文章编号:1671-251X(2019)08-0043-05 DOI:10.13272/j.issn.1671-251x.17381

煤矿工业互联网信息安全风险评估

孟庆勇[1,2,3], 顾闯[1,2,3]

(1.煤炭科学技术研究院有限公司,北京 100013;
2.煤矿应急避险技术装备工程研究中心,北京 100013;
3.北京市煤矿安全工程技术研究中心,北京 100013)

扫码移动阅读

摘要:针对煤矿工业互联网信息安全防护手段多应用于较小区域、难以对整体信息安全风险进行评估的问题,提出了一种基于静态和动态2个维度的煤矿工业互联网信息安全风险评估方法。该方法根据《信息安全技术 网络安全等级保护基本要求》及GB/T 34679—2017《智慧矿山信息系统通用技术规范》,对煤矿信息系统已实施的安全防护条例进行特征化转换,建立各系统中安全防护要求的关联系数矩阵,进而计算出系统实际实施的安全防护条例数量;再结合威胁发生数和发生更高级风险的概率,建立安全风险评估模型,进而对煤矿工业互联网进行信息安全风险评估。测试结果表明,该方法能有效评估煤矿工业互联网信息安全状况,指导煤矿企业进行信息安全风险分析、安全防护规划设计及实施,从而降低煤矿工业互联网信息安全风险。

关键词:煤矿工业互联网;智慧矿山;信息系统;信息安全;安全风险评估;安全防护
中图分类号:TD67 文献标志码:A

Information security risk assessment of industrial Internet of coal mine

MENG Qingyong[1,2,3], GU Chuang[1,2,3]

(1.China Coal Research Institute, Beijing 100013, China;
2.Coal Mine Emergency Rescue Technology Equipment Research Center, Beijing 100013, China;
3.Beijing Mine Safety Engineering Technology Research Center, Beijing 100013, China)

Abstract: For problems that information security protection measures of industrial Internet of coal mine were mostly applied to small areas and it was difficult to assess the whole information security risk, an information security risk assessment method of industrial Internet of coal mine was proposed which was based on static and dynamic dimensions. In the method, security protection regulations carried out in coal mine information systems are feature-transformed according to *Information Security Technology-baseline for Classified Protection of Cybersecurity* and GB/T 34679-2017 *General Technical Specifications for Smart Mine Information Systems*, and a correlation coefficient matrix of security protection requirements for each system is established, so as to calculate the number of security protection regulations which are actually carried out in the system. Then, a security risk assessment model is established by combining with risk number and probability of higher risk category, so as to assess information security risk of industrial Internet of coal mine. The test result shows that the method can effectively assess information security status of industrial Internet of coal mine, and guide coal mine enterprise to analyze information security

收稿日期:2019-06-30;**修回日期**:2019-07-18;**责任编辑**:李明。
基金项目:中国煤炭科工集团有限公司科技创新基金面上项目(2017MS002);天地科技股份有限公司科技创新创业资金专项项目(2018-TD-MS003);北京市科委计划项目(Z171100002317020)。
作者简介:孟庆勇(1982—),男,山东梁山人,副研究员,硕士,现主要从事矿井通信、监控和企业信息安全方面的研究工作,E-mail:mengqingyong@ccrise.cn。
引用格式:孟庆勇,顾闯.煤矿工业互联网信息安全风险评估[J].工矿自动化,2019,45(8):43-47.
MENG Qingyong, GU Chuang. Information security risk assessment of industrial Internet of coal mine[J]. Industry and Mine Automation,2019,45(8):43-47.

risk and design and carry out security protection plan, so as to decrease information security risk of industrial Internet of coal mine.

Key words: industrial Internet of coal mine; smart mine; information system; information security; security risk assessment; security protection

0 引言

近年来,随着信息技术的发展,云计算、物联网等新技术应用增多,煤炭企业生产、管理、经营等活动对信息系统的依赖不断增加。由互联网、井上下区域信息系统组成的煤矿工业互联网体系面临信息安全风险感知和防护问题。目前煤炭企业信息安全风险防护主要围绕 3 个方面展开并实施[1]:① 网络区域间隔离防护,如部署边界安全网关;② 主要系统或设施的信息安全风险隔离防护,如部署系统防火墙;③ 关键生产设施区域隔离防护,如部署井下工控网闸设备。这导致煤矿工业互联网信息安全防护手段多集中在较小区域上应用,难以对整体信息安全风险进行评估或感知[2]。

本文基于大数据分析技术,采用静态、动态 2 个维度,对煤矿工业互联网整体信息安全风险进行评估。静态评估维度是通过分析煤矿已实施的安全防护条例数量与 2019 版《信息安全技术 网络安全等级保护基本要求》(以下简称新标准)中规定的安全防护条例数量的比值,实现对煤矿工业互联网信息安全风险的评估。动态评估维度是根据煤矿工业互联网日常运行过程中统计的信息安全风险记录次数,结合泊松分布与卡方统计,得出威胁发生数和发生更高级风险的概率[3]。基于静态和动态 2 个维度的联合评估,指导煤矿企业采取相应的安全防护措施,不断减少安全防护潜在的风险问题。

1 煤矿工业互联网信息安全防护要求分析

新标准中,信息安全防护条例可分为通用安全、云计算安全、移动互联网安全、物联网安全、工业控制系统安全 5 个方面的要求。鉴于行业特点和系统实现功能,煤矿工业互联网可分为井上办公互联网、煤矿工业环网、井下工控网 3 个区域。GB/T 34679—2017《智慧矿山信息系统通用技术规范》将煤矿工业互联网信息系统分为生产类(采煤、掘进、运输、提升、供电等)、健康安全类(安全监测、人员定位、视频监控等)和技术与保障类(ERP(Enterprise Resource Planning,企业资源计划)、综合调度指挥、门户等)3 类。生产类系统单独或区域协同作业,大多采用物联网和工业控制技术融合,由井下工控网承载;健康安全类系统应用大量监测传感器,会产生海量环境数据,实现井下采集与井上监测联动,主要由煤矿工业环网承载[4];技术与保障类系统通过部署大数据和云计算平台,对企业管理、经营、安全生产等信息进行支撑,以实现智慧矿山各环节精准展示和智能决策[5]。依据智慧矿山 3 类信息系统的组成架构、技术协议和数据内容,对比新标准中安全防护条例,统计各类信息系统应完成的安全防护条例占新标准中所有安全防护条例的比例(特征化转换),结果见表 1。

表 1 智慧矿山各类信息系统安全防护条例特征化转换结果

Table 1 Feature-transformation results of security protection regulations in each information system of smart mine

煤矿工业互联网区域	智慧矿山信息系统	各类信息系统应完成新标准中安全防护条例的比例/%				
		通用安全要求(共 115 条)	云计算安全要求(共 43 条)	移动互联网安全要求(共 22 条)	物联网安全要求(共 18 条)	工业控制系统安全要求(共 19 条)
井下工控网	综掘工作面控制系统	31	30	41	67	74
	带式运输控制系统	16	19	41	72	84
	矿山供电控制系统	21	28	59	50	95
	矿井提升控制系统	13	16	55	67	89
煤矿工业环网	安全监测系统	51	10	41	44	37
	人员及车辆定位系统	42	93	36	28	58
	视频监控系统	77	88	82	61	32
井上办公互联网	ERP 系统	87	63	91	17	11
	综合调度指挥系统	95	44	95	28	21
	智慧矿山门户	90	35	95	28	21

由表 1 可知,煤矿工业互联网中井下工控网区域对于工业控制系统、物联网安全要求,煤矿工业环网区域对于云计算安全要求,井上办公互联网区域对于通用安全要求中应完成的安全防护条例具有较高比例,而对于其他安全要求中应完成的安全防护条例比例较低,说明某个区域中相应的安全防护缺失会对其主要信息系统带来潜在的安全风险[6-7]。

对煤矿工业互联网区域中智慧矿山信息系统的安全防护进行分析[8]。以安全监测系统为例,针对新标准中的 9 类安全防护要求,结合安全监测系统组成架构,采用欧几里德距离分析法计算该系统中 9 类安全防护要求之间的关联系数(即新标准 9 类安全防护要求中安全防护条例数量与实际安全防护条例数量之间的平面距离),得到关联系数矩阵,见表 2。关联系数越大,表明实际的安全防护条例与新标准中安全防护条例内容的关联性越强。

表 2　安全监测系统安全防护条例关联系数

Table 2　Correlation coefficient of security protection regulations of safety monitoring system

安全防护要求		通用安全要求					云计算安全要求	移动互联网安全要求	物联网安全要求	工业控制系统安全要求
		网络架构	访问控制	入侵防范	安全审计	接入控制				
通用安全要求	网络架构	1	0.736	0.855	0.672	0.910	0.562	0.145	0.288	0.011
	访问控制	0.736	1	0.797	0.561	0.436	0.464	0.733	0.789	0.334
	入侵防范	0.855	0.797	1	0.771	0.911	0.383	0.574	0.185	0.607
	安全审计	0.672	0.561	0.771	1	0.211	0.632	0.338	0.498	0.114
	接入控制	0.910	0.436	0.911	0.211	1	0.115	0.531	0.491	0.772
云计算安全要求		0.562	0.464	0.383	0.632	0.115	1	0.443	0.334	0.482
移动互联网安全要求		0.145	0.733	0.574	0.338	0.531	0.443	1	0.289	0.219
物联网安全要求		0.288	0.789	0.185	0.498	0.491	0.334	0.289	1	0.691
工业控制系统安全要求		0.011	0.334	0.607	0.114	0.772	0.482	0.219	0.691	1

从表 2 可看出,智慧矿山信息系统在网络架构、入侵防范、接入控制 3 个方面的安全防护条例内容的关联性最强,关联系数超过 0.8,这说明在煤矿工业互联网体系中这 3 个方面面临的安全风险属于同一聚类[9],在信息安全风险评估过程中应进行强关联,需同时存在。物联网安全要求与工业控制系统安全要求之间的关联系数为 0.6～0.7,高于各自与云计算安全要求之间的关联性[5],说明井下工控网区域信息安全风险评估中物联网和工业控制系统的安全防护条例权重应大于云计算。如果安全防护要求关联系数基本上都低于 0.5,则为弱关联或无关联,不参与评估。

2　煤矿工业互联网信息安全风险评估模型

首先定义静态评估维度,将新标准中的安全防护条例特征化,得到全事件模式集合 P,再通过现场调研确认实际事件模式集合 E[10]。

$$P = \bigcup_{i=1}^{5} P_i \tag{1}$$

$$E = E_g + E_c + E_u \tag{2}$$

式中:$P_i = \{p_i^1, p_i^2, \cdots, p_i^n\}$,$i = 1, 2, \cdots, 5$,分别代表通用安全、云计算安全、移动互联网安全、物联网安全、工业控制系统安全 5 个方面的安全防护要求,n 为新标准中特征化转换后的安全防护条例数量,p_i^n 为 i 方面安全防护要求中第 n 条安全防护条例;E_g,E_c,E_u 分别为井上办公互联网、煤矿工业环网、井下工控网的实际事件模式[11]。

设智慧矿山信息系统 9 类安全防护要求中安全防护条例数为 L_j($j = 1, 2, \cdots, 9$),关联系数为 μ_j,对属于强关联的安全防护要求进行和运算,对权重关联的安全防护条例进行关联系数乘积运算[12],最终得出实际的安全防护条例实施数量(实际事件模式)。

$$E_g = L_1 + L_3 + L_5 + \mu_4 L_4 \tag{3}$$

$$E_c = L_6 + \mu_4 L_4 \tag{4}$$

$$E_u = L_8 + L_9 + \mu_2 L_2 + \mu_5 L_5 \tag{5}$$

然后定义动态评估维度[13],包括威胁发生数 C_i 和发生更高级风险的概率 T_i。其中 C_i 表示对煤矿工业互联网运行中采集的动态信息源进行挖掘后获得的异常威胁数。

工业互联网体系面临的信息安全风险概率满足泊松分布的 3 个条件:信息安全风险是小概率事件;信息安全风险事件是独立的,不会互相影响;一段时间内信息安全风险发生概率相对稳定[14]。发生更高级风险的概率 T_i 为根据泊松分布计算公式(式(6))得出的一段时间内大于信息安全风险记录次数平均值 λ 的卡方统计量。

$$Q_l = \frac{\exp(-\lambda)\lambda^k}{k!} \tag{6}$$

式中：Q_l 为第 l（$l=1,2,\cdots$）个大于 λ 的泊松分布期望值[15]；$k=\lambda+1,\lambda+2,\cdots,\lambda+l$。

则有

$$T_i=\sum\frac{(Q_l-\lambda)^2}{\lambda} \tag{7}$$

由此可得基于静态和动态 2 个维度的煤矿工业互联网信息安全风险评估模型：

$$R_i=\frac{V}{C_iT_i} \tag{8}$$

式中 V 为实际事件模式集合与全事件模式集合的比值，即 $V=E/P$。

采用大数据和 Python 软件技术，将煤矿工业互联网信息安全风险评估模型进行可视化展现。

3 煤矿工业互联网信息安全风险评估流程

煤矿工业互联网信息安全风险评估流程如图 1 所示。

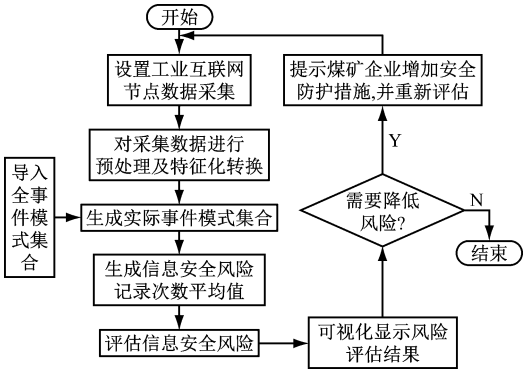

图 1 煤矿工业互联网信息安全风险评估流程

Fig. 1 Information security risk assessment process of industrial Internet of coal mine

煤矿工业互联网信息安全风险评估过程中首先进行数据采集，主要采集煤矿工业互联网体系中已部署实施的安全防护措施信息（防火墙防护记录、网络路由信息、终端入网信息等）并对其进行特征化转换。然后根据全事件模式集合、实际事件模式集合、威胁发生数、采集时间（如以月或周为单位）内信息安全风险记录次数平均值等信息，利用安全风险评估模型进行评估。最后，煤矿企业根据信息安全风险评估的可视化显示结果，结合自身信息安全要求和规划设计，制定并部署相应的安全防护措施，进行下一周期的安全风险评估，最终将信息安全风险降低至新标准要求。

4 煤矿工业互联网信息安全风险评估测试

在地面模拟煤矿工业互联网，采用信息安全风险评估模型对其进行风险评估测试，准备如下。

（1）部署 2 个井上办公互联网子系统：互联网接入带宽为 10 Mbit/s，设置 2 个公网 IP、1 个 ERP 系统供应链模块、1 个移动办公 APP。

（2）部署 2 个工业环网子系统：设置数字化安全监测系统和人员定位系统上位机服务器各 1 台。

（3）部署 2 个井下工控网络子系统：设置 2 台 PLC、2 个 RS232 转换器、1 个 4G 基站。

对网络信息安全风险进行初始评估，设置 7 处安全风险采集点：1 处互联网防火墙、1 处服务器、2 处上位机、2 处核心交换机端口、1 处移动准入服务器。基于静态评估维度计算得 6 个子系统初始完成新标准中安全防范条例的比例为 50%。各系统运行 15 d 后统计信息安全风险记录，可知共发生安全风险 115 次。

根据网络信息安全风险初步评估结果，对模拟网络增加 5 处安全防护措施实施点并设置安全风险采集点，包括 1 处数据库审计、1 处工业防火墙、1 处行为审计、2 处防病毒软件。重新运行煤矿工业互联网信息安全风险评估流程，计算得完成新标准中安全防范条例的比例为 68%；运行 15 d 后，统计的信息安全风险发生次数为 214 次。

对模拟网络进行的 2 次信息安全风险评估结果如图 2 所示，其中节点为评估结果，红色为初始评估结果，蓝色为采取相应安全防护措施后的评估结果。从图 2 可看出煤矿工业互联网信息安全风险评估模型能够准确反映通用安全、云计算安全、移动互联网安全、物联网安全、工业控制系统安全 5 个方面新增安全防护措施的评估值，指导煤矿企业进一步补充信息安全防护短板，最终实现 5 个方面安全防护效果的均衡。

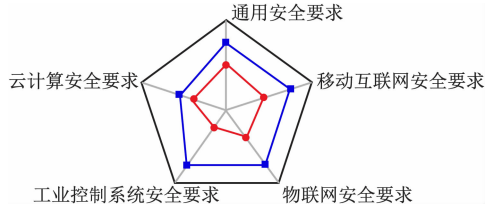

图 2 煤矿工业互联网信息安全风险评估结果

Fig. 2 Information security risk assessment results of industrial Internet of coal mine

5 结论

（1）基于新标准中安全防护要求，提出了一种基于静态和动态 2 个维度的煤矿工业互联网信息安全风险评估方法。该方法根据新标准及 GB/T 34679—2017 对煤矿信息系统实施的安全防护条例进行特征化转换，建立各系统中安全防护要求的关联系数矩阵，进而计算出系统实际实施的安全防护条例数量；再结合威胁发生数和发生更高级风险的

概率,建立安全风险评估模型,进而对煤矿工业互联网进行信息安全风险评估。

(2) 在地面组建了煤矿工业互联网 6 个子系统并进行测试,根据信息安全风险评估结果增加了网络安全防护措施,同时增加了安全风险采集点。测试结果表明,煤矿工业互联网信息安全风险评估方法能够有效评估煤矿工业互联网信息安全状况,指导煤矿企业进行信息安全风险分析、安全防护规划设计及实施,从而降低煤矿工业互联网信息安全风险。

参考文献(References):

[1] 郭斌. 互联网+煤矿安全信息化关键技术及应用构架[J]. 科技创新导报,2018,15(3):41-42.

[2] 薛东. 煤矿安全管理的可视化技术发展探析[J]. 智能城市,2018,4(8):83-84.

[3] 郜彤,刘传安. 基于大数据分析的煤矿安全风险预测系统研究[J]. 煤炭工程,2018,50(7):173-176.
GAO Tong,LIU Chuan'an. Study on coal mine safety risk prediction system based on big data analysis[J]. Coal Engineering,2018,50(7):173-176.

[4] 武福生. 矿山工业互联网技术体系架构[J]. 煤矿安全,2018,49(8):128-130.
WU Fusheng. Architecture of Internet technology system for mining industry[J]. Safety in Coal Mines,2018,49(8):128-130.

[5] 孙继平. 煤矿信息化与智能化要求与关键技术[J]. 煤炭科学技术,2014,42(9):22-25.
SUN Jiping. Requirement and key technology on mine informationalization and intelligent technology[J]. Coal Science and Technology,2014,42(9):22-25.

[6] 杜晓龙. 煤矿安全测控网络建设研究[J]. 能源与节能,2017(11):57-58.
DU Xiaolong. Research on the construction of measurement and control network for safety in coal mines[J]. Energy and Energy Conservation, 2017(11):57-58.

[7] 闫振国,常心坦,范京道,等. 面向矿井用风点的通风网络安全分区方法研究[J]. 煤炭科学技术,2019,47(2):71-76.
YAN Zhenguo,CHANG Xintan,FAN Jingdao,et al. Air-consume area oriented ventilation safety sub-region partition in coal mine[J]. Coal Science and Technology,2019,47(2):71-76.

[8] 孙继平. 煤矿井下安全避险"六大系统"建设指南[M]. 北京:煤炭工业出版社,2012.

[9] 苏艳琴,张光轶,杨小林. 层次分析法在信息系统风险评估中的应用分析[J]. 舰船电子工程,2017,37(6):75-78.
SU Yanqin, ZHANG Guangyi, YANG Xiaolin. Application of AHP in information system risk assessment[J]. Ship Electronic Engineering, 2017, 37(6):75-78.

[10] 马志程,杨鹏,张雪锋,等. 云计算环境下的电力系统动态风险评估方法研究[J]. 现代电子技术,2016,39(18):165-167.
MA Zhicheng,YANG Peng,ZHANG Xuefeng,et al. Study on dynamic risk assessment method of electric power system in cloud computing environment[J]. Modern Electronics Technique, 2016, 39(18): 165-167.

[11] 谭章禄,吴琦. 煤炭安全管理可视化方式评价研究[J]. 煤矿安全,2018,49(2):230-233.
TAN Zhanglu, WU Qi. Study on visualization evaluation of coal safety management[J]. Safety in Coal Mins,2018,49(2):230-233.

[12] 谭章禄,陈孝慈. 基于复杂网络分析的煤矿安全隐患管理研究[J]. 工矿自动化,2019,45(6):86-90.
TAN Zhanglu,CHEN Xiaoci. Research on coal mine safety hidden danger management based on complex network analysis[J]. Industry and Mine Automation, 2019,45(6):86-90.

[13] 鲁华栋,闫兵,岳小冰. 基于 AHP-SVM 的信息系统风险评估[J]. 计算机系统应用,2016,25(10):141-145.
LU Huadong, YAN Bing, YUE Xiaobing. Risk evaluation of information system security based on analytic hierarchy process and support vector machine[J]. Computer Systems & Applications, 2016, 25(10):141-145.

[14] 吴开兴,王文鼎,李丽宏. 煤矿企业工业控制系统入侵检测算法[J]. 工矿自动化,2018,44(11):75-79.
WU Kaixing,WANG Wending,LI Lihong. Intrusion detection algorithm for industrial control system of coal mine enterprise[J]. Industry and Mine Automation,2018,44(11):75-79.

[15] 董晓宁,赵华容,李殿伟,等. 基于模糊证据理论的信息系统安全风险评估研究[J]. 信息网络安全,2017,17(5):69-73.
DONG Xiaoning,ZHAO Huarong,LI Dianwei,et al. Research on information systems security risk assessment based on fuzzy theory of evidence[J]. Netinfo Security,2017,17(5):69-73.