# 变电站序列控制远方操作安全风险防治与管控

邹沛恒[1],代宇涵[2],郭 果[3],郑永康[2]
(1. 国网乐山供电公司,四川 乐山 614000; 2. 国网四川省电力公司电力科学研究院,四川 成都 610041;
3. 国网四川省电力公司,四川 成都 610041)

**摘 要:** 通过对变电站序列控制远方操作关键环节进行解析,梳理了顺序控制远方操作过程中的安全风险,同时从不同角度提出对应安全防护措施,着重阐述远方操作各环节安全风险以及防控措施。对强化顺序控制远方操作的流程风险与安全防控,保证变电站顺序控制的安全稳定执行,大幅缩短变电站操作占用时间,同时减少相关经济损失与社会影响有着重要意义。

**关键词:** 序列控制; 智能操作; 风险管控; 预演校验; 网络安全
**中图分类号:** TM63 **文献标志码:** B **文章编号:** 1003-6954(2019)05-0061-06
DOI:10.16527/j.cnki.cn51-1315/tm.2019.05.012

# Prevention and Control of Safety Risk in Remote Operation of Substation Sequence Control

Zou Peiheng[1], Dai Yuhan[2], Guo Guo[3], Zheng Yongkang[2]
(1. State Grid Sichuan Leshan Power Supply Company, Leshan 614000, Sichuan, China;
2. State Grid Sichuan Electric Power Research Institute, Chengdu 610041, Sichuan, China;
3. State Grid Sichuan Electric Power Company, Chengdu 610041, Sichuan, China)

**Abstract:** Through the analysis of the key links of remote operation of substation sequence control, the safety risks in the process of remote operation of sequence control are investigated, and the corresponding safety protection measures are put forward from different angles. The focus is on the safety risks and prevention and control measures in each link of remote operation. If the process risk and safety control of remote operation of sequential control are strengthened, it is of great significance to ensure the safe and stable execution of substation sequential control, greatly shorten the operation time of substations, and reduce the related economic losses and social impact.

**Key words:** sequential control; intelligent operation; risk management and control; preview check; network security

## 0 引 言

近年来随着调控一体化和变电站无人值守的推进,传统电网自动化、智能化程度的逐步提高,需要在调度主站、监控中心、变电站实现运行状态的快速转换。序列控制作为系统控制指令的序列处理方式,以一定时序及闭锁逻辑逐条发出校验指令,自动执行完成全部控制指令。将该技术运用在变电站设备倒闸操作中,可实现操作任务一键启动、操作步骤顺序执行、防误联锁智能校核、设备状态自动判别,从而实现变电站状态的一键转换。变电站序列控制(或称为变电站顺序控制或一键顺控)对于减少人工手动操作量,降低人员误操作概率,防止电网大面积停电事故,保障坚强智能电网的稳定运行有着重大意义。

依据国家电网公司运检部关于印发变电站一键顺控改造技术规范(试行)的通知,部分省份进行了变电站顺序控制试点,形成了一定的成功应用经验[3-5]。上述成功经验,大多是陈述顺序控制操作的具体实施方案和实际应用效果,少有涉及顺序控制远方操作全过程风险分析防治与管控的专项研究。

下面从顺序控制远方操作具体过程入手,对各

个环节进行对应的安全分析，以调端与站端通讯主流的 IEC104 通信规约为研究对象[6-8]，分析了目前顺序控制远方操作主要面临的安全风险和应对措施。其中操作环节安全风险，主要包括以下 3 方面：1) 调控主站与顺控场站在顺序控制远方操作交互过程中顺控配合失调，造成的操作失效甚至操作错误的风险；2) 主站在对单条线路连接的多端场站进行综合顺序控制时，命令有序执行的配合风险；3) 顺控场站遇到多个调控主站并发顺序控制远方命令时不当处理，造成操作异常中断甚至误操作的风险。针对上述远方操作安全风险，提出基于顺序控制操作命令展宽时间配合设定方法和调控主站命令并发预防与闭锁防范机制。

## 1 顺序控制技术架构简介及操作流程分析

智能电网调度控制系统顺序控制功能涉及调控主站、变电站监控系统以及数据传输等，技术架构如图 1 所示。

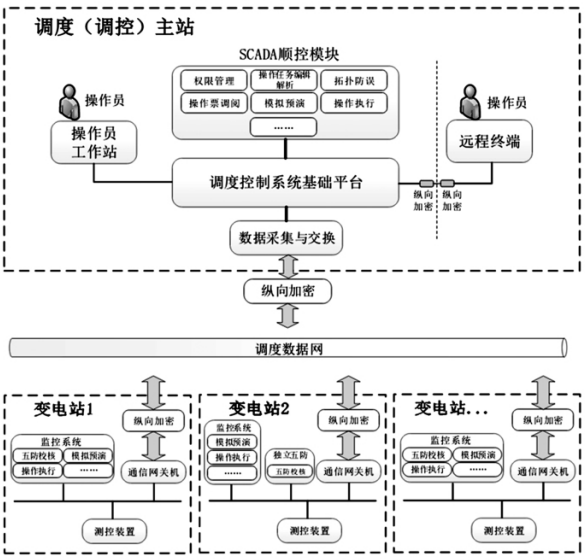


图 1　智能电网调度控制系统顺序控制功能技术架构

调控主站基于智能电网调度控制系统基础平台，实现 SCADA 顺序控制功能，主要包括权限管理、操作任务编辑解析、拓扑防误、操作票调阅、模拟预演、操作执行等功能。在操作员工作站或经过纵向加密网络延伸的远程终端上，发起顺序控制操作。操作命令在调控主站和变电站监控系统间进行交互，途经主站服务器、变电站通信网关机、变电站监控后台、智能五防系统等。借由变电站监控系统中的一键顺控功能模块，与独立五防系统、间隔测控装置配合完成顺序控制的预演、校验与执行。

1) 系统通讯方式

调度主站 SCADA 系统有 OPEN3000 系统与 D5000 系统 2 种，在此以 OPEN3000 系统为例进行分析。一键顺控在启动、调票、预演、校验、执行各阶段皆需要调度主站 OPEN3000 系统、智能五防系统及变电站后台监控进行信息交互。考虑到工程实施的规范性与通用性，建议与调度自动化 OPEN3000 系统之间接口可采用扩展了转发遥控功能的 DL/T 634.5104 规约通信，与智能五防主机建议使用 DL/T 634.5104 规约通信，若厂家相同可使用私有协议。

2) 一键顺控流程

一键顺控功能实现需要 OPEN3000 系统、变电站后台监控系统以及智能五防主机之间的顺控数据交互，从而实现 OPEN3000 系统与变电站顺控命令的传送与防误校验。顺控远动信号、遥控命令、防误校验信息交互流程如图 2 所示。

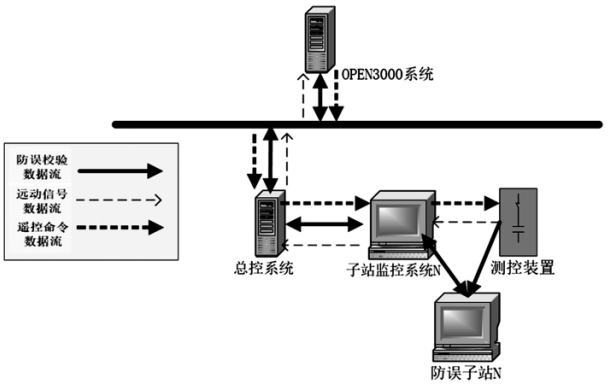


图 2　顺控信息交互流程

一键顺控功能包括顺控票管理和一键顺控操作执行两大部分，顺控操作先进行操作票固化，后开展操作对象的一键顺控操作。正常情况下，顺控过程中操作序列如果发生控制顺序错误，智能五防在校验后闭锁并否定返校。若遇到变电站端返回超时、通道短时间中断恢复等情况时，则启用操作指令的重发机制。重发次数可人工设置，若重发次数超出阈值且仍未收到变电站返回信息时，应终止操作流程并主动提示。调控主站、变电站监控系统均应配置上述重发、终止机制，保证顺序控制中的超时、中断情况的正确处置，及时重新发送操作指令或中止发送自动返回到正确状态，保证顺序控制全过程安全稳定。

## 2 顺序控制远方操作安全风险及防控分析

根据网络安全风险评估办法并结合国家电网公司运检部关于印发变电站一键顺控改造技术规范(试行)的通知与国家电网调度中心关于印发智能电网调度控制系统顺序控制功能规范的通知,具体对顺序控制功能远方操作系统构架与流程来进行风险辨识及评估,顺序控制远方操作主要考虑以下三大类安全需求,即网络信息安全、管理安全及操作流程安全。如表1所示。

表1 顺序控制远方操作安全需求

| 安全类型 | 薄弱环节 | 危险点描述 |
|---|---|---|
| 网络信息安全 | 隔离、加密装置 | 网络信息截取、窃听、篡改风险 |
| 管理安全 | 权限管理 | 操作人员权限管理等导致的误操作风险 |
| 操作流流程安全 | 主、子站顺控模块 | 主子站命令接收展宽配合失调导致的拒动、误动风险 |

### 2.1 网络信息安全

从网络通讯信息安全理论分析[9]可知,网络环境中的安全攻击分为主动攻击与被动攻击两种。主动攻击主要是通过篡改信息、伪造或采用DOS攻击达到欺骗用户、破坏网络、违规获取特权达到破坏目的。被动攻击相比于主动攻击不对数据信息做任何修改,主要是通过截取/窃听、破解数据流的方式在未经用户同意和认可的情况下获得相关信息与数据。通常情况下,可能同时遭受主动与被动方式相结合的混合攻击。

网络环境下主要通过网络隔离、防火墙加固、数据加密、双因子认证、强制访问控制及三权分立等措施防御攻击。国家电网公司规定电力网络中的信息按照安全需求应采用业务网络分区与信息多维防护等措施来提升网络安全水平。结合顺序控制远方操作信息传输环节,主要应在横向隔离、纵向加密、发起控制等方面采取针对性的安全措施,具体措施如下:

1) 纵向加密运用非对称加密算法对在生产大区中传输的主子站顺序控制交互信息进行非对称算法加密与解密,在通信通道上完成信息的密文传输,保证信息的安全性与保密性,预防信息被截取或窃听后恶意利用;

2) 横向隔离运用在顺序控制信息涉及的不同网络区域间,通过隔离装置的横向阻隔作用,保证网络中跨区域的信息交互和数据访问都经过了授权与管控,避免出现非法的流程连接与访问;

3) 发起控制在调度主站和场站监控上进行功能部署,只允许具备权限的用户调用符合既定规则的顺序操作票,不符合上述规则的请求不允许发起命令与执行。发起控制从命令发起源上避免了无权限的用户的非法控制和有权用户的违规操作。

### 2.2 管理安全

针对管理风险,通过对此类风险进行风险识别,防范非法用户登录操作或操作流程不规范等风险。主要采用人员多重认证、权限管理机制、双人双机监护等措施。其中:

1) 人员多重认证。提供基于调度数字证书、用户和密码、指纹、人脸识别等鉴别技术的两种或两种以上组合方式对用户身份进行鉴定。通过对操作人员的多重认证,保证实际操作人员操作权限的合法性。

2) 权限管理机制。支持完善的权限管理机制,按照省地县操作权限,只允许各层级单位授权用户登录维护操作。并对操作用户进行双重鉴别与细化管理,确保操作的安全可靠。

3) 双人双机监护。按照双重监护、多重验证的要求,人员必须经过可靠验证后才可执行操作。操作发起前应核对监护信息涵盖的操作场站、操作设备、设备源态和目标态等信息,并落实操作、监护分离核实制度,避免单独操作导致的误操作。建设系统监护信息场站、设备、源态、目标态的核实纠错功能,让系统记录每一项操作工作对应的操作、监护人员,保证顺控操作具有可追溯与逆向分析功能。

### 2.3 操作流程安全

顺序控制远方操作包括设备“运行”、“热备用”、“冷备用”3种状态转换,由于受到网络攻击后可能产生状态的错误转换或非完全转换,对于运行的电力系统是非常严重的事故,严重威胁电网整体的稳定安全。分别从调控主站发起的顺序控制操作包含的两种不同模式(综合控制和分步控制模式)进行操作流程安全分析。综合控制模式下,站端会对调度综合控制指令进行解析,利用下发的预置指令包含原始调度操作指令这一特点,采用操作执行或撤销复验操作预置返校信息的方式确保流程安全。分步控制模式下对操作过

程环节关键信息进行校验，并加入人工确认与执行步骤，采用主动校验调度下令信息与变电站端反馈信息一致性的方式确保流程安全，并增加异常操作终止与错误主动提示机制。

## 3 顺控操作流程风险分析及应对措施

顺控操作流程风险主要是主子站顺控配合、单主站多场站操作并发、多主站单场站操作存在的风险。

1) 主子站顺控配合失调风险

分析顺序操作流程，错误的操作序列可通过操作预演与五防闭锁进行识别和中止。操作异常延时或响应可通过操作命令重发或重发次数阈值机制以降低网络延时影响与操作中断复启动。在这样的操作模式下，调控主站的命令重发总时长与子站网关机、顺序主机设置的命令接收展宽时长的配合尤其重要。

当调控主站设置的命令重发总时长与子站网关机、顺控主机设置的命令接收展宽不匹配时，远方操作就有可能发生误动作，如图 3 所示。

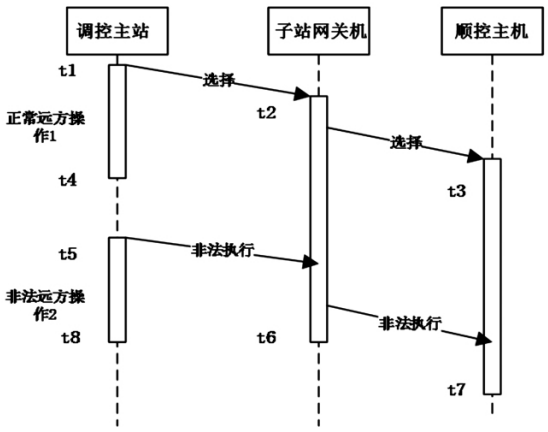


图 3 主子站顺控配合失调导致误操作风险分析

①预置命令：主站按照实际顺控操作情况需要对变电站内某间隔进行状态转换操作，在 t1 时刻启动正常流程的顺控命令，子站网关机在 t2 时刻接受命令，顺控主机 t3 时刻正确接收命令经过模拟预演后上送操作预置返校结果，等待主站下发执行命令。

②执行超时：在网络异常情况下，调控主站程序未正常下发执行命令或者网络原因导致命令未如期到达，按照正常流程全启动操作指令的重发机制。若重发次数超出阈值仍未收到返回信息，调控主站的远方操作应在在 t4 时刻超时退出，所以正常情况下子站网关机接收展宽( t2 – t6) 与顺控主机的执行展宽( t3 – t7) 只应略大于调控主站的命令启动、重发时长( t1 – t4) ，从而达到执行超时情况下自动终止命令执行。

③误操作：若子站网关机命令接收展宽与顺控主机命令执行展宽设置过长，由于网络拥堵造成在 t5 – t8 时段顺控命令重发或因受到攻击造成非法的执行命令发送，同时子站网关机接收展宽( t2 – t6) 与顺控主机执行命令展宽( t3 – t7) 设置过长，导致本该中止的命令被顺控主机下发执行，此时就产生了误操作。

同理，如果子站接受、执行命令展宽设置比主站发送命令展宽短，有可能产生正常顺控命令无法执行或执行成功率低的情况。因此针对主子站顺控配合失调的问题，调控主站、子站网关机、顺序主机三者设置的命令展宽应该是合理的逐级递增。

2) 单主站多场站操作并发风险

某些特殊情况下，线路运行状态的转换涉及电能收发两端的场站的顺序控制配合，当线路存在 T 接时还会有更多场站的配合。针对多场站协调顺序操作风险，应按照顺序控制操作规则检验多站顺控票的安全性、合理性，预先向涉及场站下发顺控预置锁定命令，避免相关变电站接收其他主站顺控命令或同主站的其他顺控命令。同时严格预演、校验、执行、回复机制，每执行下一步操作时都应校验先前执行步骤是否已到位，利用全步骤、全流程校验机制保证顺控命令执行的安全性、可靠性。

3) 多主站单场站操作风险

场站应设置多主站顺序控制防范机制，同一时刻只允许单个调控主站进行顺序操作，其他调控主站的操作指令应被闭锁或进入排队机制。为进一步防范多主站操作风险，变电站在接收到主站的顺序操作启动命令后，应锁定命令接收方，若中途接收到其他主站的顺序控制信号应丢弃错误操作指令，继续锁定、执行原主站操作流程。

## 4 工程试点情况

针对上述流程安全分析情况，为了验证相关技术安全措施的有效性，理顺顺控研发思路，检验操作校验原则，在四川攀枝花 220 kV 禹王宫变电站、110 kV 平地变电站与眉山 110 kV 龙亭变电站、110 kV 铝

城变电站进行顺控试点工程实践，以 220 kV 禹王宫变电站（该站为智能变电站，监控系统为南瑞科技 NS3000，全站 2 台主变压器、4 把中性点接地开关、220 kV 侧为双母单分段运行、4 个出线间隔，110 kV 侧为双母运行、6 个出线间隔，35 kV 侧为双母运行、10 组电容器，2 个站用变压器为例，对该站 110 kV 母联 112 断路器进行现场顺控操作实验。

1）网络信息安全情况

根据顺控网络安全要求，发起控制命令前需预先检查命令发起者身份，同时兼具密码、调度证书双重认证。为了验证顺控系统是否符合网络信息安全要求，我们用不具有控制权的用户发起 220 kV 禹王宫站 110 kV 母联 112 开关冷备用转热备用顺控命令，系统提示“收到的系统报错 - 命令 - 条件 - 不满足”，命令中止。接着我们在未安装证书的主站端发起同样的顺控命令，系统提示“收到的系统报错 - 命令 - 条件 - 不满足”，命令中止。

2）管理安全情况

根据顺序控制远方操作流程，结合现场实际情况，制定了《智能电网调度控制系统顺序控制远方操作业务指导书》《智能电网调度控制系统顺序控制远方操作流程规范》《智能电网调度控制系统顺序控制远方操作监护管理规则》等规则、规范，强化变电站序列控制远方操作流程的规范性与安全性。

3）操作流程风险管控

顺控操作利用操作票预置、校验以及多主站操作互斥等安全技术手段保护远方操作流程规范性和安全性。以检验顺序操作票预置与校验机制为例，在 220 kV 禹王宫变电站 110 kV 母联 112 断路器Ⅰ母隔离开关合、Ⅱ母隔离开关分的状态下，顺控主站端发起错误的 110 kV 母联 112 断路器冷备用转热备用操作命令，提示“收到的防误系统报错 - 第 2 步 - 条件 - 不满足”，命令中止。以检验多主站操作互斥为例，在主调与备调以 1 s 的时差发起 220 kV 禹王宫变电站 110 kV 母联 112 断路器冷备用转热备用，备调提示“收到的系统报错 - 命令 - 条件 - 不满足”，备调操作中止，主调顺控操作正常执行。可以证明顺控命令发送至监控系统顺控模块后命令读写、执行流程可有效预防操作流程风险，具体流程如图 4 所示。

四川主子站顺序控制试点期间，上述变电站现场运行稳定，顺序控制命令发起、操作票调阅、操作

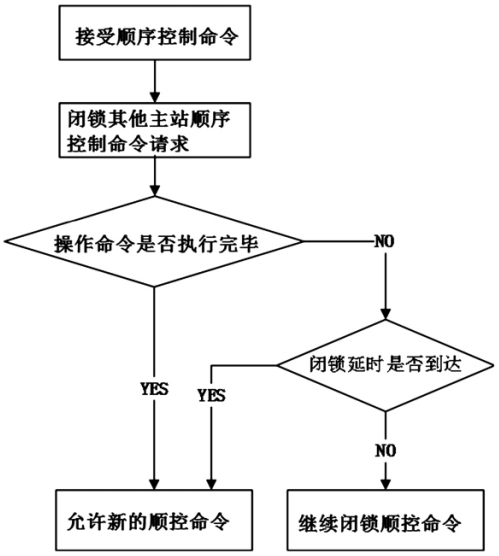


图 4　监控系统顺控模块读写顺控命令流程图

预演、五防校验、命令执行等功能正常，相关风险防控措施经测试验证安全有效。表明所提相关安全分析与风险防控措施正确、合理、有效、可推广，为远方顺序控制操作安全风险防控提供了部分理论基础和实践经验。

## 5　结　语

目前变电站序列控制改造正在全国大规模的推广，顺序控制的远方操作与安全风险防控值得深入研究。通过对顺序控制远方操作重要环节进行多维度分析，多角度阐述面临的流程、管理、操作风险并逐一提出对应的安全防控措施。保证顺序控制远方操作实际应用的安全与稳定，对实现变电站系统运行状态的快速转换，全面提升运行操作效率有着非常重要的意义。所研究成果应用在攀枝花 220 kV 禹王宫变电站、110 kV 平地变电站与眉山 110 kV 龙亭变电站、110 kV 铝城变电站顺序控制改造工程中，试点结果满足试点工作技术路线各项要求，变电站系统状态转换安全稳定。

### 参考文献

[1] 毛志强，熊倩，李彬，等. 智能变电站顺序控制技术应用研究 [J]. 山东电力技术，2016(12)：25 - 28.
[2] 韦会琪. 电力网络中的安全问题与防范对策思考 [J]. 中国新技术新产品，2016(23)：186 - 187.
[3] 言艳辉，刘坚. 变电站顺序控制的应用探究 [J]. 电工技术，2018(8)：48 - 49.

[4] 皮志勇,李勇,吴继雄,等. 变电站顺序控制的管理及技术研究 [J]. 科技创新导报,2017(19):13-15.
[5] 陈达文,李佳. 智能变电站顺序控制在站端的应用 [J]. 中国新技术新产品,2016(20):29-30.
[6] 王雷,史金伟. IEC 104 规约中程序化控制的扩展应用 [J]. 供用电,2012,29(4):52-53.
[7] 李国杰. IEC104 协议在变电站系统的应用与测试 [J]. 电力系统保护与控制,2004,32(1):43-45.
[8] 高雪飞. 基于 104 规约的远动网络通信可靠性原理探讨 [J]. 无线互联科技,2016(19):9-10.
[9] 郭国林. 基于网络通讯中信息安全的保障研究分析 [J]. 中国新通信,2017(6):15-16.

作者简介:
邹沛恒(1985),本科,从事电力系统继电保护工作;
代宇涵(1989),硕士,从事电力系统调度自动化技术工作。

(收稿日期:2019-05-28)

(上接第 60 页)

潮流约为 3×1000 MW;

⑥白鹤滩左岸电站—布拖(左岸换流站)4 回 500 kV 输送潮流约为 4×1250 MW;

⑦白鹤滩右岸电站—右岸换流站 4 回 500 kV 输送潮流约为 4×1250 MW;

⑧普提—洪沟 3 回 500 kV 输送潮流约为 3×360 MW。

上述 500 kV 输电线路导线截面为 4×400 $mm^2$/4×500 $mm^2$/4×720 $mm^2$(分别对应夏季热稳极限分别约为 2 GW/3 GW/3.9 GW)。因此,白鹤滩送端换流站丰小调峰运行方式下,近期西南电网完全可满足电网的热稳安全运行且有相当裕度。

2) 平枯水期随着水电出力的逐渐下降,整个川西南多回交直流外送通道输电容量整体亦随之降低,川西南外送电输电能力裕度相对更大,因此平枯期部分增加新能源(风电与太阳能)所发电力不会增加送电通道的输电压力,其所发电能完全可就近经接入川西南 220 kV 及以上主干电网逐级汇集升压后,再经金沙江二期的 2 回特高压直流输电平台外输区外电网。

总之,现有及规划川西南 500 kV 及以上交直流电网能适应丰期调峰运行及平枯期川西南更多富余清洁能源经 2 回金沙江二期直流输电平台外输区外电网。

## 5 结 语

上面根据金沙江二期 2 回特高压直流输电工程本身的特点与优势,结合白鹤滩水电站水电出力特性、"十四五"期新能源及四川电网电力规划发展状况等,提出了提升金沙江二期特高压直流外输电的电力举措:丰水期白鹤滩水电站参与四川电网调峰运行,金沙江二期特高压直流输电平台全年差异化接收四川电网部分富余清洁能源(季节性水电与新能源电量)。所提举措在既实现减少四川电网丰期大量弃水电量的同时,亦实现四川电网全年更多富余清洁能源外送,提高了金沙江二期 2 回 ±800 kV 特高压直流输电线路利用小时数。通过计算表明 2025 年丰水期可实现减少四川电网弃水约 5000 GW·h,可增加金沙江二期 2 回 ±800 kV 特高压直流输电线路年利用小时数约 470 h。

### 参考文献

[1] 国网经济技术研究院有限公司. 白鹤滩—江苏特高压直流输电工程预可行性研究 [R]. 北京:国网经济技术研究院有限公司,2018.
[2] 国网四川省电力公司. 四川"十三五"电网发展规划总报告 [R]. 成都:国网四川省电力公司,2015.
[3] 国网四川省电力公司. 2018 年四川电网运行方式 [R]. 成都:四川省电力公司,2018.
[4] 国网四川省电力公司. 2019 年四川电网运行方式 [R]. 成都:四川省电力公司,2019.
[5] 陈汉雄. 四川电网季节性电能外送曲线优化 [J]. 中国电力,2013,46(12):144-150.
[6] 陈汉雄. 水风互补四川清洁能源外送优化 [J]. 中国电力,2017,50(9):37-43.
[7] 陈汉雄. 四川电力发展对新能源建设规模影响分析 [J]. 四川电力技术,2018,41(2):46-50.

作者简介:
陈汉雄(1971),硕士,教授级高级工程师,从事电力系统规划设计及直流输电系统控制研究工作;
李晓明(1972),高级工程师,从事电网勘测设计。

(收稿日期:2019-05-24)