



工业控制系统安全防护方案

梁琦

(胜利石油管理局, 山东 东营 257000)

摘要: 以油田的工业控制系统为例, 结合目前的网络架构, 分析工业控制系统面临的各类安全风险, 针对国内工业控制系统安全标准和法律法规提出一套完整的能源行业工业控制安全防护方案。

关键词: 工业控制系统; 网络安全隐患; 防护方案

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018154

Security& safety protection solution of ICS

LIANG Qi

Shengli Petroleum Administration, Dongying 257000, China

Abstract: According to the oil field ICS architecture, combined with the current network security technology, all kinds of risks faced by the industrial control system were analyzed, and a complete set of industrial security & safety protection scheme standard for the energy industry was put forward.

Key words: industrial control system, risk of network security, protection scheme

1 引言

随着两化融合的深度发展, 油田内部的生产、经营、管理理念也发生着质的变化, 普遍采用高度自动化的生产技术, 结合高度信息化的运营管理手段, 集中管理采油、输油等关键生产过程, 建立统一监控平台, 集中采集、统一分析、实时展示现场设备的实时生产数据, 提升生产效率, 降低生产成本, 随着互联网技术的广泛应用, “智慧油田”建设已经取得了丰硕的成果。

信息化、智能化、集成化、可视化和实时化作为现代企业的重要标志, 生产管理对信息的依

赖程度不断加大, 随着信息系统、工业控制系统(industrial control system, ICS)集成度的不断提升, 工业控制系统不得不采用通用协议、通用硬件和通用软件, 满足两化融合、物联网建设的系统集成需求。

自2010年“震网”事件以来, 工业控制系统网络安全研究进入了持续的高热度阶段, 曝光的漏洞数量逐年上升(数据来源: CNNVD), 如图1、图2所示。

伴随而来的是工业控制安全事件频繁爆发, 呈快速增长的趋势, 2011年有140余起, 2012年有197起, 2013年有257起, 2014年有245起,

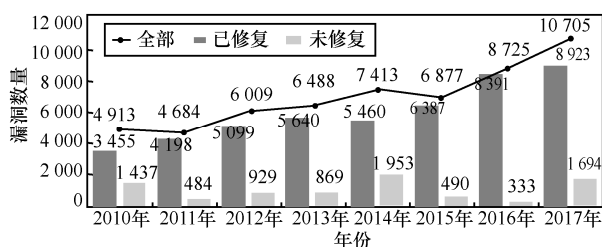


图1 漏洞趋势分布

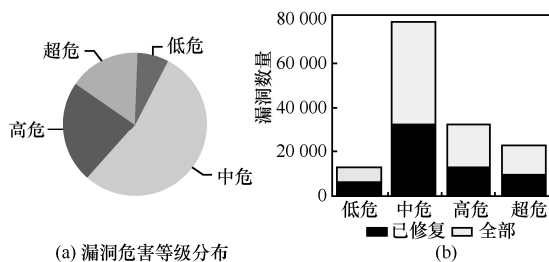


图2 漏洞危害等级分布

2015 年有 295 起，多集中在能源行业和关键制造行业。

2 工业控制系统风险分析

目前，随着计算机和网络技术的发展，加大了企业信息化管理的建设与投用，客观上形成了“两网融合”的局面，原本封闭的生产网与开放的管理网互联互通，生产网通过管理网对外暴露，病毒、木马等威胁正在向工业控制系统扩散，基于当前网络安全措施的通用性与局限性，工业控制系统依然面临病毒、黑客攻击和非法入侵等现实威胁，工业控制系统的安全就显得更为重要和迫切。

(1) 操作系统安全漏洞

目前 DCS、SCADA、PLC 等工业控制系统的操作站基本采用 Windows 平台，任一版本 Windows 系统均在不停发布漏洞补丁。

鉴于工业控制系统相对独立性，工业控制系统制造商也很少针对 Windows 系统漏洞补丁做兼容测试，用户通常不会（不敢）在工业控制系统投入运行后，对现运行的 Windows 平台设备打任何补丁，从而导致工业控制系统存在被

攻击的漏洞。

(2) TCP/IP 地址协议固有风险

TCP/IP 协议设计上就存在致命安全漏洞，TCP/IP 地址协议簇设计的基础是互相信任，仅考虑实现不同软硬件结构计算机的互通互联、资源共享，忽略了网络、网际间的安全问题。信任机制的协议设计相对简单，缺乏对应用程序层用户身份的鉴别以及网络层、传输层路由协议的鉴别等先天性缺陷。

(3) 应用软件安全漏洞

目前油田生产过程的工业控制系统厂商众多，上位机的组态软件、应用系统没有采用统一的规范进行选型、建设，从而导致了工业控制系统安全问题的防护规范难以统一。

目前的工业控制系统基本采用 Windows 环境，基于 Windows 环境下的应用软件面向网络应用时，需开放其相应的应用端口，仅 Windows Server 2008 系统使用的端口号就超过 16 000 个，攻击者通常会利用一些工业控制系统对外公开的固定通信端口、安全漏洞获取现场生产设备的控制权。

(4) 不安全的工业控制协议

现场工业控制系统的通信协议基本以 ModBus 与 OPC 为主，它们的设计基础与 TCP/IP 地址类同，同样没有考虑信息安全。

ModBus 通信协议是 1979 年由 Modicon 公司发布的用于工业现场总线规约，采用主从通信模式（master/slave），广泛应用在分散控制系统方面。

ModBus TCP 的设计以实时 I/O 优化为主，在 RTU 串口协议上加一个 MBAP 报文头，基于 TCP 的可靠连接服务，取消了 RTU 串口协议的 CRC 校验码，同时在 ModBus RTU 协议前面加上 5 个 0 以及 1 个 6，相比 RTU 串口通信降低了工业控制系统的安全防护功能。

OPC（OLE for process control）在基于



Windows 应用程序与现场过程控制应用之间建立了桥梁,在工业现场已被大量使用。

OPC 协议基于微软的 OLE 技术,远程通信需使用 Microsoft 的 DCOM 协议,OPC 服务器端开放 135、145 远程访问端口(病毒经常攻击的端口)建立握手,握手后 OPC 服务器随机动态分配数据通信的端口号,这种动态端口通信机制导致了传统防火墙无法保护 OPC 服务器,防火墙提供的安全保障被降至最低。

(5) 网络攻击与入侵

分布式拒绝服务(distributed denial of service, DDoS)攻击借助于客户端/服务器技术,操纵或由病毒自动执行,联合多台计算机作为攻击平台,将工业控制系统作为攻击对象,消耗工业控制系统的网络带宽、连接数、CPU 处理能力、缓冲内存等,阻塞正常的网络通信服务,常用的 ping flooding、UDP flooding、Syn flooding、ACK flooding 等流量型攻击手段同样威胁着工业控制系统。

工业控制系统一旦遭受 DDoS 攻击,轻则控制系统的网络通信完全中断,重则导致控制器死机,DDoS 攻击已在国外的工业控制系统中发生过多次,导致的后果也非常严重。

(6) 病毒与恶意代码

目前的工业控制系统已经广泛使用 Windows 系统平台的工业服务器(工业控制 PC),针对普通 PC 的病毒与恶意代码攻击事件同样威胁工业控制系统。

2017 年 5 月 13 日,国家计算机病毒应急处理中心通过对互联网的监测,发现 1 个名为“WannaCry”的勒索软件病毒正在全球大范围蔓延,我国部分大型企业内网也深受其害。

WannaDecryptor 利用 Windows 操作系统 445 端口存在的 SMB 漏洞(MS17-101)自我复制、主动传播,针对关闭防火墙的目标机器,实现远程代码执行,加密被攻击计算的所有类型文件,进行勒索。

著名的震网(stuxnet)病毒,利用 3 个 0-day Windows 系统漏洞和 2 个 WinCC 系统漏洞,伪造驱动程序的数字签名,通过一套完整的入侵和传播流程,突破工业专用局域网的物理限制,利用 WinCC 系统的 2 个漏洞,破坏性攻击 SIMATIC 数据采集与监控系统。

(7) 无线网络的安全漏洞

由于无线网络具有灵活的组网特点,整体网络系统具有成本低、移动性好、易安装维护等优势,目前现场井口通信设备基本采用无线通信方式。

尽管无线通信有传统有线网络无法比拟的优势,但由于无线网络传输媒介的特殊性,使得一些攻击更容易实施。例如,通过无线接入非法访问网络资源实施攻击;无线链路上传输的未被加密数据的泄露;DDoS 攻击无线网络,导致实时数据的丢失,破坏数据的完整性。

综上所述,现今 ICS 面临的安全形势十分严峻,ICS 的攻击者/黑客正变得越来越聪明、越来越高效,入侵工业控制系统的成功率也越来越高,ICS 威胁不论是数量、类型还是风险程度都呈现出快速增长趋势;从造成的后果来说,网络攻击扰乱了 ICS 运行,有的甚至对 ICS 造成物理损害。

3 工业控制网络安全标准及法律法规

随着工业自动化、信息化融合进程的快速推进,工业控制、信息、网络、通信技术的广泛应用,工业控制系统的脆弱安全状况以及日益严重的攻击威胁,已经引起了国家相关部门的高度重视,甚至提升到“国家安全战略”的高度,并在政策、标准、技术、方案等方面展开了积极应对。

2011 年 11 月,工业和信息化部发布了 451 号文件《关于加强工业控制系统信息安全管理的通知》,明确提出了重点领域工业控制系统信息安全管理要求,并强调“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则。

2016年8月组织《信息安全技术工业控制系统安全控制应用指南》等14项标准研制,指导工业企业工业控制安全保障能力建设;同年10月制定发布《工业控制系统信息安全防护指南》,提出工业企业加强工业控制系统安全防护的具体措施。

2017年6月1日实施国家《网络安全法》,明确地将工业控制安全写入立法条目,第31条明确指出:国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域以及其他一旦遭到破坏、丧失功能或数据泄露,可能严重危害国家安全、国计民生、公共利益的关键信息基础设施,在网络安全等级保护制度的基础上,实行重点保护。

针对关键信息基础设施的工业控制系统安全,又制定颁发了相关的国家标准,对工业控制系统的安全防护等级、网络隔离类设备提出了具体的要求及相应功能,如GB/T 32919-2016《信息安全技术工业控制系统安全控制应用指南》、GB/T 33009.1-2016《工业自动化和控制系统网络安全集散控制系统(DCS)第1部分:防护要求》、GB/T 20279-2015《信息安全技术网络和终端隔离产品安全技术要求》等。

4 工业控制安全防护解决方案

鉴于油田工业控制系统基于控制分散、操作和管理集中的基本设计思想,制定完整的工业控制安全防护方案,按照4个不同的生产管理级别,划分不同的安全管理区域,根据分层级的纵深安全防御策略,完善工业控制网络安全建设,全面提高安全生产管理水平、工作效率和管理效率。

- 总公司管理级,以各采油厂数据(实时、关系)平台为数据源对象,将总公司需要的数据同步上来,建立总公司管理系统;
- 采油厂管理级,部署实时数据库,接收管理区(作业区中)送来的数据,实现实时

监控、工况分析、安全管理、报表管理、设备管理;

- 生产作业区级,包含管理区办公网和管理区生产网;
- 井场现场级,以场站及油井为主。场站为有人值守,含控制系统,以有线网络为基础;油井则采用无人值守方式,通过RTU采集并上传数据,包括有线及无线网络。

4.1 传统网络安全产品

为了加强工业控制系统的安全能力,企业在管理网和生产网之间虽然增加了网络安全措施,采用了防火墙、防病毒软件等安全产品,但是由于工业控制系统与上层管理系统通信多采用OPC等方式,需要微软DCOM协议的支持,防火墙、防病毒软件等措施目前均难以弥补相应安全漏洞。

另外,传统IT网络和工业控制网络在架构、协议、安全、可信等不同维度均存在很大的差异,见表1。

表1 传统IT网络和工业控制网络的差异

特点	传统IT网络	工业控制网络
应用领域	极其广泛	工业领域, SCADA
开放性	完全开放, 互联网	相对封闭
设备更新	频繁	不频繁
软件系统更新	频繁	不频繁
数据机密性要求	高	一般
持续可靠性要求	一般	非常高
对待病毒	允许	不允许
应用数据	极其复杂	特定
应用协议	HTTP、SMTP、FTP等	OPC、ModBus、IEC104等
安全要求	网络可用的前提下, 相对安全	网络绝对安全的前提下, 网络可用

通过对比不难发现,针对工业控制网络的安全防护,迫切需要更专用、有效的网络安全技术和产品,通过使用专用网络安全设备对工业控制系统进行防护,有效消除上层应用管理系统实施



后带来工业控制系统的安全隐患，为企业的安全生产提供有力保障。

4.2 安全防护策略

4.2.1 操作系统加固

根据工业控制现场实际情况，在工程师站、操作员站、服务器上部署基于白名单机制的主机防护或主机加固类软件，确保系统完整性，实现注册表文件、配置文件、专用工程软件的保护。

对操作系统进行加固，实现对已知和未知病毒与恶意代码的防范，阻止对主机未授权的访问，弥补操作系统漏洞不能及时打补丁（或无法打补丁）引起的攻击。

4.2.2 网络安全审计

在现有的工业网络中，合理部署网络安全审计设备，实时监测工业控制网络流量，保障业务生产运行。通过对工业控制网络的流量数据、系统事件和安全态势进行实时监测和告警，帮助客户实时掌握工业控制网络安全运行状况，有效保障客户业务安全稳定运行。

完整网络安全审计记录，具备事件回溯能力，对工业控制网络中存在的所有网络活动提供安全审计、协议审计和流量审计，以完整记录形式为客户进行事件处置和事件回溯提供技术能力，为工业控制系统的安全事故调查提供坚实的基础。

可视化感知工业控制网络安全状态，全面呈现工业控制网络安全事件状态、系统运行状态和网络流量行为，帮助客户感知工业控制网络整体安全状态，提出安全防御建议，协助客户完善安全防护体系。

4.2.3 边界隔离防护

通过边界隔离防护，建立纵深防御体系，有效阻断病毒、木马程序、黑客非法攻击的传播途径，同时在关键工业控制设施串行部署工业防火墙，主动发现并阻断、隔离上述的网络非法攻击和入侵，彻底规避工业控制内网遭受攻击的可能。

（1）生产管理層和过程监控层之间的安全防护在生产管理層和过程监控层之间，部署网络

安全单向导入设备，仅允许两个网络之间合法数据的物理单向传输，实现生产网向管理网的实时、历时数据、关系数据库等生产实时信息的单向采集，预防阻止来自管理网向生产网的攻击。

（2）过程监控层和现场控制层之间的安全防护

过程监控层和现场控制层之间通常使用 OPC 工业协议通信，传统 IT 防火墙不足以满足安全需求，故采用单向导入设备、工业控制防火墙等专业的工业网络安全隔离设备（系统），基于代理模式解决 OPC 通信（135 端口）带来的安全瓶颈问题，阻止病毒和任何其他非法访问，提升网络区域划分能力，从本质上解决工业控制系统的网络安全。

（3）关键控制器防护

使用工业防火墙保护关键控制器，深度解析控制器厂商的专有协议，智能学习工业控制系统访问行为，配置工业防火墙的白名单，建立网络和通信“白环境”，管控工业控制网络通信流量、局部网络的通信速率，指定专有操作站访问指定的控制器，阻断病毒、蠕虫恶意软件扩散和入侵攻击，保护控制器的安全运行。

4.3 整体防护方案

工业控制网络安全防护项目的建设实施，提升设备、系统、网络的可靠性、稳定性，确保工业网络整体安全性。

实现管理区和生产区的纵向边界防护，有效避免来自信息网络的安全隐患对生产控制网络的威胁；实现生产区域内各业务系统之间的横向逻辑隔离和安全防护，阻止来自区域之间的越权访问、入侵攻击和非法访问。

实现上位机、工程师站、系统服务器系统的安全加固，通过白名单机制构建安全基线，防止病毒木马、恶意软件对系统的破坏；实现对整体网络的入侵检测及审计，及时发现网络或系统中违反安全策略的行为和被攻击的迹象。

整体防护方案如图 3 所示。

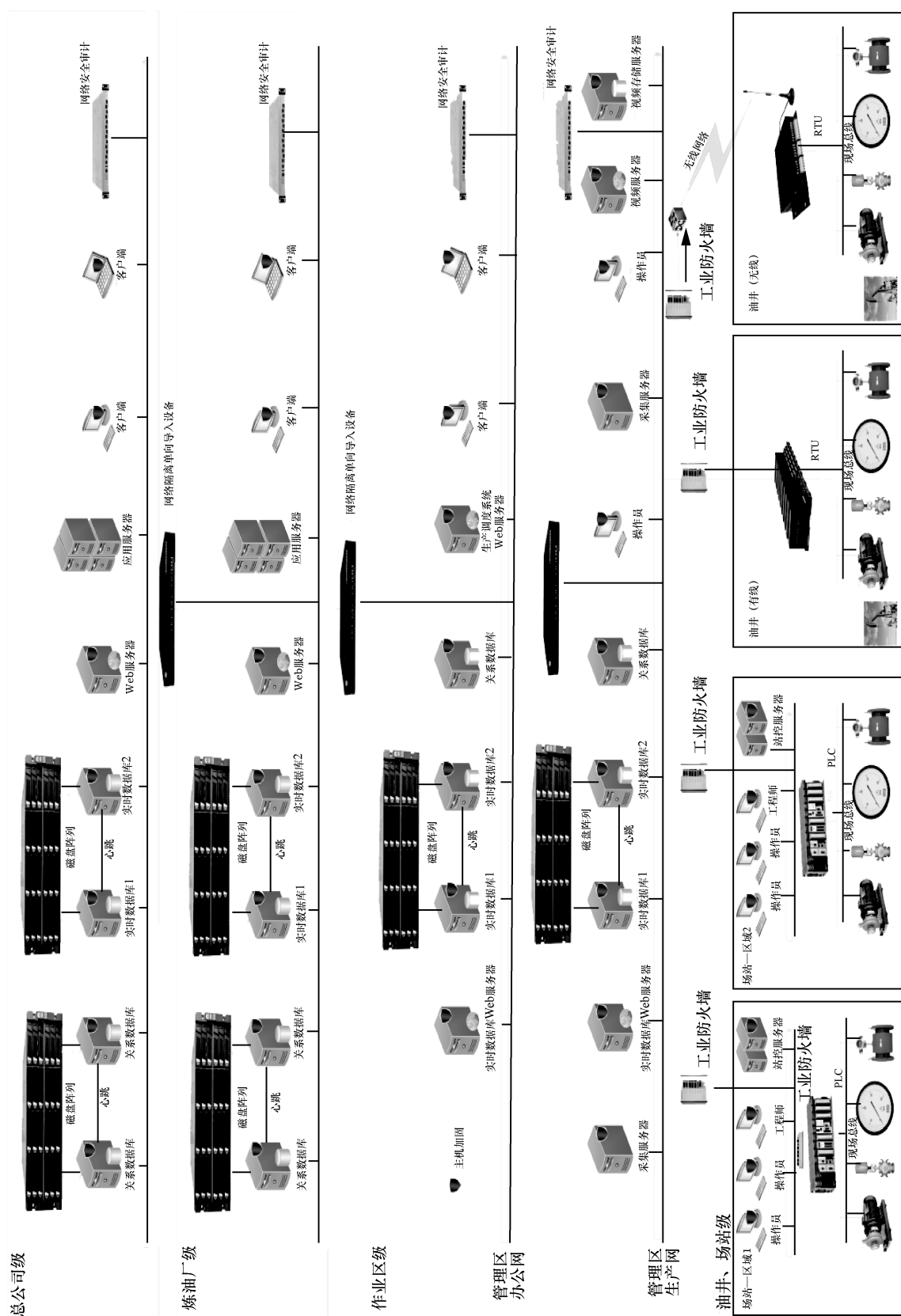


图3 整体防护方案



5 结束语

工业控制系统信息安全问题已迫在眉睫,本文针对智慧油田建设涉及的工业控制系统网络结构和安全需求,通过对需要防护的工业控制网络自身特性的研究,结合国家提出的工业控制系统安全的相关标准及法律法规,量身定制专用防护设备进行防护,提出一套完整的工业控制安全防护方案。

本文方案更加贴近生产现场需求,完善井场现场级、生产作业区级、采油厂管理级、总公司管理级4个层面的工业控制系统的网络安全建设,可以满足生产环境安全、高效运行,最终实现信息安全的纵深防御策略。

参考文献:

- [1] 工业和信息化部. 工业控制系统信息安全防护指南[S]. 2016.
Ministry of Industry and Information Technology. Industrial information security protection guide for industrial control systems[S]. 2016.
- [2] 公安部信息安全等级保护评估中心. 信息安全技术信息系统安全等级保护实施指南[S]. 2010.
Information Security Grade Protection and Assessment Center of the Ministry of Public Security. Information security technology information system security level protection implementation guide[S]. 2010.
- [3] 王玉敏. 工业控制系统信息安全第1部分: 评估规范(节选)[J]. 自动化博览, 2015(z2).
WANG Y M. Industrial control systems information security part 1:

assessment specifications[J]. Automation Panorama, 2015(z2).

- [4] 祝子涵. 浅谈工业控制系统信息安全风险与防御[J]. 大科技, 2017(28).
ZHU Z H. A brief talk on information security risk and defense in industrial control systems[J]. Big Technology, 2017(28).
- [5] 传统防火墙在工业环境中的不足及工业防火墙在工业环境中的应用[EB]. 2017.
Deficiencies of traditional firewalls in industrial environments and application of industrial firewalls in industrial environment[EB]. 2017.
- [6] 杨思维. 升级版德国“工业4.0平台”经验对我国制造业的影响[J]. 电信科学, 2016, 32(1): 108-111.
YANG S W. Impact of the upgraded version of German “industrial 4 platform” on China’s manufacturing industry [J]. Telecommunications Science, 2016, 32(1): 108-111.
- [7] 刘甲男, 杜彦洁, 孟宪义. 基于互联网思维的能源互联网发展[J]. 电信科学, 2016, 32(3): 176-182.
LIU J N, DU Y J, MENG X Y. Development of energy internet based on internet thinking [J]. Telecommunications Science, 2016, 32(3): 176-182.
- [8] 王帅, 汪来富, 金华敏, 等. 网络安全分析中的大数据技术应用[J]. 电信科学, 2015, 31(7): 145-150.
WANG S, WANG L F, JIN H M, et al. Big data application in network security analysis [J]. Telecommunications Science, 2015, 31(7): 145-150.

[作者简介]



梁琦(1978—), 男, 胜利石油管理局胜利油田信息化管理中心网络与系统管理科科长、高级工程师, 主要研究方向为系统集成、云计算、工业控制安全等。