Journal of Oil and Gas Technology 石油天然气学报, 2020, 42(4), 364-371
Published Online December 2020 in Hans. http://www.hanspub.org/journal/jogt
https://doi.org/10.12677/jogt.2020.424155

Hans汉斯

Discussion on SCADA System Cyber Security Construction of Oil and Gas Pipeline

Shaoqing Shan

China Petroleum Pipeline Engineering Co. Ltd., Langfang Hebei
Email: 1073340745@qq.com

Received: Nov. 11th, 2020; accepted: Dec. 4th, 2020; published: Dec. 15th, 2020

Abstract

Emergency shutdown (ESD) system is an important subsystem of safety instrumented system, and ESD button is the most common manual trigger device in ESD system, which is used to trigger the protection program of ESD system artificially to alleviate the expansion of hazard and reduce the loss when accidents or dangers occur. In order to standardize the configuration of ESD button and reduce the error trigger rate, the corresponding loop detection function should be added to the ESD button circuit to ensure no error trigger. The diagnosis resistance in the detection circuit is recommended by the manufacturer, and the diagnosis current needs to be configured according to the actual situation of the ESD cabinet.

Keywords

Supervisory Control and Data Acquisition System, Cyber Security, Classified Protection of Cybersecurity, Security Communication Network, Security Area Boundary, Security Computing Environment, Security Management Center

文章引用: 单少卿. 浅谈油气管道 SCADA 系统网络安全建设[J]. 石油天然气学报, 2020, 42(4): 364-371.
DOI: 10.12677/jogt.2020.424155

浅谈油气管道SCADA系统网络安全建设

单少卿

中国石油天然气管道工程有限公司，河北 廊坊
Email: 1073340745@qq.com

收稿日期：2020年11月11日；录用日期：2020年12月4日；发布日期：2020年12月15日

摘　要

油气管道的SCADA系统网络安全关系到国家的战略安全，网络安全建设是根据相应的安全保护等级，通过安全防护技术体系和安全管理体系两部分进行的。安全保护等级的确定应根据相关标准，结合定级要素与安全保护等级的关系，按照定级流程，通过对定级要素分析，综合业务信息安全等级和系统服务安全等级，确定出网络安全保护等级。防护技术体系建设需要结合五个层面存在的安全问题和可能的风险，从SCADA系统的重要程度入手，确定安全保护需求，提出针对性安全技术措施，形成系统安全技术体系结构。安全管理体系是防护技术体系的支撑，两者相互关联，相辅相成。

关键词

SCADA系统，网络安全，安全保护等级，安全通信网络，安全区域边界，安全计算环境，安全管理中心

Copyright © 2020 by author(s), Yangtze University and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

SCADA 系统(Supervision Control And Data Acquisition，数据采集与监控)是国内长输油气管道常用的工艺控制系统，用于在调控中心对站场进行现场数据采集和控制[1]，以中国石油天然气集团有限公司(简称中国石油)为例，其东北、西北、西南及海上 4 大油气通道战略布局基本完成，全国性油气管网已初具规模；通过覆盖全国管网的 SCADA 系统，实现管网全部集中调控[2]，可以说，油气管道的 SCADA 系统网络安全关系到国家的战略安全。

随着油气管道自动化水平的提高和智能管道建设的推进，SCADA 系统网络设备在不断增加，在网络安全形势与挑战日益严峻、复杂的环境下，油气管道行业的 SCADA 系统网络安全风险呈攀升趋势。

2017 年，国家发布了《网络安全法》。2019 年，网络安全等级保护 2.0 制度由公安部正式实施，并强制执行。网络安全建设的相关标准也相继发布实施。以往针对油气管道网络安全建设的文章或是只侧重某几个方面，仅在 SCADA 系统的终端防护、局域网防护和边界防护三个防御策略上进行了论证[3]，或是没有按照等保 2.0 制度进行整体要求和论证[4]，或是仅对 SCADA 系统数据传输的安全风险进行了研究[5] [6]，或是仅按照软件、硬件、网络架构和管理层保护进行简单论述[7]。目前，依据等保 2.0 制度整体要求进行油气管道 SCADA 系统网络安全建设的文章鲜有报道，在此，笔者结合等保 2.0 制度的各类

国家标准针对油气管道 SCADA 系统网络安全建设进行论述。

2. 网络安全等级保护定级

GB/T22240《信息安全技术 网络安全等级保护定级指南》[8]中指出，根据等级保护对象的重要程度及遭到损害对国家、社会等各层面的侵害程度因素，其安全保护等级共分为五级。

1) 定级要素

安全保护等级评定应结合受侵害客体、对客体侵害程度这两个定级要素，按照定级要素与安全保护等级的关系，依据定级工作流程，对保护对象进行定级。定级要素与安全保护等级的关系见表 1。

Table 1. Relationship between grading elements and classified protection of cyber security
表 1. 定级要素与安全等级关系

受侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

2) 定级流程

等级保护对象定级工作应按照流程进行，其一般流程见图 1。

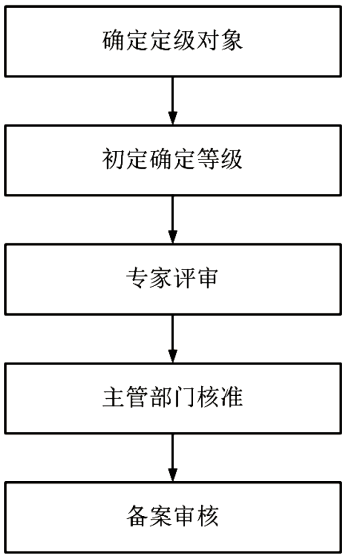

Figure 1. Work flow of grading classified protection of cyber security
图 1. 等级保护对象定级工作流程

需要注意的是，安全保护等级初步确定为第二级及以上的，定级对象的运行单位需组织信息安全专家和业务专家对定级结果的合理性进行评审，并出具专家评审意见。有行业主管(监管)部分的，还需将定级结果报请行业主管(监管)部门核准，并出具核准意见。最后，定级对象的网络运营者按照相关管理规定，将定级结果提交公安机关进行备案审核。审核不通过，其运行单位需组织重新定级；审核通过后最终确定定级对象的安全保护等级。

3) 定级方法

安全保护等级评定应在确定等级对象后，对受侵害客体、对客体侵害程度这两个定级要素进行分析，定级要素分析包括等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度这 2 个方面分析，分别得出业务信息安全等级和系统服务安全等级，依照两者的最高等级确定网络安全保护等级，网络安全保护等级确定方法见图 2。

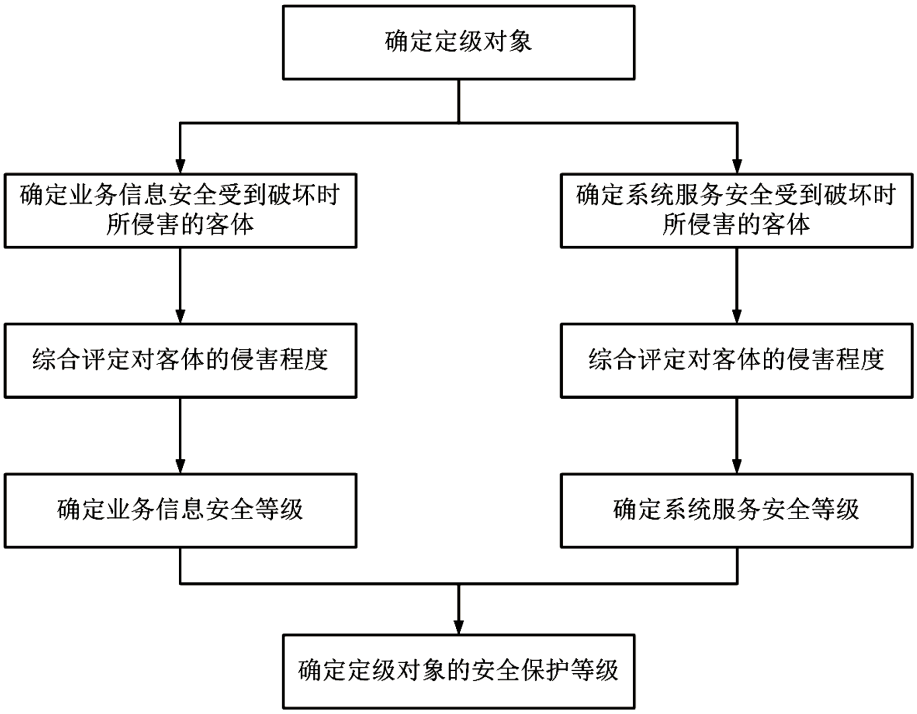

Figure 2. Schematic diagram of classified protection of cyber security
图 2. 网络安全保护等级确定示意图

一般来说，业务信息安全是指确保网络内业务信息的机密性、完整性和可用性等。系统服务安全是指确保网络可以及时、有效地提供服务，以完成预定的业务目标。

比如，油气管道地区级调控中心为一级风险，其业务信息安全遭到破坏时所侵害时，根据对所侵害客体分析，其会影响本单位和其他用油用气单位的正常生产经营秩序，在社会上造成不良影响。根据对侵害客体的侵害程度分析，其对公民、法人和其他组织的合法权益所侵害的程度为“一般损害”，即业务信息安全等级为第一级(见表 1)，社会秩序、公共利益所侵害的程度为“一般损害”，即业务信息安全等级为第二级(见表 1)，因此按照选择保护等级最高原则，确定一级风险的业务信息安全等级为第二级。同时，通过对一级风险的系统服务安全遭到破坏后对客体造成侵害的程度分析，其系统服务安全等级为第三级；依照两者的最高等级，评定一级风险的安全保护等级为三级。

可以看到，网络安全等级保护的定级工作是定性评估和半定量计算的结合，运营单位可以借鉴相关行业和企业的工作经验，邀请行业专家进行广泛的集中讨论评定，获得合适的定级，并报请行业主管(监管)部门核准，才能达到预期目标。

3. 防护技术体系建设

按照上述的定级方法，可以确定油气管道 SCADA 系统的调控中心及各站场的安全防护等级。一般

来讲，调控中心、干线管道的枢纽站、首末站等需要满足等保三级，分输站、清管站等需要满足等保二级要求。

网络安全建设均应按照网络安全防护技术体系和安全管理体系两部分进行实施，本文重点对网络安全防护技术体系进行论述。根据标准 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》[9]，SCADA 系统安全等级保护技术体系架构应包含安全物理环境、安全通信网络、安全区域边界、安全计算环境以及安全管理中心等五个层面。工业控制网络安全技术体系架构见图 3。

Figure 3. Industrial control network security architecture
图 3. 工业控制网络安全体系架构图

网络安全技术体系建设需要结合五个层面存在的安全问题和风险，从 SCADA 系统的重要程度入手，确定安全保护需求，提出针对性安全技术措施，形成机构特定的系统安全技术体系，用于指导 SCADA 系统等级保护的具体实现。

1) 安全物理环境

调控中心和站场的 SCADA 系统硬件的安全物理环境是网络安全的基石。主要关注点有：

① 硬件设备物理环境的盗窃、破坏、水火、电力供应等风险；

② 不当人员对 SCADA 系统设备的接触和使用风险。

安全物理环境建设应对调控中心、各站场的机柜间、UPS 室、控制室等重要房间设置防盗报警系统或有专人值守的视频监控系统、环境监测系统、火灾报警系统等设备来提高物理环境的安全，并通过电子门禁系统对人员的进出实施管理。

2) 安全通信网络

安全通信网络是整个 SCADA 系统网络安全运行的基础。主要风险点有：

① SCADA 系统网络拓扑的合理性；

② 生产数据传输的完整性；

③ 设备可信连接的验证性；

④ 数据传输的泄密、篡改安全风险。

安全通信网络建设应保证 SCADA 系统采用独立组网，并根据业务特点划分网络安全区域；利用隔离网闸在工控网络与非工控网络边界处进行单向隔离，利用工业防火墙在工控网络内部各安全域边界处进行逻辑隔离，从外到内形成纵深防御的防护体系；对关键网络设备和线路实现冗余备份，确保工控网络的高可用性；对广域网传输的数据采用加密技术确保传输信息的保密性等。

3) 安全区域边界

安全区域边界可以将风险控制在某一区域内，而不互相传播扩大。主要风险点有：

① 调控中心和站场网络边界入侵风险；

② 生产网和其他网的边界入侵风险；

③ 站场间区域边界的横向渗透风险。

安全区域边界建设应利用工业防火墙或网闸对工控网络内部各安全域之间以及工控网络与非工控网络的数据访问进行控制，只允许授权访问通过边界保护设备，对工控协议的深度包解析，实现在工控协议命令字层面的访问控制；利用堡垒机对非授权设备私自联到工控网络的行为进行监控；利用安全审计系统和入侵检测系统对工控网络流量进行监测审计，对工控网络中的网络攻击、病毒等安全事件进行检测，及时发现工控网络中威胁信息。

4) 安全计算环境

安全计算环境是 SCADA 系统运行的软硬件背景，是安全运行的保证。主要风险点一是来自系统本身的脆弱性风险；另一个是用户登录帐号、权限等系统使用、配置和管理等风险，主要包括：

① SCADA 系统入侵风险；

② 数据库账户、口令的安全隐患；

③ 广域网的控制指令、数据交换泄密风险；

④ 上位机终端防护软件过期风险；

⑤ 设备接口缺乏管理。

安全计算环境建设应通过信息梳理，利用主机防护软件、安全加固软件加强服务器、工程师站等重要工业主机的身份鉴别措施；建立完善的用户账户的口令策略和用户登录策略以及鉴别信息在传输过程中的加密；提高对系统账户的保护强度；加强访问控制措施，严格限制用户的访问权限；删除多余的系统账户，防止非授权操作、误操作或信息泄露。利用工控应用系统身份认证保证数据和业务的数据完整性和保密性；防止非授权操作、误操作或信息泄露；实现用户身份强认证机制，通过工业安全监测审计系统对工业用户操作行为进行安全审计，通过日志审计系统完善应用系统日志记录，加强对工业应用系统运行状况的监控。应根据需要实现数据定时备份或实时备份功能，保证数据可用性。

5) 安全管理中心

安全管理中心是安全运维管理的技术支撑，可以实现对 SCADA 系统系统安全性的有效监控和提前防范，安全运维管理方面的风险主要有：

① 人员认证、操作风险；

② 设备审计日志缺失；

③ 网络入侵；

④ 恶意代码风险；

⑤ 网络安全设备管理风险。

安全管理中心作为网络安全等级保护对象的安全策略及安全计算环境、安全区域边界和安全通信网络的安全机制实施统一管理的系统平台，实现统一管理、统一监控、综合分析和协同防护[10]。安全管理中心技术要求可以分为功能要求、接口要求和自身安全要求三个大类，技术要求框架见图 4。

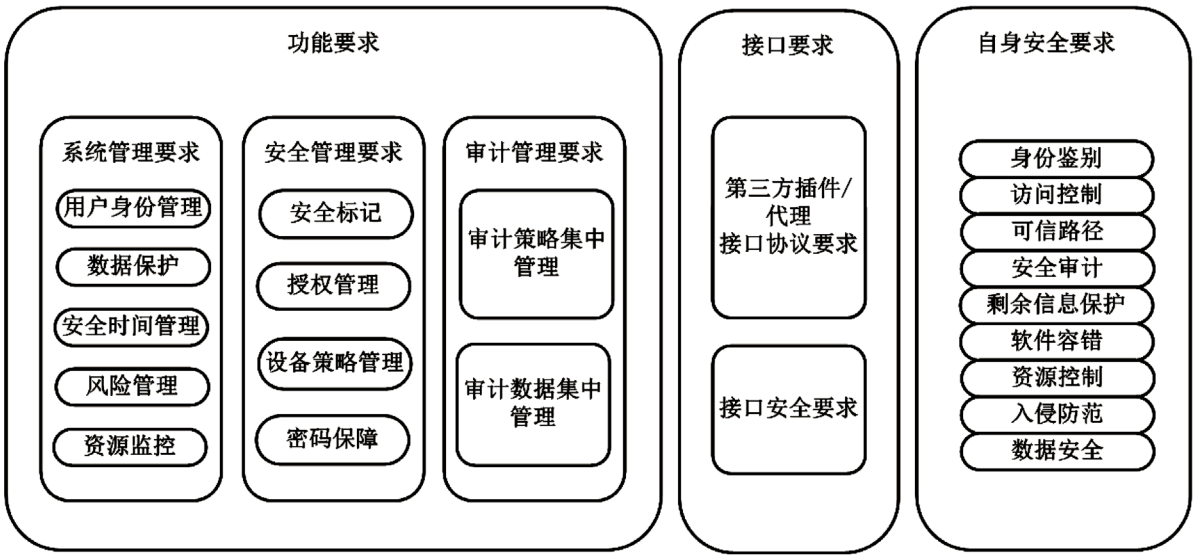

Figure 4. Framework of security management center technical requirements
图 4. 安全管理中心技术要求框架图

安全管理中心一般设置在长输管道的调控中心，划分出单独的安全管理区，利用安全管理平台、堡垒机、安全审计系统、入侵检测系统和态势感知系统，通过系统管理、安全管理和审计管理，加强网络设备和安全设备集中认证和审计日志的集中统一管理；加强对网络运行状况的集中监控；实现系统管理员、安全管理员、审计管理员的权限分离、身份鉴别以及操作过程的监控审计等功能。

4. 安全管理体系建设

安全管理体系建设应在安全管理制度、管理人员设立、管理机构建立、安全建设管理和安全运维管理五个方面开展进行，通过确立网络安全工作的方针、策略指定和发布管理制度，设立不同职责权限的安全主管、安全管理等负责人，并进行有效管理和教育培训，同时，对网络安全建设过程进行有效监控，建成后对有关硬件、账户、密码等进行日常管理，从管理体系上保证安全技术措施的有效落实，可以说，安全技术措施的有效实施需要安全管理体系的助力，同样，安全管理体系的落实也常常需要技术措施的支撑，两者是相辅相成，相互关联的。

5. 结束语

《网络安全法》明确了“国家实行网络安全等级保护制度”、“关键信息基础设施在网络安全等级保护制度的基础上实行重点保护”等内容，为网络安全等级保护工作赋予了法律依据。网络安全等级保护 2.0 制度和一系列标准的发布将等保对象从狭义的信息系统，拓展到网络基础设施、云计算平台、工业控制系统等，提出了新的技术防护体系和管理措施、安全建设设计实现方式以及等级测评方法，可有

效指导网络运行、网络安全企业、网络安全服务机构开展网络安全等级保护安全技术方案的设计和实施。

根据 GB/T28448《信息安全技术 网络安全等级保护测评要求》[11]，等级保护对象的运营单位完成网络安全建设后，必须选择国家认可的测评机构进行等级测评，并在系统运行过程中定期进行测评。在此之前，建议运营单位选择专业安全厂商进行测评协助工作，如在正式测评前协助单位进行自测和整改等，各专业安全厂商应给出等级保护对应的测评项权重系数，此系数虽然不能作为测评打分依据，但运营单位可以依据这个测评项权重系数，结合自身实际情况，有选择性地对各测评项进行建设，达到 SCADA 系统网络安全建设安全性和经济性的平衡统一。

目前，长输油气管道的 SCADA 系统网络安全建设已经是势在必行，各油气管道运营单位应尽早展开相关工作，以防止网络安全危害事件的发生，免除因此导致的责任处罚。同时，尽早开展网络安全建设工作可以获得主动性和前瞻性，避免后期网络安全设备的重复建设和兼容问题[12]-[18]。

参考文献

[1] 聂磊, 张宏伟, 罗冰. 浅谈长输管道 SCADA 系统组网结构及实现[J]. 工业控制计算机, 2018, 31(9): 108-110.

[2] 聂中文, 黄晶, 于永志, 等. 智慧管网建设进展及存在问题[J]. 油气储运, 2020, 39(1): 11-24.

[3] 梁怿, 王磊, 赵廉斌, 等. 工业网络安全深度防御策略——以西气东输天然气管道 SCADA 系统网络为例[J]. 油气储运, 2019, 38(6): 685-691.

[4] 张世斌, 贾立东, 魏义昕, 等. 输气管道 SCADA 系统网络安全策略探索与实现——以中俄东线天然气管道工程为例[J]. 油气储运, 2020, 39(6): 692-696.

[5] 黄河, 张伟, 祁国成, 等. 油气管道 SCADA 系统数据传输的安全风险及其解决方案[J]. 天然气工业, 2013(11): 115-120.

[6] 李萍, 聂磊, 张宏伟. SCADA 系统数据传输安全性的几点探讨[J]. 仪器仪表标准化与计量, 2020(2): 13-15.

[7] 许威. 油气管道 SCADA 系统安全浅析[J]. 石油化工自动化, 2017, 53(5): 43-46.

[8] 曲洁, 尚旭光, 黄顺京, 等. GB/T22240-2020 信息安全技术网络安全等级保护定级指南[S]. 北京: 中国标准出版社, 2020: 4.

[9] 马力, 陈广勇, 张振峰, 等. GB/T22239-2019 信息安全技术网络安全等级保护基本要求[S]. 北京: 中国标准出版社, 2019: 4.

[10] 霍珊珊, 任卫红, 刘健, 等. GB/T36958-2018 信息安全技术网络安全等级保护安全管理中心技术要求[S]. 北京: 中国标准出版社, 2019: 1.

[11] 朱建平, 马力, 黄洪, 等. GB/T28448-2019 信息安全技术信息系统安全等级保护测评要求[S]. 北京: 中国标准出版社, 2019: 4.

[12] 陈雪鸿, 杨帅锋, 孙岩. 工业控制系统安全等级保护测评研究[J]. 信息安全研究, 2020, 6(3): 272-278.

[13] 胡朋. SCADA 系统在长输天然气管道的应用现状及发展趋势[J]. 山东化工, 2018, 47(10): 90+92.

[14] 顾萤. SCADA 系统在输气管道工程中的应用[J]. 通信电源技术, 2020, 37(4): 157-158.

[15] 陈曦, 周峰, 郝鑫, 等. 我国 SCADA 系统发展现状、挑战与建议[J]. 工业技术创新, 2015, 2(1): 103-114.

[16] 薛义. 长距离输气管道的 SCADA 系统探讨[J]. 化工设计通讯, 2018, 44(11): 32.

[17] 赵国辉. 长输油气管道自控技术的发展与中俄东线 SCADA 系统[J/OL]. 油气储运, 2020: 1-14. http://kns.cnki.net/kcms/detail/13.1093.TE.20200315.1403.004.html, 2020-03-16.

[18] 赵国辉. 中俄东线天然气管道工程 SCADA 系统的设计与实现[J]. 油气储运, 2020, 39(4): 25-34.