

SIEMENS西门子宁夏省中卫市（授权）一级代理商——西门子西北总代理

产品名称	SIEMENS西门子宁夏省中卫市（授权）一级代理商——西门子西北总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子总代理:PLC 西门子一级代:驱动 西门子代理商:伺服电机
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	15915421161 15903418770

产品详情

次分享的内容是我在某制药厂进行网络诊断的分析过程。该制药厂控制系统是使用西门子的PCS7；控制系统的网络是由2个OSM TP62和6个SCALANCE X200系列交换机组成的光纤环网，其中的1个OSM TP62作为环网管理器。

系统的数据归档服务器系统采用的是PI系统软件（经过了FDA认证的软件），此系统软件通过KEPSERVER（专业的OPC Server）的S7驱动协议与西门子的8个S7-400 PLC实现数据通信如下图1所示。

图1

客户现场的问题是当341车间断电时（交换机和PLC都断电）如下图2所示，在PI系统上监视到其与各个PLC发给PI系统的通信心跳检测出现异常（正常看到的心跳是以1递增；异常时会出现不是以1递增）如下图3所示，且有时会在431车间产生PI系统发给431车间的PLC的心跳检测超出设定时间15S的报警信息如下图4所示。客户怀疑可能由于网络的问题导致上述的情况的出现。认为网络出现中断的现象使得一些心跳数值得丢失。

根据问题描述判断产生的原因有以下几种可能：

网络拓扑结构的变化使网络出现了问题，如环网管理出现了不正常等造成了通信的异常。

KEPSERVER OPC服务器的S7驱动在网络结构发生变化时出现了异常

PI系统的OPC 客户端与KEPSERVER OPC服务器之间的通信出现了异常导致问题的产生。网络中接入了新的设备，且此新设备的IP地址与KEPSERVER OPC服务器产生冲突导致了与所有PLC站的通信的时通时段

根据上面的分析判断与用户进行了沟通，用户给出的答案是上面的第三和第四是没有可能的。原因是PI系统的专家远程诊断了PI与KEPSERVER OPC服务器之间的通信，结果是没有出现任何异常现象。当321车间断电时，网络也没有接入任何新的设备。所以只可能的是第一条和第二条中的原因。

为了确认确切的故障原因让用户再次断321车间的电，看是否问题能重新浮现。当321车间断电后，故障现象确实能再次浮现。更进一步的排除了第三条与第四条造成问题的可能性。

那么第一条与第二条中究竟是哪一条导致的故障现象？于是我们在KEPSERVER OPC服务器的出口和331车间的PLC的出口上接入了TAP（网络分析工具）进行抓包。如下图5所示。图中KEPSERVER OPC服务器的IP地址为192.168.0.20/24；331车间PLC的IP地址为192.168.0.4/24。

图5

在KEPSERVER OPC服务器的出口处抓包后分析发现，断电前与断电后数据包的发送间隔会出现变化，在断电前数据包的发送间隔为1s左右，而断电后数据的发送间隔在某个时刻会变为7-10s左右，如图6和图7所示。但从这里只能说明数据包的发送出了问题，没有足够的证据能够说明是KEPSERVER OPC服务器的S7驱动的问题，而不是网络的问题。

图7 断电后的数据包发送情况

为了更进一步的确认问题的原因，于是在现场断开321车间的OSM

TP62的所有的光纤如下图8所示

图8

断开后发现PI系统监视到321车间发来的心跳检测仍然异常，此时把321车间的OSM TP62换为SCALANE X204-2交换机后心跳检测仍然异常，这样判断不是交换机网络引起的问题。为了更好的说明问题，把321车间的一端的光纤断开，另一端的光纤保持连接状态如图9所示，此时在PI系统上监视到321车间发来的心跳检测为正常，更进步说明了与网络无关。

图9

此时已基本确定是KEPSEVER OPC服务器的S7驱动的问题导致了故障现象。为了让客户能确认，我们又做了一个测试，环网保持正常的连接断开231车间PLC与SCALANCE X200的以太网双绞线如图10所示。断开后发现心跳检测出现了异常，在此基础上继续断开241车间PLC与SCALANCE X200的以太网双绞线，发现异常现象更为严重。

图10

造成问题的原因找到了，但为什么会会出现此现象，我们查看了KEPSEVER OPC服务器的设置，在通讯通道的设置中有一项是当KEPSEVER OPC服务器与下面的PLC通信时，当连接不能建立时有重新请求的机制，这会造成延时。如图11所示。而KEPSEVER OPC服务器对所有的站采用的是轮训机制。一个PLC站点造成的延时会影响其后站的数据刷新。这也就是为什么当有PLC出现掉站，系统就会出现用户所描述的问题。

图11

最终处理的方式是更换KEPSEVER的OPC服务器为西门子的SIMATIC Net的OPC服务器，SIMATIC Net的OPC服务器采用的不是轮训机制，所有的站都是并行发送数据，一个站点的掉站是不会影响其它的站。