ICS 13.320
A 91
备案号:25472—2009

AQ

中华人民共和国安全生产行业标准

AQ 9003.2—2008

企业安全生产网络化监测系统技术规范 第2部分:危险场所网络化监测系统集成技术规范

Technical specifications for production safety monitoring systems based on network—Part 2: Technical specifications for integration of monitoring system based on network in hazardous area

2008-11-19 发布　　2009-01-01 实施

国家安全生产监督管理总局　发布

目　次

前　言

AQ 9003—2008《企业安全生产网络化监测系统技术规范》分为三个部分：

——第1部分：危险场所网络化监测系统现场接入技术规范；

——第2部分：危险场所网络化监测系统集成技术规范；

——第3部分：危险场所网络化监测设备通用检测检验技术规范。

本部分为AQ 9003.2—2008的第2部分。

本标准由国家安全生产监督管理总局提出。

本标准由全国安全生产标准化技术委员会归口。

本标准负责起草单位：北京市安全生产监督管理局、北京首科集团公司。

本标准参加起草单位：北京亚思顿科技发展有限公司、南开大学、北京邮电大学、北京航空航天大学、北京交通大学、研华科技股份有限公司、上海横河国际贸易有限公司、北京安控自动化股份有限公司、北京阿尔泰科技发展有限公司。

本标准主要起草人：胡燕祝、张树森、汪卫国、杨春雪、李文洁、高云飞、朱军、吕宏义、常石磊、王仰东、张红光、高宁、吕英华、张洪欣、邢维巍、刘学东、周斌、彭国红、施洪生、马小龙。

引　言

中华人民共和国国家安全生产监督管理总局为规范危险场所网络化监测系统集成技术(参见本标准第2部分1章确定的适用范围),配合危险场所网络化监测系统的构建或评估,提高危险场所联网监管水平,实现系统资源共享,特制定本标准。

企业安全生产网络化监测系统技术规范 第2部分：危险场所网络化监测系统集成技术规范

1 范围

本规范规定了危险场所网络化监测系统传输网络的基本要求，以及系统集成的软硬件、供电、施工、验收等要求，是构建或评估危险场所网络化监测系统的基本依据。

本规范适用于危险场所网络化监测系统的设计、施工、验收和维护。

危险场所网络化监测系统集成除应按本规范执行外，还应符合国家现行的有关强制性标准的规定。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡标注日期的引用文件，其所有标注日期之外的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 2887—2000 电子计算机场地通用规范

GB 7260 不间断电源设备

GB/T 15278—1994 信息处理 数据加密 物理层互操作性要求

GB/T 20010—2005 信息安全技术 包过滤防火墙评估准则

GB/T 20011—2005 信息安全技术 路由器安全评估准则

GB 50254—1996 电气装置安装工程低压电器施工及验收规范

GB/T 50311—2000 建筑与建筑群综合布线系统工程设计规范

YD/T 1132—2001 防火墙设备技术要求

CECS 81：96 工业计算机监控系统抗干扰技术规范

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本规范的各部分。

3.1

服务器 server

指在网络管理系统中完成各种数据存储、数据管理、危险场所监测业务管理、网页发布等功能的核心计算机或计算机系统。

3.2

交换机 switch

一种工作在OSI第二层（数据链路层）上的、基于MAC（网卡的介质访问控制地址）识别、能完成封装转发数据包功能的网络设备。

3.3

路由器 router

一种工作在OSI参考模型第三层（网络层）上的数据包转发设备，可以支持多种协议（如TCP/IP、IPX/SPX、AppleTalk等协议）。通过路由器转发数据包来实现网络互连。

3.4

防火墙 firewall

在网络之间执行访问控制策略的一个或一组设备。

注：参见 YD/T 1132—2001《防火墙设备技术要求》

3.5

缩略语

下列缩略语适用于本标准。

IPX 网间数据包交换协议（Internetwork Packet Exchange Protocol）

SPX 顺序包交换协议（Sequences Packet Exchange）

OSI 开放式系统互联参考模型（Open System Interconnect）

GSM 环球移动通讯系统（Global System for Mobile Communications）

CDMA 码分多址技术（Code-Division Multiple Access）

ODBC 开放数据库互连（Open Database Connectivity）

VPN 虚拟专用网络（Virtual Private Network）

ADO ActiveX 数据对象（ActiveX Data Objects）

4 系统构成

4.1 监测系统结构图

以三层网络结构为例，结构图如图 1 所示。

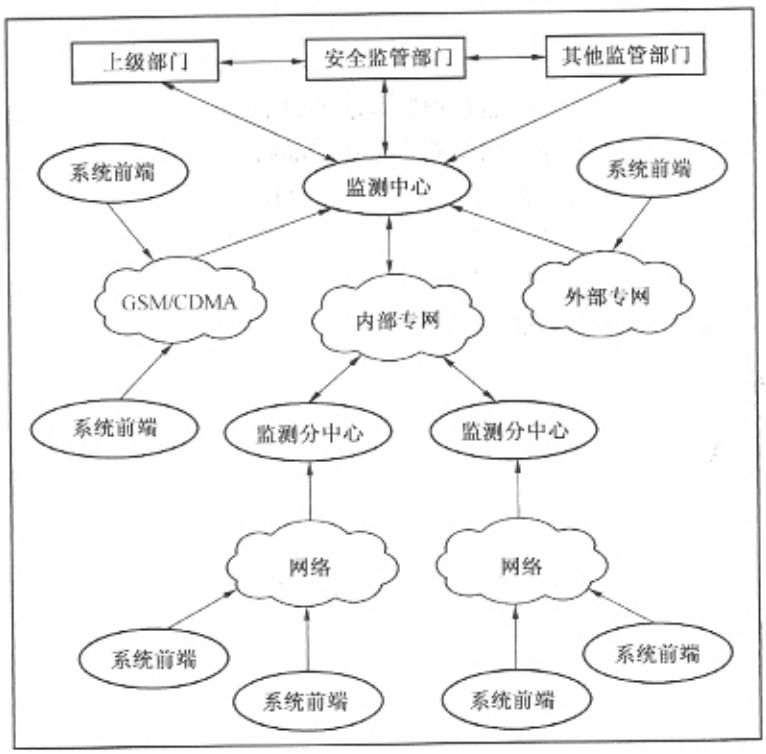

图 1 危险场所网络化监测系统结构示意图

4.2 系统组成

4.2.1 系统主要由监测系统前端、数据传输网络、监测中心及监测分中心等组成，通过数据采集系统或采集设备，将监测对象状态数据进行采集、存储、实时处理，并通过网络远程传输到上级监测中心。

4.2.2 系统前端的组成参见本规范第 1 部分 4.2。

4.2.3 数据传输网络是指具有一定资质的网络运营商提供的网络运营线路及网络设备。

4.2.4 监测中心或分中心的硬件主要由服务器/服务器群、网络设备、数据存储设备、数据显示设备以及周边设备等组成。

4.2.5 监测中心或分中心的软件主要有操作平台软件、数据库软件、专用监测软件、综合管理软件等，完成对多个系统前端的集中化综合管理。

4.3 系统设计要求

4.3.1 根据监测需要可将监测中心联网形成中心、分中心的层级网络结构，且网络层数不宜大于四层。

4.3.2 监测中心与分中心间应具有统一专用网络接口，以根据权限实现系统内数据的共享和调用。

4.3.3 监测分中心间应能够实现路由冗余，当其中一个监测分中心出现故障时，监测数据能够通过其他监测分中心上传到监测中心，以提高系统的可靠性。

4.3.4 监测中心与分中心间应实现数据冗余，当监测中心或分中心发生故障时，能够相互提供备份数据，以及时完成数据恢复。

4.3.5 监测中心及分中心应留有S端子接口、RCA接口、D-Sub接口中的一种，以提供公共视频设备接口。

4.3.6 监测网络的抗干扰能力、传送速率及传送距离应满足系统实时监测的要求，每级网络传输延时应少于10 s。

5 系统硬件功能要求

5.1 监测中心及分中心设备要求

5.1.1 监测中心设备平均无故障运行时间(MTBF)应大于8 000 h，监测分中心设备平均无故障运行时间(MTBF)应大于5 000 h，关键硬件应具有冗余备份能力。

5.1.2 监测中心及分中心服务器的处理速度应满足该中心数据处理的要求，可根据监测数据规模采用单台服务器或服务器群，服务器应保证不间断运行。

5.1.3 监测中心及分中心存储设备的容量选取应根据该中心接收监测数据量来确定，应保证监测数据、报警信息等动态数据至少保存90天。

5.1.4 监测中心及分中心应提供必要的外围设备，如打印机等。

5.2 系统前端设备要求

5.2.1 按照本规范第1部分中有关规定执行。

6 软件功能要求

6.1 一般要求

6.1.1 监测系统软件部分主要由操作平台软件、数据库软件和应用软件组成。

6.1.2 软件宜采用分层及模块化结构。

6.1.3 软件应具有数据自动备份和恢复的能力。

6.1.4 系统中所有涉及时间的信息和数据，应采用纪元表示法。

6.1.5 监测应用软件应具备时间校准功能。

6.2 操作系统要求

6.2.1 服务器应采用稳定、可靠、易于维护并具有良好的软件开发环境的操作系统，如Unix、Windows、Linux、红旗Linux等。

6.2.2 操作系统人机交互界面应采用中文界面。

6.3 数据库要求

6.3.1 监测中心及分中心应采用性能可靠的通用数据库系统，包括Oracle、Sybase、SQL Server、MySQL数据库软件。

6.3.2 监测中心及分中心数据库应支持开放式数据互连方式 ODBC 或 ADO。

6.3.3 数据库应足够承载系统产生的数据量，具有良好的多用户并发访问性能。

6.3.4 数据库应具备分级的操作/访问权限控制机制。

6.4 专用软件要求

6.4.1 性能要求

系统集成设计过程中在整体性能方面应考虑以下要求：

a) 易用性：应具有友好的可视化用户操作界面，操作方便、简单，应具有在线帮助功能。

b) 可靠性：应能够在规定条件下和规定时间内完成规定功能。

c) 鲁棒性：应能保证 7×24 h 全天候稳定运行。

d) 高效性：应具有较高的运行效率，能够对事件做出快速响应。

e) 安全性：应有很高的安全性，保护数据安全和自身的正常运行，应具备数据备份及恢复功能，同时具有用户认证机制。

f) 可扩展性：应有良好的扩展性，易于升级和扩展。

6.4.2 基本功能要求

6.4.2.1 宜采用 B/S 结构，支持 Web 发布。

6.4.2.2 应能够通过访问权限机制，对不同类型账户进行权限分级管理。

6.4.2.3 应具有容错纠错能力，一般软件故障不应引起死机、数据破坏、系统重启等反应，操作失误时，软件可以自动提示。

6.4.2.4 应提供在线软件使用说明书。

6.4.2.5 系统参数、用户数据与处理程序应有相对的独立性，任何软件版本的变更均不应影响用户数据。

6.4.2.6 对当前的系统设置、设备参数以及运行方式等进行更改，要求操作方便，具备设置向导以及操作提示。

6.4.2.7 具有自动记录功能，可记录以下数据并至少保存 90 天：

a) 系统用户登录次数；

b) 系统发生故障次数；

c) 操作日志。

6.4.3 监测业务要求

6.4.3.1 系统专用软件应具备多点监测统一管理的功能，能够对多处危险场所进行实时监测管理。

6.4.3.2 应能够存储监测企业、监测参量及监测设备等的基础信息，存储监测数据、报警信息、处理记录等动态信息。

6.4.3.3 能够实时显示系统采集的监测对象状态数据，使监测中心用户能够实时了解企业现场监测对象的状态变化。

6.4.3.4 软件报警及处理机制应满足以下要求：

a) 监测中心及分中心报警规则的设置应综合考虑系统前端监测对象报警阈值及下级中心报警处理时间等因素；

b) 监测中心及分中心软件应具有报警上传功能，即实现将报警信息向上一级监测中心发送，并同时越级发送；

c) 监测中心及分中心软件应具有报警通告等功能，即通过 E－mail 或手机短信将报警信息实时发送到有关单位或负责人。

6.4.3.5 监测中心及分中心软件应为系统前端的入网权限提供资格认证服务，确保系统信息的安全和实现统一化管理。

6.4.3.6 应具有数据抽取功能，即能够对下级监测分中心数据按照一定规则进行筛选，以满足重点数

据保存的要求。

6.4.3.7 软件应具有重点数据恢复功能，即当某一监测中心发生故障时能够根据上级监测中心保存的重点数据及时进行数据恢复。

6.4.3.8 监测中心及分中心软件设计应考虑预留开放接口，能够与其他相关系统进行跨平台链接，实现信息共享和集中管理等。

6.4.3.9 监测中心及分中心应实现对监测数据的报表打印。

7 网络传输要求

7.1 一般要求

7.1.1 系统前端与监测分中心间网络应按照本规范第1部分的要求搭建，在满足传输速度要求的前提下应尽可能利用现有网络资源。

7.1.2 监测中心与监测分中心间网络搭建应满足以下要求。

7.2 传输协议

7.2.1 系统前端与监测分中心间数据传输参见本规范第1部分4.3.4.3。

7.2.2 监测中心与分中心间数据传输应采用TCP/IP传输协议。

7.2.3 系统与外部其他系统间数据传输应采用TCP/IP传输协议。

7.3 传输速率

7.3.1 系统前端的接入选用有线网络传输时，接入网传输速率应不低于1 Mbps。

7.3.2 系统前端的接入选用无线网络传输时，接入网传输速率应不低于200 kbps。

7.3.3 监测中心与分中心间应建立有线专门传输网络，且传输速率应不低于10 Mbps。

7.3.4 系统前端与监测分中心间以及监测分中心与监测中心间网络延时均不应大于10 s。

7.3.5 图像信息的传输不应占用监测数据传输通道，如特殊需要传输图像信息时，应保证监测数据传输时间要求。

7.4 危险场所分级对传输速率的要求

7.4.1 非重大危险场所，接入网络传输速率应不低于200 kbps，可采用无线或有线方式进行数据传输。

7.4.2 重大危险场所，接入网络传输速率应不低于1 Mbps，应具备有线接入网络的条件，传输网可采用虚拟专网(VPN)，或者建立专用网络。

7.4.3 应急网络，接入网络传输速率应不低于10 Mbps，应建立专门传输网络。

7.5 网络的安全

7.5.1 操作系统应具备安全性要求，能防止病毒威胁与黑客侵入破坏。

7.5.2 网络监测系统应建设防火墙，防火墙产品应符合YD/T 1132—2001《防火墙设备技术要求》标准。

7.5.3 防火墙的安全性应符合GB/T 20010—2005《信息安全技术 包过滤防火墙评估准则》中的规定。

7.5.4 路由器的安全性应符合GB/T 20011—2005《信息安全技术 路由器安全评估准则》中的规定。

7.5.5 应根据不同的安全等级对用户进行分组访问控制管理，不同等级的用户只能访问与其等级相对应的系统资源和数据。

7.5.6 用户认证管理，应采用强有力的身份认证，只有合法用户才能够对特定的数据进行操作，包括应用程序对数据的合法权限和应用程序对用户的合法权限。

7.6 数据安全

7.6.1 系统使用公共网络传递信息时，应设置虚拟专网完成数据传递，且数据信息的存储及传递均需加密处理。

7.6.2 应充分利用行业专用网络传递信息，专用网络中的数据传输也应进行数据加/解密。

7.6.3 数据安全性加/解密应按照 GB/T 15278—1994《信息处理 数据加密 物理层互操作性要求》中的有关规定执行。

7.6.4 系统应具有数据备份及灾难恢复功能。

8 系统供电、接地

8.1 系统供电

8.1.1 监测中心及分中心设备应采用不间断电源供电，设有主电源和备用电源设备。

8.1.2 监测中心及分中心设备采用 UPS 电源供电时，应符合现行国家标准 GB 7260《不间断电源设备》中的规定。

8.1.3 监测中心及分中心设备发生断电后，备用电源备电时间应不少于 40 min。

8.2 系统接地

8.2.1 系统中各设备应可靠接地。

8.2.2 系统接地应按照 CECS 81:96《工业计算机监控系统抗干扰技术规范》中的有关规定执行。

9 工程施工要求

9.1 监测设备的安装应按照 GB 50254—1996《电气装置安装工程低压电器施工及验收规范》中的有关规定执行。

9.2 系统网络布线应按照 GB/T 50311—2000《建筑与建筑群综合布线系统工程设计规范》中的有关规定执行。

9.3 监测中心机房建设应按照 GB/T 2887—2000《电子计算机场地通用规范》中的有关规定执行。

10 系统验收

10.1 系统验收标准

10.1.1 系统严格按照设计规范进行建设，能够满足企业监管部门监测需要，确保运行合格。

10.1.2 系统主要技术指标、性能指标及运行指标均应符合监测要求。

10.1.3 需提交工程验收文件：

a) 提交竣工文件，包括：施工记录、设备材料检验总结、验收报告；

b) 提交软件文档资料，包括：需求说明书、设计说明书、测试分析报告、用户手册和操作手册；

c) 提交系统运行记录，包括：运行日志和事件记录。

10.1.4 提交系统验收测试报告。

10.2 系统验收程序

10.2.1 系统的验收应由安全生产管理部门组织实施。

10.2.2 系统验收步骤主要内容包括验收前检查、硬件检查、软件检查、系统试运行等。其中系统软件验收部分包括操作系统、数据库管理系统、专用监测软件、程序设计语言以及网络通信协议。

10.2.3 竣工技术资料应主要包括以下内容：

a) 文件清单：

竣工文件目录

b) 技术文件：

硬件设备技术文件

系统软件设计文件

通信协议

通信软件版权证书(复印件)

c) 工程设计、施工及调测文件：
各阶段设计文件
系统竣工报告
系统调测报告
变更设计文件
d) 用户操作维护文件：
系统软件安装手册
系统软件操作手册
监测系统设备产品使用说明书
产品合格证
e) 其他：
运行使用报告
系统培训技术资料及计划
备品、备件、工具仪表清单及使用说明

11 系统的运行与维护

11.1 日常维护

11.1.1 系统运行时应配备专业人员，负责系统日常管理和维护。

11.1.2 系统正式运行时，应具备文件资料，包括：操作规程、值班员手册、值班记录表。

11.1.3 系统中所有设备都要做好日常维护保养工作，注意防潮、防尘、防电磁干扰、防静电、防冲击、防碰撞等各项防护工作，保证设备良好。一般每月进行一次除尘维护，除尘前应先对系统进行断电。

11.1.4 要保持系统连续正常运行，不得随意人为中断，以免造成严重后果。

11.1.5 建立日常运行维护技术档案。

11.2 定期检查

11.2.1 监测系统及网络设备应进行定期检查，定期检查应由专业检验机构执行。

11.2.2 检验周期规定见本规范第3部分。

11.3 故障处理

11.3.1 应配备或指定专业维修人员。

11.3.2 系统发生故障时应采取应急措施，保证系统在48 h内恢复运行。