ICS XXX
CCS XXX

T/HEBQIA

团　　体　　标　　准

T/HEBQIA ××××—2025

升压站智能化监控系统通信网络设计规范

（征求意见稿）

2025－××－××发布　　2025－××－××实施

河北省质量信息协会　　发布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
3.1 1
升压站智能化监控系统 1
3.2 1
通信网络 1
3.3 1
站控层 2
3.4 2
间隔层 2
3.5 2
过程层 2
4　总则 2
4.1　设计原则 2
4.2　基本要求 2
5　系统架构 2
5.1　总体架构 3
5.2　站控层网络 3
5.3　间隔层网络 3
5.4　过程层网络 3
6　通信协议 3
6.1　站控层通信协议 3
6.2　间隔层通信协议 4
6.3　过程层通信协议 4
7　网络安全 4
7.1　网络安全防护体系 4
7.2　边界防护 4
7.3　入侵检测与防范 4
7.4　病毒防护 5
7.5　数据加密 5
7.6　身份认证与访问控制 5
8　性能指标 5

8.1 网络带宽 5
8.2 传输延时 6
8.3 可靠性 6
8.4 误码率 6
9 测试与验收 6
9.1 测试内容 6
9.2 测试方法 6
9.3 验收标准 7
10 运行维护 7
10.1 日常维护 7
10.2 故障处理 7
10.3 维护记录 7

前　言

本文件依据GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由北京沂瑞科技有限公司提出。

本文件由河北省质量信息协会归口。

本文件起草单位：北京沂瑞科技有限公司、XXX。

本文件主要起草人：XXX。

升压站智能化监控系统通信网络设计规范

1 范围

本文件规定了升压站智能化监控系统通信网络的设计原则、技术要求、网络架构、通信协议、网络安全、性能指标、测试与验收等内容。

本文件适用于新建、扩建和改建的升压站智能化监控系统通信网络的设计、施工、验收及运行维护。对于类似的变电站智能化监控系统通信网络设计可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB 50174 数据中心设计规范

GB 50343 建筑物电子信息系统防雷技术规范

DL/T 476 电力系统实时数据通信应用层协议

DL/T 634.5101 远动设备及系统 第 5-101 部分：传输规约 基本远动任务配套标准

DL/T 634.5104 远动设备及系统 第 5-104 部分：传输规约 采用标准传输协议集的 IEC 60870-5-101 网络访问

DL/T 860 变电站通信网络和系统

3 术语和定义

下列术语和定义适用于本文件。

3.1

升压站智能化监控系统

采用先进的信息技术、通信技术、自动化技术等，对升压站的运行设备进行实时监测、控制和管理，实现升压站智能化运行的系统。

3.2

通信网络

用于传输升压站智能化监控系统数据、控制指令等信息的网络，包括网络设备、通信链路、通信协议等。

3.3

站控层

升压站智能化监控系统中，实现对全站设备进行监控、管理和协调的层次，主要设备包括监控主机、数据服务器、操作员站、工程师站等。

3.4

间隔层

位于升压站智能化监控系统中间层，负责采集和处理一次设备的实时数据，并执行站控层下达的控制指令，主要设备包括测控装置、保护装置、智能终端等。

3.5

过程层

升压站智能化监控系统中直接面向一次设备的层次，实现与一次设备的信息交互，主要设备包括合并单元、智能传感器等。

4 总则

4.1 设计原则

升压站智能化监控系统通信网络的设计应遵循以下原则。

4.1.1 可靠性：通信网络应具备高可靠性，确保数据传输的准确性和实时性，避免数据丢失和通信中断。采用冗余设计，包括网络链路冗余、设备冗余等，提高系统的容错能力。

4.1.2 安全性：通信网络应采取有效的安全防护措施，防止网络攻击、数据泄露等安全事件的发生，保障升压站的安全稳定运行。

4.1.3 开放性：通信网络应具备开放性，支持多种通信协议和接口，便于与其他系统进行集成和互联互通。

4.1.4 可扩展性：通信网络应具有良好的可扩展性，能够适应升压站未来发展的需求，方便进行系统升级和功能扩展。

4.1.5 经济性：在满足系统性能要求的前提下，通信网络的设计应考虑经济性，合理选择设备和技术，降低建设和运行成本。

4.2 基本要求

升压站智能化监控系统通信网络应满足以下基本要求。

4.2.1 能够实时、准确地传输升压站运行设备的各种数据，包括遥测、遥信、遥控、遥调等信息。

4.2.2 具备快速的响应速度，满足对升压站设备的实时控制要求。

4.2.3 支持多种通信方式，如光纤通信、无线通信等，以适应不同的应用场景。

4.2.4 具备良好的兼容性，能够与升压站内现有的设备和系统进行无缝集成。

4.2.5 便于维护和管理，具备完善的故障诊断和报警功能。

5 系统架构

5.1 总体架构

升压站智能化监控系统通信网络宜采用分层分布式架构，分为站控层、间隔层和过程层。各层之间通过通信网络进行数据交互，实现对升压站设备的全面监控和管理。

5.2 站控层网络

5.2.1 设备组成

站控层网络设备主要包括监控主机、数据服务器、操作员站、工程师站、远动工作站、网络交换机、时钟同步装置等。

5.2.2 网络结构

站控层网络应采用双网冗余结构，网络拓扑宜为星型。网络交换机应具备高性能、高可靠性，支持 VLAN 划分、链路聚合、生成树协议等功能。

5.2.3 通信协议

站控层设备之间的通信应采用标准的通信协议，如 IEC 61850 MMS（制造报文规范）协议，实现设备之间的互操作性和数据共享。

5.3 间隔层网络

5.3.1 设备组成

间隔层网络设备主要包括测控装置、保护装置、智能终端、网络交换机等。

5.3.2 网络结构

间隔层网络可采用单网或双网结构，根据升压站的重要性和可靠性要求进行选择。网络拓扑宜为星型或总线型。网络交换机应具备工业级防护能力，适应变电站的恶劣环境。

5.3.3 通信协议

间隔层设备与站控层设备之间的通信应采用 IEC 61850 GOOSE（面向通用对象的变电站事件）协议和 SV(采样值)协议，实现快速的数据传输和控制命令的执行。间隔层设备之间的通信可采用 IEC 61850 协议或其他标准通信协议。

5.4 过程层网络

5.4.1 设备组成

过程层网络设备主要包括合并单元、智能传感器、网络交换机等。

5.4.2 网络结构

过程层网络应采用双网冗余结构，网络拓扑宜为星型。网络交换机应具备低延时、高带宽的特性，满足采样值和跳闸命令等实时性要求较高的数据传输。

5.4.3 通信协议

过程层设备与间隔层设备之间的通信应采用 IEC 61850 SV 协议和 GOOSE 协议，实现一次设备数据的采集和传输以及保护跳闸命令的快速执行。

6 通信协议

6.1 站控层通信协议

6.1.1 IEC 61850 MMS 协议

站控层设备之间应采用 IEC 61850 MMS 协议进行通信。该协议定义了一套面向对象的通信服务和模型，能够实现监控主机、数据服务器、操作员站等设备之间的信息交互，包括实时数据访问、历史数据查询、设备状态监测、控制命令下发等功能。

6.1.2 其他通信协议

在与外部系统进行通信时，站控层可根据需要采用其他标准通信协议，如 DL/T 476、MODBUS 等，实现与调度中心、电能质量监测系统、电量计费系统等的互联互通。

6.2 间隔层通信协议

6.2.1 IEC 61850 GOOSE 协议

间隔层设备之间以及间隔层设备与站控层设备之间应采用 IEC 61850 GOOSE 协议进行快速的状态信息传输和控制命令执行。GOOSE 协议采用发布 / 订阅机制，能够实现数据的可靠传输和快速响应，满足保护跳闸、开关变位等实时性要求较高的应用场景。

6.2.2 IEC 61850 SV 协议

对于采样值数据的传输，间隔层设备与过程层设备之间应采用 IEC 61850 SV 协议。SV 协议定义了采样值的传输格式和通信机制，能够保证采样值的高精度和实时性。

6.3 过程层通信协议

过程层设备与间隔层设备之间应采用 IEC 61850 SV 协议和 GOOSE 协议进行通信，以实现一次设备数据的采集和传输以及保护跳闸命令的快速执行。

7 网络安全

7.1 网络安全防护体系

升压站智能化监控系统通信网络应建立完善的网络安全防护体系，包括边界防护、入侵检测、病毒防护、数据加密、身份认证、访问控制等措施，确保网络安全。

7.2 边界防护

7.2.1 防火墙设置

在站控层网络与外部网络（如调度数据网、互联网等）之间应设置防火墙，对进出网络的流量进行过滤和控制，防止外部非法网络访问和攻击。防火墙应具备访问控制策略配置、入侵检测、防病毒等功能。

7.2.2 网闸应用

对于与外部网络有数据交互但安全性要求较高的系统，如与上级调度中心进行数据传输的远动工作站，可采用网闸进行隔离。网闸能够在保证数据安全交换的前提下，实现不同安全区域之间的物理隔离。

7.3 入侵检测与防范

7.3.1 入侵检测系统部署

在通信网络中应部署入侵检测系统（IDS），实时监测网络流量，及时发现并报警网络入侵行为。IDS 应具备对常见攻击类型的检测能力，如端口扫描、恶意软件传播、SQL 注入等。

7.3.2 入侵防范措施

结合入侵检测系统的报警信息，采取相应的入侵防范措施，如阻断攻击源的网络连接、调整防火墙访问控制策略等，防止入侵行为对系统造成损害。

7.4 病毒防护

7.4.1 防病毒软件安装

在站控层和间隔层的计算机设备上应安装防病毒软件，并定期进行病毒库更新，防止病毒感染和传播。防病毒软件应具备实时监控、病毒查杀、自动更新等功能。

7.4.2 移动存储设备管理

加强对移动存储设备（如 U 盘、移动硬盘等）的管理，禁止未经授权的移动存储设备接入通信网络。对于需要使用的移动存储设备，应先进行病毒查杀，确保设备无病毒后再进行数据交换。

7.5 数据加密

7.5.1 传输加密

对于通信网络中传输的敏感数据，如控制命令、重要设备参数等，应采用加密技术进行传输加密，防止数据在传输过程中被窃取或篡改。可采用 SSL/TLS 等加密协议对数据进行加密传输。

7.5.2 存储加密

在数据存储方面，对于重要的数据文件和数据库，应采取加密存储措施，确保数据的安全性。可采用磁盘加密、数据库加密等技术对数据进行加密存储。

7.6 身份认证与访问控制

7.6.1 身份认证机制

建立完善的身份认证机制，对登录通信网络的用户进行身份验证，确保用户身份的合法性。可采用用户名/密码、数字证书、动态口令等多种身份认证方式。

7.6.2 访问控制策略

根据用户的角色和职责，制定严格的访问控制策略，对用户的操作权限进行限制。只有经过授权的用户才能对相应的设备和数据进行访问和操作，防止非法用户对系统进行破坏。

8 性能指标

8.1 网络带宽

8.1.1 站控层网络带宽

站控层网络的带宽应根据系统的数据传输需求进行合理配置，确保能够满足实时数据传输、历史数据查询、画面刷新等业务的带宽要求。一般情况下，站控层网络的主干链路带宽应不低于 1000Mbps，分支链路带宽应不低于 100Mbps。

8.1.2 间隔层网络带宽

间隔层网络的带宽应满足测控装置、保护装置等设备与站控层设备之间的数据传输需求。对于采用双网结构的间隔层网络，每一条网络链路的带宽应不低于 100Mbps。

8.1.3 过程层网络带宽

过程层网络的带宽要求较高，应满足合并单元与间隔层设备之间采样值数据的高速传输需求。过程层网络的主干链路带宽应不低于 1000Mbps，分支链路带宽应不低于 100Mbps。

8.2 传输延时

8.2.1 站控层传输延时

站控层设备之间的数据传输延时应不大于 100ms，以保证监控画面的实时性和操作响应的及时性。

8.2.2 间隔层传输延时

间隔层设备与站控层设备之间的 GOOSE 报文传输延时应不大于 3ms，SV 报文传输延时应不大于 1ms，满足保护跳闸和采样值实时性的要求。

8.2.3 过程层传输延时

过程层设备与间隔层设备之间的 SV 报文传输延时应不大于 1ms，GOOSE 报文传输延时应不大于 3ms，确保一次设备数据的快速采集和保护命令的及时执行。

8.3 可靠性

8.3.1 网络链路可靠性

通信网络的链路应具备高可靠性，采用冗余链路设计，当一条链路出现故障时，能够自动切换到备用链路，保证数据传输的连续性。网络链路的可靠性应不低于 99.99%。

8.3.2 设备可靠性

网络设备(如交换机、路由器等)应采用工业级产品，具备高可靠性和稳定性，平均无故障时间(MTBF)应不低于 100000 小时。设备应具备冗余电源、热插拔等功能，便于维护和管理。

8.4 误码率

通信网络的误码率应满足以下要求：站控层网络误码率应不大于 10^-9，间隔层网络误码率应不大于 10^-10，过程层网络误码率应不大于 10^-12。

9 测试与验收

9.1 测试内容

升压站智能化监控系统通信网络在建设完成后，应进行全面的测试，测试内容包括但不限于以下方面：

a) 网络连通性测试：检查网络设备之间的连接是否正常，确保数据能够在网络中正确传输。
b) 通信协议测试：验证通信协议的一致性和正确性，确保设备之间能够按照预定的协议进行通信。
c) 网络性能测试：测试网络的带宽、传输延时、可靠性、误码率等性能指标，评估网络是否满足设计要求。
d) 网络安全测试：对网络安全防护措施进行测试，包括边界防护、入侵检测、病毒防护、数据加密、身份认证、访问控制等，检查网络安全防护体系是否有效。
e) 系统集成测试：对通信网络与升压站智能化监控系统的其他部分进行集成测试，确保系统整体运行稳定，各项功能正常。

9.2 测试方法

测试方法应根据测试内容的不同进行选择，可采用以下测试方法：

a) 工具测试：使用专业的网络测试工具，如网络分析仪、协议分析仪、性能测试工具等，对网络性能、通信协议等进行测试。
b) 模拟测试：通过模拟实际运行场景，对网络的可靠性、安全性等进行测试。例如，模拟网络链路故障，检查网络的自愈能力；模拟外部攻击，检查网络安全防护措施的有效性。
c) 实际业务测试：在实际运行环境中，通过执行各种业务操作，如数据采集、控制命令下发、报表生成等，测试网络对实际业务的支持能力。

9.3 验收标准

通信网络的验收应依据本标准及相关的设计文件进行，验收标准如下：
a) 测试结果符合要求：各项测试内容的测试结果应满足本标准规定的性能指标和技术要求。
b) 系统运行稳定：经过一定时间的试运行，通信网络应运行稳定，无明显的故障和异常现象。
c) 文档齐全：提供完整的通信网络设计文档、施工文档、测试文档等，文档内容应与实际建设情况相符。

10 运行维护

10.1 日常维护

通信网络的日常维护应包括以下内容：
a) 设备巡检：定期对网络设备进行巡检，检查设备的运行状态、温度、风扇运转等情况，及时发现设备故障隐患。
b) 网络监测：实时监测网络的运行状态，包括网络流量、带宽利用率、传输延时、误码率等指标，及时发现网络异常情况。
c) 数据备份：定期对重要的网络配置数据、用户数据、历史数据等进行备份，防止数据丢失。
d) 软件升级：及时对网络设备的操作系统、应用程序等进行升级，修复软件漏洞，提高系统性能和安全性。

10.2 故障处理

当通信网络出现故障时，应及时进行故障诊断和处理，恢复网络的正常运行。故障处理流程如下：
a) 故障报告：发现网络故障后，应及时向上级部门报告故障情况，包括故障现象、发生时间、影响范围等。
b) 故障诊断：通过网络测试工具、设备日志等手段，对故障进行诊断，确定故障原因和故障位置。
c) 故障排除：根据故障诊断结果，采取相应的措施进行故障排除，如更换故障设备、修复网络链路、调整配置参数等。
d) 恢复验证：在故障排除后，对网络进行恢复验证，确保网络恢复正常运行，各项业务功能正常。

10.3 维护记录

建立完善的通信网络维护记录制度，对日常维护和故障处理的情况进行详细记录，包括维护时间、维护内容、维护人员、故障现象、故障原因、处理措施等。维护记录应妥善保存，作为网络运行维护的重要参考资料。