衢州西门子交换机6GK7277-1AA10-0AA0授权代理商

产品名称	衢州西门子交换机6GK7277-1AA10-0AA0授权代理商
公司名称	浔之漫智控技术（上海）有限公司
价格	.00/个
规格参数	
公司地址	上海市松江区广富林路4855弄88号3楼
联系电话	158****1992 158****1992

产品详情

衢州西门子交换机6GK7277-1AA10-0AA0授权代理商

根据经验这种报错多数是Imager中RX1、RX2或硬盘问题。

因为医院患者很多且序列压缩的时间很短，颈CE患者少所以一直没有重视。

颈CE序列使用的线圈是BO1、BO2、SP2、SP3（靠近心脏位置）

有时做DWI序列时也会报这个错误。

PS.图像问题和扫描中断之间是否存在关联未知。

处理过程

1. 做线圈QA观察是否有规律：

头部QA做两次HE3没有水模HE4没结果，颈部QA 3次NE1没有水模 NE2没结果

降床再升床后头部QA次通过，第二次HE3找不到水模HE4没结果，颈部QA不变。

大柔：3号插座QA通过，4号FL4找不到水模，6号FL3找不到水模。更换备用颈线圈QA结果不变。

结论：每个插座都是固定通道故障，升降进出病床基本没有改变。（除了头部QA好过一次）

2. 做Testtools看是否能发现问题：

根据报错首先考虑Imager，然后是RF部分。

① Imager测试结果：Data RateEvaluation failed；RX1和RX2测试通过。

提示数据量问题检查网络，更换内网交换机后测试通过。但扫描水模颈CE序列仍然报错。

② RF部分：MOD/REC、RFPA、RCCS提示检查机柜温度，机柜温度确实有点高。检查发现RFSU Fans风扇不转，但实际上机柜温度高还有其他问题，另行讨论。

3. 根据测试结果得出结论：①
怀疑Receiver3故障，交换Receiver2和Receiver3后做MOD/REC测试结果变化为

2A、2B、2C、2D 测试不过，3A、3B通过。确定Receiver3故障。

② 交换Receiver后RCCS测试结果不变（故障的开关不变），所以RCCS测试不过与Receiver无关。更换RCCS后测试通过，各插座恢复正常。

③ 更换Receiver3后MOD/REC测试中Modulator-ReceiverLoop OK但Modulator-Receiver Long Time Stability中很多通道失真。

怀疑是RFSU Fans故障引起过热导致扫描过程中Receiver信号失真后报Image故障，打开机柜门使空调直吹机柜后做MOD/REC测试Modulator-Receiver Long Time Stability通过。准备更换RFSU Fans。

维修小结

1. flair序列伪影和腹部弥散伪影是因为RCCS故障引起图像信噪比差，线圈插在2、4、6插座扫描时线圈信噪比差图像差。如：头线圈、腹部线圈、8通道高分辨率膝关节线圈、大小柔线圈。因为医院患者量大对图像质量要求不高，所以只反映了突出的问题flair和腹部弥散。

2. 颈CE和头部DWI扫描中断报错，是RCCS故障引起。

近日，顶象洞见安全实验室发现西门子多款工业交换机存在高危漏洞。利用这些漏洞，黑客可远程窃取敏感信息，直接对联网的工控设备下达停止、销毁、开启、关闭等各种指令，甚至在网络内植入木马病毒。预计至少有17款西门子工业交换机设备受影响。顶象洞见安全实验室已时间将相关漏洞细节上报CNNVD（国家信息安全漏洞库）和CNVD（国家信息安全漏洞共享平台），同时建议使用这些设备的企业，在漏洞修复前应该禁止非授权IP访问设备的80和443端口。工控系统一旦遭到攻击，不仅引发故障，还会导致安全事故发生，甚至影响正常公共服务，给社会带来不可估量的损失。倪光南院士此前就表示，要解决工控安全问题，就是掌握关键核心技术，发展自主可控技术。漏洞是工控风险的源头漏洞是风险的爆发源头，无论是病毒攻击还是黑客入侵大多是基于漏洞。

CNVD“ 工控系统行业漏洞 ”共披露了2800多个漏洞，其中包含西门子、飞利浦等企业的工控设备。顶象洞见安全实验室研究员在研究中发现，西门子多款型号的工业交换机的系统固件存在权限绕过、栈溢出、堆溢出等多个高危漏洞。

分析发现，该系统固件的代码逻辑设置错误，导致权限被轻松绕过。例如，在权限控制方面，满足A或满足B的任何一个条件验证，即可执行相应特权操作。这就导致黑客无需任何权限即能够重启存在漏洞交换机设备、恢复设备的出厂设置、修改设备的管理密码、直接远程关闭存在漏洞的交换机等高权限操作。

利用该系统固件存在栈溢出、堆溢出等多个高危漏洞，导致黑客能够远程窃取网络传输的工控指令、账户密码等敏感信息，或者发动中间人攻击，使得整个网络如同裸奔。同时，黑客可以直接对联网工控设备下达停止、销毁、开启、关闭等各种指令，甚至在网络内植入木马病毒，直接关停网内生产设备。

顶象洞见安全实验室发现，西门子至少有17款工业交换机使用该系统固件。由于该漏洞是存在于某个通用框架中，因此以上漏洞是否影响其他型号设备还在确认中，受该漏洞影响的范围未知。

相关漏洞细节，顶象洞见安全实验室已时间将已上报CNNVD和CNVD。同时建议使用以上设备的企业，在漏洞修复之前，不要开启相关设备的80或者443端口，必须开启则使用VPN专用网络；如果用户网络已经配置防火墙等安全设施，建议设置相应规则过滤规则，禁止非授权IP地址访问上述端口。

工控风险的四大特征工业交换机是电力、能源、制造等工业领域内，用于互联互通的重要设备。由于工业系统的本质目标是控制，而互联网的核心目标是交换。相较于传统互联网采用平等关系的点对点传输模式，工控系统多采用基于主从关系的非对等网络。尤其随着智能化、网联化的推进，暴露出越来越多的风险。

针对工控系统风险现状，顶象洞见安全实验室总结了四个特征：1、工控系统的设计主要是专用的相对封闭可信的通信线路，也就是封闭的“ 单机系统 ”，原本没有考虑联网需求，系统和联网设备也未配置防护系统，存在很多安全缺陷和漏洞。

2、工业设备资产分布广、设备类型繁多，攻击行为难以察觉。

3、攻击门槛低，数行代码即可造成严重后果。

4、工业设备的协议、设备、系统设计复杂，潜在漏洞多，系统更新升级慢、修复维护成本高;而且大量的系统设备需要7×24小时不间断运转，没有机会及时修复补丁。中国信息通信研究院发布的《2020年上半年工业互联网安全态势报告》显示，上半年发现恶意网络攻击行为1356万次，涉及2039家企业。大量老旧工业控制系统或设备未及时升级或更新补丁，这种“ 带病运行 ”的工业设备及系统被攻击门槛很低。

自主可控是化解风险的关键倪光南院士曾表示，造成工控系统安全漏洞的原因，既有企业内网的误用和滥用，也有日趋多样的外部网络攻击，更有工控设备本身的脆弱性。他表示，国内核心控制系统和设备超70%来源于国外厂商，严重依赖进口，而进口工控设备后门广泛存在，很大程度上增加了安全风险。要解决这些问题，就是掌握关键核心技术，发展自主可控技术。“ 自主可控 ”是化解工控风险的关键。

要达成这一目标需要循序渐进：首先要实现风险自主可控，进而达成安全自主可控，后实现设备与应用的自主可控。

风险可控：工业企业尽快开展企业资产和脆弱性识别，拥有发现风险和感知攻击的能力，进而才能有效做好风险评估与防控。顶象洞见安全实验室的

IoT-Argus检测系统，能够对嵌入式固件系统进行自动化安全扫描，及时发现存在和潜在的安全漏洞与隐患，并在

30分钟内提供可视化分析报告，帮助企业时刻了解风险发现威胁，提升安全保障能力。

安全可控：工业企业需要制定安全战略，根据工控网络安全设计原则以及设计标准，进行工控网络安全方案设计，终完成工控网络安全防护目标，实现评估、防护和运营的有机结合，形成长期有效的防护机制。

设备与应用可控：工业控制系统生产商、集成商和服务商加强自主创新，攻克工控产业“ 贫血 ”软肋，建成技术先进、功能完善、安全可靠的工业操作系统、智能感知、自动控制、智能装备、网络连接、工业软件等软件和产品，并打通上下游的信息安全技术和产品壁垒，让安全一通到底，实现网络、控制、安全的统一。

面对日益复杂严峻的安全形势，需要各界持续推进工控安全态势感知建设，构建上下联动、协调配合的技术保障体系。只有做到自主可控，才能够形成可持续发展。