

ICS 29.240.01
F 21
备案号: 68928-2019

DL

中华人民共和国电力行业标准

DL/T 1941 — 2018

可再生能源发电站电力监控系统 网络安全防护技术规范

Technical specification for cyber security protection of electric power system
supervision and control in renewable energy power station

2018-12-25 发布

2019-05-01 实施

国家能源局 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 缩略语	2
5 基本要求	2
6 结构安全	2
6.1 安全分区	2
6.2 网络专用	2
6.3 横向隔离	3
6.4 纵向认证	3
7 本体安全	4
7.1 系统安全	4
7.2 业务安全	4
8 对外接口安全	4
8.1 接入电力调度主站安全	4
8.2 接入集控中心系统安全	4
9 安全管理	4
9.1 设备安全管理	4
9.2 网络安全管理	4
9.3 运维安全管理	4
参考文献	5

前 言

本标准按照 GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则编写。

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这些专利的责任。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会（SAC/TC 82）归口。

本标准起草单位：南瑞集团有限公司、国家电网有限公司、中国南方电网公司、中国华能集团公司、国家电网公司华东分部、国家电网公司西南分部、国家电网公司西北分部、国网宁夏电力公司、国网山东省电力公司。

本标准主要起草人：梁野、陶洪铸、陶文伟、周劼英、曾荣汉、马骁、张亮、刘成江、高鑫、张宏杰、刘勇、张晓、汪明、苏扬、苏达、张赛楠、梁智强、孔红磊、张骞。

本标准为首次发布。

本部分在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

可再生能源发电站电力监控系统网络安全防护技术规范

1 范围

本标准规定了可再生能源发电站电力监控系统及网络边界安全防护要求。

本标准适用于并网电压等级在 10kV~35kV 范围的可再生能源发电站电力监控系统。

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 36572 电力监控系统网络安全防护导则

国家发展和改革委员会 2014 年第 14 号令 电力监控系统安全防护规定

国能安全〔2015〕36 号 电力监控系统 安全防护总体方案

3 术语和定义

下列术语和定义适用于本文件。

3.1

可再生能源 renewable energy

太阳能、风能、水能、生物质能、地热能、海洋能等非化石能源。

3.2

可再生能源发电站 renewable energy power station

利用可再生能源转换为电能的工厂，如风电场、光伏电站等。

3.3

可再生能源发电单元 renewable energy power generation unit

将可再生能源直接转换为电能的发电终端设备，如：风力发电机、太阳能电池板等。

3.4

集控中心 centralized control center

实现可再生能源发电站集中数据采集、监视、控制和管理，并且可以在线为调度和监控人员提供系统运行信息、分析决策工具和控制手段，保证发电系统安全、可靠、经济运行。

3.5

电力监控系统 electric power system supervision and control

用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备，以及作为基础支撑的通信及数据网络等。

3.6

生产控制大区 production control zone

由具有数据采集与控制功能、纵向连接使用专用网络或专用通道的电力监控系统构成的安全区域。

3.7

管理信息大区 management information zone

生产控制大区之外，主要由企业管理办公业务系统及办公网络构成的安全区域。

3.8

电力专用横向单向安全隔离装置 **lateral unidirectional safety isolating device for electric power**

部署在生产控制大区和管理信息大区之间，用于以非网络方式（物理隔离）实现单向数据传输，按照数据通信方向，电力专用横向单向安全隔离装置分为正向型和反向型。正向安全隔离装置用于生产控制大区到管理信息大区的非网络方式的单向数据传输，反向安全隔离装置用于从管理信息大区到生产控制大区的非网络方式的单向数据传输，是管理信息大区到生产控制大区的唯一数据传输途径。

3.9

电力专用纵向加密认证装置 **vertical encryption and authentication device for electric power**

部署在生产控制大区的广域网边界处，采用认证、加密、访问控制等技术措施实现电力监控系统数据的远方安全传输以及纵向边界安全防护的装置。

3.10

硬件防火墙 **hardware firewall**

实现两个区域间逻辑隔离、报文过滤、访问控制等功能的设备。

4 缩略语

下列缩略语适用于本文件。

AGC：自动发电控制（automatic generation control）

AVC：自动电压控制（automatic voltage control）

PMU：同步相量测量装置（phasor measurement unit）

5 基本要求

可再生能源发电站电力监控系统应严格遵循 GB/T 36572《电力监控系统安全防护规定》、信息系统安全等级保护的相关要求，构建以“安全分区、网络专用、横向隔离、纵向认证”为原则的安全防护体系。

可再生能源发电站总体安全防护架构如图 1 所示。

6 结构安全

6.1 安全分区

可再生能源发电站的电力监控系统应划分为生产控制大区和管理信息大区，生产控制大区根据对一次设备的影响可划分为控制区（安全Ⅰ区）和非控制区（安全Ⅱ区），重点保护生产控制以及直接影响电力生产（机组运行）的系统。

可再生能源发电单元测控模块通过无线通信方式接入生产控制大区时，应设立安全接入区。

可再生能源发电站电力监控系统的控制区包括发电站监控系统、升压站监控系统、AGC、AVC、PMU、五防系统等；非控制区包括电能量采集装置、继电保护信息子站、故障录波装置、状态监测系统等；管理信息大区包括气象预报系统、生产管理系统等。

6.2 网络专用

可再生能源发电站的电力调度数据网应在专用通道上使用独立的网络设备组网，在物理层面上实现与电力企业其他数据网及外部公共信息网的安全隔离，应划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。

可再生能源发电站的站内通信网络应采用光纤传输为主、无线传输为辅，确保数据传输安全可靠。

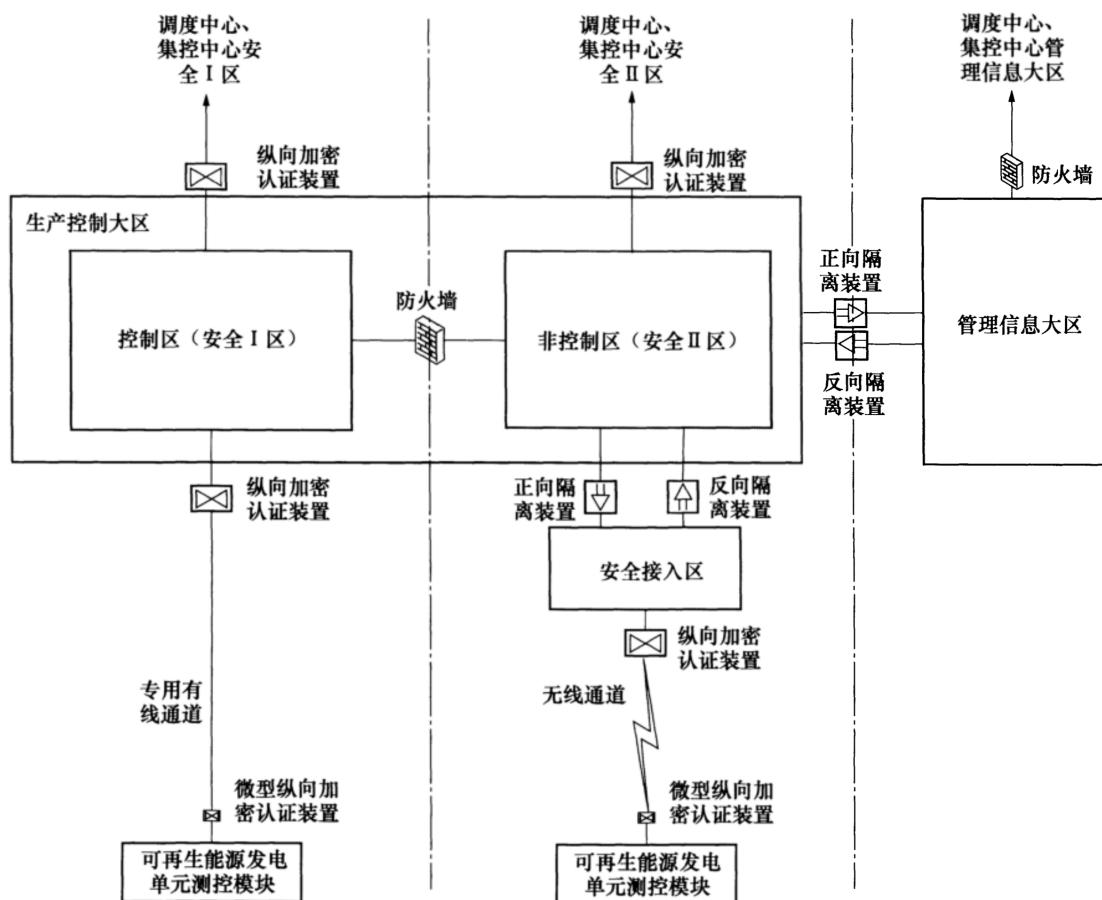


图1 可再生能源发电站总体安全防护架构

6.3 横向隔离

可再生能源发电站生产控制大区与管理信息大区之间，生产控制大区与安全接入区之间应设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

生产控制大区的控制区与非控制区之间应设置具有访问控制功能的网络设备、硬件防火墙或者相当功能的设备，实现逻辑隔离、报文过滤、访问控制等功能。

6.4 纵向认证

可再生能源发电站生产控制大区与调度数据网的纵向边界处应设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相应措施，实现发电站与调度主站的双向身份认证、数据加密和访问控制。

生产控制大区与其发电单元测控模块采用光纤方式通信，其纵向边界处应设置经过国家指定部门检测认证的电力专用纵向加密认证装置。

生产控制大区与其发电单元测控模块采用无线方式通信，应设立安全接入区。安全接入区与发电单元测控模块的纵向连接处应设置经过国家指定部门检测认证的电力专用纵向加密认证装置，应严禁任何无线通信功能设备绕过安全接入区接入生产控制大区。

可再生能源发电单元测控模块的纵向连接处应设置经过国家指定部门检测认证的电力专用微型纵向加密认证装置。

7 本体安全

7.1 系统安全

可再生能源发电站应对站内系统主机、网络设备、安全设备等进行安全监视，具备主机外设（USB 设备、串口设备、并口设备等）接入监控、网络设备接入监控，非法人员登录及操作监控等安全防范手段。

生产控制大区的主机应拆除或关闭软盘驱动、光盘驱动、USB 接口、串口等外部接口，禁止在生产控制大区和管理信息大区之间交叉使用移动存储介质以及便携式计算机。

7.2 业务安全

可再生能源发电站控制区的业务系统主机宜采用经国家指定部门认证的安全操作系统，并及时升级安全补丁，补丁更新前应进行充分的测试，禁止直接通过因特网在线更新。

生产控制大区的各业务系统应禁止以任何方式与因特网连接。

8 对外接口安全

8.1 接入电力调度主站安全

可再生能源发电站生产控制大区与调度主站的纵向边界处应设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施，与调度主站实现双向身份认证、数据加密和访问控制。

8.2 接入集控中心系统安全

可再生能源发电站与集控中心应建立独立的数据网实现可再生能源发电站自动化数据采集，不得影响各级调度数据网接入网设备正常运行，各接入网间不得互联。

可再生能源发电站与集控中心数据网传输通道应优先采用电力通信网络，如采用租赁运营商公网通信链路方式的，主备通道应采用不同运营商提供的通道。

9 安全管理

9.1 设备安全管理

可再生能源发电站生产控制大区的安全防护产品应获得国家指定机构安全检测证明，应禁止选用工信部、能源局等国家有关部门通报存在风险和漏洞的设备。在运设备存在风险和漏洞的，应按照国家要求全面落实技术和管理方面的加强措施，限期完成整改。

9.2 网络安全管理

可再生能源发电站应严格执行调度数据网运行管理规定，网络变更必须经上级调控机构审核同意。

调度数据网接入方案和安全防护方案，应经直接负责的电力调控机构审核同意，并严格执行调度数据网设备接入管理流程，未经审批不得擅自接入。

9.3 运维安全管理

可再生能源发电站应对厂家现场维护等第三方人员实施安全监控，严格控制其工作范围和操作权限。

生产控制大区应严格控制拨号访问和远程运维，确需使用的，应按照《电力监控系统安全防护总体方案》要求落实技术和管理措施，并实施严格监控和审计。

参 考 文 献

- [1] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
 - [2] GB/T 21028—2007 信息安全技术 服务器安全技术要求
 - [3] GB/T 21050—2007 信息安全技术 网络交换机安全技术要求
 - [4] GB/T 31366—2015 光伏电站监控系统技术要求
 - [5] NB/T 31071—2015 风力发电场远程监控系统技术规程
-

中 华 人 民 共 和 国
电 力 行 业 标 准
可再生能源发电站电力监控系统网络安全
防护技术规范

DL/T 1941—2018

*

中国电力出版社出版、发行

(北京市东城区北京站西街19号 100005 <http://www.cepp.sgcc.com.cn>)

北京传奇佳彩印刷有限公司印刷

*

2019年7月第一版 2019年7月北京第一次印刷

880毫米×1230毫米 16开本 0.5印张 14千字

印数 001—500册

*

统一书号 155198·1518 定价 15.00元

版 权 专 有 侵 权 必 究

本书如有印装质量问题,我社营销中心负责退换



中国电力出版社官方微信



电力标准信息微信

为您提供 **最及时、最准确、最权威** 的电力标准信息



155198.1518