并对防火墙作双机热备、负载均衡。防火墙组位于电子政务网核心路由器和与 INTERNET 连接的前级路由器设备之间，该组防火墙一方面实现电子政务办公网访问门户网站，另一方面实现 INTERNET 用户访问门户网站，同时实现电子政务公众服务网与电子政务办公网的隔离。即 INTERNET 用户可以通过防火墙访问门户网站，但是却不能访问电子政务办公网。

同时考虑到稳定可靠性的问题，对防火墙作双机热备。确保当主防火墙被宕机后，能在最短时间内启动从防火墙，不影响网络的正常运转和安全。为确保门户网站的服务器群高效、稳定工作，应对服务器群实现负载均衡。负载均衡一般用于提高服务器的整体处理能力，并提高可靠性，可用性，可维护性，最终目的是加快服务器的响应速度，从而防火墙位于资源数据中心与核心交换机之间，实现电子政务外网与提供其办公应用服务器区隔离。

考虑到二者之间的服务量、访问量很大，防火墙负担过重，会出现瓶颈问题，因此，需要对防火墙作负载均衡，以此来增加网络安全性，降低或消除瓶颈，增强防火墙甚至整个网络的可用性。

电子政务网络管理中心及数据容灾备份中心分别配置一台千兆防火墙设备，不使用双机备份。综上所述，我们在开发区电子政务门户网站的出入口、电子政务对外应用服务处、资源数据中心、网络管理中心处配置了高性能的千兆防火墙，并采用了负载均衡设备，实施相应的安全策略控制，保证网络安全，提高整体功能。

3、IDS

针对长春经济技术开发区电子政务系统，入侵检测系统设置用于如下几方面：政府门户网站区域：由于电子政务网络系统的涉密性，黑客会渗透到职能部门，内部人员也很容易通过网络安全防护不严的特点使黑客直接攻击系统漏洞、利用漏洞窃取信息、假冒身份、阻塞服务等。在政府门户网站区域配备入侵检测系统，将有效发现、抵御来自外部的恶意攻击行为。内部办公网络各节点的网络出入口：为对内部用户的网络行为进行审计时提供详尽信息，识别内部用户的非法操作，对内部用户起到一定的约束作用，降低了内部攻击的影响。

内部办公网关键区域：如内部主要服务器区域、网络管理中心等。

内部办公网关键区域，是内部网络资源、管理的核心区域。在这些区域配备入侵检测系统，将有利于进行网络异常行为分析，为内部办公网的正常运行和管理提供有力保障。

入侵检测设备是作为防火墙的合理补充，为每个监测区域根据实际安装一台符合相应带宽需求的入侵检测设备。通过交换机配置，选择合适的入侵检测点进行网络信号的监测。

4、安全漏洞扫描系统

在网络管理中心处配置一台基于网络扫描为主，同时辅以主机和数据库扫描的综合性漏洞扫描与评估系统，可扫描路由器、交换机、防火墙等网络设备以及 Windows、Unix 和 Linux 操作系统、MS SQL Server 和 Oracle 数据库。

5、防病毒系统

采取统一集中管理和分级管理相结合，除了在政务中心安装中央控管防毒软件外，在各应用服务器及用户端都要安装相应的防毒软件。电子政务网络病毒防护是一个重要而复杂的任务，必须将技术、工具和管理三者结合才行。

6、页面防篡改

页面防篡改(InforGuard，简称 iGuard）系统用来保护开发区电子政务网站不发送被篡改的页面内容，支持网页的自动发布、篡改检测、警告和自动恢复，保证传输、鉴别、审计等各个环节的安全。iGuard 使用先进和可靠的 Web 服务器核心内嵌技术，在部分操作系统上辅助以事件触发式技术，从而完全实时地杜绝篡改后的网页被访问的可能性。

Web 服务器和内容管理系统(CMS)都沿用原来的机器，需在其间增加一台发布服务器。iGuard 自动同步机制完全与内容管理系统无关，与其协同工作，内容管理系统本身无须变动。

发布服务器上具有与 Web 服务器上的网站文件完全相同的结构，任何文件/目录的变化都会自动映射到 Web 服务器的相应位置上。网页的合法变更（包括增加、修改、删除、重命名）都在发布服务器上进行，由自动发布子系统将其同步到 Web 服务器上。无论任何情况，不允许直接变更 Web 服务器上的页面文件。

在开发区电子政务网络中， Iguard 设计安装在两台机器上：Web 服务器和发布服务器。发布服务器位于内网中，有着较高的安全防护级别，其上运行自动发布程序和管理子系统。Web 服务器位于 DMZ 中，容易受到篡改攻击，其上运行防篡改模块和同步服务器程序。

7、数据备份与容灾方案的设计

根据开发区的网络结构和应用系统的特点，我们从资源数据中心备份容灾和门户网站的备份与容灾二方面目标，以及 RAID 保护、冗余结构、数据备份、故障预警等多方种方式来考虑，设计采用本地容灾和异地容灾两套系统。

在数据中心采用磁盘阵列为主要设备，采用 SAN 方式进行本地数据存储，支持 NAS 对远程数据进行异地备份。对门户网站的备份与容灾体现在 Web 服务器和防火墙的冗余备份与流量负载均衡等方面。

三、应用及结果分析

分别采取物理安全、防火墙、入侵检测、安全漏洞扫描、CA 认证、病毒防范、网页防篡改和数据备份与容灾等八项措施进行系统安全保护和防范。每种防范措施都从不同的角度，针对不同层的结构，采取相应的应对设备和策略，来阻止来自黑客、网络间谍、信息战敌对分子和恐怖分子的违法犯罪行为。

开发区电子政务外网统一出口，这一措施已经最大限度地防止了网上泄密和入侵攻击。防火墙、入侵检测、漏洞扫描等设施有效地制止了黑客侵扰和对敏感信息破坏、修改或窃取。通过 CA 认证体系，控制了外部人员非法进入电子政务系统。病毒防治和网页防篡改系统及时阻止恶意移动代码等行径的造访，数据备份与容灾系统为天灾人祸作最后的保障。

本方案在实际应用过程中，已起到很好的安全防范效果，电子政务系统得以安全运作。实践证明，使用更高、更强、更好的网络安全工具和技术，配以更有效的安全管理机制，才

会收到更好的安全效果。由于电子政务网络的复杂性，必然导致电子政务网络安全防护的复杂性。

“三分技术，七分管理”是对网络安全状况的客观描述。任何网络仅在技术上是做不到彻底的安全，还需要建立一套科学、严密的网络安全管理体系，将工具、技术和管理三种手段结合起来，才能杜绝和防止因非法访问或恶意攻击而造成损失。

四、管理政策及目标

网络安全管理目标是：采取集中控制、分级管理的模式，建立由专人负责安全事件定期报告和检查制度，从而在管理上确保全方位、多层次、快速有效的网络安全防护。

实践证明，只有通过建立科学、严密的安全管理体系，不断完善管理行为，形成一个动态的安全过程，才能为电子政务网络提供制度上的保证。

总之，本文对电子政务网络信息安全的主要安全防范措施进行了深入细致地研究，确定了具有较高性价比和实用价值的相应的解决方案。

由于能力和精力有限，有一些防范措施研究的不够透彻，也有一些电子政务的安全措施没有探讨和使用，如邮件安全、远程访问、敏感信息检查等，有待在将来的工程设计中更周全地考虑和利用。

总之，电子政务外网是政府面向公众和社会服务的重要窗口，要加强对电子政务外网的网络安全建设和管理。对网络的重要区域，要增设防火墙、入侵检测关卡，或加大防火墙的火力。对重要部门实行特殊保护。同时，加强安全管理意识，健全制度和定期培训。通过对电子政务网络信息安全的安全防范措施和报告深入细致地研究，发现问题和漏洞，及时采取措施加以解决，使电子政务更有效地行使政府职能。

另外，在电子政务安全建设中，需要权衡安全、成本、效率三者的关系。实际上，绝对的安全是没有的，电子政务系统也不是“越安全越好”。不同的电子政务系统，需要根据对信息安全的不同要求而配置安全方案和设施。一个门配几把锁取决于门内放的东西的重要程度，因为锁越多，门的安全成本也就越高，而门的使用效率就越低。因此，必须根据电子政务系统的实际要求做到恰到好处。

基于 B/S 结构的电子政务信息系统的研究与开发

随着我国政治体制改革的不断深入，政府加强了对国有资产及其产权的管理工作。国务院机关事务管理局财务司目前负责中央行政事业单位的国有资产产权管理，依照国家有关规定，中央行政事业单位的国有资产产权管理主要内容有：1.产权登记 2.产权变动 3.产权注销 4.产权年检。

本项目主要为配合此项工作顺利有效的开展设计研制基于 Internet 的产权管理软件。系统的应用规模包括中央行政事业单位及其所辖下属单位。要求通过因特网以 Web 网页形式进行如上业务信息的填报及反馈，主要功能要求国管局及主管部门方便有效地进行业务数据的审批、查询、统计、汇总、表格打印、备份等业务。而且业务数据的安全性、完整性和保密性能够得到较好的保障。

一、运行环境要求

服务器端操作系统为 Microsoft Windows 2000 server（内装 IIS 5.0）；JSP 引擎采用 Resin 1.1.3；数据库管理系统为 Microsoft SQL Server 2000。杀毒软件和放火墙设施自配。客户端操作系统为 Microsoft Windows9X/windowsMe，同时装有 Office 2000。浏览器为 IE5.0 以上。可以连接 Internet。

由于本系统服务的对象具有地理分布性，而且用户数量比较多，加之系统本身属于电子政务系统，功能变化比较快。基于这种需要，系统采用 B/S 结构设计。在这种结构下，用

户可以通过浏览器使用系统的各项功能，可以不受时空限制。同时，系统不需要安装客户端软件，对于功能的扩展和变化，仅需要修改服务器端软件，系统维护比较容易。

二、设计方案

1、网络拓扑结构

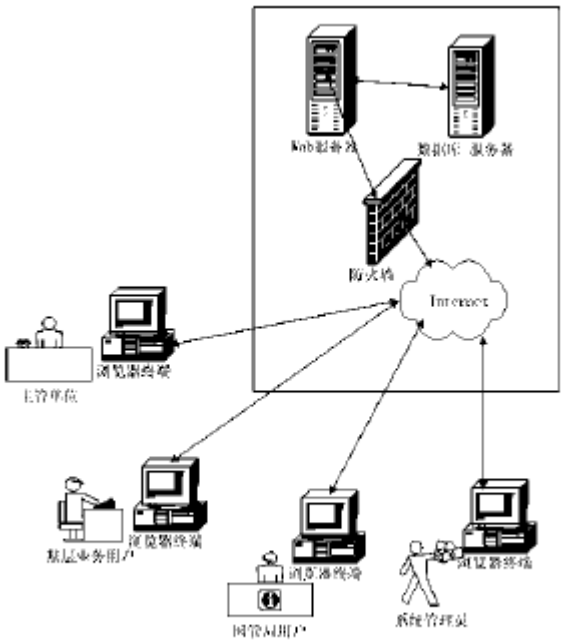


图 3-6 网络拓扑图

本系统是基于因特网的应用系统，通过 Internet 进行网络连接和通信。系统主要由 Web 服务器、数据库服务器、远程终端、Web 应用软件等构成。用户共有四种类型：基层业务用户、主管单位审核员、国管局审核员及系统管理员。

2、系统安全设计概要

该系统从四个方面来保证系统安全：数据库的安全；Web 软件的安全；用户权限的安全；网络通信安全。为防止数据库数据丢失，对数据可以进行远程导出和导入。Web 页面的访问进行严格合法性检查，防止使用者未经身份验证入口非法进入系统。用户身份验证采用密码核对和数字证书分别进行操作员有效性和机构有效性检查。不同权限的用户在系统登入时，按照权限和类别进入不同的软件子系统。浏览器和服务器通信时，利用 SSL 加密信道，保证数据机密性和完整性。

3、报表生成与打印

本系统实现报表生成和打印功能是将生成的报表在 Web 页面上显示出来，然后通过页面打印产生输出来完成的。报表信息从服务器传递到浏览器一端，可以分页传递，也可以一次传递所有的页。如果是分页传递，则需要用户对每页的打印都需要手工操作，所以这种方式比较适用于只对报表进行屏幕浏览或少量选择性打印输出。如果采用所有页面一次性传递到浏览器一端，需要在服务器端对数据库的查询结果进行处理，通过表格以事先规定的格式对信息项目进行显示，这必须根据用户的报表类型在同一页面内以多个相互独立的表格进行显示，以便用户对此页进行打印时报表可以自动进行分页。

统计图形报表利用 Frontpage 中组件生成，Frontpage 中自带有 office 电子表格和 office 电子图表组件，它们都可以通过 Frontpage 嵌入到 Web 页面中。利用这种方法生成统计图表时，可以用 office 电子表格组件为 office 电子图表组件提供数据

源由 office 电子图表组件生成统计图表。而 office 电子表格组件的数据来源可以是服务器端动态生成的文件，从而可以动态生成统计图表。

3、Web 应用软件安全性设计

页面访问合法性检查。为避免不合法用户通过获取 Web 应用程序页面的地址，绕过应用程序的正常入口直接访问有关页面。应在所有关键页面进行用户访问合法性检查，杜绝 Web 应用程序的非法入侵和信息泄密。

Web 应用程序的入口身份验证。在 Web 应用程序的正常入口处进行身份验证，防止未授权用户进入软件系统。

实施客户、服务器身份认证。为避免系统遭受“中间人”攻击，使客户端和服务器端能确认对方身份的合法性，可以为客户端和服务器端配置数字证书，在二者建立连接时验证彼此身份。

对页面输入、输出数据进行严格检查。为避免入侵者利用缓冲区溢出以及站际脚本等攻击手段或防止合法用户无意的错误输入，威胁 Web 应用的安全。可以在用户端和服务器端对用户输入数据的大小和格式实施严格的检查。对输出数据进行过滤和重新编码，去除不应该出现的 HTML 元素或对各种元字符进行编码，使输出数据不被浏览器误认为是合法的 HTML 文档。

对错误和例外进行捕获并进行相应处理，避免系统错误信息过多地泄露系统或应用程序的信息。

在服务器一端应保持一份关于应用程序执行和谁执行这些程序的确切记录，以便于审计。如果有人执行了有损系统的操作，系统管理员可以据此毫不费力地找到责任人。

对 Web 服务器和数据服务器进行严格管理及安全维护。通过设置防火墙和病毒检测程序防止服务器受病毒、黑克和木马程序的攻击。

对需要下载到客户端执行的代码，如 Applet 和 ActiveX 控件实施代码数字签名保护。

服务器端软件应实现“过载保护”。软件设计应能避免和防止客户端在短时间内同时发出无限制的事务请求，以防止有人通过事物请求轰击服务器，使服务器承受过多的负载而“瘫痪”。当然，应同时保持对用户的友好态度。一个令人满意的解决方案是限制服务器所能创建线程数。如果一个客户端的请求导致服务器过载，它就会收到服务器正忙的消息，这种方法比让服务器垮台好得多。

由于出口限制和其他原因，目前的浏览器（包括 IE 和 Netscape）只能支持 56 位对称密钥和 512 位非对称密钥长度的 SSL 连接，这在实际应用中不是非常安全，安全的 SSL 系统需要至少 128 位对称密钥和 1024 位非对称密钥长度。在 SSL 的客户机/服务器模式下，即使服务器端可以支持位数更多的密钥长度，具有较高的安全强度，但由于客户端的限制，实际 SSL 连接中只能使用客户端较低位数的密钥长度来进行安全信息传输。所以可以在客户端安装了一个 SSL 代理程序，它直接接管浏览器发送和接收的信息，利用安全的密钥长度与服务器进行交互（必要的时候还需要在服务器端安装 SSL 服务器代理）。

4、网络通信安全设计

为保证客户端和服务器端之间的通信数据的安全性、保密性、真实性和完整性，二者应建立安全信道的基础上。可以通过 SSL 协议和 HTTPS 协议建立安全信道和安全连接。本系统采用 Windows2000 的 IIS Web 服务器设置，可以建立 SSL 连接和客户端与服务器端的双向身份认证。

5、身份验证安全设计

基于 Web 的专用信息系统通常需要对软件使用者进行身份认证，以确保使用者的合法性和使用权限。本系统是政务信息系统，用户的类别较多，而且相应的业务和数据具有一定

的保密性要求，所以软件的身份认证和权限管理尤其重要。本系统由于要求较高的安全性，考虑到用户的使用方便性和管理的方便性，在身份认证设计中采用用户口令核对和数字证书双重身份认证。

6、数据库安全设计

为防止数据库服务器软、硬件损坏或遭到攻击而丢失数据，软件提供对所有业务数据的备份和恢复功能。具体如下：备份的设计：提供一个页面供用户选择要备份的的数据表，当用户点击某表名以后，服务器端读出此表的所有数据，写入一个文件，然后将此文件下载到客户端[29]，供用户保存。

数据恢复的设计：提供一个页面供用户选择要恢复的的数据表，当用户点击某表名以后，下一页面提示用户上传将要恢复的数据文件。服务器接收文件后，判断文件格式，如果正确，就将数据写入数据表。

7、逻辑结构设计

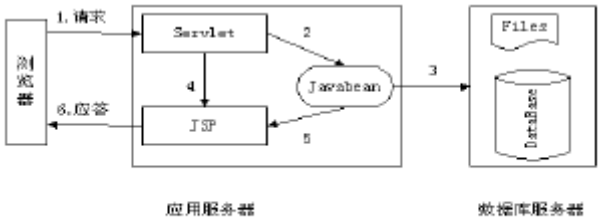


图 4-1 系统实现逻辑架构图

系统采用 B/S 结构模式开发，整体为三层：表示层、应用层和数据服务层。采用 JSP/Servlet 技术实现，整体逻辑结构如图 4-1 所示。用户通过浏览器访问 Web 服务器，服务器调用 Servlet 执行控制逻辑， Servlet 根据功能需要调用 Javabeans 进行业务逻辑处理和数据库访问，Servlet 将通过 JSP 文件来处理结果的显示，JSP 文件通过 Javabeans 得到处理结果并反馈给用户。该系统的设计特点是通过使用组件进行业务处理，不仅可以实现软件复用，同时有利于页面显示和处理逻辑分离，可以提高软件的可扩展性和可维护性。

（1）表示层的实现主要涉及页面的艺术处理、用户输入数据的格式和类型检查、输出数据的格式处理以及表示层和应用层的接口处理。

页面的艺术处理：本系统用户界面的艺术设计主要从从风格定位、版面编排、线条和形状、色彩处理等几个方面考虑，突出政府应用软件的庄重大方。利用帧结构，增加也面的容纳度和操作方便性。利用 Javascript 脚本增加页面的交互性，和操作方便性。

用户输入数据的格式和类型检查：这种功能的实现，主要是利用在页面的 HTML 语句中嵌入 Javascrip 脚本语言来实现的。主要用途为，在用户提交表单以前，检查表单中各项输入数据的格式和类型是否符合要求。实现分布式处理，以减少服务器的工作负担。同时这种实现有助于 Web 软件的安全。

输出数据的格式处理：主要是利用表格、客户端控件、Java applet、图表等数据表示方式进行数据输出，以增强数据可可用性和操作方便性。

表示层和应用层的接口处理：这部分主要是解决页面如何通过提交表单数据给服务器端，以及服务器数据如何传递到页面。本系统中所有表单数据都要传递给应用层的 Servlet。服务器数据的输出，是通过在 Servlet 中生成 Javabean，然后在页面中读取 Javabean 的数据来进行的。

（2） 应用层的实现简介

本系统应用层是由 Servlet 和 Javabean 配合来实现的。其中服务器端软件的控制

部分由一个主控制 Servlet 实现。页面和 Servlet 交互时，通过页面的隐藏数据项向 Servlet 传递一个类别标志，以表明应由哪一段控制代码处理此次交互处理。所有的业务数据处理以及和数据库、文件等的交互操作都由 Javabean 实现。

这样便于实现业务封装，不仅有利于代码复用，还可以增强可维护性和可扩展性。本系统中主要实现的 Javabean 有：文件上传、文件下载、文件读写、数据库操纵等。

（3） 数据服务层实现简介

利用 SQL Server 2000 提供强大的数据库服务功能进行数据管理与操纵。应用层与数据服务层的接口通过 Javabean 实现。具体地讲就是通过 Javabean 调用 JDBC API，由 JDBC 实现和数据库服务器的直接交互。JDBC 实现了对各种数据库的透明访问，使得应用层的代码和数据服务层各自具有独立性，便于维护和移植。

本课题在项目开发中所研究和实现的 Web 通用查询功能、报表与统计图表的生成方法、Web 软件与数据安全机制，以及所实现的通用组件，对同类软件的开发具有很好的借鉴价值。

利用计算机网络软件辅助实施国有资产产权管理，对提高管理水平，减少国有资产的浪费和流失具有重大作用。产权管理系统投入运行后，所带来的主要效益有：中央行政事业单位的产权业务申请直接通过网络传输，可在极短的时间内传递到主管单位和国管局进行审批。数据指标由按年份进行汇总统计分析，变为随时可以进行。信息的表达方式由单一报表变为统计图表和曲线以及报表相结合的方式，便于领导决策。数据的汇总工作，不需要象以往那样每年专门抽调人员进行逐级填报表格，开会统计。节省了大量人力、物力。业务申请单位可通过网络软件随时查看有关审批情况，方便了各级部门的信息交流。

总之，政务信息系统的开发中所需解决的安全性问题、分布式处理问题以及可维护性和可扩展性问题在本论文中均进行了研究和解决，此课题的开展对基于 B/S 结构的政务信息系统的开发具有重要的借鉴意义和学术价值。

基于 J2EE 架构的电子政务网上申报审批系统的设计与实现

一、系统功能需求

1．运用计算机技术，提高申报审批工作的工作效率，节约管理成本。

2．运用网络技术，增强申报审批的透明性，同时提供了申报者和审批者的交流平台。申报审批工作网络化使工作更加高效、准确。

3．将申报和审批结合在一个系统，实现一站式服务体系，方便政府机关对系统的管理和维护，有效的实现了信息共享的目的。

下面以科技厅网上申报审批系统为例对系统需求进行分析。

3.1.1 基本功能分析

1．项目申报：

1) 基本要求：包括项目申请书、项目进展报告、项目验收报告的申报。

2) 具体要求：在线申报过程中，未提交的申报材料具有“暂存”功能，可以在申报期限内无限制的修改。

3) 约束：提交后的项目除非是审核未通过需要修改时才能修改，其他情况不可修改。

2．项目审批：

1) 基本要求：

a. 非技术内容的审批：主要由项目的所归属的各级部门用户审批。

b. 技术内容的审批：主要由指定的项目所属领域的评审专家审批。每个项目至少得有三个专家进行技术审批。

c. 综合终审：主要根据项目所属的类别，由其类别所归口的科技厅各科室用户审批。

2) 具体要求：在审批过程中，未提交的审批意见具有“暂存”功能，可以在申报期限内无限制的修改。

3) 约束：提交后的审批意见不可修改。

3．系统管理

系统管理主要是对整个系统进行整体的管理，主要包括：

1) 项目管理

可查看所有项目信息；定期删除已经结束审批的所有项目，保证数据库不会因为冗余数据的膨胀而崩溃。

2) 用户管理

对所有用户信息的查看和删除。

添加用户：系统管理员直接分配用户名和密码给此类用户，用户可在登录后可修改初始密码和个人资料。

3) 信息发布

由省科技厅发布最新的公告信息和动态新闻，让用户及时的了解科技厅的最新政策措施和与申报审批相关的重要规定等信息。

4．用户注册：

用户填写注册信息后，需经过审核才能成为系统的合法注册用户。

5．用户审核：

注册用户的上一级用户负责审核各用户。通过审核注册信息是否正确可信决定该用户能否成为正式用户。

6．资料修改：

各个用户登录系统后可修改个人注册资料，用户名不可修改。如果是单位用户则同时可以修改本单位资料；如果是下属科技局用户则同时可以修改本科技局信息。

7．信息反馈：

信息反馈主要是为系统的各个用户提供了反馈意见和建议的平台。方便科技厅工作人员集中并及时获取各用户的反馈信息。

二、系统设计

1、架构设计

电子政务系统是较复杂的信息系统，要求比较高，而 J2EE 是一种利用 Java2 平台来简化企业解决方案的开发、部署和管理相关复杂问题的体系结构。J2EE 具有良好的开放性和移植性，可保留已有的信息资源，并能适应未来的变化。J2EE 支持分布式计算以及多种终端。因此在 J2EE 平台上开发电子政务系统，可保证电子政务系统的的可扩展性、可移植性，并能保证电子政务系统的稳定运行。

网上申报审批系统所用到的J2EE组件主要是：HTML，Servlet和Jsp，Java Bean和EJB；数据资源层主要是由关系数据库系统和XML文件组成。 整体架构采用MVC模式。MVC 设计模式结合J2EE各层组件后，便可看作是一个体系结构模式。它可以将J2EE规范中业务逻辑（Java Beans 和 EJB 组件)、控制器逻辑（Servlets/Jsp 动作）、客户视图（IE等客户端）清晰地分离开来。良好的分层可以带来许多好处[20]。除了使用MVC模式建立系统整体框架外，系统各层使用到的J2EE组件和主要设计模式如图4-1所示。

2、表示层实现

4.2.2.1 表示层设计思路

在JSP页面中，如果控制代码和视图创建代码或者数据访问逻辑混在一起，就会在模块化、重用、维护和开发团队的角色分工上造成麻烦，常常出现的情况是只要代码有一处改动，就要改动多个文件。因此在表现层把模型、视图和控制相互分离是很重要的设计目标。

另外控制代码在多处散放，也不便于代码维护。要想避免重复控制逻辑，把系统处理代码和视图分开并将系统访问点集中在一处，可以采取前端控制器模式，作为最初的接触点，用来处理所有相关的请求。

前端控制器能够封装控制逻辑，但是模型组件和显示组件的分离也很重要。因此采用视图助手模式解决这个问题。使用视图封装显示格式的代码，使用助手封装视图业务逻辑。有时候助手对象和模型对象——如传输对象之间会有某种重叠。

3、业务层实现

在多层的J2EE应用系统有一些服务器端的组件，这些组件可能以业务对象、POJO或者实体Bean的形式实现，如果让表示层组件直接访问他们，往往导致现以下问题：

1)在表示层组件和业务组件之间存在了紧耦合，会导致两个层次之间存在直接的依赖关系，如果修改了业务组件接口，就会直接影响表示层。

2)直接让表示层访问业务组件，也会要求表示层组件包含复杂的逻辑，加大了表示层的复杂度和责任。

使用会话门面(Session Facade)模式，封装业务层组件，对远程客户端暴露粗粒度服务，客户端不用直接访问业务组件，而是访问 Session Facade。Session Facade往往把数据信息封装成传输对象提交给表示层组件。

4、数据库层

为 Java 是面向对象语言，所以它和关系数据库在管理数据的方式上不同。在 Java 应用设计中数据以对象的方式进行建模。这些数据对象包含属性，由属性来表示对象的细节。从对象的设计角度来看，对象是不被存储的——它是持久的。对象的生命周期在应用的多次激活中一直延续。

这一切都和关系数据库不同。关系数据库用表和列来表示数据，使用非过程化的语言 SQL 来对数据进行操作。因此需要面对 Java 的面向对象模型和关系数据库的关系模型之间不相匹配这一障碍。我们最终必须通过类的设计来调和它们之间的不同。这也就是所谓的“对象－关系”(Object-Relational, OR)映射过程。OR 映射过程可以使用 OR 映射工具，也可以通过应用多种设计模式来完成。最常见的模式就是 DAO 结合传输对象实现对关系数据库数据的映射[21]。

另外 DAO 将数据源的实现细节完全隐藏起来，当底层数据源实现发生变化时，DAO 暴露给使用者的接口不需要任何改变，因此可以放心得修改 DAO 实现细节，而不会对 DAO 使用这些实现造成任何影响。这一特点在开发网上申报审批系统实际应用中是非常实用的，因为在本系统中，持久化存储介质除了使用关系型数据库管理系统外，还有 XML 文件。

5、基于角色的授权

在科技厅网上申报审批系统需求中对用户角色的规定得很明确，并且每种角色所具有的权限也都有限制。从需求以及对工作流子系统的设计考虑，要求系统对用户的授权应该是基于角色的。

如果采用静态授权，也就是规定好特定的几种角色，并分配给各角色固定的权限集合。那么，如果一个用户可以拥有多个角色，就必须在用户信息中增加一个角色列表，但是这样一来，如果系统增加或者删除角色，就得修改相应的代码。

在本系统中，由于存在部分用户可以同时拥有项目负责人、单位联系人和评审专家三种角色的不同组合这种需求，并且为了使系统具有更高的可扩展性，系统采用基于角色的动态授权机制。为了实现基于角色的动态授权机制，数据库的设计如下图 5-8 所示。

本系统中的用户角色除了必须包含需求中规定的六种角色外，系统管理员可以通过授权模块动态的增加新的角色。例如：如果一个用户已有单位联系人角色，又申请注册为项目负责人。那么系统管理员就可以增加一个新的角色名为：负责人兼联系人，将项目负责人和联系人两个角色权限集合的并集授权给这个新角色，最后修改此用户的 RoleID 为新角色 ID。这样一个用户登录系统后，就可以看到根据其角色相应确定得到的视图，也就是角色所对应的页面(Page)组合；而每个页面上的操作则由角色所对应的动作(Action)决定。

6、临时数据存储

用户在填写申报信息或者审批意见时，往往由于填写项较多，需要较长的一段时间完成。因此为了防止在填写过程中，因为网络故障或是用户的误操作而引起的数据丢失，用户希望能够随时“暂存”已经填写的信息。并且通过暂存功能，用户可以在提交期限内分多次来完成信息填报。这样的功能设计为用户的填报工作提供了很大的灵活性。而这些暂存的未经提交的数据就属于临时信息。如果用户执行提交操作，这些数据就成为持久数据；如果用户放弃提交，这些数据就失去意义而作废。

由于 XML 其自身的开放性和基于文本的结构化方式描述，我们采用 XML 文档作为存放临时信息的临时数据源。

创建临时数据源关键是建立 XML 文档。处理 XML 文件有很多 API，这里系统采用 SUN 公司用于解析和处理 XML 文档的 JDOM API。与 DOM 和 SAX 相比较，JDOM 处理 XML 的方式比 DOM 更加容易，并且它的功能比使用 SAX 更加强大。

根据系统框架，使用 DAO 模式来封装 XML 临时数据源数据存取逻辑，即将 JDOM 解析 XML 文档的业务逻辑。

7、安全性

在科技厅网上申报审批系统中，我们采取 SSL 双向认证，要求客户端和服务器都提供自己的证书。在建立连接时，双方证书传递给对方，这样在数据交互时，就会自动的进行验证和加密，保证了数据交互的保密性和可靠性。

在科技厅网上申报审批系统中，表示层主要采取的策略有：

1) 由于用户输入信息不可预测，如果程序没有考虑或者考虑不全面，用户输入就有可能成为攻击事件，且不管有意还是无意。因此必须对所有的输入信息都要通过过滤处理，剔除掉那些能够造成攻击的可疑字符后，再提交给业务逻辑组件进行进一步处理[29]。

2) 在用户的登录认证时，首先对用户输入的参数(用户名和密码)进行过滤；然后先查询用户名再进行密码验证，分两步来完成验证过程，以减小攻击风险。

3) 进入每个敏感的页面前必须进行身份验证。因为如果用户知道了一个页面 URL，而这个页面又没有验证的程序，则用户可直接输入这个页面的 URL，即绕过了登陆验证，直接进入了指定的页面。

在本系统中，采取对资源层的重要数据加密的方式避免系统管理员直接操作资源信息。例如：审批意见、资助金额等信息。通过加密，把资源信息的备份内容转换成为密文，从而能减少因备份介质失窃或丢失而造成的损失。

XML 文档作为临时数据源，其中的信息也需要进行加密。这里也体现出用 XML 实现临时数据源的优势：XML 可以对信息分片加密，而不是象过去那样必须对整个文件采取加密。这种灵活性很适合只对重要数据加密的操作[31]。

随着电子政务系统的发展以及中国信息化程度的不断提高，在构建网上申报审批系统方面还需要不断吸纳新的技术. 有待于从以下几个方面进行进一步的研究：

1. 如何在 XML 文件中使用数字签名安全技术以保证申报材料的可靠性。
2. 如何改进现有的系统框架，并将系统的功能模块抽象提取，形成通用的政务系统平台。
3. 如何在系统中利用 Web Service 实现不同语言编写的模块之间的通信。Web Service 正逐渐成为系统开发中的一种关键技术，此标准已被各个行业一致地接受。有了 WebService 技术的支持，构建面向服务的系统架构(SOA)正变得势在必行。

统一的电子政府希望能把政府的服务全部融入到整个国家网络中，实现一种整合的无缝集成的“一站式”或“无站式“服务。为了实现这个功能还必须采用“互操作框架“系统或“一站式服务框架“系统。因此J2EE技术必将成为构建电子政务系统的首选方法，所以基于此技术开发的系统框架，以及对工作流自动化的设计和实现将为今后政务的研究和系统开发提供强有力的支持。

Web 应用系统分析与设计

摘要:概述了 Web 的分析与设计的方法，介绍了 Web 设计的规范。并对在构建 Web 应用系统中要注意的具体事项作了详细介绍，提出了总体设计方案。

一、引言

在当今全球信息化大潮中，互联网带给人们的不仅仅是技术，而是一种以信息为标志的崭新的生活方式，正在改变着人们的工作和生活方式。互联网为什么有这么大的魅力呢？这不仅与人们日益增长的文化生活有关，更重要的是与互联网的技术不断更新和革命有关。

二、Web 的结构

Web 基本结构采用开放式主从结构，分布服务器端和客户接受端两个部分：

①服务器结构规定了传输设定、信息传输格式及服务器本身的基本结构。

②服务器接收结构规定了信息接收格式以构件适当的信息接收工具。

1.Web 服务器

Web 服务器是驻留在服务器上的一个程序，它和用户方面的浏览器不断传送着各种信息，它们之间使用超文本传输协议互相通信，WWW 的大量信息存放在 Web 服务器上，Web 服务器的作用就是管理这些文档，处理用户发来的各种请求，将满足用户要求的信息返回给用

户。常用的 Web 服务包括 UNIX 系统上的 CERN 和 NCSA 两种服务器软件。在 Windows NT 环境下，最常用的 Web 服务器软件是微软公司的 IIS.

2.Web 浏览器

浏览器是阅读 Web 上的信息资源的一个软件。如果用户在本地机器上安装了 Web 浏览器软件，就可以读取 Web 上的信息了。浏览器在网络上与 Web 服务器打交道，从服务器上下载文件，并根据 HTML 文件中的内容在屏幕上显示信息。如果文件中包含着图像以及其他类型文件的连接，它也会相应地处理图像及其他类型文件等信息。

三、Web 系统分析

1．系统功能分析

收集有关 Web 元素的信息并进行分析，分析过程包括收集其他可能达到相同目的的信息，或可能达到同一听众的 Web 信息。经分析可寻求以下问题的答案:1.Web 达到了所陈述的意图及规划的目标。2.Web 的操作是否有效。3．是否产生所要的结果。有关 Web 元素的信息及其派生出来的信息，将完全随着实现中已经实现 Web 的程度而变化。开发者可以从规划、设计、实现、或开发的过程中得到有关 Web 元素的信息。如果已经开始了规划的过程，则可以分析观察点并从中得到信息。分析过程的关键是检查 Web 的整体性的意义。分析过程的结果被用于其他的过程来提高 Web 的性能。分析观察点如下：

(1) 听众是否为了给定的意图而使用这个 Web

在规划的过程中，应该首先检查这个听众究竟是否能够使用该 Web。因为使用 Web 的人们的兴趣都在不断增长和变化，对 Web 的人口统计或内容的检查例程可能会给出一些假象听众的信息。

最精确 Web 用户的人员统计是很难得到的。而且，即使是一个最新的对当前用户的粗略的人员统计也无法说出当前正要开始使用的 Web 用户巨大数字。因此，对目标听众的描述与任何人员统计数字的比较都要十分小心，因为它们仅给出听众是否存在的一个“大致感觉”。

(2) 在 Web 的其他地方是否已经达到了目的

一般来说，网站开发者不想复制在其他 Web 上已经成功完成的功能。在 Web 开发的初始阶段以及 Web 的使用过程中不断的问这些问题。新的 Web 和信息在任何时候被开发，也许已经有人为用户的听众开发出了用户也想要完成的那个功能的 Web。

(3) 意图、目标和规范是否共同作用

Web 整体性的最重要的元素就是意图、目标和规范的结合。这三个元素说出了 Web 存在的原因以及它提供了什么。如果潜在听众决定使用用户的 Web ，那么意图描述将是他们所看到的信息的主体。如果意图描述不精确的话，听众可能就不会使用用户的 Web ，尽管他们本来可以从中受益。

检查意图—目标—规范的组合来确保在从意图到目标描述到 Web 规范的翻译过程中，不会遗漏什么东西。做这个检查的一个办法就是做一个图表，跟踪从意图描述、目标描述、规范的这条链。规范应该包括一个在 Web 上使用的所有的 URL 的清单以及一个对数据库的更完整的规范。

(4) 域信息是否精确

Web 所提供的以及在 Web 的开发中所使用的域信息的质量将影响用户对网站整体性能的感知。不精确或不完整的信息都会妨碍 Web 的开发者，也会导致 Web 用户的不满。必须检查这个域信息以确保它是精确的、最新的和完整的。可以根据域的属性来进行以下阶段性的检查:证实链接的新鲜性、检查信息的完整性、检查信息的精确性、检查信息的恰当性。

2．系统安全分析

自从计算机进入社会以来，风险就一直威胁着依赖于计算机的组织和个人。且不说由于自然灾害引起的灾难，也不说由于程序员或操作员的疏忽和各类错误所引起的损失，单就蓄意的计算机犯罪，就已形成了严峻的局面，而且随着计算机技术的不断发展，计算机犯罪的手段也在不断翻新。由简单的闯入系统、哄骗、窃听。发展到制造复杂的病毒、逻辑炸弹、网络蠕虫和特洛伊木马等，而且还在继续发展。

(1) Web 站点安全

Internet 不对机密信息和敏感信息提供保护，所以必须自我保护。一个 Web 站点，只要与 Internet 相联，就可以被所有人访问，除非安装某些形式的保护。作为 Web 站点的管理人员，应努力保护站点的资源、用户、以及客户。Web 的精华- 交互性也正是它的致命弱点。Web 的各种受欢迎的功能例如聊天室、电子商业和自动邮件回复，也是黑客和入侵者们的突破口。有些入侵者有意或无意在你的机器上留下痕迹，严重的是侵入你的系统而你却毫无察觉。

(2) Web 站点风险

总的来说，风险分为两类:机密信息被窃取、数据和软硬件系统被破坏。这两类风险的危害都是不可低估的。信息的泄密可能会危害及国家和民族的安全。中等风险可能关系到一个公司的兴存，关系到一些人生命的安全，名声的破坏。轻微风险可能使用户处于尴尬。

上述两类风险细分为以下四类:1.Web 服务器的信息被破译，最终导致闯入者进入服务器。2.Web 上的文件被未经授权的个人访问，损害了文件的隐私性、机密性和完整性。3．当远程用户向服务器传输信息时，交易被截获。4．系统的 BUG，使得黑客可以远程对 Web 服务器发出指令。

Web 客户机风险:客户机主要用于接受来自 Internet 任一服务器的数据。而这些被接受的数据中，就可能有危及 Web 客户机的成分。因此必须采取有效的措施监视并控制进入的数据，而不能放任各类数据的进入。

Web 服务器风险:服务器上未经授权的访问是主要的风险类型。由于 HTTP 协议提供了在 Web 服务器上写数据的功能，未经受权者可利用这一特性修改服务器的数据。应该进行适当设置以提高 HTTP 服务器的安全性能。

四、Web 系统设计

Web 的设计包括它的外观和感观，而且也要考虑 Web 中的所有元素包括观众信息、意图和目标描述、域信息、页面的规范，联合所有这些产生一个如何实现 Web 的描述。Web 的实现者使用这个设计以及 Web 规范来建立一个运行的 Web。

下面将几个方面来阐述 Web 应用系统的设计方法和特点。

1．设计原则和目标

在整个设计过程中要记住以下的原则和目标:

(1) 符合用户的需求。Web 不是为了满足设计人员的个人喜好，也不是为了实现者的方便或规划人员的一时念头而作的。他的设计是为观众服务的，达到用户的需求是 Web 最优先的考虑。

(2) 有效的使用资源。在设计和实现一个 Web 的时候，选择那些以空间、访问时间、图表和长期维护的最小代价来达到的用户需求的功能。

(3) 生成一个一致的、令人愉快的、有效的 Web 的外观和感观。Web 设计的目标应该是给用户一个有关它的页面的印象，这些页面反映了一个共同结构和一致的视觉线索。

2．用户的经验

Web 的设计坚持以用户为中心来开发，也就是说，开发过程是一个以用户的要求、兴趣、特征、能力、知识、技术为中心的过程。该规划过程应该产生一个好的观众信息集合。

3．信息空间

当浏览者在浏览器里遇到一个新的显示，浏览者想要知道的最基本的信息是“这是什么信息空间?”因为提供给浏览者的信息空间立即建立了有关怎样航行甚至在那个结点中可能会发现什么信息的用户期望。因此 Web 设计人员必须在 Web 的规范中将提供给用户什么样的信息空间和这些信息空间将如何被显示明确表达出来。信息如何组织是 Web 设计人员应该要考虑到的。信息组织指的是信息编码的媒体、信息的结构。一个用户进入一个 FTP 结点时，可能会遇到一个长长的文件清单，其中显示了多种媒体类型:图形、电影、文本文件和目录等，这种多样性就体现了媒体的类型。结构是一个信息空间的特征，比如一个连结点中的文件清单，或是在 HTML 预见文件中的一个有序或无序的列表。结构也是信息表达的模式。

4．设计方法

由于没有一个开发 Web 的定式，所以开发者可以在多种方法中进行选择。没有一个方法在所有的情况下总是工作的很好。因此在设计同一 Web 的时候甚至可以考虑改变方法。整个 Web 应该包括哪些信息，可能一时难以确定，此时自顶向下的设计方法可能是最好的。人类在一个时刻只能处理有限多的信息。帮助用户处理信息作为一个 Web 设计人员的全面挑战，设计中的一个特殊任务是给信息打包或把信息分块。

5．设计中的问题

尽管有些技术能够有助于 Web 生成一致的外观和感官，但有些特定的问题会降低 Web 的设计。这些问题包括:缺乏导航和信息线索、一个过于复杂的信息组织和结构、一个有不均匀结构页面和链接有问题的页面等。这些问题是 Web 设计人员应该注意的。

6．设计人员的检查

设计一个 Web ，主要目的就是满足用户的需要。所以一个设计者应努力遵循以用户为中心的原则和目标来开展 Web 设计工作。Web 的设计人员应该掌握用户对网站信息空间、组织和线索的体验，并使用设计技术来为信息打包和设计链接，以便满足用户需求。Web 的设计过程应该包含设计的技巧和解决问题的经验，设计者要努力去改进 Web 的设计，以便更好的满足用户的需要。

论软件项目计划的制定

摘要：

本文讨论了一个作者参与的软件项目的项目计划制订的若干问题。项目所开发的产品是一种智能电子教学设备，该设备可以实时同步地将用户在硬件端的书写内容显示在计算机屏幕上，并可以保存、 编辑、打印用户输入的数据，联网的计算机也可以实时观看用户的书写过程，并且用户还可以通过投影在硬件端的 PC 机画面交互操作 PC 机。

作者是该项目的软件开发组负责人兼软件架构师。作者针对项目计划的制定采取了：分而治之，逐步求精，经验数据三个主要策略，从而得到较好的效果。

正文：

2002 年 6 月，作者所在公司启动了一个项目，该项目开发出来的产品是一种智能教学设备，该设备可以实时同步地将用户在硬件端的书写内容显示在计算机屏幕上，用户可以保存、编辑、打印通过硬件端输入到计算机的书写内容，联网的计算机也可以实时观看用户的书写过程。另外，用户还可以通过投影在硬件端的 PC 机显示画面交互地操作 PC 机。

作者有幸全程参与该项目的开发，并且担任了项目 PC 机软件开发组的负责人兼软件构架师的角色。对于这种实时通信且具有联网功能的软件项目，我认为首先需要制定一个良好的项目计划，才可以保证项目开发的成功。

总结这次项目的经验，我认为行之有效的策略有三个，分别是分而治之、逐步求精、经验数据。下面就结合这三个策略详细讨论本次项目计划的制订。

一、分而治之

将一个过于复杂的问题分解成若干复杂度不那么高的小问题来依次解决，这种方法人类已经采用了几千年。这里我们也可以用于项目计划的制定。因为整个考虑项目的方方面面来制定计划其复杂度已经超过了人类处理问题的能力。为了解决这个问题，可以将整个项目分解为一些更小的组织体，逐一进行处理，这项工作也就是项目管理中的 WBS（工作分解结构）。

比如针对这次项目中采取的 RUP 开发过程模型，我在完成需求管理计划时我就将计划内容分解成初始、细化、构建、移交四个阶段来分别制定，最后合到一块儿就是完整的需求管理计划。

除了按时间段分解的角度来制定项目计划，我制订软件开发计划时同时按照了 RUP 过程方法的工作流的概念来分解项目计划的制定工作，根据每个工作流在四个阶段业界通用的工作量估计来制定计划，安排工作人员以及相应的软件资源。因为软件开发计划涉及到多个工作流，我认为以这种方式分解是合理的。同时因为本项目的特点，我省略了业务建模工作流，这是因为这次的产品是以硬件为主，软件为辅的消费类产品，所以业务建模不是那么必要了。

以不同的方式分解项目，可以从多个不同的角度来制定整个项目计划，有利于全面、深入地了解项目，避免“瞎子摸象”的情况发生。

二、逐步求精

计划工作其实是一种管理未来、管理未知的工作，而未来是变化莫测的，还存在许多自身无法掌握的因素，因此存在很大的难度。而解决这一困难的法宝就是逐步求精。按照先框架后细节，先粗后细地进行项目的计划。

比如在这个项目中，在接受这个项目后就开始了做了一个初步计划，这个计划的内容主要是做出时间上的安排。因为打算在 2003 的 5 月需要用这个项目的产品申请国家中小企业创新基金的支持，所以完成时间就定在了 2003 年的 4 月，预留一个月用于写申请报告。总的时间进度确定后，大概分配了三个时间段：系统工程分析、软件开发模型确定、软件产品制造时间段、项目总结。

等到确定这次项目后的 RUP 开发模型后，就可以继续对项目计划进行第二次求精了。其实 RUP 过程中出出体现了逐步求精的理念，比如在初始与细化两个阶段都要产生出项目计划的制品。这样我就可以在这个两个阶段对项目计划逐步求精，比如在初始阶段只是将我需要完成的项目计划分为了需求管理计划、软件开发计划、实施计划，然后在细化阶段我再具体地制定每类计划的详细内容。

比如在初始阶段时架构设计考虑以 MFC 为平台，根据这个决定软件开发计划的制定是比较粗略的，在细化阶段架构设计进一步详细，这时已经清楚各个模块和 MFC 的 Doc/View 主结构的接口定义，以及各模块之间的接口定义，这时我就可以根据所需开发的模块制定计划。比如这时我就计划了特效界面模块开发分两次迭代，第一次迭代计划一个月时间，第二次迭代两周时间，第一次迭代需要完成放大和缩小、树形选择、缩略显示等主要的界面效果，第二次迭代的主要任务是根据用户反馈进行修改调整。

三、经验数据

要制定一个良好的计划离不开精确的估算。不过项目计划是在项目开发的早期制定的，而在早期要完成精确的估算是非常困难的。要解决这个问题的关键就在于“经验数据”。由于整个软件产业都还十分年轻，经验数据的积累都普遍不足，才导致这一现象的出现。

但是因为这次项目开发的产品在国内还没有开发过，在加上公司没有积累深厚系统的项目历史数据。针对面临的困难，我选用了 FP 功能点分析做为项目主要的估算方法。因为 FP 方法中有大量项目经验数据可以从网络上获得，同时其数据功能 ILF、EIF，以及事务功能 EI、EO、EQ 的计算对经验数据依赖不强，只需对概念理解正确一般就可以正确估算了。在估算成本的时候，因为公司以前的生产率数据是以 LOC 为单位的，我利用软件工程书籍中的“逆火”经验数据，将 LOC 转换为功能点单位，当然，这里必然导致一些误差。为了降低估算误差，最后使用 Delphi 专家分析法对估算结果进行了调整。

Delphi 方法是一种集策法，也就是通过多名专家对估计值的不断校正的方法。当然，请专家增加了项目成本，不过最后得到高质量的项目计划还是值得的。比如，在某专家的建议下我们改变了自行开发网络层组件的计划，而是采购现有的完全可以解决项目需求的成熟的中间件产品，这个策略的调整在后来证明是正确的。一开始犯错误的原因是由于我们网络开发经验不足把用户需求想复杂了。

最后谈一下使用的工具软件。在制定项目计划过程中我采用了 Microsoft 的 Project 2003 绘制甘特图。因为项目的进度安排是和项目中每个人都是息息相关的，所以在做甘特图前我首先征集了大家对文字和条形图效果的意见，然后按大家的意见进行了美化，比如用鲜艳的颜色标识关键任务，放大任务摘要信息，突出里程碑信息等。这在有些项目管理者看来似乎是小事，不过我认为一个赏心悦目的甘特图可以带给观看者好的心情，而好的心情可以大大提高工作效率。

同时，考虑创新基金支持的项目在交互期限上有很大压力，所以在定义甘特图任务的依赖关系时我采取了业界惯用的“时间盒”的技术，也就是在每个任务的任务信息对话框中“前置任务”一栏中的“延隔时间”我填入 5%－15%，也就是说当任务完成 90%左右时就可以结束转而执行下一个任务。因为本项目中的所有人员几乎是全程参与，所以我不是很担心每个任务遗留的少量问题在下一阶段没有负责人去解决。

配合 Project 2003 使用的估算软件是 Software Productivity Research 的 KnowledgePlan。这款工具软件的最新版加强了对 Microsoft Project 2003 以及 RUP 开发模型的支持，而且其中的 Project Template 功能允许用户采用自己定制的 WBS 来进行估算，这些因素使得 KnowledgePlan 对本项目的项目计划成功制定带来很大的帮助。

在上述三个策略的指导下，以及合适工具的辅助下，使最后形成的计划有效地指导了后期的开发活动。项目开发出来的产品通过了专家的鉴定，获得了国家中小企业创新基金的支持。

项目完成后发现的问题是早期计划的估算结论偏差还是较大，看来还是受到缺乏经验数据或者经验数据不够精确的影响，所以在以后的工作中需要开展有效的度量的工作，为公司积累覆盖面广且尽量精确的经验数据。

论软件开发成本管理

摘要

2004 年 8 月，我作为项目经理开始参与某某银行授信业务系统的开发项目，主要工作职责为需求分析、系统设计和项目管理。系统基本功能包括：业务操作、业务提醒、基础资料、查询统计和权限管理等五个模块。系统采用 Struts+Hibernate 主流 Web 应用框架，实现 Web 应用程序服务器 WebSphere 与协作应用程序服务器 Lotus Domino 的高度集成。

项目的成功很大程度上归功于在项目过程中各个阶段对进度和成本的有效管理和控制。本文以该项目为例，结合作者实践，讨论了信息系统项目中的成本管理问题，主要通过在计划阶段做好工作量估算，有效管理和控制风险因素，在实施阶段进行成本跟踪和控制等方法来有效管理和控制项目成本。实施结果....

正文

2004 年 8 月，我作为项目经理开始参与某某银行授信业务系统的开发项目，主要工作职责为需求分析、系统设计和项目管理。当然也做一些编码工作，主要是基础性公用代码和关键核心代码的编写与维护。授信是指银行以自身信用向客户提供贷款（包括项目贷款）、担保、开票信用证、汇票乘兑等业务，授信业务是商业银行资金运作中最为重要的业务之一。开发授信业务系统，提高授信业务的管理水平和运行效率、充分利用共享的信息资源、减小各种风险、运用各种科学的金融分析模型指导业务开展具有十分重要的意义。系统基本功能包括：业务操作、业务提醒、基础资料、查询统计和权限管理等五个模块。系统全面实现授信业务的网上操作，实现流程的上报，审批和管理，大大提高了授信业务工作效率。提供了强大的业务查询和统计功能，便于对授信业务工作的管理和监督。其中业务操作模块实现授信业务工作流程，主要包括正常类授信业务申报、问题类授信业务申报、特殊类授信业务申报和授后监控业务等工作流程。

系统采用 Struts+Hibernate 主流 Web 应用框架，开发工具采用 WebSphere Studio Application Developer 5.0（WSAD 5.0），WSAD5.0 集成并扩展了 Eclipse 2.0 的功能。硬件配置方面：IBM P610 小型机用于安装 WebSphere 5.0，DELL 服务器用于安装 Domino R6 和 SQL Server 2000。实现 Web 应用程序服务器 WebSphere 与协作应用程序服务器 Lotus Domino 的高度集成，并使用 Single Sign On(SSO)实现单点登陆。总体架构思想，将表单数据的生成和分析采用关系型数据库来实现，通过 WebSphere 架构实现业务逻辑的处理，而表单的审核流程由 Domino 进行驱动。将基于业务为主的 J2EE 服务系统和基于协作为主的 DOMINO 流程处理系统有效的结合起来，确保整个业务流程的有效运行和各种数据查询分析统计的有机结合。

由于考虑到银行帐户年度等因素，客户要求系统在 2004 年 12 底前交付，项目开发周期为 4 个月。项目人员配备情况，项目经理 1 人，开发人员 4 人，测试人员 3 人，界面美工人员 1 人，项目行政秘书 1 人，配置管理人员 1 人，质量管理人员 1 人。其中开发人员小张来自某某银行科技处。项目行政秘书、配置管理、质量管理等人员为兼职人员，为多项目共享。由于公司属于大型软件企业，在项目基础设施方面包括开发服务器、开发机、测试服务器、配置管理服务器、开发工具等配备状况较好。

软件成本管理是软件项目管理的一个重要组成部分，也是一个十分容易被忽视但却又是十分重要的内容。成本管理的目的是通过执行项目成本管理过程和使用一些基本项目管理工具和技术来改进项目成本绩效。项目组整体上把按进度和预算交付项目作为我们最大的挑战，因此我们十分重视对项目进度和成本的控制和管理。该项目中我们借助项目管理软件 Microsoft Project 2003 来辅助进度和成本的计划和管理。我们主要通过在计划阶段做好工作量估算，有效管理和控制风险因素和在实施阶段进行成本跟踪和控制等方法和策略来有效管理和控制项目成本。

1、计划阶段做好活动历时（工作量）估算

项目需求分析阶段结束，《软件需求说明书》得到客户正式签字确认后，我们开始创建工作分解结构 WBS 和制定详细项目进度计划。我们认为工作量估算是成本估算的基础，对于项目成本管理十分关键。由于对代码行（LOC）估算、功能点（FP）估算等估算方式研究不是很深入，工作量估算主要采用基于公司项目历史绩效数据库和个人经验的估算方法。对于部分涉及流程的活动单位一般比较难一次性把握其活动的历时，事实上流程调试的工作量在页面基本功能（增加/删除/修改）的 3 倍工作量以上。例如业务操作模块——问题类授信业务申报——问题类客户行动计划申请流程页面提交工作量为 2 日/人，而流程调试需要涉及 20 多个角色和 8 条路径。对于估算把握不是很好的任务，我们一般通过提供一个乐观估算 A、悲观估算 B、正常估算 M 进行 3 次估算然后利用 PERT 公式[1(4*M+A+B)/6]计算取整。每项活动我都先确定具体人员，然后需要对活动本身进行详细分析，必要时查看公司项目历史绩效数据库。最后需要为各项活动建立了依赖关系，明确各项活动的前置任务，活动开始时间和结束时间。总体上讲活动历时估算工作量较大，我花费了数个工作日。

项目组人员流动率较低，在 J2EE 和 Struts 架构下的 WEB 应用开发已经有一定的项目积累和团队合作基础。如项目组自行开发了功能完善的 Struts-config.xml 统一维护工具，实现了 FormBean 和 ActionBean 方便管理。有大量可供复用的东西，如公共基础代码包，权限管理模块等。这些也是在我们工作量估算中需要考虑的因素。

2、有效管理和控制风险因素

项目中我们对项目风险进行了必要的管理，以避免风险事件的发生引发项目成本增加或超支。公司项目管理部门提供了风险管理计划的模板和风险事件列表模板。为了让项目组整体在各个阶段保持良好的风险意识，我尝试采用了“十大风险事项跟踪”，把项目中各主要风险事项按照排名张贴在公告栏上。由于当时有部分未明晰的需求包括：①问题类客户行动计划申请流程；②查询统计部分需求；③客户方面可能提出的新需求。需求和范围界定不清、计划不充分、用户参与不足、缺乏领导支持、技术问题等为我们项目计划阶段主要风险事件。事实表明，这种做法效果是非常明显的。特别是客户方面，我定期把风险事件列表 Email 给客户方项目负责人方某。为了能尽快落实未明晰的需求部分，我与客户方主要项目负责人方某进行了面对面的沟通。通过一番利弊关系的陈述，达成尽快明晰悬留部分需求的共识。需求问题很快得到解决。项目组整体信心十足，积极性和责任感增加。公司领导方面对项目组也表现出特别的关心，特别是公司赵总开始频繁出现在项目组的每周进度评审会议上，他们也开始担心因为对项目支持不够而导致项目的失败。

3、实施阶段进行成本跟踪和控制

实施阶段需要进行成本的跟踪和控制。Project 2003 中需要设定各项资源（人员）的工时标准费率，即人员每小时的工作成本。项目组成员每周五下班前通过内网 B/S 项目管理信息系统 PMIS 提交《项目周报》，把各自本周内完成的任务进度情况和下周任务计划进行汇报。报告要求按百分比严格量化任务完成情况，PMIS 只提供具体百分比的选择。项目经理（我）把各项任务实际完成数据输入到进度计划中，Project 2003 自动成本统计表，清楚显示任务基准和实际成本信息。通过查看跟踪甘特图就可以较好把握项目总体的进度绩效。

授信业务系统在 2004 年 12 月下旬正式上线，提前 1 周完成了项目。目前系统运行正常，受到客户方各有关部门的一致好评，对项目满意度较高。项目的成功很大程度上归功于在项目过程中各个阶段对进度和成本的有效管理和控制。没有成本管理，项目也可能成功。但没有成本管理的项目，对于项目管理质量、时间、成本三大目标的实现是具有巨大风险。

论软件开发的风险管理

摘要：

本文讨论了某公司实施 SAP 系统的风险管理。该公司原先运行着一套 ERP 系统，现在要转到 SAP 上，需要完成新系统的流程的重新定义，数据的切换，用户的培训等工作。项目要求在 11 个月的时间内完成。实施一个大型的 ERP 系统有着各种的风险，这些风险如果不加分析和控制，将会给整个项目造成致命的影响。我作为项目经理，主要从控制进度风险，人员流动风险和系统功能风险三个方面去进行风险的管理。最后这三方面的风险都得到了有效的控制，从而使项目顺利完成。

正文：

2003 年 1 月，我参与了西门子集团下某公司的 SAP 系统的实施，提任项目经理。该公司之前运行着另一套 ERP 软件：QAD 的 MFG/PRO 系统。由于集团总部的要求，要用 SAP 系统替换原先的 MFG/PRO 系统，并且要在 2003 年 11 月前完成。整个项目完成以下阶段，首先是项目的引进，包括成立项目小组，由顾问对项目小组成员进行初步的培训，让小组成员对 SAP 的标准流程有个大概的认识。接下来是要分模块进行讨论，制定出各模块的实施蓝图(blueprint)。该公司实施了以下的模块：SD（销售与分销），MM（物料管理），CO（成本控制），QM（质量管理），PP（生产控制），FI（财务核算），CO（成本控制）等。在 Blueprint 完成后，由顾问根据定下的流程配置一个测试的系统，用户在该测试环境下进行练习和测试。测试完成后就是数据的准备和切换了，要从 MFG/PRO 系统把需要的数据下载下来然后你上传到 SAP 系统。完成数据的切换，SAP 系统正式上线，同时不再使用原先的系统。

因为整个项目要在 11 个月的时间内完成，时间是非常紧迫的。如何在如此短的时间内使项目能顺利进行，控制各种可能出现的风险是必要的。为此，在项目的初始阶段，我召开了小组成员开会，专门针对项目的风险进行了讨论。会上，大家把想得到的风险都提了出来。经过分析筛选，我最后确定了三个重点进行控制的风险，并采取了相应的措施进行控制。

1、控制进度风险

ERP 的实施是一个大型的项目，涉及到企业的流程改造和其它方方面面的东西。而该项目的上线时间不能改变，所以，项目进度在这里是个潜在的风险，如果不能如期上线，则公司将的运作将会受到重大的影响。为此，我在项目启动后，召集了项目小组成员开会制定项目计划。我首先用 Microsoft Project 制定了项目的总体计划，在这个总体计划中，明确了各个阶段的任务和完成时间。如什么时候完成设计蓝图（Blueprint），什么时候进行关键用户的培训，什么时候进行测试和练习，什么时候进行数据的切换等。总体计划制定出来后，各顾问在总体计划下制定各模块的实施计划，把每个模块在每一阶段的问题细化。各模块的实施计划要在总体计划的基础上进行，在任务和时间上不能滞后于总体计划。无论是总体计划和实施计划，都要求明确各步完成的时间，要精确到哪一天，而不能用模糊的描述，比如“3 月初完成 Blueprint”这样的低描述是不充许的。为保证项目照进度进行，每周五都要召开项目会议，检讨项目的进展情况，发现有超期的任务，分析原因，及时解决。在进度的控制方面，还要应付突发的事件造成的影响，及时地调整计划以适应新的情况。2003 年 4 月—5 月，由于受到“非典”的影响，外部顾问不能出差来我公司，这使项目的进度受到了很大的影响。为了把这种影响降到最低，我即时调整了项目计划，把这段时间安排为关键用户的培训和对系统的熟悉。因为之前顾问已对关键用户进行了一些培训，所以用户对 SAP 系统有了一定的认识。通过上机的操作，更进一步了解系统。有问题我们通过 E-Mail 与顾问联系。通过这种方法，把原本以后进行的用户练习提到了前面。虽然没有顾问的现场指导，但通过自己的摸索对系统的印象更加深刻，为之后的工作打好的基础。

2、控制人员流失的风险

在实施 SAP 过程中，有两种可能会导致人员的离职，一是工作繁重乏味，压力大；二是积累了一定的 SAP 经验后找工作相对比较容易，这时如果有其它更好的机会，员工会考虑跳槽。而项目小组人员流动将会对项目造成很大的影响，甚至导致项目的失败。所以如何控制这些风险，是作为项目经理要考虑的问题。为此，我首先与人力资源部一起，制定了一套有效的激励机制。包括，把参加 SAP 项目作为年终的一个绩效考核内容；因为项目需要加班加点的，公司免费提供晚餐；设立项目基金，对表现突出的小组成员进行物质上的奖励；在整个公司的范围内大力宣传 SAP，让项目小组成员感觉到 SAP 的重要性和实施项目的价值等。其次，为了避免出现某个项目小组成员离职导致项目不能进展的情况出现，我在每个模块都安排了两个人员负责，一个是主负责，一个是次要负责。这样，可以减少人员流失造成的损失。在这里，我没有采用让项目小组成员签合同的方法，即实施项目后要在公司工作多少年。我觉得这种方法会给小组一种压抑的感觉，而公司主要要靠企业文化来吸引员工。事实证明，我所采用的措施是有效的：在整个项目的实施过程中，没有一个小组成员退出或是离职。在项目运行一年多来，只有两个当时的关键用户离职，而他们离职后后备人员可以马上顶上来，对系统没有造成什么影响。

3、控制系统的功能

有人戏称 SAP 是“Stop All Production”，这也从一个方面反映了实施 SAP 的风险所在。而造成上了系统后停产的一个原因就是系统功能不能满足物流和生产的需要，这也是我担心的一个问题。因为切换后旧系统不能再使用，如果这时候新系统满足不了需要，就真的会造成停产。为此，我在项目中采用了演化型的原型开发方法，用演化型的开发方法，可以让用户针对已配置好的原型进行测试，发现不能实现的功能及时提出来，改进后再测试，再改进。在这里，测试工作显得很重要。为此，我强调要一定要做好测试工作。在系统测试阶段，我把所有的项目成员集中在会议室中进行系统测试。在测试中，我要求用真实的数据，模拟真实的环境进行。系统测试通过后，我还特别做了 次上线前的演习，即把所有相关的数据都导致 SAP，配置一个上线后要用的系统，在此系统上进行操作。这次演习成功后，坚定了大家使用系统的信心。系统上线后也没有出现什么大的问题。

通过以上措施，使把 SAP 的主要风险基本上都控制在萌芽状态，项目没有因为这些风险受到影响，最后项目如期上线，受到了管理层和用户的肯定。

在项目进行过程中，有些风险并没有事先预计出来。比如说顾问的问题。有的顾问水平高，但项目也多。用在我们这个项目上的时间就比较少，这给项目带来了不利影响。为此，我通过和该项顾问所在的公司签定合同，注明顾问在我们公司的工作时间，否则将属违约，通过这一方式使顾问的管理得到改善。

应用 CMM 保证软件质量

【摘要】

本文论述了如何在一个规模较大的网上管理系统的开发中结合CMM二级的框架要求，以及软件工程学的质量保证策略进行项目的软件质量保证工作。

本项目的特点有：

（1）开发人员多，有40人左右；

（2）采用面向对象分析与建模技术，JAVA语言，WebLogic应用服务器等以前项目中未采用过的开发模式和技术。因此不确定性因素很多，急需采用有效的质量保证策略。

公司为了提高软件开发能力，已经于近期全面引入了当今软件界正在流行、且行之有效的CMM质量保证体系，并在顾问公司和主评审员的帮助下，由公司的SEPG结合公司实际，制定了初步的规范体系和模板文件，并决定将本项目作为试点项目。

本文详细论述了作为SEPG负责人之一，并且担任本项目质量保证人员的笔者，是如何在本项目中有效推行CMM二级质量保证措施的，并指出了其中的经验教训和有关的建议。

【正文】

本项目是一个面向政府管理部门，全市房地产企业和个人用户的网上管理系统，它既是一个电子商务项目，又是一个电子政务项目。本系统采用了B/S结构，融合了政府部门和房地产企业的内部网上管理系统于一身,同时作为全国建设系统信息化的一部分而实现Inter-net平台上的上下集成。它还提供信息发布、房屋交易等电子商务功能。

本项目对系统的安全以及可靠性等方面有着较高要求，公司决定采用三层架构模式的J2EE环境作为运行环境。另外，本项目参与人员众多，面临着新技术、工期紧等影响软件质量的不利因素，对软件质量保证工作提出了很高的要求。本人作为公司CMM实施工作的负责人之一，以质量保证人员的角色参与到项目的开发和管理工作中，主要负责质量保证策略的建立以及实施工作。

一、以CMM二级理论为指导，采取措施保证开发过程与开发规范的符合性，以过程质量的提高来保证产品的高质量

1、建立起明确的权责制度，减少因权责不明而产生的混乱

为确保质量保证人员有独立的途径向公司反映开发中的问题，同时为了避免质保经理与项目经理、软件配置经理之间过分隔阂，本人在项目启动阶段，起草了《项目管理人员责任书》，并由相关人员评审通过；并提议公司设立了高级经理支持，以快速处理纠纷。

为防止开发人员与项目管理人员在规范化开发过程中过度依赖规范而主动性不高，以及可能产生的相互埋怨，制定并实施了《项目开发人员守则》，由各项目级每个成员在参加项目之初进行签名式确认，以解决开发过程中应规范滞后和实施不力而引起的混乱问题。

2、以制定的《质量保证计划》为纲，全程监控各开发工作的过程建立和符合性问题

在项目启动阶段，就依据CMM二级要求和公司发布的项目开发规范，制定并基线化《ＸＸ项目质量保证计划书》，在计划书中详细地制定了质量保证工作的内容和进度安排。

计划书中主要有职责、培训工作、检查评审及组织工作等四方面的内容。

职责方面详细说明本人作为质量保证人员在项目中的全责以及主要活动，澄清了与各开发角色的关系，主要起到项目成员监督质量保证人员的作用。

培训方面指明了为有效推行CMM质量体系而进行的有关培训，有CMM基础理论方面的，也有本项目特色的规范方面的培训内容。

检查评审方面指出了要检查评审的过程及提交产品，并列举了相应的通过准则，即CHECK一LIST。比如要评审的过程有项目规划阶段；检查项目经理和配置经理是否按有关规范制定了各自的计划书；项目组的技术评审活动是否符合评流程和规范；风险分析过程和任务分解过程是否符合规范的执行。对提交的工作产品，如需求文档和设计文档，是否经过了正式技术评审并基线化。这些都指明了切入时间和建议人员。

组织工作方面指明QA（质保人员的简称）在开发过程要做的组织工作，如技术评审工作、测试工作、估计和工作细分等工作。这些组织工作主要是为了协助项目经理开展工作并能有效且及时地获得第一手质量方面的资料。

对项目开发过程中的跟踪和检查，主要采取了现场参与、分析项目成员日报和周报、个别交流以及项目周例会的形式。

二、以RUPCM和软件工程方面的理论为指导，制订了行之有效的技术规范文件

CMM质量体系更多的关注软件开发过程方面的事情，也就是建义由谁在什么时候做哪些工作，但没有指明各个工作如何开展，也就是偏重于管理，偏轻于技术指导。为了避免在框架方面很有效，但应实现细节不明确而出现的“一条腿走路”的现象，特在项目启动之初就制定了要建立的技术规范，如需求文档编写指南、界面设计规范等。这些都列入QA的计划中了。

考虑到本项目采用了面向对象的分析和设计技术，急需UML和Rose技术方面的指导性文档，因此将与UML高度相关的RUPCM体系为主要参考，其他软件工程理论为辅助参考，组织资源开发人员制定了各个开发阶段的规范性和指导性文档。

实践证明，项目组成员有了CMM过程方面的规范，又有了指导开发工作的详细技术文档后，开发质量有了质的提高。主要体现在以下几点：

1、各个过程的效率提高了，从而保证了各个交互成功的质量。

比如，人员的选择，时间的必备，开展的流程方面真正按照CMM的建议做了，这些都保证了开发过程的高效。一个显著的例子就是技术评审过程。如果选择的人员资格不够，所花的评审时间很少，开展的时机不对，就很难保证提交成果的质量。

2、人员之间的交流变得有效，自信心更强了。

三、不足亟待改进之处

由于是初次按照CMM的要求在项目中实践QA工作，因此不可避免地有一些不足之处，主要有：

- 因培训工作的不及时、不全面，导致QA实施工作遇到了一些麻烦。
- 质量度量数据的收集和分析工作做得还不够。仅仅有少量的度量数据，分析工作也很少。总的原因是缺少一个有效的度量数据收集和分析机制。

总之，这次项目的质量保证工作基本达到了CMM二级的框架要求，证明了过程质量是产品质量的重要因素，为本项目顺利地、高质量地完成做出很大的贡献。但也有很多教训值得吸取，需要在培训工作和QA度量数据收集和利用方面下更大气力。

论企业级信息系统项目管理体系的建立

摘要

2004 年 8 月，我作为项目经理开始参与某某银行授信业务系统的开发项目，主要工作职责为需求分析、系统设计和项目管理。系统基本功能包括：业务操作、业务提醒、基础资料、查询统计和权限管理等五个模块。系统采用 Struts+Hibernate 主流 Web 应用框架，实现 Web 应用程序服务器 WebSphere 与协作应用程序服务器 Lotus Domino 的高度集成。本文结合作者项目实践，以该项目为例，讨论了如何建立企业级信息系统项目管理体系的问题，第一阶段工作重点为普及项目管理知识，第二阶段工作重点为建立项目管理体系，推行“项目经理负责制”。后继阶段的工作重点为项目管理改进与提高。项目管理体系的确立为项目提供了良好的支持环境。

正文

2004 年 8 月，我作为项目经理开始参与某某银行授信业务系统的开发项目，主要工作职责为需求分析、系统设计和项目管理。当然也做一些编码工作，主要是基础性公用代码和关键核心代码的编写与维护。授信是指银行以自身信用向客户提供贷款（包括项目贷款）、担保、开票信用证、汇票乘兑等业务，授信业务是商业银行资金运作中最为重要的业务之一。开发授信业务系统，提高授信业务的管理水平和运行效率、充分利用共享的信息资源、减小各种风险、运用各种科学的金融分析模型指导业务开展具有十分重要的意义。系统基本功能包括：业务操作、业务提醒、基础资料、查询统计和权限管理等五个模块。系统全面实现授信业务的网上操作，实现流程的上报，审批和管理，大大提高了授信业务工作效率。提供了强大的业务查询和统计功能，便于对授信业务工作的管理和监督。其中业务操作模块实现授信业务工作流程，主要包括正常类授信业务申报、问题类授信业务申报、特殊类授信业务申报和授后监控业务等工作流程。

系统采用 Struts+Hibernate 主流 Web 应用框架，开发工具采用 WebSphere Studio Application Developer 5.0（WSAD 5.0），WSAD5.0 集成并扩展了 Eclipse 2.0 的功能。硬件配置方面：IBM P610 小型机用于安装 WebSphere 5.0，DELL 服务器用于安装 Domino R6 和 SQL Server 2000。实现 Web 应用程序服务器 WebSphere 与协作应用程序服务器 Lotus Domino 的高度集成，并使用 Single Sign On(SSO)实现单点登陆。总体架构思想，将表单数据的生成和分析采用关系型数据库来实现，通过 WebSphere 架构实现业务逻辑的处理，而表单的审核流程由 Domino 进行驱动。将基于业务为主的 J2EE 服务系统和基于协作为主的 DOMINO 流程处理系统有效的结合起来，确保整个业务流程的有效运行和各种数据查询分析统计的有机结合。

当时公司为某大型软件（上市）公司在该省的分公司和研发中心，成立不到一年。企业管理和项目管理总体上比较混乱，项目管理中出现了很多问题如项目管理缺乏系统性，项目管理体系不健全，项目风险防范意识缺乏，不注重项目经验总结，项目组之间缺乏合作与交流等。项目组间人员流动频繁，甚至出现分配下去的任务完成一半就改派到一个新的项目组的情况。部分人员同时参与两个或多个项目，双重甚至多重领导。用我们比较形象的说法是“消防队——救火”，管理随意性大，员工整体缺乏稳定的工作环境。为改变这一糟糕的现状，我向公司高层领导提出了建立和完善企业项目管理体系的建议，逐步建立与推行“项目经理负责制”。

对项目管理知识体系的良好把握和过去几年项目实践中积累的丰富经验，使我很快说服了公司领导赵总。当天召开了一次由公司项目经理以上职位人员参加的高效率会议，赵总主持了会议。会上大家总结了公司项目管理中存在的一些问题，对在公司内建立和推行项目管理体系有了很好的认识，很快达成了一致意见。最后落实了人员和责任，由公司技术总监陈某总体负责该项工作，小刘负责“项目经理负责制”相关制度和文档的起草，我负责该项工作的进度计划控制和人员安排等。高层领导的支持和参与对项目管理体系在公司内的成功建立意义重大。

第一阶段工作重点为普及项目管理知识，通过周末集中培训在公司范围内普及项目管理知识。考虑到成本问题，我们采用外派培训的方式。由于我以前参加过 PMI 的项目管理知识培训与认证又是当初工作的提议人，所以就被选中参加了一次为期 3 天的软件企业项目管理方面的专业培训。当然对我来说外派回来任务很重，要对全公司的人员进行 2 天的培训。我对公司研发人员和行政人员进行了分析，发现很多研发人员进入公司前是又项目管理意识的，但慢慢就被整个混乱的组织环境同化。我对培训内容做了 5 天充分的准备，采用多选择图片、多举例子、多讲案例的方式。尽可能增加课程的实质性内容，以项目范围管理、时间管理、费用管理、质量管理为重点，也涉及风险管理、人力资源管理、采购管理、沟通管理和项目整体管理等知识领域。事实证明那次培训是很成功的，公司员工参与程度比较高，很多员工当场提出了很多实际问题和一些好的建议。在我看来，课程最后的一段时间就是一次集思广益的“头脑风暴会议”。

第二阶段工作重点为建立项目管理体系，即“项目经理负责制”。公司整体有了基本的项目管理知识，就正式开始推行“项目经理负责制”。首先是对组织机构进行了调整，我们采用了项目型组织结构，以避免之前双重甚至多重领导而导致管理纷乱的局面。项目经理对项目组人员控制权加大，项目组人员受项目经理单独领导，明确规定部门经理不能对各项目组人员随意调动。如测试部门人员安排到项目的测试阶段，受项目经理的全权控制，测试部经理对相关人员没有控制权。部门存在的意义只是方便相关人员技术交流和问题探讨。公司设立了项目管理办公室（PMO）,主要职能包括：①提供公司项目管理的支撑环境；②公司内多项目的管理与监督；③项目管理制度、规范、文档模板等的建立与维护；④人员绩效考核与绩效数据库的建立与维护；⑤提高公司整体的项目管理能力。我作为项目管理办公室成员主要职责为各项目管理制度、规范、文档模板等的建立与维护，我把项目组中采用的比较完整的《项目管理计划》、《工作分解结构 WBS》《进度计划》等文档模板作了适当的修订供公司各项目组共享。PMO 参考软件产品生命周期模型—ISO 15504 建立了 项目过程模型，对模型中主要过程包括软件开发过程、支持过程、组织过程进行了完整的定义。确立了项目组成员、项目经理、项目管理层（PMO）、项目客户四级项目管理控制体系，明确项目范围、进度与费用控制权限在不同角色之间的分配。

后继阶段的工作重点为项目管理改进与提高。公司在形成基本的项目管理体系后，也特别注重实际项目经验及项目历史数据的积累，及时优化项目管理流程与规范。聘请了外部的项目管理顾问帮助诊断现行项目管理中存在的问题并提供了有价值的意见。

建立了项目管理体系后，公司总体项目管理状况有了较大的改善。各项目组团队凝聚力较强，混乱状态逐渐消失。企业级项目管理体系的建设需要一个逐步完善的过程，企业在关注项目管理体系建设的同时，应注重项目管理知识的普及、人员培养与项目经验积累，逐步提高组织的项目管理水平和能力，最终提高项目管理绩效。

论信息系统的需求管理和范围管理

摘要：

在 2003 年 9 月，我参与了“某省毕业生就业公共网”项目的建设。在项目中担任项目经理职务。该项目作为“数字**”的重点工程，受到了省政府和“数字**”领导小组领导的高度重视。系统以省人事厅为依托，面向全省各级政府人事部门，大中专院校，中介机构、用人单位和毕业生。集就业指导、政策宣传，人才交流，就业手续办理，政府宏观管理于一体。堪称我省至今为止，最大的电子政务项目之一。本文结合作者的经验就项目管理的需求管理和范围管理作了翔实的论述；并就项目过程中采取的措施、方法作了介绍。最后，列举了该项目范围管理的一些不足之处。

正文：

一、项目概述

为进一步加强我省毕业生就业服务体系建设，加强我省人才资源的宏观管理与合理配置，为我省广大毕业生和用人单位提供便捷的人事人才服务；在省领导、省人事厅和“数字**”建设领导小组的高度重视和支持下，“**省毕业生就业公共网”（下简称：就业网）项目作为“数字**”的重点工程于 2003 年 9 月启动了。

项目总投资 150 万元，要求在 2004 年 5 月 1 日前全面竣工并投入使用。

系统要求采用先进的技术手段，以省人事厅为依托，以 Internet 为载体，大中专毕业生就业创业为导向；面向全省各级人事部门，大中专院校，人才中介机构，用人单位和毕业生；连接人事部、教育部和其他兄弟省市就业主管部门、高等院校；构筑一个大容量，宽辐射的全省毕业生就业创业公共服务平台。为我省广大毕业和用人单位提供全面、便捷、快速的人事人才服务；为大中专院校提供集学生学籍管理与就业相关工作的办公自动化平台。预计系统建成后将成为我省第一个面向全省的、大容量的、跨区域的毕业生就业创业电子政务应用服务平台。

通过公司的项目经理竞争上岗机制，我有幸获得了公司领导与业主的信任，成为该项目的项目经理，全面主持项目的管理工作。

在省政府与“数字**”小组领导的亲切关怀下，业主的通力配合与支持下，我与项目组全体同志们一起并肩作战，通过近 8 个月的努力，终于在 2004 年 4 月 15 日全面通过验收，项目花费总成本为 96 万元。比计划提起了 15 天，为公司挣得近 50 万的利润。

二、项目范围难以管理

范围管理是项目管理的基础，也是项目管理工作的重点和难点。含糊的需求和频繁变更的范围让项目的甲乙双方吃尽了苦头。如何做好项目的需求管理与范围管理常常是项目经理最头疼的问题。就业网项目的成功，笔者一直认为得益于有效的项目范围管理机制。在此笔者就就业网项目采取的项目范围管理的一些方法做简略介绍，望各位读者批评指正。

三、项目需求与范围的区别和联系

项目范围(Project-scope)包括项目的最终产品或服务以及实现改产品或服务所需的各项具体工作。从这个意义上讲就是项目应该做什么，不应该做什么，以及如何做。也就是说，项目范围事实包括 2 个方面的内容：项目需求和项目过程。项目需求确定做什么。项目过程确定如何做。

项目范围管理也就是对项目应该做什么和怎么做做出相应的定义和控制。事实上就是对需求的管理和项目过程的管理。

四、就业网项目需求特点

1、项目干系人多

就业网是面向全省各级人事部门（省、市、县三级近 100 个人事行政单位）、大中专院校（近 200 所）、人才中介机构（200 多家）、用人单位（近百万家）、毕业生的大型电子政务项目。项目涉及面广、用户量大。在项目管理中我们必须收集广大用户的意见，获得广大项目干系人的支持。才能打造一个用户乐于使用的电子政务平台，为项目的使用推广打下基础。

2、业务涉及面广

毕业生就业公共网集毕业生就业创业指导、政策宣传、咨询，人才与用人单位的双向交流互动，网上人才市场，毕业生就业手续办理，院校学生学籍管理与就业管理，就业工作监控管理与宏观管理，资源收集整理于一体。涉及毕业生就业工作与人才管理工作的方方面面。

3、全省毕业生就业工作流程不一致

就业网项目涉及我省各级人事部门；但由于政府人事工作的区域性，各设区市都有各自不同的人事制度与毕业生引进制度。造成我省各设区市人事部门毕业生就业工作流程的不一致。

就业网项目涉及我省近 200 所大中专院校。各个学校也均有各自的就业管理工作方法和习惯。

4、各级政府部门、院校信息化程度参差不齐

我省是一个沿海城市，各设区市经济条件不一样，信息化程度更是参差不齐。沿海城市信息化程度比较高，山区城市信息化较为落后。有些单位甚至没有一台电脑。

五、项目范围管理工作方法

就业网项目需求的特点使我们对项目的范围管理狡尽了脑汁。通过专家顾问的指导与项目团队全体同志们的共同努力，采取了相关措施、方法才使的项目的范围管理工作变的更加容易。

1、全省三百多项目干系人参与的项目启动大会

考虑到项目的涉及面广，干系人众多。项目正式启动之初，在业主省人事厅的通力配合下，我们召集了全省各级人事部门、大中专院校负责毕业生就业工作的领导和业务办理同志，重点中介机构和省直重点单位的人事主管三百多人参与项目的启动大会。

在这次会议上，我作为项目经理向各项目干系人，就项目的主要目标、范围、范围管理计划、进度计划安排、沟通方式作了详细介绍。希望各项目干系人能够积极配合我们的工作，我们将尽量满足他们的要求；将就业网建设成为他们乐于使用，能确实帮助他们的网站系统。

2、有效的项目范围管理

这个项目可以说是我通过 PMP 后的第一次将项目管理知识体系知识灵活运用于实践之中。

在项目管理中我们采用了 MS Project2002 作为项目管理工具。通过 Project,我们建立了项目的 WBS。对 WBS 的每个任务明确了其可交付物。对每一个任务我们都要求细化到每个人在一周内可以完成。保证每一项任务都是可控的。

同时我们还制定了完善的项目范围管理计划，WBS 字典，范围变更计划及规程，项目核实标准（含质量控制标准）。并交由业主、项目监理单位审核后，由业主和项目监理单位共同实施。

3、多次的项目评审大会

在项目进度计划中我们确定了 5 个重要里程碑。在这些里程碑结束后，我们将邀请相关项目干系人参与项目的评审工作。目的是为了防止需求偏差、遗漏，和收集新的需求。

第一个重要里程碑是系统原型完成之后，邀请了所有项目干系人代表参与了原型的评审工作。

第二个重要里程碑是政府人事部门业务平台完成之后，邀请了相关政府人事部门的相关业务负责人参与项目评审工作。

第三个重要里程碑是院校端业务平台完成之后，邀请了各重点高校、中等职业学校的相关业务代表参与了项目的评审工作。

第四个重要里程碑是网上人才市场平台完成之后，邀请了重点中介机构，省直重点单位、毕业生代表参加项目的评审工作。

第五个重要里程碑系统基本成型之后，我们再一次组织了全体项目干系人，参加项目评审会议。

每一次的项目评审都给我们带来了很多很好的建议。让我们充分发现了我们系统的不足之处，发现了许多业务上的偏差。当然也有许多项目干系人提出了系统易用性上的建议。会后，我们按照项目范围变更计划和业主、监理单位一起对这些建议作了逐一评估；将那些有益的建议包含进项目范围管理计划中。

4、全体项目干系人的共同努力

其实这个项目的成功是全体项目干系人的成功；是全体项目干系人努力的结果。省领导的重视和项目干系人的激情是这次项目成功的关键。在项目进行过程中许多单位都给我们提出了很多很好的建议；在项目进展过程中，许多院校的负责就业工作的老师，各级人事部门的相关负责同志都纷纷给我们提建议、出点子。我们还设立了热线电话专门接听、收集他们的建议。

六、不足与展望

目前系统运行稳定，到目前为止已经成功的完成了 2 界（近 30 万）毕业生就业管理及派遣工作。并于今年 7 月份获得了省项目科技进步二等奖。

但回顾过去，确也可以发现许多不足之处。如：

1、项目需求分析做的不够充分，没有充分考虑到各设区市业务流程的差异性。造成毕业生就业手续办理流程模块的全面返工。

2、项目可行性研究做的不够充分，没有充分考虑到各设区市信息化程度的差异。造成到目前为止，许多落后的设区市、县无法真正使用就业网系统。

3、除此之外，还存在许多的不足；这里不在逐一列举。

在以后的工作中，我将继续努力学习、总结经验；继续为我国电子政务建设、企业信息化建设作贡献。

论项目的风险管理

摘要

风险就是会给项目带来威胁或机会的一些不确定性事件。2003 年 5 月，我参与了某机场信息系统集成项目的建设，并担任项目经理工作。整个项目总投资近亿元，建设工期为 3 年。因为信息系统集成在当时的国内民航系统来说，还是新兴技术，熟悉民航业务和信息集成技术的专家和技术人员很少，加上项目投资规模大、建设周期长，因此，该项目的风险很大。

为了按照既定的进度、成本和质量完成项目的目标，在该项目中，我充分重视了风险管理，根据风险管理理论，结合自己的项目实践，按照风险管理计划编制、风险识别、风险分析、风险应对计划编制、风险监控等过程，有条不紊地进行风险管理。加之进行了良好的配置管理，整个项目建设过程中，始终遵循了变更控制程序，使该项目顺利完成了其目标。2006 年 3 月，该项目建设完成，并在机场开通时投入生产运行，目前运行稳定。

正文

项目是在复杂的自然和社会环境中进行的，受众多因素的影响。对于这些内外因素，项目管理人员往往认识不足或者没有足够的力量加以控制。项目的过程和结果常常出乎人们的意料，有时不但未达到项目主体预期的目的，反而使其蒙受各种各样的损失；而有时又会给他们带来很好的机会。项目同其他经济活动一样带有风险。要避免和减少损失，将威胁化为机会，我们就必须了解和掌握项目风险的来源、性质和发生规律，进而实行有效的管理。

项目风险是一种不确定的事件或条件，一旦发生，会对项目目标产生某种正面或负面的影响。风险有其成因，同时，如果风险发生，也导致某种后果。当事件、活动或项目有损失或收益与之相联系，涉及到某种或然性或不确定性和涉及到某种选择时，才称为有风险。以上三条，每一个都是风险定义的必要条件，不是充分条件。具有不确定性的事件不一定是风险。

2003 年 5 月，我所在的单位承接了 XX 机场的机场信息系统集成项目的建设工作。该项目是国家重点建设工程项目的一个子项目，其主要工作是应用 EAI 框架，集成机场内其它各个重要信息系统，实现数据共享，整个项目总投资近亿元，建设工期 3 年。2006 年 3 月，该项目建设完成，并在机场开通时投入生产运行，该信息系统集成项目以 ORACLE 9i 为平台，建立了一个可存储机场航班信息、管理信息和运营信息的综合中心数据库，开发了航班信息管理系统、机位自动分配系统、外场管理系统、机场资源管理综合系统等，构造了千兆以太网统一的网络平台，采用了 EAI 框架集成了这些新开发的系统外，还集成了机场内其它各个重要信息系统如航班信息显示系统、离港系统、广播系统等，连接机场外的许多相关系统如空管飞行信息系统、财务系统、航空运营系统等，实现不同应用操作平台的集成、异构数据库的集成，达到数据共享，应用集成。在该项目中，我担任项目管理工作。

到 2003 年为止，我虽然已经负责了近 10 个项目的开发和管理工作，但当时被安排担任该项目的项目经理时，感觉确实是一大挑战。因为信息系统集成在当时（2003 年）的国内民航系统来说，还是新兴技术，熟悉民航业务和信息集成技术的专家和技术人员毕竟很少，因此，这种项目的风险很大。为了按照既定的进度、成本和质量，完成项目的目标，在该项目中，我充分重视了风险管理，按照项目风险管理理论，结合自己的项目实践，有条不紊地完成了该项目。具体来说，我是按照以下基本的管理过程来进行风险管理的。

1. 风险管理计划编制

在项目初期，我组织有关人员编制了风险管理计划，具体描述如何为该项目处理和执行风险管理活动。我们采用会议的方法来制定风险计划的，因为该项目投资规模比较大，所有的项目干系人代表都被邀请参加了风险管理计划会议，全面地考虑了风险对项目的影响，制订充分的风险管理计划。

在计划中，我们确定了基本的风险管理活动（如每 15 天召开一次风险评估会议），根据项目管理理论和我公司的项目实践，定义了项目中的风险管理过程，估计了风险管理的时间表和费用，并把风险管理活动纳入了项目计划，把风险管理费用纳入了成本费用计划。

2. 风险识别

根据项目的实际情况，我们把项目中的风险划分为技术风险、团队风险、外部风险三大类，采用风险分解结构（RBS）形式列举了已知的风险，如图 1 所示。

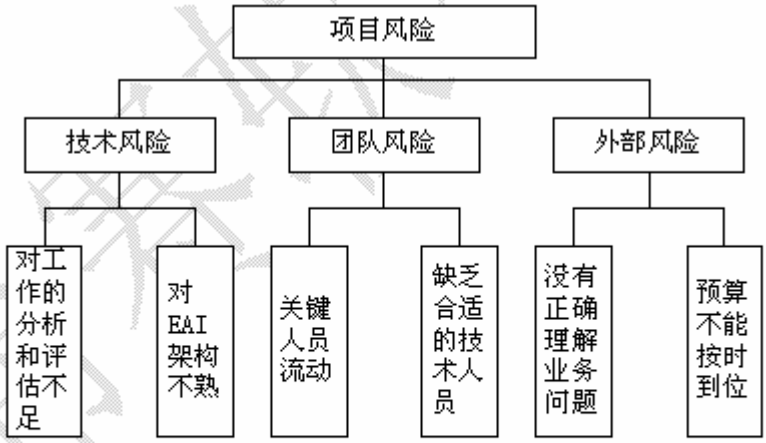


图 1 机场项目 RBS

在识别了上述风险后，我们还确定了这些风险的基本特性，引起这些风险的主要因素，以及可能会影响项目的方面，形成了详细的风险列表记录。根据试题的需要，在这里我只列出引起风险的主要因素，其他的方面限于时间和篇幅，不再介绍。

风险名称	引起风险的主要因素
对工作的分析和评估不足	缺乏类似的项目管理管理经验，对项目工作不熟悉
对 EAI 架构不熟	行业内没有使用先例
关键人员流动	项目周期长，需要长期出差
缺乏合适的技术人员	项目周期长，异地开发
没有正确理解业务问题	项目干系人对业务的认识不足、信息化水平低
预算不能按时到位	甲方资金受限

3. 风险定性分析

我们根据风险管理计划中的定义，确定每一个风险的发生可能性，并记录下来。除了风险发生的可能性，还分析了风险对项目的影响，包括对时间、成本、范围等各方面的影响。其中不仅仅包括对项目的负面影响，还分析了风险带来的机会。

在这个过程中，我们还是采用会议的方式来进行的。不过，在风险分析的会议中，除了有关项目干系人外，我们还邀请了相关领域的专家参加，以提高分析结果的准确性。例如，对于技术类风险的分析，我们就邀请了业内著名的架构专家参与评估。

在确定了风险的可能性和影响后，接下来需要进一步确定风险的优先级。风险优先级是一个综合的指标，其高低反映了风险对项目的综合影响。我们采用了风险优先级矩阵来评定风险优先级的。最后得出的结果是架构风险排在第一位，该风险的可能性很高，影响也很大。

4. 定量风险分析

对已知风险进行定性分析后，我们还进行了定量分析，定量地分析了各风险对项目目标的影响。在这个过程中，我们采用了专家评估的方法，组织相关成员对项目进行乐观、中性和悲观估计，同时，也利用了我公司历史项目的数据，用来辅助评估。

进行定量分析之后，更新了风险记录列表。

5. 风险应对计划编制

根据定性和定量分析的结果，我们对已识别的风险，制订了应对计划。对不同的风险，采取了不同的措施。

风险名称	应对措施
对工作的分析和评估不足	利用已有经验，加强学习，利用标准的技术和理论
对 EAI 架构不熟	聘请 EAI 专家做技术顾问，加强对有关人员进行架构培训
关键人员流动	紧密团结“少数人”，提高项目完成奖金，实行人才备份制
缺乏合适的技术人员	在当地招聘部分技术人员，加强制度建设，加强培训
没有正确理解业务问题	加强对机场人员的培训，提高其信息化水平
预算不能按时到位	在合同中明确规定，由此引起的后果由甲方负责

6. 风险监控

经过上述 5 个过程后，该项目中的风险已经比较清晰，这时就要进入风险跟踪与监控过程。在这个过程中，我们对已经识别出的风险的状态进行跟踪，监控风险发生标志，更深入地分析已经识别出的风险，继续识别项目中新出现的风险，复审风险应对策略的执行情况和效果。根据目前风险监控的结果修改风险应对策略，根据新识别出的风险进行分析并制定新的风险应对措施。

在这个过程中，我们主要采用了偏差分析、项目绩效分析和监控会议的方式来进行的。

总之，该机场项目由于技术领先、投资规模大、建设周期长、异地开发等原因，充满着风险，但由于我们十分重视项目的风险管理，加之进行了良好的配置管理，整个项目建设过程中，始终遵循了变更控制程序，使该项目顺利完成了其目标。2006 年 3 月，该项目建设完成，并在机场开通时投入生产运行，目前运行稳定，得到了机场方的肯定，由此，我得到了公司董事会的嘉奖。

内外网的划分

2001年，中办发17号文件中提出了建设电子政务外网和电子政务内网两个网络平台，这给各级政府的电子政务网络平台建设指明了方向。由于多数副省级城市是按照国办的部署，在17号文件下发之前就已经建成了全市范围的政府专网，因此如何按照内外网的要求，在"三网一库"建设的基础上，在保证全国政府资源网的网络和应用需求的前提下，建设统一的副省级城市政务内网和外网就需要本着慎重的态度，在充分的认证和缜密的考虑下进行。

一、面临的实际难点

要把目前已经建成并相当完善的政府专网转变为政务外网，存在很多的实际难点需要解决，特别是安全保证、IP地址互联、应用划分等问题。

1、安全问题

按照17号文件要求，政务外网与互联网进行逻辑隔离，比较普遍的理解是通过防火墙等安全设备进行隔离，但仅用防火墙是不能完全实现安全防护的，需要完整的安全解决方案。目前的政府专网与互联网物理隔离，有较好的安全保证，但一旦政府专网转成政务外网，与互联网联通后，其安全性就需要特别重视，尤其是网络病毒和木马程序的威胁不容忽视。另外，当政府专网转为政务外网后，需要按照国办要求，与全国政府信息资源与办公业务网（全国政府专网）物理隔离，与全省政府的政务内网也要进行物理隔离。即副省级城市由一个政府专网，变成一个连接省政府、市级各部门和各县（市）区政府、各乡镇和街道的政务外网，一个连接省政府、市级各部门和各县（市）区政府的政务内网，一个连接国务院办公厅、市级各部门的政府本地专网。其中政务外网与互联网联通，与其他两个网物理隔离，而政务内网和政府本地专网与其他任何网络物理隔离。

2、IP地址互联问题

当政府专网转为政务外网，IP地址的合理分配是比较紧迫和现实存在的问题。目前政府专网使用的地址是由国办统一分配的，如浙江是21开头的地址段，宁波由国办分配为35.3开头，考虑到与全省政府的统一性，实际采用了省政府分配的前两位为21.20——1.23的地址段，由于都归结于国办分配，因此不会有地址冲突的情况，与全国和全省政府专网的互通都没有问题。现在要求把政府专网转为政务外网，由于如21等地址并非互联网保留地址，就存在与互联网上地址重复的情况，需要通过办法进行解决。即使现在把地址都转为如10开头的互联网保留地址，其问题也是比较严重的：一是需要更改所有的网络设备、服务器、微机的IP地址，带来巨大的工作量和运行风险，可能会造成应用的短期停止；二是到目前为止，全国范围的政务外网地址分配方案还没有看到，如果只考虑目前的情况而选定一段保留地址，那么会给以后全国政务外网互联带来隐患。任何一个网络，其生命的起点就是IP地址，需要切实解决IP地址的互联问题。

3、应用划分问题

在政府专网上的应用，主要有三类：一是各部门的纵向系统，如计委纵向网、水利远程会商系统、计生纵

向系统等，这类系统是在市级部门和各县(市)对应的部门之间进行数据交换的应用系统；二是各部门之间的横向系统，如财政局会计核算系统、工商局的信用城市系统等，这类系统是在市级各部门之间进行数据交换的应用系统；三是纵向和横向单位都涉及的系统，如市政府办公厅的公文传输系统、人大政协的议案提案办理系统、市委组织部的党内信息管理系统等，这些系统是在全市范围内进行数据交换的应用系统。以上三类是局限在副省级城市范围的应用，除此之外，还有从国务院、省政府下来到市政府的应用，从国家各部委下来到市级各部门的应用，这些应用是通过全国政府专网或各部委的独立纵向网来实现的。目前所有的应用都在政府专网上跑，但当政府专网转为政府外网时，就需要对这些应用的安全需求进行区分，把不同要求的应用划到不同的网络中，从而也带来了如何保证应用的平滑过渡问题。

二、建设思路和难点问题的对策

针对以上的难点，需要有可行的解决对策，要对现有的网络结构进行分析并进行整合，可能需要进行合理的分割、调整和联接，要对目前专网上的用户进行划分和明确需求。

总体建设思路是把现有的市政府专网转为政府外网，并与全国政府专网物理隔离，重新建一套政务内网与全国政府专网互联，如果按照上级要求政务内网不能与全国政府专网互联，那么还需要建一套市政府专网，并与全国政府专网互联。在考虑应用需求和安全要求的基础上，可以对新建的政务内网和市政府专网的网络范围适当控制，初步设想是先建设网络核心层和汇聚层，各单位的内网接入可以按需要有一个接一个，逐步扩大。从实际出发，目前副省级城市建一套政务外网和一套政务内网是比较合适的。

(一)建设原则

任何一个信息系统的建设都存在技术、实施和资金的可行性问题，对于像副省级城市政府专网向政务外网过渡这样的信息系统建设，应该充分考虑其技术和实施的可行性。而技术上一定要考虑采用的技术符合实际情况，能够在确保安全和应用完整的情况下平滑地进行过渡；实施上要充分保证应用完整，确保可行。总的原则是"实事求是，保证应用，平滑过渡"。

(二)网络结构总体设想

为描述和建设的明确性、方便性，网络结构的设计以建一套政务内网和一套政务外网为样本。另外，本方案设想是以笔者所在城市的政府网络为案例。

目前市政府专网向上采用2M的帧中继专线方式分别连接全国和全省政府专网，向下采用155M SDH线路或物理光纤100M以太方式连接各县(市)区政府专网，与各部门的局域网采用物理光纤100M以太方式连接。市政府专网与各网络之间的连接通过防火墙进行逻辑隔离，整个网络与互联网物理隔离。专网核心为千兆，到各接入点为百兆，目前已稳定运行二年，接入计算机三千多台，个别县(市)区已接到乡镇。

建设政务外网的目的主要提供为民服务，因此需要与互联网进行连接，同时为保证安全，与政务内网物理隔离，向上与全省政务外网互联，向下与各县(市)政务外网互联。按照总体建设思路，政务外网由市政府专网继承过来的，因此其网络结构基本保持不变，主要工作是增加了与互联网的统一出口，切断了与全国政府专网的连接，而原来与全省政府专网的连接变为与全省政务外网的连接。

由于安全要求，政务内网的接入范围相比政务外网要小一些，向上连接国家广域政务内网和全省政务内网，因国家广域政务内网现没有明确，考虑先接到全国政府专网，向下连接各县(市)区党委机要系统和政府办公室，各部门的接入按照机要范围确定。综合目前实际和将来发展等情况，政务内网需要新建，但接入范围进行严格控制。

根据性能需要、网络安全和投资规模，政务内网在市区内可采用物理光纤，在市区外可采用SDH线路，核心采用三层骨干交换机，市区汇集点可采用中档交换机以千兆方式接入核心层，市区内各单位以百兆光纤收发器接入汇聚层，市区外各单位以2M SDH方式接入。由于接入市政府专网的各单位光纤一般为6芯，因此再用2芯来接入政务内网是非常方便的，可以很快地建成政务内网。

(三)难点问题的解决对策

针对安全保证、IP地址互联、应用划分和保证等难点，在充分考虑各方面因素的基础上，提出相应的解决对策。

1、安全问题解决对策

通过对政府专网的调整补充，安全问题主要是解决政务外网、政务内网和全国政府专网的安全。政务外网与互联网逻辑连通后，主要安全焦点

集中在与互联网的出口处，建议全市政府外网以一个统一出口到互联网，这样一是可以在人员安排上能保证集中精力进行有效管理和安全审计，二是可以集中投入安全设备，保证有效投资，这些安全设备通常包括防火墙、入侵检测、漏洞扫描等，三是在费用上实现统一支付，可以降低互联网出口资费。在出口处还应该确定安全策略，既互联网的计算机不允许直接访问外网内的任何设备，外网的计算机有限度地访问互联网。由于外网可以定位为工作网，与互联网存在着区别，因此外网访问互联网可以只开放如web访问、邮件等功能，避免全部开放带来的管理和安全问题。政务内网按上级要求以涉密网建设，应按照有关的保密要求确保安全，包括独立的线路和设备，与其他网络物理隔离。全国政府专网与政务外网应该物理隔离，其接入范围限于市政府办公厅和对上有业务联系的部分政府单位，实际上还需要建一套网络。考虑到资金和业务相关性，建议市政府内网作为全国政府专网在本地的网络延伸，不再另建网络，同时安全性也符合全国政府专网的要求。

2、IP地址互联问题解决对策

政府专网转到政务外网，其IP地址互联是非常迫切和现实的问题，要解决这个问题有两个办法：一是专网转成外网后，保持目前的IP地址不动，与互联网的数据交换通过在网络设备上进行地址转换（NAT）来实现，这个办法存在一个缺陷，即由于外网用的地址不是互联网保留地址，所以就不能访问互联网上相同IP地址段的服务器，因为网络路由不会转到互联网上，只在外网内部传递，但大部分互联网服务器都能够访问。二是专网转成外网后，所有的IP地址都重新规划和更改成互联网保留地址。这种方式实施起来难度大，要影响正常网络运行，也有存在以后与全国政务外网互联的隐患。比较两种办法，建议在目前阶段使用第一种办法，以避免较大的风险。

3、应用划分问题解决对策

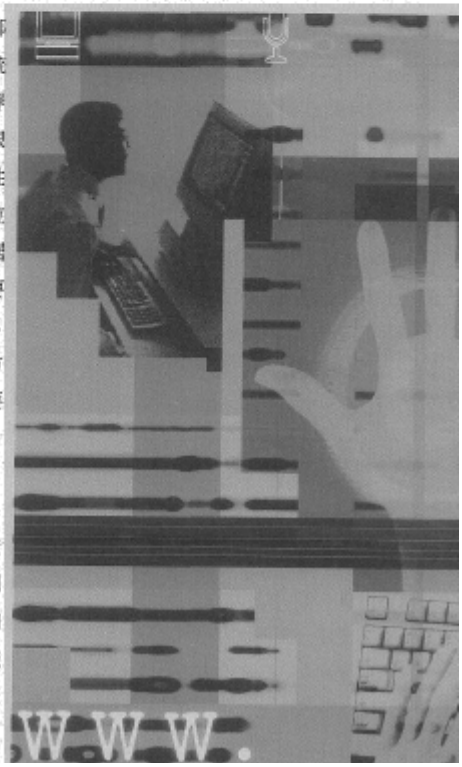
考虑到专网上应用的多样性和复杂性，应用的划分是一个很棘手的问题。根据建设内外网的初衷，是要把副省级以下政府的各项应用划到政务外网上，而政务内网到副省级城市为止。按照这样的出发点和目前实际应用情况，尽量把目前专网上的大部分应用都划到外网上，如网上办公、公文和信息交换、电子邮件等。同时要考虑到有些系统如财政税收系统、劳动局的养老保险医疗保险系统涉及到很多经济方面的数据，其重要性也非常明显。而目前这些单位都表示与互联网不能互通，据了解上级部门也有这样的要求，那么就要区分这些应用，建议在政务外网上利用VPN方式满足这些单位的安全保密要求。

（四）统一实施

政府专网向政务外网的过渡，是对原有网络进行改造、调整和补充，由于受原有条件和资源的限制，这项工作的实施难度就非常大，最起码要保证网络的安全和应用的连续性，在实施时要保证全国政府专网的安全，要保证关键应用不受影响。由于同一个省内，省政府、副省级城市都接在全国政府专网上，因此在网络的分离中，要由省政府进行统一安排，否则会造成一边与互联网连通，而一边还接着国办的情况，形成安全问题。另外，如果IP地址要更改，也要全省统一，而地址更改的实施难度巨大，涉及面太广，因此非到万不得已，不要进行地址的更改。

总之，副省级城市政府专网向政务内外网发展是政务信息化建设的一项重要任务和必然趋势，只要我们思想重视、实事求是、认真负责，相信一定能够圆满地完成此项任务。

（作者单位：宁波市人民政府办公厅信息中心）



企业信息系统的需求获取

企业管理信息系统项目的实施,无论按何种方式来组织,都必须经历需求分析阶段,因为需求性是系统开发的源头,是信息系统开发过程中关键的一环,只有真正弄清楚企业信息化需求的目标和要求,才能做到对症下药、在后续的开发中设计出达成目标的系统体系构架和实现方式,并且不断改进,使之逐步完善。需求获取是需求工程的第一阶段。对于较大型的开发项目,其复杂性主要来自客观和主观两个方面。从客观上说,需求工程面对的问题几乎是没有范围的。由于企业信息系统的应用涉及企业管理的各个层面和广泛的活动领域,与其管理活动的特征和施行过程的习惯性密切相关;此外,客观上的难度还体现在非功能性需求及其与功能性需求的错综复杂的联系上, 当前对非功能性需求分析建模技术的缺乏也大大增加了需求获取的难度。从主观意义上说,需求工程需要方方面面人员的参与(如领域专家、领域用户、系统投资人、系统分析员、需求分析员等等),各方面人员有不同的着眼点和不同的知识背景,沟通上的困难也人为增加了需求获取的难度。信息系统的需求不像制造产品需要原材料那样简单,本文试图通过规范需求获取的行为,帮助需求分析人员把握好方法与技巧,恰当地启发引导用户表达自己的需求,以便为项目的成功奠定一个好的基石。

1 需求定义

需求定义是将用户的非形式化的信息系统需求变为形式化的需求规范的过程。用户需求是指用户对目标系统在功能、行为、性能、设计约束等方面的期望。需求定义是需求工程的第一步,他通过对应用问题及其环境的理解与分析,将用户需求精确化、标准化,最终形成规范的需求说明书,从而为问题涉及的信息、功能及系统行为建立模型。

企业信息系统的需求是开发项目最难把握的问题之一,许多开发项目的经验证明,用户对系统的需求始终处于变化之中,有些开发项目都快完成了,而用户还有新的需求在提出。特别是目前大部分较小的开发项目往往轻视系统调查或者调研过程过于简单,造成用户需求定义不准,使得系统难以达到预期目标,有的还需要二次开发和修改,浪费了大量的人力和财力。

影响需求定义的因素很多。首先是不符合国际通行的规范,主要症状表现为需求内容的层次不清晰,往往是庞杂软件需求细节的简单堆砌,很难从高层次上理解软件产品“为什么做和做什么”。其次是需求对象的不确定性,可以说需求是一种模型,是产品的早期雏形,通过进行需求分析,我们可以对最终产品做出优化,需要始终保持注意的是,需求性是始终处于变化之中的。再就是系统分析人员和用户之间的沟通问题,由于他们的知识背景不同,看问题的角度不一样,造成了这种通讯的差异。需求工程无疑是当前系统开发中的关键问题,美国在1995年开始对全国的8000个软件项目进行跟踪调查,结果表明,有1/3的项目没能完成,而在完成的2/3项目中,又有1/2的项目没有成功实施。仔细分析这些失败的原因后发现,与需求过程相关的原因占了45%,而其中缺乏最终用户的参与以及需求定义不准又是两大首要原因,各占13%和12%。

用户需求是整个开发项目最关键的一个输入, 和一般的工程项目相比较, 信息系统的需求具有模糊性、不确定性、变化性和主观性的特点,他不像水利工程、建筑工程等实体项目的需求,是有形的、客观的、可描述的、可检测的,所以,需求定义是系统开发最难把握的问题,主要表现在以下方面:

需求描述:不幸的是,在我们开发的项目中,大多数系统的需求事先都难以说清,更谈不上完整的定义。一方面,用户心目中的“需求”只是一个模糊概念,即使在开发者即使在开发者的再三启发下,用户也只能把有关系统的功能等一些模糊概念加以重新阐述,使之成为具体细节。另一方面,系统分析人员只起着询问者或顾问的作用,他们不可能很清楚地了解具体业务细节和全部要求,因此,在大量与用户交换意见的过程中, 传错信息和发生误解的可能性极大, 尽管需求定义过程一直强调需求获取是一个不断地启发、揭示和判断过程,然而,问题是我们应如何进行这个过程,人们对已经存在的事物总是容易作出评价的,却不善于描述不存在的东西。更不幸的是,不同的业务人员对同一业务过程的描述也会是不尽相同的。不同层次的用户关心的问题也是不一样的,想要每个用户都成为需求专家是不现实的。有这样一个案例,当系统开发完成后,业务部门讲“这不是我们最初所反映的需求,我们说的不是这样的!”。缺少正式的完整的需求文档浪费了大量的人力、物力,但是有了需求文档又出现了新的问题。曾经有不少项目经理抱怨过,在用户方进行的需求评审会完全是走形式,因为用户根本不去听他们读那上百页的需求文档。

需求完备程度：如何准确划定系统的范围？如何使需求做到没有遗漏？这确实是一个两难问题，稍大一点系统要想穷举需求几乎是不可能的，每次开需求评审会时，总会冒出新的需求，以至于系统没有一个准确的范围界定。即使这样，系统还是要开发，没办法，系统的范围还要硬性划定一个，从而建立一个基线。

需求细致程度：需求到底描述到什么程度，才算可以结束了？仁者见仁，智者见智，并没有定论，如果时间允许，要想细致就总可以细下去。这样，需求定义的周期就越长，可能的变化越多，对设计的限制越严格，对需求的共性提取要求也越高，所以只要大家（客户、用户、需求分析人员、设计人员、测试人员）一致认为描述清楚了，就可以进入下阶段工作。

需求变化：在系统开发过程中如果只有一条真理的话，那一定是：需求的变化是永恒的，需求不可能是完备的。信息系统开发的过程实际上就是在不断满足变化的需求的过程，需求的变更不一定都是坏事，需求变化的原因很多，如："开始对项目认识不全，现在需要增加需求"，"用户的业务发生了变化，需求必须变化"，"开始的需求弄错了"，"需求定义不清楚"等。需求变化的问题是每个开发人员、每个项目经理都要遇到的问题，也是最头痛的问题，一旦发生了需求变化，你不得不修改你的设计、重写你的代码、修改你的测试用例、调整你的项目计划等等，需求变化的代价常常使项目搁置，为项目的正常进展带来无数的麻烦。

2　需求获取的管理

需求获取是指需求定义的过程。由于需求定义的复杂性和变化性，常常会影响到系统开发的成效，使得人们越来越重视需求获取的管理问题。使需求在受控的状态下发生变化，而不是随意变化，需求获取的管理就是要按照标准的流程来控制需求的变化。

2.1　需求调研步骤

第一步：调研开发对象系统的组织结构、岗位设置、职责范围，可采用U/C图等从功能上区分有多少个子系统，划定系统的边界，明确系统的目标。

第二步：调研每个子系统所需的工作流程、功能与处理规则，收集单据、报表、帐本等原始资料，分析物流、资金流、信息流三者的关系，以及如何用数据流来表示这三者的关系。

第三步：设计调研方案，针对不同管理层次的用户询问不同的问题，列出问题清单或事先准备好问卷。将操作层、管理层、决策层的需求既联系又区分开来，形成一个金字塔，使下层能满足上层的需求。

第四步：尽量熟悉用户的业务情况，对与用户沟通的情况及时总结归纳，整理调研结果，找出新的疑点，初步构成需求基线。

第五步：若基线符合要求，则需求获取完毕。反之返回到第一步或第二或第三步，如此循环多次，直到需求定义使双方满意为止。

2.2　需求引导

需求获取阶段是和用户交往最多的一段时间，而绝大部分用户是不懂得需求分析方法的，他们不知道怎样全面而又准确无误地表达自己的需求，因而对于需求分析人员来讲，需要掌握很好的方法与技巧，恰当地启发引导用户表达自己的需求，以便准确的定义需求。

1）在调研前和用户讲清楚调研的意义、过程、以及需要注意的问题。调研过程要经过多次反复，用户不一定理解这个过程，调查时一定要对用户讲清楚。

2）做好调查前的准备工作。在每次和用户见面前，要准备好问题单，对问题进行合理的分类，安排提问的次序，并事先提供给用户，便于用户准备，以提高工作效率。减少用户的反感情绪。

3）发问时要以一人为主，其他人注意记录与查找问题。

4）在用户讲解时，不要中断用户，使对方有充分的演说机会。

5）对询问的问题要有记录，这样便于整理文档，也便于统计工作量。

6）调研时注意以"IPO"图作为总体主线。在与用户接触时，最容易和用户交流的是他们的业务，即每天他们在干什么？这些业务流程基本是一样的：收到别人传来的单据报表，进行加工处理，再传给其他人。就这样"接受、处理、传出"，如此循环，就象车间里的流水生产线，原材料"输入"(Input)、生产线加工、"处理"(Process)、产成品"输出"(Output)，就是"IPO"的基本思想，因而在调研时采用这种思想易于同用户交流。

7）注意交谈的技巧，并尽可能多的记住用户的姓名、职务、爱好等。要在用户提供的单据中提炼出其中最本质的内容来。在调研开始、结束、中间疲劳时适当的闲侃，拉近和用户的距离，尽量与用户交朋友。

2.3 需求获取管理的要点

需求共识：需求管理的首要任务在于使开发人员和用户双方对于需求都有一个明确的认识。因此用来进行需求定义的语言组织应当使所有相关人员都能够理解，进而对整个项目有一个整体把握，并明确每一个人在项目中所起的作用。要使所有相关人员达成共识，首要的任务，就是与用户共同制定需求定义表述的规范，必要时可对项目参加者进行基础知识培训，使用户尽可能通过术语的形式表述需求，这种表述应当使每一位开发者明确自己的职责所在，并且清楚知道不同开发工作之间的关联。

以流程为主线：在与用户交流的过程中，应该用流程将所有的内容串起来，如单据、信息、组织结构、处理规则等，这样便于交流沟通，符合用户的思维习惯。流程的描述既要有宏观，又要有微观。即要强调总体的业务流程、全生命周期的业务流程，又要对流程细化，有分支的业务流程。在分析企业流程并进行优化时，要注意把握以下几方面的问题：

1）该流程中是否存在不必要的环节？

2）是否可以将决策的权力下放到作业部门？

3）流程是否可以简化？

4）是否可以省略一些环节？

5）流程中的每个处理环节是否起到了增值的作用？

6）哪些流程可以并行处理？

7）与需求并行可提前做的设计工作有哪些？例如：数据库概念模型设计？基础数据字典设计？

需求整理与表达：需求整理可以采用穷举、归纳、抽象等方法。采用穷举的方法可以避免遗漏，可通过列出各种情况的排列组合达到穷举目地；采用归纳的方法可以使问题更加条理化，可通过对各种情况进行综合分类达到归纳的目地；采用抽象的方法，可以发现问题实质，抓住问题的主要矛盾，忽略其次要矛盾。在整理时可以多种手段共用，如组织结构图、业务流程图、多叉树、关系矩阵、文字叙述(对其他描述手段的一种补充)、表格(如单据调查表、帐本调查表、业务调查表、报表调查表等)、图形等多种手段。对需求的描述可以从组织结构与岗位定义、业务流程、处理规则、数据项、处理功能以及相互之间的关系方面来进行。

需求变化的控制：将来用户需求的变化是很正常的现象，如果仅仅着眼于现在，而不对将来有所考虑，系统的寿命便不会长久，对用户的投资是一种浪费，故此要"防患于未然"，将以后可能的变化予以充分的考虑。需求中的变化一般不是突发性的变化，最常见的是"项目需求的渐变"(ProjectScopeCreep)问题，这种渐变很可能是用户与开发方都没有意识到的，当达到一定程度时，双方才蓦然惊醒，发现已经物是人非。控制需求渐变需要把握以下几点原则：

1）需求一定要与投入有明确联系，否则如果需求变更的成本由开发方来承担，则项目需求的变更就成为必然了。所以，在项目的开始无论是开发方还是出资方都要明确这一条：需求变，软件开发的投入也要变。

2）需求的变更要经过出资者的认可，需求的变更会引起投入的变化，所以要通过出资者的认可，这样才会对需求的变更有成本的概念，能够慎重地对待需求的变更。

3）小的需求变更也要经过正规的需求管理流程，否则会积少成多。在实践中，人们往往不愿意为小的需求变更去执行正规的需求管理过程，认为降低了开发效率，浪费了时间。正式由于这种观念才使需求的渐变不可控，最终导致项目的失败。

4）精确的需求与范围定义并不会阻止需求的变更。并非对需求定义的越细，越能避免需求的渐变，这是两个不同层面的问题。太细的需求定义对需求渐变没有任何效果。因为需求的变化是永恒的，并非由于需求写细了，它就不会变化了。

需求复用：需求获取是一个需要高度合作的活动，而并不是用户所说的需求的简单拷贝。作为一个分析者，必须透过用户所提出的表面需求理解他们的真正需求。询问一个可扩充的问题有助于你更好地理解用户目前的业务过程并且知道新系统如何帮助或改进他们的工作。需求获取要充分利用所有可用的信息来源以提高效率，这些信息描述了问题域或在系统解决方案中许多合理的特性。典型的问题是分析人员往往受其业务背景的局限并不重视领域专家的意见，尤其是对业已形成的需求文档没有很好的复用。基于此，必须对需求进行管理，使需求能够真正成为需求工程和管理的基线，使开发计划、活动和工作产品同系统需求保持一致，使需求可以复用。所以需求管理一个很重要的目标就是提高需求的复用率。

3 结 语

需求管理恰如裁缝的量体裁衣,它直接关系到最终产品的成型。如果一个产品满足了客户需求,那它无疑就是成功的。需求管理的过程,从需求定义开始贯穿整个开发项目始终,力图实现最终产品同需求性的最佳结合。需求获取的管理同项目管理是密不可分的,通过对需求管理在项目进程中实施的不同任务进行分析,我们不难看出需求管理所起的作用。因为对需求定义的任何改进,设计上都必须大量的返工。无序的,没有经过精心策划的需求管理是不可能产生效益的。如果我们把每一个需求的解决看作一个里程碑,并以此出发对整个开发进程进行监控,就应该对整体开发工作进行精密细致的划分,从而将需求分析具体化。从这层意义上来说,需求获取的管理是保证系统产品质量的基础。