油气集输领域工业控制系统等级保护2.0标准安全设计技术要求分析

李世斌，郭永振，唐刚
（中国软件评测中心，北京 100048）

摘 要： 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）标准于2019年正式发布，相应的安全设计技术要求、测评要求也相继施行，形成了等级保护2.0标准体系。重要领域工业控制系统作为关键信息基础设施，是等级保护2.0标准的重点安全防护对象。针对油气集输领域，结合典型工业控制系统分层架构，对照等级保护2.0标准安全设计技术要求进行比较分析和综合研判，提出了油气集输领域工业控制系统的安全扩展要求、安全控制点和监控预警要求。围绕油气集输领域工业控制系统防护对象选择实践，提出了根据承载业务、网络结构、系统规模、主机资产等因素的差异对安全防护对象进行裁剪化防护的对策建议。

关键词： 油气集输；工业控制系统；网络安全防护；等级保护2.0；安全设计技术要求

中图分类号： TP393.0 **文献标识码：** A **文章编号：** 2095-8412 (2020) 01-001-05

工业技术创新 URL: http: //www.china-iti.com DOI: 10.14103/j.issn.2095-8412.2020.01.001

引言

随着我国石油化工行业的发展以及西气东输等战略布局的推进，我国油气开采与输送管道网络部署越来越广泛，石油天然气集输（以下简称“油气集输”）行业成为国家基础产业。对遍布全国的油气集输工业控制系统（以下简称“工控系统”）进行安全防护，以风险管控、预警预判为前提的工控系统网络安全可靠运行机制研究具有重大意义。

目前在工业领域主机操作系统、数据库设备、服务器设备、PLC设备、工业SCADA系统、DCS系统中，国外产品占据很大比例。在石油化工领域中，这些系统或设备应用广泛，品牌众多而繁杂，技术、管理层面的网络安全防护标准较难统一。在此背景下，《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）[1]标准应运而生，与其相应的安全设计技术要求、测评要求也相继施行。以上标准统称“等级保护2.0标准”，它可以将工控系统纳入安全保护范围，将安全通用要求与扩展要求相结合，加固工控系统安全防护策略，保障工控系统的保密性、可用性、完整性。

本文以油气集输领域为研究对象，首先结合典型工控系统架构分层方式，提出等级保护2.0标准对工控系统防护的分层架构；其次对等级保护2.0标准安全设计技术要求进行分析；最后围绕油气集输领域工控系统防护对象选择实践，提出对策建议。

1 油气集输领域工业控制系统

1.1 典型工业控制系统架构分层防护对象

目前按业务定义对工控系统进行架构分层，一般分为现场设备层、现场控制层、过程监控层、生产管理层与企业资源层。等级保护2.0标准对工控系统的防护也采用这种架构分层方式，如图1所示。工控系统与企业信息系统的边界一般从企业资源层向下划分。为提升企业信息化程度与生产效率，SCADA、DCS、PLC等工控系统与管理信息系统、MES等进行了不同程度的融合，在降低生产与管理成本的同时，解决了工控系统的信息孤岛问题，但因此而引入的网络安全问题有待进一步解决[2-3]。

1.2 油气集输领域工业控制系统类型

油气集输领域中一般有业务承载专网、集团级/分公司级SCADA系统、分站场SCADA系统等，而DCS集中于净化厂级，PLC、RTU和SIS集中于井站、集气站、阀室级，各个系统承载的

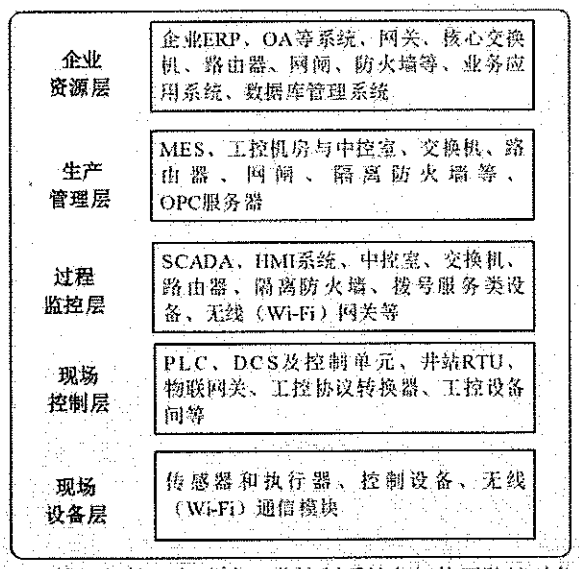

图1 等级保护2.0标准中工业控制系统各架构层防护对象

业务、网络结构、系统规模、主机资产等均有差异。在石油化工领域，工业SCADA系统一般部署到集团级、分公司级、油气矿级。工业SCADA系统由站场设备和调控中心组成，站场设备提供由各种传感器等设备通过站场路由器及其他收发器连接而形成的监控和保护装置，调控中心对远程传输信号进行处理与反馈。SCADA系统联接现场设备层、现场控制层、过程监控层，形成覆盖生产过程的数据采集监视网络。

油气集输系统具有大型化、网络化、数字化和智能化的发展趋势。随着新技术的发展变革，油气集输工控系统正朝着由物联网、5G、云计算、移动互联网、大数据融合而成的工业互联网应用系统方向发展。例如油气田的火气系统核心一般采用高性能的PLC，现场层面有火焰探测器、感温探头、可燃气体探测器等。当现场发生火情或危险气体泄漏时，借助5G等无线通信技术，可迅速将现场警情上传到指挥中心。工控系统底层的采集执行设备将生产状态下感知的过程参数转换成计算机可以识别的数字信号，再利用通信技术将采集的数据和监控信息上传至分公司级调控中心。工业无线通信技术的应用可改变油气集输行业的传统监控手段，实现原始数据的整合、分析、共享，同时结合建立的模型机理与AI专家系统，实现对油气田的智能化控制。因此，基于工业无线通信技术的网络安全防护也是一大重点。油气集输领域已进入数字油田建设阶段，因此安全防护对象已从普通的企业网、终端主机延伸到数字仪表设备，如无线压力变送器、数字传感器、智能RTU等[4]。

1.3 油气集输领域工业控制系统监控预警

根据等级保护2.0标准实现油气集输领域工控系统的风险管控是保障其网络安全的基础，同时可构建安全监控与预警预判能力，确保工控系统网络安全可靠运行。常规的防火墙、IDS、IPS、安全网关等设备策略是一种被动防护，而安全监控与预警预判是主动式安全监控预警技术。

油气集输领域工控系统的态势感知与预警机制应符合基本要素，如具备云端监测数据、实时流量分析数据、端点防护系统数据、第三方推送数据、威胁情报诱捕数据[5]。通过分析行业通信协议并研发协议一致性、安全性扫描组件，提取工控指纹特征并创建工控指纹库，对工控安全防护对象的设备种类、型号、操作系统、固件版本等信息形成知识库，挖掘系统或设备开放的服务及接口类型，主动监控是否有符合CNVD、CNNVD、CVE等漏洞库中已识别的漏洞，结合APT攻击线索、蜜罐系统、安全实时监测系统等，对工控系统的网络安全脆弱性进行监控预警。

2 油气集输领域等级保护2.0标准安全设计技术要求

油气集输领域SCADA、DCS、PLC及RTU等工控系统网络安全防护体系包含总体策略、技术指导体系、安全管理与服务等。这些内容在电力等行业被总结为“安全分区、网络专用、纵向隔离、横向认证”，而等级保护2.0标准中也在通用要求及扩展要求两方面体现了该安全策略的内容。油气集输领域工控系统的部署有一定分散性特征，由于不同层级的工控设备、用户、协议、应用数据对安全性的要求不尽相同，因此等级保护2.0标准针对工控系统的安全设计技术要求应当考虑系统边界需要部署的工控安全产品特征以及工控协议与其他网络通信协议的区别。对工控系统的网络安全进行定级，一般要先划分安全区域，如分为企业管理、生产监控、现场控制三个大区，根据每个区的生产业务流程、软硬件资源独立情况、管理责任，明确可单独定级的系统。石油化工等行业涉及社会公共服务及国家安全，多数系统为3级，其中与过程监控、工业现场控制相关的系统包含4级安全保护系统。下面根据等级保护2.0标准中的“一个中心、三重防御”理念对3级系统的工控安全扩展要求进行阐述[1, 6]。

2.1 工业控制系统安全管理中心防护要求

安全管理中心的控制点为系统管理、审计管理、安全管理与集中管控，主要对工控系统企业资源层、生产管理层、过程监控层提出安全设计技术要求，并且偏重于系统整体的安全防护，没有工控系统安全扩展要求。安全管理中心的防护对象是可提供集中管理功能的系统，如部署油气输送企业中分公司级的综合安全审计系统，对系统管理员、审计管理员、安全管理员进行身份鉴别、权限划分与操作审计，同时对集中安全管控系统的安全策略、恶意代码防范、补丁升级等方面提出要求。

2.2 工业控制系统安全通信网络防护要求

安全通信网络是等级保护重点防护对象，在工控系统架构的每一层都有安全通用要求。安全通信网络也对除企业资源层之外的其他四层提出了工控系统安全扩展要求。安全通信网络的控制点为网络架构、通信传输、可信验证，具体安全设计技术要求包括网络设备业务处理能力，网络区域划分与边界隔离，系统及数据的可用性、完整性、保密性要求，可信验证等。某气矿作业区通信网络整改工程计划搭建油气矿级SCADA系统，对上，与分公司管理信息系统进行逻辑隔离，实现监控视频图像远传、智能仪表等无线物联网功能；对下，与生产网中的DCS、PLC等系统集成。将油气集输系统现状与等级保护2.0标准要求相结合的安全通信网络扩展要求如表1所示。

2.3 工业控制系统安全区域边界防护要求

工控系统架构的每一层都有安全区域边界的通用要求，安全区域边界的扩展要求也对除企业资源层之外的其他四层适用。根据安全通用要求，安全区域边界主要安全控制点为边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证，具体要求包括跨越边界的访问和数据流管理、非授权网络连接管理、无线网络使用管理、网络边界或区域之间的访问控制策略管理、关键网络节点入侵防范、恶意代码和垃圾邮件防范、网络边界与重要节点安全审计、可信验证要求。在一些工业领域，如ZigBee、3G/4G、LORA等，无线技术已成为连接传输层的重要技术，因此等级保护2.0标准中强调了对无线通信网络的安全设计技术要求。将油气集输系统现状与等级保护2.0标准要求相结合的安全区域边界扩展要求如表2所示。

2.4 工业控制系统安全计算环境防护要求

工控系统架构的每一层都有安全计算环境的通用要求，而安全计算环境的扩展要求只对现场设备层和现场控制层提出。安全计算环境控制点为身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据的完整性、数据的保密性、数据备份恢复、剩余信息保护、个人信息保护等，防护对象是工控系统终端和服务器等设备中的操作系统、网络设备、安全设备、移动终端、管理系统和客户端、感知节点与网关设备、控制设备、业务应用系统、数据库管理系统、中间件等。结合某油气田SCADA系统建设情况，其调控中心的数据服务器、历史数据服务器、OPC服务器，以及连接了片区的PLC和RTU设备，都是安全计算环境的防护对象。将油气集输系统现状与等级保护2.0标准要求相结合的安全计算环境扩展要求如表3所示。

3 油气集输领域工业控制系统防护对象选择实践

工控系统与管理信息系统是安全防护的两大

表1 油气集输系统安全通信网络扩展要求

工控系统扩展要求	油气集输行业安全防护对象
工控系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段	集团级/分公司级/站场级不同层间连接的交换机、工控单向隔离网闸、边界防火墙、边界路由器、无线接入设备
工控系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段	分公司SCADA系统/DCS、站场PLC、连接交换机、无线接入设备、工控防火墙等
涉及实时控制和数据传输的工控系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离	采输、管网等工控系统与信息系统的网络拓扑
在工控系统内使用广域网进行控制指令或相关数据交互的，应采用加密认证技术手段实现身份认证、访问控制和数据加密传输	交换机、系统边界路由器、无线接入设备、工控防火墙、工控系统应用的加密认证设备

表2 油气集输系统安全区域边界扩展要求

工控系统扩展要求	油气集输行业安全防护对象
应在工控系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-mail、Web、Telnet、Rlogin、FTP等通用网络服务	网闸、工业防火墙、路由器和交换机等提供访问控制功能的设备及监控预警设备
应在工控系统内安全域和安全域之间的边界防护机制失效时，及时进行报警	
工控系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施	拨号服务类设备
拨号服务和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施	
应对所有参与无线通信的用户提供唯一性标识和鉴别	无线通信网络及设备、生产系统区域内手机等设备、认证网关、3G/4G/5G路由器等
应对所有参与无线通信的用户进行授权以及执行使用限制	
应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护	
对采用无线通信技术进行控制的工控系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰工控系统的行为	

表3 油气集输系统安全计算环境扩展要求

工控系统扩展要求	油气集输行业安全防护对象
控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如控制设备受条件限制无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制	应用及数据服务器、历史数据服务器、OPC服务器、工程师站等主机设备操作系统、站场控制系统、RTU、PLC终端、手持操作终端、SCADA、HMI、业务应用系统等
应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作	
应关闭或拆除控制设备的软盘驱动、光盘驱动、USB接口、串行扣或多余网口等确需保留的应通过相关的技术措施实施严格的监控管理	
应使用专用设备和专用软件对控制设备进行更新	
应保证控制设备在上线前经过安全性检测、避免控制设备固件中存在恶意代码程序	

主要对象。我国某地区油气田的企业资源层以企业资源计划等系统为主要组成部分，与底层工控系统进行物理与逻辑隔离，一般归类为企业办公信息系统；生产管理层对现场进行生产调度等管理操作，可细化生产过程并维护与生产相关的记录，需要一定的实时性与可靠性，保证工作班时达到分钟级至秒级的实时性；过程监控层包括监控服务器与功能单元，对生产过程数据进行采集与监控，并利用HMI系统实现人机交互，由于该层直接管理和监控工业自动生产运行，因此需要具备较高实时性要求，保证实时性达到分钟级至秒级；现场控制层主要包括集散控制系统、节点控制终端和PLC单元，用于对各执行设备进行控制，需要保证秒级至毫秒级的实时性与高可靠性；现场设备层主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

基于以上系统分区及网络隔离的特征，自上向下分析该油气田工控系统应重点防护的对象。SCADA系统对上通过工业协议与分公司级SCADA系统互联互通，对下连接多个油气站场的PLC系统及RTU设备。该SCADA系统调控中心具备冗余部署的数据服务器、历史数据服务器、OPC服务器、工程师站等主机设备，通过核心交换机与各片区连接，片区内部站场控制系统、操作员站、RTU等设备形成局域网[7]，而每个单独的SCADA系统可通过典型工控系统架构分层方式，在生产管理层重点防护防病毒服务器、DPC服务器，在过程监控层重点防护DCS/SIS工程师站与操作员站、打印机、GPS等，在现场控制层重点防护SIS控制器、DCS控制器、火气系统关联的控制器等，每层之间都部署工业防火墙[8]。该油气田的某DCS对上通过工业协议与分公司级

SCADA系统互联互通，对下连接多个油气站场的生产网，生产网内部具备多个SIS及RTU设备。该DCS调控中心具备由历史服务器、工程师站组成的局域网，通过多台工业交换机分别连接不同井站的RTU系统和SIS。该油气田的PLC和RTU设备位于工控系统架构中的现场控制层及现场设备层，一般集中于井站、集气站、阀室等。该油气田工控系统的部署具备油气集输领域系统的共同特征，即呈现一定的分散性，不同层级的工控设备、用户、协议、应用数据对安全性的要求不尽相同，因此，通用要求及工控系统扩展要求并非可以在所有工控系统中得到最佳实践。在等级保护2.0标准落地实施方面，应分析工控系统承载的业务、网络结构、系统规模、主机资产，对不同工业领域、不同规模系统等差异性进行分析，根据企业具体情况准确定义被测评对象，尤其是针对现场控制层、现场设备层中的PLC系统、RTU设备、现场传感器等系统或设备进行资产划分，对安全保护对象进行裁剪化防护，合理适应安全计算环境中的控制点要求。

4 结束语

本文分析了油气集输行业典型的SCADA、DCS、PLC与RTU等工业控制系统在网络安全防护能力建设过程中的技术要点，阐述了等级保护2.0标准中安全设计技术要求中的安全通用要求及扩展要求及相应的安全控制点。油气集输行业工业控制系统的网络安全防护对象包括机房、工控设备间、中控室等物理环境，以及软硬件主机、用户应用、数据等信息资产。由于工业控制系统承载的业务、网络结构、系统规模、主机资产等均有差异，因此不同的工业领域、不同规模的系统、不同实力的企业建设的工业控制系统在实际等级保护建设、评估、整改过程中，需要对安全控制点进行分析，准确定义不适用项，合理划分安全区域，并通过每个安全区域的生产业务流程、软硬件资源独立情况、管理责任来确认需要进行安全保护的工业控制系统及相应的安全防护对象。

下转第11页

参考文献

[1] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239-2019 [S].

[2] 张翔宇, 路来顺. 工业控制系统网络安全分析与研究[J]. 网络空间安全, 2019, 10(5): 114-120.

[3] 傅一帆, 霍玉鲜. 网络安全等级保护工业控制系统安全防护技术体系设计[J]. 警察技术, 2017(5): 19-22.

[4] 许洪东, 张春宇, 杨帆. 浅谈油气生产企业网络安全体系研究与建设[J]. 中国管理信息化, 2019, 22(22): 65-66.

[5] 宋雪冬. 网络安全态势感知通报预警与防御解决方案[J]. 信息技术与标准化, 2019(9):15-17.

[6] 陈广勇, 祝国邦, 范春玲. 《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)标准解读[J]. 信息网络安全, 2019(7): 1-7.

[7] 胡启超. 油气集输SCADA系统攻击与防御模拟平台研究[D]. 成都: 西南石油大学, 2015.

[8] 孟凡丽. 油气处理厂工控系统网络安全的方案讨论[J]. 天然气与石油, 2019, 37(4): 116-119, 124.

作者简介:

李世斌（1992—），男，硕士，北京人，工程师。研究方向：网络安全测评与工业控制系统安全可靠性评估。
E-mail: lishibin@cstc.org.cn

郭永振（1984—），通信作者，男，硕士，北京人，高级工程师。研究方向：网络安全。
E-mail: guoyongzhen@cstc.org.cn

唐刚（1981—），男，硕士，北京人，高级工程师。研究方向：网络安全。
E-mail: tanggang@cstc.org.cn

（收稿日期：2019-11-19）

Security Risk Assessment for Industrial Control System Based on Multi-Attribute Decision-Making

WANG Jia
(*China Software Testing Center, Beijing 100048, China*)

Abstract: A method of security risk assessment of industrial control system based on multi-attribute decision-making is proposed for the workshop of intelligent production shop. According to the network structure of the intelligent industrial control system, the security risk points are analyzed and assured, and the security risk assessment model of the industrial control system is constructed. The assets are divided into 7 index attributes, namely, data, software, hardware, service, personnel, structure characteristics and complexity of industrial control system, importance and influence of management characteristics. The importance of each attribute is judged, the asset security related topology is obtained, and the hazard degree of each asset is calculated. The basic process of security risk assessment of industrial control system is formed, which makes the security risk quantified, providing a basic compliance for the security deployment of industrial control system.

Key words: Intelligent Factory; Multi-Attribute Decision-Making; Security Risk Assessment; Industrial Control System; Asset; Security Deployment

上接第5页

Analysis on Technical Requirements of Security Design of Classified Protection 2.0 Standard for Oil-gas Gathering and Transportation ICS

LI Shi-bin, GUO Yong-zhen, TANG Gang
(*China Software Testing Center, Beijing 100048, China*)

Abstract: "Information security technology—Baseline for classified protection of cybersecurity" (GB/T 22239-2019) is officially released in 2019. The corresponding technical requirements of security design and evaluation requirements are also implemented, forming a classified protection 2.0 standard system. As a critical information infrastructure, the industrial control system (ICS) in the important fields is the key security protection object in the classified protection 2.0 standard. Aiming at the oil-gas gathering and transportation, combined with the typical ICS architecture, the technical requirements of security design of classified protection 2.0 standard are analyzed in comparison and determined comprehensively, so that the security extended requirements, security control points, monitoring and pre-warning requirements of the ICS in the oil-gas gathering and transportation are put forward. Based on the protection object selection practice of the ICS in the oil-gas gathering and transportation, countermeasure and suggestion is put forward: carry out a tailoring protection on the security protection object as per the variances from factors including carried business, network structure, system scale and host assets.

Key words: Oil-gas Gathering and Transportation; Industrial Control System(ICS); Classified Protection 2.0; Technical Requirements of Security Design