发电企业计算机网络信息安全与防护浅谈

董 珊
（徐州华润电力有限公司，江苏 徐州 221000）

摘 要：发电企业计算机网络信息安全问题已威胁电力系统安全、稳定、可靠、优质地运行。通过对发电企业计算机网络系统信息安全危险分析，根据发电企业的特点提出了相应的风险防范措施。

关键词：计算机网络；风险分析；安全体系机构；信息安全；安全防护
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1674-7720(2011)12-0001-02

Brief talk of the security and defense of network information in power-generating enterprise

Dong Shan
(China Resources Power Co., Ltd., Xuzhou 221000, China)

Abstract: The network information security has becomes an essential issue for the power enterprises that threatens the secure, stable, reliable and smooth operation of their power systems. Therefore, to guarantee the security and reliability of information transmission is the important aspect of recent information-based work. This thesis is going to analyze threatens of network information security of power enterprises, and in related to their characters, propose some measures to deal with them.

Key words: computer networks; risk analysis; structure of security system; information security; security defense

随着信息化不断扩展，各类网络版应用软件得到推广应用。计算机网络在提高数据传输效率、实现数据集中、数据共享等方面发挥着越来越重要的作用，计算机网络与信息系统建设已逐步成为各项工作的重要基础设施。但病毒传播、黑客入侵、恶意软件肆虐，时刻威胁着计算机网络信息，并造成严重危害。新版《火力发电厂安全性评价》加入了网络信息安全评价标准，安评工作中计算机网络和系统安全建设尤为重要。

1 发电企业网络系统简介

1.1 总体结构图

图 1 是发电厂信息系统的结构示意图。

发电厂信息系统由厂控二次系统、管理信息系统及相关的网络和网络接口构成。根据发电厂信息系统的组成，厂控二次系统中包括电量计量、DCS、输煤除灰、化学制水、远动、脱硫等多个业务系统及其网络。各厂控二次业务系统通过独立的接口机连接到管理信息系统的实时数据库服务器端，向管理信息系统提供实时业务的数据，供发电厂各相关管理

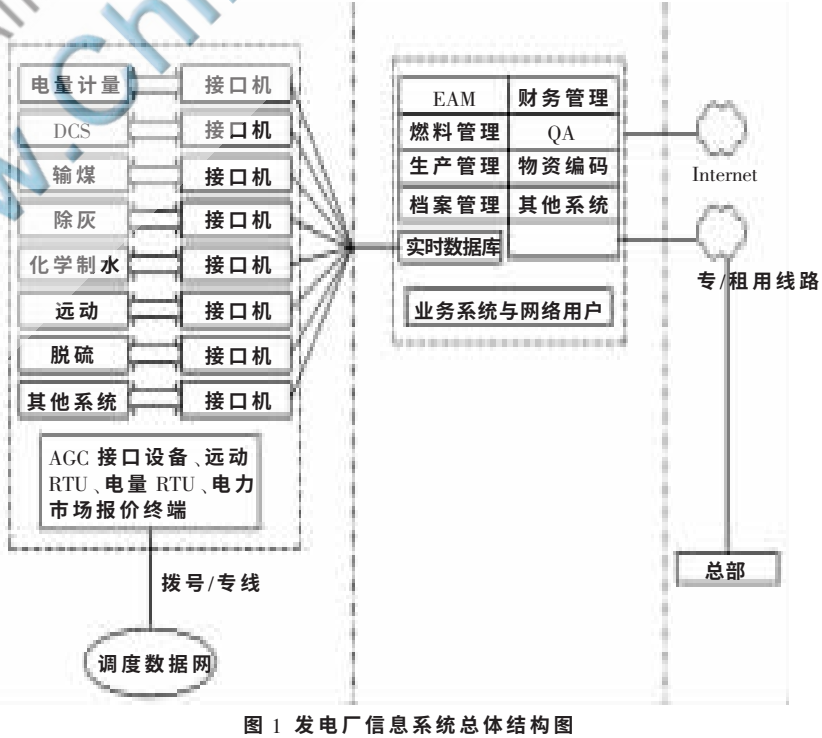

图 1 发电厂信息系统总体结构图

部门使用。

管理信息系统包括了EAM、财务管理、OA、燃料管理、生产管理、实时数据库等多个系统和系统用户，还有相关的网络与网络接口。其中，实时数据库系统服务器接收厂控端接口机采集的实时数据，并将数据提供给管理信息系统中的其他业务系统。

1.2 应用系统

1.2.1 EAM(设备管理系统)

EAM系统主要提供对电厂设备的编码管理、电厂设备维护工作流程的管理、电厂生产过程中的运行值班情况的管理及电厂的备品备件的管理功能。

EAM系统中数据主要包括用户信息/权限、设备数据、维修管理数据、运行管理数据、备件数据等。因用户信息/权限的机密性要求高，所以EAM系统数据的完整性和可用性要求都为高。

1.2.2 实时数据库系统

实时数据库系统服务器负责通过多个和厂控系统相连的接口机收集与厂控系统相关的实时数据。接口机分布与各厂控系统现场连接，其中的实时数据来自于DCS系统、远动系统、电量采集系统、输煤除灰系统等。

实时数据库系统存在与厂控系统、管理信息网络其他业务系统的通信关系。授权用户对实时数据库服务器的访问，采用用户名/密码的认证方式，访问控制通过防火墙控制。

1.3 安全分区

根据《电力二次系统安全防护规定》的安全分区原则，对发电厂信息系统进行分区，按照AGC接口设备、远动RTU、电量计量RTU和电力市场报价终端与管理信息系统通信方式的不同，划分成两个分区：生产控制大区(安全区Ⅰ和安全区Ⅱ)和管理信息大区。实时数据系统各组件分布于安全区Ⅰ、Ⅱ和管理信息大区中，根据实时数据系统的结构，将实时数据系统分为两部分：

(1) 安全区Ⅰ、Ⅱ的接口机：用于采集来自安全区Ⅰ和安全区Ⅱ的实时系统数据，同时将这些实时数据单向传给管理信息大区的实时服务器。

(2) 管理信息大区的实时数据库服务器：从安全区Ⅰ、Ⅱ的接口机获取数据，并与管理信息区的其他业务系统间进行数据交互。

2 网络安全体系机构

电力企业信息安全体系机构由网络安全防护、数据备份和恢复、应用系统安全、信息安全管理等几部分组成[1-2]。

2.1 网络安全防护

2.1.1 安全域防护

管理信息系统划分为服务器集群、终端用户、对外应用服务器三个网络安全域，将终端用户安全域划分成多个子安全域，包括财务系统、管理人员、生产部门、一般用户等多个安全域；将对外提供服务的应用服务器部署在对外应用服务器域中。

2.1.2 网络的高可靠性

(1) 核心层网络设备应采取双冗余结构，两台核心层设备相互热备；

(2) 关键终端用户安全域接入交换设备到核心层应采用双链路冗余结构，确保用户接入核心层链路的冗余和可靠；

(3) 对关键业务系统服务器域和重要业务系统服务器域通过两条链路接入核心层；

2.1.3 防病毒

(1) 发电厂管理信息大区应统一部署病毒防护措施，禁止安全区Ⅰ、Ⅱ与管理信息系统共用一个防病毒管理服务器。

(2) 对所有系统的服务器、用户工作站都应当部署适当的防病毒产品的客户端。

(3) 在与Internet的网络接口处应当部署防病毒网关，防止病毒、蠕虫从Internet蔓延到发电厂管理信息系统内部。

(4) 在布置独立的电子邮件系统时，必须在邮件服务器前端部署邮件病毒网关，防止邮件病毒在办公网络中蔓延。

(5) 加强防病毒管理，保证病毒特征码的及时、全面更新，及时查看病毒查杀记录，掌握病毒威胁情况。

2.1.4 防火墙

在到Internet的每个网络接口处都必须部署一台防火墙；对外应用的服务器安全域应连接到防火墙停火区(DMZ)，选用硬件防火墙，其功能、性能、电磁兼容性必须经过相关测试。防火墙应支持DMZ功能，发电厂对外部公开的系统(如Web系统、邮件系统)需放置在DMZ区。

2.1.5 入侵检测系统

发电厂管理信息系统中应部署一套入侵检测系统，至少应在核心层网络设备上部署一个入侵检测系统的探头。

2.1.6 虚拟专用网

发电厂厂控自动化系统与调度中心的通信，应满足《电力二次系统安全防护规定》中提出的实时和非实时VPN建设的要求。穿越公用线路与发电厂管理信息系统进行业务通信、远程办公时，应采用VPN产品，以保障数据通信的安全性。

2.1.7 主机安全加固

关键应用系统(如财务系统、EAM系统、实时数据库系统等)的主服务器应定期进行主机安全加固。主机安全加固方式包括：安全配置、安全补丁、采用专用的软件强化操作系统访问控制能力以及配置安全的应用。

2.2 备份与恢复

对于关键业务系统(财务系统、EAM、实时数据库系统)数据，安排专人负责数据的备份，确保对业务数据每月进行一次全备。关键业务系统需双机备份，安排专人对

备份介质进行保管,备份介质必须与原数据异地存储。

2.3 应用系统安全

管理信息大区中应用系统较多,确保应用的安全性是管理信息系统信息安全建设的重点内容。包括:访问控制、账户与权限管理、审计管理、输入/输出完整性、加密管理、系统生命周期安全管理、数据完整性等。

2.4 信息安全管理

信息安全管理工作包含 3 个方面:

(1) 建立专门的组织机构负责信息安全工作的管理;

(2) 建立专门的策略体系和管理制度体系约束人员行为;

(3) 建立专门的人员队伍进行具体的管理操作。

网络信息安全是一个系统工程,不能仅靠杀毒软件、防火墙、漏洞扫描等硬件设备的防护,还要意识到计算机网络系统是一个人机系统,在建立以计算机网络安全硬件产品为基础的网络安全系统的同时,也应树立用户的网络信息安全意识才能防微杜渐,构建一个高效、安全的网络系统。

参考文献

[1] 张世永.网络安全原理与应用[M].北京:科学出版社,2003.

[2] 葛秀慧.计算机网络安全管理(第二版)[M].北京:清华大学出版社,2008.

(收稿日期:2011-04-25)

作者简介

董珊,女,1975 年生,高级程序员,工程师,主要研究方向:发电行业信息化建设和管理。