国家防汛抗旱指挥系统安全体系建设方案

周维续　常志华　詹全忠　（水利部水利信息中心　100053）

摘要：国家防汛抗旱指挥系统作为一个大型的信息系统，其安全体系的建设是一项非常重要的内容。本文从系统和应用出发，分析存在的安全风险，提出包含安全管理体系、安全技术体系和安全咨询体系三方面内容的国家防汛抗旱指挥系统安全体系建设方案。

关键词：国家防汛抗旱指挥系统　安全　体系

1　引言

国家防汛抗旱指挥系统作为一个大型的信息系统，其安全体系的建设是一项非常重要的内容。从水利系统的信息化建设现状看，各单位已经进行了不同程度的网络安全系统的建设工作，主要采用防火墙、防病毒等安全控制机制，但是并没有形成统一的安全体系。因此，需要对整个防汛抗旱指挥系统工程进行全面的安全规划和建设工作。

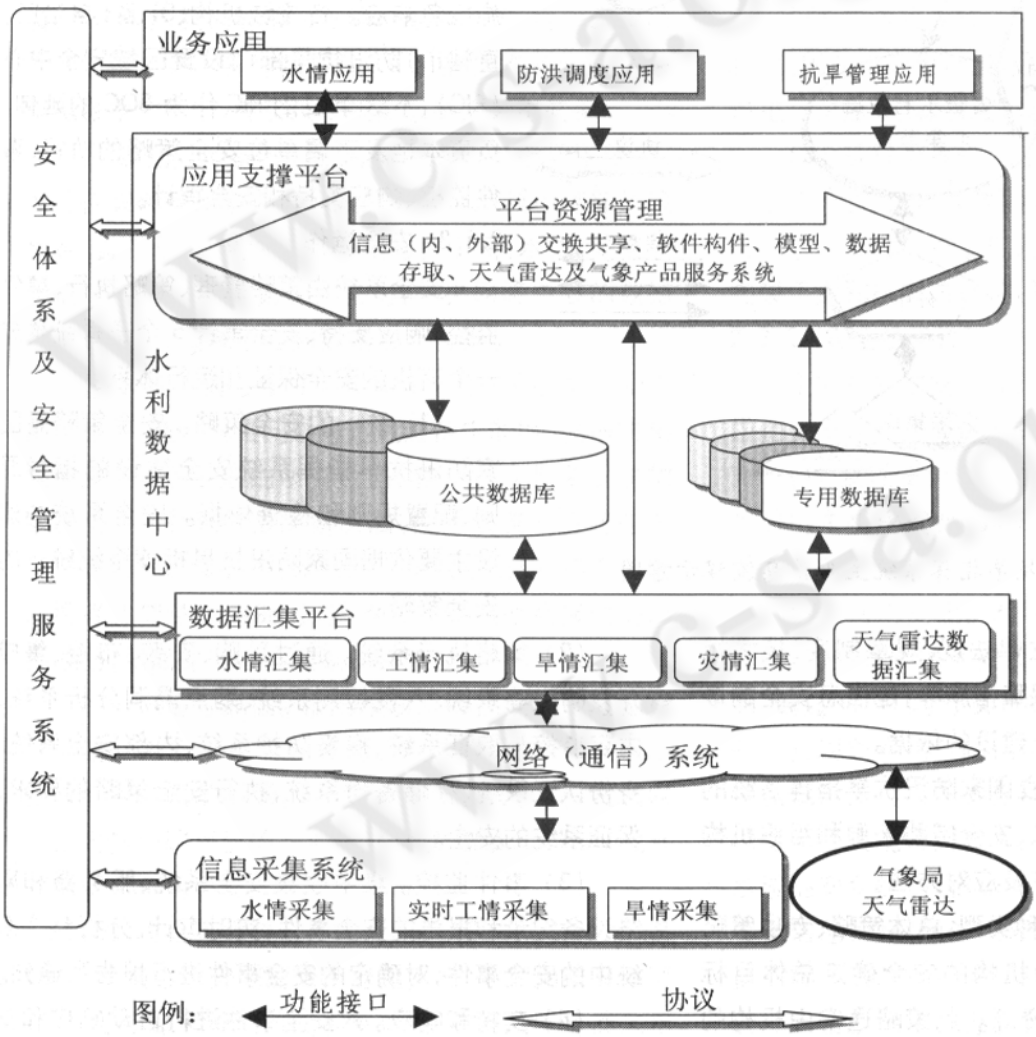

图 1　国家防汛抗旱指挥系统体系结构示意图

国家防汛抗旱指挥系统工程建设以水利数据中心为核心，以满足国家防汛抗旱指挥系统需求为主线，以构造水利信息化综合体系为基本目标，以全面提高防汛抗旱业务的效率和效能为根本宗旨，通过设计与实现各类功能构件，定义相关协议与接口，形成可持续改进的系统。系统由信息采集系统、网络（通信）系统、数据汇集平台、数据库、应用支撑平台、应用系统和安全体系及安全管理服务系统等组成。各个部分间由标准化的协议与接口结合为一个有机的整体。系统体系结构如图 1 所示，系统主要信息流程如图 2 所示。

2　安全体系建设

安全不仅仅是一个技术问题，完整的安全体系，应包括安全管理体系、安全技术体系。

2.1 安全管理体系

2.1.1 安全策略

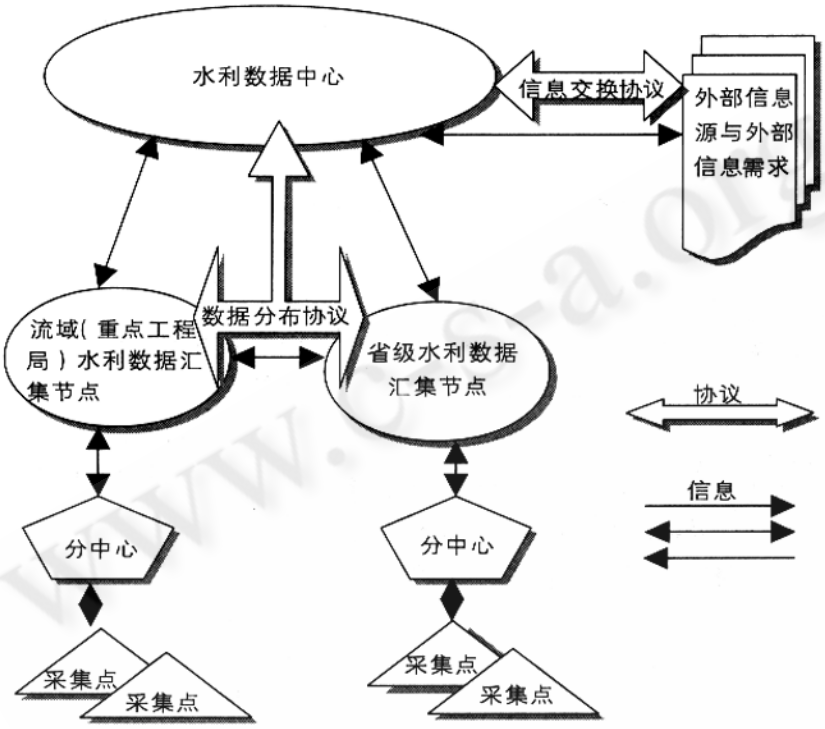

图 2　国家防汛抗旱指挥系统主要信息流程示意图

安全策略包括各种法律法规、规章制度、技术标准、管理规范和其它安全保障措施等，是信息安全的最核心问题，是整个信息安全建设的依据。

安全策略用于帮助建立国家防汛抗旱指挥系统的安全规则，即根据安全需求、安全威胁来源和组织机构来定义安全对象、安全状态及应对方法。

安全策略通常分为三种类型：总体策略、专项策略和系统策略。总体策略为机构的安全确定总体目标（方向），并为其实现分配资源。此策略通常由机构的高级管理人员（如 CIO）制订，用来规定机构的安全流程和管理执行机构；专项策略通常针对一项业务（服务）制订，它规定当前信息安全特定方面的目标、适用条件、角色、负责人以及策略的一致性要求。如针对电子邮件系统、因特网浏览等制订的安全策略；系统策略是针对某个具体的系统（包含涉及的硬件、软件、人员等）制订的安全策略，它主要包含：安全对象、不同安全对象的安全规则、实现的技术手段。

安全策略目前主要作为规定、指南，通过文件方式在全系统范围内发布。

2.1.2 安全组织

全系统使用一个安全运行中心（SOC），作为中央网络中心的组成部分。SOC 为全网范围提供策略制订和管理、事件监控、响应支持等后台运行服务。同时，通过 SOC 对全系统的安全部件进行集中配置和管理，处理安全事件，对安全事件实施应急响应。各流域机构、31 省（自治区、直辖市）防汛抗旱部门设置区域安全中心（RIC），下级单位的 RIC 作为 SOC 的延伸，负责本地及下属单位安全策略的执行、事件监控、响应支持和安全审计。

2.1.3 安全运作

安全系统由策略管理、策略执行、事件监控、响应支持、安全审计 5 个子系统构成一个有机的安全保证和运行体系。

（1）统一的安全策略。安全策略是国家防汛抗旱指挥系统安全建设的指导原则、配置规则和检查依据。安全系统的建设主要依据国家防汛抗旱指挥系统统一的安全策略。

（2）策略执行系统。通过采购、安装、布控、集成开发防火墙系统、入侵检测系统、弱点漏洞分析系统、内容监控与取证系统、病毒防护系统、内部安全系统、身份认证系统、存储备份系统，执行安全策略的要求，保证系统的安全。

（3）事件监控。集中收集安全系统、服务器和网络设备纪录和报告的安全事件，实时审计、分析整个系统中的安全事件，对确定的安全事件进行报告和通知。

（4）支持和响应。对安全事件进行自动响应和支持处理。包含事件通知、事件处理过程管理、事件历史管理等。

（5）安全审计。对整个系统的安全漏洞进行定期分析报告和修补；定期检查审计安全日志；对关键的服务器系统和数据进行的完整性检查。

2.2 安全技术体系

安全防护主要包括可靠性和安全性两方面内容。根据前面的安全风险分析可靠性主要通过数据、线路、路由、设备的冗余，软件可靠性设计，雷电防护和断电保护措施来保证；安全性主要从物理安全、网络安全、系统安全、应用安全几个方面考虑。

2.2.1 可靠性设计

为了保证系统的可靠运行，主要考虑数据、信道、路由、设备、防雷、接地和电源等因素，具体如下。

(1) 数据可靠性。主要包括数据本地备份、数据异地容灾和数据传输的可靠性三个方面。

① 数据本地备份。为了保证所有中央报汛站雨量、水位观测数据能够被正确自动地重传，需要配置固态存储器。针对各种数据库，采用数据库备份软件来实现数据的备份，并实现长历史数据的导出转储。

② 数据异地备份。在国家防汛抗旱指挥系统中，数据存储架构为集中与分散的架构。从数据存储的架构看，省中心、流域中心的数据与各工情、水情、旱情试验站(分中心)的数据互为备份，中央网络中心的数据又与省中心、流域中心的数据互为备份。

③ 数据传输可靠性。采集系统发送方在数据发送的过程中，遇有网络问题等造成通信中断时，发送方要保留没有正确发送的所有数据(整个本次需要发送的数据文件)，待系统故障解决后，由系统自动再将整个文件重新发往接收方；接收方在接收过程中，遇有网络问题等造成通信中断时，接收方要删除已经接收的部分数据，从而保证接收数据的完整性。

(2) 信道可靠性。报汛通信网络在设计中应坚持双信道互为备份并实现自动切换的设计方案，确保水情等信息传输的畅通。骨干网、流域省区网和城域网采用电信公网提供的 SDH 信道为主信道，以 ISDN 或其它信道为备用信道。

(3) 设备可靠性。在中央、流域和省(自治区、直辖市)网络中心分别配置两台路由器，主路由器具有双电源、双引擎和模块热插拔等功能；重要的服务器采用双机系统，并采用磁盘阵列增加可靠性；中央网络中心的防火墙、入侵检测、认证服务器均为冗余配置。

(4) 路由可靠性。在骨干网、流域省区网和城域网中主线路均采用 OSPF 动态路由，备份线路采用静态路由。

(5) 雷电防护。雷电防护主要考虑分中心和水情报汛通信的防雷。在交流电线上安装泄放电流大、响应速度快的避雷器，水情报汛通信的传感器信号线、电话线、电源线和其他各类连线都应进行屏蔽，并给出抗雷电的措施。

(6) 接地。各类站点的接地电阻应达到指标：

网络中心：<1Ω

分中心：<5Ω

报汛站：<10Ω

如接地电阻难以达到要求，对野外站可视情况稍加放宽，对分中心和重要测站可在屋顶安装闭合均压带，室内安装闭合环行接地母线等措施改进防雷性能。

(7) 电源可靠性。目前各地电源系统均采用双路供电，因此电源设计应考虑电源电压范围、直流电池防过电和欠压、电源管理等。各级机房配置 UPS 电源。

(8) 软件可靠性。应用软件能检测信道和测站设备的工作状态，发现故障时自动切换到备用信道上。

(9) 其他方面。应注意各种设备的接口保护、抗电磁干扰和抗雷击保护，并注意电源电压的适应性。

2.2.2 安全性设计

主要从物理安全、网络安全、系统安全、数据安全、应用安全几个方面进行安全设计。

(1) 物理安全。主要考虑放置路由器、服务器和交换机的主机房安全，其安全按照有关国家标准进行建设。

(2) 网络安全。网络安全设计实现基本安全的原则，通过在网络上安装防火墙实现用户网络访问控制；通过 VLAN 划分实现网段隔离；通过 AAA 认证服务器实现拨号用户的认证授权；通过网络入侵监测系统实现对黑客攻击的主动防范和及时报警；通过漏洞扫描系统实现及时发现系统新的漏洞、及时分析评估系统的安全状态，根据评估结果及时调整系统的整体安全防范策略；通过安全审计和日志管理系统，对重要的网上活动进行监视和记录，这样一旦系统瘫痪或者被入侵就能够进行侦破和取证，并能够发现安全防范系统的不足，加以改进；通过防病毒系统实现病毒防范，综合以上多种安全手段，实现对网络系统的安全管理。

(3) 系统安全。系统安全包括主机系统安全、数据库系统安全、中间件系统安全。系统的安全是利用

安全手段防止系统本身被破坏,防止非法用户对计算机资源及信息资源的窃取。结合国家防汛抗旱指挥系统的应用现状,系统的安全保障措施,包含如下要求:

① 主机系统安全增强配置:对各类主机系统采用配置修改、系统裁剪、服务监管、完整性检测、打 Patch 等手段来增强主机系统的安全性;

② 主机系统定制:对 Web 服务器、DNS 服务器、Email 服务器、Ftp 服务器、数据库服务器、应用服务器等主机系统根据各自的应用特点采用参数修改、应用加固、访问控制、功能定制等手段来增强系统的安全性;

③ 数据库系统安全增强配置:数据库系统的补丁、账号管理、口令强度和有效期检查、远程登陆和远程服务、存储过程、审核层次、备份过程、角色和权限审核、并发事件资源限制、访问时间限制、审核跟踪、特洛依木马等。

(4) 数据安全。各种数据的安全保障措施如下:

① 工情、灾情信息等信息在传输过程中采用加密方式传输,数据汇集平台接收到数据后进行解密、处理并入库;

② 通过构造运行于不同地域层次的水雨情、工情、旱情、灾情和天气雷达数据汇集设施与软件,实现数据入库前的分类综合、格式转换等,并构造支持数据分布与传输的管理系统,保障系统信息分散冗余存储规则的实现及数据的一致性。

(5) 应用安全。应用系统的安全访问主要是保证正确的用户使用正确的资源,这包含认证和授权两方面内容。认证系统控制每个用户是否是合法用户,授权系统控制某个用户对某个应用系统资源的访问权限,其基础是对用户的管理和对资源目录的管理与授权。另外还需审计系统,记录用户的访问操作。

① 认证系统。目前,对于广域范围的安全认证应用较多较成熟的系统是 CA 认证系统。认证系统的目标在于建设一个功能完善、技术先进、安全可靠、服务领先的基于公开密钥基础架构的 CA 中心。数字证书认证系统由一个独立的密钥管理系统(KM 中心)和一个具有可扩充性的证书认证系统(CA 中心)构成:根 CA、一级 CA、二级 CA、注册审核中心(RA)。

在中央网络中心设置根 CA,为 CA 系统生成根证书密钥对,并为一级 CA 服务器的证书签名,考虑安全性,根 CA 设计为离线方式。在中央网络中心设置一级 CA,主要为部机关用户签发数字证书,为二级 CA 签发根证书,当有跨地域访问行为发生时,CA 证书要进行交叉认证,由各二级 CA 反馈到一级 CA,由一级 CA 进行验证。在各流域机构和省(区、市)水利(务)部门设置二级 CA,主要为流域机构和省(区、市)水利(务)部门的证书用户签发数字证书。在水利部机关和各流域机构和省(区、市)水利(务)部门设置 RA,主要负责为用户生成证书申请、对用户的证书申请进行真实性审核等。

② 授权管理系统。在数字认证 PKI 系统的基础上使用 PMI 系统,利用 PMI 系统及身份管理功能,根据水利系统不同业务范围,进行业务权限分组、分级,在自己的职权范围内进行工作,同时通过系统的不可抵赖性,可对相关人员进行工作业绩考核,尤其对有关国家安全责任的认定具有明确的指导作用。

2.2.3 安全咨询体系

安全工作涉及内容非常广泛而且专业,国家防汛抗旱指挥系统需要建立安全咨询体系,以获得权威安全机构、安全专家、第三方安全厂商的技术支持,起到事半功倍的效果。安全咨询包括风险评估、安全顾问和紧急响应等内容。

3 结束语

国家防汛抗旱指挥系统目前处于安全体系建设的起步阶段,需要确立符合水利系统业务特点和网络状况、并且具有充分的前瞻性和可行性,以保证体系建设的可扩展性、可持续性以及投资的有效性和最终目标的达成。在国家防汛抗旱指挥系统中,从建设进度、经费和性能多个因素考虑,安全体系应分期实施。

参考文献

1 水利部水利信息中心, 国家防汛抗旱指挥系统一期工程初步设计,2004。

2 张晓伟、金涛, 信息安全策略与机制, 机械工业出版社,2004-04-01。

3 宁雨鹏、陈昕, PKI 技术, 机械工业出版社,2004-04-01。

4 牛云、徐庆、辛阳, 机械工业出版社,2004-06-01。