

基于以太网的长输管线 SCADA 系统

王文顺 汪秉文

(华中科技大学 控制科学与工程系 湖北 武汉 430074)

摘 要 :为改善以太网通信的实时性 ,系统引入了一种简单的数据调度模型。在此基础上 ,实现了长输管线的 SCADA 系统。说明了长输管线监测系统运行时的特殊性 ,就此提出了关于长输管线 SCADA 系统应用中的可扩展性问题 ,并就采集原理、数据通讯规约等方面提出了一种解决方法。

关键词 :长输管线 ;SCADA 系统 ;数据调度

中图分类号 :TP274⁺.2

文献标识码 :A

文章编号 :1673-629X(2007)02-0125-03

Long Distance Transportation Pipeline SCADA System Based on Ethernet

WANG Wen-shun , WANG Bing-wen

(Dept. of Control Sci. and Eng. , Huazhong Univ. of Sci. and Tech. , Wuhan 430074 , China)

Abstract :To improve the real-time communication performance of Ethernet , a simple data schedule model is introduced. A long distance transportation pipeline SCADA system is designed based on it. It illustrates the particularities during the running of the long distance transportation pipeline SCADA system , and puts forward the problem of system expansibility , and gives a performable method on data-sample , data communication stipulations of agreements.

Key words :long distance transportation pipeline ; SCADA system ; data schedule

0 引 言

在中国长输管线被广泛地用于石油、天然气等的输送。一般完整的输油管线由转油站、加温站、联合站、原油外输系统、油罐以及油田的其它分散设施组成。长输管线的各种设施的工作状态及采出油品的数据(主要有温度、压力、流量、含水率等)关系到油田生产的稳定及原油质量 ,同时管线的输差是采油厂计量原油产量的依据 ,以及输油管线运行安全的重要数据参照。因此长输管线的运行监测有着重要的意义。SCADA(Supervisory Control And Data Acquisition)系统具有良好的实时监控和数据采集分析能力 ,在过程监控领域表现出良好的发展前景。

由于一般油田地区的输油站、加温站、集输站分布较广 ,相对分散 ,长输管线纵深较大 ,各站间地形复杂且往往有山相隔。工业应用中的现场总线虽然实时性好但是成本过高 ,而无线技术由于地形的复杂 ,存在勘测和调试等困难。采用企业现有的局域网为基础 ,实

现数据的共享以及实时监控 ,实现油田数据信息化、网络化 ,可实现数据全局共享 ,厂长、总工等管理人员利用现有的网络系统查看其监控点的数据 ,打破各个监控现场相互之间长期形成的“信息孤岛”局面。

文中从网络架构、采集原理、记录方式、数据通讯规约、数据存储等多方面 ,对油田广泛分布各地的监控站点的信息提出了输油管线监测计量解决方法。

系统在设计上采用 C/S + B/S 模式 ,其中 C/S 部分负责数据采集与存储 ,油田各个非现场单位采用系统提供的 WebService 浏览数据变化以及进行生产所需的计量工作。

1 通信模式

根据油田工业生产具体需求 ,为了选择合理、经济的通信方案 ,必须因地制宜 ,在充分考虑资金投入可能性的前提下 ,高度重视油田所处的环境和条件 ,这也是影响通信系统设计选型的重要因素。

系统数据总线分现场数据采集总线和数据传输总线两部分。其中现场采用 RS485 总线有线组网 ,具有投资少见效快、数据带宽经济适宜、技术简单的特点。另外同时也由于 RS485 总线受通信距离的限制 ,结合以太网的优势使系统接入局域网 ,使除底层仪表数据

收稿日期 2006-04-12

作者简介 :王文顺(1978-) ,男 ,天津人 ,硕士研究生 ,研究方向为计算机集成控制及网络通信技术 ;汪秉文 ,教授 ,博士生导师 ,研究方向为生产过程综合自动化系统集成优化与决策、人工智能、专家系统及其应用、系统故障监测与诊断。

以外数据流均在以太网内。

整体结构上系统可以分为 4 层,分别是以太网网络为基础的厂管理层,信息中心(数据存储),输油站点(监控房)和以 RS485 为基础的仪表现场。服务程序运行于信息中心服务器主机,负责数据收集和写入数据库。客户端程序运行于站点(监控房),现场的操作人员可以通过输油站点装有的监测软件,随时对采油设备的运转状态、生产数据、工作参数进行监视和设置。

1.1 以太网数据总线通信改进

根据以太网实时扩展的不同技术方案,可将其通信协议模型分为 6 类:

- ①是经过常规最大努力提高实时性,一般工业以太网的通信协议模型;
- ②采用在 TCP/IP 之上进行实时数据交换方案;
- ③采用经优化处理和提供旁路实时通道的通信协议模型;
- ④采用集中调度提高实时性的解决方案;
- ⑤采用类似 Interbus 现场总线“集总帧”通信方式;
- ⑥在物理层使用总线拓扑结构提升以太网实时性能^[1]。

由于现场局域网网络数据流量较大,因此为减少冲突,避免给数据传输造成损失,基于传输整形方法改进报文格式,使传输层(如 TCP/UDP)负载始终保持在某个较低的规定值,利用低负载、低冲突概率的原理来保证消息传输时间的可靠性^[2]。建立了一个简单的基于时间的调度模型,由于工业过程中信息通信的多样性和信息实时通信的重要性,把信息区分为周期和非周期,并采用集中控制策略,在任何时候单网段上只有一个活动节点起到节点仲裁作用即负责网络上各个节点之间的信息通信^[3]。周期信息如(传感器变送器现场设备周期性的测量值)具有时间确定性的特点,可以通过建立调度表来管理周期信息通信,但是非周期信息具有相对复杂的发生时间不确定性(如现场设备的报警信号控制参数调整等),因此需要进行特别的处理^[4]。

* 周期数据的调度。

服务器程序自动根据节点挂接到服务器端的顺序进行仲裁,然后对有效节点进行数据采样。这里仲裁的目的是验证节点的有效性,有连接而某间隔内无数据的或同节点地址多个连接中的首个连接视为无效节点。

另外由于各站有效数据量不一,数据调度程序会在每次通信会晤后,如果发现情况变化,会根据各站情

况以及数据实时性的要求重新安排周期性数据的调度周期。

* 非周期数据的调度。

非周期数据分为报警信息和控制信息两种,即分为两级。报警信息和控制信息优先级均高于普通信息。其中报警信息优先级别最高,控制其次,优先级高的数据信息优先发送,以保证非周期数据信息以最快速率到达。在存在非周期数据的情况下仲裁器保证高优先的数据优先发送^[5]。仲裁器根据数据信息的不同级别予以排队,并保证非周期数据迅速送至发送器模块立即发送。

1.2 现场数据采集总线

现场数据采集部分是由 RS485 总线将各数据采集仪表相连。计算机通过轮询总线上各仪表来获取现场的实时数据信息。由于 485 通信的半双工机制,所以数据查询必然是周期性轮询,调度图安排如图 1 所示。当有非周期性信息(如控制信息)时,仲裁方式采用如上以太网类似的方式,中断数据轮询优先发送非周期数据。

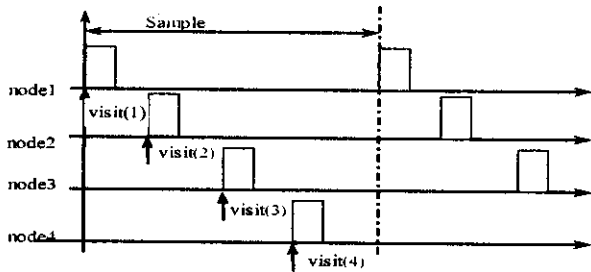


图 1 以太网总线的调度

2 数据采集与处理

2.1 现场数据采集格式

现场通过二次仪表与传感器相连实时采集现场数据。计算机通过控制柜内的 RS485 总线轮询各仪表数据。数据采集部分采用传统的 C/S 架构。输油站、加温站安装客户端数据采集软件,负责从现场控制箱采集数据(如图 2 所示)。现场需要采集的数据量主要是压力、温度、流量,累计流量、含水量等信号。现场信号类型分模拟信号和脉冲信号两种。模拟信号的数据采集仪表为多通道数据巡检设备,脉冲信号采集仪表为单一量数据采集仪表。

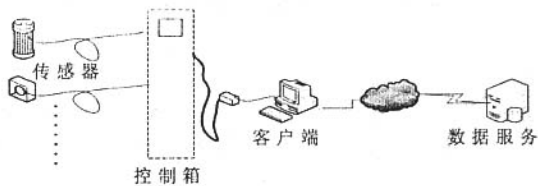


图 2 数据采集的部分的结构

现场的数据采集,通信协议为 modbus。

2.2 以太网数据信息的组织形式

对长输管线来油和外输(长输管线两端)的温度、压力、流量、含水率的监测能够监测现场设备的用行情况,对来油和外输侧累计流量差值的比较,能够监测输油管线输油量,以及油量损失。

由于采油站、加温站、集输站各站功能管线的特殊性,各站采样数据的种类及数量不同(比如有的管线需要采集温度信号,有的不需要,有的管线采集含水率,个别则不需),拥有长输管线的数量、名称不同,甚至相同情况下仪表数据通道使用情况也不同。

另外还要考虑到可扩展性系统有可能需要增加一种采样数据类型(比如压力、温度等),增加一条管线,增加一台仪表,甚至增加、改变仪表数据通道的使用情况。因此系统通信协议为保证协议具有协议的可扩充性,使适当的硬件变更,通道使用情况变化尽量少的甚至不会影响软件使用情况和稳定性。

通过对协议信息的适当配置使系统实现数据的自动识别。

※ 配置信息的获取。

配置信息的获取由手动和自动部分组成,如图 3 所示。

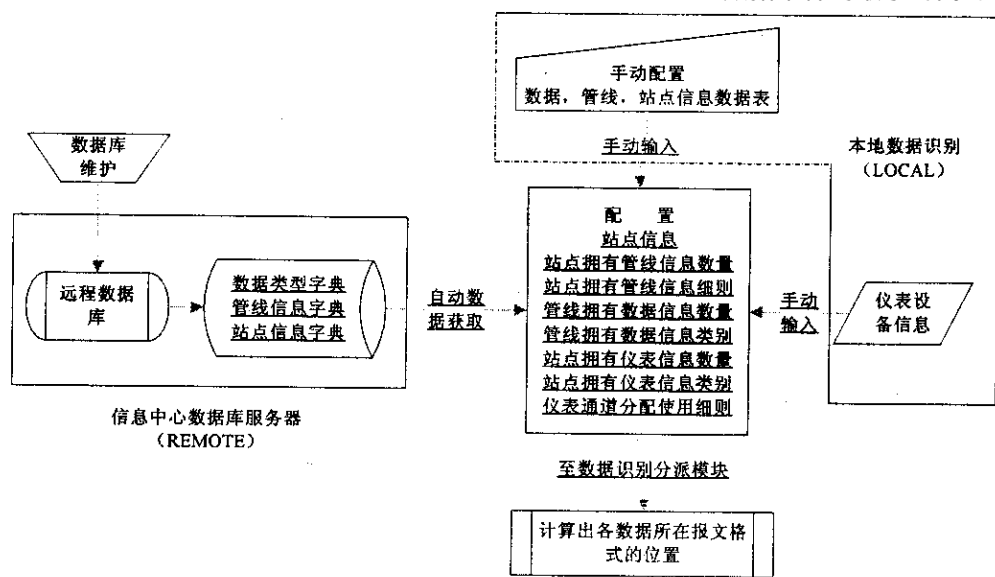


图 3 数据协议识别流程

所谓自动就是在数据库服务器配置好的情况下,程序自动下载数据信息,这样做的优点是:减少操作人员的干预,不需要操作者对数据库信息有太多认识,能够保持数据信息与数据库信息良好的一致性(管线、站点、数据类型字典的标示,统一由服务器程序分配)。

手动操作是在使用前在配制导航系统的指导下进行的操作,需要对系统数据格式有所了解,配置错误

将导致数据库服务器无法识别。

另外由于输油过程中可能出现的过滤阀堵塞等问题,现场输油管线上一般都有备用管道或者旁通,备用管线或旁通一般也会采集数据如压力、温度等。这样一条管线就有多组数据,而实际中只有一条正在使用。根据现场主备用设备倒换时数据的变化特性,制定判定准则,选取适当数据上传至数据库。采样后,数据处理程序需要做的就是将多组同类型数据映射到相应的管线数据组(每组包含一条管线的一系列相关数据)内部的同一个采样数据类型上。如图 3 所示,识别程序将会自动判定。

※ 报文格式(如图 4 所示)。

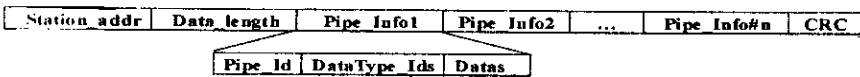


图 4 数据报文格式

其中 Station_addr 为数据来源站点标示;Pipe_Id 为站点所辖管线信息标示;DataType_Id 为管线采样的有效数据类型序列;Data 为有效数据内容。

配置所得各信息升序排列,依次映射到报文中,因此报文中 Pipe_Id, DataType_Id(数据类型 ID)以及数据内容,均为有序的有效数据。

2.3 数据的采样时间

数据采样的最小时间与现场仪表的反应时间和仪

表数量乃至仪表通道的使用情况相关。因此各站采样最小时间也不相同。若系统各站采样时间相同,则管线数量较多以及采样的数据类型种类也较多的站点相对其他站点总线负荷会较重,因此为了减少网络负担,保证各站通信的实时性,制定一个平衡的措施。

各站根据对实时性的不同需求定义各

自不同的数据采样时间。

3 程序实现

数据采集程序采用 C/S 模式,分客户端程序和服务端程序两个部分。程序主要模块分为:总线调度模块、仲裁模块、以太网通信模块、RS485 通信模块、数据

配置 IPSec。当主机 A 要向主机 B 发送数据包时,路由器(网关)C 要对数据包进行封装,封装后的包通过隧道穿越公用网络后到达路由器(网关)D,由 D 对该数据包解封,再转发给主机 B。反之亦然。

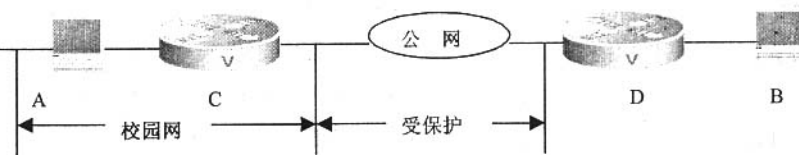


图 4 路由级的安全保护

除此之外,还可以通过隧道嵌套的方式实现网络安全。当配置了 IPSec 的主机通过隧道接入到配置了 IPSec 网关的路由器,并且该路由器作为外部隧道的终结点将外部隧道封装剥除时,嵌套的内部安全隧道就构成了对内部网络的安全隔离。

5 结束语

由于 IPSec 提供了两种工作模式:传输模式和隧道模式。再结合 AH 和 ESP 提供的不同的安全服务,在 IPSec 的实际应用中就有了多种选择。总的说来,ESP 隧道模式认证和加密服务所提供的安全性要强于传输模式,但由于隧道模式将比传输模式服务占用更多带宽,所以如果在带宽利用率非常重要的情况下,传输模式可能是更合适的选择。另外,尽管理论上 ESP 隧道模式认证提供的安全服务不如 AH 传输模式的安全性高,但由于包含 IP 数据包源地址的内部 IP 头被

加密了,因此,它可以提供一定的数据流保密服务,而这是 AH 所不具备的。

未来几年里,基于 IPv6 的校园网建设将是大势所趋,而校园网安全机制研究也是重中之重。IPv6 作为新一代的网络互连协议是一个建立可靠的、可管理的、安全和高效的 IP 网络的长期解决方案,其先进性和灵活性正在得到越来越多人的认可。从技术上看,并不是使用了 IPv6 就能彻底保证安全,因为 IPv6 虽然内在具有一些安全的特性,但是应用系统、各种各样的基础设施,要充分利用这些特性才行。

参考文献:

- [1] 华为 3COM 技术有限公司. IPv6 技术[M]. 北京:清华大学出版社,2004.
- [2] 江伟. 基于 Linux 的 IPv4 和 IPv6 的互连研究[D]. 合肥:合肥工业大学,2005.
- [3] Kent S, Athinson R. RFC2403. IP Encapsulating Security Payload[S]. 1998.
- [4] Kent S, Athinson R. RFC2402. IP Authentication for the Internet Protocol[S]. 1998.
- [5] Kent S, Athinson R. RFC2401. Security Architecture for the Internet Protocol[S]. 1998.
- [6] 陈卓. IPsec 中 ASP 和 ESP 协议的比较与应用[J]. 计算机应用与软件,2004(7):105-106.
- [7] 刘玉山. IPsec 原理及其在网络安全中的应用[J]. 山东电子,2004(1):39-41.

(上接第 127 页)

报识别模块,数据库存储模块(包括程序与数据库数据同步部分)。

4 总结

两类通信总线的结合使用节约了成本也使系统层次更为突出,加入调度算法后的数据通信,增强了数据的可靠性和实时性。可配制和智能化可自动识别的数据格式使系统更具适用性。系统的数据采集与处理部分具有以下特点:

- * 当硬件变动和通道使用情况变更时,保证用户最小程度上的配置变动,安装简便。

- * 数据调度使数据冲突概率减小,通信更具实时性,通信更安全。

- * 采样时间由用户自定义,根据采样时间的间隔适应不同数据通道、仪表,甚至不同采油站点对数据通信实时性的不同要求。

- * 系统具有较好的可扩展性,简单配置就可以增

加需要采样的输油管线,增加采样管线,管线需要采样的数据类型,以及为某个数据采样点增设多条采样备用管道。

- * 具有智能的用户连接,能自动断开和恢复与服务

参考文献:

- [1] 缪学勤. 论六种实时以太网的通信协议[J]. 自动化仪表,2005,26(4):26-31.
- [2] 杨仕平,桑楠,熊光泽. 基于 Ethernet 技术的安全关键实时网络[J]. 软件学报,2005,16(1):121-134.
- [3] 冯冬琴,廖智军. 基于以太网的工业控制网络实时通信模型研究[J]. 仪器仪表学报,2003,24(4):714-718.
- [4] 王智,王天然,孙优贤. 工业实时通讯网络(现场总线)的基础理论与现状(上)[J]. 信息与控制,2002,31(2):146-163.
- [5] 陈积明,王智, Song Ye-qiong, 等. 基金会现场总线非周期实时信息的调度问题研究[J]. 浙江大学学报,2003,37(3):273-277.