油田工业控制系统网络安全解决方案研究

王 晔,靳方略,吕铭心
(中国电子信息产业集团有限公司第六研究所,北京 100083)

摘 要:工业控制系统现已广泛应用在油田行业,随着两化融合、智慧油田建设进程的加速,油田工控网络从相对封闭到趋于开放,工控系统的脆弱性和外部威胁被进一步放大,严重影响着国家油田行业的安全生产、稳定运营。从油田工控实际需求出发,依据工业控制系统等级保护扩展要求,结合油田工业控制系统协议多样、设备可靠性要求高、安全机制不能影响实时性等特点,从安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面着手,研究贴合油田行业特征的工控网络安全解决方案。

关键词:油田;工业控制系统;工控网络;网络安全
中图分类号:TP393.1 文献标识码:A DOI:10.19358/j.issn.2096-5133.2020.10.008
引用格式:王晔,靳方略,吕铭心. 油田工业控制系统网络安全解决方案研究[J].信息技术与网络安全,2020,39(10):38-43.

Research on network security solution for petroleum industrial control system

Wang Ye, Jin Fanglue, Lv Mingxin
(The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: Industry control systems have been widely used in petroleum industry. Nowadays, with the integration of information technology and industrialization in petroleum enterprises, the ICS networks have changed from relatively isolate to open with the outside net world, so it magnifies the ICS vulnerability and external net threats, which seriously affects the safe production and stable operation of the national petroleum industry. The research is based on the actual needs of ICS security in petroleum industry, referring to the information system classified protection of ICS, considering the characteristics of the petroleum industrial control system, such as the diversity of protocols, high reliability requirements of equipment, and the safety mechanism can not affect the real-time system operation, etc. The research will follow the aspects of secure communication network, secure area boundary, secure computing environment and safety management center, trying to find a complete set of ICS security solution and fit the petroleum industry in an all-round way.

Key words: petroleum industry; industry control system; ICS network; network security

0 引言

工业控制系统,如分散控制系统(Distributed Control System, DCS)、数据采集与监视控制系统(Supervisory Control And Data Acquisition, SCADA)、可编程逻辑控制器(Programmable Logic Controller, PLC)以及各种远程终端单元(Remote Terminal Unit, RTU)等,广泛应用于石油化工、电力、水利、冶金、航空航天等诸多现代工业。我国油田行业,普遍采用RTU、PLC、SCADA等控制系统完成对原油的采集、存储、输送、销售等环节。

随着计算机和网络技术的不断进步,两化深度融合以及“智慧油田”的快速发展[1],物联网技术、系统级联技术、嵌入式技术、无线技术等广泛使用,使原本相对分散、独立的油田工控系统集成度越来越高,其与上层管理信息网络的互联程度也随之提高,这些技术融合在拓展了油田工业发展空间的同时也带来了网络安全问题。例如:2015年1月,安全研究人员发现一款专门窃取全球能源企业机密的木马Laziok,它们的目标主要是中东地区,多数被攻击的目标与石油、天然气有关;2017年5月,WannaCry(及其变种)致部分中石油加油站无法正常工作;2017年8月,沙特阿拉伯的一家石油工厂使用的Triconex

安全控制器系统中存在漏洞，恶意软件试图利用漏洞破坏设备并企图以此引发爆炸摧毁整个工厂。

上述这些安全事件标志着网络攻击从传统“软攻击”升级为直接攻击关键信息基础设施系统的“硬摧毁”，工业控制系统网络安全风险所带来的，不再仅仅是信息泄露、信息系统无法使用等“小”问题，而是会对国家和社会造成直接的、实质性影响的大问题。由此可见，如果不对油田工控系统加强匹配信息化建设的网络安全防护措施，将会在系统中留下大量的安全盲点与灰色地带，留给网络威胁可乘之机，特定条件下可能导致停产，甚至造成人员伤亡等严重社会事件。

综上所述，新形势下立足油田工控的安全现状，设计有效的油田工控系统网络安全解决方案，提高油田工控系统整体安全防护能力，保证油田工控系统的稳定有序运行刻不容缓。

1 油田工控系统典型架构及风险分析

油田工业控制系统主要完成油井、场站的数据采集和实时监控，并将数据上传到上层的管理信息系统。由于油井和场站的地域跨度大，环境比较恶劣，常使用 RTU 设备采集数据并通过无线技术实现通信。计量站、联合站等实时性要求高、逻辑联锁控制较多的场站，常使用 PLC 系统实现控制和监控。管理层级往往要求多系统集成，常使用 SCADA 用于数据的监视与管理[2]。

1.1 系统业务架构

按照油田典型的业务架构，可将油田网络分成 4 个网络层次，从上往下依次为：公司级网络、采油厂级网络(一般包含多个作业区)、作业区级网络(一个管理单位，一般包含几百口油井和相关的各类站)、场站级设备及网路(为生产现场，主要包含两部分：油井和各类场站，如注水站、联合站、计量站等)。整体网络架构如图 1 所示。

(1)总公司网络架构

以各采油厂数据、网络作为数据源对象，将总公司需要的数据同步至总公司数据库中，建立总公司管理子系统模块。

(2)采油厂网络架构

按照采油厂生产管理平台的需求，将各个管理区数据汇总，进行统一平台集成，提供有效的数据分析结果，实现数据监控、工况分析、安全管理、报表管理等功能，同时给油田总公司提供数据通信接口。

(3)作业区网络架构

作业区将其管辖范围内站点、井场生产数据通过无线或有线的网络通信方式整合，并对所有设备信息、区域位置及状态进行统一标识，建立标准的生产数据点表、数据库结构，向采油厂级数据平台提供数据通信接口。

由于作业区与场站等工控系统可进行实时数据交互，为了提高生产的安全性，一般通过网络隔离设备将作业区分为管理网和生产网两部分，以减少信息网络对生产网络的影响，保证工控系统的安全性。

(4)场站级设备及网络架构

油田现场分为油井和场站两类：油井采用无人值守站的方式，RTU 作为无人值守站的数据通信中心，与油井进行数据采集和通信。作业区的采集通信服务器则通过 RTU 采集油井的数据；场站包括联合站、计量站、增压站、注水站等各类站控系统，是集数据采集、自动控制和智能分析于一体的综合自动化系统。

1.2 系统安全风险分析

油田跨度大、覆盖地域范围广、涉及网络层级多，常规规模油田即包含多个作业区和采油厂，每个作业区有几百口油井和站控系统，而每口井配置的 I/O 等点数有上千点，总点数可达几十万，甚至千万。此外，油田工控系统由于业务、建设周期先后等原因会涉及无线技术、多种品牌工控系统以及信息系统等，系统集成和互联更多。

基于油田业务特点，目前油田工业控制系统存在的安全风险主要如下。

1.2.1 政策、管理及运维层面

(1)油田行业在工控网络安全方面制度、标准和规范较少，没有成熟的管理办法以及工控系统安全指导准则。

(2)企业工控安全管理制度、组织尚不完善。

(3)人员工控安全意识薄弱。一方面没有工控安全意识可能使重要岗位人员沦为外部威胁入侵的跳板；另一方面，工控安全意识淡薄可能致使员工某些操作给生产带来安全隐患。

1.2.2 设备、技术层面

(1)工控系统本身的脆弱性

一方面工业通信协议具有脆弱性：油田工控系统中工业协议较多，这些协议在设计时通常只强调

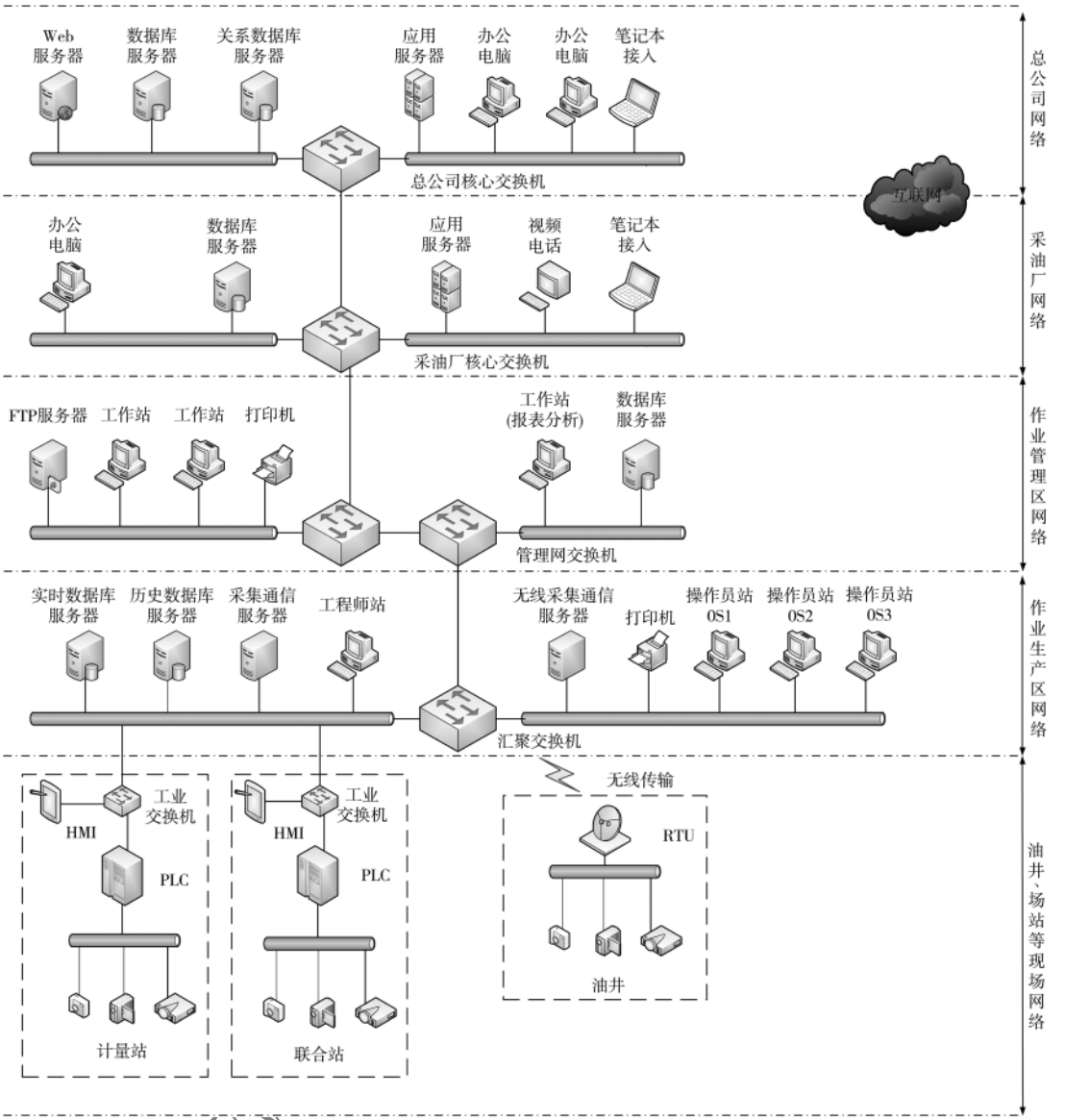

图 1 油田业务网络架构

通信的实时性及可用性，对安全性普遍考虑不足，缺乏有效的用户安全认证，数据传输加解密等基本信息安全手段。尤其是工业控制系统中的无线通信协议，更容易遭受第三者的窃听及欺骗性攻击。

另一方面应用软件存在安全威胁：首先，油田工控系统涉及自动化厂商众多，工控应用软件也是多种多样，很难形成统一的防护规范；其次，由于油田工控系统数据交互多，对软件开放性设计要求更多，也带来了安全风险。

(2)无线技术的应用风险

无线网络技术组网灵活、移动性好，没有长距离敷设线缆的限制，因此油田油井通信多采用无线传输。但无线传输易被攻击者伪装接入，简单加密的数据也容易被截获从而曝露敏感信息。

(3)工控主机缺乏安全防护

PC+Windows 的技术架构现已成为油田控制系统工程师站、操作站等上位机的主流，是实现人机交互的节点。目前油田工控系统在主机安全防护方面做得并不到位，很多都没有安装防护软件，即便安装了防病毒软件，病毒库也得不到及时更新，安全防护相对滞后。

(4)网络缺乏访问控制措施

由于油田工控系统项目建设周期长、集成商多、技改难度大等客观原因存在，许多控制网络都是“敞

开的”，不同的生产区域之间为了连接的便利性未做有效的区域划分，缺少边界防护。此外，追求业务需求和工作的便捷性，很多防火墙策略基本是全开的或没有严格的访问控制，一旦发生安全事件，例如勒索病毒事件，很容易造成安全威胁在工控网络迅速蔓延。

(5)移动存储介质滥用风险

一方面，可能由于用户个人原因，有意或无意通过移动存储介质拷贝数据并传播出去；另一方面，当移动存储介质感染病毒后，滥用将导致病毒在工业网络中扩散而带来风险。

2 油田工控系统等保 2.0 解决方案研究

《中华人民共和国网络安全法》第二十一条规定：国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改[3]。

网络安全等级保护是指对网络和信息系统按照重要性等级分级别保护的一种工作。安全保护等级越高，安全保护能力就越强。等保 2.0 的施行则把云计算、大数据、物联网、工业控制等行业也纳入了监管，把监管对象拓展到了全社会。

网络安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高网络安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度，等保工作的有序开展对促进我国整体网络安全发展可起到重要的推动作用。本节将依据等保相关标准要求探讨油田工控系统的解决方案[4-6]。

2.1 安全策略及管理

安全策略及管理制度是油田工控系统安全的基础，油田企业可从管理者的角度，制定安全管理策略和管理流程，确保不会出现因为误操作和管理制度的漏洞而造成安全隐患：

(1)建立安全管理机构；

(2)主管部门制定工业控制系统的安全政策；

(3)企业根据安全政策制定正规、可备案的安全流程；

(4)企业制定工业控制系统设备安全部署的实施指南；

(5)企业制定针对工控业务连续性、灾难性恢复计划以及应急处理机制；

(6)加强工业控制系统的配置变更管理；

(7)进行工控安全培训与安全意识培养。

2.2 安全通信网络

(1)安全目标

根据油田的系统或者业务划分不同的安全域[7]，工业控制系统网络与企业其他系统网络进行分区管理；安全域之间部署工业防火墙、网闸等隔离设备，配置访问控制策略并运行在防护模式；对网络内的重要网络设备进行冗余加固，提升设备性能与可靠性。

(2)控制措施

在安全区域划分的基础上，针对不同安全区域的业务重要性以及区域之间的通信与数据交换需求，部署适当防护强度的隔离防护设备。比如，以往巡井以人工方式去各个井场观测，现在电子巡井则由计算机完成，通过视频、抽油机参数、功图工况等信息直接在计算机上显示。为保证业务的连续性和网络安全，需要对传输网络、交换机等进行冗余加固，在井场数据出口处增加工业防火墙，配置访问控制策略，保障通信网络安全。

2.3 安全区域边界

(1)安全目标

确认工控网络边界，部署访问控制设备（工业防火墙或者工业网闸等）；通过白名单策略和协议分析实现工控网络之间、工控网络与管理信息网络之间的边界访问控制；对违规连接采取专门的监控措施，对非授权设备私自联到内部网络的行为以及内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；无线网络设备通过网络安全边界设备接入内部网络；对区域网络行为和重要的安全事件进行审计；定期备份或采取其他保护措施对审计记录进行保护。

(2)控制措施

在网络边界，如作业区生产网和管理网边界部署工业网闸、场站边界部署工业防火墙设备对违规连接行为进行监控，实现访问控制、操作行为监测、工控威胁检测、工控异常行为检测和基本网络攻击防护。对网络中的各种设备实施严格的日志审计、有效阻断、定位报警等措施降低网络中出现违规连接的风险。

在各网络区域核心交换机处部署工业监测审计系统，实现动态端口监测、流量实时监测、操作行

为监测、入侵检测、网络流量跟踪和取证等功能，加强工控网络异常行为和入侵行为发现能力，有效提升事件发现、安全处置和事件回溯等安全能力水平。

2.4 安全计算环境

(1)安全目标

对照主机最小化安装清单，只保留系统中必须安装的组件和应用程序，避免安装过多组件和应用，出现暴露的漏洞和风险。关闭不需要的系统服务，检查并关闭系统中默认共享文件夹，关闭易出现安全风险的高危端口；在指定位置的指定终端上加强安全管理，如采用 IP 地址限制或 IP+MAC 地址绑定等方式指定终端；采用免受恶意代码攻击的技术措施，或者基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；检查是否有保护重要系统程序或文件完整性的措施。

(2)控制措施

在服务器与操作员站、工程师站上部署主机安全防护卫士，利用软件的白名单功能，对设备和计算机的病毒入侵进行防范，确保非法进程和应用程序无法通过安全检查，确保将病毒、木马以及恶意软件阻挡在终端运行环境之外。同时对 USB 端口、蓝牙、无线接口进行管控，未授权设备禁止接入终端计算机，防范通过 USB 接口发起的高级攻击[8]。

在监控层汇聚交换机旁路部署运维堡垒机，可对作业区生产网络进行权重等级的划分和访问控制权限的划分，同时接管服务器、工程师站等设备的登录功能，人员统一在堡垒机上操作。实现权限分配、操作审计、身份合规性管理等功能。

2.5 安全管理中心

(1)安全目标

划分出管理区域，对分布在网络中的安全设备或安全组件进行管控，消除信息安全孤岛[9]；安全管理中心系统对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；对系统的资源和运行进行配置、控制和管理，包括用户身份鉴别、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等操作；对系统中的安全策略进行配置，包括安全参数的设置，对主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等操作。

(2)控制措施

在作业区管理层部署工业安全设备统一管理平台[10]，将油田系统内所有工控安全设备采集到的网络流量信息、人员操作信息、异常告警信息进行统一收集和整理分析，结合管理平台自身的安全漏洞库和攻击特征库，识别、跟踪分析和判断各项操作行为和动作的合规性与安全性，对于超出当前安全基线的行为提供全程的行为审计，进而掌握整个油田工控系统中存在的安全隐患和风险，对于明显不符合当前工控系统操作工艺流程和安全规定的异常行为和事件加以管控。

2.6 工控安全设备部署

基于以上安全分析，工控系统安全设备部署如图 2 所示。

3 结论

综上所述，面对油田工控系统目前存在的安全问题及两化融合进程中出现的安全隐患，需要在发展的过程中，对油田工业控制系统进行安全防护体系设计，并采取相应的技术防护手段，结合管理等体制机制手段，动态解决油田行业工控系统存在的安全问题，保障国家关键信息基础设施领域的网络安全。

参考文献

[1] 冯玉敏，张辉，谢文满，等.智慧油田是油田发展的未来[J].信息系统工程，2012(6)：101－103，105.

[2] 王迪，鲁晓斌，李海涛，等.油田生产过程中的 SCADA 管理[J].化学工程与装备，2018(2)：122－123.

[3] 中华人民共和国网络安全法[S].2017.

[4] GB/T 22239－2019 信息安全技术网络安全等级保护基本要求[S].2019.

[5] GB/T 25070－2019 信息安全技术网络安全等级保护安全设计技术要求[S].2019.

[6] 王晓龙.油田工控网络信息安全防护系统的研究与实现[D].大连：大连理工大学，2018.

[7] 宋杰，李文虎.工业控制系统安全设计方法研究[J].公路交通科技(应用技术版)，2018(8)：327－330.

[8] 工业和信息化部.工业控制系统信息安全防护指南[Z].2016.

[9] 汪俊华.国内石油企业“数字油田”建设的研究[J].中国管理信息化，2013(8)：56－57.

[10] 姜海庆.统一安全管理平台在网络管理中的应用[J].通信技术，2017，50(9)：2089－2093.

(收稿日期：2020－06－22)

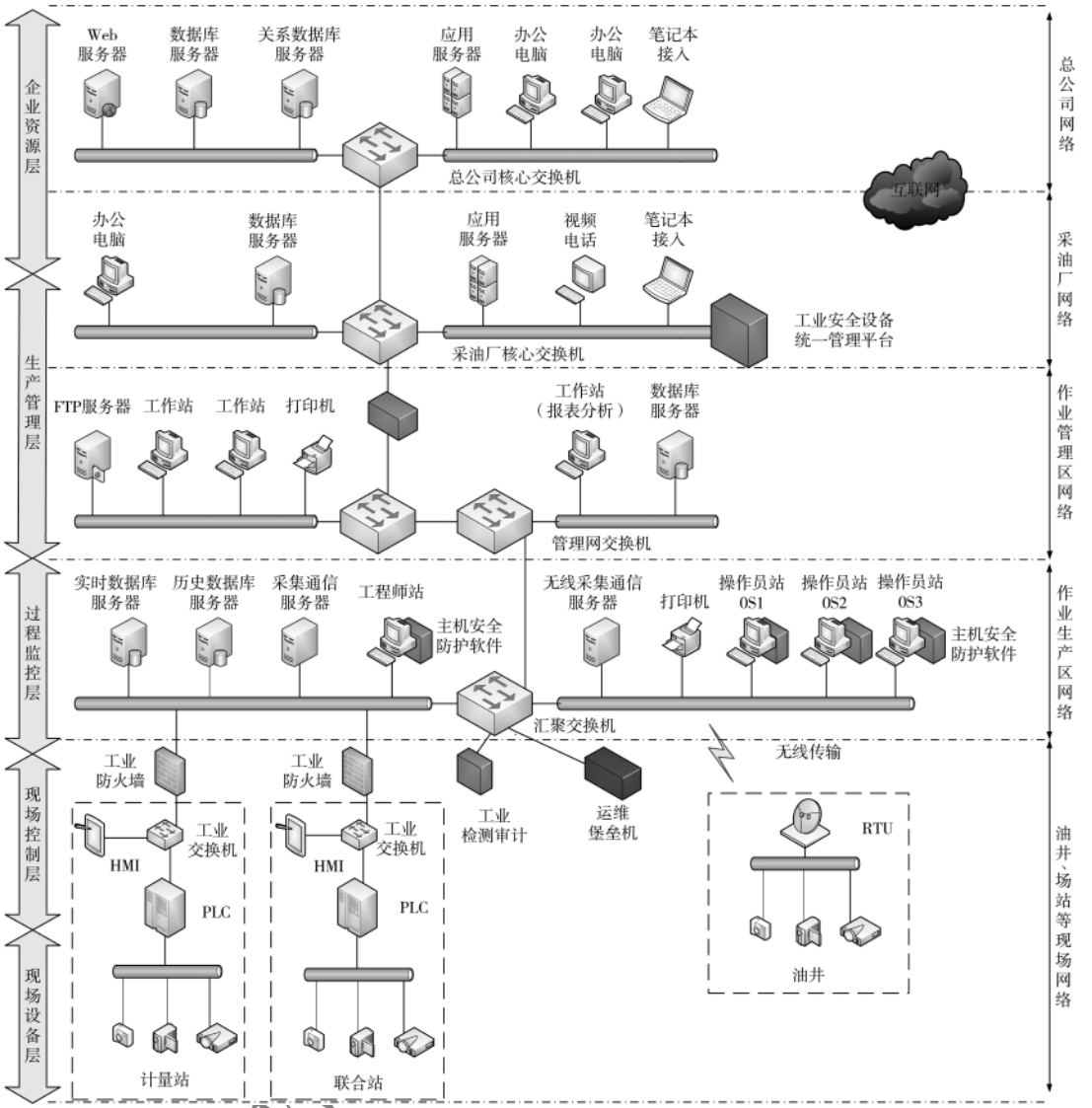

图 2 工控系统安全设备部署示意图

作者简介：

王晔(1986–)，女，硕士，工程师，主要研究方向：工控信息安全。

靳方略(1990–)，女，本科，工程师，主要研究方向：工控信息安全。

吕铭心(1992–)，女，本科，工程师，主要研究方向：工控信息安全。

版权声明