山西省地方煤矿工业信息网络安全现状分析及对策初探

杨建宏

（山西兰花科技创业股份有限公司信息中心）

摘　要：从山西省地方煤矿信息网络现状出发，总结分析了目前安全方面存在的主要问题及根本原因，就信息网络安全的管理与建设的对策初步进行了探究，旨在进一步提高煤矿管网治网用网的能力和水平，保证系统安全稳定地运行。

关键词：煤矿；网络；信息安全；管理

1　前言

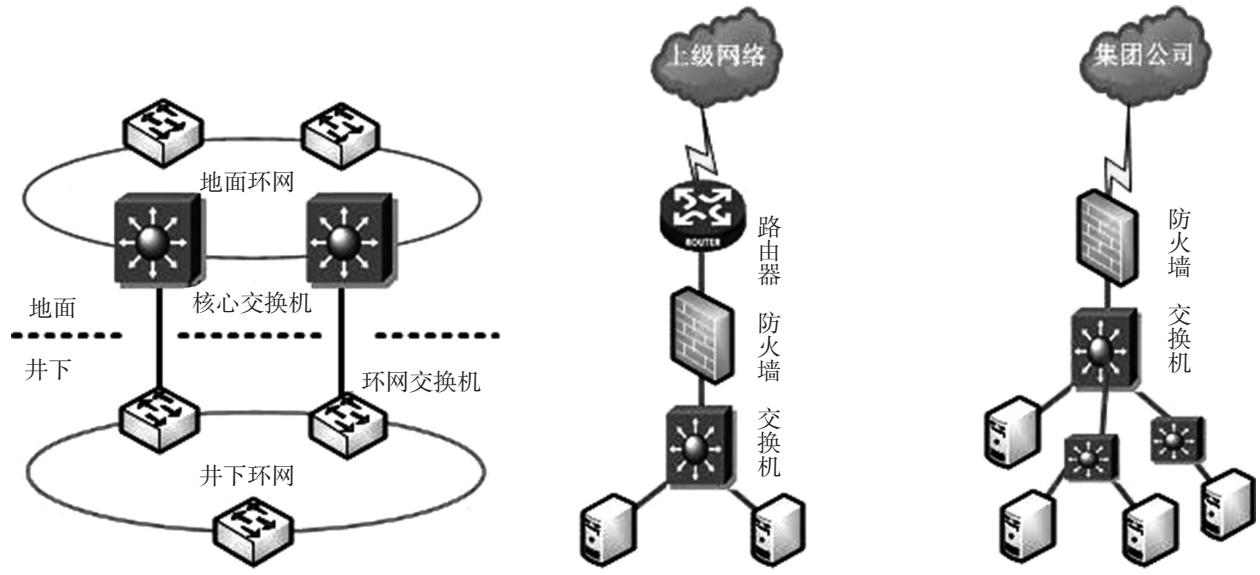
近年来，随着国家对煤矿安全生产发展的要求和企业自身发展的需要，煤矿陆续建设了工业以太网、煤炭专网与办公网，实现了对企业生产经营管理，井下现场采掘环境、生产设备等监测、预警、闭锁以及控制等。通过对晋城、长治、阳泉等地方煤矿调研了解，煤矿信息网络系统的安全防护任务依然存在一些问题。本文将就地方煤矿企业信息网络安全现状及管理进行分析和初步探究。

2　地方煤矿企业信息化网络现状

山西省地方煤矿信息化网络在多年的建设中，根据上级主管部门的要求以及企业自身的要求，主要建设有以下三个子系统：

2.1 工业以太网

根据山西省质量标准化[1]以及国家煤矿安监局关于安全监控系统升级改造多系统融合[2]的要求，全省大部分地方煤矿陆续建设了覆盖井上下的工业以太网，见图1.(a)。系统一般由地面、井下分别组成的1000M以上环形网络组成，地面与井下分别



(a)煤矿工业以太网　(b)煤矿煤炭专网　(c)煤矿企业办公网

图1　煤矿信息化网络拓扑示意图

通过布置在不同井筒或一个井筒保持一定间距不同位置的光纤骨干线缆进行耦合。地面一般覆盖调度室、风机房、变电站、洗煤厂、瓦斯抽放泵站等,井下一般覆盖中央变电所、各采区变电站等主要机电硐室。工业以太网主要担负着两化融合,以及井上下采掘环境、生产设备等的远程监测、预警、闭锁以及各种控制等,对煤矿少人化或无人化起到至关重要的作用。

2.2 煤炭专网

根据山西省煤炭专网建设[3]以及煤炭监管信息平台建设[4]等要求,煤矿企业建设了煤炭专网,见图1.(b)。系统一般呈星形结构,通过"煤矿→集团公司(主体企业)→县(市、区)局→市局→省厅"逐级上联到山西省煤炭厅,是主管部门对煤矿安全生产信息化监管的源头,担负着煤矿安全生产信息调度、产运销经济运行数据采集和填报等30多个安全生产系统的实时数据采集、汇总、上传以及上级主管部门日常对煤矿的安全监管、指挥、协调等职能。

2.3 企业办公网

企业办公网是煤矿企业根据自身管理需要,建设的集办公、财务、销售、供应等一体的管理网络,见图1.(c),作为企业管理网络的核心,接收、综合工业以太网、煤炭专网等信息,进行数据集成显示、关联分析等,覆盖了企业主要生产经营管理业务。

3　地方煤矿企业信息网络安全存在的主要问题[5]

煤矿信息网络,尤其是覆盖了生产控制系统的工业以太网,万一被非法入侵者攻入控制了系统,随意控制煤矿井下设备(尤其是主通风机或掘进面局部通风机)供电电源,很可能造成恶性生产事故。但在实际运行中,煤矿信息网络安全防护工作,并未引起更多管理层的重视,存在很多突出的安全问题,以下是比较常见的问题:

3.1 管理方面

(1)有的煤矿领导层并没有认识到新形势下做

好网络安全工作的重要性、复杂性和艰巨性，责任不清，也没有落实到具体岗位，《网络安全法》出台后也未进行过任何专题宣传和教育培训，网络安全意识和依法管网治网用网的能力和水平比较薄弱。

（2）有的煤矿并没有按照《网络安全法》认真履行网络安全等级保护义务，没有按照《关键信息基础设施确定指南（试行）》对本企业存在管理和运营的关键信息基础设施或者重要的信息网络系统确定名录，对本企业核心信息系统的安全可控程度低。

（3）有的煤矿基本没有日常网络安全监测，没有任何安全审计措施，也没有定期开展网络安全自查工作和风险评估，对本企业信息系统的风险状况不明，没有对供应商的产品或服务风险和隐患进行防护，没有对核心技术人员的安全风险进行控制，整体上处于一种失控状态。

（4）有的煤矿没有制定信息网络安全应急机制和应急预案，也没有成立应急处理机构，没有进行应急演练，技术人员和管理人员的应急处置能力普遍较低，在发生突发事件，往往不知如何处理。

3.2 技术方面

（1）有的煤矿工业以太网和其它网络边界之间没有任何隔离措施，边界安全防护意识差，闹得沸沸扬扬的勒索病毒等容易受到攻击传染的恶意端口没有进行封堵，网络边界路由器（或防火墙）设备的参数随意外传，非常容易受到病毒感染或被外部人员入侵。晋城市煤矿安全生产信息调度中心部署的全网安全态势感知系统，就发现了大量来自域外国家网络攻击，以及等待触发的勒索病毒。

（2）有的煤矿企业缺少灾患意识，杀毒软件甚至自安装后就没有升级过病毒库，重要系统的数据库和应用软件没有备份，或者象征性的与数据库和应用软件备份在同一台服务器上，万一系统因某种原因故障宕机或崩溃，尤其是磁盘损坏，带来的问题可能是灾难性的。

（3）有的煤矿信息安全自身防护意识不强，服务器操作系统、应用软件登录密码为空、弱密码的现象比比皆是；数据库超级管理员的密码不仅非常简单，而且所有数据操作都是用超级管理员，其实数据库超级管理员甚至可以远程格式化服务器硬盘。

（4）有的煤矿与供应商没有签署任何保密协议，对其技术人员过于相信，远程操作网络设备或服务器无人监护的现象比较严重，随便出入机房单独操作且无人监护的现象也比较突出。笔者就曾遇到外单位技术人员离职后抱着对原工作单位报复的心态，对煤矿网络进行破坏的情况。

4 煤矿企业信息网络安全问题的根本原因分析

地方煤矿信息化网络安全存在的问题，不是一朝一夕形成的，不仅有管理方面的原因，也有技术层面原因，但笔者认为最根本的是人的因素，是管理者安全意识缺失、人才缺乏以及制度不能有效执行造成的：

（1）煤矿管理者已经习惯了什么喊的紧就抓什么的管理模式（比如安全、环保），信息网络的安全并没有提到管理者的议事日程，更没有引起管理者的足够重视。《网络安全法》出台以前，虽然国家也出台了很多安全管理条例法规，但失责追责的力度不足以使管理者真正树立信息网络安全红线意识。

（2）煤矿企业由于行业特点，更多的是采、掘、机、运、通、防治水、地质等涉煤主体专业，信息化专业作为辅助专业，技术人员少之又少，而且知识层次普遍较低，专业技能和安全知识相对匮乏，外出参训的机会基本没有，往往管理者和技术人员既不知道如何做，也不知道会有什么后果，所以也就习以为

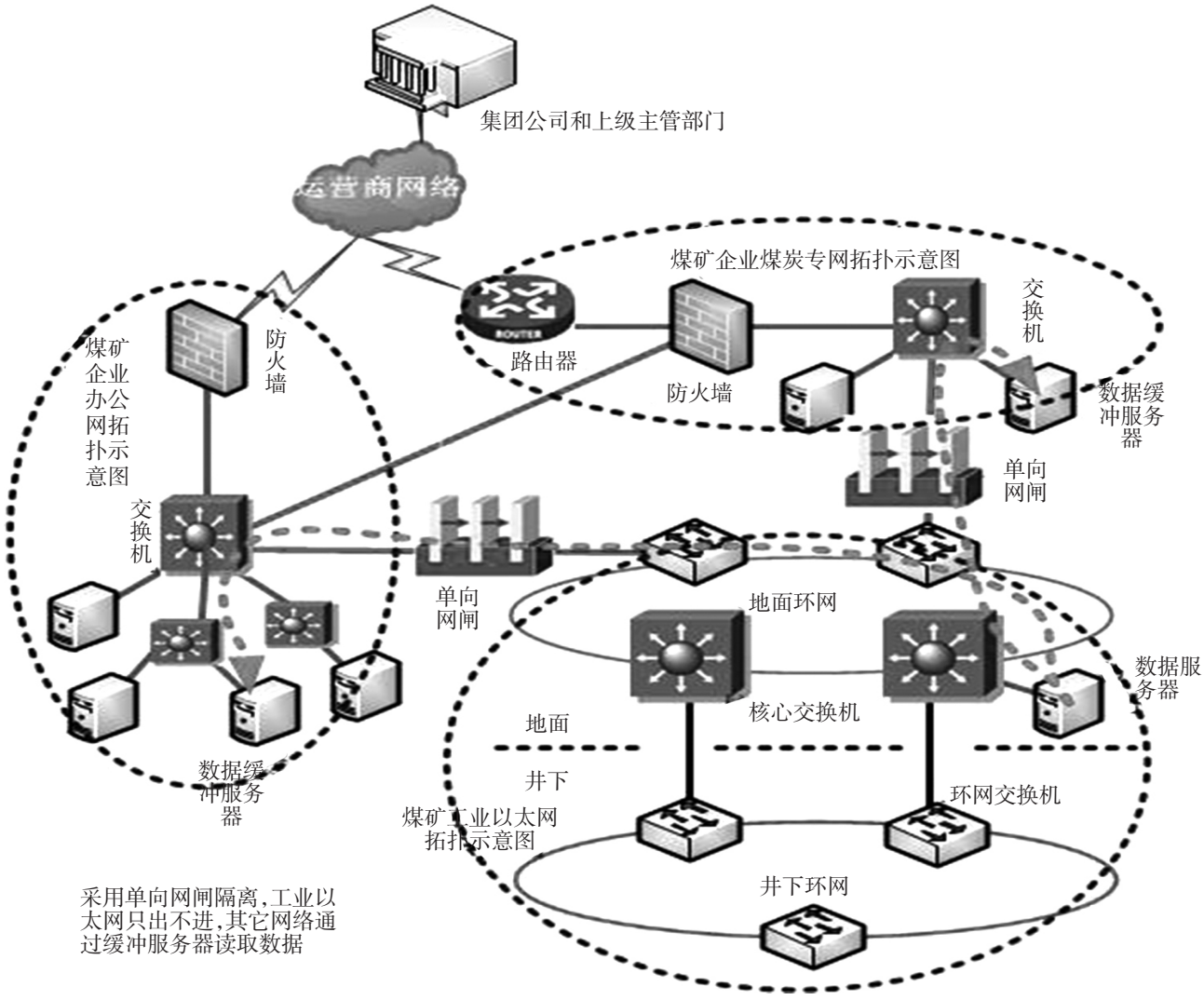


图2　不同安全级别信息网络子系统之间隔离和保护示意图

常、无所畏惧了。

（3）不少煤矿企业的信息部门制定了较为详细的信息网络安全措施与管理制度，但往往缺乏行业或上级管理部门行之有效的安全检查、督查，仅仅靠管理人员和技术人员的自律进行落实，效果往往大打折扣。

5　地方煤矿信息网络安全管理与建设对策探究

5.1 管理方面

（1）煤矿单位必须从全局高度，深刻认识新形势下做好网络安全工作的重要性、复杂性和艰巨性，党政主要负责人和分管领导一定要树立第一责任人和直接责任人的责任意识，按照责任分工，一级抓一级，层层推进落实，才能切实抓好信息网络系统的安全工作。

（2）要加强《网络安全法》相关法律法规以及网络安全知识的宣传教育和培训工作，提高全员的安全意识和安全知识，不仅要制定完善的安全管理体制和制度，还要坚持贯彻执行，只有全员共同参与，

才能切实提高管网治网用网的能力和水平。

（3）要认真履行网络安全等级保护义务，明确本单位重要（如工业以太网和PLC控制系统等）的信息系统防护对象，深入查找薄弱环节，及时核查整改，加强对系统间、业务间关联风险的评估，安全技术措施与系统建设同步规划、同步建设、同步使用，坚持管理和技术并重，做好识别、防护、监测、预警、响应、处置等环节的技术支撑和管理衔接。

（4）要结合本单位实际情况制定完善应急机制和应急预案，成立应急领导和技术处置机构，定期组织开展各种专项或综合应急演练，可以充分利用系统中发生的各种安全事件，举一反三，不断提高管理人员和技术人员的应急处置能力。

5.2 技术方面

（1）做好信息网络子系统自身的安全防护，树立“防外为主、内外兼防”的安全意识，在确保设施、设备、空间等的物理安全的基础上，要以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，做好网络加密、病毒防治、数据备份、漏洞扫描、区域隔离、访问控制、认证审计等工作，加强采购和使用过程中的风险管理，加强对服务供应商及核心技术人员的安全风控，尤其是防范外来服务和产品带来的风险隐患。

（2）具有不同安全级别信息网络子系统之间必须进行隔离和保护[6]，绝不能没有安全措施的直联，防护不到位的工业以太网极有可能造成安全生产事故。不同安全级别信息网络子系统之间必须配置必要的安全设备（如网闸、防火墙等，见图2），控制互相之间信息（或指令）的安全流动，具备真实、完整、可用、保密与不可抵赖[7]，必要时还需要具备防窃听、防篡改、防伪造、防重放、防抵赖等能力。

（3）要尽量减少信息网络对煤矿外部的互联出口，并尽可能扎紧“篱笆”。采用安全、审计、认证等各种设施，不断提升防入侵、防攻击、堵漏洞等能力，尤其是要做好远程访问用户的操作审计。同时，还要重点解决好管理者“互联网+管理”的安全防护要求，内网资源层层通过NAT映射至互联网后可能带来的各种安全隐患。也可考虑将服务资源加密后同步到租赁的公有云，而且随着租赁费用越来越廉价，基本不会增加企业的负担。

6 结论

新形势下，煤矿的信息网络安全工作将越来越重要、越来越复杂、越来越艰巨。煤矿管理人员和技术人员一定要从思想上引起高度重视，不断提高安全管理能力和水平，并不断总结经验，从根本上解决网络安全问题。

参考文献：

[1] 山西省煤炭厅《关于印发山西省煤矿安全质量标准化考核评级办法的通知》（晋煤安发〔2013〕500号）2013.05.

[2] 国家煤矿安监局《关于印发〈煤矿安全监控系统升级改造技术方案〉的通知》（煤安监函〔2016〕5号）2016.12.

[3] 山西省煤炭厅《关于印发〈山西省煤炭专网升级改造技术方案〉的通知》（晋煤办信发〔2010〕1687号）2010.12.

[4] 山西省煤炭厅《关于加快山西省煤炭监管信息平台建设的实施意见》（晋煤办发[2016]251号）2016.12.

[5] 何同林,冯丹.煤炭企业网络信息安全问题分析及对策探讨[J].矿业安全与环保,2007(3):66-68.

[6] GB/T 22240-2008信息系统安全等级保护定级指南[S].

[7] GB／T18336《信息技术安全性评估准则》[S].