国电投某发电厂 DCS 网络故障分析及处理方案

安磊

上海新华控制技术集团科技有限公司，上海 200000

DOI:10.61369/EPTSM.2025050015

摘　　要： 本文针对国电投某发电厂 DCS（分散控制系统）网络突发故障展开深入分析，旨在明确故障根源并提出系统性处理方案。故障发生时，操作员无法对控制器内的设备进行监控和操作。本次网络故障的核心诱因是千兆网络与百兆网络混用，具体是从 OPU5 站问题，交换机功能失效，工控安全卫士影响，网络环境不佳等方面进行总结分析，经过对现场的报警历史记录的分析以及现场 DCS 网络设备的勘查，提出了系统性解决方案，为同类电厂 DCS 网络的稳定运行提供参考。

关 键 词： 发电厂；DCS 网络故障；分析；处理方案

Analysis and Handling Scheme of DCS Network Fault in a Power Plant of SPIC

An Lei

Shanghai Xinhua Control Technology Group Co., Ltd., Shanghai 200000

Abstract: This paper conducts an in-depth analysis on the sudden DCS (Distributed Control System) network fault in a power plant of SPIC, aiming to identify the root cause of the fault and propose a systematic handling scheme. When the fault occurred, operators were unable to monitor and operate the equipment in the controller. The core cause of this network fault is the mixed use of gigabit network and 100-megabit network. Specifically, the analysis is summarized from aspects such as the problem of OPU5 station, failure of switch function, impact of industrial control security guard, and poor network environment. Through the analysis of on-site alarm history records and the investigation of on-site DCS network equipment, a systematic solution is put forward, which provides a reference for the stable operation of DCS networks in similar power plants.

Keywords: power plant; DCS network fault; analysis; handling scheme

一、故障现象及背景

国家电力投资集团有限公司某发电公司 #6机组 DCS 采用的是新华集团的 XDPS 系统，本台机组 DCS 系统自2005年左右机组建成投运后一直使用至今，此前设备运行稳定正常，但于2021年02月26日13点10分至13点49分之间先后有26个控制器自动重启复位的现象，其中 DPU03/DPU23和 DPU16/DPU26这两对控制器在一分钟内先后自动重启，使得操作员在控制器重启的一分钟内无法对控制器内的设备进行监控和操作。[1] 控制器的重启时间表如下：

控制器重启时间统计			
控制器号	启动时间	控制器号	启动时间
DPU01		DPU21	
DPU02	13:41:43	DPU22	13:36:06
DPU03	13:39:23	DPU23	13:38:43
DPU04	13:33:28	DPU24	
DPU05	13:40:30	DPU25	13:38:40
DPU06		DPU26	
DPU07	13:40:28	DPU27	13:35:46
DPU08	13:31:26	DPU28	
DPU09	13:40:50	DPU29	13:42:24
DPU10	13:31:14	DPU30	13:39:25
DPU11	13:39:40	DPU31	13:32:16
DPU12	13:32:35	DPU32	13:36:27
DPU13	13:38:09	DPU33	13:40:38
DPU14		DPU34	13:44:38
DPU15	13:24:44	DPU35	
DPU16	13:39:46	DPU36	13:39:22
DPU17	13:39:01	DPU37	13:12:08
DPU18		DPU38	
DPU19		DPU39	
DPU20		DPU40	

二、故障分析及处理方案

通过查询本台机组的新华 DCS 历史报警和操作记录等信息，以及检修人员对事发时现场现象的描述，判断应该不是 DPU 硬件

作者简介：安磊（1982.04-），汉族，河南南阳人，本科，工程师，研究方向：DCS 控制系统应用。

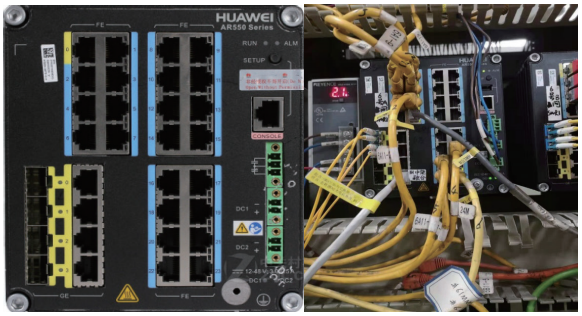
故障，而是因为网络拥堵，造成控制器来不及处理大量的网络信息，引起控制器复位重启。[2]

2021年03月08日在电厂检修人员的配合下，全面检查了整个DCS网络内的设备情况，包括DPU、交换机的状态，HMI站的软件及网络负荷，发现了以下情况：

1. 交换机

#6机DCS系统的A、B网交换机采用的是华为AR55O系列，具体型号为AR550-24FE-D-H，是2020年电厂自行采购更换的，此型号的交换机未曾在任何新华DCS系统中使用过。华为AR550系列一款三层路由交换机，具备了耐高/低温、防尘、抗震、抗强电磁干扰等优秀品质，主要应用在物联网方面，此交换机端口数量为24个，控制端口为4×GE combo、8×FE，支持SEP、STP、RSTP、MSTP等网络协议，安全管理包含访问控制列表（ACL），802.1x认证，AAA认证，RADIUS认证，HWTACACS认证，广播风暴抑制， ARP安全，ICMP防攻击，URPF，CPCAR，黑名单，PKI。但AR550-24FE-D-H交换机自2019年12月31日已经停止整机销售，2024年12月31日将停止任何服务（包含服务热线电话）。[3]

#6机实时数据网分为A网和B网(A、B网络互为冗余)，A网配置了4台AR550-24FE-D-H交换机(A1、A2、A3、A4)，交换机之间通过光跳线连接，形成环网结构(A1→A2→A3→A4→A1)，B网的网络配置和A网相同。[4]具体如下图所示：



此交换机的控制端口为4×GE combo，即左侧上图中的黄色端口（0,1,2,3），此端口是千兆网络端口。新华XDPS系统中DPU的网卡是百兆网卡，所以新华采用的交换机大多为百兆网络或者千兆/百兆网络自适应的交换机。[5]

2.DCS人机接口站(以下简称HMI站)

HMI站是整个DCS网络最关键的设备之一，是操作员控制监视设备运行的窗口。在检查过程中发现#6机的HMI站型号多种，都不是从原DCS厂家采购的，HMI站的网卡类型多种，如Realtek pcie Gbe family controller、Realtek Rtl8139、82566Dm Gigabit等。其配置也比较混乱，网卡的驱动也不是通过光盘安装，有的通过驱动精灵等网络软件下载安装。[6]

在HMI站中，100、1000M的网卡均有配置，网络流量控制选项也未关闭，有些A/B网卡的网络文件共享与打印机共享打开。[7]

通过检查发现，所有的HMI站安装了很多与DCS系统无关的软件，如360杀毒软件等，占据了HMI站的大量内存，有的HMI站的防火墙和自动更新处于打开状态，与新华要求的DCS软件安装环境矛盾。具体的HMI站网络情况如下表所示：

豫新电厂HMI站网卡及软件状态

HMI	操作系统(windows)	AM1 网卡类型	AM1 共享设置	HMI 网卡类型	HMI 共享设置	CRH 网卡类型	CRH 共享设置	所含软件	备注
HIS (32)	windows 7	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	360杀毒，工控安全卫士	
EWS (51)	windows 7	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	361杀毒，工控安全卫士	
HMI (35)	windows 7	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	362杀毒，工控安全卫士	
OPI1 (41)	windows XP	D-Link DFE-530TX	共享	D-Link DFE-530TX	共享	Intel (R)	共享	363杀毒，工控安全卫士	
OPI2 (42)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	364杀毒，工控安全卫士	
OPI3 (43)	windows XP	Realtek RTL8139	不共享	Realtek RTL8139	不共享	Intel (R)	共享	365杀毒，工控安全卫士	
OPI4 (44)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	366杀毒，工控安全卫士	
OPI5 (45)	windows XP	Realtek PCIe GBE	共享	Realtek PCIe GBE	不共享	D-Link DFE-530TX	共享	367杀毒，工控安全卫士	工控安全卫士卡顿
STS (53)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	366杀毒，工控安全卫士	
大屏 (54)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	369杀毒，工控安全卫士	
GTR (61)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	370杀毒，工控安全卫士	
GTR (81)	windows XP	D-Link DFE-530TX	不共享	D-Link DFE-530TX	不共享	Intel (R)	共享	371杀毒，工控安全卫士	

通过检查发现及运行人员反映，操作员站OPU3和OPU5操作比较卡顿，反应迟缓，其中OPU3的A、B网网卡是Realtek RTL8139的，也安装了360杀毒等软件，占用整个HMI站的内存比例较大。[8]

OPU5的电脑型号是研华610H，A、B网网卡是电脑自带的Realtek pcie Gbe family controller的网卡，此网卡属于千兆网络网卡，并且OPU5的A网共享一直处于打开状态。本台电脑也安装了360杀毒、工控安全卫士等软件，并且工控安全卫士软件一直在发送一个名为ucl.dll、libxm12.dll等一系列文件不合法的报警。工控安全卫士所占的内存也高于其他电脑。具体情况如下图：

3. 软件

随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及工业互联网的快速发展，工控系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工控系统扩散，工控系统信息安全问题日益突出。[9]

根据《工业自动化和控制系统网络安全集散控制系统(DCS)》要求DCS系统网络与外部网之间应使用物理或逻辑隔离技术措施进行防护；《防止电力生产事故的二十五项重点要求》(2023版)：其中9.8条为防止分散控制系统网络事故，规定分散控制系统与管理信息大区之间必须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；与其他生产大区之间应当采用具有访问控制功能的设备等实现逻辑隔离；与广域网的纵向交接处应当设置电力专用纵向加密认证装置等。所以在工控机内除了安装DCS软件外不建议安装其他软件，如360杀毒软件，同时建议使用DCS

厂家配套的工控安全防护软件，原厂家的工控安全防护软件是经过长期拷机验证的，也在别的项目实际验证过的，对工控机安全具有更好的防护作用。[10]

三、处理方案及意见

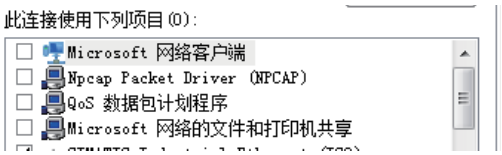
经过对现场的报警历史记录的分析以及现场 DCS 网络设备的勘查，具体的处理方案如下：

1. 交换机

联系原交换机服务厂商，检查交换机的网络配置，确认是否已经配置了广播风暴抑制功能，咨询华为或者要求服务厂商将环网的千兆网络改为百兆或者百兆 / 千兆自适应网络。

2.HMI 站

（1）将所有 HMI 站的 A、B 网络网属性中的 Microsoft 网络的文件和打印机共享不勾选。



（2）所有 HMI 站的 A、B 网网卡选用百兆网卡，如 D-Link(DFE-530TX)，网卡驱动用所带的光盘安装。

（3）将比较卡顿的电脑进行更换。

（4）所有的 HMI 站 windows 防火墙关闭。

3. 软件

卸载掉所有 HMI 站的360杀毒软件，删除掉360杀毒软件的文件等，减少对工控机的内存使用。

咨询工控安全卫士厂家关于 OPU5 中的报警含义，加强对所有 HMI 站的管理。

因为 #6机已经接入了中能融合的态势感知平台，咨询中能融合厂家关于事故发生当天的网络数据流量情况，能否更清楚直接的判断出是那个端口的数据流量过大造成整个网络堵塞，引起了网络风暴。

四、分析原因及注意事项

本次网络故障可能是千兆网络和百兆网络混用导致的，主要原因具体分析如下：

1.OPU5站

OPU5站的 A、B 网网卡是千兆网络网卡，并且 A 网的共享没有关闭，网卡流量限制也未关闭，OPU5站的工控安全卫士一直在发送报警信息，OPU5站的最直观状态是操作反应缓慢，卡涩，在某一时间段内，OPU5站自身的原因，向系统 A、B 网发送了大量的无用信息，DPU 在收到大量的无用信息后，来不及处理，导致 DPU 的 watchdog 建设定时器溢出，从而复位。

2. 交换机

网管型交换机具备抑制广播风暴的功能，但是此交换机并没有起到抑制风暴的作用，并且环网是千兆网络，不是千兆 / 百兆自适应网络或者百兆网络。

3. 工控安全卫士软件

主动防御系统的连续报警也很有可能是诱发本次网络风暴的一个原因，不停的发送报警信息，通过网络传播，造成网络拥堵。

4. 网络环境

本次网络风暴的一个客观的主要原因是网络环境差，即系统用了很多不是原厂家提供的工控机，工控机的型号多样，网卡网速、芯片驱动都各不相同，一旦出现网卡不稳定的情况，HMI 站会频繁向系统 A、B 网发送大量的无用信息，导致控制器复位。

五、预防措施建议

事故在于麻痹，安全在于防范。此次网络故障应引起重视，加强对 DCS 系统网络的管理，所以提出的建议如下：

1. 选用新华 DCS 厂家提供的工控机，保证型号统一，软件版本正版并且一致，所有软硬件设置遵循原厂家要求。

2. 选用新华 DCS 厂家推荐的工业以太网交换机，所推荐的交换机是出厂前经过长时间静态拷机实验和现场实际考验的设备，具备安全、可靠的使用性能，可以放心使用。

3. 加强对工控机的管理监视，针对出现有卡顿、数据刷新缓慢的工控机应该引起重视，建议更换或者返修。

4. 加强工控机内软件管理，除 DCS 软件及 OFFICE 软件外，不要安装其他软件。

5. 建议工控防护软件使用新华 DCS 厂家所提供的工控防护软件。

6. 加强整个 DCS 网络内的网络设备管理，如交换机、光端机等设备，在使用寿命到期前就进行更换。

参考文献

[1] 辛丽梅 . 火电厂热工自动化 DCS 控制系统的运用分析 [J]. 科技视界 ,2024,14(33):65-68.

[2] 邢智成 . 电厂热控 DCS 控制保护回路误动作原因与处理措施研究 [J]. 电力设备管理 ,2024,(21):67-69.

[3] 陈迪新 , 潘宇 , 杨超 . 一种核电站安全级 DCS 网络故障分析及处理方法 [J]. 设备管理与维修 ,2023(13):95-97.

[4] 舒小兰 , 梁雅媚 , 刘恩锋 . 一种工控机压力自动测试系统 [J]. 工业控制计算机 ,2024,37(7):1-2,5.

[5] 刘文娟 , 常芸 . 网络监控系统故障分析及处理措施 [J]. 科技风 ,2011(20):129-129.

[6] 刘传德 , 刘俊峰 , 陈雷 . 基于双 PLC 和工控机的定位绞车变频电控系统设计研究 [J]. 现代工程科技 ,2024,3(8):77-80.

[7] 陈国杰 . 数字油田 4G 网络下的数据通信故障分析及解决方案 [J]. 中国设备工程 ,2022(8):31-32.

[8] 刘枫 . 国产工控机在高档数控系统上的应用 [J]. 精密制造与自动化 ,2024(4):50-53.

[9] 胡益群 , 许光 . 网管型交换机在组播通信中的应用研究 [J]. 数字技术与应用 ,2019,37(6):37-38.

[10] 姜冬旭 . 无人机高清图传系统光通信终端光机系统设计 [D]. 吉林 : 长春理工大学 ,2024.

