

气田工业以太网安全网络研究与应用

刘国洞 苗立民 徐小龙 陈纯见

中国石化中原油田普光分公司 四川 达州 635000

摘要: 随着信息技术的不断发展,信息交换技术覆盖了各行各业。在自动化领域,越来越多的企业需要建立包含从工厂现场设备层到控制层、管理层等各个层次的综合自动化网络管控平台,建立以工业控制网络技术为基础的企业信息化系统。工业以太网提供了针对制造业控制网络的数据传输的以太网标准,该技术基于工业标准,利用了交换以太网结构,有很高的网络安全性、可操作性和实效性,最大限度地满足了工业现场的需求。普光气田的自动控制系统的数据传输通道采用工业以太网,以实现数据采集、集中监控、联锁关断指令的传达等目的,因此,工业以太网的网络质量对气田的安全平稳生产运行至关重要。本次通过对普光气田以太网安全网络的研究和优化,提高网络质量,为自动化系统之间的数据传输提供安全保证,确保安全仪表系统数据传输及时有效,为紧急状态下的应急处置提供保障,以供经验分享。

关键词: 气田 以太网 安全网络 SafeNet 自动化控制 联锁关断 应急处置

1 普光气田集输系统工业以太网概况

1.1 工业以太网介绍

工业以太网是基于IEEE 802.3 (Ethernet)强大的区域和单元网络。利用工业以太网, SIMATIC NET 提供了一个无缝集成到新的多媒体世界的途径。企业内部互联网(Intranet), 外部互联网(Extranet), 以及国际互联网(Internet) 提供的广泛应用不但已经进入今天的办公室领域, 而且还应用于生产和过程自动化。继10M波特率以太网成功运行之后, 具有交换功能, 全双工和自适应的100M波特率快速以太网(Fast Ethernet, 符合IEEE 802.3u的标准)也已成功运行多年。

1.2 普光气田工业以太网系统组成

普光气田地面集输系统中采用的工业以太网系统采用有线与无线结合的解决方案。有线网络采用双网冗余结构, 使用工业以太网构架网络; 无线网络作为有线网络的备用通道。系统骨干网络为1000Mbit/s全双工线速交换能力(实际提供2000Mbit/s双向带宽)光纤以太网网络, 中控室、场站及阀室内部的子系统网络为100Mbit/s的电气以太网网络, 基于具体设备实际连接距离需要, 子系统网络内部亦可采用100Mbit/s的光纤以太网网络。有线网络向无线网络(5.8G 无线以太网)提供标准以太网接口。整个系统采用西门子工业级SCALANCE-X系列交换机进行构架^[1]。

1.3 普光气田工业以太网拓扑结构

工业以太网骨干网络采用双环网冗余结构, 沿工艺管线敷设42km埋地光缆, 与电力线路同时架设51km架空光缆, 使用长距离光纤模块将中控室、场站以及各个阀

室连接在一个环网上。与中控室较近的场站, 分别采用星型连接以光缆直接接入中控室系统。

骨干环网络利用西门子工业级交换机SCALANCE X308-LH组成1000Mbit光纤网络。骨干环网由西门子HSR协议提供单点故障保护, 保证骨干链路故障情况下通讯不受影响。骨干网络提供的1000Mbit/s全双工线速交换能力。并可通过VLAN划分方式, 对各子系统网络流量进行划分并优化流量。

1.4 Safety Manager SafeNet (安全网络)

Safety Manager通过其广泛的网络功能支持分布式安全解决方案(DSSTM)。安全管理网络提供了通过中央过程监控和控制能力分散过程保护的手段。在DSS网络中, 多个SM 控制器通过专用的以太网(或串行)通信链路互连。支持点对点 and 多点网络。为了实现通信的最佳可用性, 冗余Safety Manager配置需要使用冗余通信链接。

通信基于霍尼韦尔专有的TÜV-approved SIL 4 SafeNet通信协议。SafeNet是目前工艺工业中唯一的SIL4认证协议。SafeNet协议包括高水平的错误检测和恢复, 这使得它适合于交换与安全相关的信息, 同时保持最佳可用性。该网络还用于将诊断数据路由到中央操作员站和维护工作站^[2]。

Safety Manager网络中的通信基于主从(串行)或点对点(以太网)概念。在主从概念中, 主系统负责所有的通信活动。它从从属系统发起数据请求, 并向从属系统发送数据。通过对等概念, 可以与SafeNet拓扑中任何连接的SM 控制器进行数据通信。只有当使用以太网作为传输媒体时, 才有可能应用点对点概念。

SafeNet概念支持符合工厂设计的安全解决方案,每个独立的工艺单元都由独立的Safety Manager维护。这将在设备维护过程中最大限度地减少对设备的干扰。SM控制器支持SafeNet通信通过以太网,RS232,RS485和光纤。这允许通过第三方设备(黑通道)轻松集成故障安全网络,使用现有媒体、设备和电缆交换安全关键的Safety Manager数据,例如使用公共电话线、卫星或无线电链路。该TUV-approved功能为FPSOs、管道和其他远程系统应用提供了灵活的解决方案。它完全嵌入到Safety Manager设计中,不需要额外的工作来配置这种通信类型。

SafeNet可以在任何媒体上运行,包括过程控制基础设施。例如普光现场的工业以太网环网。但是,建议将SafeNet与其他物理基础设施隔离开来。操作安全不会受到影响,因为SIL 4认证协议只保证了安全性。然而,可用性取决于传输数据的基础设施和能力。在一个物理SafeNet网段中,最多可以连接63个控制器。一个SafeNet网络最多由1024个控制器组成^[1]。

1.5 普光气田工业以太网的功能

普光气田自动控制系统采用以计算机为核心的监控和数据采集SCADA系统,即数据采集与监视控制系统,SCADA系统包括安全仪表系统(SIS)、过程控制系统(PCS),其中,SIS系统采用SMS(Safety Management System)系统,完成装置或单元安全停车控制功能(ESD)。该系统对气田集输系统进行监控、管理、应急处置的自动化水平,为气田的生产运行提供安全保障。工业以太网将SCADA系统的各个控制节点链接起来,提供数据传输通道,因此,工业以太网的网络质量对SCADA系统数据采集、集中监控、连锁关断指令的传达至关重要,同时,也对整个气田的安全平稳运行提高保障。

2 安全仪表系统(SIS)网络架构及难点分析

针对普光集输系统现有网络硬件不能满足SIL3网络架构,国际上无大节点安全网络先例,现有西门子交换机与霍尼韦尔SM系统未认证等难点,探索实现网络硬件架构不变动,双环型以太网、SafeNet网络安全隔离新模式、47个大节点安全网络成功应用技术。

2.1 难点一:霍尼韦尔SM系统未与西门子交换机认证

为了保证PKS系统内数据在控制器、服务器和操作站之间顺畅传输,网络必须具备高效性和容错性。Honeywell与Cisco合作,开发了具有专利技术的网络-FTE(Fault Tolerance Ethernet),容错型以太网,大大提升了其SM系统可靠性。但是,普光气田地面集输工业以太网以西门子308交换机为基础的网络架构,并未与SM系统进行认证。

2.2 难点二:国内外无SM组建大节点SIS系统成熟经验

SM系统目前在国内应用约2000余套,大部分应用在炼化企业和化工企业,极少数应用在集输系统。上述企业在应用过程中,主要通过SM系统组建SIS、FGS、GDS等系统,且最大的系统数量不超过20套,即节点不超过20个。

本次普光气田集输SIS系统改造节点多达47个,据了解国外并无先例,导致本次在普光的应用无成熟经验可循。

2.3 难点三:光纤备用芯无法满足安全网络独立需求

SM控制器在运行过程中需要与PKS之间进行通信(用于人机交互);同时,SM控制器之间也需要进行通信(用于连锁逻辑执行)。

SM系统中安全网络要满足SIL3等级,需要通过安全管理器之间特殊的safenet通信实现,即用于SM控制器之间的通信。按照honeywell厂家要求,safenet需要物理上独立的网络链路。但是,备用光纤芯数严重不足,即现有光纤网络无法满足上述需求。

3 SIS系统网络优化

3.1 SafeNet网络设备兼容性测试

为确保SafeNet网络能在西门子组建的工业以太网中使用,用DEMO箱在现场开展为期1周的测试。分别在1个阀室、2座集气站各放置1台DEMO进行2组测试。

第一组技术方案,选取环网上的三个节点,通过搭建星型网络结构的方式,由普光1个阀室这一节点作为整个网络的主设备Master,其他两座集气站这两个节点作为整个网络中的两个从设备Slave。

从阀室发出信号,两个集气站均能正常接收,延迟时间为1秒。通讯2小时后,A网retries次数180,B网105,同时出现30次以上Timeout。将Timeout设置为5000ms,12小时后通讯中断,故障代码182(外部通讯故障),复位后消失。Timeout设为20000ms,运行12小时通讯未中断。

第二组技术方案,选取环网上的三个节点,通过搭建树型网络结构的方式,由阀室这一节点作为整个网络的中间设备,集气站作为阀室的Master、阀室既作为集气站的Master,同时也作为集气站的Slave,集气站作为阀室的从设备Slave。站场发出信号,另一座站场正常接收,未出现接收延迟报警,但出现retries以及丢包现象,相比于第一种方式由于通讯节点减少,retries以及丢包减少。

测试结论:3台Demo在现有工业以太网上Safenet运行正常,存在数据丢包现象,需要通过数据配置优化,解决了网络硬件不兼容问题。

3.2 SafeNet网络与PKS数据传输网络分开技术方案

鉴于在用光缆无法通过物理链接再单独组建专业安全网络，且无法重新组建经SM认证的网络架构等现实因素。通过研究，提出利用现有西门子308交换机备用电口，通过逻辑划分方式，将原网络划分为两个VLAN，VLAN1用于SafeNet，VLAN2用于PKS与控制器之间通信^[4]。

4 应用效果测试

现场开展A网和B网单独断开，AB环网同时断开1个节点和2个节点，中控室发出连锁指令，各集气站/阀室对中控室逻辑响应情况，均符合设计要求。

4.1 SIS系统在A网或B网硬件断开的情况下，中控

室能实现连锁控制，且参与测试的各场站/阀室系统运行正常。

4.2 SIS系统在AB环网同时出现一个断点（某个网络节点全部失效）的情况下，中控室依然能实现连锁控制，且参与测试的各场站/阀室系统运行正常。

4.3 SIS系统在AB环网同时出现2个及以上断点的情况下，断点区域内的SIS系统时不执行任何外部连锁。

4.4 考虑到SIS系统执行自身程序需要扫描时间、指令发送系统和接收系统存在扫描间隙，SOE记录周期设置为100ms，从参与测试的场站/阀室连锁执行情况来看，现有的网络记录延时不影响连锁控制^[5]。

表1 AB环网断点测试

序号	测试内容	中控室是否正常连锁控制	集气站连锁控制是否正常	阀室连锁控制是否正常	备注
1	A网断开	是	是	是	满足设计要求
2	B网断开	是	是	是	满足设计要求
3	A/B网同时1个断点	是	否	否	满足设计要求
4	A/B网同时2个断点	是	断点外正常 断点内连锁	断点外正常 断点内连锁	

5 结语

通过对普光气田集输安全仪表系统以太网安全网络的研究，结合工业以太网和安全网络的架构原理，摸清了集输系统安全网络存在的问题，通过对工业以太网重新划分VLAN，为安全仪表系统独立划出数据通道，提高安全仪表系统数据传输质量，缩短紧急情况下应急连锁关断响应时间，提高应急处置效率，为气田的安全平稳运行提供保障。

参考文献

[1]王丙强、毛仲德、刘俊成等。自动化仪表工程施

工及质量验收规范.GB 50093—2013

[2]胡迈清、朱瑞苗、郭晓明等。油气田及管道工程仪表控制系统设计规范.GB/T 50892—2013

[3]田京山、王静、李亚云等。石油天然气工程可燃气体检测报警系统安全规范.SY/T 6503-2022

[4]田京山、张德发、李玉明等。油气田工程安全仪表系统设计规范. SY/T 7351-2016

[5]田京山、程云海、王怀义等。油气田及管道工程计算机控制系统设计规范. GB 50823—2013