

T/CASME

中国中小商业企业协会团体标准

T/CASME XXXX—XXXX

太阳能光伏发电智能云系统数据通信技术 规范

Technical specification for data communication of intelligent cloud system for solar
photovoltaic power generation

征求意见稿

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中国中小商业企业协会 发布

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。

本文件由广东威阳科技有限公司提出。

本文件由中国中小商业企业协会归口。

本文件起草单位：广东威阳科技有限公司、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX。

太阳能光伏发电智能云系统数据通信技术规范

1 范围

本文件规定了太阳能光伏发电智能云系统（以下简称“智能云系统”）数据通信的总体要求、数据的技术、通信协议、数据通信安全要求、通信接口要求以及网络安全的内容。

本文件适用于太阳能光伏发电智能云系统中涉及数据通信的设备研发、系统集成等相关环节。

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 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20273-2019 信息安全技术 数据库管理系统安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 40104-2021 太阳能光热发电站 术语

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 860（所有部分） 电力自动化通信网络和系统

YD/T 3865-2021 工业互联网数据安全保护要求

3 术语和定义

GB/T 40104-2021界定的以及下列术语和定义适用于本文件。

3.1

太阳能光伏发电智能云系统 intelligent cloud system for solar photovoltaic power generation

集成了太阳能光伏发电场现场设备、通信网络以及云端计算和存储资源的综合性系统。系统通过在光伏电站现场部署的各类传感器、数据采集设备收集光伏组件、逆变器、汇流箱等设备的运行数据，通过通信网络（有线或无线方式）传输至云平台，云平台对数据进行存储、分析和处理，实现对光伏电站的远程监控、故障诊断、发电功率预测、运行优化等功能。

4 总体要求

4.1 智能云系统数据通信的接口和协议应具有通用性和开放性。

4.2 数据通信安全应满足 GB/T 20271、GB/T 22239 和 GB/T 25070 的要求。

4.3 智能云系统内相关设备应具有唯一设备编码。

4.4 应支持双机冗余运行，提高运行可靠性。

5 数据通信技术要求

5.1 通信数据

5.1.1 数据采集

- 5.1.1.1 数据采集应支持采集量测数据的时标、品质信息、支持数据时标和品质信息的存储与远传。
- 5.1.1.2 应支持双网冗余运行方式，主链路出现故障时，应能够自动进行备链路的切换。
- 5.1.1.3 采用 DL/T 860（所有部分）通信时，双网冗余连接应支持同一报告实例号。

5.1.2 数据处理

- 5.1.2.1 智能云系统应支持采集信号的检修状态处理，正确识别采集信号的检修品质位。
- 5.1.2.2 智能云系统应支持通信中断处理，将汇集的相关数据置可疑品质位，通信中断恢复后应对相关设备进行数据总召唤。
- 5.1.2.3 应支持采集数据品质与传输协议数据品质转换。
- 5.1.2.4 在光伏电站处于峰值发电状态或进行大规模数据采集（如启动全面巡检）时，系统应能自动调整传输速率，保证数据不丢失且传输时延在可接受范围内。
- 5.1.2.5 对于实时性要求较高的控制指令数据（如逆变器的功率调节指令），从云平台发出到现场设备接收并执行的传输时延应不超过 200 ms，以保证系统的快速响应能力，确保电站的稳定运行。
- 5.1.2.6 对于设备运行状态数据的上传，从现场设备检测到故障到云平台接收到完整信息的时延不应超过 200 ms，以便运维人员能够及时获取故障信息并采取相应措施。
- 5.1.2.7 历史数据的查询请求从云平台发出到相应数据返回的时延，不应超过 500 ms，使用户能够及时获取所需的历史数据用于分析。

5.2 通信可靠性要求

5.2.1 冗余设计

- 5.2.1.1 光伏电站与云平台之间应建立至少两条独立的通信链路，链路切换时间应 ≤ 10 s。主链路正常工作时，系统使用主链路进行数据传输；当主链路出现故障时，系统应能自动切换至备用链路，确保数据通信不中断。
- 5.2.1.2 在云平台端，通信服务器应采用冗余配置，包括硬件冗余（如双电源、多处理器等）和软件冗余（如热备份的操作系统和应用程序）。

5.2.2 故障恢复时间

- 5.2.2.1 系统应在检测到故障后自动切换到备用通信链路，并在 5 min 内尝试自动恢复主链路通信。若自动恢复失败，应及时向运维人员发出警报，并提供详细的故障信息，以便人工干预修复。
- 5.2.2.2 在通信设备出现故障的情况下，对于可自动修复的故障，设备应具备自动重启并恢复正常运行功能；对于需要人工维修的硬件故障，从故障报警到运维人员完成维修并恢复设备通信功能的时间不应超过 0.5 h。

6 通信协议

6.1 通用通信协议

6.1.1 TCP/IP 协议

在太阳能光伏发电智能云系统中，TCP/IP协议作为网络层和传输层的基础协议，用于实现设备之间的互联互通。在现场设备与通信网关之间，以及通信网关与云平台之间的网络通信中，IP协议负责为每个设备分配唯一的网络地址，确保数据能够准确地在网络中路由；TCP协议则用于建立可靠的、面向连接的通信通道。

6.1.2 HTTPS 协议

应用于云平台与用户终端（如 Web 浏览器、移动 APP）之间的通信。云平台通过HTTPS协议向用户提供数据查询、系统配置等服务接口。用户通过发送HTTPS请求获取光伏电站的运行数据、历史报表等信息，或者向云平台提交设备控制指令、参数修改请求等。。

6.1.3 其他通用协议

分布式的光伏电站监控系统中，传感器节点之间可通过MQTT协议进行数据交互，然后再统一将数据转发至通信网关。MQTT协议的消息主题设计应清晰明了，与光伏电站的设备和数据类型相对应。

6.1.4 协议版本兼容性

在系统升级过程中，通信设备和软件应支持向下兼容。当新设备接入系统或旧设备更新协议版本时，应能自动协商并选择双方都支持的最高版本协议进行通信，确保系统的稳定性和兼容性。

6.1.5 通信协议升级

6.1.5.1 在设备更新或系统扩展时，如涉及到通用通信协议的升级，应提前进行兼容性测试。

——TCP/IP 协议升级，重点测试新老版本设备在不同网络环境下的通信能力。

——HTTPS 协议升级，应检查新的接口定义和请求/响应格式是否与现有用户终端兼容，避免出现用户无法正常访问云平台的情况。

6.1.5.2 向用户发布协议升级通知和相关的操作指南，以使用户及时调整终端设备或应用程序的设置。

6.2 专用通信协议

6.2.1 协议栈结构

太阳能光伏发电智能云系统的专用通信协议栈分为多层。

——物理层：实现设备间的电气连接；

——数据链路层：将物理层接收到的数据进行成帧处理的；

——网络层：将数据从源设备路由到目标设备；

——传输层：上层应用提供可靠的端到端通信服务，支持面向连接和无连接两种传输模式；

——应用层：根据光伏电站的具体业务需求定义了各种数据类型和操作指令。

6.2.2 交互方式

6.2.2.1 专用通信协议与通用通信协议在系统中相互协作。主要交互方式如下：

a) 现场设备使用专用通信协议在本地网络内进行数据采集和设备间的初步通信。

b) 通信网关作为转换节点，将专用协议格式的数据转换为通用协议格式；

c) 通过广域网将数据传输到云平台；

6.2.2.2 云平台向现场设备发送控制指令时，过程相反，云平台将基于通用协议的指令发送到通信网关，通信网关再将其转换为专用协议格式的指令发送给目标现场设备。

6.2.3 转换机制

通信网关中应配置协议转换模块。当接收到专用协议数据时，根据映射表中的规则将数据字段提取并重新封装为通用协议的数据格式。在反向转换过程中，同样依据映射表将通用协议的指令和数据转换为专用协议格式，确保数据在不同协议之间的准确转换和通信的顺畅进行。

7 数据通信安全要求

7.1 数据加密

7.1.1 智能云系统通信的数据加密应符合 GB/T 39786-2021 第 5 章的要求。

7.1.2 传输的敏感数据应符合 GB/T 39786-2021 第 9 章的要求。

7.1.3 对于密钥交换和数字签名等操作，可采用非对称加密算法。在系统初始化和设备认证阶段，利用 RSA 算法进行密钥交换和数字签名，保证通信双方身份的真实性和密钥的安全性。

7.1.4 对于一些对加密速度要求较高但安全性要求相对较低的数据（如部分历史数据查询请求），宜使用轻量级加密算法。

7.2 密钥管理

7.2.1 密钥生成

对称加密密钥应在设备初始化阶段通过安全的随机数生成器生成。非对称加密密钥（如 RSA 密钥对）应使用专门的密钥生成工具生成，其中私钥应妥善保存在设备的安全存储区域（如硬件安全模块），防止泄露。

7.2.2 密钥分发

对于对称加密密钥，在现场设备与通信网关之间，可以通过预共享密钥的方式在设备部署阶段进行分发。

7.2.2.1 在通信网关与云平台之间，可以利用非对称加密算法（如 RSA）对对称加密密钥进行加密后再传输，确保密钥在分发过程中的安全性。

7.2.2.2 对于非对称加密的公钥，可通过数字证书的方式进行分发，数字证书由权威的证书颁发机构（CA）颁发，包含公钥和设备的相关信息，通过验证证书的有效性来获取公钥。

7.2.3 密钥存储

7.2.3.1 所有密钥在设备中都应存储在安全的存储介质中。

7.2.3.2 对于现场设备，宜采用具有加密功能的闪存芯片或硬件安全模块来存储密钥。

7.2.3.3 在云平台端，密钥应存储在具有高安全性的密钥管理系统中，该系统应具备访问控制、审计等功能，防止非法访问。

7.2.4 密钥更新

7.2.4.1 对称加密密钥应定期更新，更新过程应确保新旧密钥的平滑切换，避免数据通信中断。

7.2.4.2 非对称加密密钥的更新相对复杂，涉及到证书的重新颁发和更新，应根据证书的有效期和安全策略进行更新，同时要通知通信对端更新相应的密钥信息。

7.3 身份认证

7.3.1 用户身份认证

用户名及密码认证应符合GB/T 35273-2020第4章的要求。

7.3.2 设备身份认证

7.3.2.1 每个现场设备（如逆变器、数据采集器等）在出厂时都应具有唯一的设备标识。在设备首次接入系统时，设备将其标识信息发送到通信网关或云平台，系统对标识信息进行验证，确认设备是否合法。对于非法设备，系统应拒绝其接入，并记录相关信息。

7.3.2.2 设备在与通信网关或云平台通信时，应通过数字证书中的公钥和私钥对通信数据进行签名和验证，以证明自身身份。设备数字证书应由系统管理员或专门的证书颁发机构颁发，并与设备的唯一标识相关联，确保证书的唯一性和安全性。

7.4 访问控制

7.4.1 基于角色的访问控制

智能云系统应定义不同的用户角色，包括系统管理员、运维人员、普通用户等。

——系统管理员拥有最高权限，可以对整个太阳能光伏发电智能云系统进行配置、管理用户账户、查看和修改所有设备的运行参数等操作。

——运维人员主要负责光伏电站的日常维护，可以查看设备的运行状态、接收故障报警信息、执行设备的维护操作（如设备重启、参数调整等）。

——普通用户只能查看光伏电站的基本运行数据（如发电量、实时功率等），不能进行修改操作。

7.4.2 权限分配

根据角色定义，为每个角色分配不同的访问权限。

——系统管理员，对数据库的完全访问权、对通信设备和现场设备的配置权、对用户账户的创建和删除权等。

- 运维人员，对设备运行数据的读 / 写权限，如可以读取设备的实时和历史运行数据，在设备出现故障时可以写入控制指令进行修复操作，但不能修改系统的核心配置信息。
- 普通用户仅，具有对特定数据的只读权限，通过安全的查询接口获取所需信息。

7.4.3 数据访问审计

7.4.3.1 系统应记录所有的数据访问行为，包括访问时间、用户/设备标识、访问的数据类型、操作类型等信息。

7.4.3.2 审计数据应存储在专门的审计数据库中，存储格式宜采用关系型数据库中的表格形式或其他适合存储日志数据的格式。审计数据库应具备足够的存储容量和性能，以满足长期的数据存储和快速查询需求。

8 通信接口

8.1.1 现场设备与通信设备之间的接口宜采用控制器局域网、以太网或 RS-485。控制器局域网接口通信协议宜 CAN 2.0B；以太网和 RS-485 接口通信协议宜采用 Modbus。

8.1.2 通信设备与智能云系统通信接口应采用以太网，接口应采用双网冗余设计。以太网接口通信协议应符合 DL/T 634.5104、Modbus 或 DL/T 860（所有部分）的要求。

8.1.3 通信设备与智能云平台之间的接口速率应不低于 100 Mbps，对于大型光伏电站或数据传输量较大的系统，应采用 1000 Mbps 或更高速率的以太网接口，以满足数据的快速传输需求。接口应支持全双工通信模式，提高通信效率。

9 网络安全

9.1.1 采用 TCP/IP 以太网通信应采用网络安全防护措施，防护措施应包括但不限于身份认证、访问控制、数据加密或数据完整性保护。

9.1.2 大数据的安全应符合 GB/T 37973-2019 第 5 章的规定。

9.1.3 身份认证用密码设置应符合 GB/T 39786-2021 第 9 章的规定。

9.1.4 智能云系统中个人信息的安全应符合 GB/T 35273 的规定。

9.1.5 智能云系统数据安全保护范围应符合 YD/T 3865-2021 第 4 章的规定。

9.1.6 智能云系统数据的保护级别应符合 YD/T 3865-2021 第 9 章高重要性数据安全保护的要求。

9.1.7 智能云系统数据库管理的安全应满足 GB/T 20273-2019 第 7 章要求。