论信息系统的安全体系

摘要：

2005 年 2 月，我参加了某水库管理信息系统项目的实施。通过系统的实施和运行，实现防汛、供水、发电、闸门监控、水文等各种数据的采集、分析、存储，并通过网络及时地向有关部门汇报，以便相关领导进行调度指挥，为领导决策提供大力支持，为业务人员办公提供服务。系统的应用将有效提高某市政府水库管理所的工作效率。

我作为该项目的项目负责人，主要负责项目管理，同时负责项目的需求分析、系统集成、系统测试和系统验收的工作，并负责系统投用后的运行维护。为了确保项目顺利的实施和安全的投入运行，我从软件、硬件、运行环境、用户四个角度对系统的脆弱性进行了分析，从实体安全、操作系统平台的安全、数据安全、访问控制的安全性、管理制度的安全保护五个方面对水库管理信息系统的安全体系进行了分析，最后探讨了安全体系设计中的方法和原则，参照现行信息系统安全架构体系，分析了本系统中安全体系的不足之处。

正文：

2005 年 2 月，我参加了某水库管理信息系统项目的实施。以某市政府某水库管理所为核心建立中心管理局域网，通过水库管理信息系统全面地进行雨水情等信息的收集、输入、修改、查询，并实时动态显示有关信息，通过人机交互进行洪水预报、水库安全运行分析、调度方案制订、调度方案评价与优选、调度成果管理、防洪、发电、灌溉工程信息管理、调度控制、系统管理等。根据实时和定期水、雨、工情准确分析防洪、水库安全及兴利形势，形成调度预案，供各级调度指挥人员参考，并通过专家经验加以修正，最终形成调度方案，供水库管理机构决策，供执行人员实施。上级主管部门可通过 internet 实现与水库管理所的信息共享和信息传输，其他单位（在授权许可下）以同样的方式实现对水库管理所的信息访问。系统的应用将有效提高水库管理所的工作效率。我作为该项目的项目负责人，主要负责项目管理，同时负责项目的需求分析、系统集成、系统测试和系统验收的工作，并负责系统投用后的运行维护。

系统采用 C/S 和 B/S 混合架构，其中 C/S 部分实现各部门管理功能子系统，以数据采

集和数据处理为主；B/S 部分则实现存在交叉业务的部门管理子系统、部分共享数据的网上发布和数据的网上查询、浏览。所有的数据都存放在后台的 Oracle 数据库服务器上进行统一管理和维护。

水库管理信息系统采集和处理数据的过程均在局域网内，内部用户可以查询中间结果和发布审核过的信息，经过授权的外部用户只能通过 internet 查询已经发布的信息。所以本系统是一个相对独立的、封闭的专用信息系统，绝大多数的恶意攻击是来自内部的，水库管理的工作性质决定了本系统信息的机密性显得尤其重要，因此，除了防止来自 internet 外部的攻击外，如何制定内部安全防范体系的问题也必须解决。

信息安全是指防止信息被故意的或偶然的非法授权泄露、更改、破坏或使信息被非法辨识、控制。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别等七个方面。如果采集的水库管理数据不正确，或者在上传和发布的过程中被篡改、破坏，将影响到防汛、供水、发电等多项决策，信息安全工作做不好，信息系统将无法正常实施和应用。如果系统分析时不充分考虑信息安全因素，将为系统将来的运行留下隐患。

一个完整的安全体系包含的内容有：风险管理；行为管理；信息管理；安全边界；系统安全；身份认证与授权；应用安全；数据库安全；链路安全；桌面系统安全；病毒防治；灾难恢复与备份；集中安全管理等。作为一个政府部门的信息系统，水库管理信息系统应建立一个以内部控制机制为核心的安全防护体系，以降低其带来的风险。从系统的开发到运行和完善，在各个不同阶段，都应把安全问题作为重中之重，并贯穿于整个过程之中。要确保水库管理信息系统的安全可靠，离不开信息安全技术的应用，我对系统的脆弱性和安全体系进行了如下分析。

一、系统的脆弱性分析

水库管理信息系统是一个包括计算机软硬件、通信设施并与监控设施和组织高度集成的人机系统，不可避免面临着来自各方面的潜在威胁。软件、硬件、运行环境、用户各方面都可以形成系统的脆弱性。

软件方面：水库管理信息系统软件的开发人员的专业背景、业务能力、对水库管理信息系统的理解深度等都会对系统开发的成败产生重大的影响，系统开发过程主要以手工为主，没有成熟的软件产品，是造成水库信息软件缺乏可靠性和安全性的重要因素。

硬件方面：除了计算机设备和网络设备，系统用到的水位探测仪、监控设备、数据采集设备，均由大量的电子元件和芯片组成，而芯片和电子元件的老化和一些安插件之间的接触不良都会造成系统的失灵，系统的采样点和监控点分布在野外，受自然环境的影响很大。

运行环境方面：水库管理信息系统中使用传感器技术和数据采集技术，将野外遥测站点的数据传到 10 多个数据接收工作站，数据经过处理后再进入调度室，要经过多个部门和多个环节。即便环境能完全达到信息系统的安全技术要求，但因整个系统分散在各个部门，也就很难避免因为环境因素而导致意外事件的发生。

用户方面：系统的用户数量多，层次也多，能否充分发挥信息系统的作用，并能安全正常的运行系统，这与使用人员对计算机的基本知识了解程度、在系统开发过程中与开发人员配合程度、投入使用后是否按规章操作、对系统运行所需的数据收集是否及时和充分，是否有假的、错误的数据采集输入都密切相关。系统在为水库管理所的上级和各部门提供数据共享时，也可能为入侵者、信息偷窥者提供了方便之门。

二、系统的安全体系分析

设计安全体系时要根据实际情况，综合考虑各种因素。

实体安全方面：水库所处的地理位置在夏季会受到雷电灾害的影响，在野外的雨水情遥测设备，如摄像头、云台、信号采集器必须有防雷设施，办公楼内外的网络设备（交换机、HUB 等）也要有防雷功能，对信息系统实体的破坏，不仅可以造成巨大的经济损失，也会导致系统中的机密信息数据丢失和破坏

操作系统平台的安全方面：作为水库管理信息系统的支撑部分，操作系统安全的内容包括保密性、可靠性和抗干扰性等几方面内容。在选择操作系统时，既要考虑操作系统的实用性与可靠性，又要考虑到操作系统的安全性。操作系统还应该安装防火墙及病毒查杀程序，以提高整个信息系统的可靠性与安全性。

数据安全方面：水库管理信息系统的数据安全性，除了一般由存和取的控制来保证外，还要加强对数据库的管理和对数据采取必要的加密等手段，以防止信息泄漏。

访问控制的安全性方面：通过对用户进行系统功能授权，即系统每一功能，只有被授权的用户才能使用，未被授权的用户无法使用。系统中的每一个用户在完成其工作时，只应拥有最小的必要的系统功能，使出错或蓄意破坏造成的危害的概率降到最低。水库信息

系统的功能只对授权用户是可视的，对非授权用户是不可视的，这样可预防蓄意破坏的发生。

管理制度的安全保护方面：在开发人员和使用人员中建立完善的安全制度，并使其充分认识计算机系统安全的重要性，自觉执行安全制度，从而形成对水库管理信息系统的一个管理保护层。

水库管理信息系统安全体系的分析应贯穿系统的开发、实施、运行各个阶段。作为一个政府部门的信息系统，安全性永远是第一位的。水库管理信息系统在 2006 年 3 月正式投入使用后，安全平稳的运行了 1 年多，在政府部门的水库管理工作发挥着作用，这与安全体系设计时充分的分析是分不开的。安全体系的质量直接决定着安全工程的质量，我们在安全体系设计之后，聘请了第三方专家对体系的质量进行评审，对评审结果进行论证，对发现的不妥之处及时修正，做好安全体系的评估工作，保证安全体系的质量，从而保证信息系统开发和运行的各阶段的质量。

安全体系的设计和实施要有一定的灵活性、适应性，还要遵循风险和成本的平衡性，安全体系服务于信息系统的应用，当安全体系的代价大于信息系统应用的价值时，就不再具有可行性。安全体系的分析要具有前瞻性，在系统分析时就要考虑系统运行、维护时的各种安全因素，如果系统投用后才发现安全体系不能保障系统的正常运行，会造成维护成本的剧增甚至信息系统的失败。在系统建设之初就考虑系统安全对策，比等系统建设好后再考虑，不但容易，而且花费也少得多。

现行信息系统安全架构体系以信息安全程度从低到高可分为：MIS+S；S-MIS；S2-MIS。水库管理信息系统的安全体系属于 MIS+S，是一个低级的信息安全保障系统，没有对水库信息系统作任何改变，为防止自然灾害、病毒、黑客等增加一些安全措施和安全防范设备，提高了水库信息系统的安全强度，基本满足了安全需要，实施成本较低，但并没有从根本上解决信息系统的安全问题，这也是目前受安全成本和应用效益约束的实际情况，当以后水库信息系统二期工程开展时，我们会考虑往较高层次的安全体系上发展。