ICS 国际标准分类号

CCS 中国标准文献分类号

团　　体　　标　　准

T/CES XXX-XXXX

低压分布式光伏运行管理与调控信息安全导则

Guidelines for Information Security in the Operation Management and Dispatching of Low-Voltage Distributed Photovoltaic Systems

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电工技术学会　发布

目　　次

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》给出的规则起草。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会分布式电源运行与控制工作组归口。

本文件起草单位：中国电力科学研究院有限公司、华北电力大学、国网山东省电力公司、清华大学、国网河南省电力公司、内蒙古电力(集团)有限责任公司、河南许继仪表有限公司 、三未信安科技股份有限公司、清华四川能源互联网研究院、中电科网络安全科技股份有限公司等。

本文件主要起草人：冯云、翟峰、孙毅 、吴文传、李勇、孙树敏、段晓萌、梁晓兵、许斌、姜俊廷、朱亮 、陈岑、董坤鹏 、吴鹏、高飞、胡东方等

本文件为首次发布。

低压分布式光伏运行管理与调控信息安全导则

1 范围

本文件规定了低压分布式光伏接入在边界防护、通信信道防护、设备本体防护以及密钥管理四个方面的技术要求。

本文件适用于指导 10 kV 以下电压等级分布式光伏终端安全接入。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2019 信息安全技术 信息系统安全等级保护基本要求

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

3.2

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3

解密 decipherment/decryption

加密过程对应的逆过程。

3.4

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.5

密钥 key

控制密码算法运算的关键信息或参数。

3.6

身份鉴别 authentication

确认一个实体所声称身份的过程。

3.7

低压分布式光伏终端 low voltage distributed photovoltaic terminal

380V/220V 电压等级的分布式光伏发电相关设备，包括智能光伏逆变器、智能断路器、分布式光伏开关、通信规约转换器等。

3.8

台区采集装置 transformer district intelligent collection terminal

负责数据采集并上报的装置，包括集中器、智能融合终端、能源控制器等。

3.9

集群控制设备 cluster controller

负责接入汇集、密钥管理和光伏装置管理，实现对控制指令的上报和下发。

3.10

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.11

密码模块 cryptographic module

嵌入在设备内，实现安全存储、数据加/解密、双向身份认证、存取权限控制、线路加密传输等密码功能的硬/软件模块。

3.12

数字证书（或证书） digital certificate

经一个权威的、可信赖的、公正的第三方机构证书认证中心（CA）数字签名的包含公开密钥拥有者信息以及公开密钥的文件。

3.13

对称密码算法 symmetric cryptographic

加/解密使用相同密钥的密码算法。

3.14

非对称密码算法 asymmetric cryptographic algorithm

加解密使用不同密钥的算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.15

虚拟专用网络 virtual private network（VPN）

通过一个公用网络（可以是服务提供者IP、帧中继、ATM 主干网、Internet 等广域网）建立一个临时的安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

3.16

无线APN wireless access point name

无线运营商为企业提供的一种无线专线网络服务，网络通道有GPRS/CDMA/3G，同一无线APN 内的无线节点可以互相通信，不能和运营商网络内的其他节点通信。

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

VPN：虚拟专用网络（Virtual Private Network）

APN：无线专线网络服务（Wireless Access Point Name）

MAC：消息认证码（Message Authentication Code）

5 总体要求

5.1 防护原则

根据电力监控系统安全防护规定，低压分布式光伏作为具有监视和控制电力生产及供应过程的电力监控系统，安全防护坚持“安全分区、网络专用、横向隔离、纵向认证”的总体原则，低压分布式光伏网络与信息安全从边界防护、通信信道防护、终端防护以及密钥管理四个层次进行防护设计，实现层层递进，纵深防御。

5.2 防护目标

通过实现低压分布式光伏终端在接入过程中的安全技术应用防止低压电网系统网络瘫痪、业务数据丢失与篡改、信息泄密以及终端身份伪造假冒等安全风险。确保信息系统安全稳定运行，促进低压分布式光伏运行监控规范管理，保障低压分布式光伏终端的安全接入，支撑以新能源为主体的新型电力系统建设。

5.3 通用要求

通用要求包括以下内容。

a) 低压分布式光伏使用的密码技术、密码产品和密码服务应经过国家密码管理部门批准；

b) 低压分布式光伏运行管理与调控系统应根据其接入方式及对电网生产运行的影响程度，参照 GB/T 22239 确定网络安全保护等级；
c) 各级业务系统及终端设备的密码模块安全等级应参照 GB/T 37092 与系统定级要求相匹配；
d) 低压分布式光伏运行管理与调控系统的密码应用方案设计、建设及运行，应遵循 GB/T 39786 中与系统安全保护等级对应的技术要求与管理要求。

5.4 防护框架

结合低压分布式光伏终端接入实际应用情况，依据“分区、分级、分域”防护方针，确保低压分布式光伏终端安全有序接入。具体如图 1、2 所示。

5.4.1 非直连接入

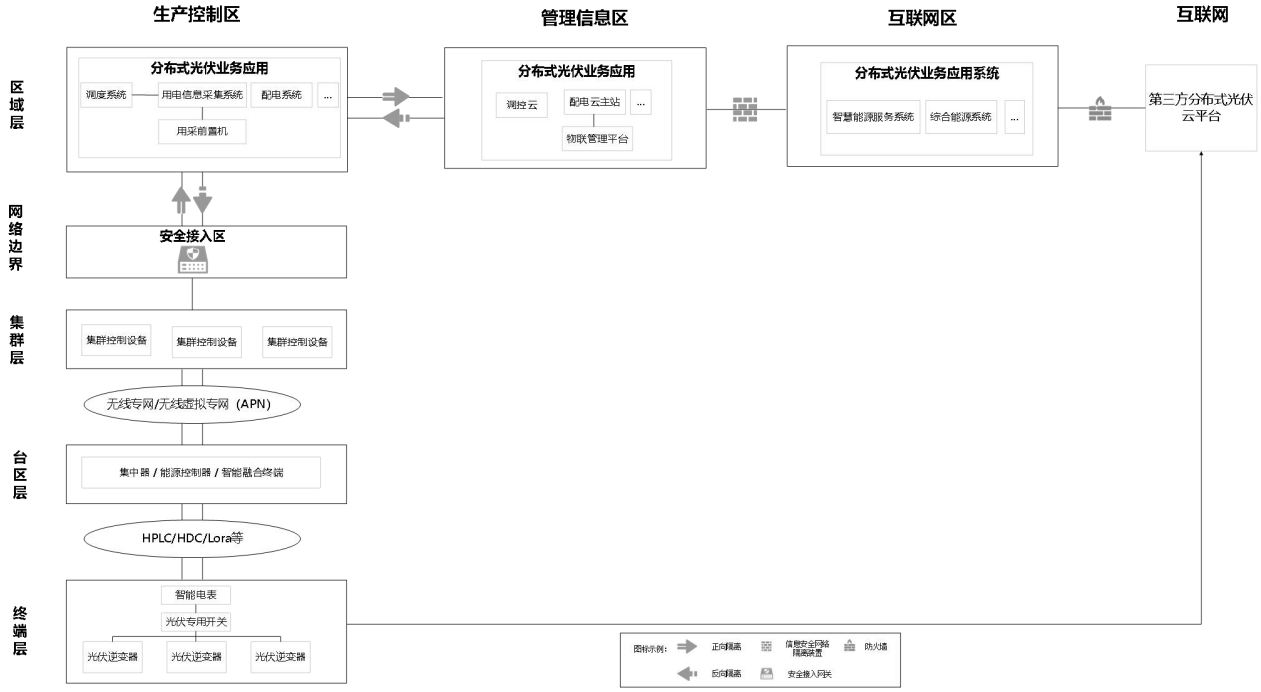

图 1　低压分布式光伏安全接入防护框架（非直连接入）

5.4.2 直连接入

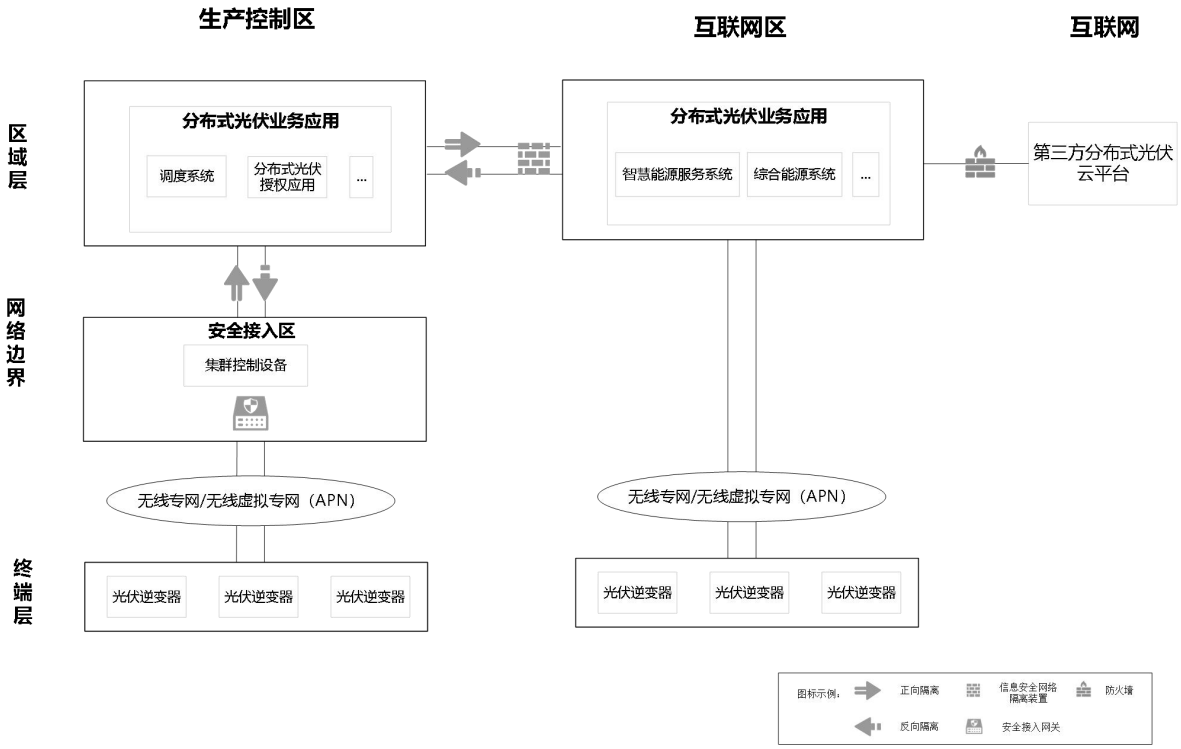

图 2　低压分布式光伏安全接入防护框架（直连接入）

6　边界防护

6.1　非直连接入

低压分布式光伏终端通过已有的电力线路将数据耦合传输到台区的集中器或融合终端，集中器再将数据上传至生产控制区主站业务系统。该接入方式主要分为终端层分布式光伏设备与台区层采集设备的安全边界、台区层采集设备与集群层集群控制设备的安全边界、集群层集群控制设备与区域层生产控制区业务系统的安全边界、第三方分布式光伏云平台与区域层互联网区业务系统的安全边界。如图 3 所示。

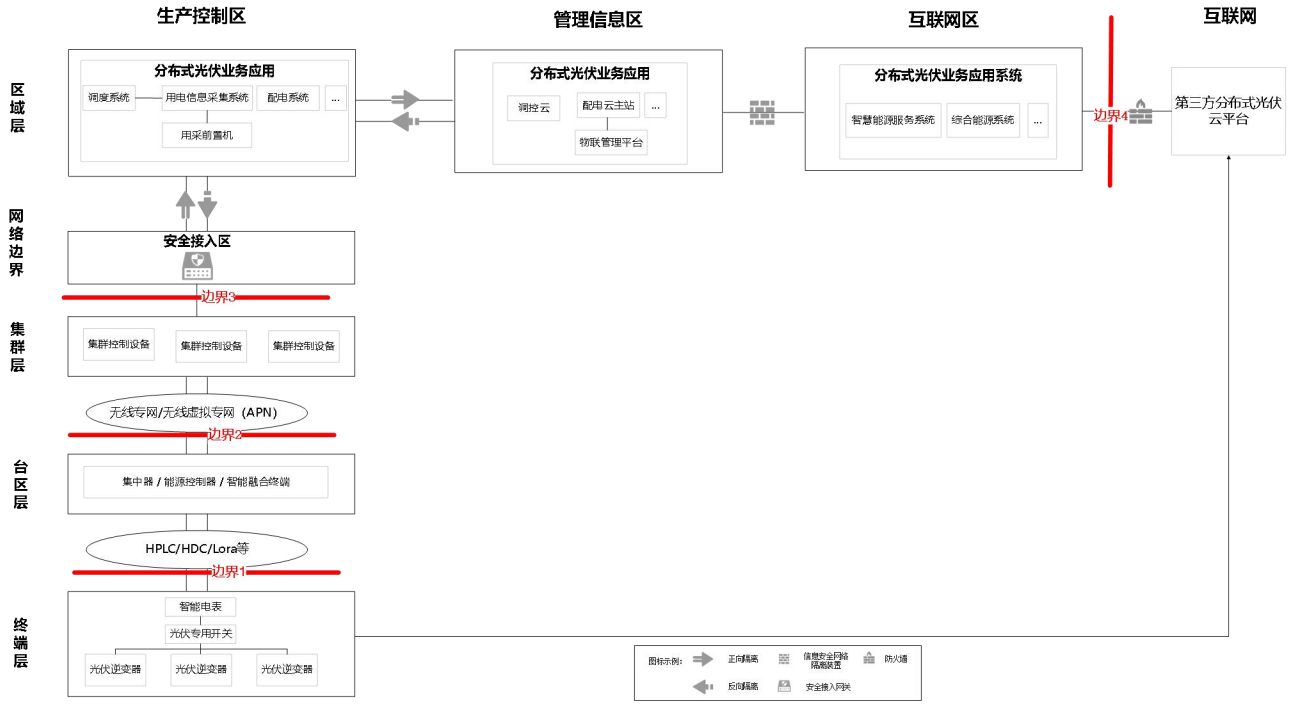

图 3　低压分布式光伏安全接入边界（非直连接入）

6.1.1　终端层与台区层边界 1

该边界主要指终端层低压分布式光伏设备与台区层采集设备之间的安全边界，相关安全防护措施主要包括终端设备与采集设备之间的交互对象和交互内容控制、数据的安全传输等。具体安全防护措施和实现的功能如表1所示。

表 1　终端层与台区层边界 1 安全防护

终端层与台区层边界防护内容	实现形式	配置方式	实现效果
交互对象和交互内容控制	白名单	在协议转换模组或者电能表上增加协议白名单和设备白名单	防止非法协议和非法设备与台区设备交互
数据传输安全	密码模块	基于光伏逆变器身份标识（设备唯一）等设备信息签发数字证书或生成无证书密钥，植入设备密码模块，并基于密码模块建立身份认证、数据传输加密及数据完整性校验机制	防止数据泄露、保证数据安全等

6.1.2　台区层与集群层边界 2

该边界主要指台区层采集设备与集群层集群控制设备之间的安全边界，相关安全防护措施主要包括用台区层设备与集群层设备之间的身份鉴别、数据的安全传输等。具体安全防护措施和实现的功能如表2所示。

表 2　台区层与集群层边界 2 安全防护

台区层与集群层边界安全内容	实现形式	配置方式	实现效果

身份鉴别	密码模块	为台区层采集设备签发数字证书或生成无证书密钥，并将密码模块安装于采集设备中，基于密码模块，完成设备接入身份认证。	实现台区层设备与集群层设备之间的身份鉴别
数据安全传输	密码模块	基于密码模块，台区层设备生成主密钥和协商群组加密密钥，实现数据传输加密及数据完整性校验机制。	防止数据泄露、保证数据安全等

6.1.3 集群层与生产控制区边界 3

该边界指集群层集群控制设备与区域层生产控制区业务系统之间的安全边界，相关安全防护措施主要包括边界网络通信实体身份鉴别、通信数据的机密性和完整性保护、边界网络访问控制信息的完整性等。具体安全防护措施和实现的功能如表3所示。

表 3 集群层与生产控制区边界 3 安全防护

集群层与生产控制区边界防护内容	实现形式	配置方式	实现效果
接入设备身份鉴别	安全接入网关	对集群层设备和生产控制区系统配置数字证书进行网络边界通信过程中的身份认证。	实现接入主体和客体之间身份鉴别
通信数据机密性和完整性保护	安全接入网关	采用 VPN 技术实现网络通信数据的机密性和完整性保护	实现通信数据包加密、通信信息完整性保护
边界网络访问控制信息完整性	安全接入网关	通过安全接入网关自身机制实现访问控制信息完整性保护。	实现通信过程中访问控制信息完整性保护

6.1.4 第三方系统与互联网区边界 4

该第三方分布式光伏云平台与互联网区业务系统之间的安全边界，相关安全防护措施主要包括边界网络通信实体身份鉴别、通信数据的机密性和完整性保护、边界网络访问控制信息的完整性、信息入侵检测、远程接入控制等。具体安全防护措施和实现的功能如表4所示。

表 4 第三方系统与互联网区边界 4 安全防护

第三方系统与互联网区边界防护内容	安全防护措施实现形式	配置方式	实现效果
接入系统身份鉴别	安全接入网关	对第三方聚合平台和互联网区业务系统配置数字证书进行网络边界通信过程中的身份认证	实现接入主体和客体之间身份鉴别
通信数据机密性和完整性保护	安全接入网关	采用 VPN 技术实现网络通信数据的机密性和完整性保护	实现通信数据包加密、通信信息完整性保护
边界网络访问控制信息完整性	安全接入网关	通过安全接入网关自身机制实现访问控制信息完整性保护。	实现通信过程中访问控制信息完整性保护
信息入侵检测	入侵检测系统	将互联网区第三方边界的流量映射至入侵检测探头所在的交换机端口进行入侵监测	检测发现隐藏于流经边界正常信息流中的入侵行为

6.2 直连接入

低压分布式光伏终端直接采集数据，并通过专网或公网经安全接入区传至生产控制区主站系统。该连接方式分为终端层分布式光伏设备与区域层生产控制区业务系统的安全边界、第三方分布式光伏云平台与区域层互联网区业务系统的安全边界。如图 4 所示。

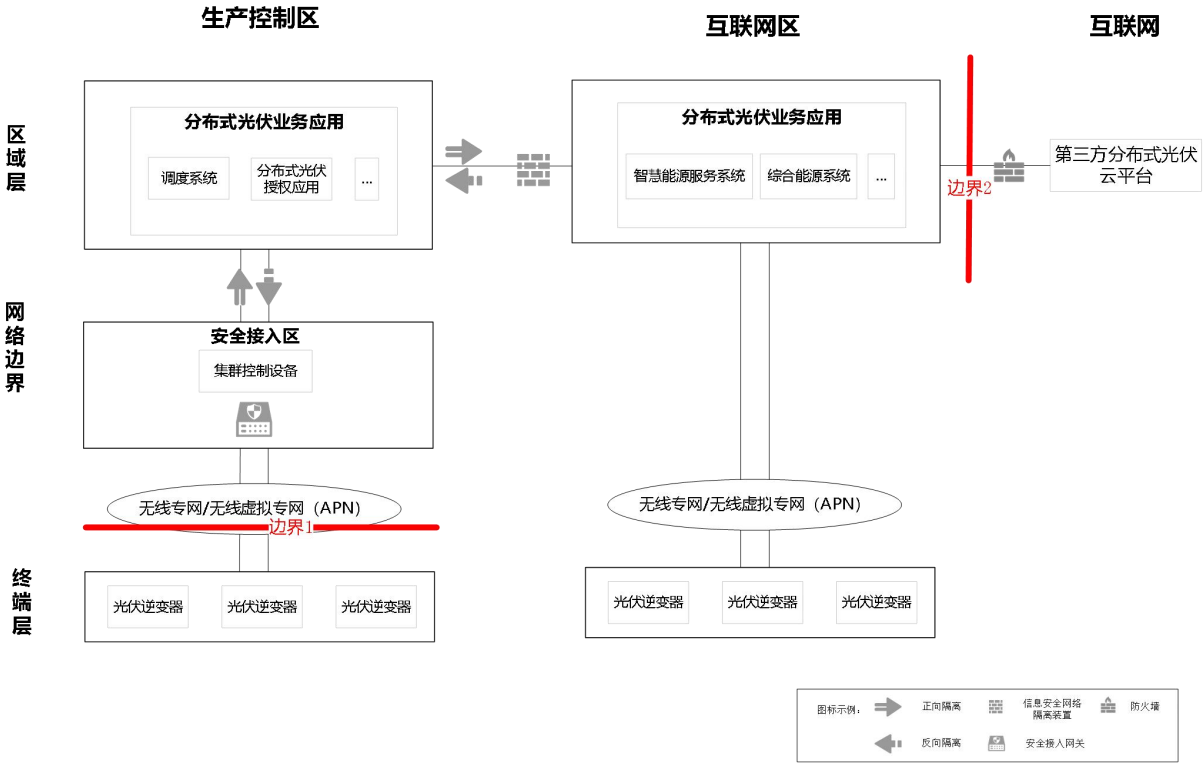

图 4　低压分布式光伏安全接入边界（直连接入）

6.2.1　终端层与生产控制区边界 1

该边界指终端层低压分布式光伏设备与区域层生产控制区业务系统之间的安全边界，相关安全防护措施主要包括边界网络通信实体身份鉴别、通信数据的机密性和完整性保护、边界网络访问控制信息的完整性等。具体安全防护措施和实现的功能如表5所示。

表 5　终端层与生产控制区边界 1 安全防护

终端层与生产控制区边界防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
接入设备身份鉴别	密码模块	基于光伏逆变器身份标识（设备唯一）等设备信息签发数字证书或生成无证书密钥，植入设备密码模块，基于密码模块，实现接入设备身份鉴别	实现接入主体和客体之间身份鉴别
通信数据机密性和完整性保护	安全接入网关	采用 VPN 技术实现网络通信数据的机密性和完整性保护	实现通信数据包加密、通信信息完整性保护
边界网络访问控制信息完整性	安全接入网关	通过安全接入网关自身机制实现访问控制信息完整性保护。	实现通信过程中访问控制信息完整性保护

6.2.2　第三方系统与互联网区边界 2

该边界指第三方分布式光伏云平台与互联网区业务系统之间的安全边界，相关安全防护措施主要包括边界网络通信实体身份鉴别、通信数据的机密性和完整性保护、边界网络访问控制信息的完整性、信息入侵检测、远程接入控制等。具体安全防护措施和实现的功能如表6所示。

表 6　第三方系统与互联网区边界 2 安全防护

第三方系统与互联网区边界防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
接入系统身份鉴别	安全接入网关	对第三方聚合平台和互联网区业务系统配置数字证书进行网络边界通信过程中的身份认证	实现接入主体和客体之间身份鉴别
通信数据机密性和完整性保护	安全接入网关	采用 VPN 技术实现网络通信数据的机密性和完整性保护	实现通信数据包加密、通信信息完整性保护
边界网络访问控制信息完整性	安全接入网关	通过安全接入网关自身机制实现访问控制信息完整性保护。	实现通信过程中访问控制信息完整性保护
信息入侵检测	入侵检测系统	将互联网区第三方边界的流量映射至入侵检测探头所在的交换机端口进行入侵监测	检测发现隐藏于流经边界正常信息流中的入侵行为

7　通信信道防护

7.1 通信方式

低压分布式光伏通信通道传输方式应满足要求如下：

a) 低压分布式光伏终端（如逆变器、数据通信棒等）与台区采集装置（如集中器、融合终端）之间的数据交互，可采用 RS485、电力线载波（HPLC）或微功率无线等本地通信方式。涉及控制类指令（如启停、有功/无功调节等）时，应优先采用电力线载波（HPLC）、RS485 等有线/电力线专用介质或采用微功率无线通信方式。
b) 低压分布式光伏终端与集群层集群控制设备、区域层生产控制区主站系统、新能源发电企业远程监视中心远程通信可采用光纤专网、无线通信网络方式进行数据交互。控制类指令应采用电力光纤专网、电力无线虚拟专网（4G/5G APN），并经过安全接入区进行数据交互。

7.2 协议安全

分布式光伏发电系统协议安全应遵循电力监控系统安全防护相关规定，根据通信链路的安防属性差异分级实施，要求如下：

a) 低压分布式光伏终端与台区采集装置之间应采用具备安全认证机制的通信协议进行通信，在通信链路建立阶段和报文下发阶段，基于国产商用密码算法实现应用层认证和数据加密，并在报文中增加时间戳、随机数等方式保证报文的时效性，防止重放攻击；
b) 低压分布式光伏终端与区域层生产控制区用采系统、新能源发电企业远程监视中心之间应采用以下防护：
    1) 网络层安全：在安全接入区边界部署安全认证网关，基于国产商用密码算法建立加密隧道，实现网络层的身份认证、数据加密和访问控制。

2) 应用层安全：在通信链路建立和控制报文下发阶段，控制指令的应用层报文应实现端到端的安全认证，在报文中基于密码技术生成的时间戳、随机数，保证报文时效性并防止重放。
3) 控制链路应采用集成了安全机制的通信协议，不应采用原生无安全机制的 MQTT 或 Modbus TCP 透传。

8 终端防护

8.1 集群控制设备

集群控制设备应满足以下要求：

a) 集群控制设备应加装密码模块实现安全功能，密码模块应满足 GB/T 37092 相关要求；

b) 集群控制设备应支持与交互对象之间进行身份识别，确保设备身份的真实性；

c) 集群控制设备应对传输的关键信息和敏感信息进行加密和完整性保护，确保通信数据的机密性和完整性；

8.2 台区采集装置

台区采集装置应满足以下要求：

a) 台区采集装置应安装密码模块实现安全功能，密码模块应满足 GB/T 37092 相关要求；

b) 台区采集装置应支持与交互对象之间进行身份识别，确保设备身份的真实性；

c) 台区采集装置应对传输的关键信息和敏感信息进行加密和完整性保护，确保通信数据的机密性和完整性；

8.3 低压分布式光伏终端

低压分布式光伏终端主要包括智能电表、智能断路器、分布式光伏开关、智能光伏逆变器等设备。低压分布式光伏终端防护应满足以下要求：

a) 低压分布式光伏终端应安装密码模块实现安全功能，密码模块应满足 GB/T 37092 相关要求；

b) 低压分布式光伏终端应支持与交互对象之间的身份识别、安全认证，宜支持关键信息和敏感信息安全加密传输；

8.4 安全审计

低压分布式光伏终端、台区采集装置及集群控制设备应具备基础安全审计能力，具体要求如下：

a) 设备应记录并本地存储以下安全事件日志：登录尝试（含成功与失败）、密钥更新操作、非法访问请求（被白名单或访问控制策略拒绝的记录）、时间同步异常事件；

b) 日志记录应包含事件发生的精确时间、事件类型、源 IP 或源设备标识、操作结果；

c) 日志数据应受到完整性保护（如存储时附加 MAC 校验），防止本地非授权篡改；

d) 日志数据存储时间不应少于 6 个月，并支持主站远程只读接口调用。

9 密钥管理

9.1 密钥类型

低压分布式光伏终端设备密钥类型如表 7 所示：

表 7 密钥类型

密钥种类	密钥类型	密码算法
低压分布式光伏终端设备身份密钥	非对称密钥	SM2 等国产商用密码算法
终端设备加密主密钥	对称密钥	SM4 等国产商用密码算法
传输数据加密密钥	对称密钥	SM4 等国产商用密码算法
传输数据完整性保护密钥	对称密钥	SM4 等国产商用密码算法

9.2 密钥全生命周期管理

低压分布式光伏密钥生命周期如表 8 所示：

表 8 密钥全生命周期

密钥	生成	存储	分发	更新	使用	销毁
设备身份私钥	密码模块内生成	存储在密码模块内	不涉及分发	设备初始化/根据生命周期更新	对身份信息进行签名	在密码模块内部销毁
设备身份公钥	密码模块内生成	以数字证书或无证书密钥形式存储	公开发布	设备初始化/根据生命周期更新	对身份信息进行验签	数字证书由 CA 机构撤销；无证书密钥由密钥分发中心标记注销
设备加密主密钥	在分布式光伏密码模块内生成	存储在密码模块内	不涉及下发	设备初始化时更新	加密本地存储的数据保护密钥	在密码模块内部销毁
传输数据加密密钥	通信主体之间协商生成	临时存放到终端设备中	不涉及密钥的分发	不涉及密钥更新	对传输数据做加密保护	一次一密，会话结束自动销毁。
传输数据完整性保护密钥	通信主体之间协商生成	临时存放到终端设备中	不涉及密钥的分发	不涉及密钥更新	对传输数据做完整性保护	一次一密，会话结束自动销毁。