油气管道 SCADA 系统数据传输的安全风险及其解决方案

黄　河　张　伟　祁国成　闫　峰　陈　鹏
中国石油北京油气调控中心

黄河等.油气管道 SCADA 系统数据传输的安全风险及其解决方案.天然气工业,2013,33(11):115-120.

摘　要　中国石油天然气股份有限公司的长输油气管道在北京油气调控中心实施集中调度,逐渐形成了依托于通信网络的分布式 SCADA 系统,对安全提出了更高的要求。当前油气管道 SCADA 系统的数据传输过程中存在的主要风险因素有:缺少接入控制、使用开放的标准协议、采用明文传输并接入了大量不安全的网络设备,而相应的防护措施不多,特别是中控系统和站控系统之间的数据传输依托光纤网、卫星和公网,使用基于以太网 TCP\IP 的应用层协议,存在较大风险。为此,结合国内外已有的 SCADA 安全相关的标准和一些学者提出的防护策略,提出了一种安全防护解决方案,即通过建立基于认证和权限控制的接入控制机制、部署硬件防火墙和加密网关、加强对外安全等方法进行安全防护。该方案可为工程设计提供参考。

关键词　油气管道　SCADA 系统　安全　数据传输　协议　接入控制　认证　权限　加密
DOI:10.3787/j.issn.1000-0976.2013.11.020

Risk analysis of data transmission security in an oil and gas pipeline SCADA system and countermeasures

Huang He, Zhang Wei, Qi Guocheng, Yan Feng, Chen Peng
(*PetroChina Oil and Gas Pipeline Control Center*, *Beijing* 100007, *China*)

NATUR. GAS IND. VOLUME 33, ISSUE 11, pp.115-120, 11/25/2013. (ISSN 1000-0976; In Chinese)

Abstract: As the Beijing Oil and Gas Control Center plays its role in undertaking the centralized control of long-distance pipelines operated by PetroChina, a distributed SCADA system relying on communication network is gradually formed, for which security is highly required. There exist many risks in data transmission of such a SCADA system at present: lacking access control, using open standard protocols, transmitting in plain texts, and connecting a plenty of insecure network devices without appropriate protection measures. Especially, a potential higher risk even threatens the data transmission between the central control system and station control system with an application layer protocol based on Ethernet and TCP/IP, which relies on the optical fiber network, satellite and public network. In view of this, according to the standards published at home and abroad associated with SCADA security and many security protection strategies proposed by some scholars, this paper presents the following countermeasures: setting up an access control mechanisms based on authentication and authority control, deploying hardware firewalls and encryption gateways, strengthening the exterior security, etc. This study will be a reference for engineering design.

Keywords: oil and gas pipeline, SCADA, security, data transmission, protocol, access control, authentication, privilege, encryption

---

基金项目:西气东输二线关键技术研究重大科技专项(二期)(编号:2009E—0102)。

作者简介:黄河,1984 年生,工程师,硕士;主要从事管道自动化、智能化的研究工作。地址:(100007)北京东城区东直门北大街 9 号中国石油大厦 B 座中国石油北京油气调控中心。电话:(010)59983718。E-mail:riverhuang@petrochina.com.cn

油气管道 SCADA(Supervisory Control And Data Acquisition,监视控制与数据采集)系统,是一种针对油气长输过程进行数据采集、监视和控制的工业控制系统,通过对现场设备信号进行实时采集、加工、汇总、计算和展示,以实现设备监控、参数调节以及信号报警等远程监控功能[1]。

中国石油北京油气调控中心(以下简称调控中心)针对中国石油天然气股份有限公司所属的长输油气管道实施集中式的远程监控、操作运行、调度管理和应急协调,以优化管道运营管理体制,提高油气管输效率。目前中国石油油气管道 SCADA 系统已完成从集中式到分布式的过渡发展,管网调度实行三级控制,即中心控制(以下简称中控)、站场控制(以下简称站控)和就地控制。分布式的 SCADA 系统运行需要依托通信网络。

随着油气调度一体化、网络化的发展,SCADA 系统安全成为保证油气管道生产平稳运行的关键因素,直接影响石油工业生产运行乃至国家经济命脉安全。据美国仪器系统和自动化协会(ISA)的一份报告称,当前各种 SCADA 系统普遍存在弱点,安全评估和风险防范迫在眉睫[2],重点区域和重要环节的安全防护已经成为一项重要的研究课题。以往有针对调控中心的安全防护研究,较常见的策略有冗余、灾备[3]。

笔者将针对油气管道 SCADA 系统在数据传输环节中存在的风险进行分析,结合国内外已有的标准和先进技术,提出了有效的安全防护解决方案。

1 油气管道 SCADA 系统数据传输

油气管道 SCADA 系统采用分布式架构,可以分为中控系统、站控系统和通信系统等 3 个主要部分,如图 1 所示。

为保证调控需要,日常生产过程中 SCADA 系统内全天 24 h 不间断地传输着大量实时数据。这些数据可粗略分为两类:即上行数据和下行数据。上行主要是采集的量测数据,下行主要是控制指令。数据传输过程可以分为两个阶段:①站场内站控系统和现场设备之间的数据交换;②中控系统和站控系统之间的数据交换。数据传输过程的实时性、安全性和可靠性要求都非常高。

1.1 数据传输的特点

1)数据传输吞吐量大、实时性强,据粗略统计,系统并行监控的数据点总数接近百万,时间精度通常为毫秒级。

2)进行数据交换的设备之间通常存在上位、下位关系[4]。上位设备是可以对其他设备下发指令进行操作控制的一类设备,例如 SCADA 服务器、PLC。下位设备负责发送数据给上位设备并执行收到的操作指令,例如传感器、驱动器。需要特别说明的是,上位、下位是相对的概念,并不是绝对的分类,例如 PLC 相对于 SCADA 服务器是下位设备,相对于传感器、驱动器则是上位设备。某些上位设备之间也存在数据交换,例如 SCADA 服务站之间需要进行数据共享。

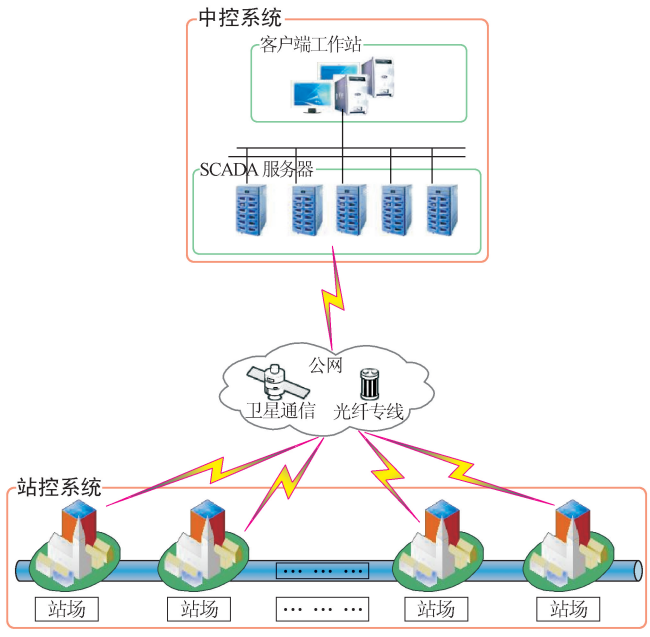

图 1 油气管道 SCADA 系统结构图

3)数据传输具有不对称性[5]。例如,从下位发往上位的采集数据远远大于上位发往下位的控制指令。

4)数据传输还具有优先级特性和可选择性[4]。例如 ESD 等应急指令应当较普通控制指令优先下发;某些设备仅接收报警等关键信息。

5)数据传输依托于通信网络,需要使用特定的通信协议,协议的选择需要考虑满足上述的数据传输特点。

1.2 常用通信协议

SCADA 数据传输使用的通信协议,应能保证数据在限定时间内正确送达。根据美国燃气协会(AGA)发布的 AGA-12:1 标准[6],SCADA 系统中使用的协议有近 200 个,大都是由不同厂商研发提供的私有协议。经过多年的发展,一些开放的标准协议在工业界得到广泛应用。表 1 中列举了油气管道 SCADA 系统中最常用的几种标准协议。

目前,一些工业级标准协议中已经明确提出了安全相关内容[7],比如最新版本的 DNP3 标准中就加入了安全相关内容,支持在进行关键信息交换时以“质疑—回应”(challenge-response)机制进行认证。

表 1　油气管道 SCADA 系统常用协议表

协议名称	发布组织
IEC-104	IEC
DNP3	IEC
MODBUS	MODBUS-IDA
CIP	ODVA
ControlNet	ControlNet International
DeviceNet	ODVA

1.3　站控系统和现场设备传输数据

站控系统和现场设备通常都部署在同一站场内，站场内一般建有百兆/千兆的局域网或串行通讯连接，并与外界网络进行了物理隔离。

站控系统可分为 SCADA 工作站和 PLC 两部分，工作站上安装了服务端、客户端一体化的站控 SCADA 软件。此外，可能还配备一个数据通信网关(GW)用以协议转换。

站控系统通过 PLC 连接现场传感器、驱动器等设备，并进行信号采集和控制，常用的协议有 MODBUS RTU、DeviceNet 等。PLC 之间可以使用 MODBUS PLUS 或 ControlNet 协议进行数据交换。PLC 和 GW、SCADA 工作站之间的数据传输使用 MODBUS TCP 或 CIP 协议。GW 和 SCADA 工作站之间的数据传输可以使用 IEC-104、DNP3、MODBUS TCP、CIP 等协议。

根据不同的数据流策略，数据可以在 PLC、GW 或 SCADA 工作站等不同处实现汇聚，如图 2 所示。

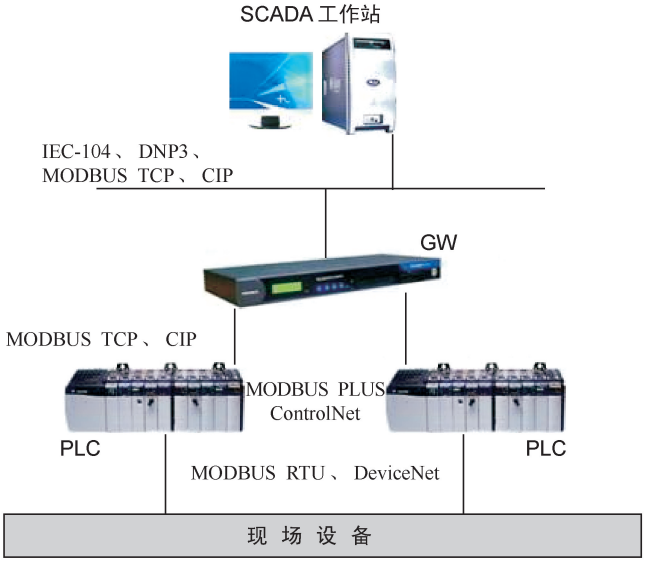

图 2　站场内数据传输示意图

1.4　中控系统和站控系统传输数据

中控系统和站控系统通常部署在相距很远的不同地方，之间利用通信系统进行数据传输。油气管道 SCADA 通信系统主要以光纤通信为主信道，卫星或租用公网为备用信道。一些没有进行光通信改造的管道，仍利用微波、公网等通信系统。中控系统和站控系统之间的通信采用 IEC-104、DNP3、MODBUS TCP、CIP 等多种协议。

中控系统可分为 SCADA 服务器和客户端工作站两部分，此外还配备一个总数据通信网关(MGW)。

中控系统和站控系统之间的数据传输，一般有两种方式，如图 3 所示。

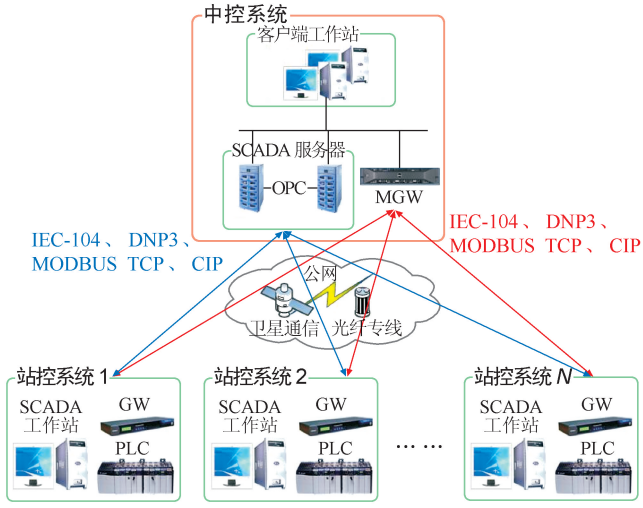

图 3　中控、站控数据传输示意图

一种方式是，中控系统的 SCADA 服务器使用 MODBUS TCP、CIP 等协议直接采集和控制站控系统的 PLC，或者使用 IEC-104、DNP3、MODBUS TCP、CIP 等协议采集站控系统 GW 上的数据或下发指令。

另一种方式是，中控系统通过 MGW 使用 IEC-104、DNP3、MODBUS TCP、CIP 等协议实现对所有站控系统的数据采集和控制指令下发。

此外，中控系统的多台 SCADA 服务器之间还可以使用“用于过程控制的对象连接与嵌入”(OPC)协议进行数据交换。

1.5　外部系统数据传输数据

日常生产中，中控系统需要和许多外部系统进行数据交换，包括管道生产管理系统、模拟仿真系统、能耗计量系统、批次跟踪系统、调度培训系统、调度评价系统等。

目前一般有两种方式实现中控系统和外部系统的数据传输：

1)数据库直接读写方式。中控系统使用 OPC 协议向 PI 数据库写入数据作为镜像,外部系统直接连接访问 PI 数据库。比如模拟仿真系统就通过这种方式间接获取 SCADA 实时数据。

2)文件传输方式。源系统将数据写入一个 XML 文件中,并传至一个共享文件区或 FTP,目标系统将自动读取文件获取数据。比如成品油的批次计划信息就通过这种方式传入 SCADA 系统中。

2 风险分析及解决方案

2.1 风险分析

当前油气管道 SCADA 系统中数据传输安全方面的防护措施不多,风险主要存在于中控系统和站控系统的数据传输过程,主要有以下几个方面。

2.1.1 非法接入风险

Risley 等认为攻击者无法入侵物理隔离网络的看法是一种理解错误[5],Byres 更是直言物理隔离在现实世界中毫无用处,建议工业用户开始放弃这种方法[8]。

中国石油一直在大力建设中控系统和站控系统的物理安全防护设施,但是若干系统之间的数据交换需求促使各个简单孤立的系统逐渐形成一个复杂的 SCADA 网络。

现在的网络技术发展非常快,对于任何形式的网络都可以提供多种接入方式,SCADA 网络也不例外。局域网无论怎么隔离,只要有对外的数据传输,就总会通过一根专线、一台设备或者一个内网和更大的企业网相连。攻击者完全有可能利用这些链接获取到对站场设备的接入途径[4],一旦非法接入,后果不可设想。

2.1.2 协议开放风险

Byres 等认为使用私有协议是更安全的[9]。但是目前出于工程实施难度和成本的考虑,油气管道 SCADA 系统中使用的是一些开放的标准协议,且多是基于以太网和 TCP/IP 协议栈的应用层协议。

标准开放的同时,也使得攻击者能够更容易、更深层次地理解 SCADA 网络运行的机制,从而大大增加了风险。

2.1.3 明文数据风险

油气管道 SCADA 系统中传输的是明文数据,没有进行特殊的安全处理,其保密性、完整性无法得到保证。

数据在传输过程中或者存储在终端设备时都有可能被侵入网络和设备的攻击者轻松获得、更改。如果攻击者对数据进行了篡改,甚至伪造重要的控制指令,系统本身不具备任何能力发现。一旦这些数据进入 SCADA 系统,可能引起严重事故,造成不可估量的损失。

2.1.4 非定制的软硬件产品带来的风险

油气管道 SCADA 系统在建设过程中,很少选择定制产品,而是选择市场上较大厂商的典型软硬件产品,这样做大大降低了设计难度和建设成本,但同时也带来了潜在的风险。

由于绝大多数产品不是为了 SCADA 系统专门设计的,都不带任何安全功能。这些产品通常兼容一些基于以太网和 TCP/IP 协议栈的应用层协议,在基于 TCP/IP 的网络攻击面前非常脆弱。如果不加入一些专门的网络安全设备,SCADA 网络和普通的互联网一样,安全性和可靠性非常低。

2.2 安全标准

针对上述数据传输存在的风险进行安全防护设计时,应当遵循目前已有的油气管道 SCADA 系统安全相关标准。表 2 中列举了本文参考文献的主要标准[10-13]。

表 2 油气管道 SCADA 系统安全相关标准表

标准号	说 明
API 1164	美国石油学会 SCADA 安全
AGA-12:2	美国燃气协会 性能测试结果
IEEE P1711-2010	美国电气和电子工程师协会同 AGA-12:2
Q/SY BD 46-2010	中国石油企业标准 油气管道 SCADA 系统网络安全技术规范

2.3 常见安全策略

2.3.1 接入控制

接入控制是一种常见的 SCADA 系统安全策略。完善 SCADA 系统的接入控制机制是非常必要的。对于企业级安全来说,必须严格执行网络安全接入管理制度,并辅以适当的技术手段,才能事半功倍。

要在技术层面实现接入控制,首先要做到针对所有的接入对象进行认证,这里的对象可能是用户,也可能是设备。然后,应当赋予通过认证的用户相应的角色和权限。

2.3.1.1 认证

针对用户的认证可以保证控制指令是授权用户下达的,针对设备的认证可以保证数据来自正确的来源。双重认证比较严格,要求用户必须在特定的设备上才能接入系统,且只能在该设备上查看数据和发送指令。

身份认证的实现一般有软硬两种方式。软件实现

可以是软件系统登录时要求使用用户名、口令进行身份认证，也可以结合 CA 证书。硬件实现可以使用 USBKey，或者智能卡[4]。软硬方式也可以结合起来，加大认证安全的强度。

有一种较新的做法是在现场设备近端部署支持 DNP3 协议并具有认证和完整性功能的设备，在中控系统内部署相对应的软件或硬件[14]，在数据传输时利用“质疑—回应”机制进行认证。这种方式可以确保现场一些特别重要的设备收到来源合法的控制指令，但是仅支持 DNP3 协议，而且实施成本非常高。

2.3.1.2　权限控制

用户权限一般是通过角色来赋予的，角色是权限的集合，系统定义了若干个角色，并分配给用户，用户只能进行权限范围以内的操作。

在 SCADA 系统中，通常有多种角色，比如调度员、工程师、管理员以及开发商等。使用基于角色的分配策略大大简化了权限管理工作。

当用户通过认证后发出操作请求时，需要检查其是否具备实施该操作的权限。如果权限条件不满足，系统将自动拒绝用户的请求。

用户认证和权限的信息，通常统一存储在一台身份认证服务器中。

2.3.2　数据加密

加密是一种有效的数据安全策略，可以有效地提高数据的保密性和完整性。SCADA 系统的加密可以在不同的网络分层实现，比如在应用层加密和在网络层加密。

2.3.2.1　应用层加密

应用层加密是在应用通过网络进行数据传输的接口中来实现的，通信双方均需支持相匹配的加解密算法。运行时，需要依赖复杂的加密确认机制，每次发送和接收数据前，应用之间需先交互确认彼此加密、解密状态，才能开始传输数据。应用层加密方式与数据传输的实际网络路径无关，但是其扩展性较差，系统一旦进行应用扩展，新的应用必须实现数据加解密功能。

2.3.2.2　网络层加密

网络层加密实现较之应用层加密实现更为底层。网络层加密直接对网络通道进行加密，与具体的应用无关，在加密通道中传输的数据都将获到保护。这种方式将加密功能和系统应用分离开来，有利于系统扩展。不过网络层加密需要引入额外的加密设备，一定程度上增加了建设成本。

在 AGA-12:2 和 IEEE P1711-2010 标准中[11-12]，均定义了子站串行保护协议(SSPP)，要求加密设备必须以网络嵌入式(BITW)的形式串行接入网络，并部署在数据传输网络路径的起始两端，加密应对数据传输过程实现透明。

2.3.2.3　密钥管理

数据加密还需要建立有效的密钥管理机制，AGA 也建立了并仍在完善相关的标准。Kang 在他的研究中列举了一些有效的密钥管理策略[15]。

2.3.3　网络安全设备

网络安全设备是一种特殊的硬件设备，它们结合了接入控制和加密策略，针对特定需求定制开发软件并嵌入到硬件中。这些设备可以用来对数据传输网络进行安全防护，常见的有硬件防火墙和安全网关。

2.3.3.1　硬件防火墙

硬件防火墙具有软件防火墙所有功能，并具有内容过滤(CF)、入侵侦测(IDS)、入侵防护(IPS)以及虚拟专用网络(VPN)等功能。

硬件防火墙可以在应用系统访问控制、流量控制、防病毒网关、用户权限控制、恶意代码的阻止、异常行为阻断等方面对 SCADA 网络进行控制。

2.3.3.2　安全网关

通常，SCADA 系统内的数据网关是用来进行协议转换的，并不具备安全功能。安全网关是一类针对数据传输安全需求设计出来的设备，除了兼容油气管道 SCADA 系统常用的协议，还提供认证、加密、杀毒等安全功能。

2.4　油气管道 SCADA 系统数据传输安全方案

为降低前述的数据传输风险，本文参考常见安全策略，结合中国石油油气管道 SCADA 系统的实际情况，针对中控系统与站控系统的数据传输过程，初步设计了以下安全方案。

2.4.1　建立接入控制机制

部署证书体系，为全网用户提供统一身份标识；部署身份认证服务器，为全网用户提供统一身份认证服务，并统一管理权限；部署网络认证服务器，加强全网统一接入认证管理。

采用 USBKey、证书、口令相结合的身份认证方式：SCADA 系统验证用户身份时，首先确认用户是否插入 USBKey，然后验证口令是否正确，最后确认证书是否有效。当以上三者均通过验证，用户才能进行权限内的操作。

2.4.2　部署网络安全设备

在中控系统和站控系统接入通信系统的边界上部署硬件防火墙和加密网关，以抵御基于 TCP/IP 的网络攻击，并对传输数据进行加密保护。

加密网关需特别定制且具有以下特点：

1)选用国家密码管理局认可的商密算法。

2)支持网络层 BITW 部署模式，对原有网络和使用协议无影响。

3)支持对端无加密网关的部署模式。

4)支持对通道加密，仅对重要设备数据进行加密。

5)支持单向加密，可仅对下行指令加密，对上行数据不加密。

6)支持旁路(bypass)功能，当设备无法正常工作时，可以自动切换为明文传输模式。

网络安全设备的部署方式如图 4 所示。

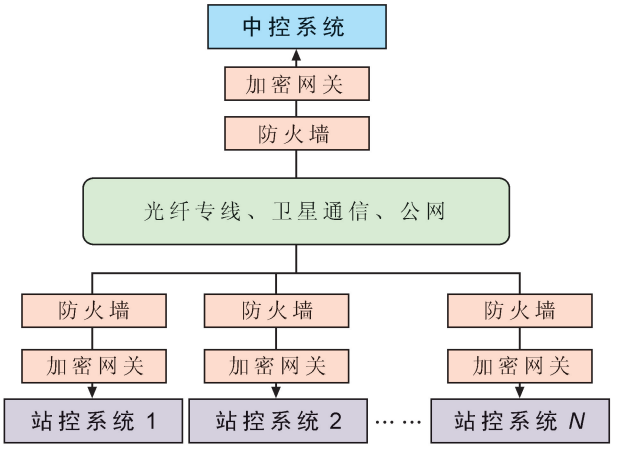

图 4 网络安全设备部署示意图

此外，还应部署设备管理中心和密钥管理中心，对全网的加密网关进行管理。

2.4.3 *加强对外安全*

将中控系统和外部系统进行物理隔离，并对所有系统及设备进行认证；对所有数据传输通道进行加密；使用加密的文件传输方式。

3 结束语

油气管道 SCADA 系统安全直接影响油气管道生产安全，乃至国家能源、经济安全，因此格外重要。该系统经过多年的发展，已经形成依托于通信网络的分布式架构。本文针对该系统中数据传输的情况进行了介绍，并对目前存在的主要风险进行了分析。参照国内外一些 SCADA 安全方面相关的标准，结合中国石油油气管道 SCADA 系统建设现状，本文提出了一个基于接入控制和加密的数据传输安全方案，并计划在未来的工业实验中进行验证。

参 考 文 献

[1] National Transportation Safety Board (NTSB).Supervisory control and data acquisition (SCADA) in liquid pipelines [R].Washington DC:NTSB,2006.

[2] BOYER S A.SCADA supervisory control and data acquisition[M].USA:International Society of Automation (ISA),2010.

[3] 谢安俊.油气管线 SCADA 系统调度控制中心的安全策略[J].天然气工业,2005,25(6):113-115.
XIE Anjun.Safe strategy of SCADA system dispatching and controlling center for oil/gas pipeline[J].Natural Gas Industry,2005,25(6):113-115.

[4] VINAY M I, SEAN A L, RONALD D W.Security issues in SCADA networks[J].Computers & Security,2006,25(7):498-506.

[5] RISLEY A, ROBERTS J, LADOW P.Electronic security of real-time protection and SCADA communications[C]// Fifth Annual Western Power Delivery Automation Conference,1-3 April 2003,Washington DC,USA.

[6] American Gas Association (AGA).cryptographic protection of SCADA communications, Part 1: Background, policies and test plan (AGA 12,Part 1)[S].Washington DC:AGA,2006.

[7] KEVIN M.Data and command encryption for SCADA[R].Schneider Electric,Canada,2012.

[8] BYRES E.Privacy and security the air gap:SCADA's enduring security myth[J].Communication of the ACM,2013,56(8):29-31.

[9] BYRES E, LOWE J.The myths and facts behind cyber security risks for industrial control systems[C]// VDE Congress,VDE Association for Electrical,Electronic & Information Technologies,October 2004,Berlin,Germany.

[10] American Petroleum Institute (API).SCADA Security (API 1164)[S].API,2004.

[11] American Gas Association (AGA).Cryptographic protection of SCADA communications,Part 2:Performance test results (AGA 12, Part 2)[S].Washington DC: AGA,2007.

[12] Institute of Electrical and Electronics Engineers (IEEE).Trial use standard for a cryptographic protocol for cyber security of substation serial links (IEEE P1711-2010)[S].USA:IEEE,2011.

[13] 中国石油北京油气调控中心.油气管道 SCADA 系统网络安全技术规范 Q/SY BD 46—2010[S].北京:中国石油天然气股份有限公司,2010.
PetroChina Oil and Gas Pipeline Control Center.Q/SY BD 46-2010 Network security and protection for SCADA of oil & gas pipelines[S].Beijing:PetroChina,2010.

[14] JEFFREY L H, JACOB S, JAMES H G.A security-hardened appliance for implementing authentication and access control in SCADA infrastructures with legacy field devices [J].International Journal of Critical Infrastructure Protection,2013(6):12-24.

[15] KANG D J, LEE J J, KIM B H, et al.Proposal strategies of key management for data encryption in SCADA network of electric power systems[J].Electrical Power and Energy Systems,2011,33:1521-1526.

(修改回稿日期 2013-10-08 编辑 **赵 勤**)