[特高压]

某特高压直流工程站控层路由器改造方案

文/赵冠华　庞科伟　姚福洲　邵瑞博　张　玲
许继电气股份有限公司直流输电分公司

针对某特高压直流工程站控层路由器运行时间已超过设备生命周期且CPU负载率高的现状，提出了一种改造方案，利用交换机加路由器的方式将原路由器进行替换。该方案不仅满足换流站站内通信和站间通信的要求，而且站控层网络结构清晰，交换机和路由器的CPU负载率较低，降低了通信故障风险，有利于该特高压直流工程的稳定运行。

特高压换流站内站控层交换机、路由器等网络通信设备作为站内控制保护系统、远动系统、运行人员控制系统等设备之间信息沟通的桥梁，是换流站一区站内局域网（LAN）业务的核心承载者，对于直流系统的稳定运行起着举足轻重的作用，运行状态牵一发而动全身，故障也可能导致严重后果甚至闭锁。

某特高压直流工程已投运多年，目前站控层使用的思科路由器运行时间已经超过了其生命周期，而且CPU负载率较高。为保障控制保护系统的稳定运行，计划对该工程整流站和逆变站现用的思科路由器进行改造。

文章提出了一种改造方案，根据此方案完成了该特高压直流工程整流站和逆变站的站控层路由器改造。

网络现状

1. 站内通信

特高压直流输电工程换流站内的LAN是一个在计算机系统内部分布的传送数字信号的多路存取和数据切换的通信系统，采用双重冗余以太网（LAN1和LAN2），网络覆盖整个交流场与直流场、换流阀厅与控制大楼，以及站内其他需要的设备或区域，继电小室与主控制室之间采用光纤网络连接，站内LAN采用分段星形网络结构。

双重冗余以太网LAN1和LAN2主要用于监视和控制站内监控子系统之间的通信，也用于监视和控制站内监控子系统和对站及总调的通信。通常各个子监控系统称为通信节点，各节点有两个接口，分别接到LAN1和LAN2。正常运行时，LAN1为主系统，LAN2是热备用系统，各节点在LAN1上进行通信。当LAN1上出现通信故障时，切换到LAN2上进行通信，故障排除后自动切换回LAN1。

2. 站间通信

换流站内LAN与广域网（WAN）桥及通信传输通道相连接即构成站间WAN，换流站数据采集与监控系统（SCADA）通过站间WAN相互传送有关信息，使两端换流站都能监视到对站的运行状况。采用路由器以G703标准2M通过同轴电缆直接接入通信传输设备。

某特高压直流工程控制保护系统采用SIMATIC TDC模块化装置，站间通信包括极1控制系统站间通信、极1保护系统站间通信、极2控制系统站间通信、极2保护系统站间通信和直流站控系统站间通信。

每个站间通信WAN共配置2个站间通信通道，当通道1出现通信故障时，切换到通道2上进行通信，故障排除后自动切换回通道1。

该特高压直流工程站控层通信设备为思科路由器，安装有1个16口交换模块，路由器集成了交换和路由功能。下面以LAN1为例对该工程整流站和逆变站现有网络结构进行说明。

3. 整流站站控层网络拓扑

整流站站控层网络拓扑如图1所示。

主控楼通信屏一的路由器－U31、－U32和－U33通过网线级联起来，组建站内LAN；－U31通过同轴电缆实现与对站的站控通信；－U32通过同轴电缆实现与对站的极1控制和极1保护站间通信；－U33通过同轴电缆实现与对站的极2控制和极2保护站间通信。

整流站辅控楼和主控楼共有4个光电转换装置，实现了站内LAN的延伸和链路的备份。极1控制和保护设备接入辅控楼光纤接口屏路由器－U31，通过物理双链路接入站内LAN。

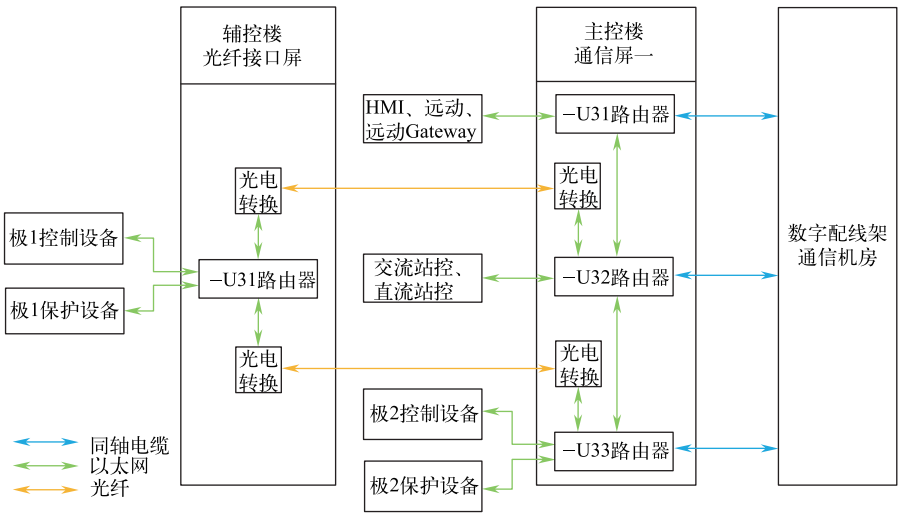

图1　整流站现有站控层网络拓扑

4. 逆变站站控层网络拓扑

逆变站站控层网络拓扑如图2所示。

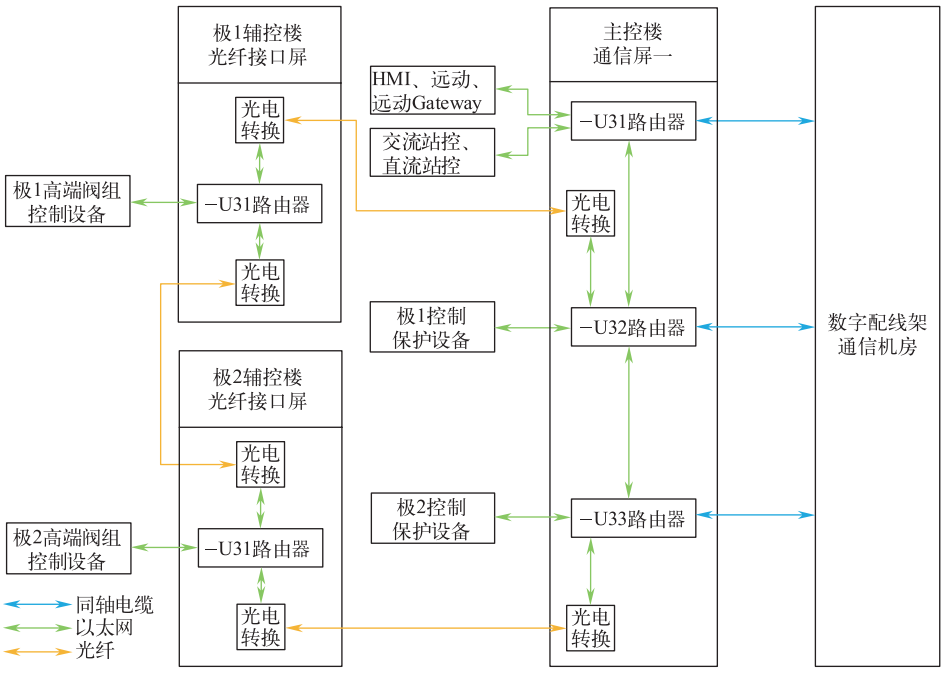

图2　逆变站现有站控层网络拓扑

主控楼通信屏一的路由器－U31、－U32和－U33通过网线级联起来，组建站内LAN；－U31通过同轴电缆实现与对站的站控通信；－U32通过同轴电缆实现与对站的极1控制和极1保护站间通信；－U33通过同轴电缆实现与对站的极2控制和极2保护站间通信。

逆变站辅控楼和主控楼共有6个光电转换装置，实现了站内LAN的延伸和链路的备份。极1高端阀组控制设备和极2高端阀组控制设备接入各自辅控楼光纤接口屏内的－U31路由器，通过物理双链路接入站内LAN。

改造方案

1. 改造思路

该特高压直流工程现用的思科路由器都安装有1个16口交换模块，路由器集成了交换和路由功能，同时处理站内通信和站间通信。这样设计的优点是可以节省通信设备，缺点是路由器CPU负载率特别高，主控楼通信屏的路由器CPU负载率常年保持在90%以上，发生通信故障的风险较大，整机故障会导致该路由器处理的站内通信和站间通信同时中断。

针对站控层现用通信设备组织方式的缺点，提出了采用交换机加路由器的方式对现用思科路由器进行替代的改造方案。

方案设计将站内通信和站间通信分别交由不同的网络通信设备处理，站内通信通过交换机实现，站间通信通过路由器实现，这种交换机加路由器的通信设备组织方式不仅网络结构清晰，而且每种通信设备分别处理站内和站间通信报文，可以降低通信设备的CPU负载，从而降低通信故障风险。

下面以LAN1为例对该工程整流站和逆变站改造后的网络结构进行说明。

2. 整流站改造后的站控层网络拓扑

整流站改造后的站控层网络拓扑如图3所示。

整流站新增一面站间通信路由器屏柜。

辅控楼光纤接口屏路由器替换为交换机，主控楼通信屏的原－U31、－U32和－U33路由器替换为1台48口交换机－U31，并通过网线连接到新增屏柜的－U11、－U12、－U13、－U14和－U15路由器。

－U11路由器用于站控站间通信，－U12路由器用于极1控制系统站间通信，－U13路由器用于极1保护系统站间通信，－U14路由器用于极2控制系统站间通信，－U15路由器用于极2保护系统站间通信。

交换机只处理站内通信，路由器只处理站间通信，且1台路由器只处理1个通道的站间通信。

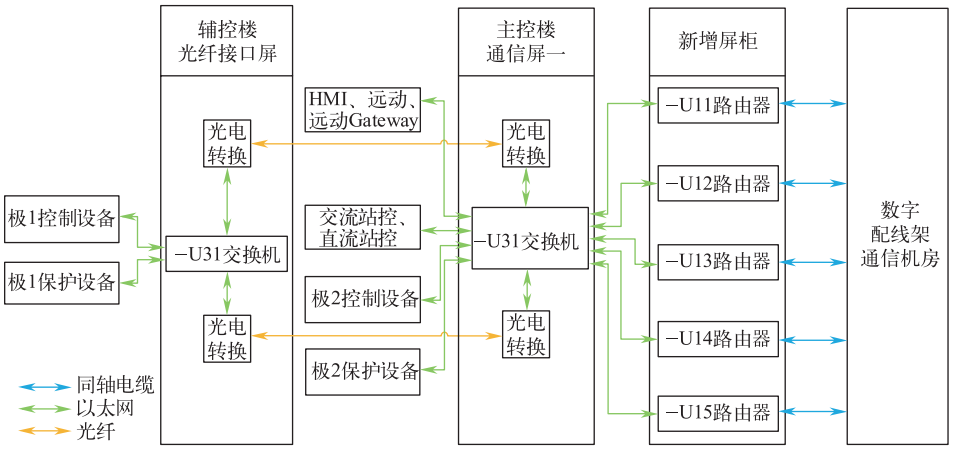

图3　整流站改造后的站控层网络拓扑

3. 逆变站改造后的站控层网络拓扑

逆变站改造后的站控层网络拓扑如图4所示。

逆变站新增一面站间通信路由器屏柜。

极1和极2辅控楼光纤接口屏路由器替换为交换机，主控楼通信屏的原－U31、－U32和－U33路由器替换为1台48口交换机－U31，并通过网线连接到新增屏柜的－U11、－U12、－U13、－U14和－U15路由器。

－U11路由器用于站控站间通信，－U12路由器用于极1控制系统站间通信，－U13路由器用于极1保

护系统站间通信，－U14路由器用于极2控制系统站间通信，－U15路由器用于极2保护系统站间通信。

交换机只处理站内通信，路由器只处理站间通信，且1台路由器只处理1个通道的站间通信。

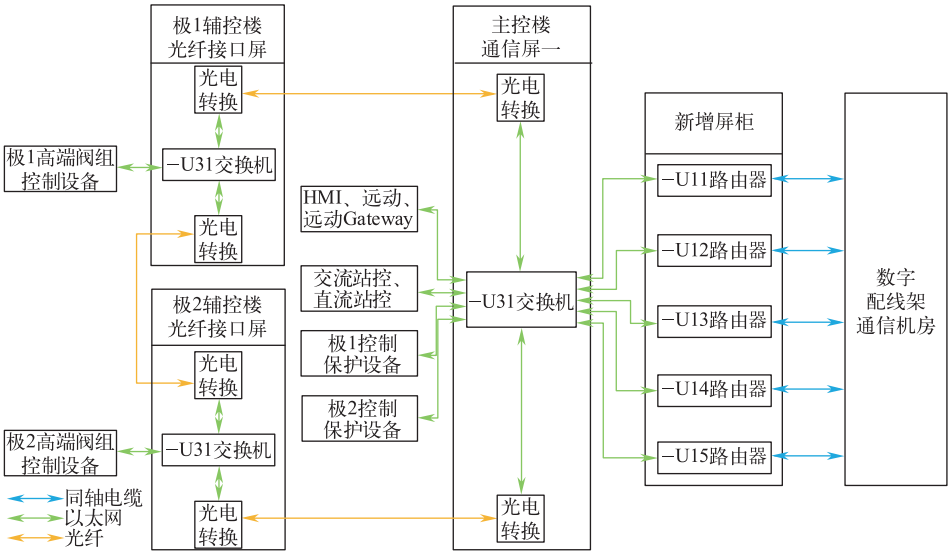

图4　逆变站改造后的站控层网络拓扑

4. 路由器选型

该特高压直流工程极控制系统和极保护系统站间通信采用用户数据报协议（UDP），以UDP广播报文方式进行站间通信。极控制系统和极保护系统站间通信的报文发送周期为4 ms，接收周期为2 ms，接收报文最大容忍时间为100 ms，超过100 ms接收不到对站报文即认为站间通信出现故障。正常通信时，路由器通过的报文速率为500 Pbit/s，即CPU每秒处理500个UDP报文。

在当今日益复杂的网络中，存在大量针对CPU的恶意攻击报文，如果上送的CPU报文过多，会导致CPU占用率过高，性能下降。为保证CPU对正常业务的处理，有些型号的国产路由器增加了CPU防护策略，对未知报文进行限速，超保护阈值后将报文丢弃。

为确保SIMATIC TDC站间通信广播报文能顺利转发，在进行路由器选型时，需要选择具备转发广播功能的路由器，而且最好是避开启用CPU防护策略的路由器。

最后选用H3C某型号的交换机和路由器替换思科路由器。

配置事项

对交换机和路由器进行配置时，不仅要实现站内通信和站间通信的业务功能，还要实现安全防护方面的功能。

1. 访问方式

将交换机和路由器设置为用户名加密码的登录方式，那么攻击者不光要破解密码，还要破解登录名，增加了非法登录的难度。在电力通信网中不允许通过远程方式管理网络设备，所以一般只配置Console口数据，通过Console口方式登录后，使用设备提供的命令行对设备进行管理和配置。

设置交换机和路由器维护管理只能通过Console口开展，禁止远程登录，使用用户名和密码认证方式登录。

2. 划分VLAN

虚拟局域网（Virtual Local Area Network，VLAN）是将一个物理的LAN在逻辑上划分成多个广播域的通信技术。

VLAN技术广泛应用于当下的网络交换机安全防护中。使用这一安全技术后，经由VLAN划分的端口，只有在同网段内才可实现数据传输，在不同的网段之间，数据传输无法正常开展。一旦某一网段遇到了非法入侵，其他网段的运行和数据传输都不会受其干扰。

目前TDC控制设备和保护设备的IP地址划分为不同的网段，配置交换机时，将交换机上连接控制

设备和保护设备的端口分别划分为不同的VLAN。

另外，将连接控制保护主机和HMI主机的端口类型配置为Access，整流站主控楼和辅控楼交换机连接光电转换装置的端口的类型配置为Trunk，并允许控制系统VALN和保护系统VLAN的数据包都通过Trunk端口。

3. 开启生成树协议

生成树协议是网络二层设备的基础协议之一，它通过分布式计算使网络活动拓扑为树形结构，从而有效地防止了网络中回路的出现，避免了由于帧的无限循环和重复接收所导致的网络风暴的发生。

由于辅控楼控制保护设备交换机通过物理上的双链路接入站控层LAN，因此交换机需要开启生成树协议，通过有选择性地阻塞网络冗余链路来消除网络二层环路。

4. 转发广播

配置路由器时，要对连接交换机的端口以及串行端口进行转发广播配置，确保站间通信UDP广播通过路由器转发对站。对于发往对站的站间通信报文，在配置路由器时设置静态路由，下一跳接口为对站路由器串行端口。

5. 接入态势感知

根据目前对电力系统网络的要求，换流站网络通信设备需要接入态势感知系统。

智能电网网络安全态势感知系统以安全大数据为基础，全面收集安全日志、网络流量、终端日志、业务数据、用户行为及资产状态等多源数据，结合外部威胁情报，实现网络安全风险的实时监控、分析、响应和预测，从威胁、风险、资产、业务及用户等多个视角，对全局网络安全态势进行态势感知、态势认知、态势处置和态势呈现。

因此，对交换机和路由器进行配置时，需要进行启动SNMP服务、配置团体名称及设置版本等简单网络管理协议（Simple Network Management Protocol，SNMP）的相关配置，还需要启用Syslog日志功能，以及配置镜像目的端口和镜像源端口，确保态势感知系统完成数据采集。

测试验证

搭建该工程的控制保护以及HMI仿真平台，对提出的站控层路由器改造方案进行测试。测试结果见表1。

表1　改造方案测试结果

序号	测试内容	测试方法	预期结果	测试结果
1	极控系统的新华三交换机、路由器通信能力验证	查看交换机CPU负载率	1.站间通信没有扰动 2.HMI没有出现通信故障告警 3.直流控保系统正常运行 4.CPU负载率低于50%	CPU负载率≤15%
2		查看路由器CPU负载率、端口负载率		CPU负载率≤3%、端口负载率＜0.2%（2 bit/s）
3		直流顺控解闭锁操作		正常解闭锁，HMI未出现通信故障告警
4		直流功率升降操作		正常升降功率，HMI未出现通信故障告警
5		模拟整流侧、逆变侧交流故障，包括长时间单相故障、短时三相故障等		保护正常动作，HMI未出现通信故障告警
6		模拟站控系统掉电		直流系统正常运行，HMI未出现通信故障告警
7		系统连续运行48 h		直流系统正常运行，HMI未出现通信故障告警

从测试的结果中可以看出，交换机CPU负载率不大于15%，路由器CPU负载率不大于3%、端口负载率小于0.2%（2 bit/s），直流系统可正常解闭锁、升降功率，保护可以正常动作，HMI未出现通信故障告警。

测试结果符合预期，满足改造要求，具备在现场实施条件。

结束语

依据文章提出的改造方案，该特高压直流工程的整流站和逆变站进行了站控层路由器改造。改造后，运行人员控制层与控制保护层设备之间通信正常，控制保护设备相互之间通信正常，远动系统与调度主站通信正常，路由器能够与对端站路由器正常通信，所有站间通道通信状态正常，站内控制保系统与对端站控制保护系统正常通信，且可正常切换通道。该改造方案不仅网络结构清晰，而且交换机和路由器的CPU负载率都较低，降低了通信故障风险，有利于该特高压直流工程的安全稳定运行。EA

（收稿日期：2023-03-23）