提高远程遥控安全性的 IEC 60870-5-104 规约扩展研究

朱海兵[1],吴 奕[1],陈 宁[2],朱志华[2],刘 翌[1],熊 浩[1]
(1.江苏省电力公司,江苏 南京 210024;2.国电南瑞科技股份有限公司,江苏 南京 210061)

摘 要:国家电网公司新的运行模式要求调控中心监控人员对变电站设备开展远程遥控。现有调度技术支持系统采用的 IEC 60870-5-104 规约在遥控命令传输和校验过程只校验点号信息,存在因点号对应关系错误导致误遥控的可能性。通过扩展 IEC 60870-5-104 规约,实现设备编号和点号的双重校验,以及测控装置 IP 校验,可以大幅降低因主站和变电站综自系统监控信息表点号不对应带来误遥控的可能性。

关键词:遥控;IEC 60870-5-104;规约;数据采集与监视控制系统
中图分类号:TM764.2 **文献标志码**:B **文章编号**:1009-0665(2014)06-0051-04

目前,调度控制中心主站系统与变电站综自系统的远动规约主要采用 IEC 60870-5-104 规约[1],它们传送的遥控命令中只包含遥控信息点号和遥控值,变电站综自系统接收到遥控命令后,只对遥控命令的遥控点号进行检验,只要判断到该点号存在,就进行遥控,一旦主站系统遥控点关联出错或站端系统遥控点出现与主站端系统发生不对应,就会有可能发生误遥控,这给自动化人员和调度监控人员都带来了极大的压力,也会给电网的安全运行带来威胁。《国家电网公司电力安全工作规程》对于现场操作防止误操作有完备的技术和管理措施,但远程遥控与现场操作和变电站后台操作具有很大的差异性,许多现场操作的防止误操作技术措施无法直接应用到远程遥控中,因此对于“大运行”模式下调度控制中心开展远程遥控需要因地制宜的研究防误技术和管理手段。

1 双重校验设计思路

目前调度控制中心对变电站断路器、刀闸等开合设备的远程遥控通过调度技术支持系统的数据采集与监视控制(SCADA)[2]应用来实现,整个过程包括“选择”、“返校”和“执行”。“选择”过程监控人员在 SCADA 客户端上输入遥控命令后,SCADA 应用根据遥控命令找到遥控对象对应的设备 ID,发至前置应用,前置应用服务根据设备 ID 和监控信息表找到相应的信息点号,然后使用 IEC 60870-5-104 规约将该信息点的遥控值(“0”和“1”)发至变电站综自系统的总控,传输过程只传输信息点号和遥控值,“返校”和“执行”过程同样只检验主站系统和变电站端综自系统信息表点号是否存在和是否可执行,并没有电气防止误操作逻辑。尽管主站系统和站端综自系统的信息表对应关系都经过运行维护人员的验收校对,但涉及到变电站局部改造时,并不对全站信息表进行核对,不能排除人为因素导致主站系统和站端综自系统信息表不对应的情况。如果出现这种情况,现有 IEC 60870-5-104 规约无法校验此种错误,可能会导致误遥控的发生。因此,有必要对现有 IEC 60870-5-104 规约传输校验机制进行改进研究,提高远程遥控的安全性。

收稿日期:2014-05-18;修回日期:2014-07-29

为了避免上述远程遥控过程潜在的安全隐患,本文从遥控校验机理和 IEC 60870-5-104 规约扩展性方面开展研究,提出建立遥控命令传输过程的双重校验机制。在现有 IEC 60870-5-104 规约仅传输和校验点号的基础上,对规约进行扩展,在遥控命令中增加设备编号或名称,同时对调控中心主站系统的 SCADA 和前置应用进行适当改造,对变电站综合自动化系统进行改造,扩充监控信息表,增加设备编号或名称,遥控命令传输和执行时,同时传输遥控点号和设备编号,校验时同时判断遥控点号和设备编号对应关系,同时校验测控装置的 IP 地址。

采用“宁可拒绝执行而减少误操作可能性”的原则,在命令传输和校验过程增加判断量,实现双重化校验,从而保证遥控命令的准确、可靠执行,大幅降低因主站和变电站综合自动化系统监控信息表点号不对应带来误遥控的可能性。

2 规约扩展实现方法

在现有 IEC 60870-5-104 规约基础上扩展遥控预置与执行报文结构,应用层引用 DL/T 634.5101—2002[3],主站系统下发点号时,能够将设备编号或名称一起下发。同时,返回错误码能够明确错误原因(点号与名称不一致、存在重复点号、无法校验等),并将原因返回给主站系统 SCADA 的遥控界面显示并告警。遥控的预置、执行都增加此校验环节,保证遥控命令的安全可靠执行。带名称校验的单命令类型标识[4]为 54,如图 1 所示。

校验信息为字符串,包含结束符。传输时校验信息

0	0	1	1	0	1	1	0	类型标识（TYP）	数据单元标识符在DL/T 634.5101—2002的7.1中定义
0	0	0	0	0	0	0	1	可变结构限定词（VSQ）	
在DL/T 634.5101—2002的7.2.3中定义								传送原因（COT）	
在DL/T 634.5101—2002的7.2.4中定义								应用服务数据单元公共地址	
在DL/T 634.5101—2002的7.2.5中定义								信息对象地址	信息对象
S/E		QU		0		SCS		SCO=单命令（在DL/T 634.5101—2002的7.2.6.15中定义）	
校验信息 n byte								校验信息（n 可利用报文长度计算得出）	

图1 带名称校验的单命令数据单元

按照实际的长度发送，校验信息字符串长度可由报文长度计算得出。IEC 60870-5-104规约中一帧报文的最大长度为255字节（包括起始字节和报文长度字节），去除报文的其他部分后，校验信息的最大长度239字节，119个汉字。校验信息一般可采用调度编号或调度命名。“选择”、“返校”、“执行”等遥控命令的ASDU信息格式[5,6]具体规定如图2—7所示。

36 H(TYPE)
01 H(VSQ)
06 H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
校验信息（n 个字节 ASCII 码）

图2 遥控选择

36 H(TYPE)
01 H(VSQ)
07 H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
返校出错信息（n 个字节 ASCII 码，返校成功时 n 为0）

图3 遥控选择返校

36 H(TYPE)
01 H(VSQ)
06 H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
校验信息（n 个字节 ASCII 码）

图4 遥控执行

36 H(TYPE)
01 H(VSQ)
07 H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
出错信息（n 个字节 ASCII 码，执行成功时 n 为0）

图5 遥控执行返校

36 H(TYPE)
01 H(VSQ)
08 H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
校验信息（n 个字节 ASCII 码）

图6 遥控撤销

36H(TYPE)
01H(VSQ)
09H(COT) 源发站地址
公共地址低字节 公共地址高字节
信息体地址低位 信息体地址中位 信息体地址高位
单命令选择
出错信息（n 个字节 ASCII 码，执行成功时 n 为0）

图7 遥控撤销返校

遥控开关编号可以是开关刀闸等设备编号，远动装置对遥控点号和开关编号进行一致性检验。遥控出口编码为遥控对象的相应变电站间隔装置的出口继电器编码，给远动和主站系统进行遥控真实出口校验，内容包含间隔装置地址和遥控对象序号，全站编码不重复，其中返校遥控出口编码必须由间隔装置返校信息自动生成，上送给调度再次进行核对。

间隔装置如果是网络通讯方式的，则遥控出口编

码方式为“［网络介质号:］IP 地址:遥控序号”,其中网络介质号可选。例如对接在远动网口“1”的 IP 地址为“192.168.1.2”测控装置上遥控对象“2”进行遥控,则遥控出口编码为“NET1:192.168.1.2:2”。

间隔装置如果是以串口、CAN 网等非网络方式通讯的,则编码为“[通讯介质号:]装置地址:遥控序号”,其中通讯介质号可选。例如对接在远动串口“1”的装置地址为“2”测控装置上遥控对象“1”进行遥控,则遥控出口编码为“COM1:2:1”。

遥控返校出错码定义如下:

“0” 为返校正确;

“1” 为调度下发选择命令遥控点号和遥控对象编码不一致,可能是调度遥控数据库出错;

“2” 为远动对调度下发遥控出口编码校核出错,可能是远动装置遥控数据库出错;

“3” 为间隔装置超时未返校,可能是远动和间隔装置通讯故障;

“4” 为间隔装置返校出错(就地 / 检修 / 闭锁 / 硬件出错等)。

3 主站系统和站端系统处理流程

3.1 主站系统处理流程

主站系统在遥控操作时,监控人员在厂站接线图上通过右键对设备进行遥控操作,在弹出的遥控操作界面上,监控人员需要再次输入所遥控设备的设备编号(以设备编号为例),程序会判断所输入的设备编号与所操作的设备的编号是否相同,如相同才允许继续进行遥控预置操作。主站系统的画面、SCADA 应用、前置应用间传输遥控命令时使用的是系统内部的设备 ID,前置应用在下发遥控命令时通过设备 ID 从数据库中取出设备遥控点号组装到遥控命令中,站端系统收到遥控命令后,根据命令中的遥控点号和站端预设的点号和设备的对应关系找到所要操作的设备,并对其进行控制操作。

主站系统在判断监控人员输入的设备编号正确后,需要将此编号与原有的 ID、状态等信息一并通过 SCADA 应用发给前置应用,前置应用在下发到站端的遥控命令时,需要再通过设备 ID 从数据库中取出设备所在测控装置的 IP 地址和遥控点号,并与遥控状态和设备编号信息按照新的遥控命令格式组装报文。站端系统在收到遥控命令后,先判断命令中的遥控点号、设备编号和测控装置 IP 地址与站端系统设置的是否一致。对应关系一致则继续,否则就返回出错信息给主站系统。主站系统在接收处理站端系统上送的遥控返校报文时,需要将站端系统上送的校核结果文本信息返送给画面,显示在主站系统的遥控操作界面上。

3.2 站端系统处理流程

传统遥控过程由站端系统前置通讯软件接到遥控命令,根据遥控点号从转发信息表中检索出相应的数据库遥控记录索引号(OID),然后通过 OID 检索出遥控设备对象的记录信息,根据该设备对象的记录信息属性,对测控装置进行相应的控制操作。在变电站一体化监控系统体系下,所有控制操作都是依据遥控设备对象数据库数据属性统一进行相应操作[7],因此在传统常规变电站,只要可靠地验证了该对象库正确性,基本就能保证站端系统对装置操作的正确性。在新型智能变电站,站控层网络是基于 IEC 61850 协议体系,由于强大的互操作性及丰富的扩展性能,让装置实现对带编号校核属性的遥控功能支持是能够实现的,这样就在整个遥控过程上的所有环节实现双重化校验,从而保证遥控操作的可靠性和惟一性。对于变电站一体化监控系统,可分别由总控对带编号遥控操作的校核和由总控和装置对带编号遥控操作的校核 2 种方案。

(1) 方案 1 实现流程:站端系统从主站系统下发的遥控命令信息中,在获取遥控点号的同时,也获取该遥控的校核信息,并将校核信息与该遥控的设备记录信息终端遥控别名域匹配和装置 IP 地址匹配,如果匹配不成功,返回主站遥控校核错误信息,若校核匹配成功即转为传统遥控流程操作。

(2) 方案 2 实现流程:监控系统从主站下发的遥控命令信息中,在获取遥控号的同时,也获取该遥控的校核信息,并将校核信息与该遥控的开关记录信息终端遥控别名域匹配和装置 IP 地址匹配,如果匹配不成功,返回主站遥控校核错误信息,校核匹配成功,再根据遥控开关对象将校核信息发送给对应装置,由装置根据本设备配置再次校核遥控编号信息是否正确,校核成功进行常规控制操作,否则就取消该控制操作,并将错误信息返回给一体化监控系统,再由一体化监控系统返回给主站。

4 结束语

现有 IEC 60870-5-104 规约传输遥控命令仅仅依据点号,主站系统和站端系统信息表一旦出现点号错位等不对应情况,很容易导致误遥控。通过规约扩展,实现点号和设备编号的双重校验,同时校验测控装置的 IP 地址,彻底消除了主站系统和站端系统的点号对应关系错误带来的误遥控可能性,是一种非常安全可靠的防误遥控改进技术,对于提高电网安全可靠运行水平具有重要意义。

参考文献:

[1] IEC 60870-5-104 规约(2000 版),采用标准传输协议子集 IEC 60870-5-101 网络访问[S]:50-60.

[2] 刘革辉,李 向,秦力军. IEC 60870-5-104 远动规约在 SCADA 系统中的应用[C]. 北京:2002 年全国电力系统自动化学术研讨会,2002:2-4.
[3] DL/T 634.5101—2002,基本远动任务配套标准[S]:30-32.
[4] 徐立子. 变电站自动化系统 IEC 60870-5-103 和 IEC 60870-5-104 协议的分析和实施[J]. 电网技术,2002,26(4):1-3.
[5] 黄云龙,郑 翔. IEC 60870-5-104 在调度自动化系统中的应用[J].上海电力学院学报,2005,21(4):326-328.
[6] 何 松,李育林. IEC 60870-5-104 规约应用分析[J]. 山西电力,2007(4):18-21.
[7] 李 晔,朱 江,吴 玲. 基于综合自动化系统的断路器遥控操作分析[J]. 江苏电机工程,2013,32(4):45-52.

作者简介:
朱海兵(1978),男,江苏张家港人,高级工程师,从事调度监控运行管理工作;
吴 奕(1968),男,重庆人,高级工程师,从事调度监控运行管理的工作;
陈 宁(1973),男,广东大埔人,高级工程师,从事电网调度自动化系统研发工作;
朱志华(1971),男,江苏南通人,高级工程师,从事变电站自动化的工作;
刘 翌(1971),男,广东兴宁人,高级工程师,从事调度监控运行管理工作;
熊 浩(1982),男,江苏南京人,工程师,从事调度监控运行管理的工作。

Extension Research on IEC 60870–5–104 to Improve the Security of Remote Control

ZHU Haibing[1], WU Yi[1], CHEN Ning[2], ZHU Zhihua[2], LIU Yi[1], XIONG Hao[1]
(1.Jiangsu Electric Power Company, Nanjing 210024, China;
2.NARI Technology Development Co. Ltd., Nanjing 210003, China)

Abstract: The new operation mode in the State Grid requires the operator to control substation equipment remotely. In the current dispatching support system, the IEC 60870-5-104 protocol only checks control point number during remote control command transmission and verification process. This may result in mal-operation of remote control because wrong corresponding relation between control point number and device. By extending the IEC 60870-5-104 protocol, double check among device ID, control point number, and device IP is achieved. It greatly reduce the possibility of mal-operation of remote control caused by wrong corresponding relation between control point number and device.

Key words: remote control; IEC 60870-5-104; protocol; SCADA

(上接第 50 页)

作者简介:
颜庆国(1968),男,江苏扬州人,高级工程师,从事电力营销的管理工作;
薛溟枫(1976),男,江苏无锡人,助理工程师,从事有序用电的管理工作;
范 洁(1977),女,江苏南通人,高级工程师,从事电力计量工作;
陈 霄(1985),男,江苏连云港人,工程师,从事电力计量工作;
周 玉(1982),男,江苏镇江人,工程师,从事电力计量工作;.
易永仙(1988),男,浙江苍南人,工程师,从事电力计量工作。

Load Property Analysis Method for Demanders Participating Orderly Power Utilization

YAN Qingguo[1], XUE Mingfeng[1], FAN Jie[2], CHEN Xiao[2], ZHOU Yu[2],YI Yongxian[2],
(1. Jiangsu Electric Power Company, Nanjing 210024, China;
2. Jiangsu Electric Power Company Electric Power Research Institute
State Grid Laboratory of Electric Energy Measurement,Nanjing 211103, China)

Abstract: Our country has been long-term facing the regional, seasonal, periodical and structural shortage of power. Orderly power utilization is a tool to keep balance in supply and demand of power and so as to ensure the power supply to residential and important demanders. However, currently choosing demanders to participate into orderly power utilization program is mostly subjectively decided by the operator, which is lacking of scientific basis, unreasonable and injustice. This paper proposes a load characteristic analysis method for orderly power utilization demanders based on fine management object. Through clustering the historical load of the demanders, typical daily load curve of demanders are figured out. Then through combining the sampling points clusters of typical daily load curve, power utilization pattern and power utilization interval of demanders are obtained. The peak load shifting and holiday staggering plan value of the demanders are calculated. Rules and strategies for orderly power utilization demander selection are constituted based on the analysis of load property, which, is public to the community, makes the orderly power utilization work more scientifically and orderly.

Key words: orderly power utilization; load property; power utilization pattern; power utilization interval