

DB4403

深 圳 市 地 方 标 准

DB4403/T XXX—XXXX

电力系统用通信机房分布式协同巡检技术要求

Technical requirements for distributed collaborative inspection of
communication equipment rooms for power systems

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 技术要求 2

5 通信接口协议要求 3

6 组网及数据接入要求 4

7 安全要求 4

8 试验要求 6

前 言

本文件按照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。

本文件由深圳市发展和改革委员会提出并归口。

本文件起草单位：深圳供电局有限公司、深圳市标准技术研究院、南京南瑞信息通信科技有限公司、华南理工大学、广东工业大学、深圳电气科学研究院、凯通科技股份有限公司、成合科技（深圳）有限公司、广东九联开鸿科技发展有限公司。

本文件主要起草人：陈嘉、李媛红、吕为、孙沛杰、田志峰、翁俊鸿、黄儒雅、黄晓奇、谭康、吴谦、曾凌烽、章秀银、韩国军、易检长、丁长兴、周建勇、宋英杰、张天李翼、张越、高强、吴彤浩、陈岳、张玉兵、赵华、乔治中、肖敏英、李伟生、陈瑞、郭桃勋、方鸣山、刘畅、李淳伟。

电力系统用通信机房分布式协同巡检技术要求

1 范围

本文件规定了电力系统用通信机房分布式协同巡检技术要求、通信接口协议要求、组网及数据接入要求、安全要求、试验要求等。

本文件适用于电力系统通信机房巡检系统的建设与运维。

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 26865.2 电力系统实时动态监测系统 第2部分：数据传输协议

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5101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IEC60870-5-101 网络访问

DL/T 667 远动设备及系统 第5部分：传输规约 第103篇：继电保护设备信息接口配套标准

DL/T 719 远动设备及系统 第5部分：传输规约 第102篇：电力系统电能累计量传输配套标准

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

智能终端设备 smart terminal devices

用于数据采集或执行控制命令的设备，同时具备计算和处理能力，能够执行任务、处理数据并与其他设备交互，通常具有自主决策和适应环境的能力。

3.2

终端设备 terminal devices

能利用通信设施与远程设备或系统连接工作的设备，具有数据传感、采集、测量、通信处理、控制等一项或多项功能。通常不具备复杂的处理能力，依赖外部系统进行数据处理和决策。

[来源：DL/T 1933.5-2018]

3.3

分布式协同 distributed collaboration

两个或两个以上的分布式资源或个体，通过网络通信和协调机制，协同一致地完成某一目标的过程或能力。

[来源：DB33/T 944.2-2017]

3.4

分布式协同巡检 distributed collaborative inspection

多个智能终端设备与终端设备在机房中协同完成任务分配、任务执行、实时互联、自适应协作和动态状态共享的巡检作业。

3.5

分布式软总线 distributed soft bus

用于在分布式协同巡检系统的各个组件（如不同的传感器、巡检设备、数据处理单元等）之间建立高效、灵活且可靠连接的通信机制。

3.6

南北向通信 North-South Communication

在分层系统架构中，不同层级之间的数据交换与控制指令传递。特指应用层与设备层之间的垂直方向通信。

3.7

东西向通信 East-West Communication

在系统架构的同一层级内部，各组件或设备之间的数据交换与功能协作。特指设备层内部各智能终端设备、终端设备之间，通过分布式软总线技术实现的水平方向通信。

4 技术要求

4.1 基本要求

4.1.1 电力系统用通信机房分布式协同巡检系统架构分为应用层和设备层，如图 1 所示。

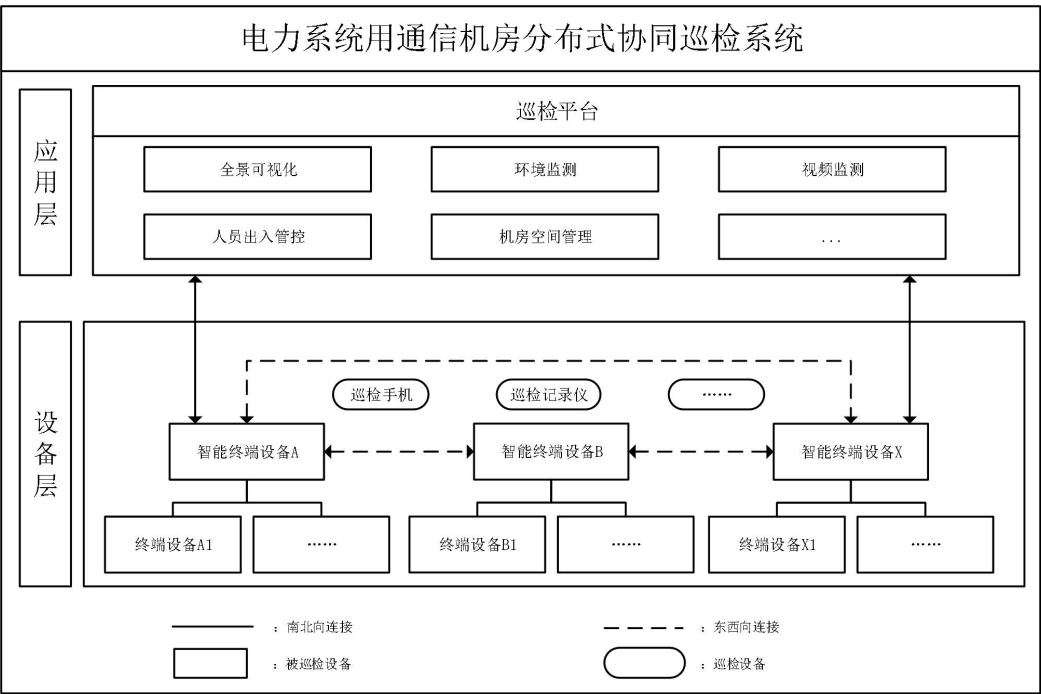


图 1 电力系统用通信机房分布式协同巡检系统架构图

4.1.2 在电力系统用通信机房分布式协同巡检系统中，智能终端设备与终端设备应协同任务分配与任务执行。

4.1.3 应确保巡检平台和设备层能够实时互联与连接，自适应协作，并动态共享设备状态。

4.1.4 南北向通信应保障应用层与设备层之间的数据传输与控制指令传递，确保系统的垂直联动和集中管理。

4.1.5 高层级控制指令可通过南北向通信通道自上而上传达至底层设备，底层设备的状态和运行数据可由下而上传输至应用层。

4.1.6 机房内的设备或系统，如智能网关、传感器、监控摄像头等，可通过东西向通信实现数据共享和功能协作。东西向通信宜采取软件定义的方式，替代传统硬总线功能。东西向通信组网的应用可包括：

- a) 通过软件配置实现设备间的灵活互联，无需物理更改网络布线；
- b) 根据系统运行状态和需求，动态调整网络连接和数据流向。

4.2 分布式协同要求

4.2.1 南北向协同应满足下列要求：

- a) 南北向协同具备跨层级的数据传输与控制能力，保障上下级设备的数据交互和指令传递；
- b) 智能终端设备宜实时采集并传输数据至上级平台，同时支持接收巡检平台指令，包括任务调度、参数调整和启停控制等功能；
- c) 系统在发生异常或故障时迅速上报至平台并接收应急指令；
- d) 设备与巡检平台应保持数据同步与状态一致，避免网络波动引发数据延迟或丢失。

4.2.2 东西向协同应满足下列要求：

- a) 设备宜通过分布式软总线实现实时互联、动态共享状态、负荷和任务进展；
- b) 系统可根据设备位置和负载情况，基于任务分配机制灵活分派任务，自动优化资源利用率。

4.3 巡检功能要求

4.3.1 南北向巡检应满足下列要求：

- a) 巡检系统具备自动化、智能化的巡检能力；
- b) 巡检系统宜支持预设的自动巡检任务，并根据实际需求动态调整巡检频率和内容；
- c) 巡检系统在发现异常时自动生成报警，并根据设定的响应规则采取相应措施；
- d) 巡检系统支持远程调试功能，减少现场维护需求；
- e) 巡检系统可通过自适应调度机制，根据设备状态和运行负荷，动态调整巡检任务优先级与频次。

4.3.2 东西向巡检应满足下列要求：

- a) 东西向巡检宜利用分布式软总线技术，设备间实时互联与状态共享，以满足多设备间的高效协作需求；
- b) 巡检系统可支持设备间的任务分配和进度同步，基于设备位置、状态和负载情况动态调整任务；
- c) 巡检系统可支持设备间基于 WAPI、蓝牙或其他通信方式进行资源共享和任务协作；
- d) 分布式软总线可动态共享巡检设备的负荷与任务进展，建立设备间的高效协作网络；
- e) 巡检系统宜支持基于任务需求和设备能力的自动化任务分派机制，确保巡检任务按优先级和资源分配的优化策略执行。

5 通信接口协议要求

5.1 智能终端设备南向通信接口协议应满足下列要求：

- a) 南向通信宜支持 WAPI、蓝牙、星闪等无线通信方式；
- b) 南向通信宜支持终端设备接入时可根据设备要求选择合适链路；
- c) 数据采集的通信协议支持 DL/T 667、DL/T 860 等规范。

5.2 智能终端设备北向通信接口协议应满足下列要求：

- a) 北向通信宜采用统一的标准化通信协议；

DB4403/T XXX—XXXX

注：标准化通信协议包括https、MQTT、CORBA、SNMP。

b) 北向通信宜采用可扩展的数据格式；

注：数据格式包括XML、JSON。

c) 北向通信宜支持与巡检平台通过多种方式进行通讯；

注：通讯方式包括4G/5G、WAPI、有线专网等。

d) 北向通信应支持定义统一的数据上报、控制数据下发的格式；

e) 应支持 DL/T 634.5101、DL/T 634.5104、DL/T 719、DL/T 476、GB/T 26865.2 等协议。

5.3 东西向接口协议应满足下列要求：

a) 智能终端设备宜支持不同的物理链路通信，发布、注册并告知其他设备其自身能力，实现设备基于一定规则的自动发现并建立安全连接；

b) 组网能力宜支持物理异构组网；

c) 东西向通信协议宜通过操作系统功能进行东西向互联互通；

d) 东西向通信应以分布式软总线为核心，通过操作系统底层功能（如设备驱动、进程管理）实现互联互通，支持 WAPI / 蓝牙 / RFID 等协议进行设备发现与连接；

e) 设备间应支持组网认证，以及设备间消息、字节、流、文件的传输。

6 组网及数据接入要求

6.1 设备间发现和连接

设备处于同一网络段、已完成 IP 地址等基础配置时，智能终端设备、终端设备可支持自动发现机制，宜支持分布式软总线，并通过软总线中枢模块实现设备的主动探测和识别。

6.2 多设备互联组网

智能终端设备、终端设备宜支持异构网络组网，不同类型、品牌、协议的设备能在同一网络中互联，并支持近端数据获取、设备控制、设备巡检等功能。

6.3 多设备多协议间传输实现

6.3.1 智能终端设备、终端设备流式传输应基于 TCP 实现数据的保序和可靠传输。

6.3.2 智能终端设备、终端设备宜采用智能感知网络变化、自适应流量控制和拥塞控制策略。

7 安全要求

7.1 电力系统用通信机房分布式协同巡检系统安全架构如图 2 所示。

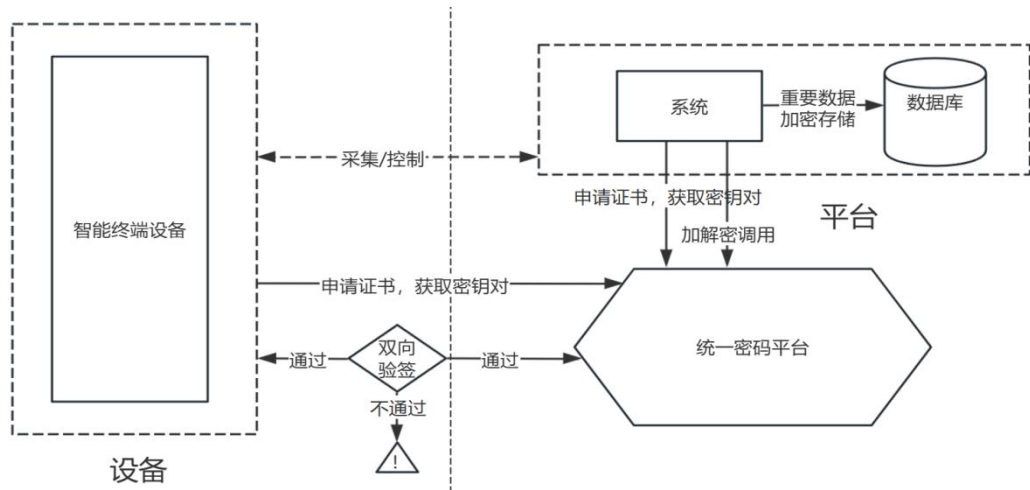


图 2 电力系统用通信机房分布式协同巡检系统安全架构

7.2 设备接入安全要求应符合下列规定：

- a) 智能终端设备支持国密算法或电力加密算法验签对系统进行验证。系统验签不通过时，设备应拒绝执行下发控制指令并返回拒绝执行原因、输出告警通知，系统收到返回信息后执行保底策略措施；
- b) 设备及系统向统一密码平台申请密钥证书，获得密钥对；
- c) 系统调用统一密码平台进行加解密；
- d) 系统采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，并采取相应的访问控制措施限制其在权限范围内访问业务数据；
- e) 系统中控制命令操作必须实施应用层面的端到端加密和认证措施，并在通信消息中加入时间戳和随机数等安全特征。

7.3 系统部署安全要求应符合下列规定：

- a) 系统所需数据库服务器、应用服务器、接口服务器、采集服务器、交换机等硬件设备均满足 N-1 条件下不影响系统功能与对外提供服务的要求，即要求双机热备份；
- b) 主备设备在常规情况下能实现主备机器的负载均衡，任何一台设备出现故障，备用设备能实现全部业务的承载；
- c) 系统支持对自身硬件运行状态监视，任何一台设备出现运行异常，系统对外告警并自动通知相关人员，同时将自身承载业务自动无缝切换至备用设备；
- d) 系统网络连接满足双配置，并通过独立的设备、不交叠的电路路由实现数据传输。

7.4 系统数据满足机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）原则，具体包括：

- a) 系统数据区分敏感数据和普通数据，对敏感数据通过国密算法存储加密，并验证敏感数据来源；
- b) 系统数据支持按照角色身份权限访问和维护；
- c) 系统具备记录数据访问过程、访问者、操作内容、操作时间等日志，具备审计和监视异常操作的能力；
- d) 系统数据定期备份（敏感数据每日备份，普通数据每周备份），备份介质宜采用“本地硬盘 + 云端服务器”双备份，还原数据前需通过 SM3 哈希校验验证数据完整性，确保数据未被篡改；
- e) 系统支持集群部署架构，在单节点故障时仍能提供数据访问、数据维护功能；
- f) 系统具备应急破壁机制，在特定紧急情况下，允许授权人员绕过正常访问控制限制，快速获得关键系统或数据的访问权限。应急破壁机制严格遵守最小权限原则，在正常操作中不会过度暴露敏感数据，在紧急情况下仍能保持业务连续性和系统的可恢复性。

8 试验要求

8.1 系统试验要求

8.1.1 试验环境要求应符合下列规定：

- a) 具备畅通的测试网络环境，测试环境与正式网络环境在配置、性能和通信质量等方面保持一致；
 - b) 系统正常部署并能稳定运行，服务器、硬件设备以及系统组件无故障或性能异常；
- 注：故障或性能异常包括内存占用过高、CPU负载过高或磁盘空间不足等。
- c) 所有设备的协议正常启用，设备之间网络连通性通过验证，无数据丢失或通信中断现象。
 - d) 系统所需试验数据提前准备完毕，确保数据完整、准确。

8.1.2 试验过程要求应符合下列规定：

- a) 试验过程覆盖单场景测试、混合场景测试、疲劳场景测试。
- b) 试验方式包括系统压力测试、设备接入测试、告警测试。

8.2 分布式协同巡检功能测试要求

8.2.1 南北向协同应符合下列规定：

- a) 搭建上下级设备通信环境，模拟数据上传和指令下发进行试验，系统正确完成上下级间的数据传输和控制指令交互，信息传递无异常中断或失真；
- b) 对智能终端设备施加持续运行任务，以数据采集、上报，平台指令接收、执行进行试验。终端设备能够稳定采集数据、准确上传，并能响应上级平台下发的任务调度、参数调整和启停控制指令；
- c) 模拟系统异常状态，系统能主动上报异常信息并接收平台下发的应急响应指令；

注：系统异常状态包括通信异常、电源中断、模块故障等。

- d) 在网络波动或间歇性中断环境下测试设备与平台的数据同步与状态一致性，系统在网络恢复后能够及时完成数据同步，设备状态与平台保持一致，无明显滞后或数据丢失。

8.2.2 东西向协同应符合下列规定：

- a) 构建多个智能终端设备及终端设备组成的协同运行环境，采用模拟任务下发、状态变化与进度更新等操作进行测试。记录各设备是否能够实时交换状态、任务执行情况和负载信息；
- b) 设置不同地理位置和负载并向系统下发多个任务，进行任务分配和资源调度行为试验，系统能自动进行任务分派且任务分布均衡。

8.2.3 南北向巡检应符合下列规定：

- a) 对巡检系统进行无人干预运行测试，系统能独立执行预设巡检任务，并提供巡检结果反馈；
- b) 动态调整巡检计划，系统能适应任务调整；

注：巡检计划包括巡检频率、巡检事项等。

- c) 模拟现场异常，系统能及时识别并自动生成报警信息；
- d) 通过平台远程发出测试指令验证，现场设备能正确响应远程命令并支持参数修改、模块测试等操作；
- e) 在设备状态和负载波动条件下进行动态巡检调度测试，系统能根据实时情况调整巡检任务的优先级与频次。

8.2.4 东西向巡检应符合下列规定：

- a) 设置需要多个设备协同完成的巡检任务，系统能根据设备状态、位置及负载条件安排任务分配并保持进度一致；
- b) 向系统连续下发多批巡检指令或降低系统运行频率、暂停系统任务，系统能动态分配任务，调整任务执行路径和设备协作方案；
- c) 设定不同类型的巡检任务，系统能根据任务紧急程度、设备能力匹配情况，自动做出任务分派决策。

注：不同类型的巡检任务包括周期性任务、临时应急任务、优先级不同的计划任务等。

8.3 安全测试要求

8.3.1 设备接入安全测试应符合下列规定：

- a) 模拟系统向设备下发控制指令，使用国密算法 SM2 进行签名，校验设备是否返回验签结果，并且模拟使用错误密钥签名，校验设备是否返回异常结果，检查系统是否执行保底策略；
- b) 使用一台设备模拟接入情况，校验系统是否能获取签名串和原文，并且使用国密算法 SM2 进行验签。模拟设备使用错误的密钥时，检查系统验签失败后是否输出告警通知，并执行保底策略措施；
- c) 检查系统和设备是否可以向密码平台申请密钥证书，确保接口的连通性，检查密钥证书的申请、分发、更新和撤销流程是否顺畅；
- d) 模拟系统调用密码平台的接口进行数据加密和解密操作，检查是否能返回正常的加密和解密结果；
- e) 检查系统是否具备使用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，模拟系统用户使用相应的下发控制功能，检查是否具备权限限制功能；
- f) 检查系统进行控制命令操作时的通信消息中是否包含时间戳和随机数等安全特征，模拟攻击者尝试篡改消息内容或时间戳，检查系统是否能有效检测和拒绝这些篡改后的消息。

8.3.2 系统部署安全测试应符合下列规定：

- a) 模拟其中一台主服务器强制断电或者断网等异常情况，验证备用服务器是否立即接管相应服务；
- b) 通过测试工具进行压力测试，模拟并发请求，测试主备设备是否均衡地负担了相应请求响应处理。模拟主服务器被人为关闭、强制中断等情况，发送的请求是否被备用设备承载；
- c) 模拟硬件设备出现内存占用过高、CPU 负载过高或磁盘空间不足等运行异常情况，验证系统是否及时发出告警通知，并自动发送短信或邮件通知相关人员；
- d) 检查系统相关的网络连接是否配置了双配置，并通过独立的设备、不交叠的网络链路实现数据可靠传输。模拟其中一条网络链路出现故障，验证另一条链路是否能继续传输数据。

8.3.3 系统数据安全测试应符合下列规定：

- a) 检查系统数据是否对敏感信息进行存储加密，使用 SM2、SM3 等国密算法对加密数据进行解密测试；
- b) 模拟不同角色人员访问系统数据，检查其是否能访问或修改与其权限相匹配和不匹配的数据；
- c) 模拟系统人员对数据进行访问和修改，检查系统是否提供日志记录功能，记录访问过程、访问者、操作内容、操作时间等日志，并且具备对异常操作进行标识和提示的功能；
- d) 检查系统是否具备对敏感数据进行验证来源和完整性的能力，例如通过数字签名和哈希函数方式验证；
- e) 检查系统是否具备数据定期备份功能，模拟数据丢失情况下使用备份数据进行还原，验证还原数据是否可用，并验证数据是否具备防篡改能力；
- f) 检查系统是否为集群部署，模拟其中一个节点再来故障，系统是否能继续提供数据访问、数据维护功能；
- g) 模拟紧急情况下测试授权人员能否绕过正常的访问控制限制，快速获得对关键系统或数据的访问权限，并检查是否遵守最小权限原则，是否过度暴露敏感数据，同时检查业务功能和系统是否可用。